GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

CORPORANSOM

DISCLAIMER

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains recommendations on how to protect against future attacks. The details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. Any information outlined in the report is not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

HI-TECH CRIME TRENDS 2021/2022

Corporansom: threat number one

PART 2

The history and analysis of affiliate programs and trends in the ransomware market

TABLE OF CONTENTS

GROUP-IB HI-TECH CRIME TRENDS REPORT

00

The Hi-Tech Crime Trends report analyzes cyberattacks, examines how the cybercrime industry functions, and forecasts upcoming changes in the threat landscape for various sectors of the global economy. Group-IB has published the report every year since 2012, integrating valuable data and key insights that the team has gained through over 70,000 hours of experience in responding to cybersecurity incidents worldwide.

The information provided in Hi-Tech Crime Trends enables businesses, NGOs, governments, and law enforcement agencies around the world to fight cybercrime and help potential victims. Intended for IT directors, heads of cybersecurity teams, SOC analysts, incident responders, and other security professionals, the Hi-Tech Crime Trends report serves as a practical guide for strategic and tactical planning.

Using unique tools for tracking threat-actor infrastructures and through careful analysis by specialists worldwide, every year Group-IB experts identify and confirm patterns of cyber threats. This information serves as a basis for forecasts, which have proven accurate every year since the first Hi-Tech Crime Trends report was published. These forecasts help companies around the world build effective cybersecurity strategies with relevant threats in mind.

The forecasts and recommendations contained in Hi-Tech Crime Trends are aimed at reducing financial losses and infrastructure downtime. They are also designed to help organizations take preventive measures to counteract targeted attacks, espionage, and cyber-terrorism operations.

Group-IB strongly believes that the continual exchange of data, combined with lasting partnerships between private companies and international law enforcement agencies, is the most effective way to combat cybercrime. Cybersecurity awareness helps preserve and protect digital spaces and freedom of communication. It is to these ends that the Hi-Tech Crime Trends report is published.

INTRODUCTION 01

The first malware prototype that vaguely resembles today's ransomware was spread using floppy disks and compact disks (CDs) as early as **1989** and was used to extort money from users through social engineering techniques. The scam was relatively small-scale: the Trojan could not encrypt data and its creators were unaware of monetization methods other than deception.

The first ransomware-as-a-service (RaaS) affiliate programs came into existence about twenty years after the first malware prototype. Data leak sites (DLSs)— websites where the data belonging to companies who refuse to pay a ransom are published— emerged around a decade later.

During this time, the term ransomware became a synonym for cyber extortion and a technological foundation for this shadow industry. Ransomware has developed into the biggest threat to the commercial and government sectors worldwide, while ransomware operators and affiliate program participants make millions of dollars by damaging companies around the globe.

Thousands of threat actors involved in network breaches, traffic generation, malware development and delivery, and targeted attacks have found themselves in high demand in this massive new trend in cybercrime. Thus a ransomware cyber empire was born.

In the first 11 months of 2021, over **60% of all incidents investigated by Group-IB involved ransomware**. The RaaS market's active growth, coupled with many financially motivated groups shifting their focus to ransomware attacks, has significantly affected how many such incidents are investigated.

over 60%

of all incidents investigated
by Group-IB involved ransomware

To understand how cybercrime transitioned from advanced targeted attacks to non-targeted affiliate malware distribution programs, we need to look into the history of how these services developed, which is what this paper aims to do.

By using the capabilities of Group-IB's **Threat Intelligence & Attribution** system, which stores historical data about malware, threat actors, and their connections from the last 15 years, Group-IB looks in detail into major malware samples, tactics, techniques, and tools used by threat actors, as well as into events in the dark web that led to the rise of the ransomware empire.

Historical milestones: from $13 to $240,000,000

Extortion used to be a common technique for threat actors who carried out DDoS attacks to make money off their victims. It became popular mainly because content delivery networks (CDNs) were rare, which made it extremely difficult for regular users to protect themselves against DDoS attacks. The emergence of CDNs with built-in DDoS protection forced threat actors to devise other monetization methods.

Malware that could encrypt data on a victim's device emerged in 2004. The malware was called PGPcoder and it cost 13 dollars to decrypt the victim's data — a negligible sum by today's standards.

2004

the year that the first ransomware appeared — PGPcoder

PGPcoder failed to become popular because it only targeted individuals and significantly strained victims' then low-performance machines. This made it easy to detect malware activity.

Towards the end of the 2000s, threat actors decided to adopt a simpler approach: blocking certain operating system functionalities and demanding a ransom. This marked the beginning of the **WinLock** era, which brought forth a phenomenon known today as "ransomware as a service" (RaaS).

The year 2010 saw the appearance of malware developers who realized that developing, improving, and distributing Trojans all at the same time is challenging, so they started paying third-parties for traffic generation and malware downloads to victim machines. To optimize their activity, they created the first affiliate program prototypes, which all modern RaaS model services later adopted and improved upon. Locker ransomware activity continued until 2013, when the ransomware called **Cryptolocker** emerged.

≈2009

the beginning of the era of winlockers and the emergence of Ransomware-as-a-Service (RaaS)

The popularity of CryptoLocker and countless media reports about 2013–2014 attacks involving CryptoLocker sent the number of crypto ransomware related affiliate programs and sale offers on underground forums skyrocketing. Yet most ransomware victims were individuals.

In 2016–2017, the world faced a wave of attacks involving **WannaCry** and **NotPetya**, which made businesses think seriously about this threat for the first time.

In 2018, the first professional affiliate program called **GandCrab** emerged. It differed from previous attempts in that threat actors created dedicated teams for different activities, one of which was attacking major enterprises. The phenomenon was later dubbed **big game hunting**.

Subsequent years showed that it was big game hunting that had become the main target for all affiliate programs. The next global change was brought by the threat groups **Snatch** and **Maze**, when in addition to encrypting companies' data, they started downloading it from their victims' networks and publishing it on their own resources. This markedly increased the conversion rate (share of attacked companies that pay the ransom) and the technique has been widely adopted.

2018

the emergence of the affiliate program GandCrab, which targeted large companies only

What happened next put ransomware in the headlines of media outlets worldwide: the victims included Garmin, JBS, Colonial Pipeline, Kaseya, and MediaMarkt, from which **Hive** ransomware operators demanded **$240 million**.

Between H2 2020 and H1 2021 alone, **21 new active affiliate** programs appeared in the underground and 28 DLSs were created and used by threat actors to publish the data of **2,371 companies**.

In this report, Group-IB looks into how and why the ransomware industry has developed, provides in-depth analyses of certain affiliate programs from within, and shares statistics on the countries and industries that are attacked most often.

KEY TRENDS 02

DLSs WITH FAKE DATA ABOUT ATTACKS HAVE EMERGED

A DLS with fake data about attacks has been identified for the first time.

SOME COMPANIES PAY AFTER RANSOMWARE ATTACKS

About 30% of companies pay the ransom.

THE LIST OF ATTACKED COUNTRIES HAS NOT CHANGED

The United States (49.2%) and Canada (5.6%) still have the most ransomware victims. They are followed by France (5.2%), which has replaced the United Kingdom for third place.

THREAT ACTORS ARE ATTACKING THE MOST LUCRATIVE INDUSTRIES

The most often attacked industries are manufacturing (9.6%), real estate (9.5%), and transportation (8.2%).

THE NEW TOP THREE RANSOMWARE HAVE EMERGED

The hacker groups that have conducted the most attacks are Conti (16.5%), Lockbit (11.5%), and Avaddon (7.5%). Maze, which topped the list last year, has ceased to exist.

NOT ALL DATA IS PUBLISHED ON DLS

Only 10% of attacked companies have their data published on DLSs.

THE NUMBER OF NEW PUBLIC AFFILIATE PROGRAMS IS GROWING

The number of new public affiliate programs offered by ransomware operators has increased by 23%, from 17 new programs in H2 2019 – H1 2020 to 21 new ones in H2 2020 – H1 2021.

THE NUMBER OF NEW DLSs IS GROWING

The number of new DLSs has grown by 115%, from 13 new DLSs in H2 2019 – H1 2020 to 28 new ones in H2 2020 – H1 2021.

THE NUMBER OF VICTIMS WHOSE DATA IS SHARED ON DLSs IS GROWING

The number of victims whose data has been published on DLSs has grown by 935%, from 229 (in H2 2019 – H1 2020) to 2,371 (in H2 2020 – H1 2021).

AFFILIATE PROGRAMS ARE BECOMING PRIVATE

Most affiliate programs (87%) have become private, but many can still be joined if the “applicant” knows the threat actors personally.

PAYING A RANSOM DOESN’T PREVENT DATA BEING LEAKED

When companies pay a ransom, many threat actors delete the victim’s data from the DLS, but compromised files may still be available through links.

FORECASTS 03

THE BAN ON AFFILIATE PROGRAMS ON UNDERGROUND FORUMS WILL NOT PREVENT NEW RAAS PROGRAMS FROM EMERGING

The ban on advertising public affiliate programs on underground forums was followed by the emergence of RAMP, a forum that allows ransomware activity. This could mean that the rate at which new affiliate programs emerge will remain the same.

DLSs MAY BECOME A NEW PLATFORM FOR SELLING DATA

Threat actors may start selling data belonging to compromised companies on DLSs. This has occurred before, but it has not become a trend yet.

THE TOP THREE ATTACKED INDUSTRIES WILL REMAIN THE SAME

The most often attacked industries are unlikely to change given that threat actors believe they are the ones that can be monetized the most.

THE NUMBER OF RANSOMWARE VICTIMS AND DLSs WILL GROW

The amount of compromised data posted on DLSs will grow, as will the number of DLSs.

RAAS MARKET HISTORY

04

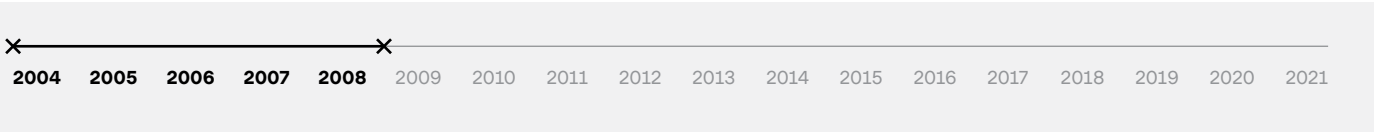
History of the ransomware cyber empire: 1989–2021

Date	Event
January 1989	AIDS Trojan emerges
December 2004	The first quasi-modern crypto ransomware called PGPcoder emerges
November 2005	The first known operating system locker called Krotten emerges
March 2006	The Cryzip crypto ransomware involving ZIP archives emerges
June 2006	The first guides on how to create crypto ransomware appear in the underground
May 2009	The Winlock ransomware is put up for sale on underground forums for the first time
June 2009	Sales of various locker ransomwares surge on forums
July 2009	Articles about developing locker ransomware appear in the underground
January 2010	The first locker ransomware affiliate programs emerge
December 2010	Crypto ransomware returns with Encoder Builder, which is made freely available
July 2011	An improved version of Encoder is sold
January 2012	Locker ransomware with the MBR overwrite functionality appears
September 2012	A series of crypto ransomware attacks starts in Australia
June 2013	The first crypto ransomware affiliate program emerges
September 2013	The first CryptoLocker attacks and affiliate programs begin
December 2013	Known underground users report that the locker ransomware trade is dead and that the crypto ransomware era has begun
January 2014	Many new crypto ransomware and affiliate programs emerge
May 2015	The publicly available crypto ransomware called Tox emerges
November 2015	The ransomware called Chimera is used to attack law firms only and hackers threaten to publish stolen data
November 2015	The first Linux ransomware called Linux.Encoder emerges
December 2015	Many threads on underground forums are created, in which threat actors discuss that only legal entities should be attacked
February 2016	One of the most large-scale and notorious affiliate programs, Cerber ransomware, starts
March 2016	The first macOS ransomware called KeRanger emerges

Date	Event
March 2016	The notorious ransomware called Petya, with the MBR overwrite functionality, emerges
November 2016	Some pieces of ransomware start using Telegram as a command-and-control (C&C) server
May 2017	Attacks involving the ransomware WannaCry, with automatic spreading functionality, begin
June 2017	The ransomware NotPetya, which continued the WannaCry activity, emerges
January 2018	The first modern ransomware affiliate program called GandCrab is born and the targeting of legal entities begins
March 2019	The first RaaS called Snatch, which uses the double extortion technique, is released
May 2019	The ransomware called Maze is created
December 2019	The first DLS (Maze) appears
June 2020	The number of new RaaS affiliate programs surges
May 2021	"No more ransoms!": publishing RaaS on underground forums is banned
July 2021	Ramp, a ransomware-related forum, emerges

Inception

2004—2008



PGPcoder, Cryzip, Archiveus

Retrospective analysis of how the ransomware cyber empire evolved will help shed light on how businesses worldwide lose millions of dollars to cybercriminals today.

Let's first define what the commonly-used term ransomware means. Ransomware's key feature is blocking access to a system or files and demanding a ransom to restore it.

The idea of demanding ransoms was borrowed from another threat that was popular in the early 2000s: DDoS attacks. At the time, threat actors sent their victims emails threatening to carry out DDoS attacks and demanding that the victims pay a certain sum to avoid being attacked. Threat actors made good money on this type of blackmail because businesses were not prepared to experience down time or counteract such attacks. Following the emergence of CDNs with integrated anti-DDoS functionality, however, the commercial potential of such incidents dropped. Threat actors started looking for new ways of conducting extortion attacks.

Secondly, ransomware has two subgroups: locker ransomware and crypto ransomware.

- **Locker ransomware** blocks access to a device (e.g., blocks the victim's access to MS Windows unless an additional password is entered).
- **Crypto ransomware** finds and encrypts valuable data found on the victim's device.

Interestingly, the ransomware market started with crypto ransomware, then switched to locker ransomware, and has now switched back to crypto ransomware. This can be seen **above**.

This report does not analyze the first proto-ransomware called **AIDS Trojan**[1], which was distributed on floppy disks as early as **1989**. Hackers used AIDS (also known as Aids Info Disk and PC Cyborg Trojan) to extort money from users, citing a license agreement with a non-existent corporation called PC Cyborg Corporation for which victims had to pay, otherwise AIDS would hide catalogs and encrypt the names of all files on the C drive:

Here and below you can go to the "Trojans" page with a detailed description of the Trojans

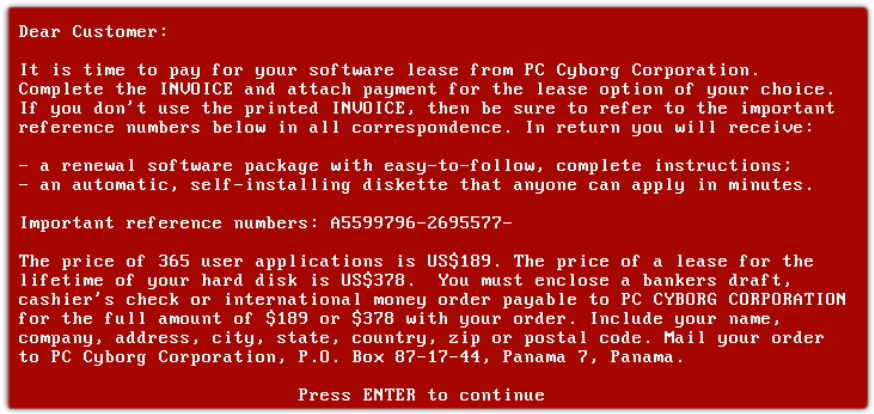


Fig. 1. A message from the developers of AIDS Trojan, 1989

Group-IB has also left out the fake antivirus family called **Spysheriff** from this report. The antivirus was used to extort money by threatening to infect a user's computer with many pieces of malware.

One of the first relatively modern pieces of crypto ransomware emerged in late 2004. At the time, users on many IT resources complained that they had been infected with malware that had encrypted almost all their important files using the algorithm called **CRZ**. On each victim device, a special text file (which we now call a ransom note) was generated. This is a message from the ransomware operators saying that the victim's data has been encrypted and that the victim needs to contact the threat actors via email to decrypt it. After writing to the ransomware operators, victims received a link to the threat actors' website, where they could buy a decoder for **$13**. The header of every encrypted file contained the inscription **PGPcoder**[2], from which the first crypto ransomware derives its name. The malware mainly had targets in Russia.

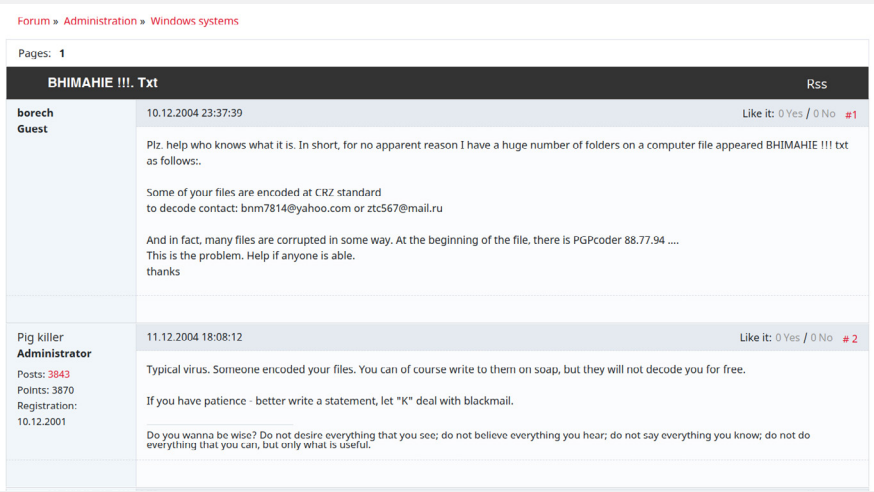


Fig. 2. A message from a user about files encrypted by PGPCoder, 2004

Group-IB specialists have seen several malicious campaigns that spread PGPcoder. One was in December 2004 and another in June 2005. The ransomware was distributed through mailouts of .doc files with malicious macros. In 2006, the developer improved the encryption algorithm and switched to RSA.

PGPcoder marked the beginning of the third wave of ransomware Trojans that started in 2004 and continued until 2008.

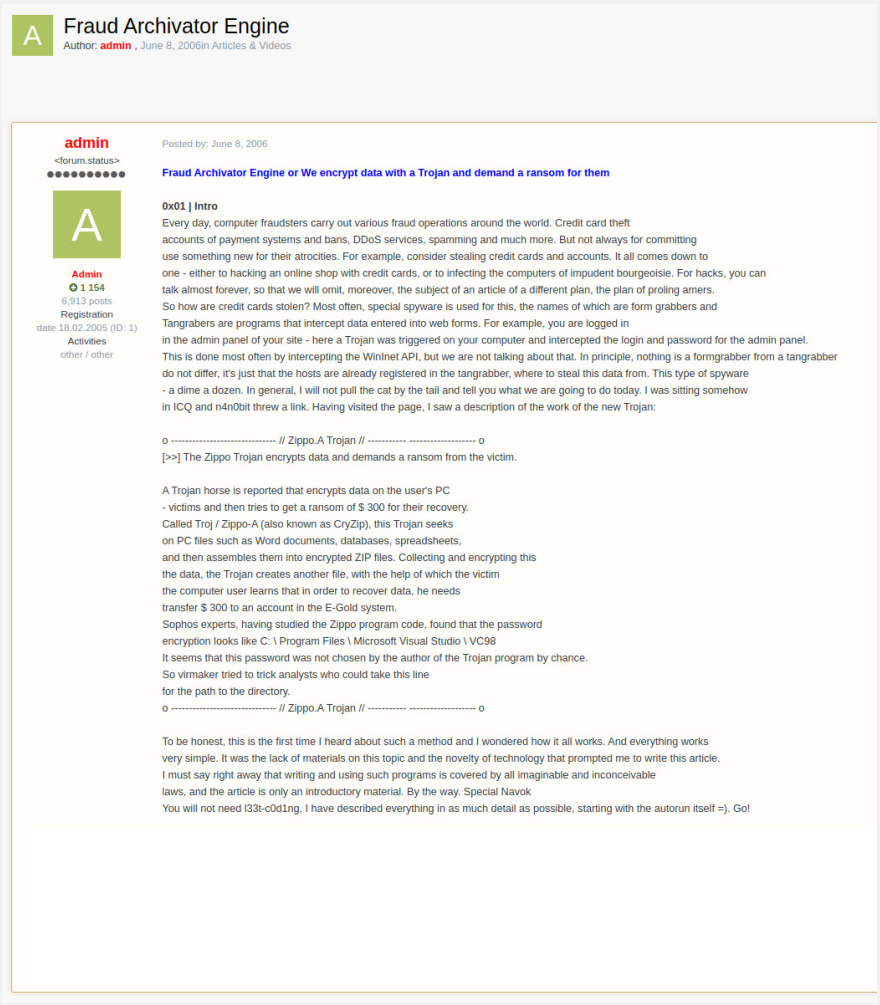
Traditionally, the testing ground for honing techniques has been Russia: the Trojan's victims were in Russia and other CIS (the Commonwealth of Independent States) countries. Only two years later did the threat actors start attacking targets in other parts of the world.

March 2006 saw the emergence of the malware called **Cryzip**[3], which used a simpler logic to encrypt files: it archived every file in a password-protected ZIP archive and deleted the original. The malware had a text file containing a ransom demand in English. Unzipping the files required a password, for which the threat actors demanded a ransom. At the time, E-Gold was used as the payment system.

After **Cryzip's** successful campaigns, demanding a ransom after encrypting systems gained popularity on underground forums.

Cryzip was even called a new generation of Trojans. In June 2006, for instance, an administrator on exploit.in (a notorious underground forum) published a guide on how to develop malware based on Cryzip*.

* https://forum.exploit.in/topic/3175/?tab=comments#comment-18200



Fraud Archivator Engine
Author: admin , June 8, 2006in Articles & Videos

admin
<forum.status>

Admin
1 154
6,913 posts
Registration
date 18.02.2005 (ID: 1)
Activities
other / other

Posted by: June 8, 2006

Fraud Archivator Engine or We encrypt data with a Trojan and demand a ransom for them

0x01 | Intro
Every day, computer fraudsters carry out various fraud operations around the world. Credit card theft
accounts of payment systems and bans, DDoS services, spamming and much more. But not always for committing
use something new for their atrocities. For example, consider stealing credit cards and accounts. It all comes down to
one - either to hacking an online shop with credit cards, or to infecting the computers of impudent bourgeoisie. For hacks, you can
talk almost forever, so that we will omit, moreover, the subject of an article of a different plan, the plan of proling amers.
So how are credit cards stolen? Most often, special spyware is used for this, the names of which are form grabbers and
Tangrabers are programs that intercept data entered into web forms. For example, you are logged in
in the admin panel of your site - here a Trojan was triggered on your computer and intercepted the login and password for the admin panel.
This is done most often by intercepting the WinInet API, but we are not talking about that. In principle, nothing is a formgrabber from a tangrabber
do not differ, it's just that the hosts are already registered in the tangrabber, where to steal this data from. This type of spyware
- a dime a dozen. In general, I will not pull the cat by the tail and tell you what we are going to do today. I was sitting somehow
in ICQ and n4n0bit threw a link. Having visited the page, I saw a description of the work of the new Trojan:

o ---------- // Zippo.A Trojan // ---------- ---------- o
[>>] The Zippo Trojan encrypts data and demands a ransom from the victim.

A Trojan horse is reported that encrypts data on the user's PC
- victims and then tries to get a ransom of $ 300 for their recovery.
Called Troj / Zippo-A (also known as CryZip), this Trojan seeks
on PC files such as Word documents, databases, spreadsheets,
and then assembles them into encrypted ZIP files. Collecting and encrypting this
the data, the Trojan creates another file, with the help of which the victim
the computer user learns that in order to recover data, he needs
transfer $ 300 to an account in the E-Gold system.
Sophos experts, having studied the Zippo program code, found that the password
encryption looks like C: \ Program Files \ Microsoft Visual Studio \ VC98
It seems that this password was not chosen by the author of the Trojan program by chance.
So virmaker tried to trick analysts who could take this line
for the path to the directory.
o ---------- // Zippo.A Trojan // ---------- ---------- o

To be honest, this is the first time I heard about such a method and I wondered how it all works. And everything works
very simple. It was the lack of materials on this topic and the novelty of technology that prompted me to write this article.
I must say right away that writing and using such programs is covered by all imaginable and inconceivable
laws, and the article is only an introductory material. By the way. Special Navok
You will not need l33t-c0d1ng, I have described everything in as much detail as possible, starting with the autorun itself =). Go!

Fig. 3. A guide on how to encrypt data using a Trojan, 2006

Interest in the ZIP Trojan Cryzip led to the emergence of a similar malware, **Archiveus** (aka MayArchive), which used RSA-1024 to encrypt files.

Interestingly, at the time there was talk on underground forums that one of the hardest things about this type of malware was obtaining money from the victim— Bitcoin did not yet exist.

Before then, such malware was not put up for sale on underground forums, which suggests that it was either shared through private messages or handled by only one group that both developed and distributed the malware.

Locker, Winlock, and the first affiliate programs

2009—2012

Krotten, Winlock

There used to be another well-known Trojan called **Krotten**[4]. It emerged in 2005, after PGPcoder, and used a different extortion technique. Instead of encrypting files, it edited the registry, which disrupted the system's normal functioning. The malware then displayed a ransom note. The Trojan can be considered locker ransomware.

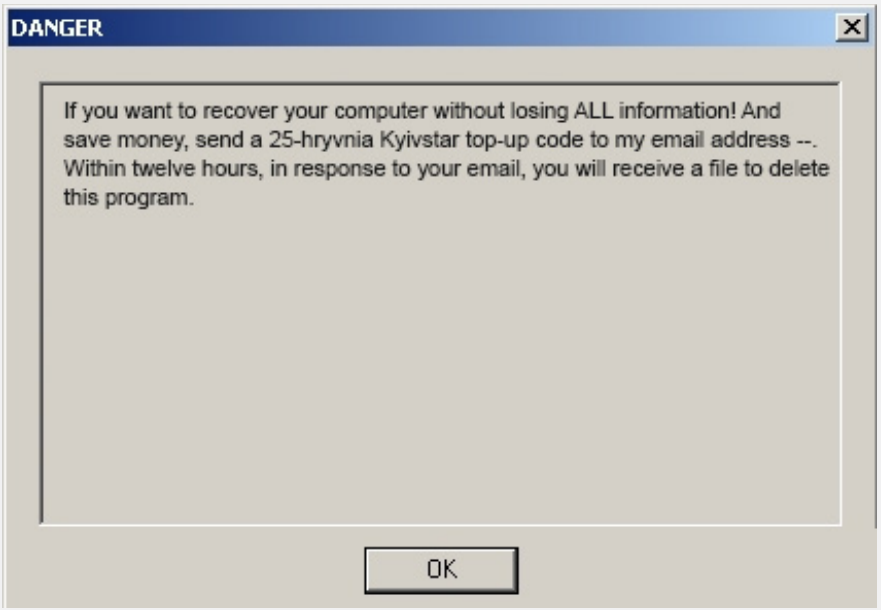


Fig. 4. A Krotten ransom note

Other similar Trojans called SMS lockers went in the same direction. The most notorious among them was a Trojan called **Winlock**[5] (aka Winlocker). Before this malware became common, **Winlock Pro** was popular and performed similar actions, namely blocked access to the operating system after a certain time. It was often used in Internet cafes.

The year 2009 saw many types of such Trojans based on a common idea: they blocked the operating system, using built-in system features, and then showed the user a message saying that the device could be unlocked only by paying the threat actors a ransom. Some Trojans were disguised as banners with erotic content, while others informed victims that unlicensed software had been detected on their device.

Winlock's key innovation was that it was the first malware sold and distributed on underground forums by threat actors. This led to an unprecedented rise in the number of attacks involving this Trojan.

Winlock was put up for sale on underground forums for the first time in late May 2009:

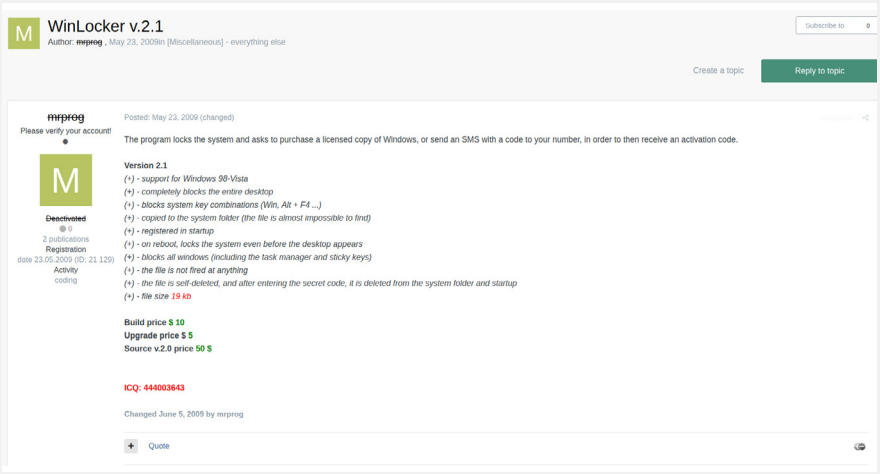


Fig. 5. A message about selling Winlock, 2009

Winlock was relatively cheap: in 2009 the Trojan's source code cost just $50. Many requests to develop full-fledged locker ransomware of this type later appeared on forums.

As early as July 2009, a post about how to create such locker ransomware independently appeared on exploit.in:

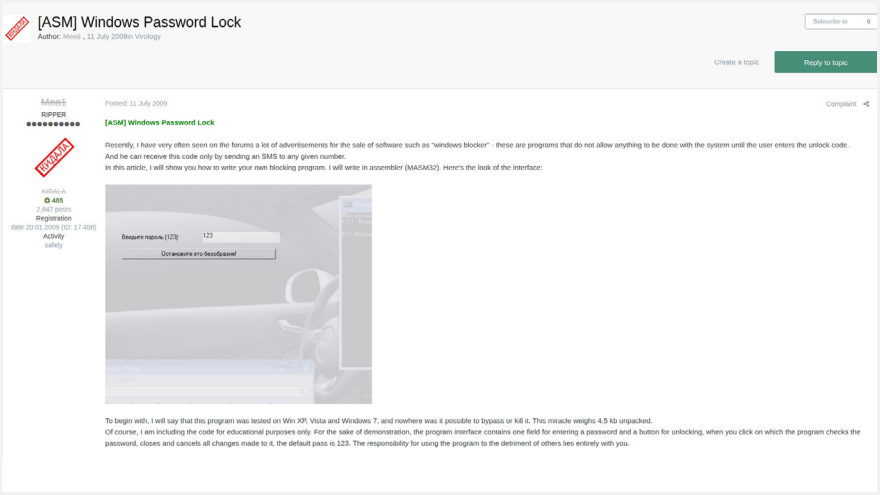


Fig. 6. A guide on creating locker ransomware, 2009

Judging by forum messages, the key problem at the time was finding a bulletproof billing service that would accept paid SMS messages for unlocking machines belonging to the victims.

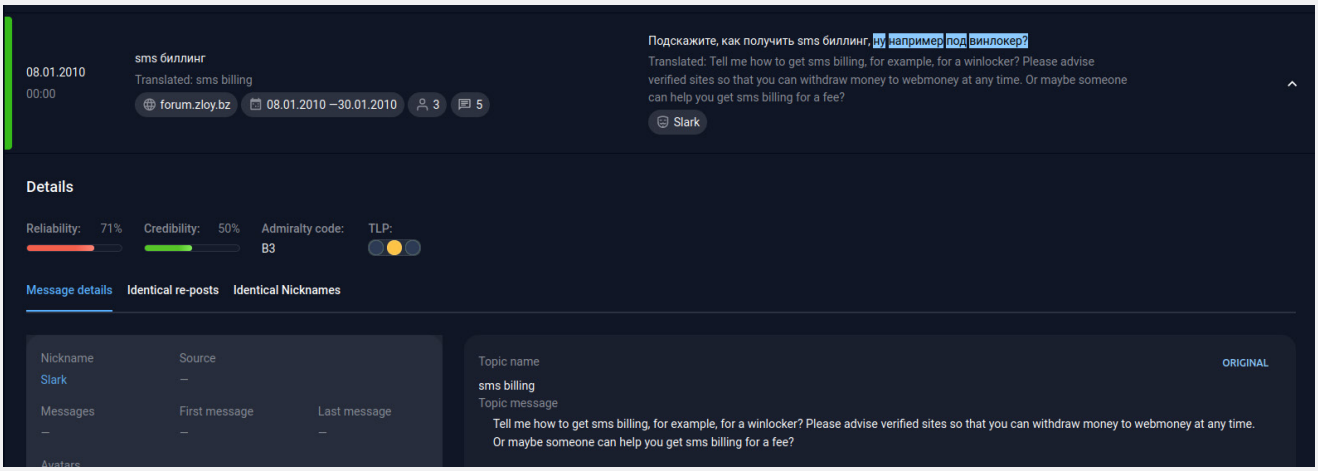


Fig. 7. A post about looking for an SMS billing service for locker ransomware, 2010

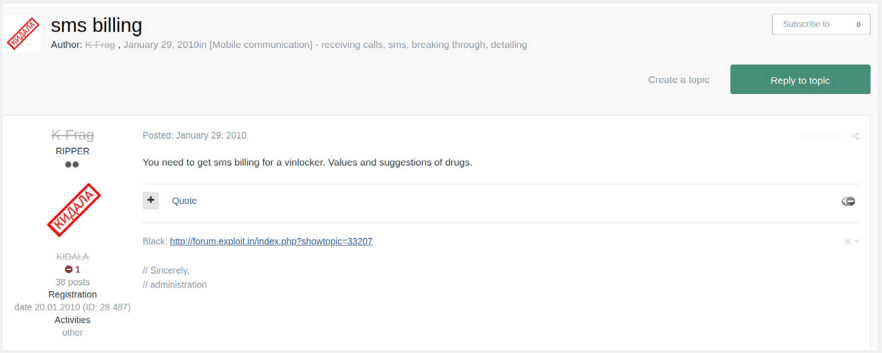


Fig. 8. Another post about SMS billing for locker ransomware, 2010

The development of **the first ransomware affiliate programs** started with Winlock. One of the first such affiliate programs related to locker ransomware emerged in **January 2010**:

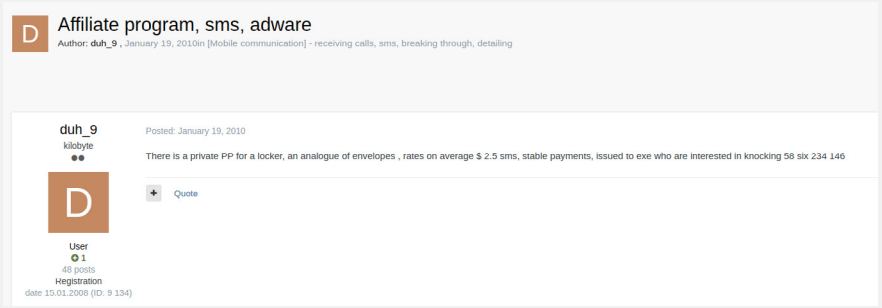
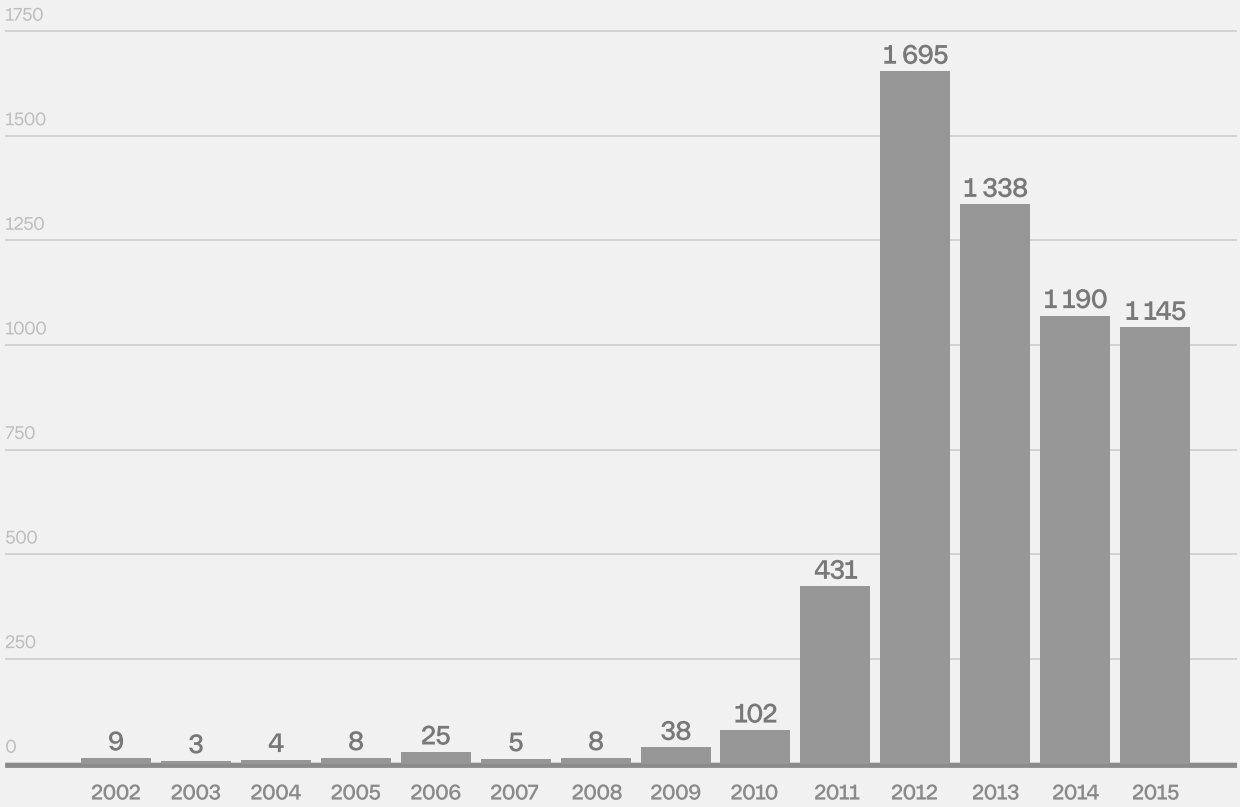


Fig. 9. A message about the Winlock affiliate program, 2010

The main idea behind these affiliate programs was simple: to give participants a Trojan to spread to victims, a task for which they would receive a commission on the profit from ransoms paid by victims to unlock their devices.

