Acronis

Report
2022

Acronis Cyber Protection Operation Centers Report:

Ransomware dominates threat landscape

Acronis
Cyber Protection Operation Centers Report

Table of contents

Authors:

Alexander Ivanyuk
Senior Director, Product and Technology Positioning, Acronis

Candid Wuest
Vice President of Cyber Protection Research, Acronis

Irina Lukasheva
Cyber Protection Evangelist, Acronis

Introduction and summary

Acronis was the first company to implement complete integrated cyber protection to protect all data, applications and systems. Cyber protection requires the researching and monitoring of threats, as well as abiding by the five vectors of safety, accessibility, privacy, authenticity and security, or SAPAS. As part of the strategy, we've established four Cyber Protection Operation Centers (CPOCs) around the world to monitor and research cyberthreats 24/7.

We've also upgraded our current flagship products: Acronis Cyber Protect Cloud, a cloud solution added into the Acronis Cyber Cloud platform, and Acronis Cyber Protect 15, an on-premises solution. Prior to these releases, Acronis had been a leader in the data protection market with its innovative Acronis Active Protection anti-ransomware technology, which evolved over time to demonstrate Acronis' unique expertise at stopping threats aimed at data. However, it's important to note that the artificial intelligence (AI)- and behavior-based detection technologies that Acronis first developed in 2016 were expanded to address all forms of malware and other potential threats.

This report covers the threat landscape, as encountered by our sensors and analysts, during the first half of 2022.

General malware data presented in the report is gathered from January–June of this year and reflects threats targeting endpoints that we detected in these six months.

This report represents a global outlook and is based on over 700,000 unique endpoints distributed around the world. Most of the statistics discussed focus on threats for Windows operating systems, as they are much more prevalent compared to macOS and Linux. We will see how this situation develops and may include data on macOS and Linux threats in the next report.

The top six numbers of H1 2022: ↘

- The most malware-attacked countries in Q2 2022 were the U.S., Germany and Brazil.
- 21 million URLs were blocked on endpoints by Acronis in Q2 2022 — a 10% increase over Q1.
- 26.5% of all received emails were spam and 1% contained malware or phishing links.
- Each malware sample lives an average of 2.3 days in the wild before it disappears. 81% of samples were only seen once.
- The Conti ransomware gang has earned $2.7 billion in cryptocurrency in only two years, and in January 2022, the statistics show over 1,000 victims and victim payouts exceeding $150 million.
- Global ransomware damages are estimated to exceed $30 billion by 2023.

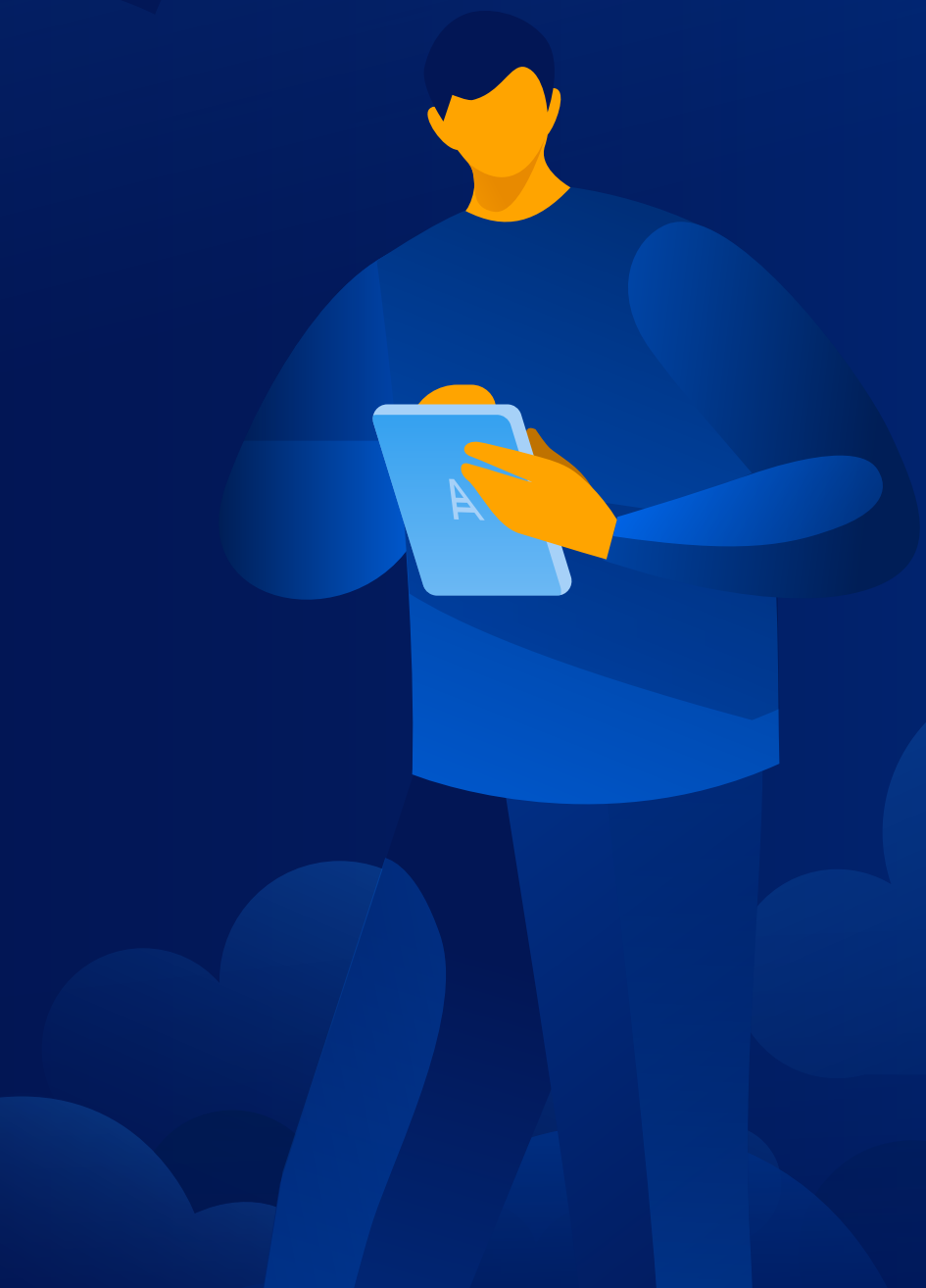
Among the cybersecurity trends we saw in the first half of 2022: ↘

- Ransomware continues to be the number-one threat to large and medium businesses — including government, healthcare and other critical organizations.
- Leaked or stolen credentials were the cause of almost half of reported breaches in H1 2022. Stolen credentials continue to be a driving force behind breaches, and with these credentials, attackers can easily execute phishing and ransomware campaigns.
- Social media platforms Twitter and Facebook, as well as DHL and Microsoft, were among the most-phished brands globally for the first half of 2022.
- MSPs are under attack, and liability questions have been raised. Over 80% of MSPs reported seeing more attacks against their customers in the last 12 months.
- 475 out of 12,985 reported vulnerabilities were being actively exploited in the first half of 2022.
- Linux OSs are getting more and more attention from cybercriminals, especially as they target cloud instances and containers.

What you will find in this report:

- The top security / threat trends we observed in the first half of 2022
- Why we're seeing more and more threats to cryptocurrencies
- Why MSPs and alternative operating systems are increasingly under threat
- General malware statistics and key families reviewed
- Ransomware statistics with a deep-dive analysis of the most dangerous threats
- Which vulnerabilities contribute to the success of attacks
- Our security recommendations

Key cyberthreats and trends for the first half of 2022



Several ransomware groups wreaking havoc globally

As we predicted in last year's final report, ransomware is getting worse — worse, in fact, than we had predicted.

While there are not many gangs left, and few new ones appeared during the first half of the year, those that are operating have done significant damage already. Conti and LockBit 2.0 were behind 58% of all publicly reported ransomware incidents in Q1 2022.

The threat is becoming so bad that the U.S. Department of State is offering up to $15 million for information that helps identify and locate leadership and co-conspirators of the Conti ransomware gang. Another big name of 2022 is the Lapsus$ gang, but let's start with Conti's recent "achievements."

Conti

Just recently, in May 2022, the notorious Conti ransomware gang officially shut down operations, with infrastructure taken offline and team leaders saying that the brand no longer exists. That may be a result of a bounty put on their heads by the FBI. The experienced Conti pen testers, negotiators and operators have joined smaller ransomware gangs to gain mobility, and now focus entirely on data exfiltration instead of data encryption. While the public-facing 'Conti News' data leak and ransom negotiation sites were online for a few weeks longer, the Tor admin panels used by members to perform negotiations and publish "news" on their data leak site are now offline.

That's nothing new for the ransomware criminal world — we saw other gangs officially "quit" just to continue under different names right away. For instance, Midas ransomware (previously known as Avaddon, then Haron) recently rebranded to Axxes ransomware. Leaked documents show that Conti had an HR department, performance reviews and even an "employee of the month." Rather than simply vanishing, Conti will almost certainly be rebranded and repurposed.

In any event, the Conti gang created real havoc before disbanding, and even started a trend of country-focused ransomware attacks. At the beginning of May, Costa Rican President Rodrigo Chaves declared a national emergency following cyberattacks from the Conti group in April on multiple government bodies. The list has since expanded to the Ministry of Labor and Social Security (MTSS), the Social Development and Family Allowances Fund (FODESAF) and the Interuniversity Headquarters of Alajuela (SIUA).

Conti ransomware attacks have affected multiple government services in Costa Rica, from the Finance Ministry to the Labor Ministry. One of the more recent victims was the Electricity Service of Cartago (JASEC). The Finance Ministry had to shut down for several hours, which also stopped handling pension and other payments. The Conti gang demanded $10 million in ransom, but Costa Rica said they will not pay anything. As a result, Conti published 97% of the stolen 672 GB data dump. Rather than attributing this cyberattack to nation-state attackers, Conti threat actor "UNC1756" along with their affiliate have claimed sole responsibility for it. After the attack against Costa Rica, they next hit Peru.

Other ransomware attacks have hit government organizations in Latin America, including Brazilian and Peruvian government organizations. Earlier, Costa Rica's public health service (known as Costa Rican Social Security Fund or CCCS) had to switch all computer systems on their network offline after they were hit with a Hive ransomware attack. All of these indicate a steep rise in ransomware attacks in 2022 — especially

against government organizations. We saw more than 20 countries hit the same way by targeted ransomware attacks in 2022.

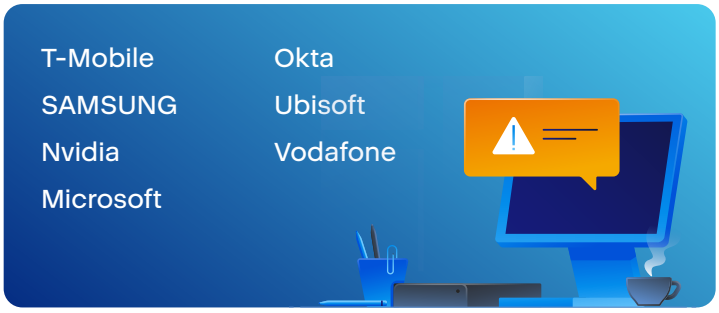
But don't think that Conti only was targeting government organizations — they've also attacked a fair number of regular companies. Among these is Newlat Food SPA, one of the largest Italian companies dedicated to food and dairy production. The company has over 1,500 employees and has listed an annual revenue of over €500 million. Conti published 2 GB of their data within the warning post, exfiltrated from the company's IT infrastructure — reporting that this is only 5% of what they possess.

The European company Nordex Group, known as one of the largest manufacturers of wind turbines and possessing an annual revenue of over $4 billion, was another Conti victim. KP Snacks, a popular snack producer in England with over 2,000 employees and an estimated annual revenue of over $600 million, was on Conti's list after companies such as Bank of Indonesia and the Nordic Choice Hotel Group had been victimized by them.

Unfortunately, it is again hard to believe that these attacks have come to an end, despite Conti's official cessation of operations.

Lapsus$

Another big development at the beginning of 2022 was the Lapsus$ gang. The group was first cited in December 2021 for a breach in the Brazilian Health Ministry's computer systems. And in March 2022, a prominent member of the group with the pseudonym White was arrested in Oxford, England. Later, several more arrests were made by the City of London Police in connection to a police investigation into Lapsus$. Within this short time, Lapsus$ was still able to hit such big companies as:



This is even more impressive when considering that the mastermind of the attacks and many other alleged accomplices were teenagers. And unlike more traditional ransomware criminal groups, Lapsus$ was extremely active on social media. The gang was communicating via a Telegram channel, which had at least 54,000 members and was the venue chosen by the group to release visual proof of their attacks.