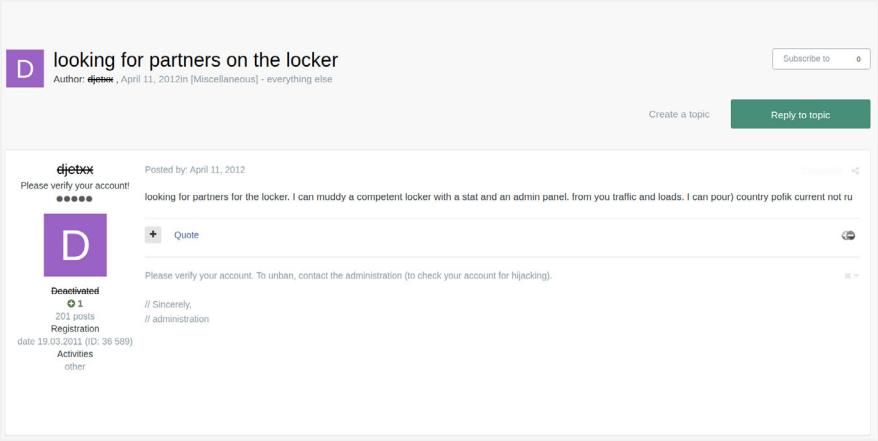
An analysis of messages published on underground forums and related to discussions about locker ransomware served as the basis for the histogram below:

Fig. 10. Mentions of locker ransomware on forums, 2002–2015



The histogram shows that locker ransomware started gaining popularity in 2009, then peaked in 2012 and later declined. In 2011, locker ransomware started being used in attacks beyond Russia. Moreover, some affiliate programs looked for people that would target victims outside Russia only:

Fig. 11. Looking for people for an affiliate program, 2012



Modern-day crypto ransomware: locker ransomware continues to dominate

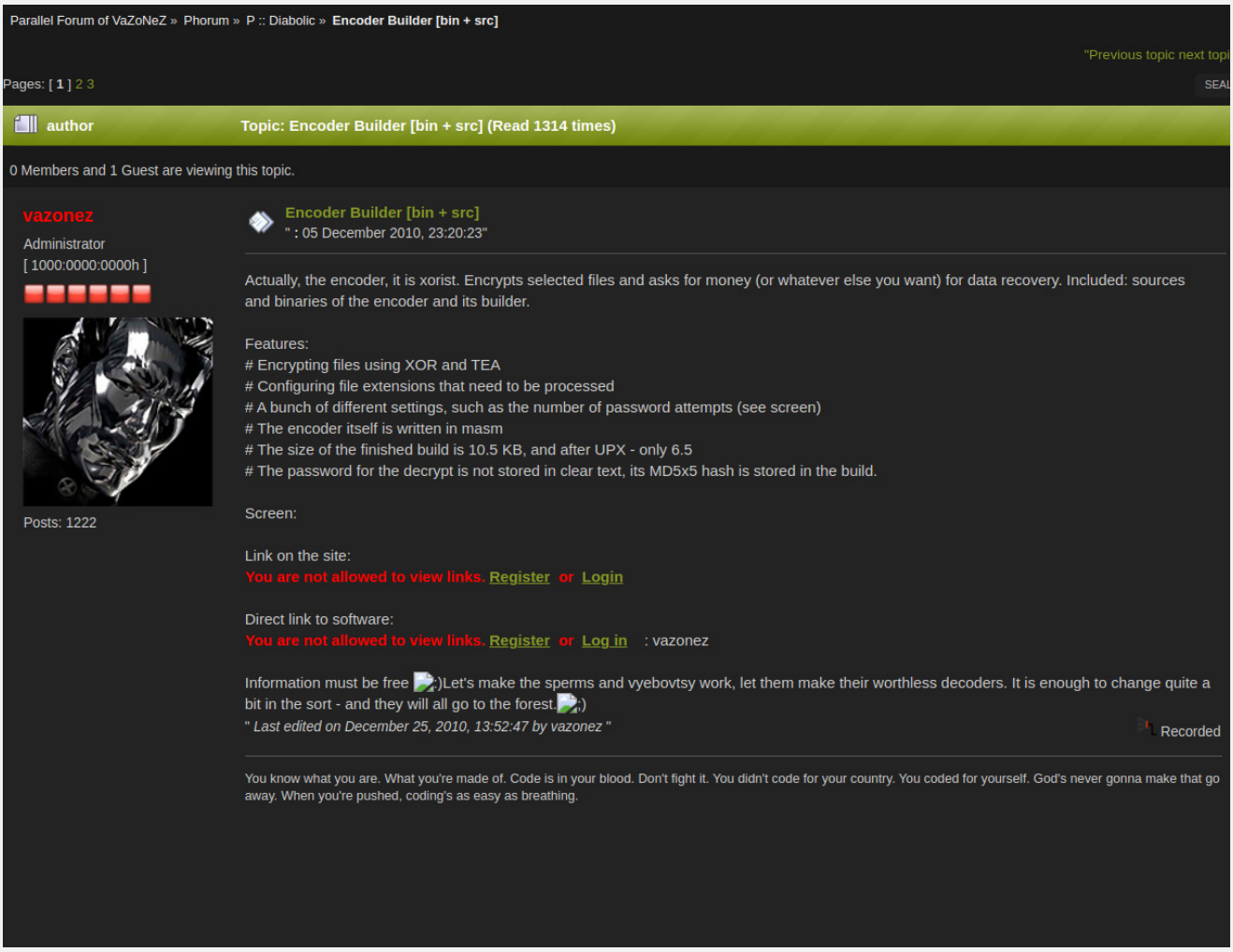
2011—2013

Encoder, Ulocker, Reveton, Citadel

The popularity of locker ransomware had no sooner declined than Trojans designed for encrypting data and demanding a ransom resurfaced on underground forums. The crypto ransomware era had begun.

In late 2010, **Encoder**[6] (aka xorist) emerged on underground forums and was the first known Trojan to be used for that type of activity.

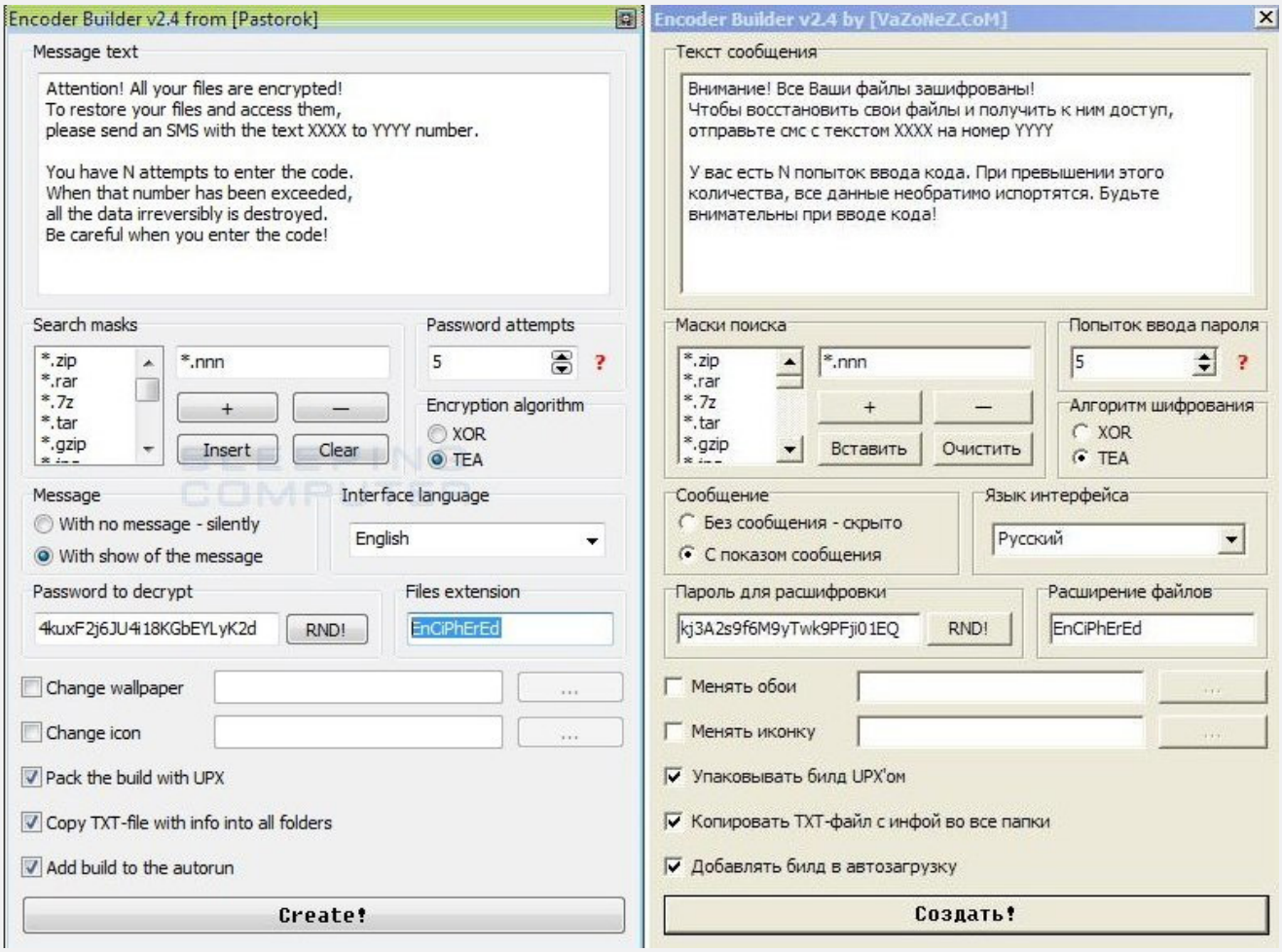
Fig. 12. A description of the xorist Trojan, 2010



The Trojan developer was a hacker with the alias **VaZoNeZ.**

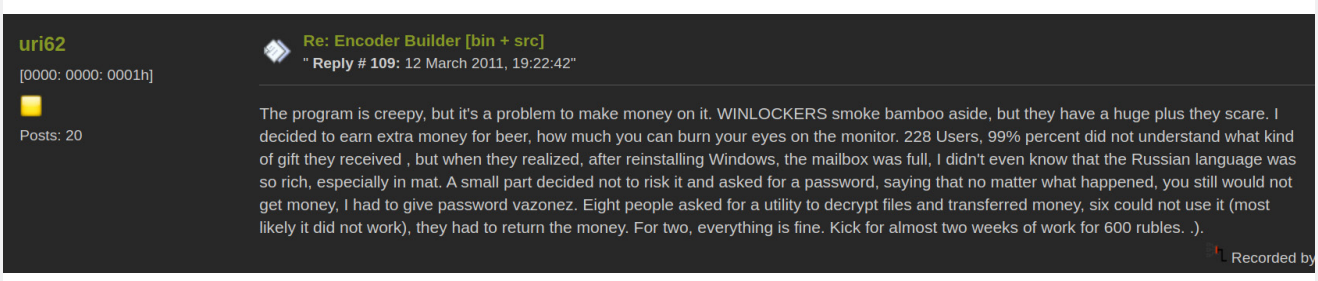
The developer of the Trojan published not just the malware's source code but also its builder, which enabled users to automatically generate malicious samples with custom settings.

Fig. 13. Encoder builder, 2010



However, the threat actors who tested the malware thought its conversion rate was too low.

Fig. 14. Complaints about Encoder's low conversion rate, 2011



The initial problem was that victims did not understand what exactly had happened or how to use the decryptor.

Additionally, locker and crypto ransomware was unpopular among threat actors, as they believed that it attracted too much attention. The second problem was where to receive money.

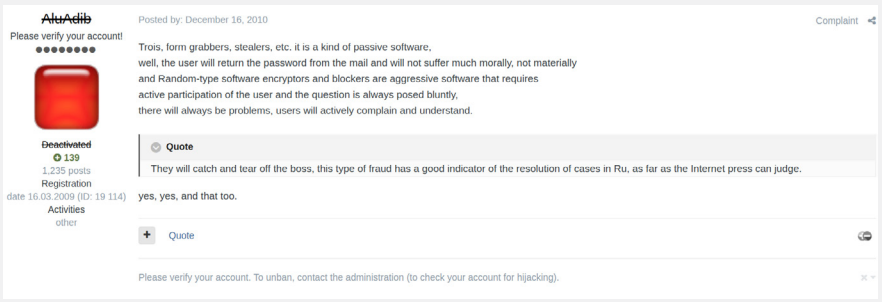


Fig. 15. A discussion about where to receive profit from locker ransomware, 2010

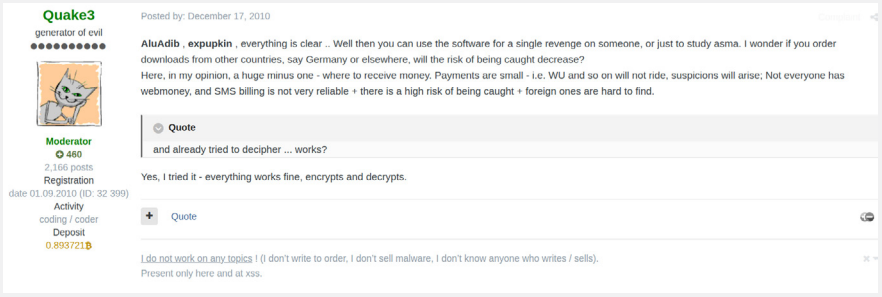


Fig. 16. A discussion about where to receive profit from locker ransomware, 2010

In July 2011, the user Galahem started selling improved crypto ransomware.

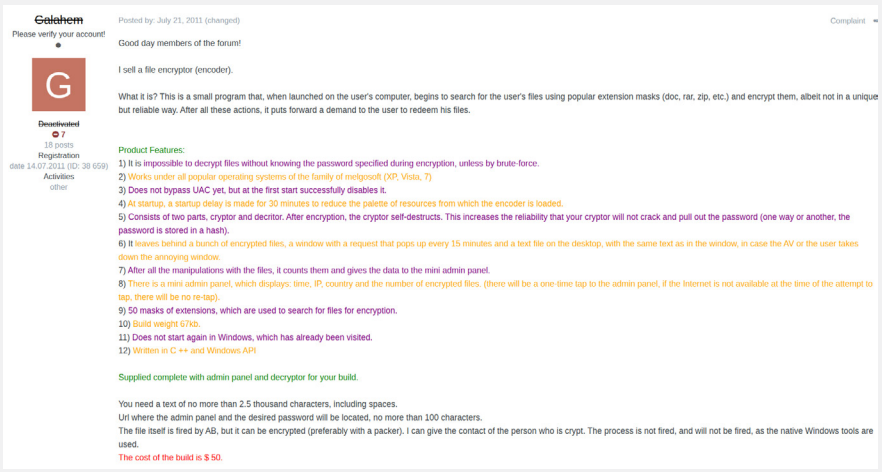


Fig. 17. Sale of crypto ransomware, 2011

The malware was not popular. Judging by messages on underground forums, threat actors continued being interested only in locker ransomware because it was easier to monetize, thanks to affiliate programs and other factors. To accept payments, threat actors started using **Paysafecard** vouchers and **Ukash**. New locker ransomware targeted many countries, but it did not work against Russia and other CIS countries. Back then, threat actors implemented the practice of not working against these countries in order to minimize the risk of getting caught.

For example, July 2012 saw the emergence of new locker ransomware called **Ulocker**[7]. Judging by its description, the malware was used in the following countries:

Austria, Germany, Greece,
Spain, Italy, Cyprus,
Netherlands, Poland,
Portugal, Romania,
Finland, France,
Switzerland, Sweden

xfrzx
petabyte
User
53
422 posts
Registration
date 10.11.2011 (ID: 40 624)
Activities
other

Posted by: July 29, 2012

ULocker

Ulocker is a software for monetizing euro downloads. Ukash, Psc vouchers of 50,100 euros are accepted as payment .
Currently AT, CH, CY, DE, ES, FI, FR, GR, IT, NL, PL, PT, RO, SE . You can add and change the number of languages.

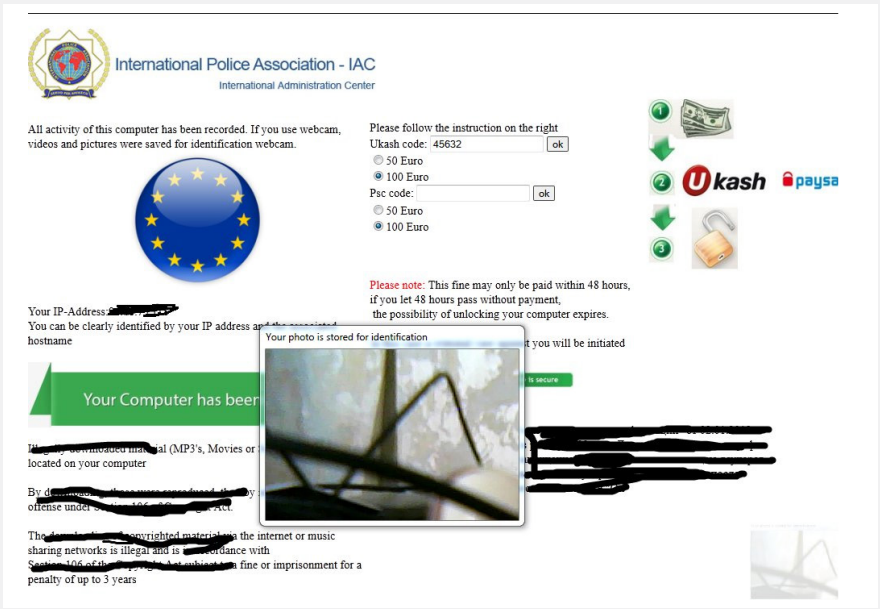
Details:
1.Weight ~ 22kb without compression
2.Kills MSCONFIG.exe, regedit.exe, regedt32.exe, CMD.exe, taskmgr.exe
3. Accepts Ukash, Psc.
4.Hides the start and panel.
5.Locks system keys.
6. The ability to remotely change the text.
7. Does not turn on when the Internet is off (Optional).
8.Auto download.
9. Disabling Safe Mode (xn)
10. Hangs on top of all windows.
11. After input is not removed.
12. The ability to quickly and conveniently add your own languages to work with specific countries (!)

Server part:
1st option - without panel writes date to file || ip || ukash || denomination || country .C psc is similar. Writes responses to a file.
2nd option - a simple panel, displaying vouchers (ukash, psc), displaying responses. Php + MySql is required.
The response is the sound of the infected machine, not necessarily unique.

Price:
First 3 buyers - 250 $ 0/3.
The price does not depend on the version of the server part.

Fig. 18. A message about the emergence of Ulocker, 2012

Ulocker also had highly advanced landing pages that showed webcam images intercepted by the malware.



International Police Association - IAC
International Administration Center

All activity of this computer has been recorded. If you use webcam, videos and pictures were saved for identification webcam.

Please follow the instruction on the right
Ukash code: 45632 ok
50 Euro
100 Euro
Psc code: ok
50 Euro
100 Euro

ukash paysa

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

Your IP-Address [redacted]
You can be clearly identified by your IP address and the associated hostname

Your photo is stored for identification

Your Computer has been

[redacted] located on your computer

[redacted] offense under [redacted]

[redacted] sharing networks is illegal and is [redacted] fine or imprisonment for a penalty of up to 3 years

Fig. 19. Ulocker landing page

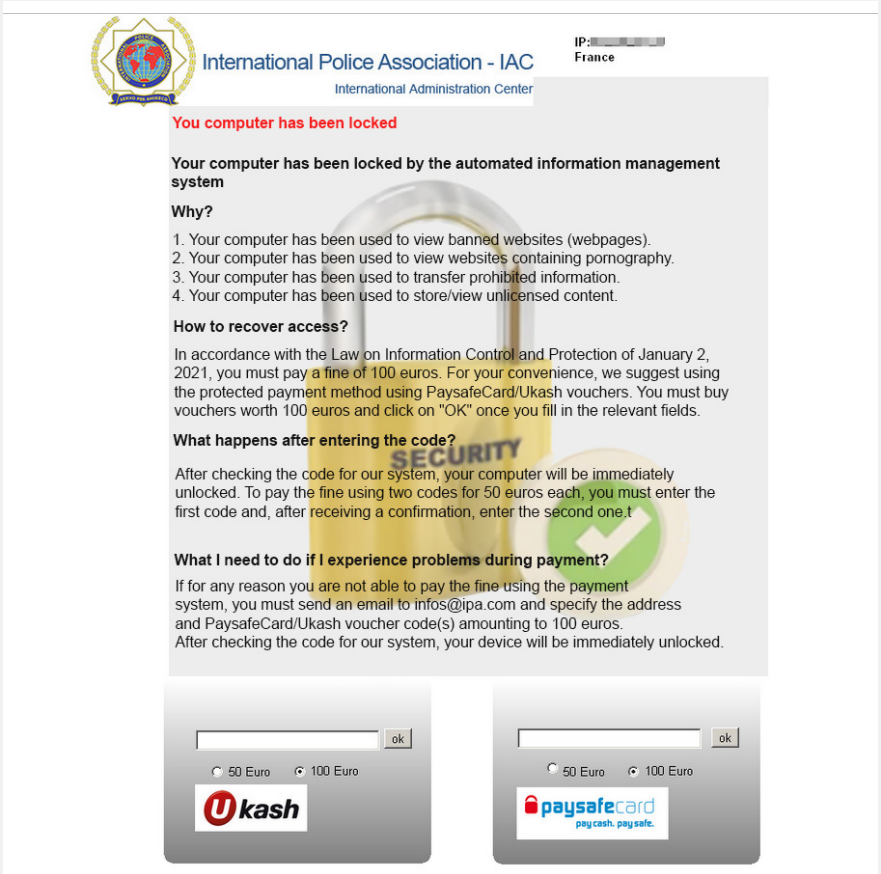


Fig. 20. A Ulocker message demanding a ransom for unlocking the computer, 2012

In 2012, some locker ransomware started using a new tactic: they overwrote the Master Boot Record (MBR), which resulted in the victim being unable to even start the operating system.

Around the same time, another notorious piece of locker ransomware called **Reveton** emerged. It also locked the victim's operating system and demanded a $100 fine. The landing page was designed to look like a document issued by the US Department of Justice. The ransomware was distributed using malware called **Citadel**[8], which was well-known at the time.

Given how popular Citadel was, many threat actors added it to their payload on infected devices.

The old crypto ransomware **GPCode** also continued to be developed, but it still targeted regular individuals.

From the second half of 2012, the situation began to change. Four Australian organizations fell victim to crypto ransomware attacks:

Company	Date	Ransom ($)	Industry
TDC Refrigeration and Electrical	September 2012	3,000	Manufacturing
Byron Community Primary School	October 2012	5,000	Education
Deanes Buslines	November 2012	3,000	Transportation
Gold Coast Medical Centre	December 2012	4,000	Healthcare

In exchange for decryption, the threat actors demanded tiny sums compared to today's figures. However, 2012 showed that attacks against businesses could be much more effective than attacks against individuals. Moreover, threat actors noticed that ordinary locker ransomware stopped being profitable and realized that they should switch to crypto ransomware. In late 2013, a well-known user with the alias upO wrote the following:

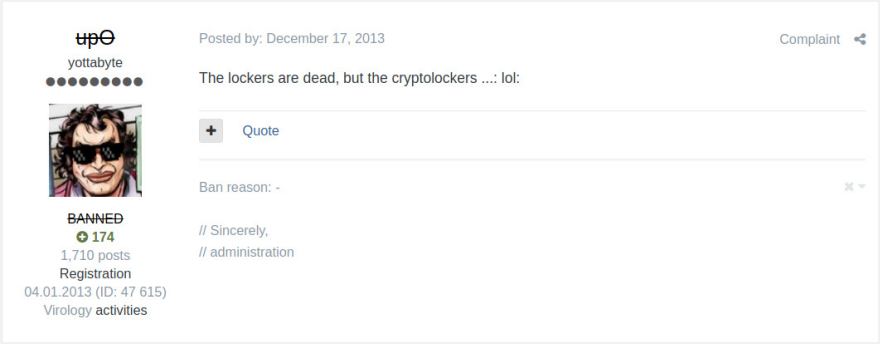


Fig. 21. The shift to using crypto ransomware emerging on underground forums, 2013

Emergence of crypto ransomware affiliate programs; CryptoLocker affiliate program and author

2012—2014

One of the first affiliate programs that focused on encrypting files emerged in June 2013 on the forum antichat:

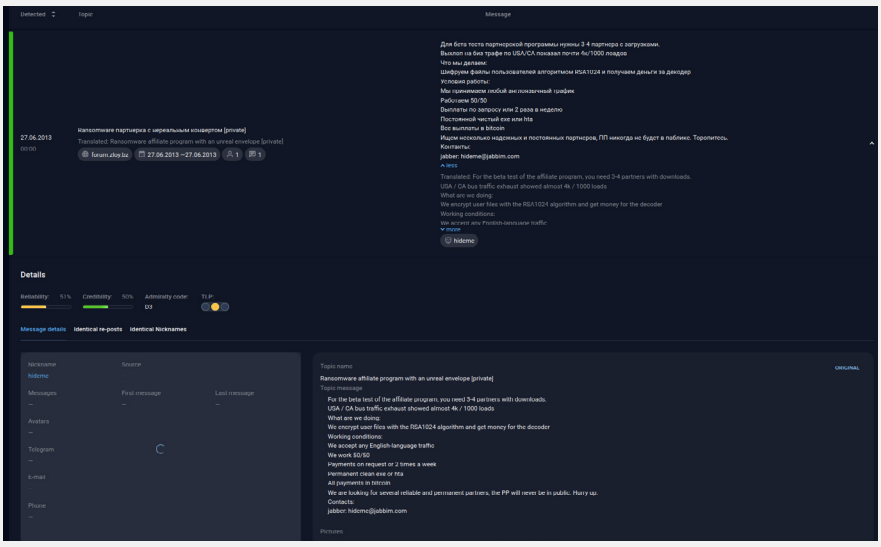


Fig. 22. One of the first affiliate programs, 2013

As the description suggests, the ransomware encrypted files using the RSA1024 algorithm and the developers used a 50/50 payment scheme (50% to the developers, 50% to affiliates). Unfortunately, neither the name nor reviews of this affiliate program could be uncovered.

September 2013 saw the emergence of one of the most notorious crypto ransomware strains at the time: **CryptoLocker**[9].

The first mention of CryptoLocker-type malware appeared on the underground forum exploit six months before attacks first came to light:

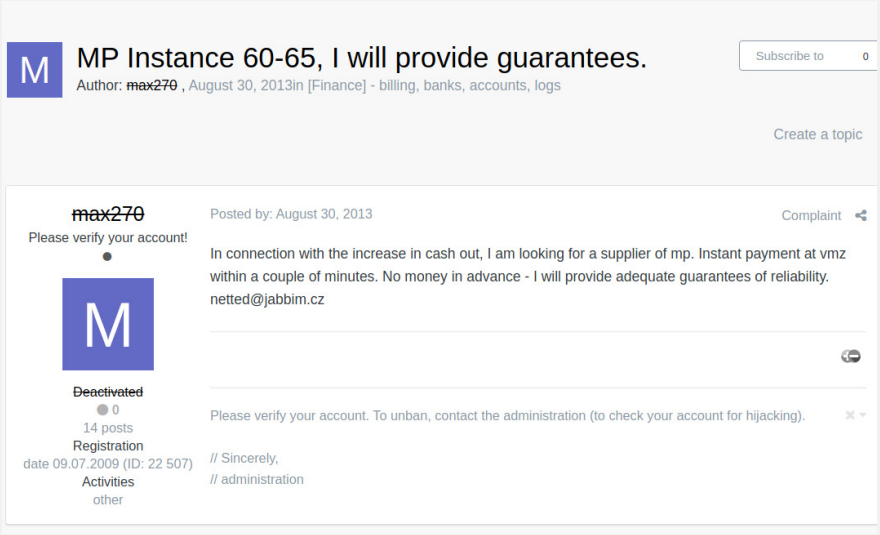


Fig. 23. A message about looking for a programmer that could create CryptoLocker-type malware, 2013

As can be seen in the screenshot, the forum user **max270** (aka max2 and nyservol) was looking for people to develop crypto ransomware and maintain it. The subsequent discussion between the threat actors reveals that in late August they announced that their cash-out activities had surged.

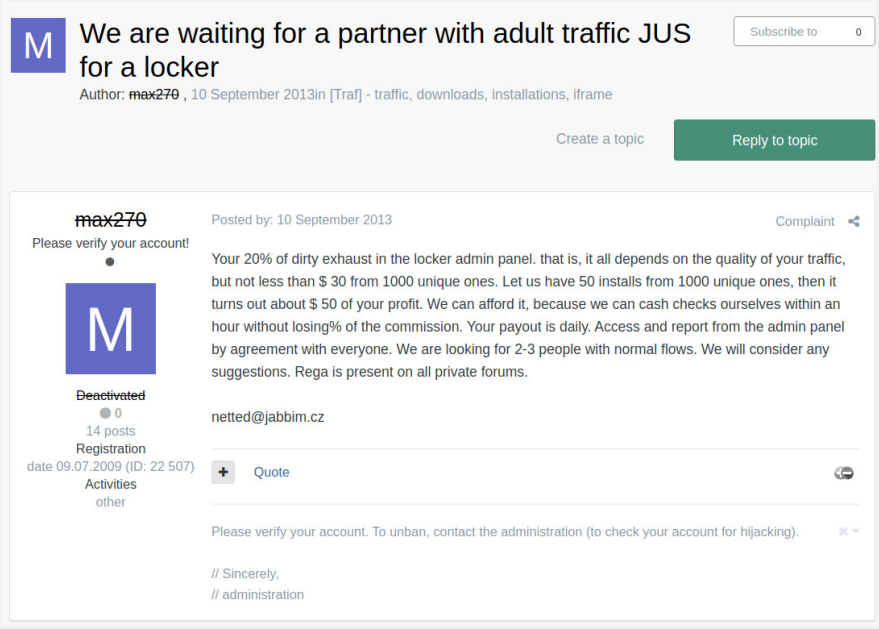


Fig. 24. A message about a surge in cash-out activities, 2013

In September 2013, offers of a new ransomware affiliate program (which could be related to CryptoLocker) were posted on several forums.

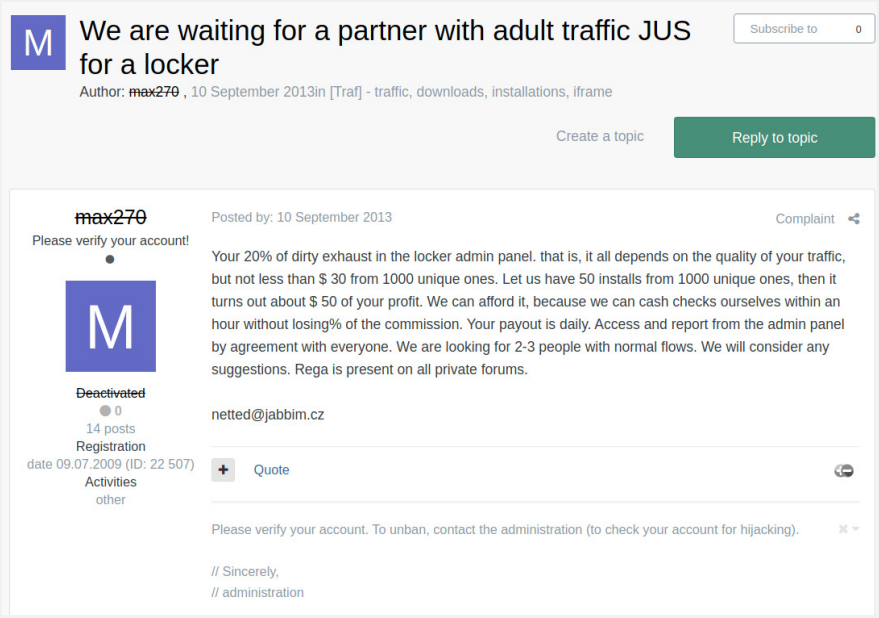


Fig. 25. A post about a new affiliate program, 2013

Based on publicly available research, the campaign used to spread CryptoLocker started on September 5, 2013, which suggests that this affiliate program was related to this specific malware.

After completing the infection, the Trojan's window looked like this:

Fig. 26. Cryptolocker, 2013

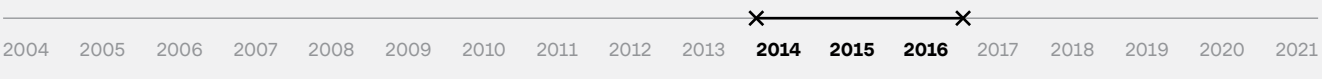
The malware then offered different payment options:

Fig. 27. Cryptolocker, 2013

CryptoLocker was one of the first pieces of crypto ransomware that infected a huge number of victims within a short period of time. Researchers say that by December 2013 (over the course of three months), over 200,000 machines were infected. CryptoLocker was active until May 2014, when it was isolated as part of operation Tovar, in which private decryption keys were obtained. The decryption keys were used to build an online tool for recovering files without paying the ransom. The affiliate program participants are believed to have made about $3 million.

RaaS evolution, focus on businesses, and threats to publish files

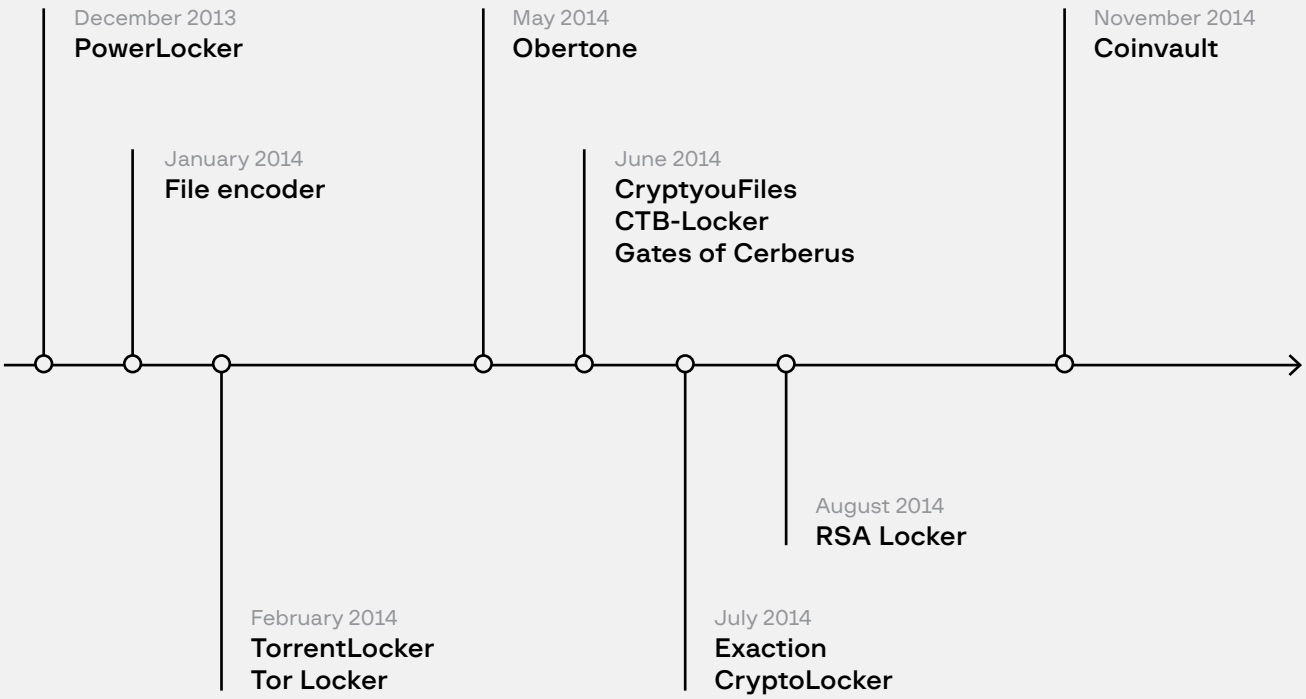
2014—2016



TorrentLocker, VaultCrypt, Tox Ransomware, LowLevel04, Chimera, Linux.Encoder, CryptoWall

The popularity of CryptoLocker led to a rise in the number of threat actors selling various pieces of malware with file encryption functionality.

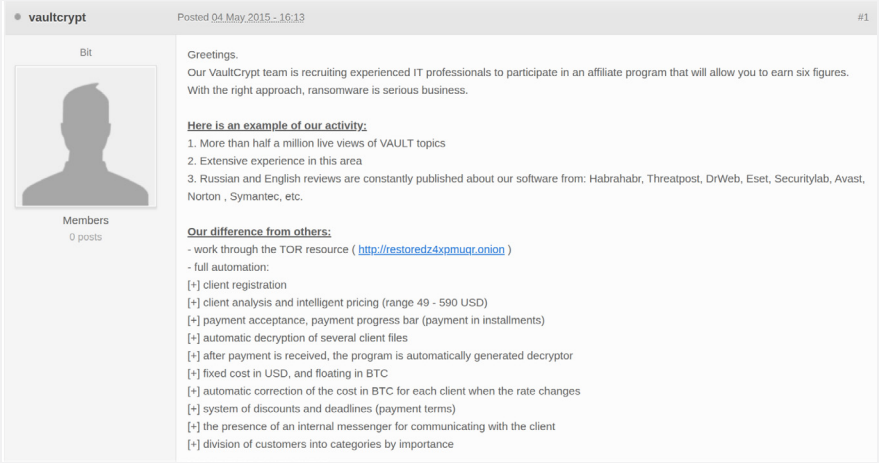
Trojans with a file encryption functionality, 2013–2014



The most widely spread crypto ransomware in 2014 was **TorrentLocker**[10]. In that year, its owners made about $500,000.

The development of locker ransomware changed, too, as threat actors began selling locker ransomware for mobile phones.

In February 2015, the crypto ransomware called **VaultCrypt**[11] became active. The campaign targeted mainly Russian-speaking users. In March 2015, a full-fledged affiliate program for this ransomware was launched. It is worth highlighting that the offer was extremely similar to modern-day affiliate programs.



vaultcrypt — Posted 04 May 2015 - 16:13 — #1

Bit

Members
0 posts

Greetings.
Our VaultCrypt team is recruiting experienced IT professionals to participate in an affiliate program that will allow you to earn six figures.
With the right approach, ransomware is serious business.

Here is an example of our activity:
1. More than half a million live views of VAULT topics
2. Extensive experience in this area
3. Russian and English reviews are constantly published about our software from: Habrahabr, Threatpost, DrWeb, Eset, Securitylab, Avast, Norton , Symantec, etc.

Our difference from others:
- work through the TOR resource (http://restoredz4xpmuqr.onion)
- full automation:
[+] client registration
[+] client analysis and intelligent pricing (range 49 - 590 USD)
[+] payment acceptance, payment progress bar (payment in installments)
[+] automatic decryption of several client files
[+] after payment is received, the program is automatically generated decryptor
[+] fixed cost in USD, and floating in BTC
[+] automatic correction of the cost in BTC for each client when the rate changes
[+] system of discounts and deadlines (payment terms)
[+] the presence of an internal messenger for communicating with the client
[+] division of customers into categories by importance

Fig. 28. A post about the VaultCrypt affiliate program, 2015

Another event worth highlighting is the emergence of the ransomware called **Tox** in May 2015. Its affiliate program involved an online malware builder available on a .onion website:

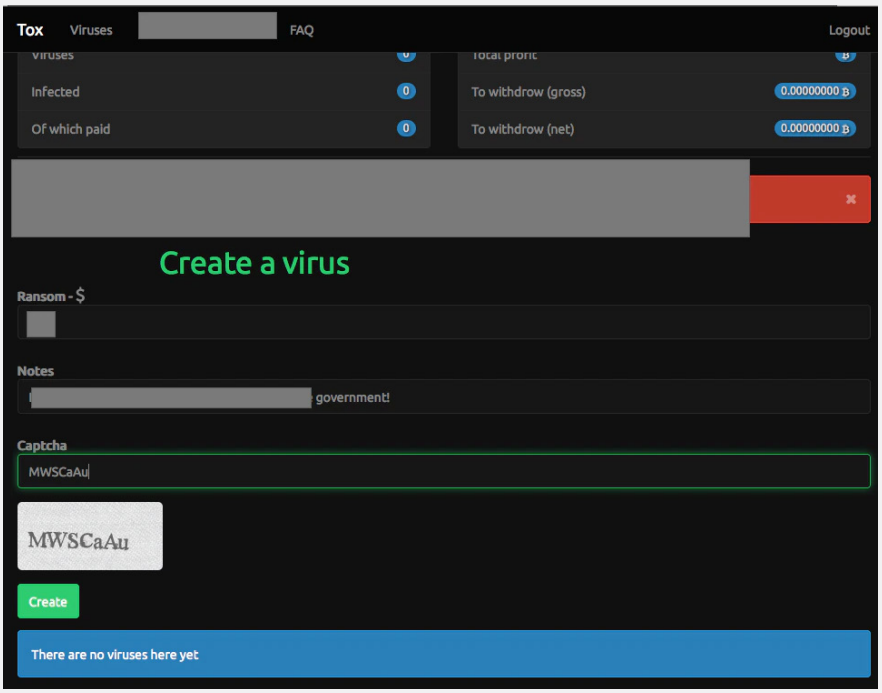


Fig. 29. Tox ransomware affiliate program, 2015

Any user could generate a ransomware sample on this website, specify the sum required for decryption, and use it to make a profit.

Some affiliate programs were private, which meant that there were few posts seeking affiliates on underground resources. Periodically, however, they did appear on underground forums in search of new people to recruit. For example, a post about a private affiliate program was published in October 2015 on a forum called verified. The post explicitly states that the affiliate program is not intended to be used against Russia and other CIS countries:

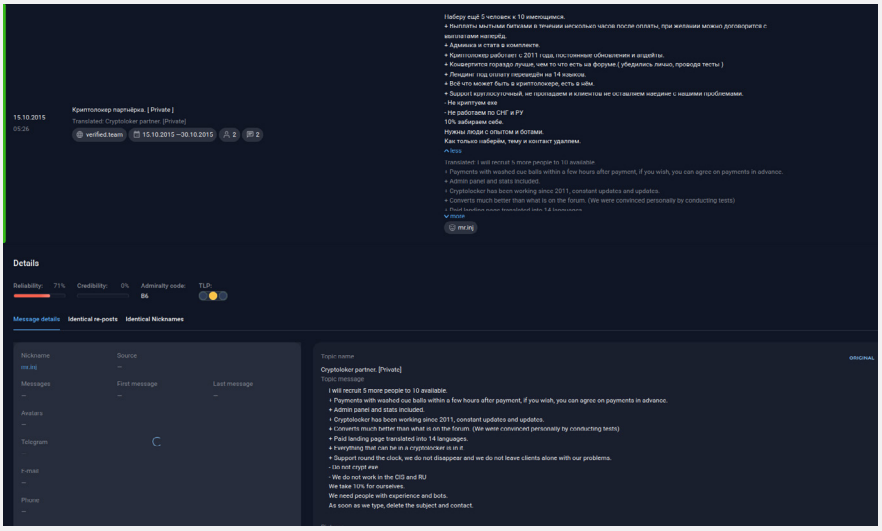


Fig. 30. A private affiliate program, 2015

According to the author of the post, the affiliate program had been operating since as early as 2011. Given that they became interested in crypto ransomware only in 2014, however, the statement seems dubious. Still, it is clear that RaaS was gaining momentum at that time.

A major ransomware attack occurred in May 2015 during which the computers of the Vietnamese Ministry of Justice were infected. The ransom amount was not disclosed. In October 2015, another attack was carried out against the computer network of a New Jersey school district, as part of which the threat actors demanded about $124,000. This is close to the size of current ransoms demanded by notorious groups carrying out ransomware attacks.

In October 2015, some users complained that their servers running Windows Server had fallen victim to malware called **LowLevel04**. It became clear that some threat groups had started using modern-day techniques. This particular case involved RDP brute-force attacks. From that moment on, ransomware victims were increasingly often legal entities rather than individuals.

It is worth highlighting the ransomware called **Chimera**[12], which emerged in November 2015. It had two distinctive features: it was used to attack legal entities only and the hackers threatened to make the encrypted data public.

Fig. 31. A threat by Chimera to publish data, 2015

The threat actors did not actually publish any data, but the technique was later adopted by all modern ransomware operators.

November 2015 also saw the emergence of Linux ransomware called **Linux.Encoder**. Its main targets are Linux servers, which are more likely to belong to companies rather than individual users.

The most notorious ransomware in 2015 was **CryptoWall**[13], which was discovered in 2014. Experts estimate that the threat actors made $18 million in 2014 and $325 million in 2015.

Notably, the threat actors did not have a public affiliate program and only one group was responsible for the ransomware, judging by the same Bitcoin wallets.

The year 2015 was a watershed period for the evolution of ransomware: threat actors increasingly shifted their focus onto businesses. Financially motivated groups realized that attacking legal entities is much more profitable. Such discussions can be found on underground forums:

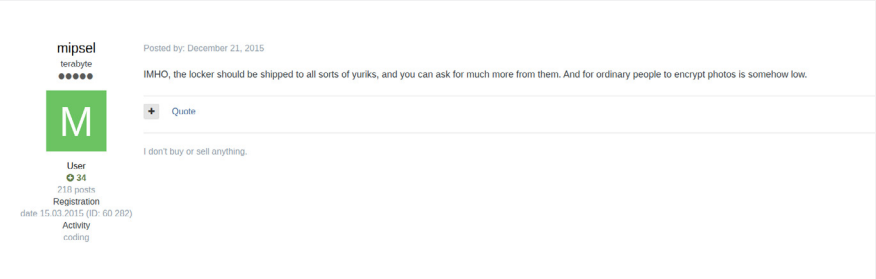
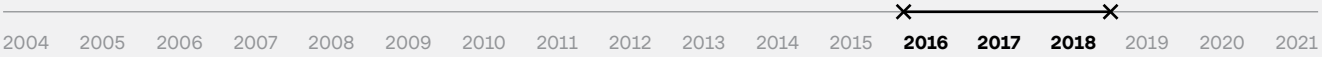


Fig. 32. A forum discussion about attacking legal entities being more profitable than attacks against regular users, 2015

The increasing popularity of ransomware, WannaCry

2016—2018



Cerber Ransomware, KeRanger, Petya, Mischa, Satana, ZCryptor, CTB-Locker, Locky, TeslaCrypt

As cybercriminals began focusing their attacks on companies throughout 2015, new targets were constantly discussed on underground forums:

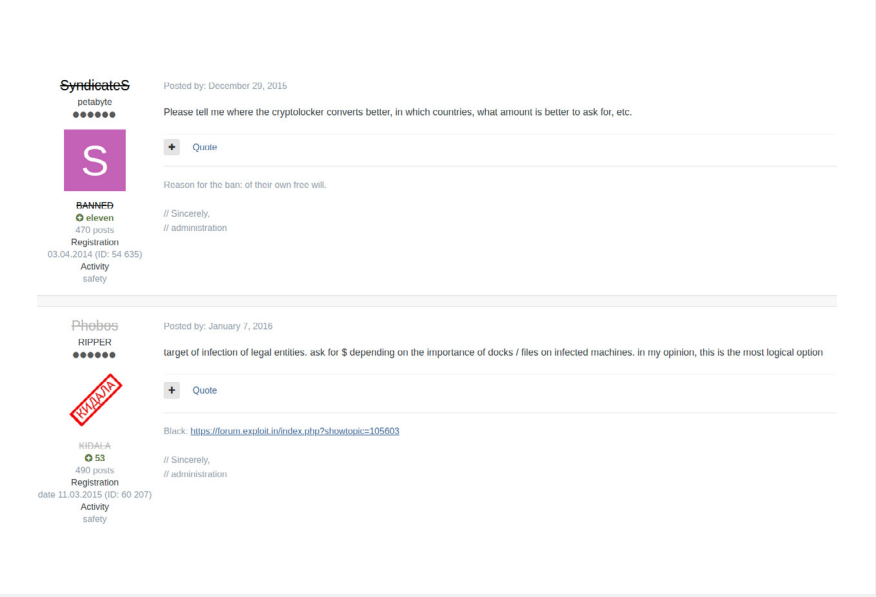


Fig. 33. Discussion on an underground forum about using locker ransomware to target a company, 2015

Cybercriminals began collecting email addresses from various corporations and government agencies to carry out attacks:

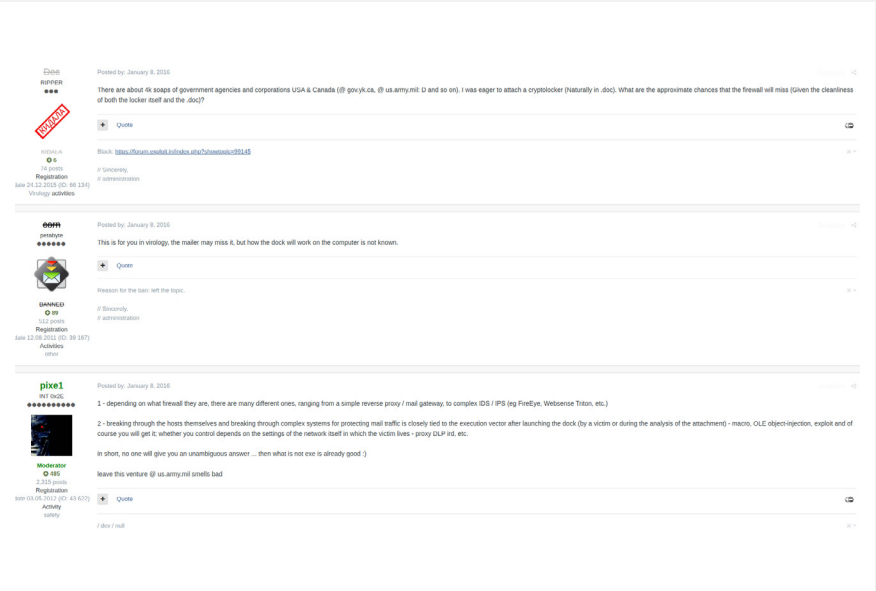


Fig. 34. Discussion about the possibility of an attack on organizations using pre-collected email addresses, 2016

From this point in the report, we will not detail each new strain of ransomware but instead focus only on the most interesting events that have occurred over the years and discuss the influence they had on how the ransomware cyber empire has evolved.

On February 24, 2016, threat actors launched one of the most infamous and largest ransomware affiliate programs at the time: **Cerber**. The extortionists demanded $500 for decryption. To pay the ransom, they required victims to visit their website hosted in the Tor network. In July 2016, Cerber became the most widespread type of ransomware.

In March 2016, the first fully functional ransomware for Mac OS X called **KeRanger**[14] was uncovered. To spread it, cybercriminals compromised the website of the popular software Transmission and replaced it with an infected file.

In late March 2016, another new Trojan called **Petya** emerged. In addition to encryption, the tool used another technique that was used in ordinary ransomware in 2012, i.e., overwriting the Master Boot Record (MBR), which ultimately meant that the victim could not even start the operating system. A little later, along with this ransomware, the ransomware called **Mischa** began to spread as well, which encrypted files without MBR if the privilege to use it was restricted. In July, another strain of ransomware called **Satana** began using the same technique.

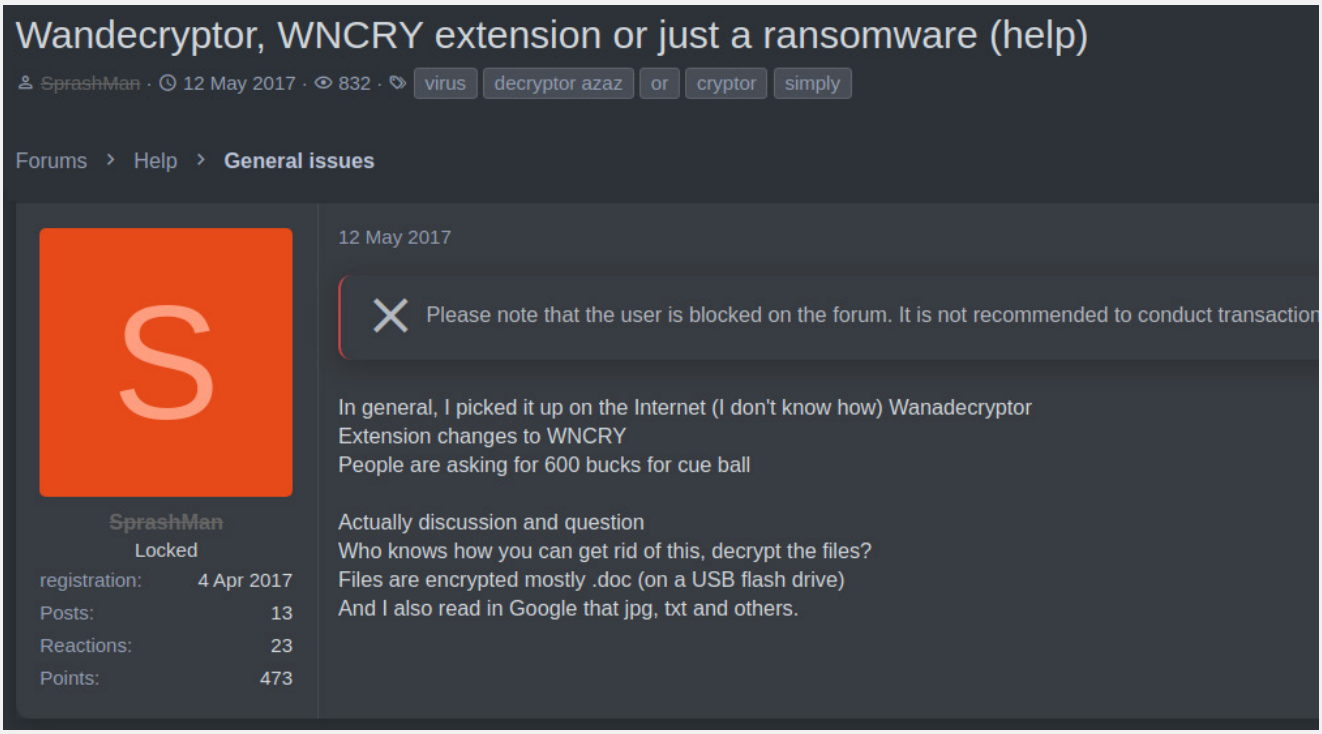
In May 2016, the ransomware **ZCryptor** emerged. It involved a new technique that is typical of classic viruses: self-propagation to various devices.

In November 2016, researchers uncovered new ransomware samples that used the messaging app Telegram as a C&C server for their Trojans. The ransomware contained the bot's API key in Telegram and reported the infection and other actions to certain channels or directly to the attackers. The technique is now often used in information stealers.

The most common ransomware strains in 2016 were **CTB-Locker**, **Locky**, and **TeslaCrypt**.

On May 12, 2017, users (including those on underground forums) began complaining that their files had been encrypted with a new ransomware that changes the extension to WNCRY:

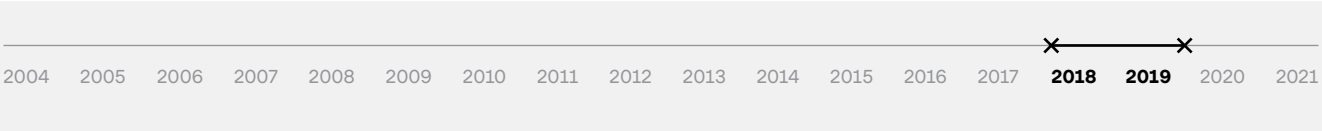
Fig. 35. Announcement of the new ransomware WNCRY, 2017



During one of the malware's attacks, about half a million machines were encrypted in a short time. The main reason for such a rapid spread was that the Trojan self-propagated using the exploit **EternalBlue** and subsequently installed the backdoor **DoublePulsar**. This showed cybercriminals that known vulnerabilities could be exploited to spread malware on a massive scale. A little later, on June 27, 2017, another ransomware called **NotPetya** used the same vulnerability for its attacks.

Current Ransomware-as-a-Service trends emerge: GandCrab

2018—2019



GandCrab, REvil, Mephistophilu

In January 2018, one of the most famous affiliate programs came to light: **GandCrab**. The malware's source code is believed to have been used by the hacker group **REvil** to develop their Trojan. GandCrab is the ancestor of almost all the major affiliate programs and trends that are still used by cybercriminals today.

Fig. 36. Description of the GandCrab affiliate program, 2018

GandCrab described in detail how to attack victims and pointed out that a current popular method involved the Cobalt Strike framework.

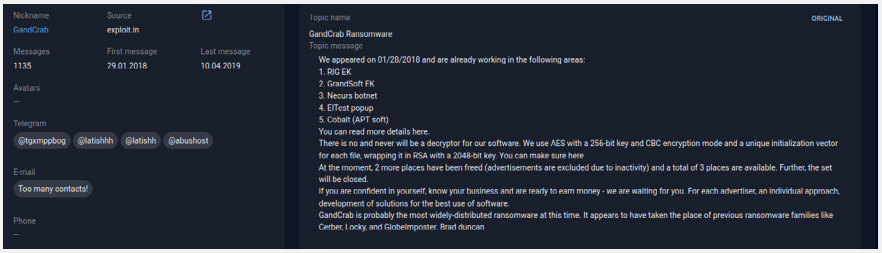


Fig. 37. Post by GandCrab owners on exploit.in, 2018

As can be seen from this post, the criminals began recruiting teams of dedicated partners that focused on large targets. As such, the affiliate program is considered the ancestor of **big game hunting**.

On February 28, 2018, the GandCrab web panel was hacked, which resulted in a quarter of their private decryption keys being leaked:

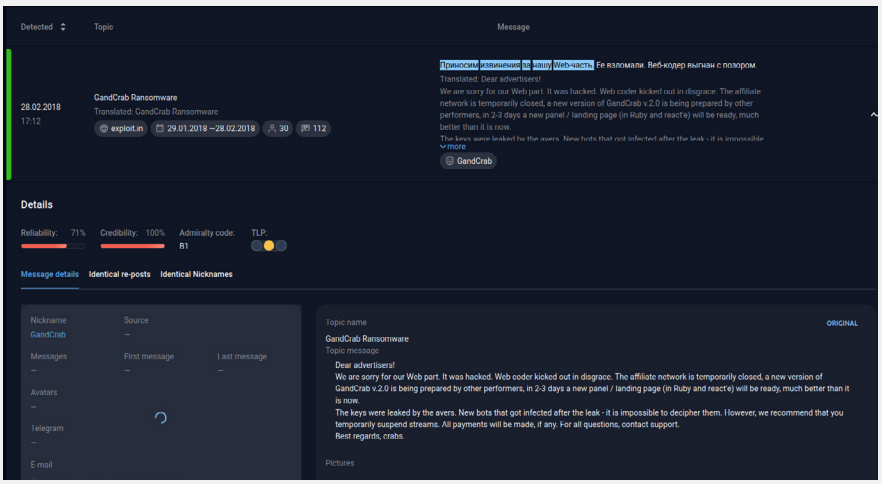


Fig. 38. Message on GandGrab hack, 2018

The hack did not stop the attackers, however, and on March 7, 2018, they relaunched the affiliate program, noting that they now stored the keys on a server separate from the administrative panel.

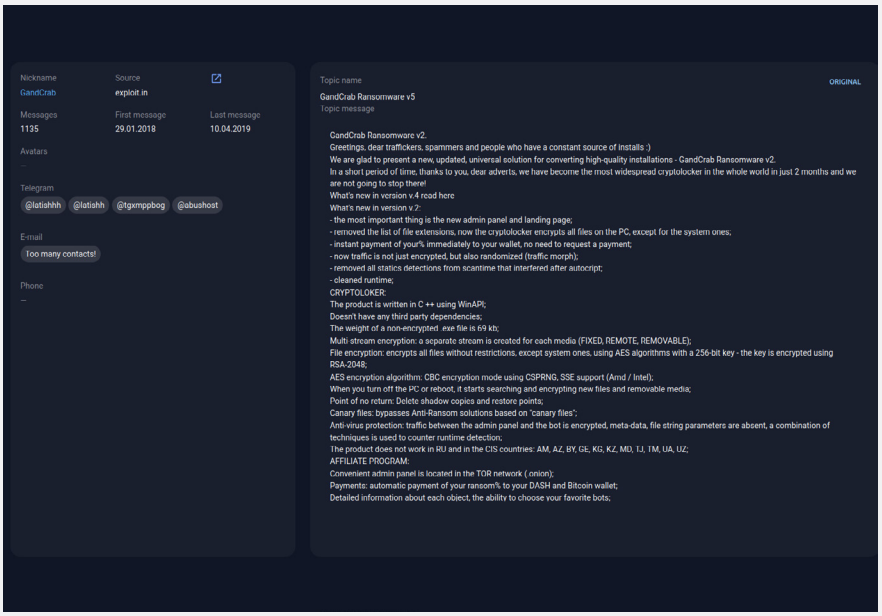


Fig. 39. Restarting GandCrab, 2018

The affiliate program differed from the rest with a thoughtful approach to working with partners, constant improvements to the malware, and the search for new technologies to increase the conversion of downloads into payments from customers. In February 2018, for example, the hackers were the first to introduce DASH payments.

GandCrab thoroughly examined various methods of gaining access to networks. In addition to typical frameworks such as **Cobalt Strike** and **MSF**, the threat actors used various apps that helped use social engineering as the main attack vector. For example, they used **Mephistophilus**, a system for targeted phishing attacks.

Moreover, GandCrab was the first to officially declare that they had partnered with data recovery companies:

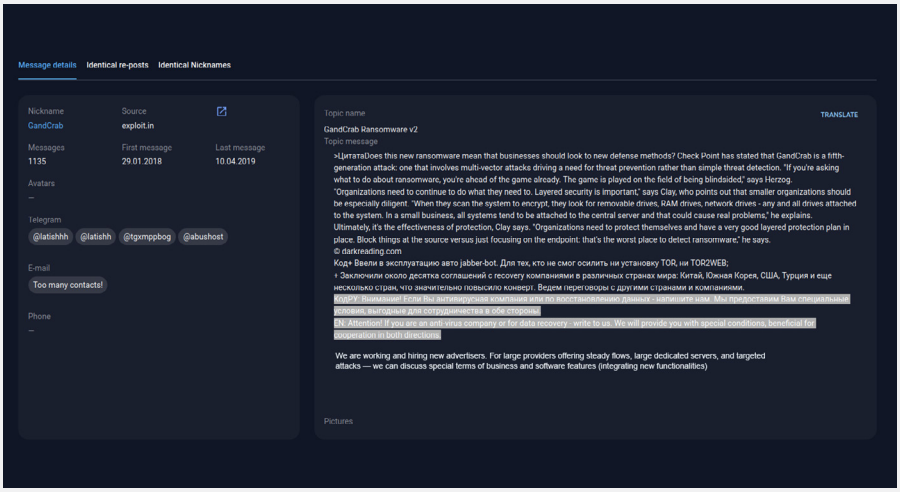


Fig. 40. GandCrab's announcement about its agreements with data recovery companies in various countries, 2018

In April 2018, the hackers once again started a new trend: buying access to dedicated servers in order to propagate attacks and gain full control over the victim's internal network.

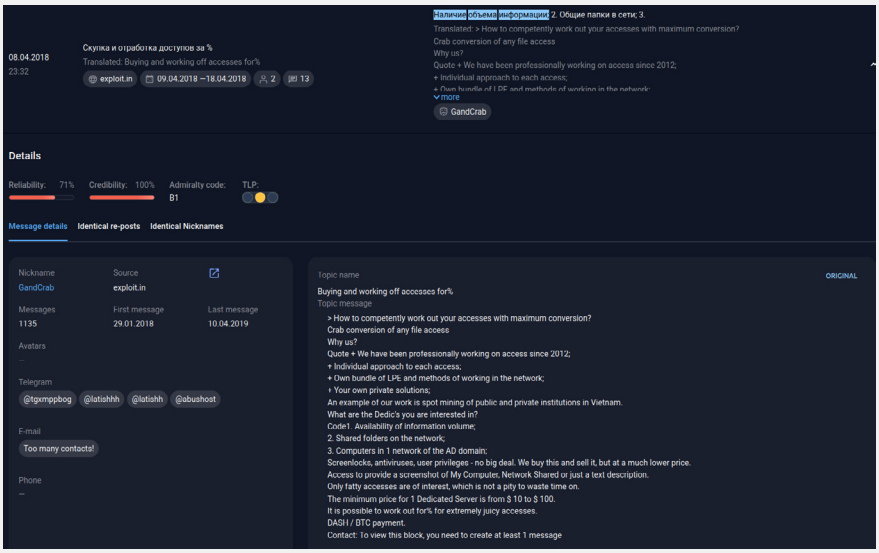


Fig. 41. GandCrab's message about buying access, 2018

According to GandCrab, as of April 2018 their weekly turnover was over $100,000. In May, the group shared statistics about their partners, revealing that some of them earned between $100,000 and $200,000 per month. In June 2018, the group mentioned that 315,365 computers were infected in a month. The threat actors once again stressed that they were looking for an APT group* to gain targeted access to major companies.

In July 2018, GandCrab concluded 210 contracts with data recovery companies worldwide. In the same month, a new version of GandCrab was released, which allowed for automatic encryption of network drives. The feature was later used in other ransomware. After one of the first Initial Access Brokers (IABs) left the public access market, a huge number of new offers to sell access appeared on underground forums. Read more about this in the report entitled: **Unexpected guests: The sale of access to corporate networks**. GandCrab was the first group to regularly purchase access from IABs.

In August 2018, GandCrab changed the requirements for accepting new partners: potential partners now needed to pass an interview to join the program. This practice was later adopted by other attackers.

Based on other messages from the criminal group, GandCrab used an exploit kit called Fallout to gain access.

In September 2018, GandCrab released another update. The attackers claimed that their monthly income amounted to more than $1 million. Their innovative features included a PowerShell script builder added to the administrative panel, which allowed a payload to be downloaded, thereby bypassing anti-virus systems. In addition, encrypted files now had dynamic expansion, which means that they changed from machine to machine. What is more, GandCrab operators partnered with the crypter service **NTCrypt**.

In the following October update, the developers implemented Mimikatz in their solution to automate the collection of credentials. The threat actors also openly declared a fight against other ransomware operators, as they considered it unacceptable to encrypt the same victims twice.

* APT (Advanced Persistent Threat) group usually means a group linked to a government, in other words, a nation-state hacker group.

Unexpected guests: The sale of access to corporate networks

On October 17, 2018, the attackers announced that they were providing a free decryptor to Syrian citizens. As a result, on October 27 anti-virus companies obtained the master key by analyzing the generated keys and created a universal decryptor. In response, on October 28 the attackers developed a new master key and began transitioning to a new encryption scheme that did not depend on it.

In the October 31 update, the ransomware had the function of scanning for RDP and brute-forcing RDP within the network using passwords obtained by Mimikatz.

In January 2019, GandCrab launched a new service for monetizing remote access to compromised corporate networks gained by third-party threat actors. GandCrab was looking for entry to corporate networks through RDP or VPN software. If forum members could provide GandCrab with entry, the group would try to deploy its ransomware onto the victim network and split all proceeds. Alternatively, the group offered to buy the access in question after assessing it.