Lapsus$ was focusing on data exfiltration. The group has stolen source code, service information, and often leaked confidential data and intellectual property online. They used a variety of approaches to compromise victims — like payments to insiders to enter systems, and stolen passwords. Lapsus$ has been observed using the RedLine Stealer to obtain session tokens and user credentials, among other methods for accessing these dark web-like marketplaces, initial access brokers and code repositories. They also made a few attempts to go after service and consulting companies that had an active relationship to the final victim — an extended variant of the supply chain attack method. Once they have gained a foothold in a network, they attempt to elevate privileges and exfiltrate data.

For instance, T-Mobile, with a revenue of $80 billion by the end of 2021, confirmed that the Lapsus$ extortion gang breached its network using stolen employee credentials (purchased online) to gain access to internal systems. Once they made it into the network, the attackers had access to internal tools like Atlas, T-Mobile's customer management system. According to leaked Telegram messages, the cybercrime group had stolen 30 GB of T-Mobile's source code; but per T-Mobile, the attackers didn't steal sensitive customer or government information during the incident.

The American technology company Nvidia, known for its computer graphic cards, was another major victim. The attackers gained access to hundreds of gigabytes of service data, including information on the company's developed chips. They stole 1 TB of data and leaked credentials of over 70,000 users and other documents including two old digital signing certificates, which have since been used to digitally sign new malware. Nvidia did fight back, as the attackers had to use a VPN client which also uses an MDM solution in order to connect to the corporate network. After the company realized this, they used this to connect back and encrypt the stolen data on the attacker's side.

Later on, the Lapsus$ gang attacked Samsung Electronics and leaked 190 GB of data, including the

source code of bootloaders, activation servers and trusted applets. Brazilian e-commerce giant Americanas was hit as well at the end of February. Americanas' financial report showed a loss of $183 million in sales due to their online shops not functioning. After five days, the company had restored normal operations.

Microsoft and secure identity platform Okta have both joined the ranks of the high-profile organizations that recently fell victim to the Lapsus$ gang. Microsoft said that the group gained limited access to their systems; however, Okta has confirmed that nearly 375, or 2.5%, of their customers may have had their data compromised in the attack, which has the potential to affect hundreds of companies.

Before the arrests, Lapsus$ also hit video game developer Ubisoft, which is known for the Assassin's Creed, Far Cry, Just Dance and Prince of Persia games, among others. While there were issues with accessing Ubisoft's web-based services in the wake of the attack, it does not appear that any personal information of players was put at risk, and all games and services have already been restored to full functionality.

Last but not least, they released 70 GB of data from IT firm Globant, making the firm the latest in a string of victims that include the likes of DHL, Facebook, BNP Paribas Cardif and Citibanamex, among others.

LockBit

LockBit is one of the most prolific ransomware families at the moment, with over 200 victims listed on their leak site in the third quarter of 2021, following the emergence of LockBit 2.0 in July. LockBit was also responsible for the ransomware attack on Accenture, in which they allegedly demanded a ransom of $50 million from the company.

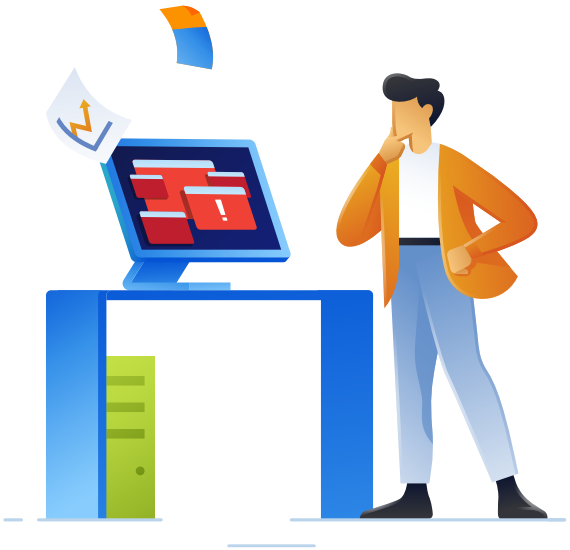
LockBit 2.0 has remained the dominant threat actor, accounting for over 400 victims in first half of 2022. Among the top cases for LockBit in 2022 were Taiwan-based manufacturing giant Foxconn, whose customers include Apple, Nintendo, Google and Microsoft. A ransomware attack in late May disrupted operations at one of its Mexico-based production plants, located in the city of Tijuana, on the border with California. That facility has 5,000 employees. The group behind the LockBit ransomware service carried out the attack and threatened to release the files on the internet if Foxconn didn't pay a ransom by June 11 — though neither LockBit nor Foxconn have indicated what files were stolen.

What is more alarming is that there is a new version of LockBit ransomware designed to encrypt files on Linux servers. The new version is specifically targeting ESXi servers, which means that encrypting a single server could impact a company significantly, as this would mean that many virtual machines (VMs) would be encrypted on each impacted server. The Linux variant of LockBit is harder to detect, but employs the same tactics as LockBit 2.0 — stealing data before encrypting it to use double-extortion tactics in the form of a threat that the data will be released or sold, and even offering a cut of the profits to individuals who are willing to give up their corporate credentials in order to spread the ransomware more efficiently.

At the end of June, the LockBit ransomware operation released "LockBit 3.0", and introduced the first official ransomware bug bounty program — asking security researchers to submit bug reports in return for rewards ranging between $1,000 and $1 million. This includes a head bounty for any information that would identify any of the main operators. Moreover, they have expanded the "services" for their victims, among which are:

- **Extend the "countdown":** The victim can pay money to extend the countdown for the publication of their data.
- **Destroy all information:** The victim can pay to destroy all information exfiltrated from their organization.
- **Download the data at any time:** The victim can pay to retrieve the company's exfiltrated data.

Obviously, the cost for each type of "service" is different and victims can pay via their choice of cryptocurrency: Bitcoin, Monero or Zcash.