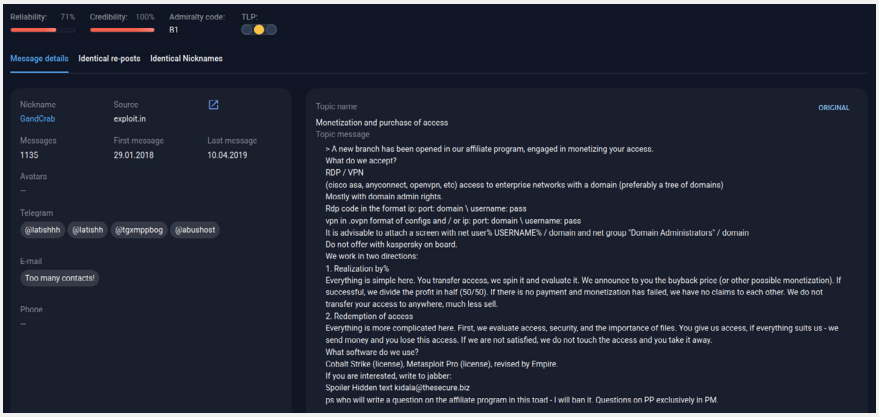


Fig. 42. GandCrab's message about the group's new monetization service, 2019

In February 2019, another attack was carried out against GandCrab servers during which the secret keys were obtained again, which led to the appearance of yet another decryptor.

On May 31, 2019, GandCrab suddenly left the market.

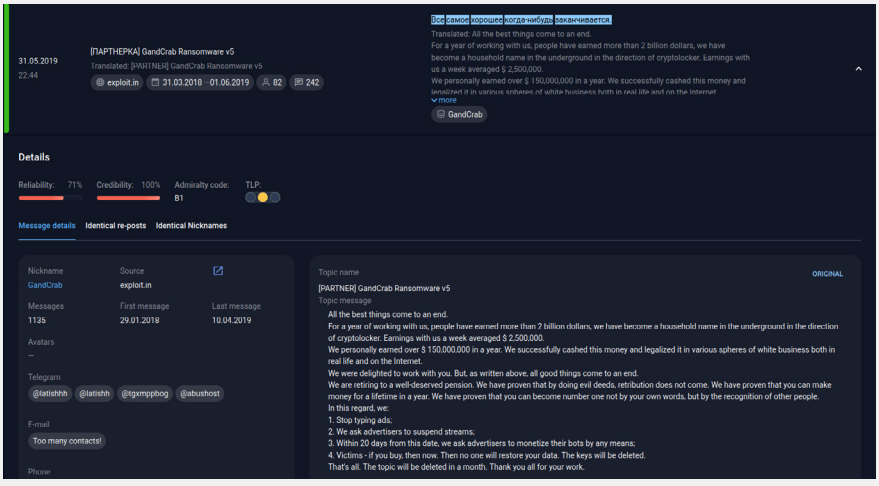


Fig. 43. GandCrab's message about terminating their activity, 2019

In the group's last message, GandCrab's owner asked all parties involved to delete their accounts and anything else connected to GandCrab.

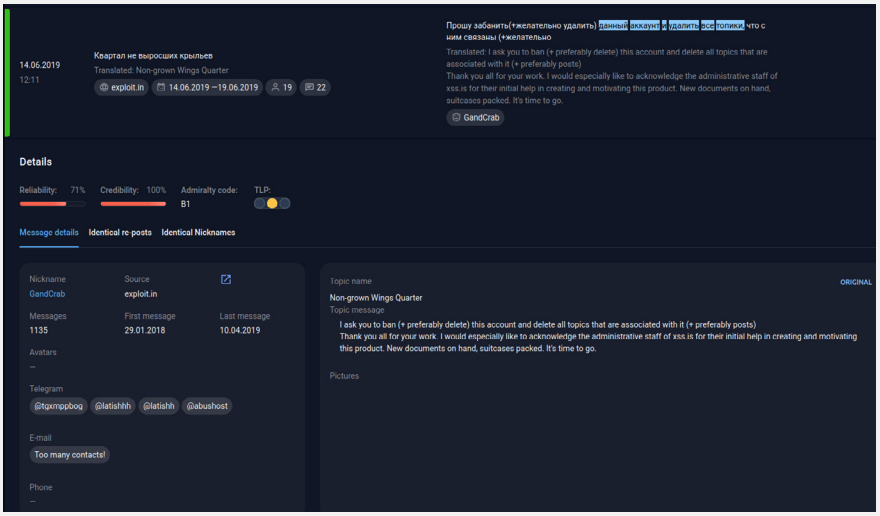


Fig. 44. Post asking to delete all threads and posts related to GandCrab, 2019

Current trends: double extortion, the emergence of DLS, affiliate programs forbidden on forums

2019—2021

2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 **2019** **2020** **2021**

Ransomware Snatch, ChaCha/Maze, REvil, Babuk

In March 2019, an advertisement for the new **Ransomware Snatch** affiliate program appeared on the forum exploit.in:

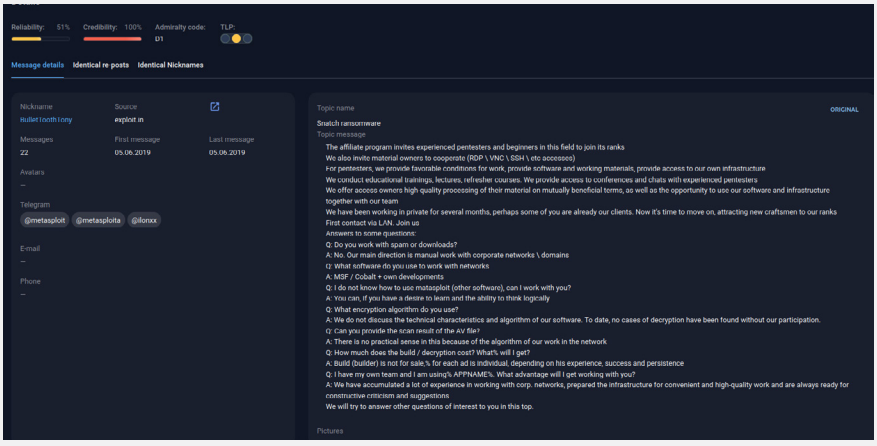


Fig. 45. Announcement about a new affiliate program called Ransomware Snatch, 2019

One of the affiliate program's distinctive features was that it did not work with traffic and downloads, but instead focused exclusively on attacks on corporate networks.

On April 28, 2019, a user with the alias **truniger** published an interesting post on exploit.in. The user mentioned that **Citycomp's** network had been hacked and encrypted, and that all its data had been exfiltrated.

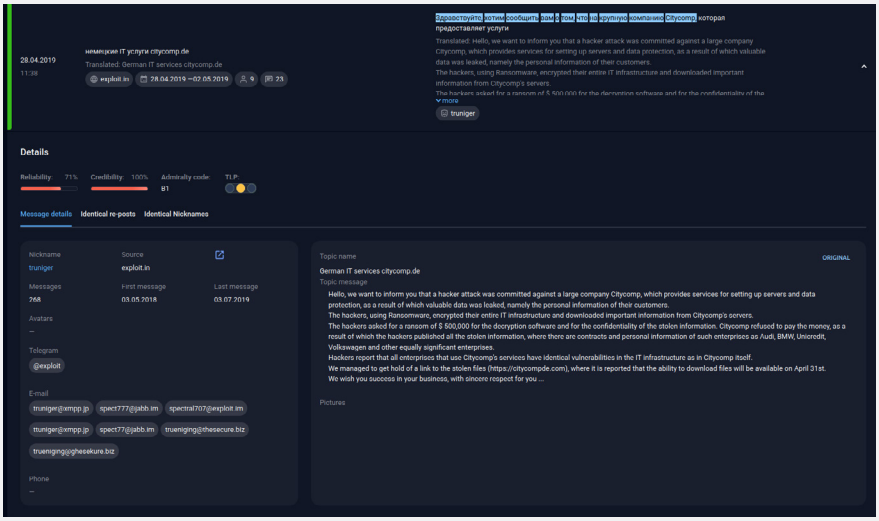
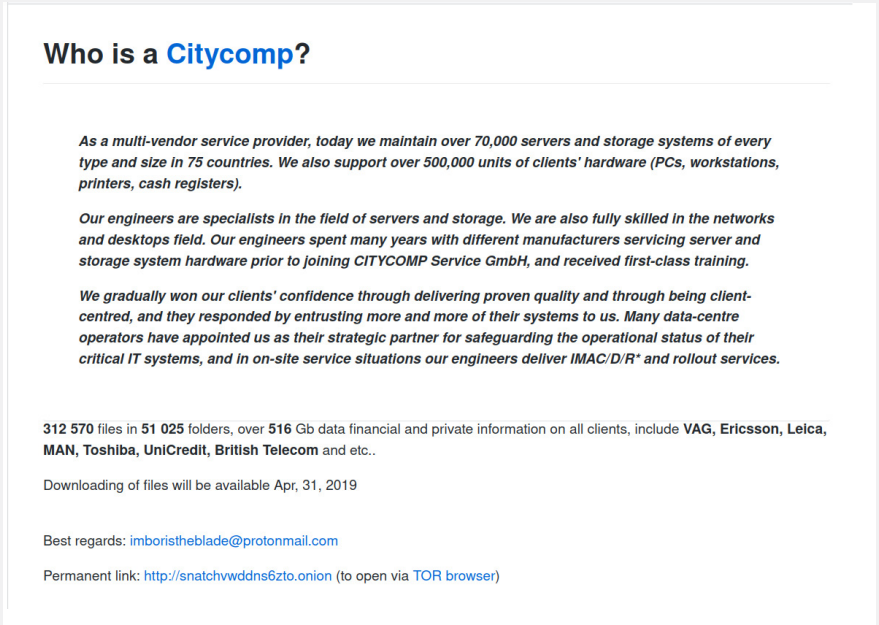


Fig. 46. Message about Citycomp data being compromised, 2019

According to the attacker, the company had refused to pay the ransom for the decryption, so some threat actors decided to make their data publicly available:



Who is a Citycomp?

As a multi-vendor service provider, today we maintain over 70,000 servers and storage systems of every type and size in 75 countries. We also support over 500,000 units of clients' hardware (PCs, workstations, printers, cash registers).

Our engineers are specialists in the field of servers and storage. We are also fully skilled in the networks and desktops field. Our engineers spent many years with different manufacturers servicing server and storage system hardware prior to joining CITYCOMP Service GmbH, and received first-class training.

We gradually won our clients' confidence through delivering proven quality and through being client-centred, and they responded by entrusting more and more of their systems to us. Many data-centre operators have appointed us as their strategic partner for safeguarding the operational status of their critical IT systems, and in on-site service situations our engineers deliver IMAC/D/R* and rollout services.

312 570 files in **51 025** folders, over **516** Gb data financial and private information on all clients, include **VAG, Ericsson, Leica, MAN, Toshiba, UniCredit, British Telecom** and etc..

Downloading of files will be available Apr, 31, 2019

Best regards: imboristheblade@protonmail.com

Permanent link: http://snatchvwddns6zto.onion (to open via TOR browser)

Fig. 47. Citycomp data being made public, 2019

The resource on which the data was published also indicated the .onion domain where the threat actors planned to store the leaked data in the future: snatchvwddns6zto.onion.

When discussing the leak, the user clarified that they had initially intended to publish the data if the company refused to pay the ransom:

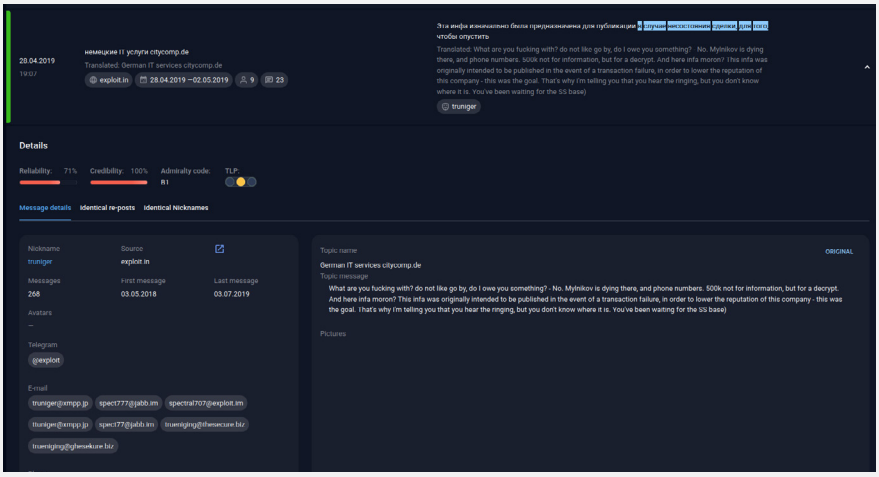


Fig. 48. "This information was intended to be published", 2019

Further analysis revealed that truniger was involved in gaining access to networks and had worked with the GandCrab affiliate program. It is likely that truniger then switched to the **Snatch** affiliate program. Later, the domain snatchvwddns6zto.onion was used to publish data about companies that refused to pay ransoms. This was the first time that a ransomware group put double pressure on a victim. Other groups did not immediately adopt this technique, however.

In May 2019, researchers detected a new ransomware, initially named **ChaCha** (after the encryption algorithm), that was distributed using the exploit kit Fallout. In the past, this EK was used by GandCrab. In June 2019, the malware operators named the ransomware in question **Maze**. The most noteworthy event happened in November 2019: the criminal group registered an account on the underground forum xss.is and posted a message about **Allied Universal's** data being compromised and encrypted. The victim contacted the group but refused to pay the ransom even after being given evidence of the hack. The attackers then published 10% of the data on an underground forum:

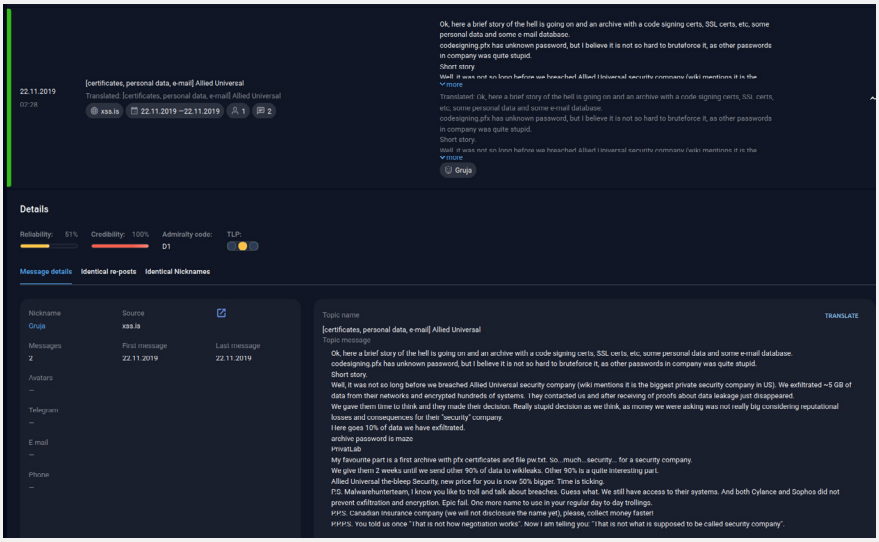


Fig. 49. Post about Allied Universal's data compromised, 2019

In the same post, the user announced that they would send the remaining 90% of the compromised data to WikiLeaks if the company did not pay them. They also warned other companies that this will be the case for anyone who refuses to pay.

In December 2019, Maze realized that the best way to put pressure on their victims would be to create their own **Data Leak Site (DLS)** where they could publish data belonging to companies that refused to pay the ransoms. As a result, on December 9, 2019, they registered the domain mazenews.top, which Maze used to publish leaks. The first leaks were published on December 15.

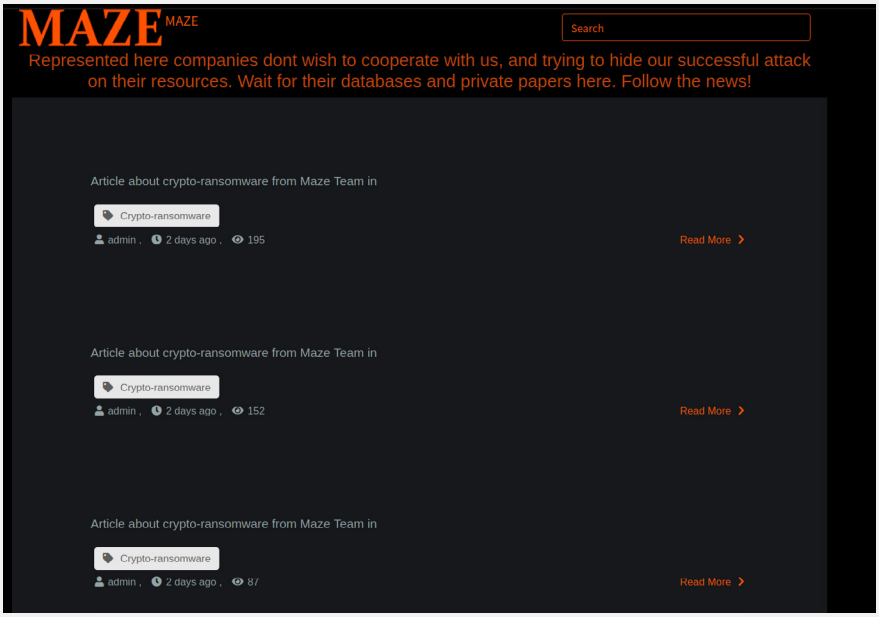
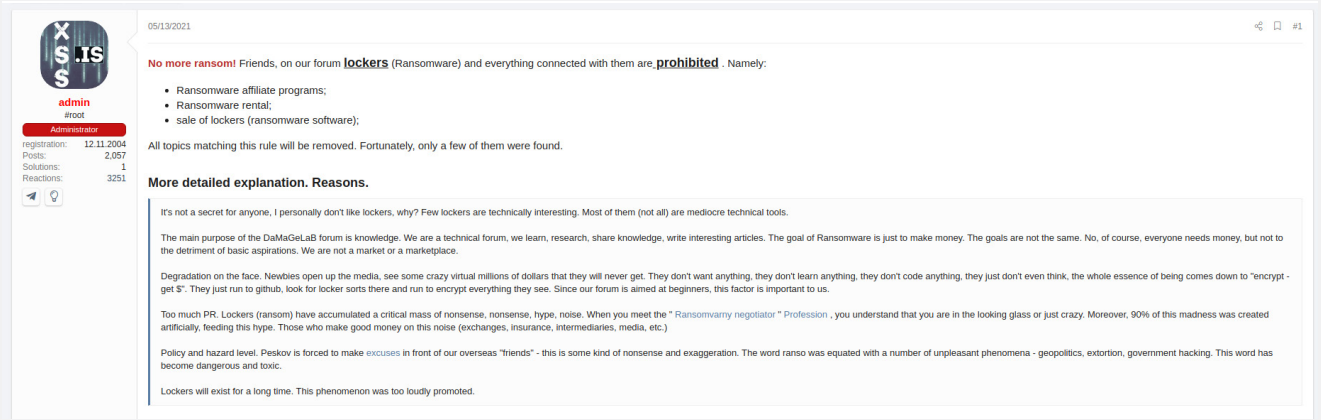


Fig. 50. Maze DLS website, 2019

The tactics used by Maze and Snatch were later adopted by most known ransomware operators.

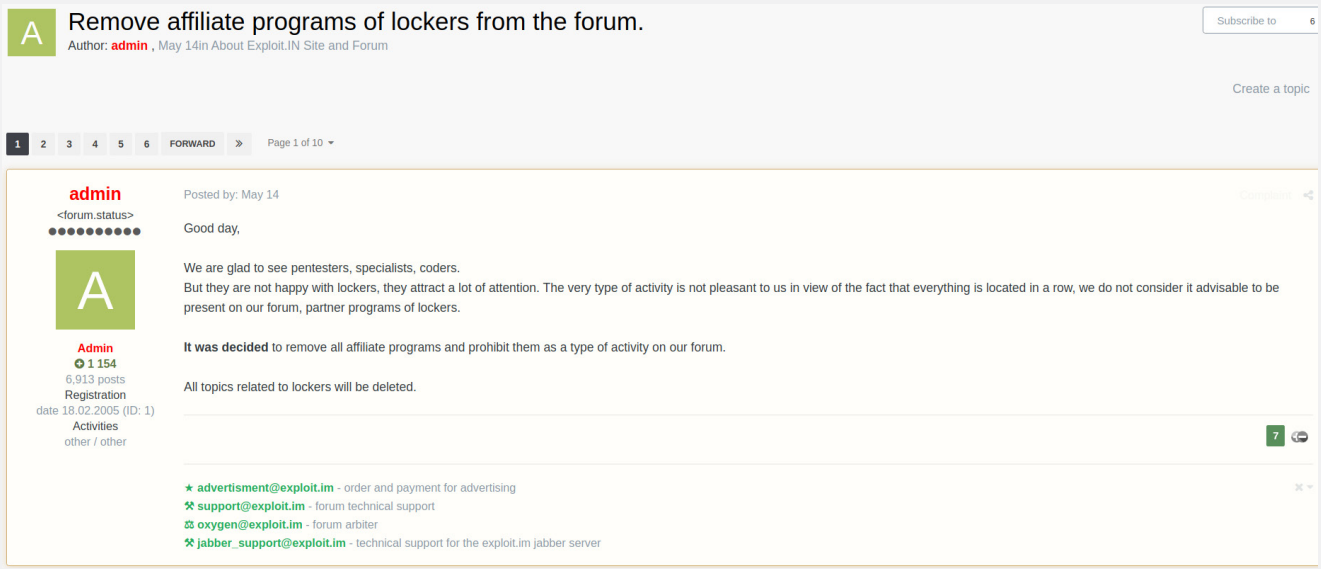
The last significant event in the evolution of RaaS occurred in May 2021. Following large attacks by various groups, especially **REvil**, forum owners banned advertising affiliate programs on underground forums. They explained that spreading ransomware drew too much attention to other hacker activities.

Fig. 51. Ban on lockers on an underground forum, 2021



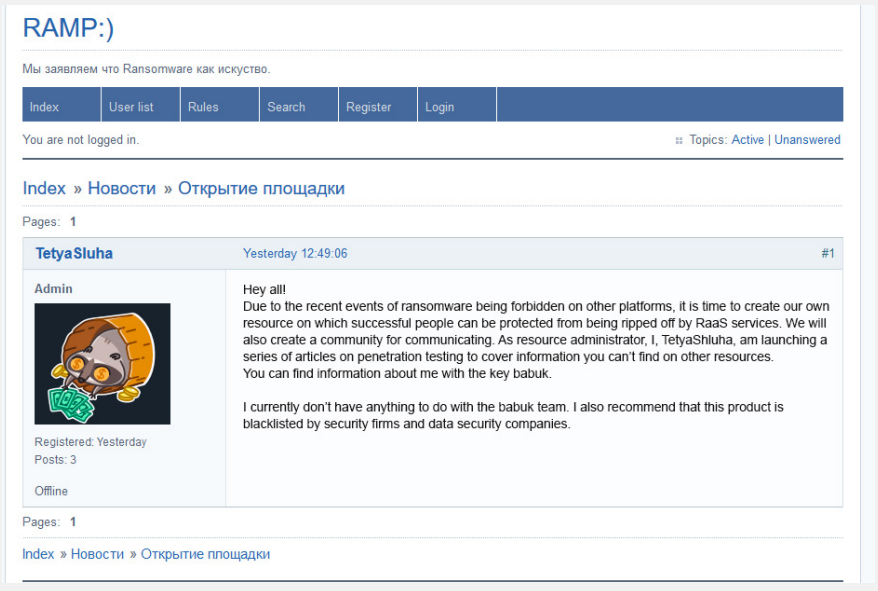
A day later, another major underground forum, exploit.in, joined the movement “No more ransoms!”:

Fig. 52. Locker ban on exploit.in, 2021



This did not stop the attackers, however. In July 2021, instead of data belonging to compromised companies, an advertisement for a new forum called RAMP appeared on the DLS page run by the group **Babuk**:

Fig. 53. New RAMP forum allowing RaaS offers, 2021



According to the forum’s creators, its main goal is to provide a new platform for advertising ransomware affiliate programs. The following programs soon began to be advertised on the new platform: **Lockbit v.2**, **Avos**, **Caodabi Locker**, **RTM**, and **Hive**.

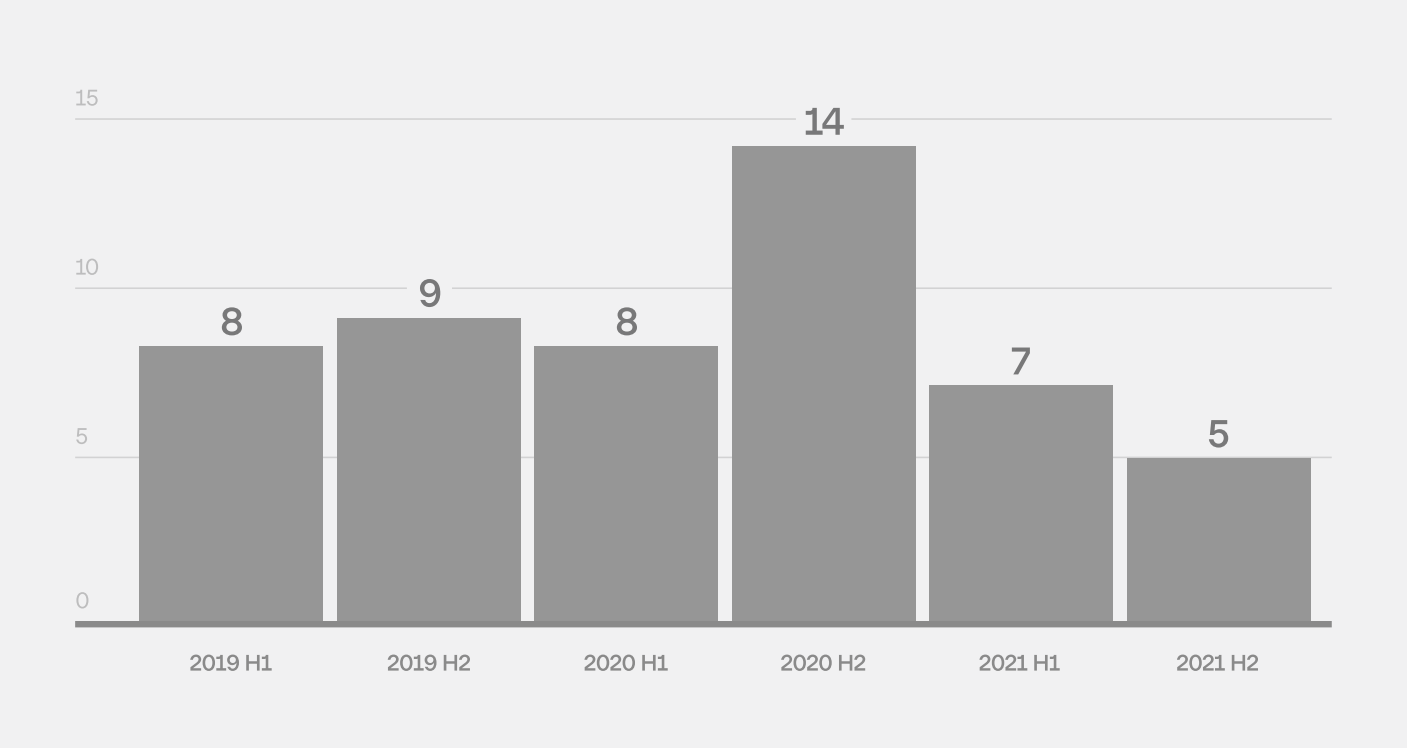
ANALYSIS OF CURRENT RAAS TRENDS 05

Public affiliate programs

As mentioned in the section above, RaaS began gaining momentum back in 2014. However, all modern affiliate programs emerged on the back of the glory gained by the criminal group **GandCrab**.

By public affiliate programs (RaaS), Group-IB refers to forum messages offering to collaborate with a ransomware operator in order to spread malware in return for a percentage of the ransom. Previously, such affiliates were mainly cybercriminals involved in downloading traffic and malware. Now that Big Hunting Game is on the rise, such partners are professional “dark” penetration testers or Initial Access Brokers who gain access to networks belonging to large companies for the purposes of reselling the access or taking part in ransomware affiliate programs.

Fig. 54. Dynamics of new affiliate programs emerging on underground forums



Since 2019, **51 offers of various affiliate programs (RaaS)** have been published on underground forums. Among them were common RaaS such as LockBit, Hive, SunCrypt and Avaddon, as well as others that never became popular (e.g., realOnline Locker, Keystore Locker, Jingo Locker).

During the reporting period (H2 2020—H1 2021), **21 new affiliate programs** emerged on underground forums, which is 19% more than during the previous period (H2 2019—H1 2020), when there were 17 programs. In total, **34 new affiliate programs** were identified in 2020 and 2021.

It is noteworthy that there are still private RaaS programs that hackers can join if they know the right people to contact. In addition, some affiliate programs are being readied, as developers hone their malware to encrypt data. For example, in 2021 Group-IB identified 12 new affiliate programs on underground forums. Four (**Babuk**, **Lockbit**, **Avos**, **Hive**) have well-known DLS resources for publishing data. During the same period, however, Group-IB discovered 29 new DLS resources (not including the above), which suggests that private affiliate programs are behind them.

As can be seen in the above graph, new affiliate programs were most popular in the second half of 2020. In 2021, their number dropped sharply: in the first three quarters of the year, only **12 new affiliate programs** appeared on forums, **which is 14%** less than in the second half of 2020.

The main reasons for the decrease are the following:

1. Publications on new RaaS programs were banned on major underground forums.
2. Many Initial Access Brokers began to openly sell their goods on underground forums, which allows ransomware groups to select victims directly on the forums, like in a store.

Between H1 2019 and H2 2021, at least **15 underground forums** run by Russian-speaking administrators were used to advertise RaaS programs. The main resource was exploit.in (before its administrators banned RaaS in May 2021). The top three forums also include RAMP and xss.is:

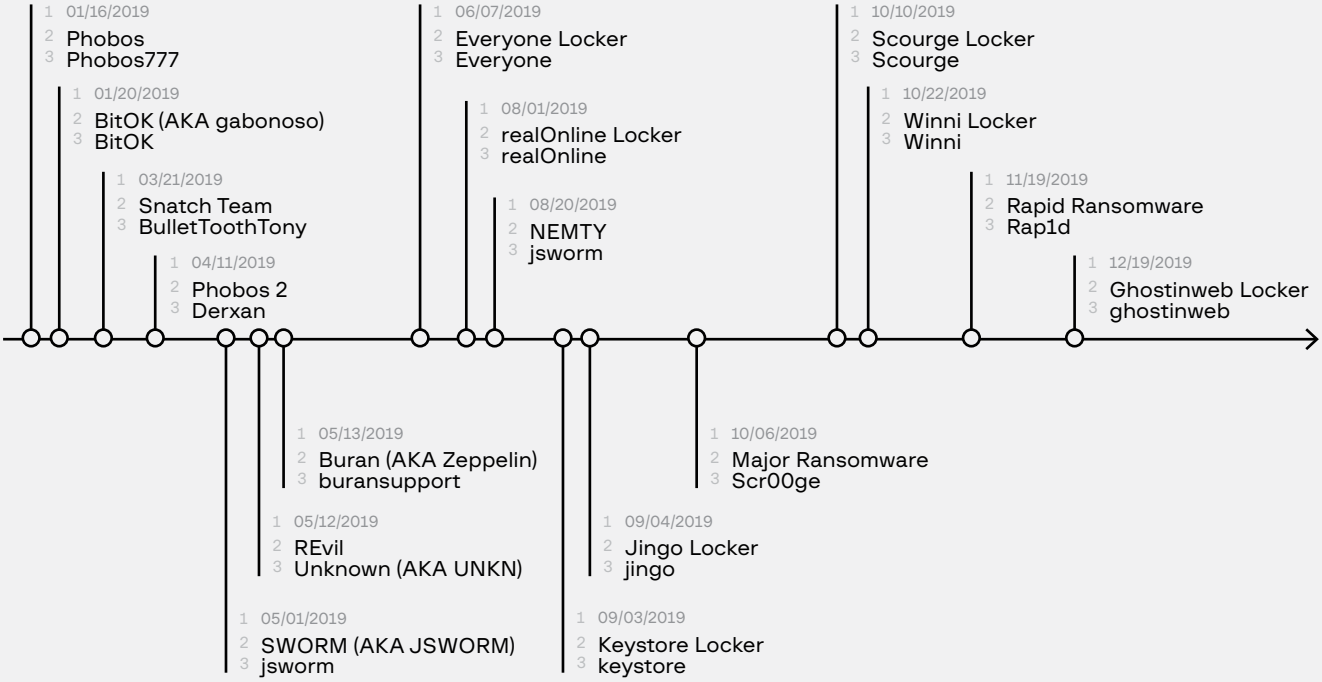
Fig. 55. Distribution of RaaS on underground forums, 2019-2021

Name	Quantity
exploit.in	27
RAMP	5
xss.is	4
center.bz	3
crdclub.ws	2
sindicat.biz	1
xakfor.net	1
sky-fraud.ru	1
wwh-club.net	1
unity	1
v-h.su	1
maza	1
darknet.ug	1
badkarma.ru	1
bhf.io	1

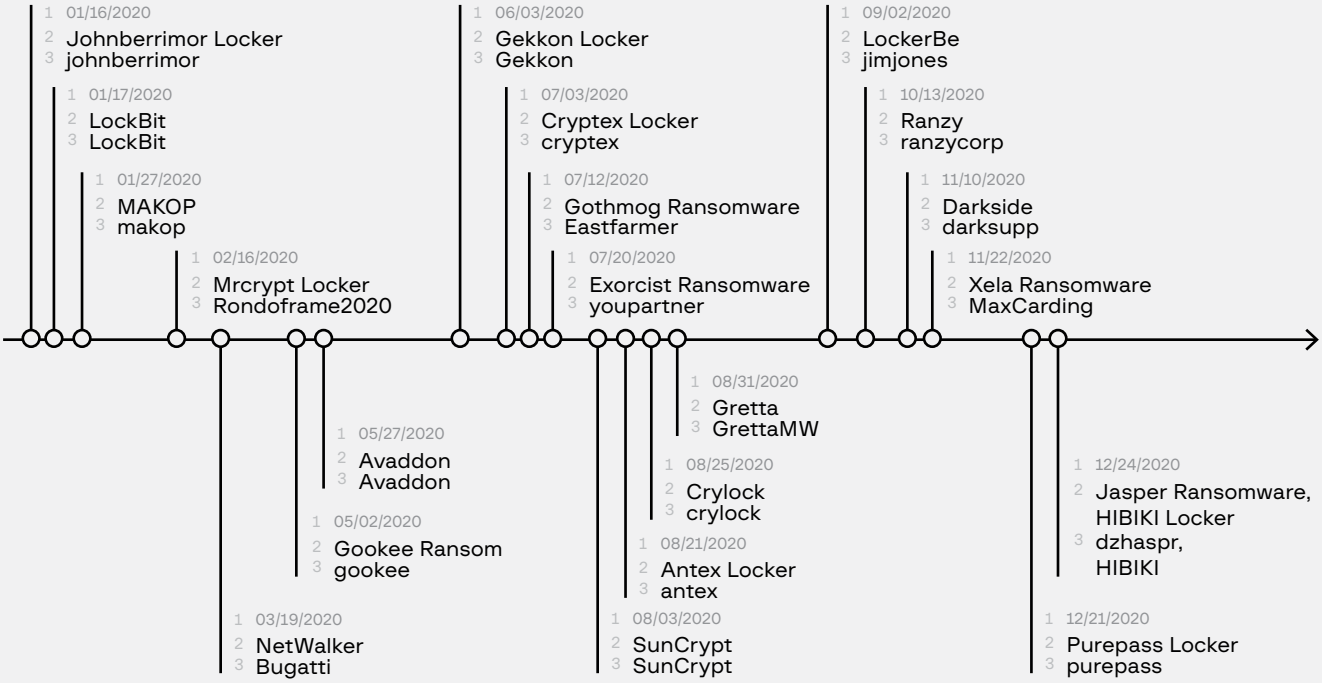
After RaaS was banned on exploit.in, RAMP quickly gained in popularity. The diagram below shows a timeline of when affiliate programs appeared on underground forums starting in 2019. Private affiliate programs are not included on the list.

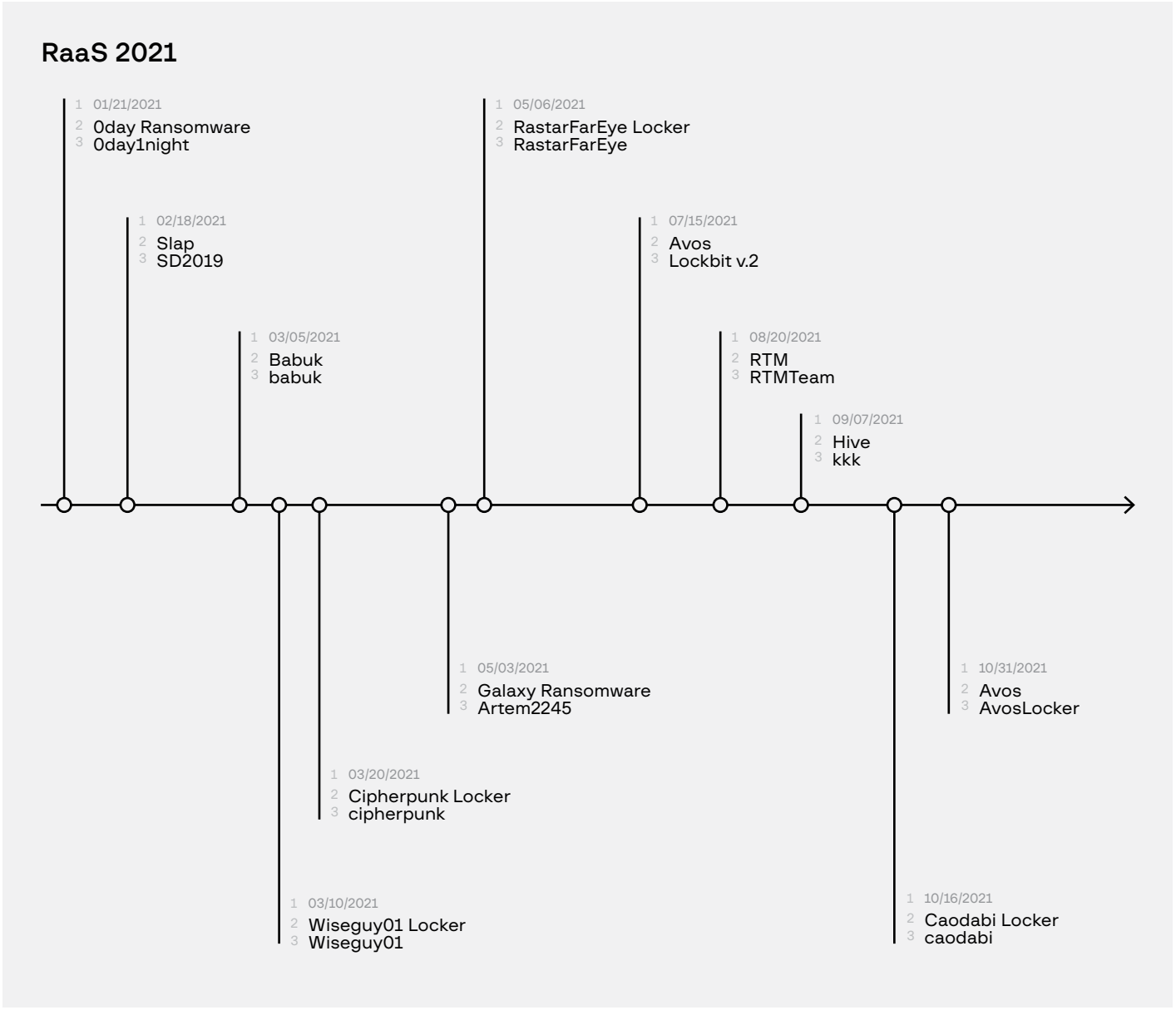
1 — Date
2 — Name
3 — Forum alias

RaaS 2019



RaaS 2020





Analysis of ransomware attacks based on data published on DLS*

As noted in the previous section, DLSs are used by ransomware operators as a **double** extortion technique, i.e., it exerts additional pressure on victims to pay ransoms. As a rule, ransomware operators promise to remove the compromised data from the DLS or to not make it publicly available after the ransom is paid.

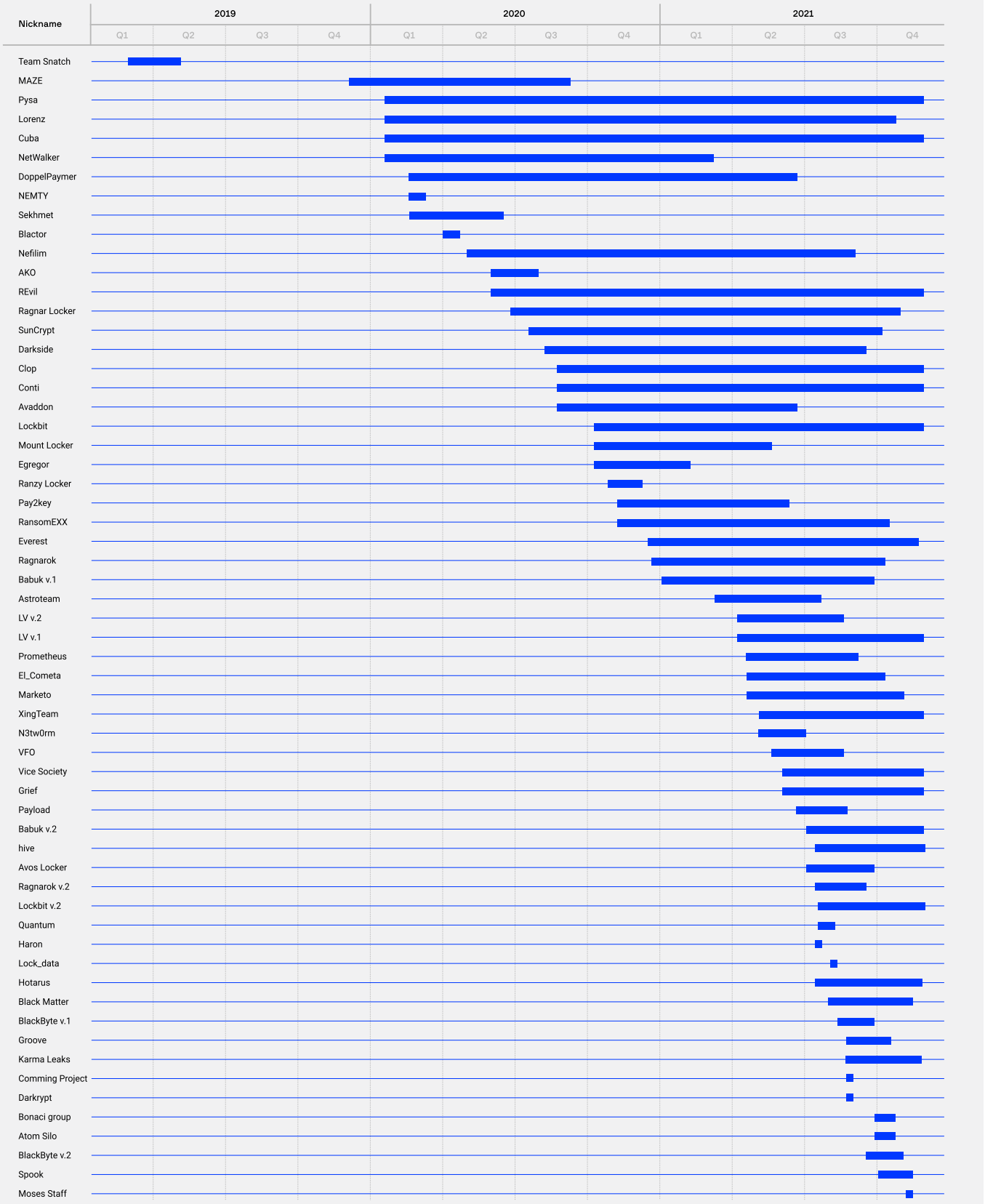
The situation is different in real life, however. According to Group-IB research, even if an ad is removed from the DLS, links that lead to the compromised files (located on other servers used by other cybercriminals) remain accessible.

The technique was first used by the group **Snatch**, but it was made popular by **Maze**, probably because the latter was better known.

The graph below shows which ransomware operators started using DLSs to publish data in chronological order

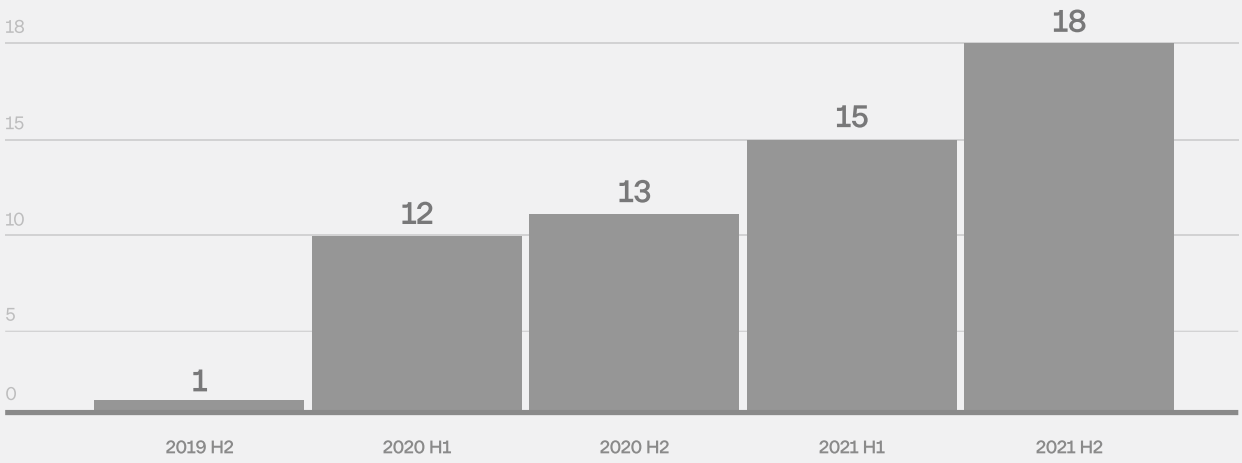
* Data mentioned in this section refers to Q1 2020–Q3 2021 as Q4 2021 has not yet ended.

Ransomware operators using DLS, 2019–2021



As noted in the previous section, the number of new affiliate programs decreased in 2021. This does not prevent new DLSs from emerging, however, which means that many ransomware operators continue to be active without public affiliate programs.

Fig. 56. The emergence of new Data Leak Sites, 2019-2021

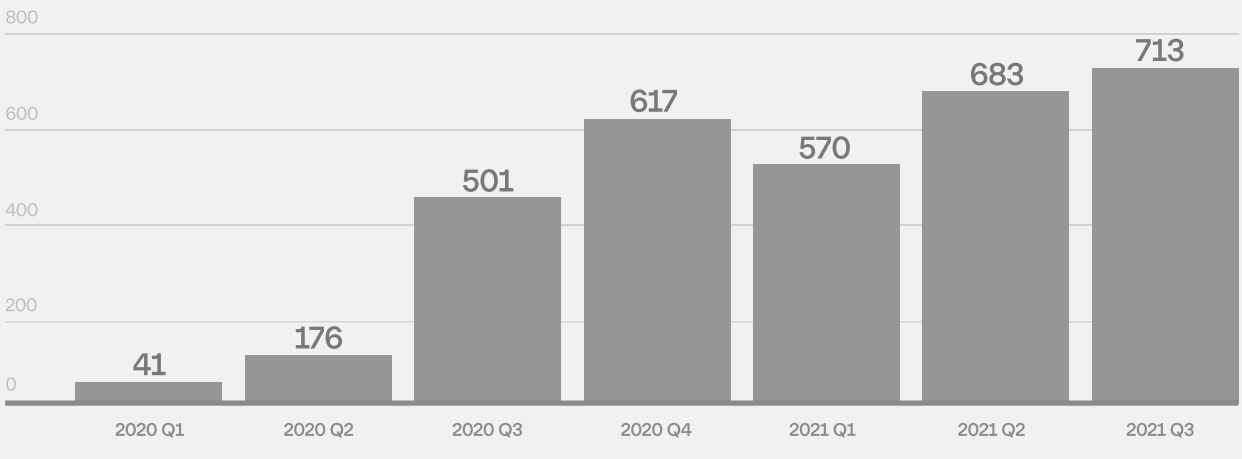


As can be seen from the graph, the number of new Data Leak Sites for publishing data exfiltrated from encrypted networks increased by 115% (from 13 to 28) in the two periods spanning H2 2020 and H1 2021, as compared to H2 2019–H1 2020.

As a result, more and more data belonging to new victim companies has been published on DLSs. During the analyzed period (H2 2020–H1 2021), data belonging to **2,371 companies** was leaked on DLSs. Moreover, during the previous period (H2 2019–H1 2020) only **229 companies** were exposed, which means that the number of companies affected has grown by **935%**.

As such, for the whole of 2020, data belonging to **1,335 ransomware victims** was published on DLSs, and in the first three quarters of 2021 alone, data belonging to **1,966** victims was published, which is **47%** more than for the entire previous year.

Fig. 57. Increase in data publications about compromised companies on DLSs, 2020-2021

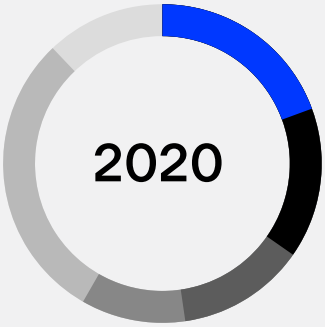


Group-IB experts emphasize that this statistic also partially reflects the fact that more people fall victim to ransomware operators, but it does not reflect the real number of victims. For example, an analysis of **Hive's** administrative panel and the amount of data published on the DLS revealed that only 13% of the group's victims were publicly exposed. This means that the real number of victims may be 10 times higher.

In 2020, the most active groups were **Maze**, **Egregor**, **Conti**, and **REvil**. These groups posted about the most companies on DLSs:

Fig. 58. Distribution of victims exposed on DLSs by ransomware operators, 2020

Name	Quantity	%
MAZE	259	19.4
Egregor	204	15.3
Conti	173	13.0
REvil	141	10.6
Pysa	123	9.2
NetWalker	121	9.1
DoppelPaymer	105	7.7
Ragnar Locker	24	1.8
Darkside	24	1.8
Other	161	12.1



In 2021, the situation changed: the percentage of companies victimized by major threat actors fell while the number of small groups of ransomware operators increased. Nevertheless, Conti remains the leader in terms of the number of victims, followed by Lockbit:

Fig. 59. Distribution of victims by ransomware operator, 2021

Name	Quantity	%
Conti	361	16.5
Lockbit	251	11.5
Avaddon	164	7.5
REvil	155	7.1
Pysa	118	5.4
DoppelPaymer	99	4.5
Darkside	75	3.4
Clop	73	3.3
Marketo	63	2.9
Grief	52	2.4
Prometheus	48	2,2
hive	48	2.2
Other	628	31.1

The United Stateswere the country attacked most often in 2020, followed by Canada and the United Kingdom. The top five attacked countries also included France and Germany:

Fig. 60. Distribution of victims by region, 2020

Country	Quantity	%
US	740	54.9
Canada	97	7.2
UK	78	5.8
France	66	4.9
Germany	50	3.7
Italy	43	3.2
Australia	29	2.2
Spain	27	2.0
Brazil	24	1.8
India	16	1.2
Switzerland	13	1.0
Other	131	12.2

The situation did not change significantly in 2021 for the countries with the largest number of ransomware victims. France appeared in the top 3, however, while Germany fell to sixth place.

Fig. 61. Distribution of victims by region, 2021

Country	Quantity	%
US	968	49.4
Canada	110	5.6
France	103	5.2
UK	92	4.7
Italy	76	3.9
Germany	72	3.6
Spain	42	2.1
Australia	41	2.1
Brazil	39	2.0
India	24	1.2
Netherlands	22	1.1
Other	295	6.0

In 2020 and 2021, the regions with the most victims were North America, Europe and the Asia-Pacific region:

Fig. 62. Distribution of victims by region, 2020-2021

2020

Region	Quantity
North America	845
Europe	324
APAC	82
Latin America	41
Middle East	27
Africa	14
Other	2

2021

Region	Quantity
North America	1213
Europe	598
APAC	199
Latin America	93
Middle East	50
Africa	21
Other	8

The main industries targeted in 2020 were manufacturing, real estate, and transportation:

Fig. 63. Distribution of victims by industry, 2020

Industry	Quantity
Manufacturing	142
Real estate	132
Transportation	113
Commerce and shopping	82
Professional services	81
Healthcare	71
Information technology	66
Education	57
Financial services	57
Other industry	53
Government and military	53
Food and beverage	50
Science and engineering	46
Consumer goods	42
Energy	35
Administrative services	34
Messaging and telecommunications	25
Privacy and security	21
Consumer electronics	20
Media and entertainment	20
Travel and tourism	19
Software	16
Clothing and apparel	15
Natural resources	14
Hardware	12
Agriculture and farming	10
Other	49

The situation in 2021 remained almost unchanged, which suggests that attackers mainly targeted the same types of companies that they believe to be the most profitable.

Fig. 64. Distribution of victims by industry, 2021

Industry	Quantity
Manufacturing	210
Real estate	207
Transportation	178
Professional services	169
Financial services	140
Commerce and shopping	128
Healthcare	125
Other	104
Information technology	97
Government and military	82
Food and beverage	79
Science and engineering	75
Education	70
Energy	50
Administrative services	45
Consumer goods	43
Hardware	40
Messaging and telecommunications	31
Media and entertainment	30
Privacy and security	29
Travel and tourism	27
Software	27
Clothing and apparel	24
Consumer electronics	23
Natural resources	23
Sales and marketing	21
Data and analytics	18
Agriculture and farming	16
Other	56

Overview of tactics, methods and techniques used in ransomware attacks

The market for ransomware as a service (RaaS) has rapidly expanded and many financially motivated groups have shifted their focus to ransomware attacks, two factors which both led to a spike in the number of investigated incidents of this kind.

In Q1-Q3 2021, ransomware attacks accounted for over 60% of all incidents investigated by Group-IB. However, despite the fact that this type of attack has increased rapidly and that many different cybercriminal groups have been involved, there have been substantial overlaps in the tactics, techniques and procedures used by attackers. Furthermore, the typical set of ransomware techniques and tools has remained essentially the same. This may be because these tools have been reliably proven to help attackers achieve their goals, as well as to create training materials that allow even inexperienced hackers to get involved in malicious activities.

A good relevant example is the Conti affiliate guide, which was made public in August 2021 by a former participant known as **m1Geelka**.

60%

In Q1-Q3 2021, 60% of all incidents investigated by Group-IB were ransomware attacks

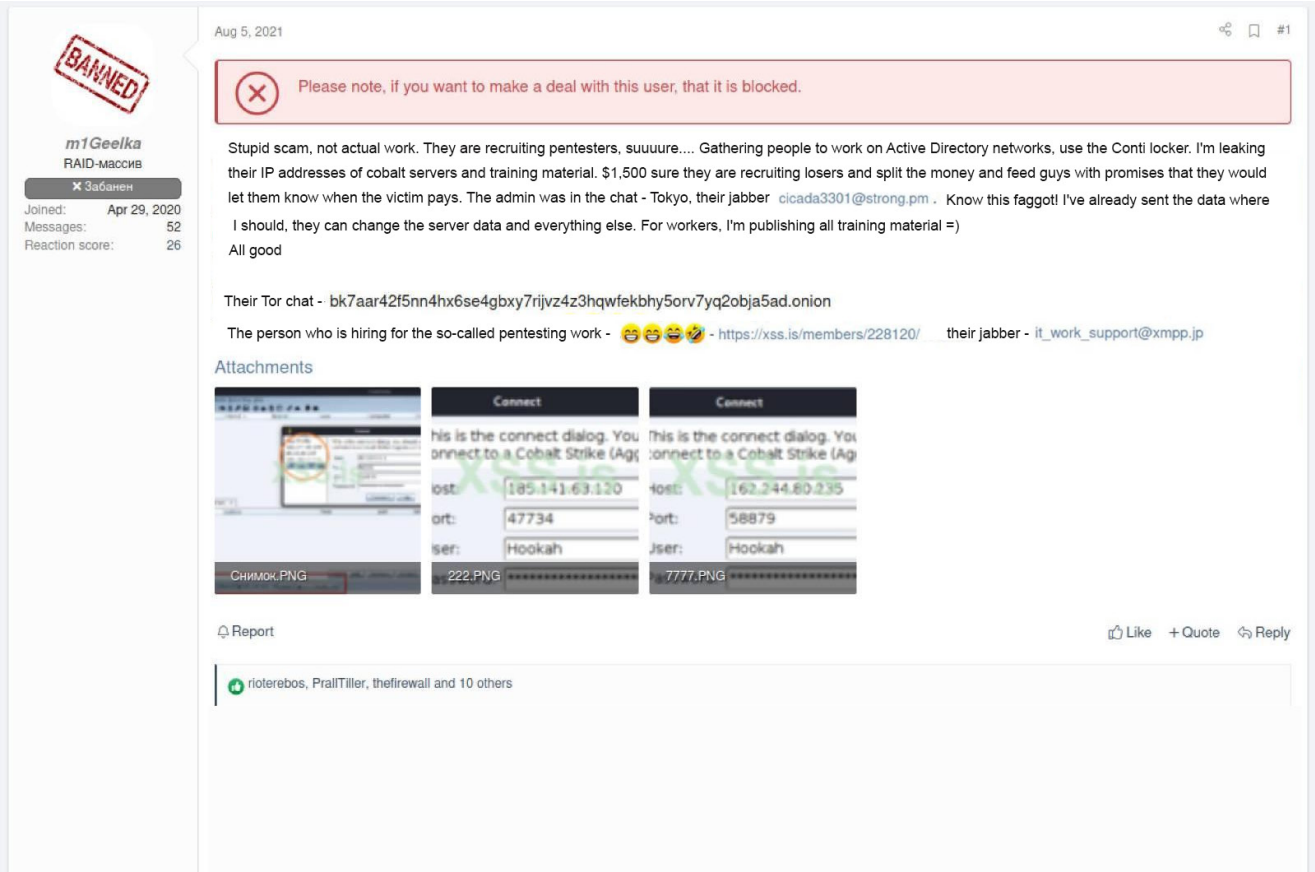


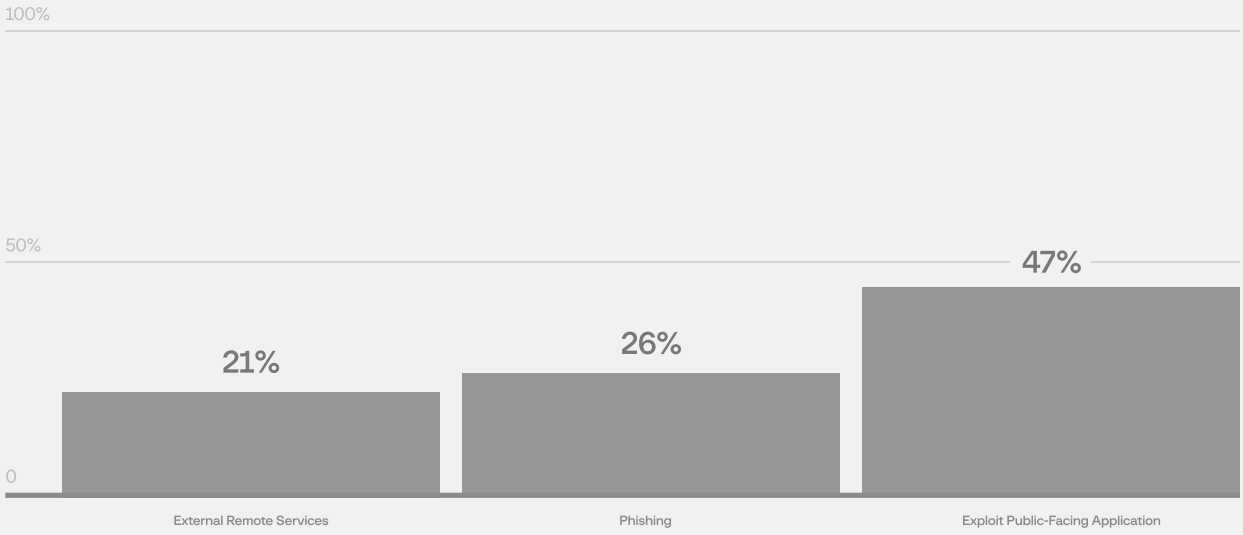
Fig. 65. Conti's affiliate program guide, made publicly available in 2021

Another factor that has significantly influenced the volume and success of ransomware attacks was the development of a market for initial access brokers, which allowed many attackers to gain easy access to networks.

In general, similarly to the previous reporting period, the most commonly used initial access techniques were:

- Compromising remote access services
- Phishing
- Exploiting publicly-facing applications

Fig. 66. Breakdown of methods used to gain initial access, 2020—2021



Use of RDP and VPN

The most common method of compromising remote access services remains attacking publicly accessible terminal servers with available Remote Desktop Protocol (RDP) connections. In such cases, attackers most often gain access by brute-forcing passwords, for example by using NLBrute.

In some cases, attackers exploited the BlueKeep (CVE- 2019-0708) vulnerability. Despite its instability, this technique proved to be effective in some cases.

The lack of multifactor authentication allowed attackers to actively compromise accounts and establish connections via VPNs. Moreover, a number of vulnerabilities (including old ones such as those in Pulse Secure and Fortinet) also made it possible to use VPNs to access corporate networks.

The popularity of RDP and VPNs is visible on underground forums, too:

RDP protocol

for connecting users to remote desktops through terminal servers

Topic name

We will buy access from you

Topic message

Hi!

We're recruiting regular brokers of access to corporate networks
We buy vpn, rdp, citrix access with domain administrator rights
Country criteria (except Russia and CIS) and revenue:
USA - from 5kk
Europe - 20kk
Third world - 40kk
We'll also consider individual cases with little deviation from the criteria
The types of activity we do not accept: healthcare, education, government, non-commercials
Contacts in PM
A deposit on this and the neighboring forums has been made, link is in PM
We're also willing to take your access with a commission

Fig. 67. A post about wanting to buy access to corporate networks on an underground forum, 2021

Almost immediately after the post was published, recent vulnerabilities allowing initial access to networks were exploited in ransomware attacks.

For instance, **Conti** and **AvosLocker** affiliates actively used ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), which enabled them to attack vulnerable Microsoft Exchange servers in much the same way as state-sponsored groups.

Another example is **HelloKitty**: ransomware that gained prominence after attacking **CD Projekt RED** in which affiliates exploited vulnerable SonicWall devices. They first used an old vulnerability (CVE-2019-7481), then a recent one (CVE-2021-20016).

In some cases, attackers used zero-day vulnerabilities. A good example is the **REvil** affiliate attack against **Kaseya** that exploited zero-day vulnerabilities, which were subsequently labeled CVE-2021-30116, CVE-2021-30119 and CVE-2021-30120.

Use of botnets

To gain initial access, ransomware operators continue to actively use popular botnets, in particular **IcedID**, **Qakbot**, **Hancitor**, and **Trickbot**.

As often as not, the content of emails sent by threat actors is trivial, while the malicious document that is attached contains instructions for running a macro that will download a bot to the compromised computer.

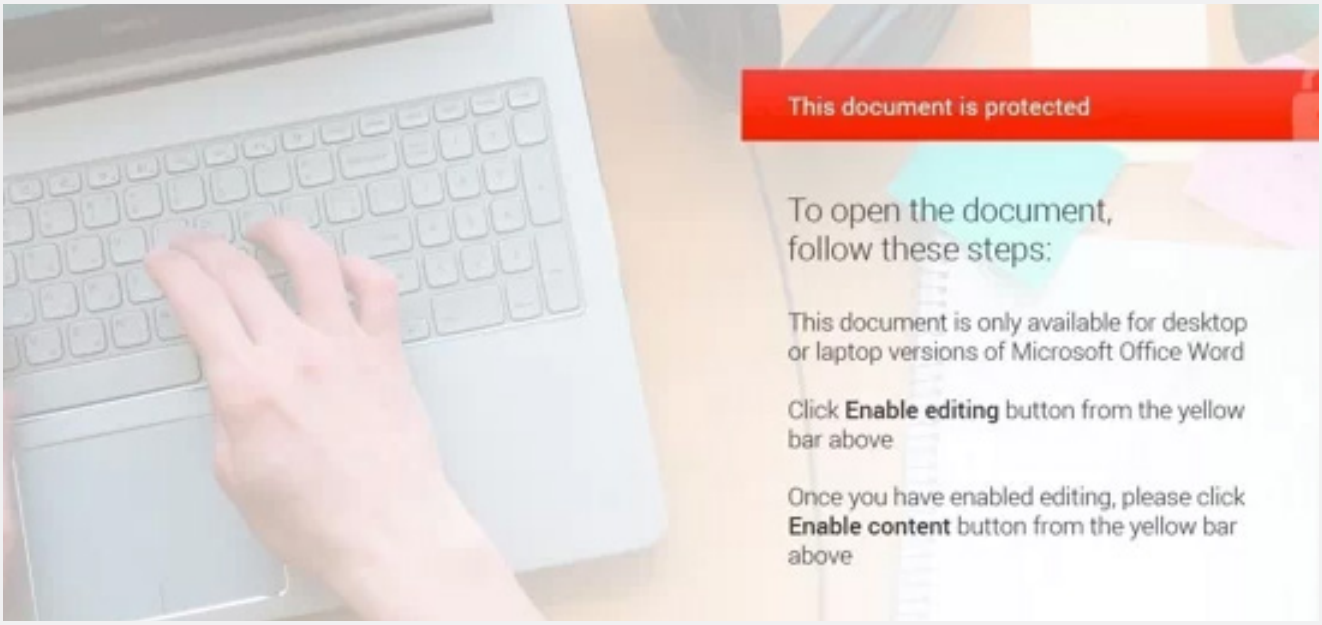


Fig. 68. Contents of a malicious document used by Hancitor operators, 2021

In some cases, attackers also exploited vulnerabilities to download and run malicious code. For example, **BazarLoader** operators (active distributors of Ryuk ransomware) exploited a vulnerability in MSHTML (CVE-2021-40444) to infect documents shared by email.

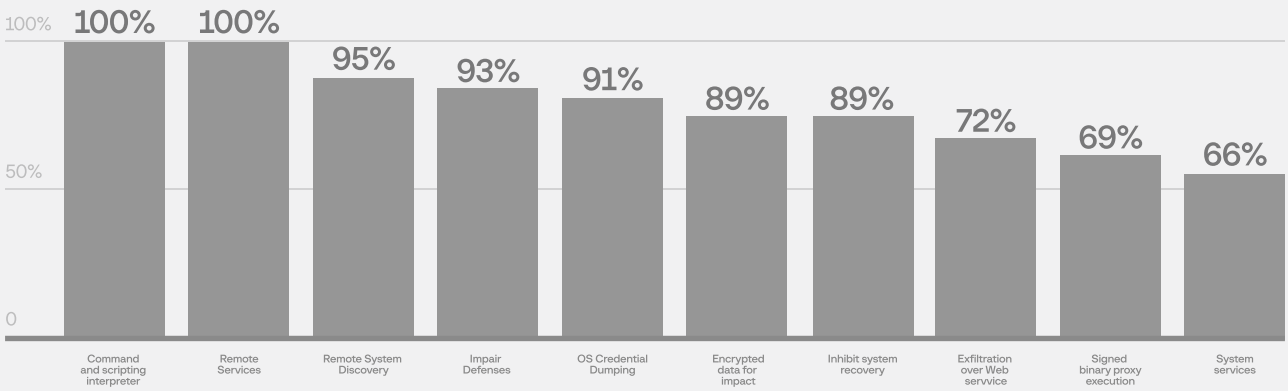
In addition to traditional phishing, BazarLoader operators also used **vishing**. They sent emails containing information about a paid subscription and phone numbers to cancel it. The victims who called were told to visit the website and download a subscription cancellation form, which was in fact a malicious document.

Fig. 69. An example of a phishing website that users visited after communicating with the attackers, 2021

Post-exploitation techniques

With regard to post-exploitation, Group-IB experts identified the attack techniques most frequently used in security incidents.

Fig. 70. Techniques popular with attackers, 2020-2021



Use of command and script interpreters

Traditionally, **command and script interpreters** are widely used in attacks. Threat actors used them in 100% of incidents investigated by Group-IB

The following interpreters are especially noteworthy:

- Windows command prompt
- PowerShell
- Visual Basic
- JavaScript

The first two are traditionally used by threat actors at various stages of the attack lifecycle, while Visual Basic is actively exploited by malicious macros. JavaScript is less common, which means that it is more difficult to detect and more likely to result in the target being compromised.

IcedID operators, who have worked with representatives of various affiliate programs, used JavaScript files packed in ZIP archives to deliver payloads. Links to the archives were posted on Google sites, which threw the victims off their guard. Moreover, victims were asked to log into their Google account, after which the archive was downloaded automatically.