Other gangs

While the three gangs covered above did a lot of damage globally, that doesn't mean that other ransomware gangs were silent. Hive ransomware was active as well, netting several big targets. One of these was Rompetrol, the operator of Romania's largest oil refinery, which produces more than five million tons of oil per year. As a result of the ransomware attack, Rompetrol has had to shut down its websites and the Fill&Go service at its gas stations, and has stated that the attack affected most of the company's IT services. The Hive group was threatening to leak data stolen in the attack unless Rompetrol paid a ransom of $2 million to keep their data private and receive the decryption key.

The Hive extortion group was targeting Microsoft Exchange servers, using them to deploy ransomware. The gang used the ProxyShell vulnerability that was patched last year to access the servers, and could complete their attack in as little as 72 hours.

Perusahaan Gas Negara (PGN) was hit by a Hive ransomware attack just days after the group also hit American healthcare provider Partnership HealthPlan of California (PHC). Being a healthcare organization, PHC is a more typical target for the Hive group. So far, Hive has leaked 400 GB of data containing 850,000 records as proof of the attack, but no patient data was included in what has already been leaked. They also hit the computer systems of the Italian train operations company Trenitalia, causing disruptions to ticket purchasing as well as to the tablets and applications used by onboard staff members. The Hive operators have demanded a ransom of $5 million in Bitcoin, with an ultimatum that the amount will double to $10 million if not paid within three days. The attack has also affected Trenord, as that company has a ticketing system connected to Trenitalia's system. However, Trenord was able to continue relatively normal operations by blocking affected ticket sales.

The Austrian state of Carinthia has suffered a BlackCat ransomware attack that encrypted around 3,000 computers, disrupting COVID-19 testing and contact tracing services. A ransom of $5 million has been demanded by the attacker.

A massive malware campaign distributed Magniber ransomware in April and May, disguised as Microsoft Windows updates. The campaign is affecting users around the world, and distributes the fake updates from fake warez and cracked software sites. The average ransom demand is for the equivalent of $2,500 worth of Bitcoin, and the campaign appears to be targeting students and other consumers instead of large organizations.

Some new/rebranded players appeared as well. Pandora ransomware hit Japanese auto giant DENSO, one of the largest automotive parts manufacturers in the world. Pandora is a new ransomware group that began operation in March, that steals data prior to encrypting files with a .pandora extension for use in multiextortion tactics. One working theory is that Pandora is a rebranding of Rook ransomware, as the two families share similar code and packers. DENSO has confirmed that their corporate network in Germany was breached, and they worked quickly to prevent the attacker from damaging additional systems. The company has stated that operations were not impacted; however, Pandora has begun leaking some of the 1.4 TB of files they claim to have stolen.

Another new ransomware threat known as Black Basta has emerged, attacking at least 12 companies within its first three weeks of operation — including the American Dental Association and wind farm operator Deutsche Windtechnik. Black Basta continues a trend of multiple-extortion tactics, in which data is stolen before encryption. This allows cybercriminals to threaten its public release if the ransom — one reaching $2 million so far — is not paid.

Still going strong, the Black Basta ransomware-as-a-service (RaaS) syndicate has amassed nearly 50 victims in the U.S., Canada, the U.K., Australia and New Zealand within two months of its emergence in the wild, starting in April 2022 — making it a prominent threat in a short window.

There are similarities between the code and websites used by Black Basta and Conti, leading some researchers to believe that Black Basta may be a rebranding of Conti. This is a common tactic used by threat actors to circumvent law enforcement. You can read a detailed analysis of Black Basta later in this report.

Phishing and malicious emails remain the main vector of infection

The following email and phishing statistics are taken from Perception Point, with whom we partner to deliver the Advanced Email Security pack for Acronis Cyber Protect Cloud. Acronis and Perception Point work together to protect organizations every minute to ensure they are safe from email-borne threats. The data was gathered for the first half of 2022 and combined with Acronis telemetry data for malware and URL blocks on the endpoints.

On average, each of the scanned emails contained 2.7 files and URLs — all of which might be a potential threat to the organization.

The Advanced Email Security pack for Acronis Cyber Protect Cloud is often deployed as a second layer of email filtering after traditional filtering is applied by the provider. This makes it even more surprising that at 26.5%, over one in four emails that came through were spam.

One out of 100, or 1%, of the received emails were malicious. In total, we observed 600 malicious email campaigns, of which 81% were phishing campaigns, with an average of 10 attacked organizations per campaign.

Not surprisingly, phishing made up over half of the malicious emails.

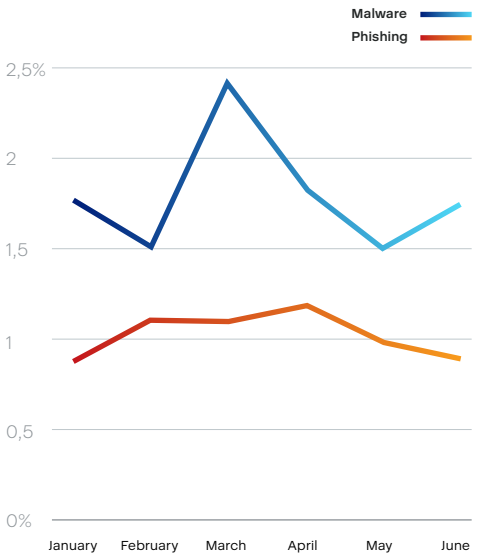
The Acronis CPOCs blocked 21,150,710 phishing and malicious URLs in Q2 2022. This constitutes a 10% spike over Q1 with a sum of 19,151,211.

Unfortunately, many emails with malicious content, especially URLs, still get through basic email filters and reach the user's endpoint. The malicious attachments are often multiple layers as well — for example, password-protected ZIP archives containing LNK files that download the final payload. This is another reason why it is important to have a multilayered defense approach.

Of course, the attackers are also often spoofing the target's own company brand — impersonating their IT department or HR.

Month in 2022	Blocked URLs
January	5,786,801
February	5,288,611
March	8,075,799
April	9,306,368
May	4,903,640
June	6,940,702

Rate of phishing and malware in emails per month in 2022



The top 10 most commonly impersonated brands in phishing emails were:

DHL	Facebook
Microsoft	AOL
Gmail	Hotmail
PayPal	Hewlett-Packard
Twitter	WeTransfer

Big cases and phishing trends

According to various reports and surveys, the top three cybercrimes reported by victims in 2021 were phishing scams, nonpayment/nondelivery scams and personal data breaches. This is nothing new, as business email compromise (BEC) scams are at an all-time high and growing. Investment and shopping fraud, as well as business correspondence with various malicious/weaponized attachments, will always be popular. The FBI has attributed a total loss of $2.4 billion to BEC for 2021 alone, and this only applies to the reported cases.

January kicked off with an ongoing spam wave of malicious emails containing a PowerPoint attachment with an obfuscated macro that uses a combination of PowerShell and MSHTA to run the payload once activated. This script then downloads either the Ave Maria or Agent Tesla malware. These are two common Trojans that can steal data, download further payloads and disable Microsoft Defender. Some of these payloads are hosted on legitimate cloud services in order to add more trust to the downloads. As we saw, one of the additional modules that was downloaded is an information stealer for cryptocurrency wallets, which also monitors the clipboard for any Bitcoin transaction address that it could replace with its own.

A similar approach was used in a malicious email campaign aimed at French entities that leverages the Chocolatey Windows package manager to deliver the Serpent backdoor. The phishing messages used a weaponized Microsoft Word document masquerading as information relating to the "règlement général sur la protection des données (RGPD)" or the European Union's General Data Protection Regulations (GDPR). The threat actor used steganography, including a cartoon image, to download and install the Serpent backdoor on the victim's device, which allows remote administration, command-and-control (C2) connections, data theft, or the delivery of additional payloads.

Fake online stores got a new spin. Cybercriminals have been creating many copies of online stores of popular brands. Thousands of victims were affected in Portugal, France, Spain, Italy, Chile, Mexico, Columbia and other countries. 617 active shopping platforms were identified during the research. The servers are located in three countries: the U.S., the Netherlands, and Turkey. A new campaign typically starts with the authors setting up the malicious domain at the top of Google search results through Google Ads. After some days, users are hit as the malicious URL appears at the top of searches. In specific cases, social ads were also found on the Instagram and Facebook social media platforms. The store collects personally identifiable information (PII), credit card details and other private data entered on the site when completing the order. Afterwards, they share a link to track the package but the victims will actually receive garbage, not clothes.

The campaign, which is targeting the electric vehicle market, has affected tens of thousands of victims, and has caused as much as $1 million in damages. It is abusing Google Ads and SEO practices to trick victims into providing personal information to malicious websites impersonating legitimate brands. With the rise of electric vehicles, the industry has become a valuable target for phishers who want a piece of this $200 billion sector.

There was also a large-scale phishing operation that abused Facebook and Messenger to lure millions of users to phishing pages, tricking them into entering their account credentials and seeing advertisements. More than 400 unique usernames were used as campaign identifiers, each having a separate Facebook phishing page. These phishing pages had page views ranging from only 4,000 views to the millions — in one case, as high as six million.

Cybercriminals also explored new vectors of attacks — for instance, a new phishing campaign targeting Calendly, an automated meeting scheduling tool, aims to steal users' credentials by embedding malicious links into event invitations. Phishing actors used the clever sequence to

trick targets into entering their email account credentials on the phishing page. These include generating malicious messages sent from a legitimate online service, asking the user to log in to view a blurred document in the background, forcing the victims to enter their credentials twice, and redirecting them to a trustworthy website at the end to withdraw any suspicion.

Two obvious signs of fraud in this campaign are the requirement to use Microsoft SharePoint credentials to view Calendly-hosted content and the URL on the phishing page, which is neither on the Microsoft nor on the Calendly domains.

Another trend is an uptick in the use of reverse-tunnel services along with URL shorteners for large-scale phishing campaigns, making the malicious activity more difficult to stop. More than 500 sites were hosted and distributed this way. Among them are ngrok, Localhost.run, Cloudflare's Argo, Bitly, is.gd and cutt.ly. Many of the phishing links are refreshed in less than 24 hours, making tracking and taking down the domains a more challenging task. With reverse tunnels, threat actors can host phishing pages locally on their computers and route connections through the external service. Using a URL shortening service, they can generate new links as often as they want to bypass detection. And then adversaries distribute these links through WhatsApp, Telegram, emails, texts or fake social media pages.

Last but not least, banking-related phishing didn't go away. The good news here is that there has been some success at catching the criminals. One example from May: Spanish police announced the arrest of 13 people and the launch of investigations into another seven for their participation in a phishing ring that stole online bank credentials. The police say the threat actors stole at least €443,600 from approximately 146 victims as part of these phishing attacks.

The threat actors used phishing lures to trick their victims into believing they received an alert from their bank and proceeded to steal their account credentials. Having access to banking accounts, the adversaries used their victims' money to make online purchases, direct transfers to "money mule" accounts or request personal loans.