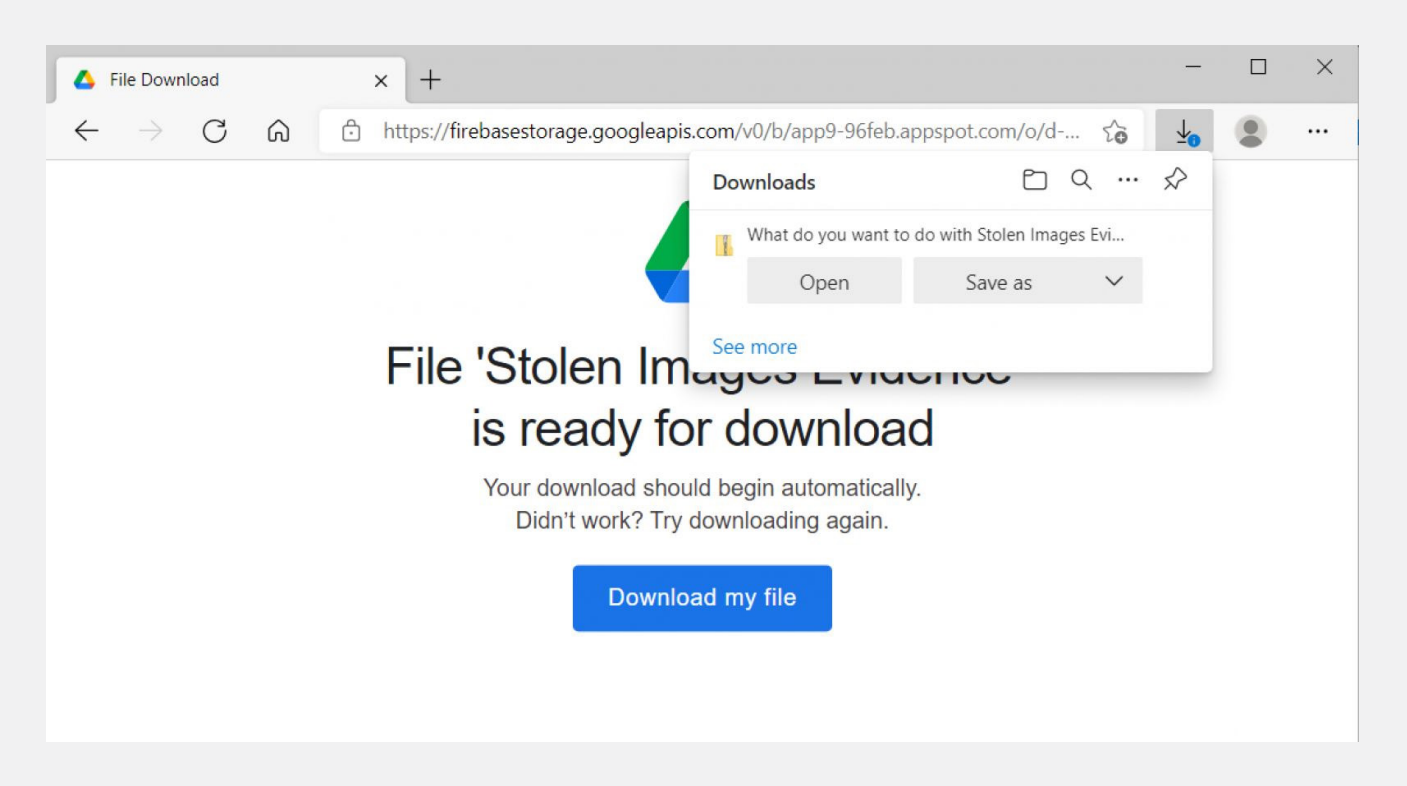


Fig. 71. An archive with a malicious JavaScript file, 2021

The group **OldGremlin**, which attacked companies in Russia by actively using the NodeJS interpreter, is especially worth highlighting.

In most cases, gaining access to the corporate network is merely the first stage of an attack lifecycle. Attackers use any means available to escalate existing privileges and move across the network. This claim is corroborated by the fact that Group-IB has seen remote access services used in attacks **100% of the time**.

Remote Desktop Protocol (RDP) remains one of the most common methods. Some threat groups even have specific scripts to enable this type of access.

For example, **REvil** affiliates have used the following script:

```
(Get-WmiObject Win32_TerminalServiceSetting -Namespace root\cimv2\
TerminalServices).SetAllowTsConnections(1,1)
(Get-WmiObject -Class «Win32_TSGeneralSetting» -Namespace root\cimv2\
TerminalServices -Filter «TerminalName='RDP-tcp'»).SetUserAuthentica-
tionRequired(0)
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\
Terminal Server\WinStations\RDP-Tcp' -name «UserAuthentication»
-Value 1
Enable-NetFirewallRule -DisplayGroup «Remote Desktop»
```

The Server Message Block (SMB) protocol is no less popular, for both moving across the network and deploying ransomware.

Methods of collecting data on remote systems

No discussion about moving across networks would be complete without mentioning methods of **collecting data about remote systems**. Attackers actively rely on various network scanners as well as Active Directory data collection tools. However, some cases involved Windows admin tools, such as PowerShell:

```
Get-ADComputer -Filter {enabled -eq $true} -properties * | select
Name, DNSHostName, OperatingSystem, LastLogonDate | Export-CSV C:\
temp\AllWindows.csv -NoTypeInformation -Encoding UTF8
```

Scenarios to neutralize defenses

It would be nearly impossible to successfully deploy ransomware without **neutralizing defenses** first. Pre-recorded scripts are often used for this purpose and they are run on target hosts by modifying a group policy or PsExec. Moreover, many samples of ransomware also contain lists of defensive processes and services to be disabled while running the malware. For instance, “sophos” (a string referring to a popular antivirus tool) was among strings used by a sample of **BlackMatter** ransomware to identify processes and services to disable.

Account data dumping

Account data dumping remains highly popular. In addition to widespread tools such as Mimikatz, which are easily detected by network defenses, hackers have begun to use subtler methods, including some based on exploiting built-in Windows elements. One example is comsvcs.dll, a library allowing for a memory dump of a specific process, including lsass.exe:

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 900
C:\Users\Public\lsass.dmp full
```

Attackers used **data encryption for extortion in 89% of the incidents** investigated by Group-IB. The remaining 11% is explained by malefactors restricting themselves to downloading data and customers detecting suspicious activity before ransomware was deployed.

As part of the same 89% of incidents, attackers **breached system recovery tools** by damaging Windows backup shadow copies. This functionality was sometimes a part of the ransomware itself and sometimes implemented through scripts. Usually, either vssadmin or Windows Management Instrumentation was exploited for the purpose:

```
wmic shadowcopy delete /nointeractive
```

Using web services

Many groups engaging in ransomware attacks still actively download data from compromised networks. **Web services** are often used for that purpose. Various cloud storage systems are especially popular: MEGA, DropMeFiles, and SendSpace to name just a few.

Executing code through a signed application

Speaking of popular post-exploitation techniques, we cannot overlook **execution of code through a signed application**. Exploiting rundll32.exe and regsvr32.exe are good examples of this technique. For example, IcedID operators used rundll32.exe to launch the uploaded malicious payload:

```
C:\Windows\System32\rundll32.exe»
«C:\users\public\leftSwapStorage.jpg,PluginInit
```

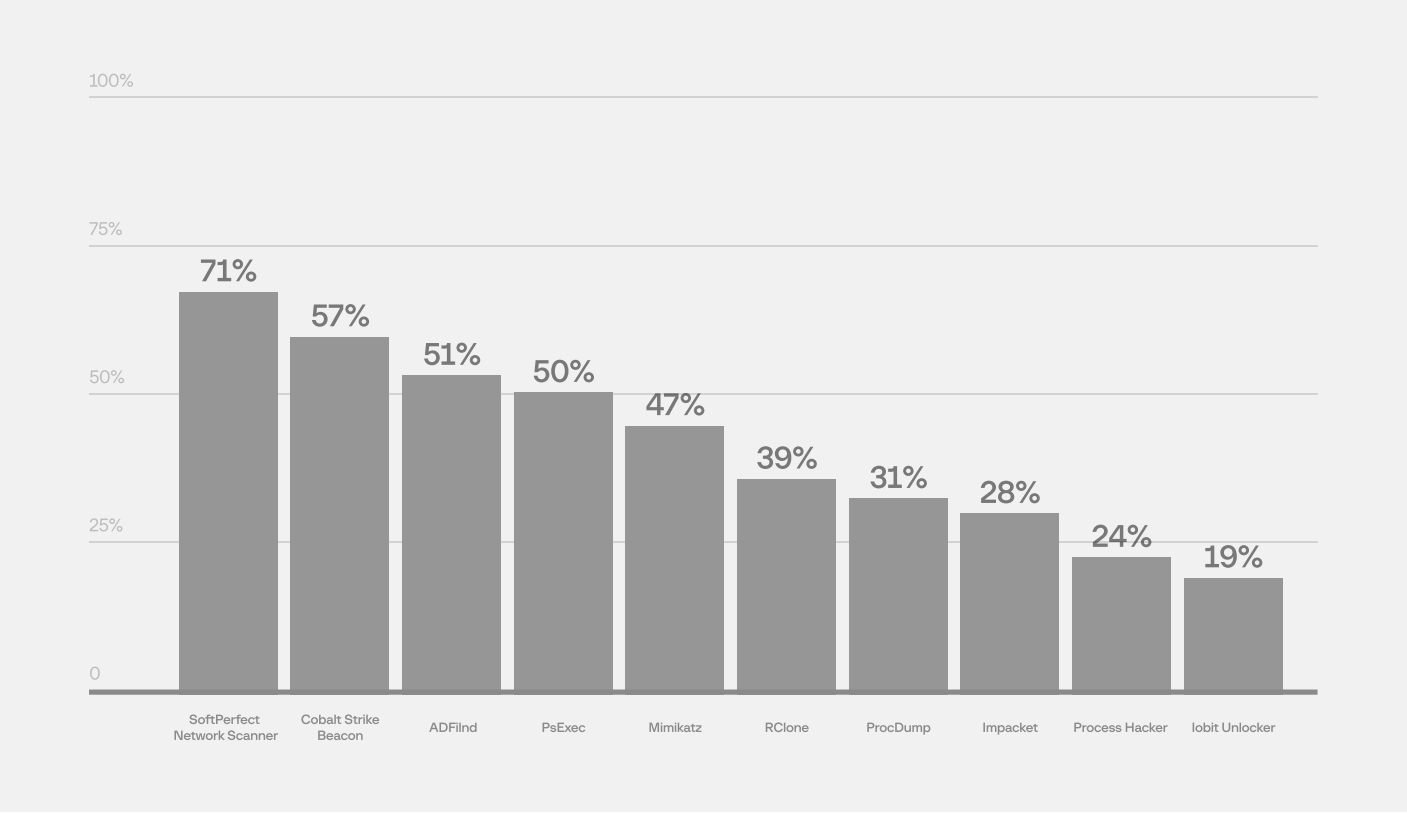
Using system services

The last technique is the use of system services. The method largely has to do with criminals' propensity to frequently use PsExec and its implementations, including those that are part of post-exploitation frameworks such as Cobalt Strike.

Top 10 most popular tools used in ransomware attacks

A list of the ten most popular tools encountered by Group-IB experts in their response to ransomware attacks is provided below.

Fig. 72. The most popular tools used by ransomware operators in 2021, according to Group-IB



As noted above, one of the key goals for ransomware operators is to identify vulnerable remote systems to be able to move through the network or deploy ransomware. The most popular tool to achieve this goal is **SoftPerfect Network Scanner**, a commercially available network scanner which was found in the toolkits used in 71% of all the attacks investigated by Group-IB.

Cobalt Strike was another highly popular tool. Group-IB detected its use in 57% of all incidents. In some cases, attackers replaced bots with Beacon, the main payload of Cobalt Strike, for their phishing campaigns. Attackers have thus been sending phishing emails with malware-infected document attachments to deliver the Squirrelwaffle loader, which was then used to load Cobalt Strike Beacon.

Almost as often as Cobalt Strike, attackers used **ADFind**, a tool for collecting Active Directory data. Attackers loaded ADFind in the early stages of an attack to explore the compromised infrastructure. It was usually launched using scripts, for example:

```
adfind.exe -f «(objectcategory=person)»
adfind.exe -f «(objectcategory=organizationalUnit)»
adfind.exe -f «objectcategory=computer»
adfind.exe -gcb -sc trustdmp
adfind.exe -f «(objectcategory=group)»
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -sc trustdmp
```

As noted above, one of the goals for ransomware operators is to navigate through a network, which includes executing commands and malicious code on remote hosts. In relation to this, traces of **PsExec** have been identified in approximately half of all incidents investigated by Group-IB, both as a way to run commands and as a direct method of propagating ransomware.

Mimikatz, a tool for extracting account data and memory dumps, is still relevant. Moreover, criminals are also using its variants, e.g. the Invoke-Mimikatz version for PowerShell and the Python-focused version Pypykatz.

Some ransomware operators have made life easier for their affiliates by expanding their arsenal with tools for automated data collection and downloading. StealBit by LockBit ransomware operators is a good example. However, many affiliates still use their own tools to download data from compromised systems. **RClone** has become the most popular tool for this purpose. Group-IB observed its use in 39% of all ransomware incidents.

Given that popular tools for extracting user account data from memory are easy to detect, some criminals resort to legitimate tools for dumping lsass.exe. Group-IB has identified the use of **ProcDump** in 31% of all ransomware incidents.

Besides PsExec, criminals have widely used the SMBExec script from the **Impacket** package to run commands on remote hosts. Group-IB has seen it used in 28% of ransomware incidents.

Process Hacker, a popular tool for monitoring system resources, has also been frequently used by ransomware operators to collect information about the security tools in use, then circumvent or disable them.

Iobit Unlocker was another tool used for similar purposes. The tool was identified in 19% of ransomware attacks and, among other things, was used to terminate processes that interact with databases, thereby preventing their encryption.

The list of techniques and tools described here is not exhaustive. Group-IB intends to publish a detailed analysis of the tactics, techniques and procedures typical of ransomware attacks in our upcoming report entitled **Ransomware 2021-2022**.

Ransomware Uncovered 2020—2021

BEHIND THE SCENES OF RANSOMWARE OPERATORS

06

An inside look at affiliate programs, ransomware groups' forum activity and Hive attack statistics. This is what affiliate program interface looks like

History of Hive and DLS discussion

The first activity of the criminal group **Hive** was detected in June 2021. By July 25, 2021, the group had a DLS with one victim.

Fig. 73. DLS of the group Hive, 2021

Hive used a combination of AES/RSA to encrypt the victim's data. After the data was encrypted, the malware uploaded it to a remote server. Encrypted files can be recognized by their .hive extension.

Hive did not have any public affiliate programs, so it was initially unclear whether the group was using the RaaS business model or was an impossible-to-join private group.

DLS was different in that it was running through API. Only two groups besides Hive have used API: **Grief** and **DoppelPaymer**.

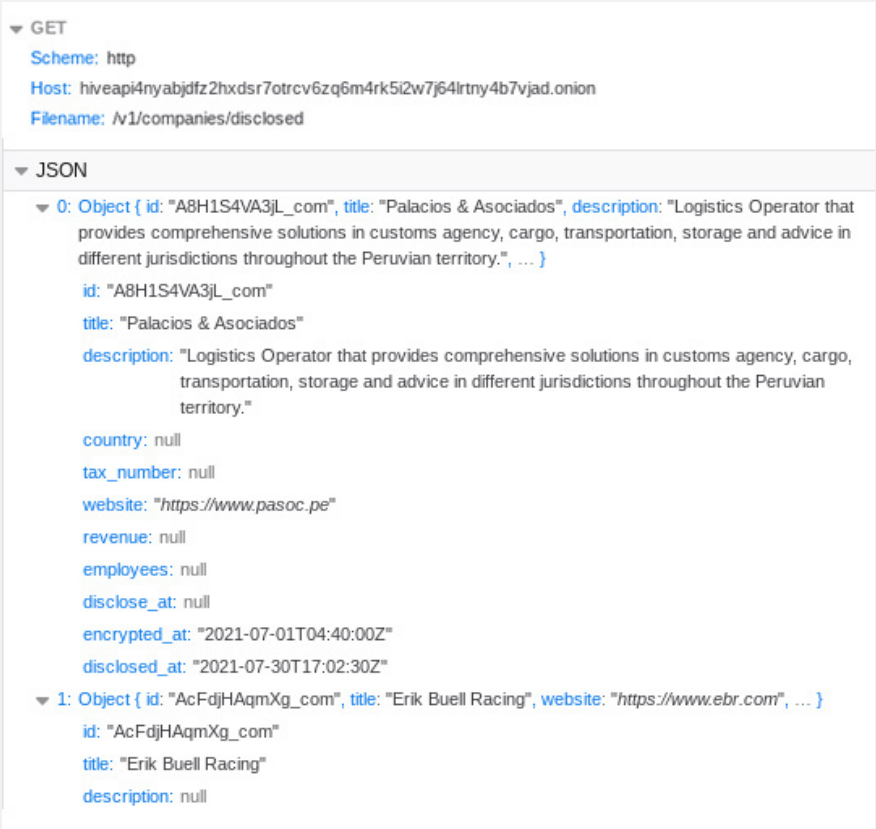


Fig. 74. Response from the server used by Hive, 2021

Hive uploaded stolen files to file sharing resources such as **sendspace**, **anonfiles**, and **send.exploit**. Curiously, the size of uploaded files was often less than 500 MB, and only one data leak exceeded 200 GB.

Hive and RAMP

The user kkk posted a message on the private forum RAMP on September 7, 2021, advertising an affiliate program.

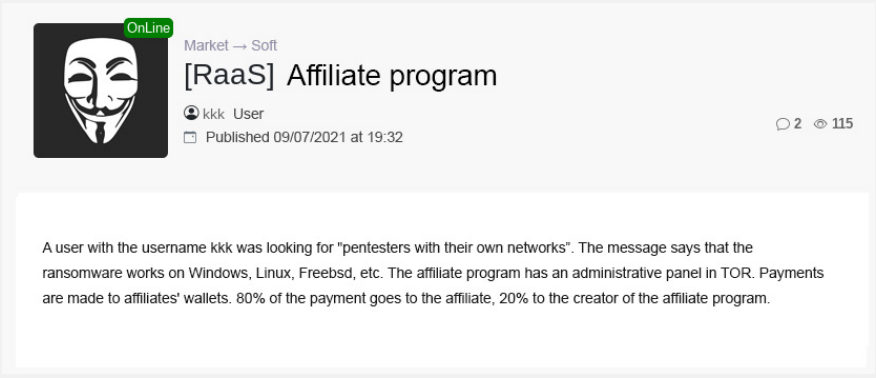


Fig. 75. Message announcing search for a pentester, 2021

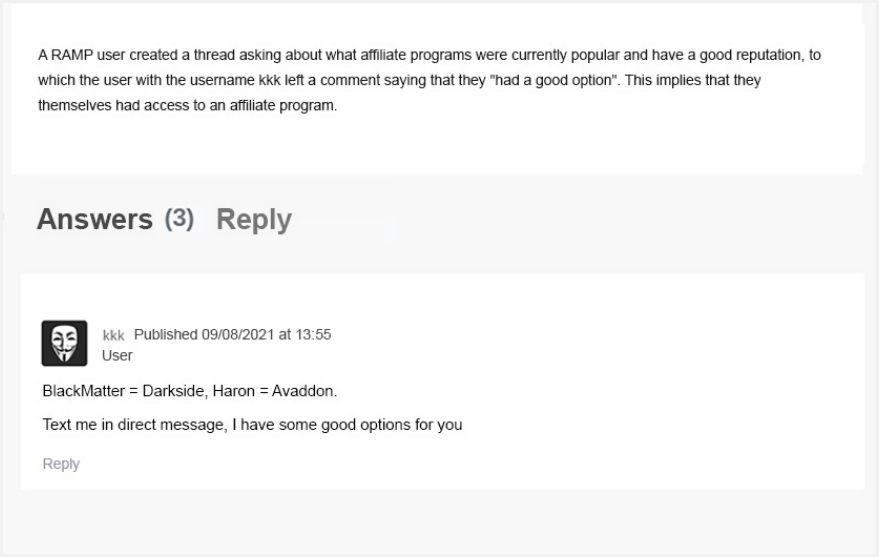


Fig. 76. Answer related to search for a pentester, 2021

By communicating with the abovementioned threat actor, details about the malware were obtained:

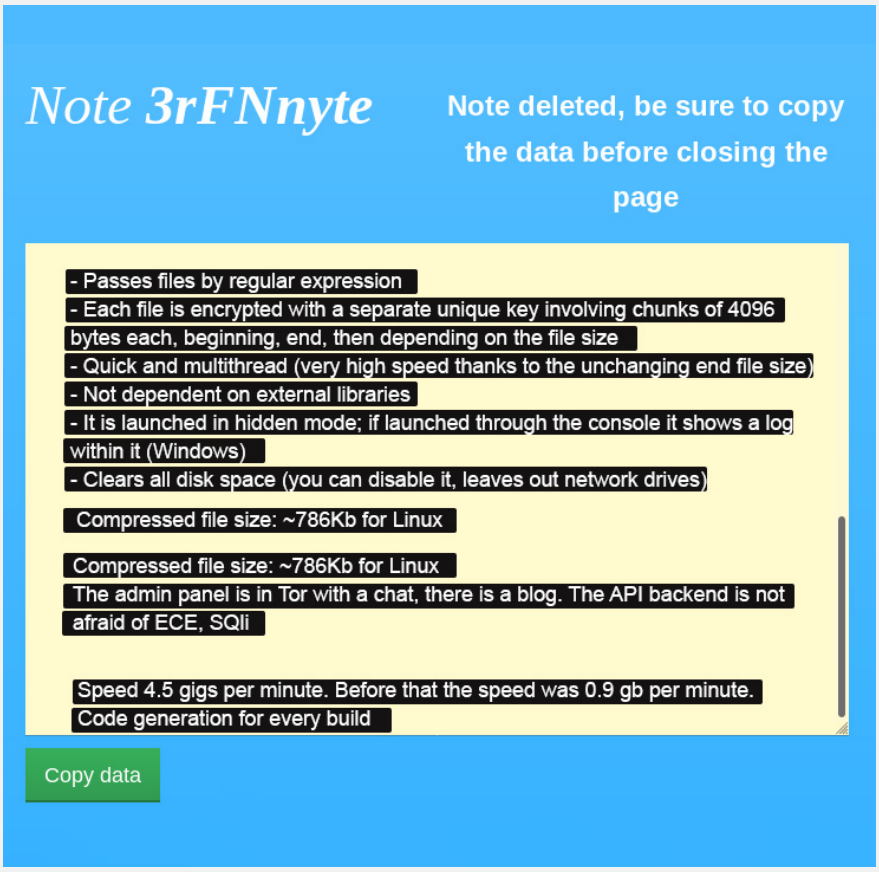


Fig. 77. Malware details, 2021

When Group-IB experts read the ransomware parameters, they concluded that it was Hive. Subsequent communication with kkk confirmed this.

Hive affiliate program from the inside

Communicating with a cybercriminal helped gain access to a private affiliate program. The hacker provided an address for the admin panel and login information.

After accessing to the admin panel located at hxxp://hiveaffi5ci2xxaz2fj-frfi5mwpqvuw4wtomc3fflzcvopxt2654ryqd[.]onion/auth, Group-IB experts were able to confirm their suspicions that it was a Hive affiliate program.

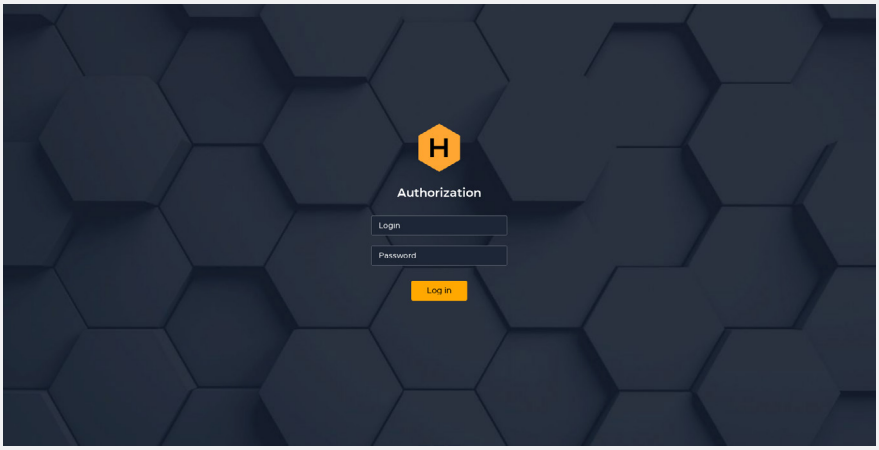


Fig. 78. Hive admin panel login screen, 2021

Upon entering the credentials provided by the threat actor, the home page of the affiliate program opens.

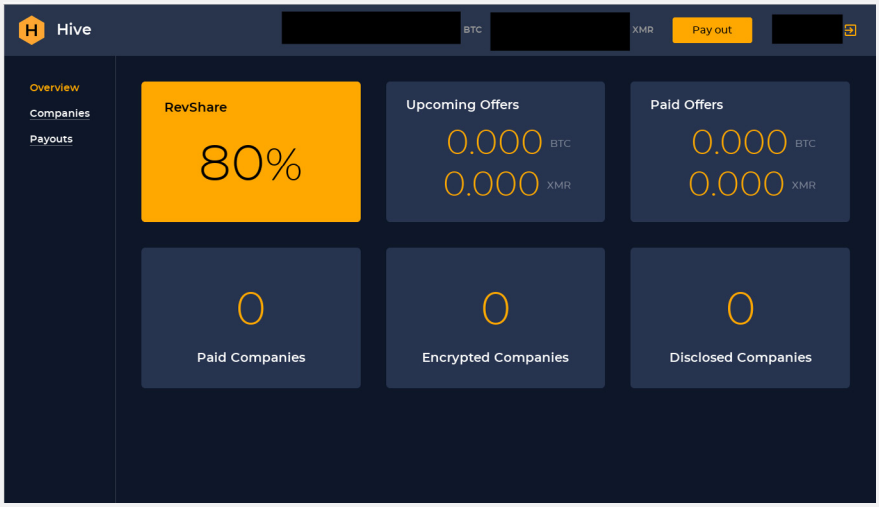


Fig. 79. The home page of the Hive affiliate program, 2021

The home page provides a brief summary and key statistics: what percentage of the ransom is paid to the criminal affiliate, how much money they can expect to be paid in the future, and how much they have received so far, as well as the number of companies that have paid up and have had their data encrypted and decrypted. The total balance and the username (redacted in the screenshot) are also displayed. The “Payouts” tab provides a way to transfer funds from the criminal affiliate program to the affiliate’s personal wallet.

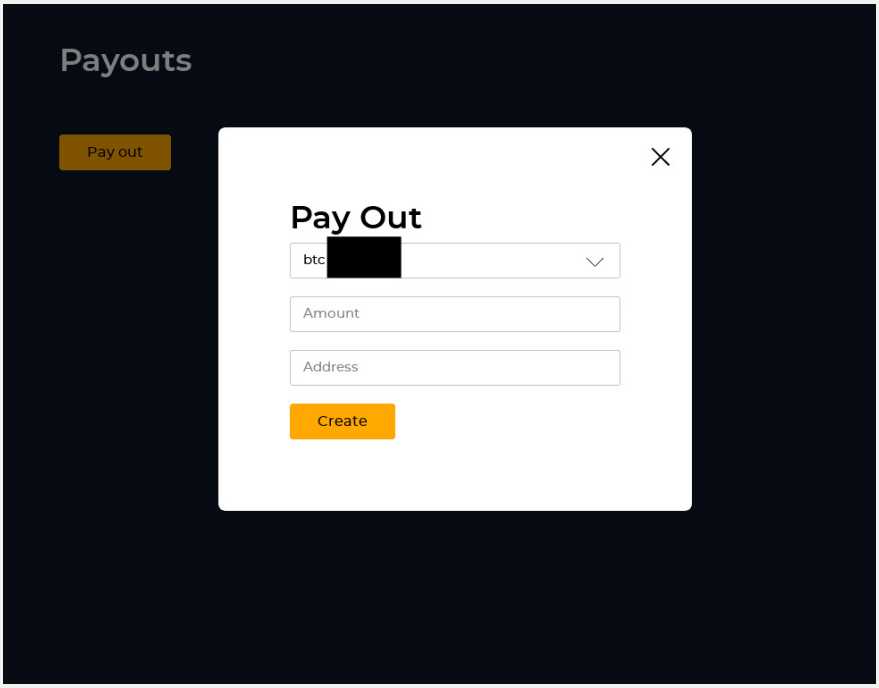


Fig. 80. "Payouts" tab in the Hive affiliate program, 2021

The most intriguing data can be found under the "Companies" tab. Here the criminals record the victim company's name and website, a brief description, and sometimes its annual revenue and number of employees.

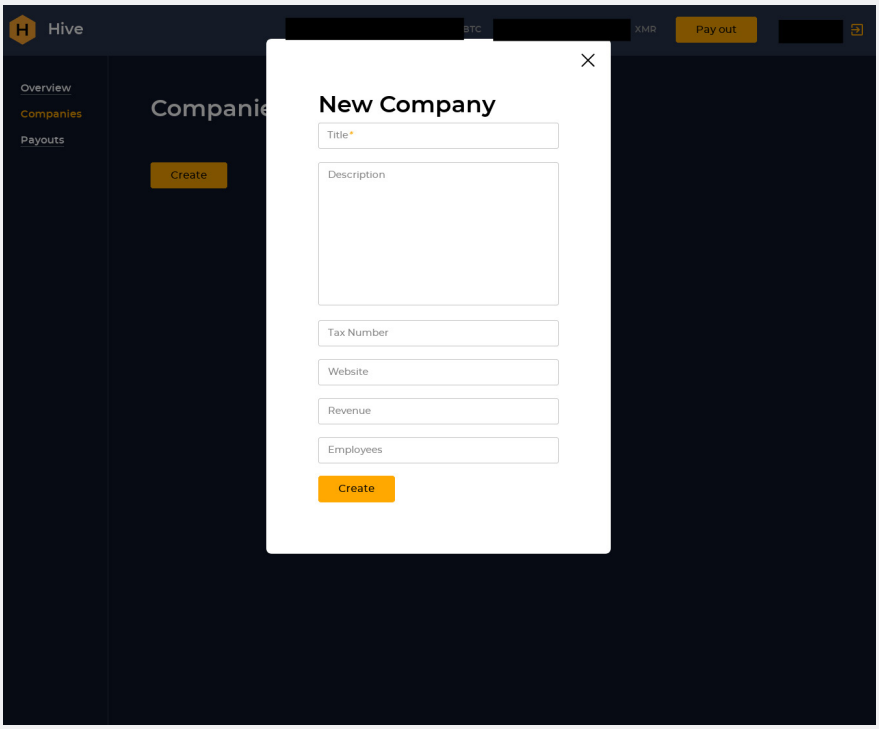


Fig. 81. Creating a new victim company's profile in the Hive affiliate program, 2021

After entering the victim's details, the hacker would see the following screen:

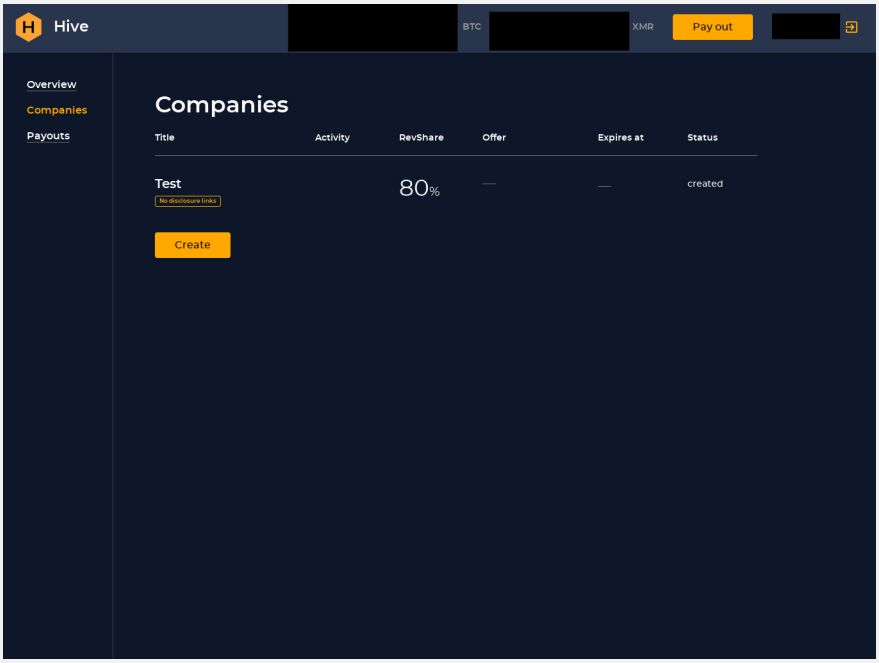


Fig. 82. Tab listing victim companies in the Hive affiliate program, 2021

On the left side of the page, clicking on a company will display a company summary, plus a link to leave a comment for the admin and a button to update the victim's details. On the right side of the page, hackers can download the ransomware to use on a future corporate victim and make a note about whether encrypting the company's data was successful.

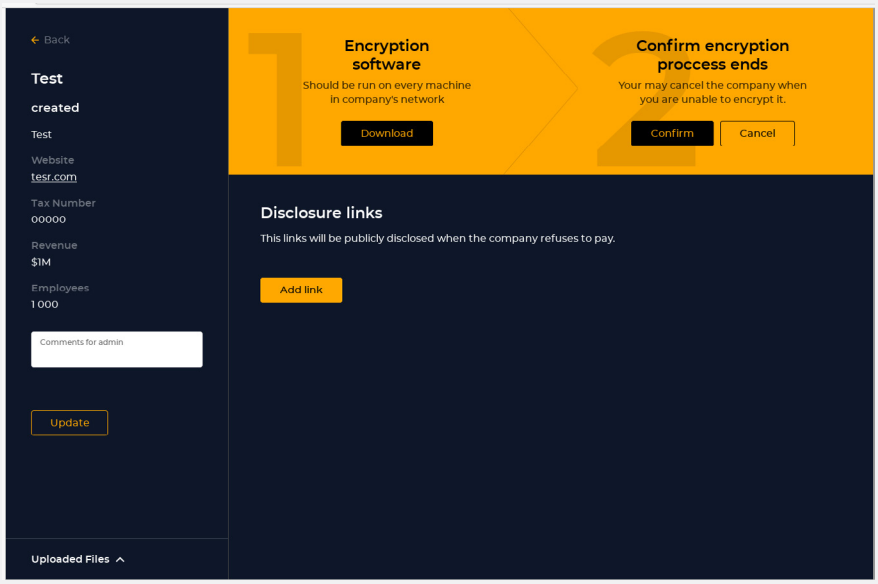


Fig. 83. Victim company's profile in the Hive affiliate program, 2021

Generating the ransomware may take up to 15 minutes. If a company refuses to pay the ransom, it is possible to add a link that will be posted on the Hive blog.

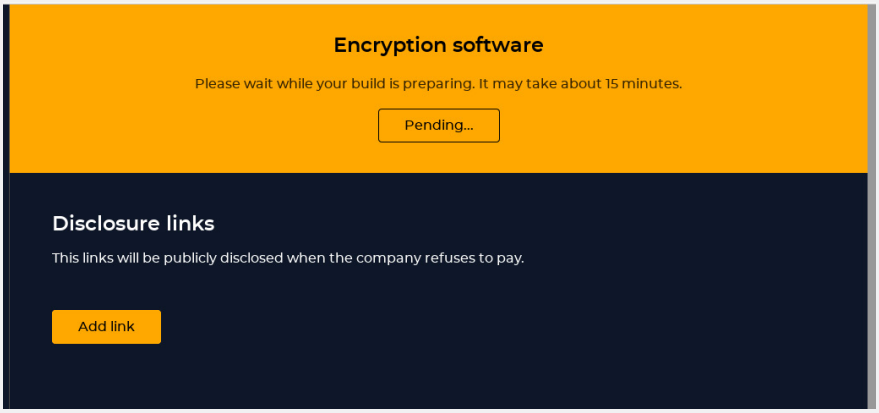


Fig. 84. Generating the ransomware within the Hive affiliate program, 2021

After the ransomware is created, a .rar archive is generated containing the following files:

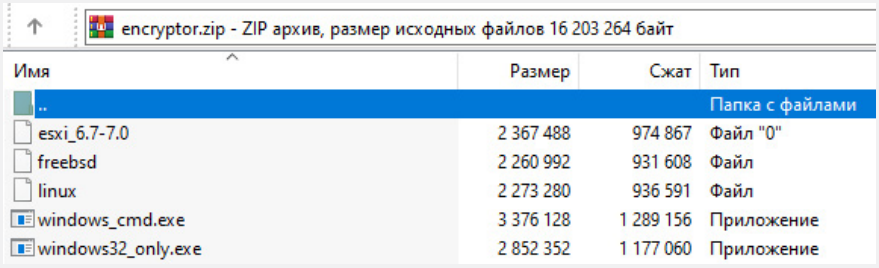


Fig. 85. An archive containing the ransomware, 2021

After a victim is infected, a ransom note will be generated automatically and contain a link to the website as well as the access login and password:

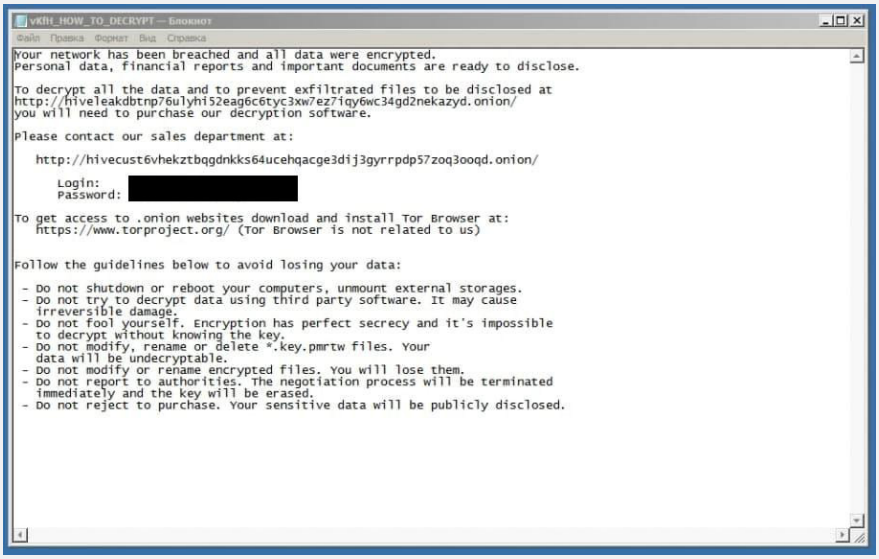


Fig. 86. A generated ransom note, 2021

If the hacker ascertains that the company was encrypted, a chat with the victim will open. Communication with the victim will take place as follows:

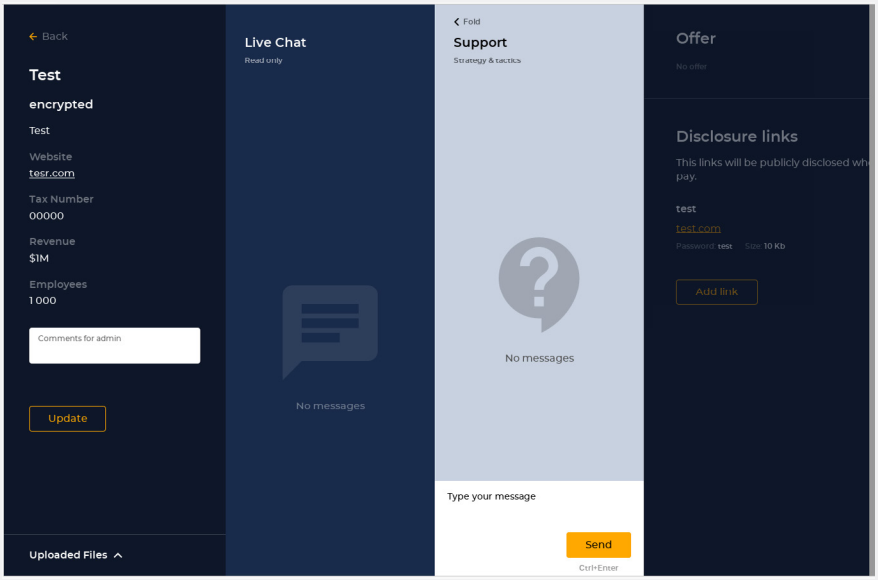


Fig. 87. Chat and support tabs within the Hive affiliate program, 2021

1. The victim writes a chat message to the admin (on the left), which is visible to the affiliate participant.
2. The affiliate participant writes a chat message to the admin (on the right).
3. The administrator relays the message to their chat with the victim.

Under this arrangement, the victim and the criminal are not in direct communication: they exchange messages entirely via the administrator.

After the victim pays the ransom, they are allowed to download the decryptor with a step-by-step guide on how to use it.

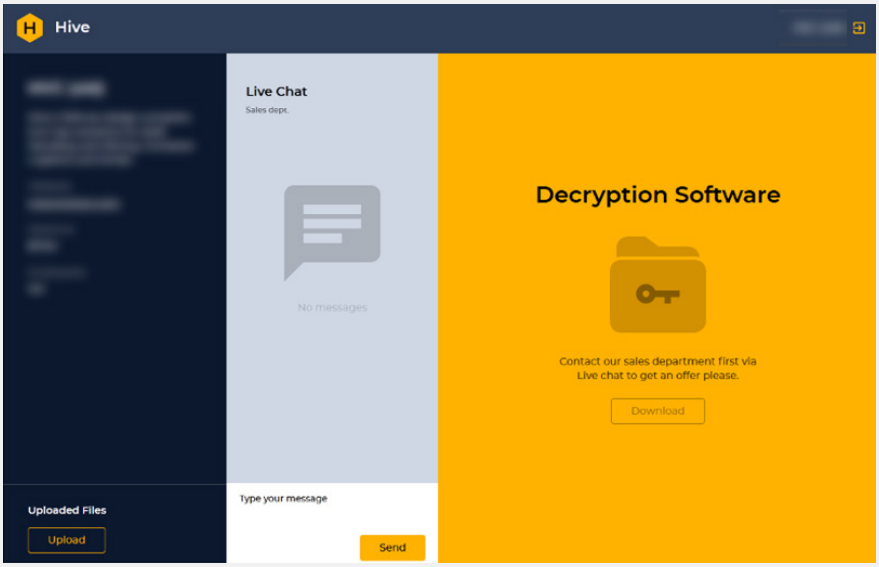


Fig. 88. Decryptor in the Hive affiliate program interface, 2021

The actual number of Hive victims and the technical features of the group's website

By early September 2021, profiles for as many as **181 companies** were created within the Hive affiliate program, with the number rising to **312** by late October. The Hive admin panel and the DLS rely on API. Each victim company is assigned a unique ID which can also be found on the DLS.

"Companies that had correspondence with the Hive operators and whose data was not published" means that the victim had messages in their chat with the threat actors but the victim's data was not published on the DLS. "Companies that did not have correspondence with the Hive operators and whose data was not published on the DLS" means that the victim had zero messages in their chat with the threat actors but their data was not published on the DLS.

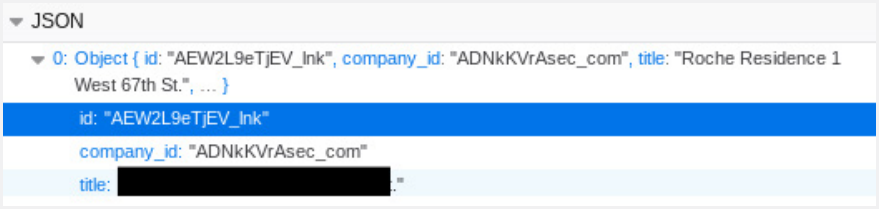


Fig. 89. The victim company's unique ID

Curiously, every affiliate program participant has access to all the company IDs in the database. The profile also includes the number of messages that the victim and the criminal have exchanged.

Fig. 90. Victim company data: IDs and number of chat messages, 2021

This helps gather statistics on the number of victims and make assumptions about amounts that companies have paid to the threat actors for not disclosing their private data.

Fig. 91. A chart showing the breakdown of Hive victims for September 2021

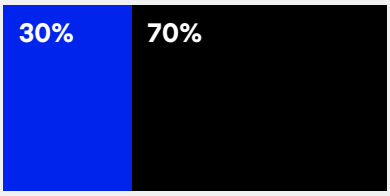
Category	Quantity	%
Companies whose data was published on the Hive DLS	36	20
Companies that had correspondence with the Hive operators and whose data was not published	35	20
Companies that did not have correspondence with the Hive operators and whose data was not published on the DLS	110	60
Total number of Hive victims about which there are records in the affiliate program API	181	—

Group-IB specialists found discrepancies between the data from the threat actors' API and DLS. The API did not return one company that had already been published on the DLS; it later disappeared from both the API and DLS. This may suggest that after its data was published, the company in question agreed to pay the threat actors.

Analysis of the companies published on the DLS reveals that most of the companies did not have correspondence with the threat actors.

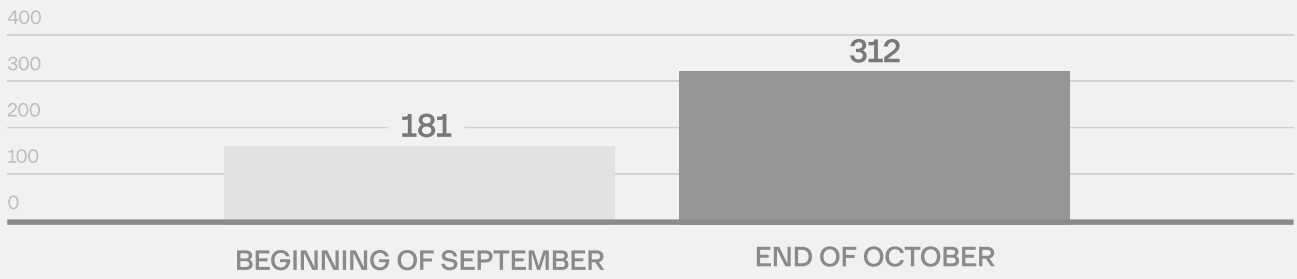
Fig. 92. A chart showing the breakdown of Hive victims for 2021

Category	Quantity	%
Companies that had correspondence with the Hive operators and whose data was published	11	30
Companies who did not have correspondence with the Hive operators and whose data was published on the DLS	25	70



Analysis of companies obtained through the API revealed that the number of victims almost doubled in a month:

Fig. 93. Chart showing Hive victim statistics for September-October 2021



Moreover, 43 companies listed as victims in September disappeared from the October victim list. An estimated **24% of companies attacked paid the ransom**.

The October statistics were slightly different:

Fig. 94. Chart showing the breakdown of victim companies in October 2021

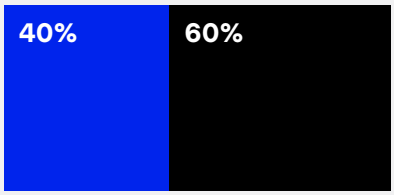
Category	Quantity	%
Companies whose data was published on the Hive DLS	34	11
Companies that had correspondence with the Hive operators and whose data was not published	104	33
Companies that did not have correspondence with the Hive operators and whose data was not published on the DLS	174	56
Total number of Hive victims about which there are records in the affiliate program API	312	—

The number of companies shown in the table differs from earlier data because 14 companies were removed from the DLS and API after their data was published. It is certain that these companies were breached and had their data stolen. It can be assumed that the companies agreed to pay the ransom in the end, which is why the information about them was completely removed.

As for correspondence with the threat actors, most of the victims whose data was published did not exchange messages with the threat actors.

Fig. 95. Chart showing the breakdown of victim companies, 2021

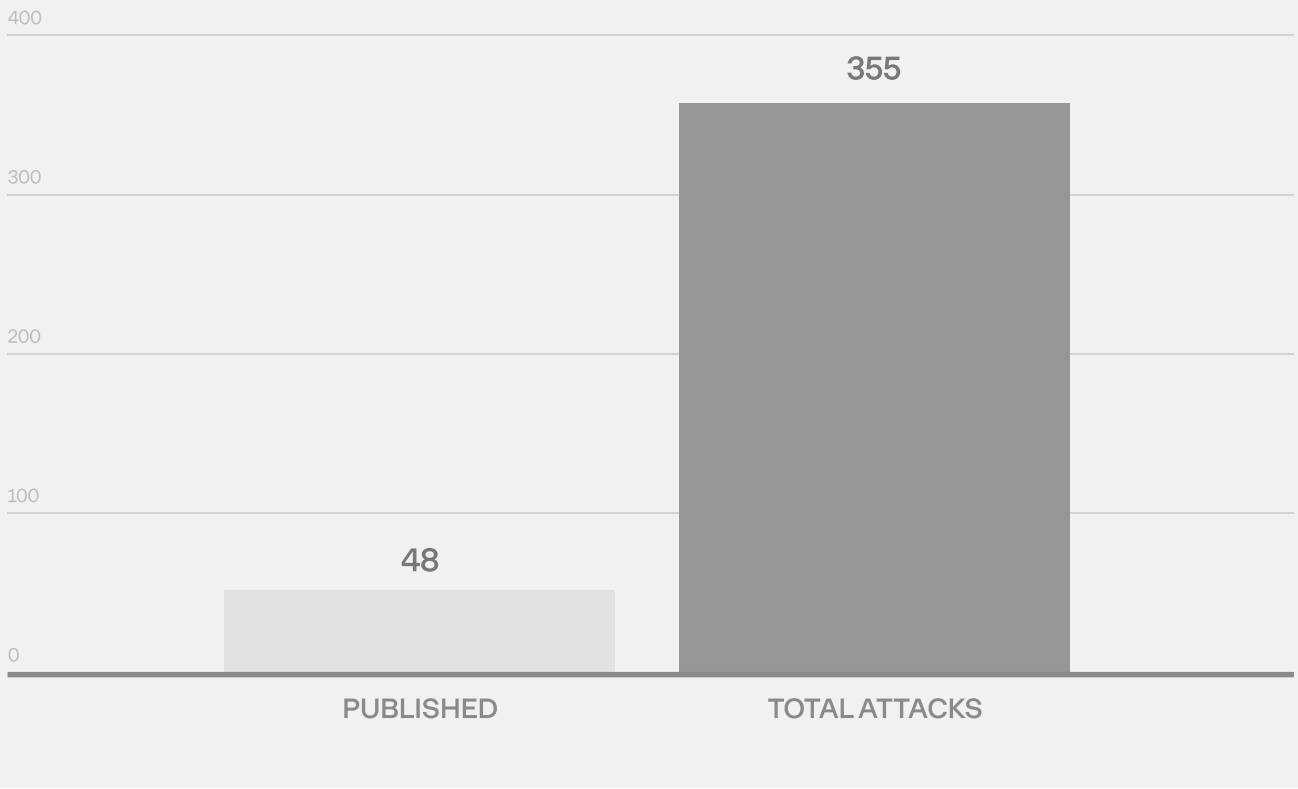
Category	Quantity	%
Companies that had correspondence with the Hive operators and whose data was published	14	40
Companies who did not have correspondence with the Hive operators and whose data was published on the DLS	20	60



At the time of writing, information about only 48 companies had been put on the Hive blog, including ones that were later removed from the DLS and API. However, an API error enabled Group-IB experts to identify the number of attacks between September and late October 2021.

Adding up the number of unique company IDs (312) for October and the IDs of the companies that disappeared from the API between September and October (43) shows that the total number of attacks was 355.

Fig. 96. A chart of victim statistics, 2021



Based on this data, Group-IB can conclude that only 13.5% of victim companies are reported in the blog. The other attacks either failed or involved victims who paid to cover up the attack. Most victims are companies based and operating in the US. The main industries targeted by these criminals are IT and real estate.

Breakdown of Hive attacks by country and industry, 2020-2021

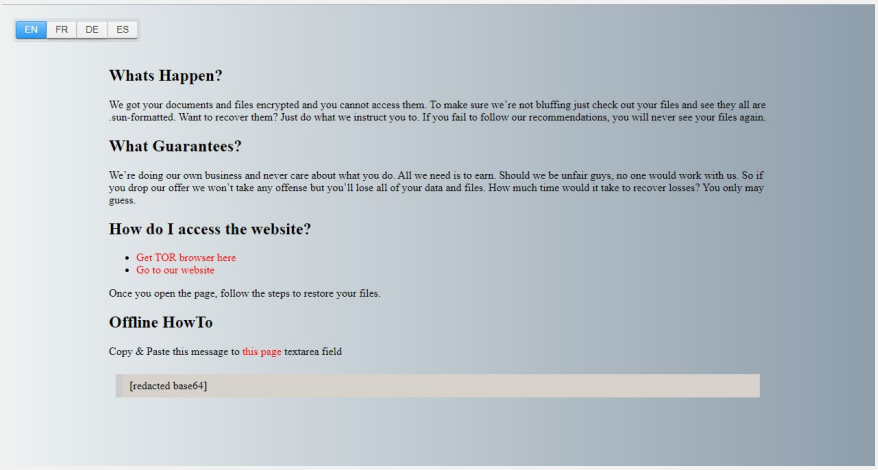
Country	Quantity
US	28
UK	2
Australia	2
Netherlands	2
China	2
Canada	1
Peru	1
Switzerland	1
Portugal	1
Thailand	1
India	1
Norway	1
Spain	1
Germany	1
Taiwan	1
France	1
Italy	1

Industry	Quantity
Real estate	5
Information technology	5
Manufacturing	5
Other	4
Commerce and shopping	3
Transportation	3
Media and entertainment	3
Financial services	3
Professional services	2
Administrative services	2
Food and beverage	2
Hardware	2
Healthcare	2
Lending and investments	1
Clothing and apparel	1
Education	1
Privacy and security	1
Consumer goods	1
Gaming	1
Software	1

Suncrypt

DLS

Another interesting example is the group called **SunCrypt**, whose activities were first detected in October 2019. Their ransom note at the time looked like this and was displayed in English, French, German and Spanish:


EN FR DE ES

Whats Happen?

We got your documents and files encrypted and you cannot access them. To make sure we're not bluffing just check out your files and see they all are .sun-formatted. Want to recover them? Just do what we instruct you to. If you fail to follow our recommendations, you will never see your files again.

What Guarantees?

We're doing our own business and never care about what you do. All we need is to earn. Should we be unfair guys, no one would work with us. So if you drop our offer we won't take any offense but you'll lose all of your data and files. How much time would it take to recover losses? You only may guess.

How do I access the website?

- Get TOR browser here
- Go to our website

Once you open the page, follow the steps to restore your files.

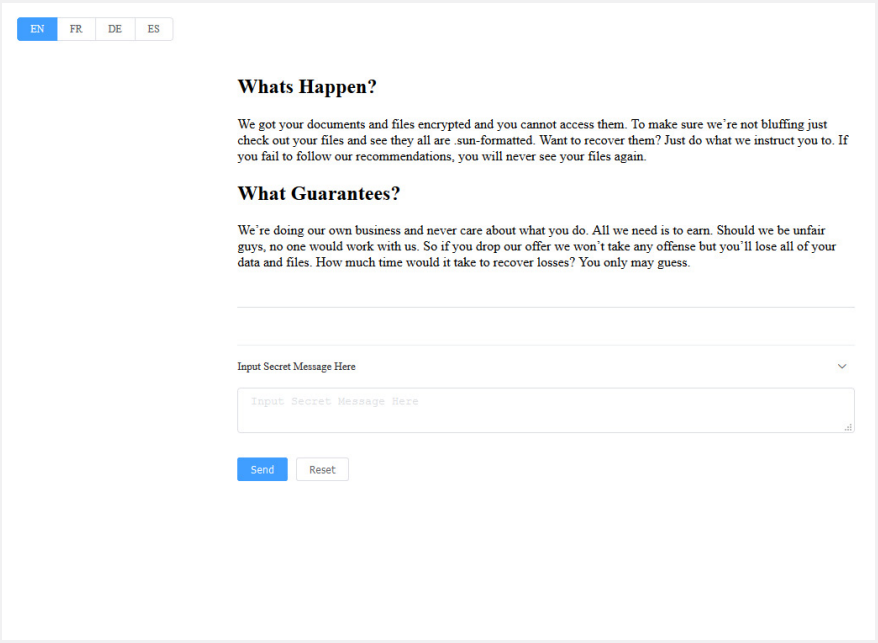
Offline HowTo

Copy & Paste this message to this page textarea field

[redacted base64]

Fig. 97. A ransomware note by SunCrypt, 2019

The note contained a standard message saying that the victim's files had been encrypted, as well as a unique victim-specific base64 code and a link to the criminals' resource: hxxp://sunlocksmdmv65mf.onion/. The resource was a web form that required the victims to enter their unique code to communicate with the criminal group.


EN FR DE ES

Whats Happen?

We got your documents and files encrypted and you cannot access them. To make sure we're not bluffing just check out your files and see they all are .sun-formatted. Want to recover them? Just do what we instruct you to. If you fail to follow our recommendations, you will never see your files again.

What Guarantees?

We're doing our own business and never care about what you do. All we need is to earn. Should we be unfair guys, no one would work with us. So if you drop our offer we won't take any offense but you'll lose all of your data and files. How much time would it take to recover losses? You only may guess.

Input Secret Message Here

Input Secret Message Here

Send Reset

Fig. 98. SunCrypt reply form for communicating with the ransomware operators from 2019

The first samples of this ransomware (including their current DLS website) were discovered in ransom notes in late August 2020.

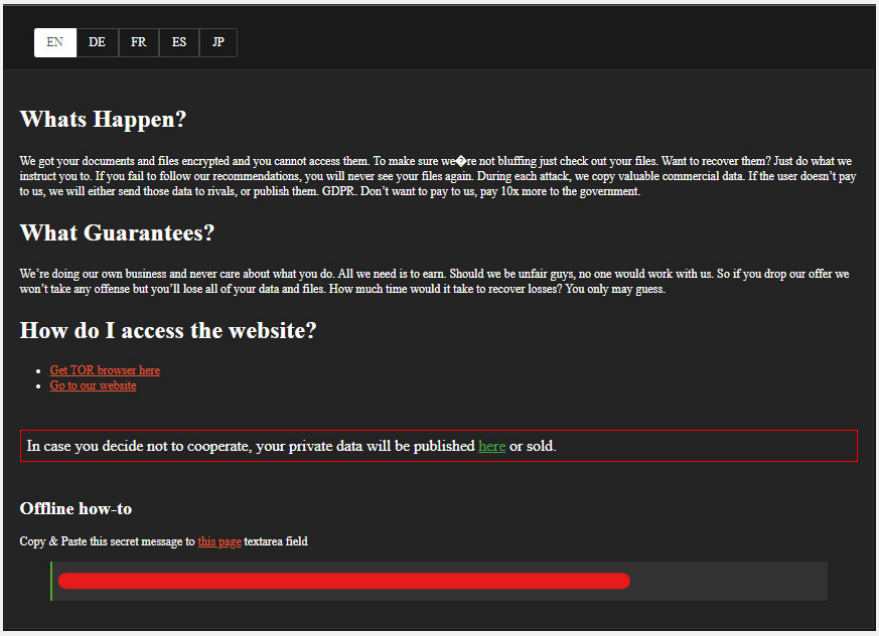


Fig. 99. A ransomware note by SunCrypt, 2020

The ransom note looks nearly identical except that it includes a Japanese translation and new links. Clicking on the first link takes victims to the group's DLS: hxxp://nbzzb6sa6xuura2z.onion.

The second link takes victims to a private chat: hxxp://ebwexiymbsib4rmw.onion/chat.html. A personal ID, which is generated for each victim and is passed as a parameter, would look like this*:

```
1abc137b7d-2e7d3314f2-f8e60fc37a-b06f444368-f012d06402-d4bda6390a-daea3c5b58-b68cf150d5
```

* Some numbers have been changed to protect the victim's privacy.

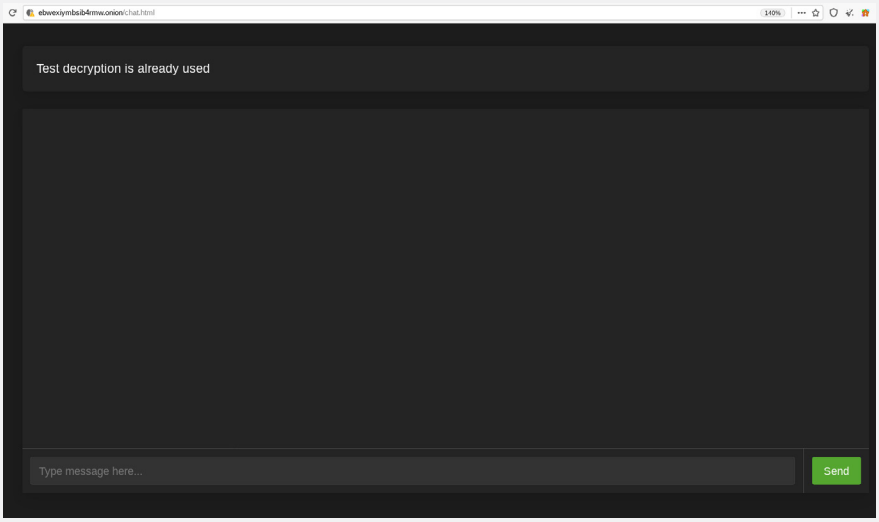


Fig. 100. Chat with a SunCrypt victim from 2020

When SunCrypt's DLS was first made public, it already contained compromised data belonging to five victims. Three were located in the USA, one was in Canada, and the final victim was in Norway.

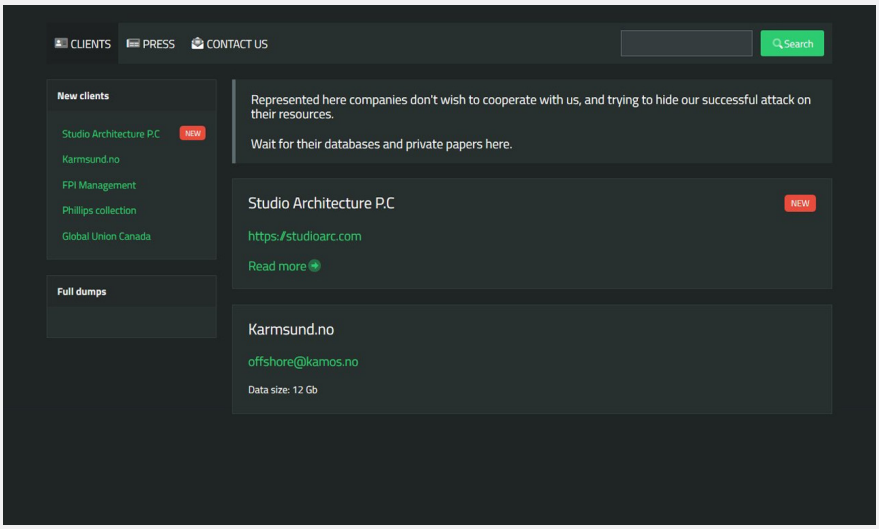


Fig. 101. SunCrypt victim list, 2020

Industry	Country	Publication	ID
Government and military: Government	US	2020-08-01 0:00:00	5
Software	Canada	2020-08-08 0:00:00	3
Privacy and security	US	2020-08-14 0:00:00	6
Manufacturing	Norway	2020-08-14 0:00:00	7
Real estate: Construction	US	2020-08-21 0:00:00	8

The subsequent investigation revealed that each compromised company listed on the DLS had a unique ID in the cybercriminals' database in the following format:

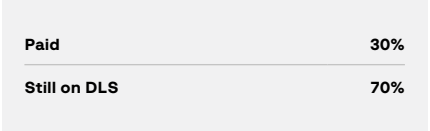
```
/client?id=ID
```

What sets this DLS apart is that some entries return "Forbidden" in response to a query. At the time when the DLS appeared online, IDs 1, 2, and 4 were already unavailable.

As of August 2021, data relating to **21 companies** were available on the resource with different assigned IDs. The highest ID (30) represented a developer of e-commerce automation solutions. Nine different IDs returned "Forbidden". Group-IB's investigation revealed that some of the IDs marked as "Forbidden" corresponded to previously attacked companies whose data had been removed from the DLS, presumably because they had paid the ransom.

It is therefore reasonable to estimate that **30% of companies attacked by SunCrypt eventually paid the ransom** and had their data removed from the group's resource.

Fig. 102. Chart showing the ratio of the number of companies that paid the ransom to those still listed on the DLS, 2020



It's important to highlight one distinctive feature of the cybercriminal group's activities, namely that they publicly announce on their website that they are willing to sell full sets of data to any interested party. This means that any victims' data could have also been sold to other parties.

The resource itself has two major sections: "New Clients" and "Full Dumps." According to the criminals themselves, they start by posting 10% of the stolen data belonging to a compromised company and only later put all the data up for sale. If the victim's data is not purchased within a week, the criminals post a full dump containing the victim company's data.

In the first year of operating their DLS (2020), the criminal group used mega.nz, a public file exchange server, to disclose compromised data. In 2021, they switched to using their own file server: http://l4sd5qtsofedx7ss.onion/.

SunCrypt's activity on darknet platforms

A user with the alias SunCrypt created their first account on Maza, a private darknet forum, in July 2020 and paid a deposit of $5,000 (https://mfclubjof2s67ire.onion/member.php?u=17277). A public affiliate program appeared on the same forum on August 3, 2020.

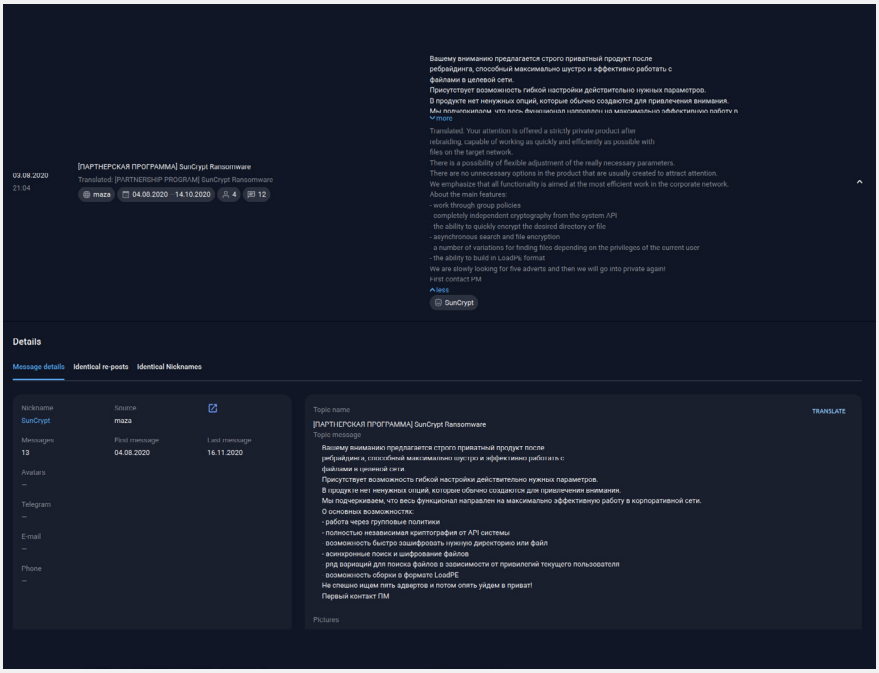


Fig. 103. A message announcing the SunCrypt affiliate program, 2020

According to SunCrypt, the group was temporarily going public in order to find five new affiliates. In addition to sharing malware descriptions, the group announced that they had a team responsible for exfiltrating data from networks and that all they needed from would-be affiliates was to obtain sessions with domain administrator access. They also informed that if a victim refused to pay the ransom, they would contact media representatives and the victim's customers as "encouragement" to pay up.

A Maza forum moderator known as **Moderator 7** (mod6@mfclub.ws) claimed to know this criminal group and had supposedly been collaborating with them for a long time.

On August 12, 2020 SunCrypt posted an ad for their affiliate program on exploit.in, another private forum.

SunCrypt registered their exploit.in account in October 2019 (https://exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/profile/96576-suncrypt/), which coincides with the launch of the first SunCrypt malware campaign. It would be reasonable to assume that the cybercriminals started by looking for affiliates via private messaging on exploit.in. The deposit on this forum is BTC 0.5.

SunCrypt used an image by **DASHA PLISKA**, a Ukrainian artist, as their avatar. Pliska is not a particularly popular artist, which either indicates the hacker group's interest in niche artwork or points to their country of origin.

Fig. 104. SunCrypt avatar, 2020

On August 16, 2020 SunCrypt announced that they had two vacant spots left. They had only one available spot by August 20, and had recruited all five affiliates by August 29.

On September 3, SunCrypt reported that they had added the capability to launch their malicious payload using a fileless technique.

On September 16, the hackers announced that they once again had a vacancy for a prospective affiliate.

On September 23, they shared a post about adding .exe and .dll AutoCrypt, and said that they were still looking for new affiliates to join their program.

On October 1, they wrote that they were looking to fill the last spot remaining in the affiliate program. What came next was puzzling— a post on October 8 announced the group's decision to shut down the affiliate program:

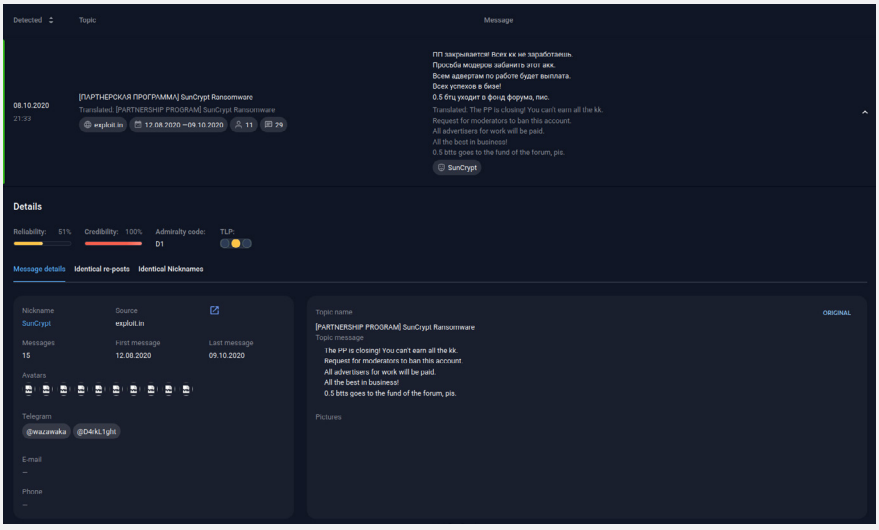


Fig. 105. SunCrypt post announcing the closure of their affiliate program, 2020

Conflict between criminal accomplices

On October 18, 2020 a threat actor known as **TrueFighter** posted a complaint about not getting paid by SunCrypt and avx on exploit.in. TrueFighter described the experience working with the team, but after the affiliate program was shut down, TrueFighter did not get the money he was allegedly promised

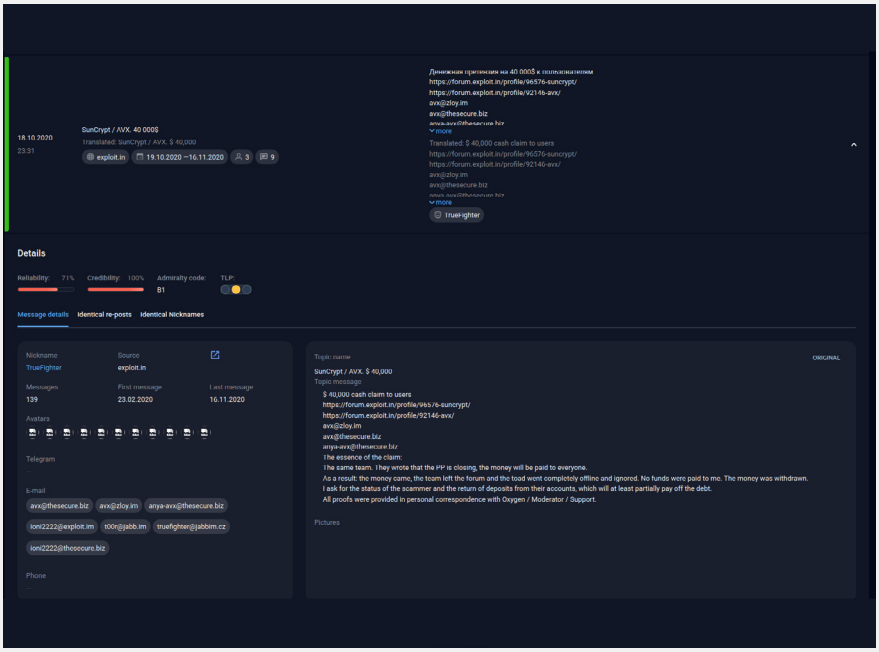


Fig. 106. TrueFighter's complaint against SunCrypt and avx, 2020

During subsequent discussions about the matter on another forum, Maza, SunCrypt clarified that they had worked directly with avx and paid the amounts owed in full, but had no knowledge of the forum user known as TrueFighter. It is most likely that avx had failed to pay one of their own hired hands. SunCrypt also said that avx was based in the US.

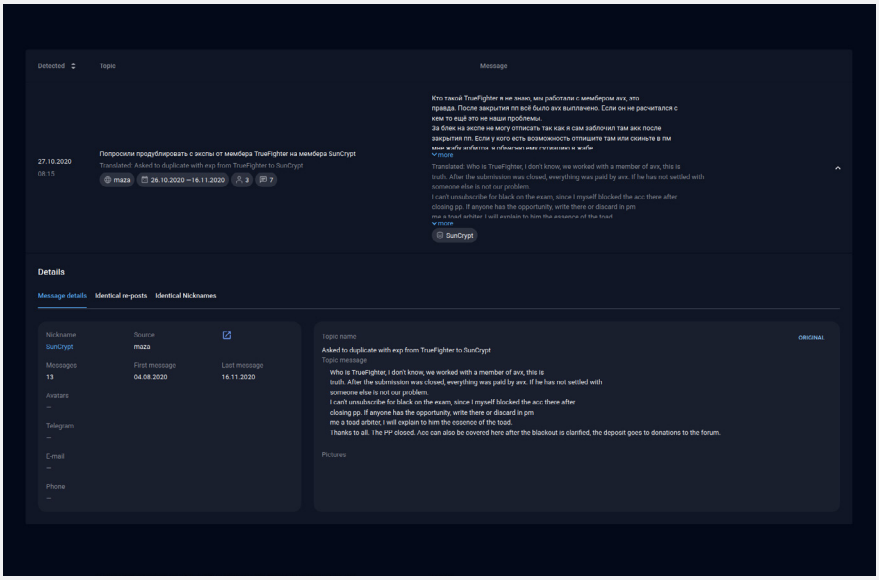


Fig. 107. SunCrypt's reply with regard to TrueFighter's complaint, 2020

Moreover, a forum user known as D4rkL1ght (https://forum.exploit.in/profile/104635-d4rkl1ght/) was presumably among SunCrypt's affiliates. In one of their posts, D4rkL1ght shared a guide obtained from the SunCrypt affiliate program dashboard:

```
What the processing order is?