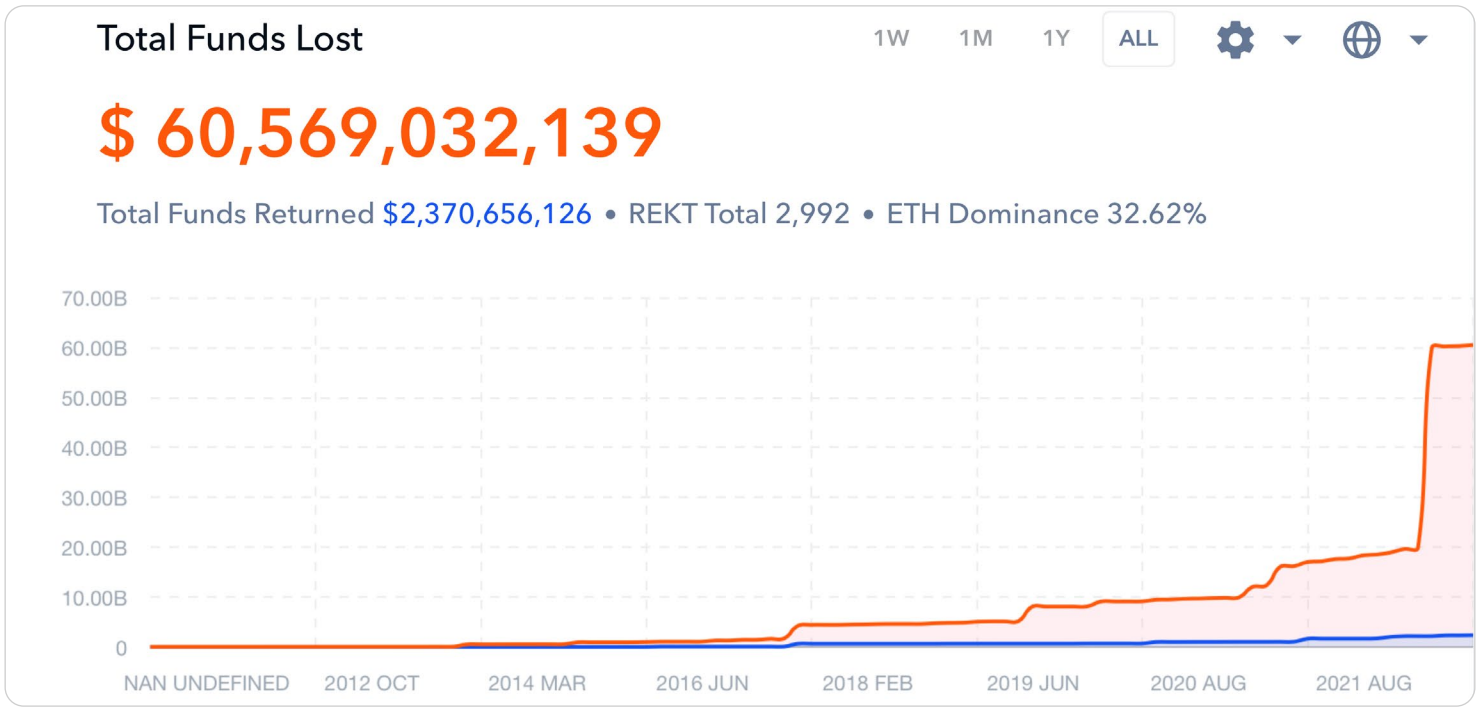
In Gloucester (U.K.), services have been offline for six months due to a cyberattack. It was reported that the malware entered the city administration network via a phishing email received by one of the employees. The city administration has allocated £630,000 for the restoration work, but opposition representatives fear that the total damage could be in the millions.

To summarize:

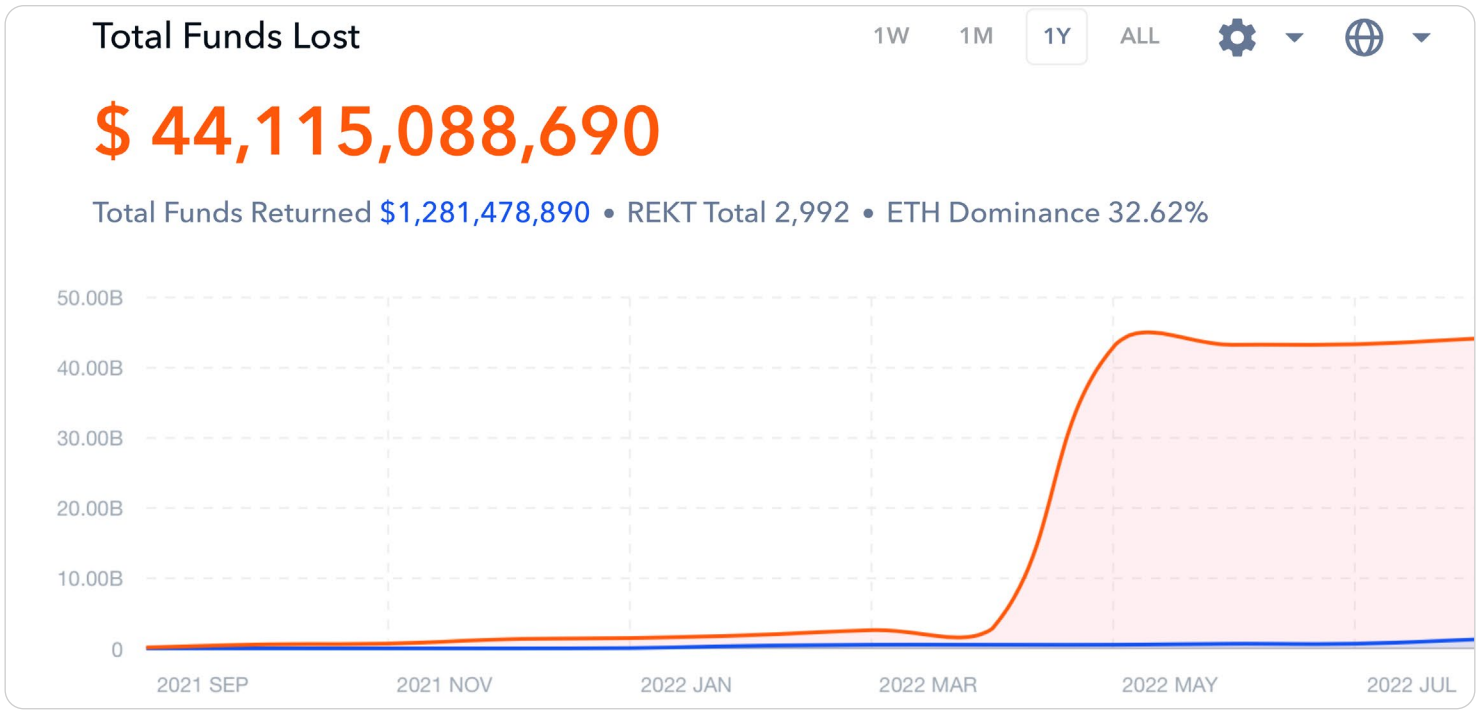
Phishing was, is, and will continue to be one of the most popular vectors of attack. Follow our recommendations at the end of the report to stay safe.

Cryptocurrencies under attack

While the value of most cryptocurrencies dropped dramatically in May and June, it is still and will be a valuable asset to steal for cybercriminals. Since this summer, we saw some of the biggest hacks in cryptocurrency industry history. More and more cybercriminals are focusing on less-secured decentralized finance planforms.



According to Rekt Database, a fully-featured database of DeFi scams, hacks and exploits, the total known loss of DeFi (decentralized finance) funds across all time was more than $60 billion at the time of this report's preparation, with $44 billion of those losses occurring in the last year.



Source: https://defiyield.app/rekt-database

Many DeFi protocols suffered flaws in their smart contracts that were exploitable, had other logic flaws, or were scammed by insiders.

In January, the DeFi protocol Qubit Finance was hit by cybercriminals who stole 206,809 Binance Coins (BNB) from Qubit's QBridge protocol, worth about $80 million at the time.

Just a week after that, Wormhole, a cryptocurrency platform that offers bridges to Solana and other blockchains, was hacked for 120,000 Ethereum (ETH) on February 2. Token bridges like Wormhole let users work with cryptocurrencies of different forms — Ethereum, Solana and more — without needing a centralized exchange. It allows users to receive and send cryptocurrencies in Solana, Binance Smart Chain (BSC), Polygon, Oasis, Avalanche and Terra. Wormhole has offered a bug bounty of $10 million to anyone who can return the funds. But in tracking hackers' activities, researchers saw that they already spent most of the funds they stole — either on other cryptoassets, or in preparation to cashout.

However, this hack was outperformed by the one conducted by the Lazarus APT group, which in March stole 173,600 ETH and 25.5 million USD Coins (USDC) from the Ronin cross-chain bridge, which allows users to transfer their digital assets from one cryptonetwork to another. According to Ronin, on March 23, Sky Mavis's Ronin validator nodes and Axie DAO validator nodes were compromised, resulting in 173,600 ETH and 25.5 million USDC drained from the Ronin bridge in two transactions. The attacker used hacked private keys in order to forge fake withdrawals. The U.S. government, specifically the Department of the Treasury, has sanctioned the address that received the stolen funds.

The Beanstalk attack cost $181 million at the time of its commencement in April. During the attack, 250,000 USDC was donated to the Ukraine Crypto Donation address. $181 million was drained from Beanstalk, but the hacker only kept $76 million, which was swapped on Ether and deposited into a Tornado Cash mixer in a bunch of transactions.

In June, Maiar DEX was exploited for about $113 million. Three wallets were used to sell a very substantial amount of EGLD. Addresses were created at the same time and received some funds from Binance, and they then deployed a smart contract. After the smart contract deployment, the attackers were able to withdraw over 1.65 million EGLD in blocks of 800k, 400k and 450k. They then began to dump the tokens, swapping them for blocks of 200k USDC.

Blockchain company Harmony reported another incident in June, when threat actors stole $100 million in cryptoassets. The FBI is investigating the cyberheist with the help of several cybersecurity firms.

On June 27, the threat actors behind the cyberheist began transferring the funds (roughly $39 million) through the Tornado Cash mixer service to launder the illicit profits. The blockchain security firm Elliptic was able to analyze the transactions even after the use of the mixer service; according to Elliptic, the Lazarus APT gang was behind the attack. It is not uncommon for nation-state APTs to use cryptocurrencies to bypass sanctions imposed against their respective countries.

Harmony offered one final opportunity for the cyberthieves to send the funds back with anonymity, allowing them to retain $10 million in exchange for the return of the rest.

Smart contract issues are just one of the risks in DeFi. We have also seen an uptick in malware that tries to steal the secret recovery phrases and passwords for online cryptowallets. Some targeted phishing campaigns were even going after owners of offline hardware wallets in order to steal coins. Strong passwords and good email and URL filters are therefore a must if you are in these fields.

Sometimes, the risks are not related to cybercriminals at all. For example, a weak design combined with unexpected selling pressure resulted in the Terra (LUNA) cryptocurrency dropping by 99% in May, leading to cascading effects and destroying around $45 billion in the process.

We will keep a close eye on what the combination of DeFi and upcoming metaverses will bring with regard to new attacks. But the current trend is clearly negative and unlikely to reverse.

One big challenge with cryptocurrencies is that very often the stolen funds cannot be recovered later. Because of the decentralized nature of DeFi, there is no central entity that can reset your account or return your coins. That's why if you or your business are investing in cryptocurrencies, we highly recommend storing your assets in an offline wallet and researching your choice of currencies carefully.

General malware threats

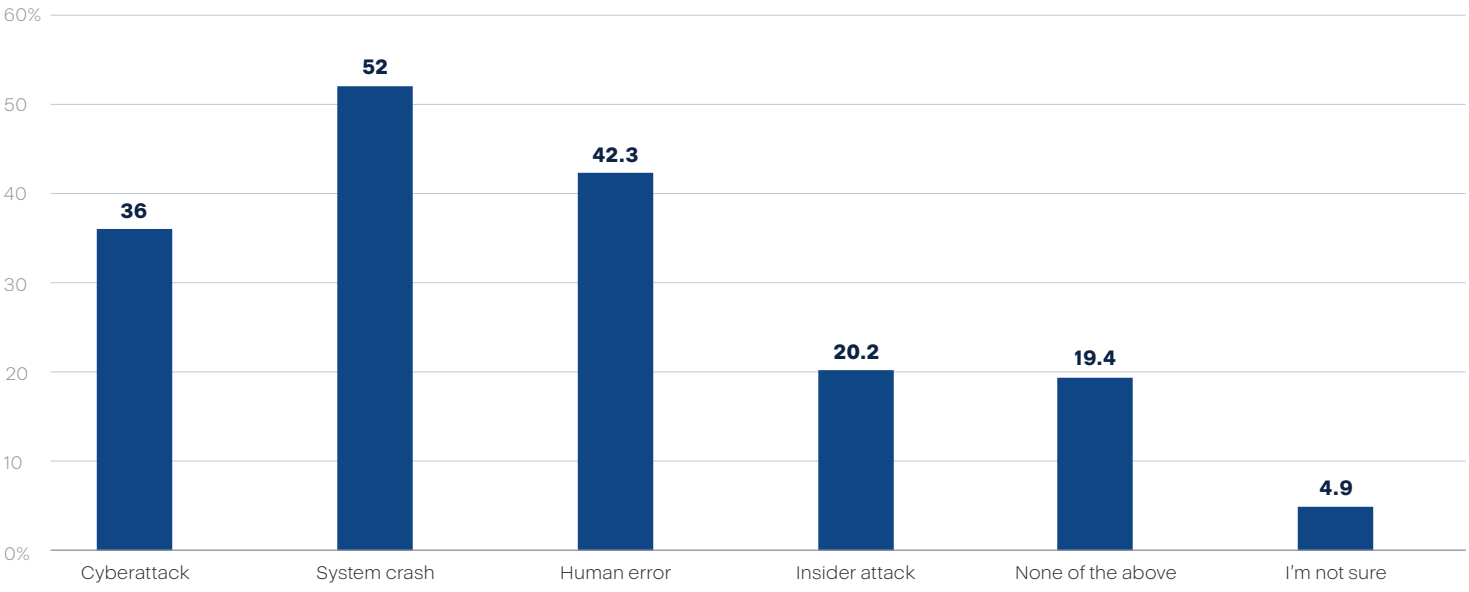
In Q2 2022, an average of 9.4% of our clients had at least one malware attack successfully blocked on their endpoints in any given month. This is a slight increase from 9.1% in Q1 2022. These percentages show that one out of 10 threats still makes it to the endpoint, despite the awareness training and patching performed by organizations. As these numbers are from detections on the endpoints, this also means that any proxy or email security that was deployed did not block these threats.