    Stop services (In agressive mode only, check -agr argument below)
    Remove shadow copies
    Mount local volumes (connected to the computer but isn't mounted)
    Encrypt shares
    Encrypt local volumes
    Report
    Exit

Does it encrypt all the files?

In agressive mode (-agr argument):
Yes, except: exe, dll, sys, lnk, ico

In normal mode:
No, it does encrypt only certain extension.
You can check extension list HERE.

In addition it completely skips following folders:

    Windows
    Program Files
    Program Files (x86)
    $Recycle.bin
    System Volume Information

When it create the note?

After all supported files are encrypted in the folder.
Folder proceesing order is:

    Enter the folder
    Encrypt files
    Create note
    Go to the next folder

Which arguments can be passed to the EXE?

-noreport
Don't report to the server after encryption is done

-noshares
Don't encrypt network shares and network disks, work only with local disks

-nomutex
Ignore mutex, start new instance even if another instance of cryptor is already running

-log
Create console window and write log

-path <folder/disk>
Work only with specified path

-skip
(BETA only)
Don't encrypt folder or file with specified name

-agr
(BETA only)
Stop non-standard services (except Citrix), encrypt all extensions except: exe, dll, sys,
lnk, ico
Is there a difference in the logic or processing order between PS1, EXE and DLL?

No, they are the same.
How to run PS1?

    powershell -ep bypass -file cryptor.ps1
    [ ! ] PS1 doesn't support arguments (e.g. -log, -path, etc.)

How to run DLL?

    rundll32 cryptor.dll,DllRegisterServer
    [ ! ] rundll32 does support arguments
    regsvr32 cryptor.dll
    [ ! ] regsvr32 doesn't support arguments

What is the difference between EXE and EXE-beta?

EXE has been tested a lot and considered to be stable
EXE-beta contains latest fixes, updates and so on, but less tested
```

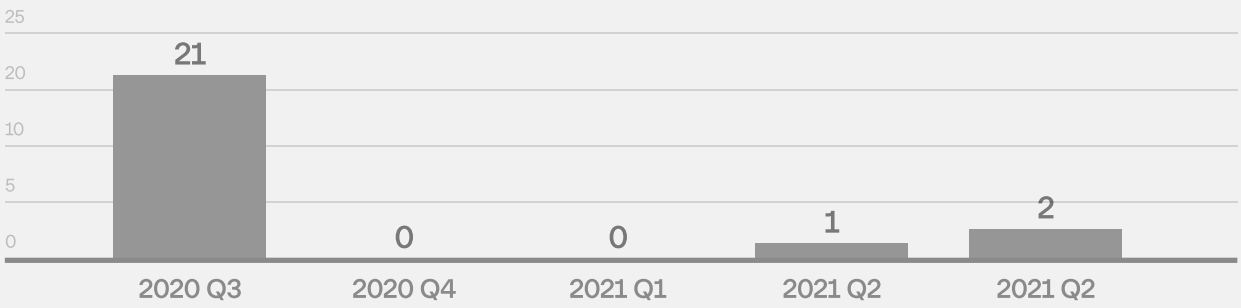
Fig. 108. User guide obtained from the SunCrypt affiliate program dashboard, 2020

The hacker known as SunCrypt had entered into a conflict with this forum participant because some of the attack targets were hospitals. SunCrypt had noted that it was an accident because the affiliate had not been informed about the ban on attacking such targets.

Attack statistics

As noted above, the SunCrypt group of ransomware operators has shared details of **30 companies** in total on its blog. Out of the 30, 24 are currently known. Most of the group's activity was concentrated in Q3 2020 and its affiliate program had only three known victims in 2021.

Fig. 109. SunCrypt attack statistics, 2020-2021



The criminal group focused their attacks on the manufacturing and energy sectors. The criminal group finds most of its targets in the US:

Breakdown of SunCrypt attacks by country and industry, 2020-2021

Country	Quantity
US	12
Norway	3
Canada	2
Belgium	2
Germany	2
Italy	1
UK	1
Australia	1

Industry	Quantity
Manufacturing	5
Energy	4
Commerce and shopping	3
Real estate	2
Professional services	2
Government and military	1
Education	1
Information technology	1
Transportation	1
Privacy and security	1
Healthcare	1
Financial services	1
Science and engineering	1

RTM: How new affiliate programs come about, or quiet lockers

In the past two years, ransomware has become a major threat to businesses and organizations. Encouraged by the success of criminal groups such as **REvil** and **Lockbit**, more and more cybercriminals are switching from other illicit activities to ransomware, attracted by its clear path to monetization and strong potential for financial gain. Some threat actors attempt to replicate Lockbit's success by setting up their own Ransomware-as-a-Service operation. This trend is clearly illustrated by the example of an individual known as **RTM Team** (aka BlackBet). RTM's transformation process follows a fairly typical pattern.

BlackBet first appeared on underground forums on February 17, 2017, advertising their own marketplace for various types of data.

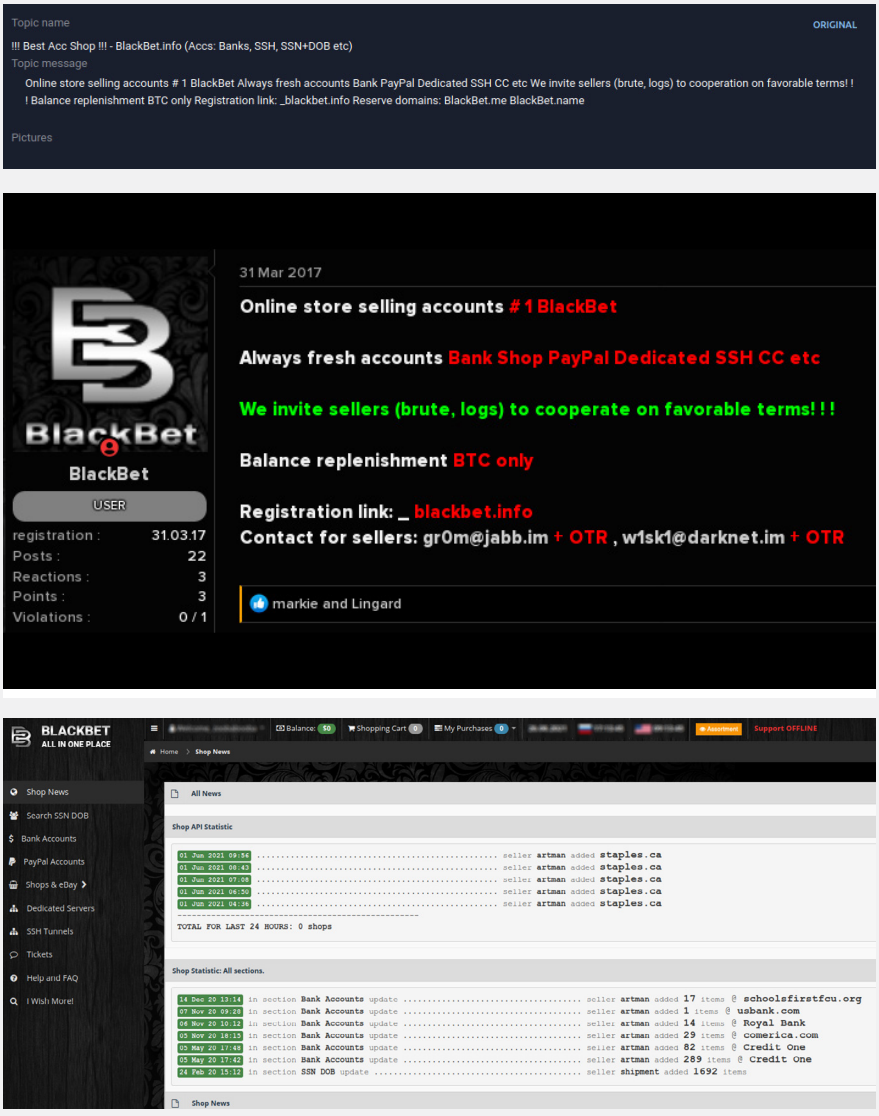


Fig. 110. An ad for the marketplace BlackBet, 2017

A little later, the hacker started an affiliate program for the marketplace.

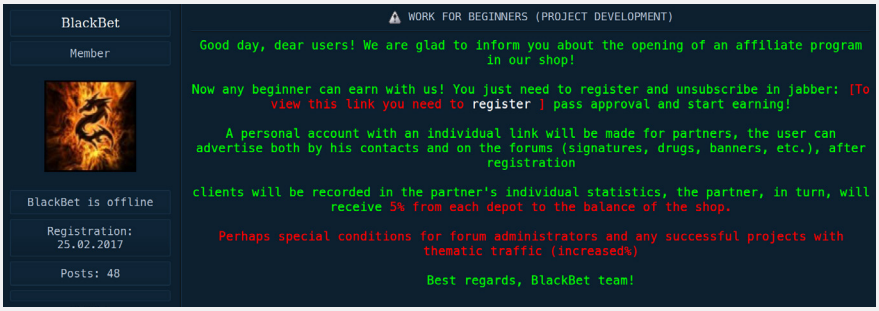


Fig. 111. Announcement of the affiliate program, 2017

BlackBet also purchased logs around the United States and was involved in mining, buying and selling malware, selling network access credentials, and other malicious activities. BlackBet's key distinguishing feature was that the hacker was always on the lookout for the most profitable trends.

When the cybercriminal realized that ransomware was such a trend, BlackBet decided to try it out.

On December 1, 2020, BlackBet started their search for a coder who could write ransomware and a pentester to join "their team."

Fig. 112. BlackBet's message about looking for a team to create a crypto locker, 2020

Private affiliate program

On August 19, 2021, **Orange** (a RAMP forum admin) inquired about ransomware affiliate programs. Someone using the handle **RTMTeam** (aka BlackBet) responded that an affiliate program would be ready soon and invited other people to join it.

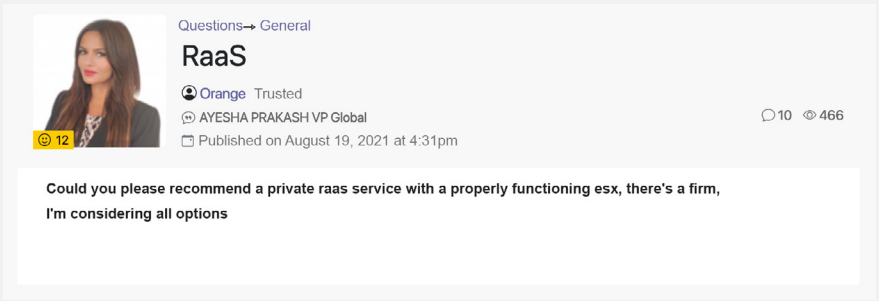


Fig. 113. Thread on an affiliate program, 2021

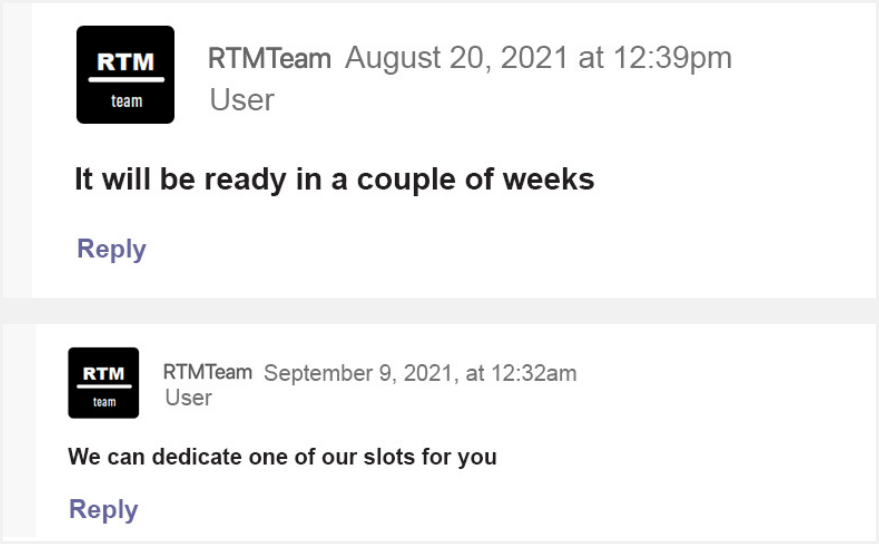


Fig. 114. Exchange of messages about the upcoming launch of a new affiliate program, 2021

RAMP admin (Orange) is asking about any new Ransomware as a Service. This post is answered by someone with the username RTMTeam, who says that an affiliate program will be ready within "a couple of weeks"

The subsequent exchange of messages clarified the key details of the affiliate program, as well as yielded a malware sample.

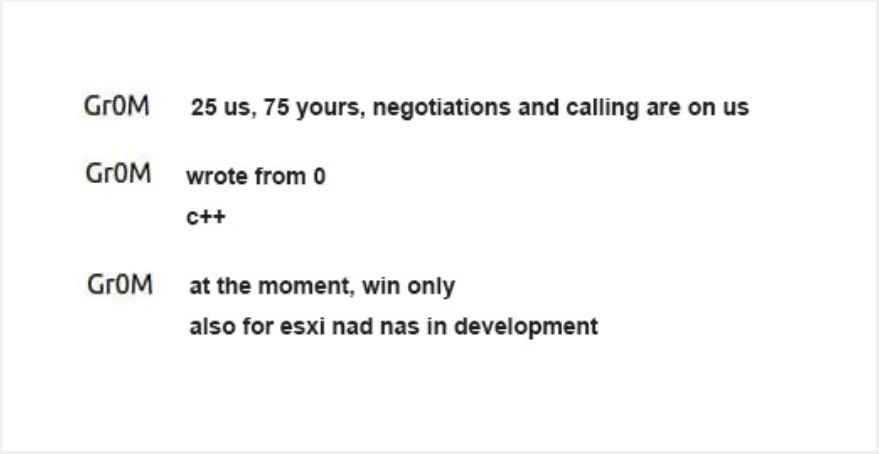


Fig. 115. RTM Team's affiliate program details, 2021

Gr0m writes that the profits will be divided 75% for the attacker and 25% for Gr0m. The ransomware was written «from scratch in C++»; at present there is a Windows version, and later one for Linux will appear

Analysis revealed that the samples provided were indeed malware capable of selectively encrypting files using the asymmetric encryption algorithms Chacha20 and Curve25519, as well as AES through x86 extensions.

During the infection process, the malware counts the lines of internal hard drives, then checks for the active root drive and mounted removable disk drives. It skips the OS paths and some application folders, proceeding to encrypt all the user files, making them impossible to recover without a backup copy or a decryption key. The malware also checks for any available processes and services whose lines are added to the last segment of a binary file in order to properly complete the process or service.

Furthermore, the malware empties the recycle bin on all the drives it has identified, then clears system event logs, application logs and the infected system's security logs, after which it checks for shadow copies of volumes containing the shadow copy access and query code, using WMI as its interface.

After the user files have been encrypted, the desktop background is replaced by a .jpeg ransom note, with a ransom note text file added to every folder in which files have been successfully encrypted. After infecting the system, the malware removes itself from the launch path.

Fig. 116. Desktop after ransomware infection, 2021

Samples provided in the archive and a sample received through a PS dropper are equivalent in terms of their functionality and are only visibly different in their static attributes, including encryption keys and ID numbers. This also indicates that they could be generated samples with different IDs for each infected system.

The history of Groove and the first-ever fake DLS

History of its origins

The first mention of **Groove** is dated August 23, 2021, when Orange, the main admin of the RAMP forum, asked for help creating a website for Groove.

Fig. 117. Developer competition announcement, 2021

The website Groove was empty for a long time, and then several batches of leaked data were posted there. The website looked like a regular DLS until 10,000 **Fortinet** VPN access points were posted on it.

10,000 Fortinet access points

On August 31, 2021, the RAMP forum moderator started a thread about giving away an archive containing 10,000 Fortinet VPN access points.

Fig. 118. Message announcing an archive of 10,000 Fortinet access points, 2021

The moderator wrote that the user selection process would be very strict, and if any of the access points became publicly available, anyone to whom they had been provided would be banned from the forum.

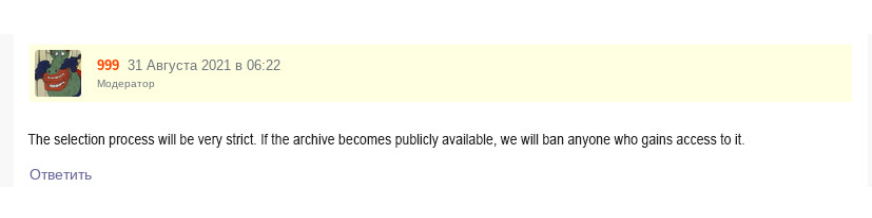


Fig. 119. «The selection process is going to be very strict», 2021

On September 7, 2021, however, the archive was uploaded to Groove, a resource run by the RAMP admin. He said that all the account credentials were checked for authenticity.

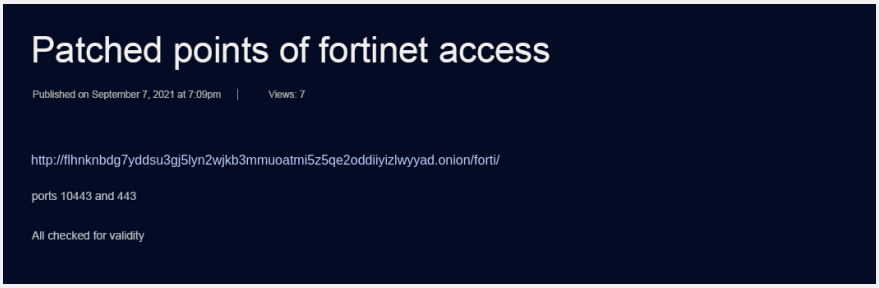
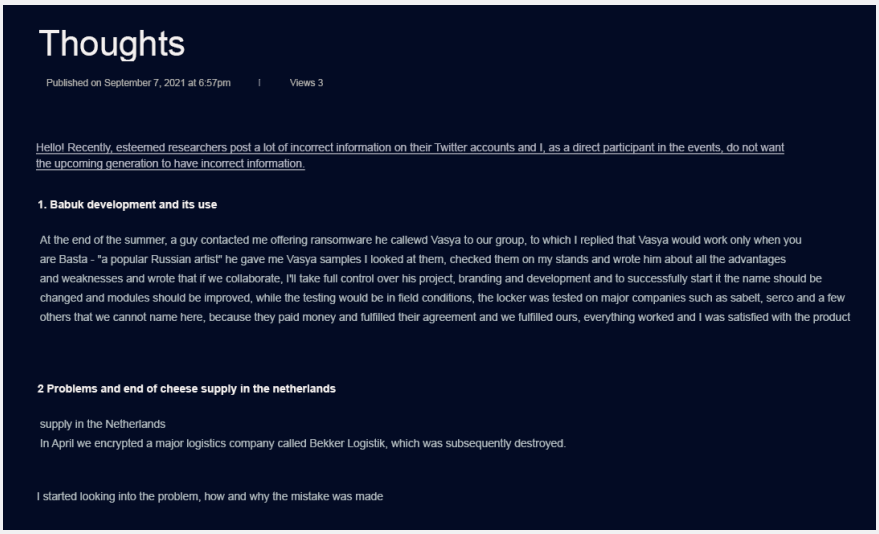


Fig. 120. Uploaded archive of access credentials, 2021

Aftermath and strange posts on DLS

After posting about 10,000 Fortinet access points, Groove attracted a lot of attention from both RAMP participants and the media. However, this was followed by strange posts detailing the hacker's thoughts:



Thoughts

Published on September 7, 2021 at 6:57pm | Views 3

Hello! Recently, esteemed researchers post a lot of incorrect information on their Twitter accounts and I, as a direct participant in the events, do not want the upcoming generation to have incorrect information.

1. Babuk development and its use

At the end of the summer, a guy contacted me offering ransomware he callewd Vasya to our group, to which I replied that Vasya would work only when you are Basta - "a popular Russian artist" he gave me Vasya samples I looked at them, checked them on my stands and wrote him about all the advantages and weaknesses and wrote that if we collaborate, I'll take full control over his project, branding and development and to successfully start it the name should be changed and modules should be improved, while the testing would be in field conditions, the locker was tested on major companies such as sabelt, serco and a few others that we cannot name here, because they paid money and fulfilled their agreement and we fulfilled ours, everything worked and I was satisfied with the product

2 Problems and end of cheese supply in the netherlands

supply in the Netherlands
In April we encrypted a major logistics company called Bekker Logistik, which was subsequently destroyed.

I started looking into the problem, how and why the mistake was made

Fig. 121. Post on RAMP, 2021

In October 2021, however, Groove's owner (**boriselcin**) created a post on xss.is explaining that the DLS had been a fake all along and was created exclusively to manipulate the media because ransomware seems to be a hot topic that attracts a lot of media attention.

The growing popularity of ransomware and affiliate programs therefore makes it reasonable to expect more fake DLS and fake Ransomware-as-a-Service offers to appear in the future. Potential participants would be asked to pay to join such an "affiliate program," after which the admin would disappear and "ghost" the new affiliates.

As for the data on the fake DLS, they could have been obtained from lower-profile ransomware operators or using OSINT, or simply generated as fake data. In the case of Groove, the fake DLS was created as an experiment and a way to manipulate the media, but this does not rule out the possibility that cybercriminals might actually resort to this tactic. Moreover, a similar scheme has already been successfully implemented by carders, a development that Group-IB experts described in detail on our blog in the entry entitled **Cannibal Carders**.

RECOMMENDATIONS FOR THREAT HUNTING

07

1. Focus on winword.exe/excel.exe creating suspicious folders and files or start processes such as rundll32.exe and regsvr32.exe.
2. Hunt for suspicious cscript.exe / wscript.exe executions, especially involving network activity.
3. Search for powershell.exe processes with suspicious or obfuscated command lines.
4. Analyze executables and scripts dropped into the Startup folder, added to the Run keys, or run via scheduled tasks.
5. Monitor sdbinst.exe execution for suspicious command line arguments.
6. Monitor sub keys creation under HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options.
7. Make sure your security controls can detect command lines that are typical for credential dumping tools like Mimikatz.
8. Hunt for common artifacts of network reconnaissance tools, such as AdFind's command line arguments.
9. Search for file execution artifacts from uncommon locations such as C:\ProgramData, %TEMP% or %AppData% .
10. Hunt for RDP-related Windows Registry and Firewall modifications.
11. Collect and analyze RDP connection data to uncover any potential lateral movement.
12. Hunt for wmic.exe executions with suspicious command lines.
13. Monitor bitsadmin.exe for abnormal behavior, especially related to potentially malicious file downloads.
14. Make sure you are able to detect Cobalt Strike Beacons and similar payloads typical for post-exploitation frameworks in your environment, at least those launched with common command line arguments and from common locations.
15. Hunt for network connections from common system processes. You can also use known Cobalt Strike team servers lists obtained, for example, from your Cyber Threat Intelligence provider.
16. Search for new service creation events related to PsExec, SMBExec and other dual-use or offensive security tools.
17. Hunt executables masqueraded as common system files (e.g. svchost.exe) but have uncommon execution parents or locations.
18. Monitor remote access software in your network for signs of unauthorized usage.
19. Search for cloud storage client installation events and cloud storage access events and check whether they are legitimate.
20. Hunt for common FTP software on endpoints to uncover installations with malicious configurations.

[1] Aids Info Disk or PC Cyborg Trojan is a Trojan that replaces the AUTOEXEC.BAT file, which is then used by AIDS to count the number of times the computer has booted. Once the boot count reaches 90, AIDS hides directories and encrypts the names of all the files on drive C: (thereby rendering the system unusable), at which point the user is asked to "renew the license" and contact PC Cyborg Corporation for payment (which would involve sending US$189 to a post office box in Panama). There is more than one version of AIDS, and at least one version does not wait to lock the C drive. Instead, it hides directories and encrypts file names upon the first boot after AIDS is installed. page 12

[2] PGPCoder, also known as GPCode, emerged in 2004. It's a Trojan that encrypts files on the infected device and then asks for a ransom to release the files. Victims have reported that the header of each encrypted file contained the string "PGPcoder 88.77.94". The ransomware encrypts .txt, .zip, .doc, and .xls files. It has been reported that "antivirus software does not detect this virus." page 12

[3] Cryzip, which came onto the scene in 2006, is a Trojan family that encrypts data and is used to demand a ransom. Once it is on the victim's device, the Trojan looks for 44 types of files, encrypts them, and leaves a message demanding $300 in exchange for the password to restore the files. Cryzip puts files into a password-protected ZIP file using a commercial compression library. The password to all the encrypted files is the same: C:Program FilesMicrosoft Visual StudioVC98. This string is stored in the Trojan in unencrypted form. The string can often be found in projects compiled using Visual C++ 6. It seems that the malware developer hoped that if anyone searched for the password in the Trojan, they would not pay attention to this string. page 13

[4] Krotten is a family of Trojans that emerged in 2005. It is distributed under the guise of a fake code generator for illegally topping up mobile phones. Attempting to top up using Krotten results in the computer being infected and the user being unable to fully use the operating system resources. To recover the system, the user is asked to top up the account of the threat actor, who will recover the system in return (the screenshot mentions 25 Ukrainian hryvnias, which is about $1). page 14

[5] Winlock is a malware family that blocks or disrupts the operating system and is used by threat actors to demand money for recovering the system. The first Winlock versions were discovered in 2007, but this type of Trojan did not become popular until 2009. page 14

[6] Trojan.Encoder is a Trojan for encrypting user files. To do so, the malware used XOR and TEA. It was written in MASM. page 18

[7] Ulocker is a family of ransomware Trojans that uses fake messages supposedly sent by the police in order to scare inexperienced computer users into making large payments. It is easy to distinguish Ulocker from other ransomware Trojans because it uses a distinctive image that includes a background with a large picture of a padlock. page 21

[8] Citadel is a Trojan for stealing banking data. It was launched in 2011 and is a modified version of the Trojan called Zeus. Citadel has caused at least $500 million worth of damage and infected about 5 million computers. In addition to stealing data, it can significantly slow down the target computer and download other malware. page 22

[9] CryptoLocker is a ransomware family that infects computers running Microsoft Windows. The program was first published online on September 5, 2013. The Trojan was distributed via email attachments or when users visited infected websites. The malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's C&C servers. The malware then displays a ransom message offering to decrypt the data. If the deadline for paying the ransom (most often in cryptocurrency) is missed, CryptoLocker offers to decrypt data via an online service provided by its operators for a significantly higher price in Bitcoin. page 24

[10] TorrentLocker is a ransomware Trojan that targets Microsoft Windows. The malware encrypts files in a similar way to CryptoLocker by implementing a symmetric block cipher called AES, where the key is encrypted with an asymmetric cipher. page 27

[11] VaultCrypt is a piece of ransomware that encrypts data using RSA-1024 and then demands that the victim visit a Tor website to pay the ransom in order to recover their files. The ransomware did not show a ransom note. Instead, it added a new extension, .vault, which changed the icon of all encrypted files to a lock. Double clicking on such a file showed a message saying "Stored in Vault". page 27

[12] Chimera is ransomware that encrypts all files it finds on connected drives and then demands a ransom of 0.939 Bitcoin to recover them. After encrypting files, Chimera displays a ransom note featuring instructions on how to make a payment and receive a link to a decryptor. In addition to encrypting files, Chimera threatens to publish them on the Internet if the ransom is not paid. page 29

[13] CryptoWall is a ransomware family that emerged in 2014. It is notable for its use of unbreakable AES encryption, unique CHM infection mechanism, and robust C&C activity over the Tor anonymous network. The threat actors running the CryptoWall operation also provided a free single-use decryption service to prove they hold the keys necessary to restore the hijacked files. The ransom amount is $700 and must be paid in Bitcoin (equivalent to 1.8 BTC at the time). page 29

[14] KeRanger is ransomware that targets macOS computers. It was discovered on March 4, 2016 by Palo Alto Networks and it has affected over 7,000 macOS users. page 31

Group-IB

A global leader in high-fidelity Threat hunting and Intelligence, best-in-class fraud prevention solutions, and high-profile cyber investigations.

Group-IB's mission: Fight Against Cybercrime

Interpol and Europol

Partner and active collaborator in global investigations

APAC TOP 10

Ranked among the Top 10 cybersecurity companies in the APAC region according to APAC CIO Outlook

Group-IB Threat Intelligence and Research Centers

- Globally distributed cybercrime monitoring infrastructure
- Digital Forensics & Malware Analysis laboratory
- Incident Response and High-Tech Crime Investigations
- CERT-GIB: 24/7 monitoring centers and Computer Emergency Response Team

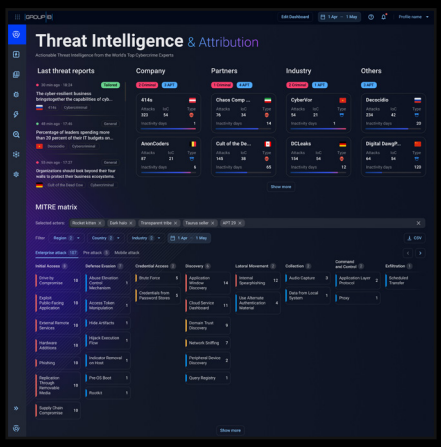
- Europe
- Russia
- Middle East
- Asia-Pacific

Group-IB's technologies & innovations

Group-IB's experience in performing successful global investigations with state-of-the-art threat intelligence and detecting cybercriminals at every stage of attack preparation has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

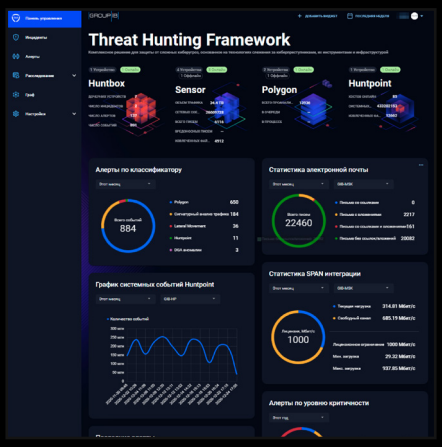
Group-IB's technologies are recognized by the world's leading research agencies

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN



Threat Intelligence & Attribution

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

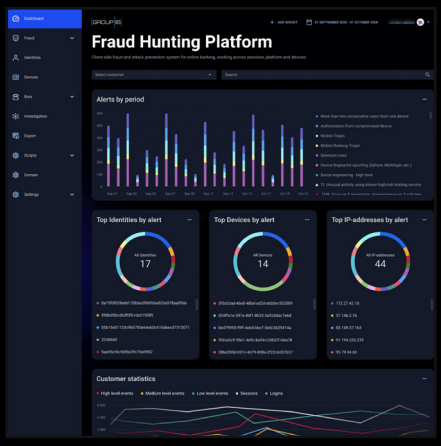


Threat Hunting Framework

Adversary-centric detection of targeted attacks and unknown threats within the infrastructure and beyond

Digital Risk Protection

AI-driven platform for digital risk identification and mitigation



Fraud Hunting Platform

Real-time client-side digital identity protection and fraud prevention

Atmosphere: Cloud Email Protection

Patented email security technology that blocks, detonates and hunts for the most advanced email threats

AssetZero

Intelligence-driven attack surface management that continuously discovers all external-facing IT assets

Group-IB Expertise

600+
world-class experts

70,000+
hours of incident response

1,300+
successful investigations worldwide

18 years
practical experience

Intelligence-driven services

Group-IB's technological leadership and R&D capabilities are built on the company's 18 years of hands-on experience in performing successful cybercrime investigations worldwide and the 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory and CERT-GIB.

Prevention

- Security Assessment
- Compliance Audit
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Response

- Managed Incident reponse
- Managed detection and threat hunting

Investigation

- Digital Forensics
- Investigations
- Financial Forensics
- eDiscovery

PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

www.group-ib.com info@group-ib.com group-ib.com/blog +7 495 984 3364