Percentage of clients with blocked malware

Month in 2022	Percentage of clients with blocked malware
January	10.7
February	8.7
March	8
April	9.2
May	9.7
June	9.4

The recent Acronis Cyber Protection Week Global Report 2022 showed that 76% of companies suffered IT service downtime in the last 12 months. Although only 36% of the downtime was caused by cyberattacks, malware was still the top cyberthreat that companies worried about — with 68% of respondents rating it a top priority. This is a huge jump from its position in last year's rankings, where malware attacks were in third place behind phishing and DDoS attacks. Of course, not every cyberattack leads to a system outage. Classic data theft attacks usually leave systems running without any disruption.

In the past year, has your organization experienced downtime due to any of the below?



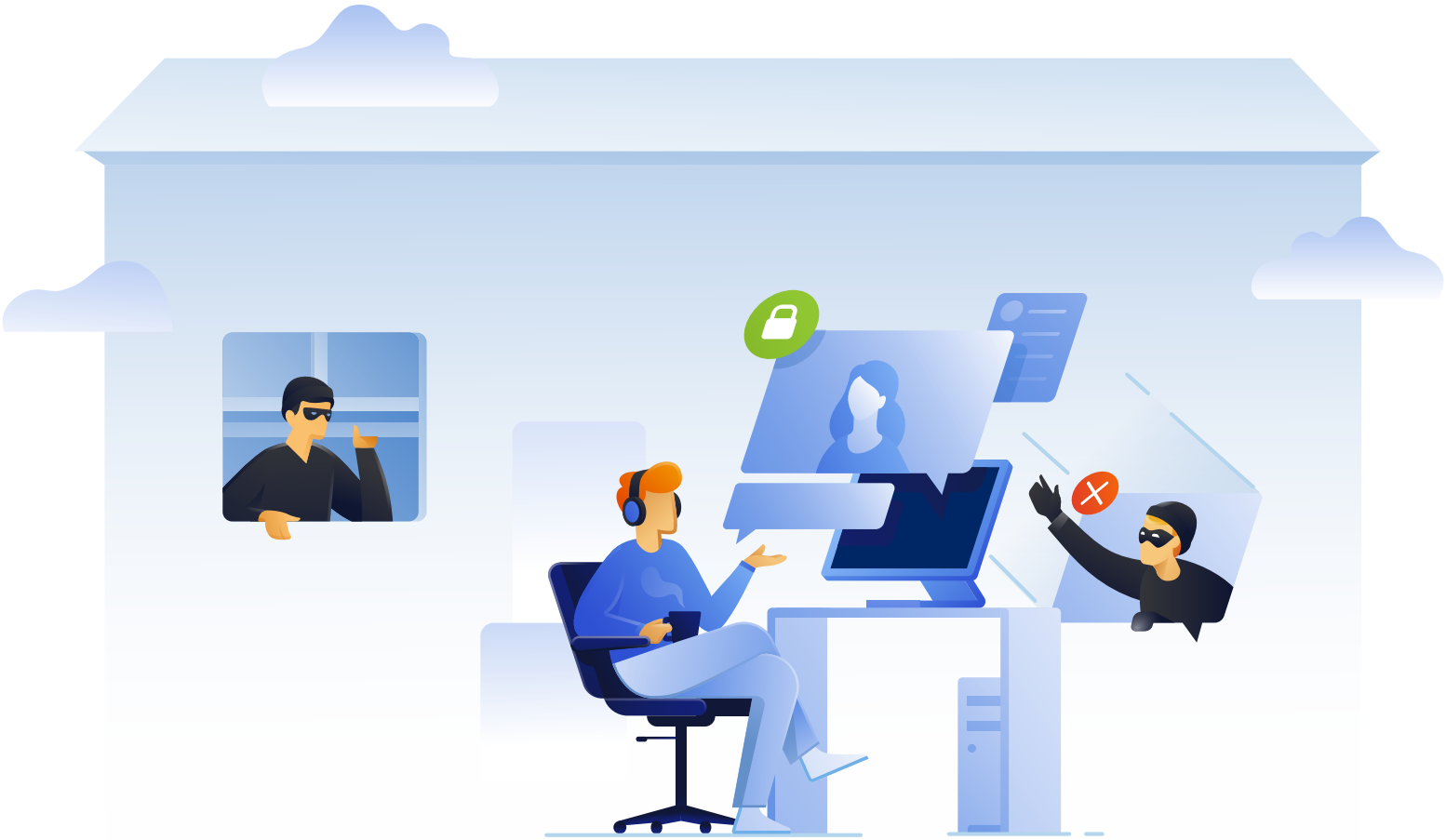
The number of new malware samples appearing in the wild has decreased slightly since 2021. The independent malware testing lab AV-TEST recorded 425,000 new malware samples per day in Q4 2021. In Q1 2022, this figure decreased by 24%, to 323,000 new malware samples per day. This proportion matches the number of new samples seen by the Acronis CPOCs. This decrease could be the result of some spikes at the end of last year, and more targeted distribution methods of malware — for example, through malware droppers and distribution networks.

The average lifetime of a malware sample in June 2022 was a mere 2.3 days. That's down from 3.4 days in Q3 2020. Automation on the attackers' side creates new and personalized malware at a higher frequency in order to bypass traditional signature-based detection. Eighty-one percent of the samples observed were only seen once across our entire customer base.

The following were the most commonly seen malware families in Q2, showing a clear focus on droppers and information stealers: ↘

- Formbook/XLoader
- Snake Keylogger
- Ave Maria
- Remcos
- LokiBot
- Agent Tesla
- Emotet
- RedLine Stealer
- QakBot
- Nanocore

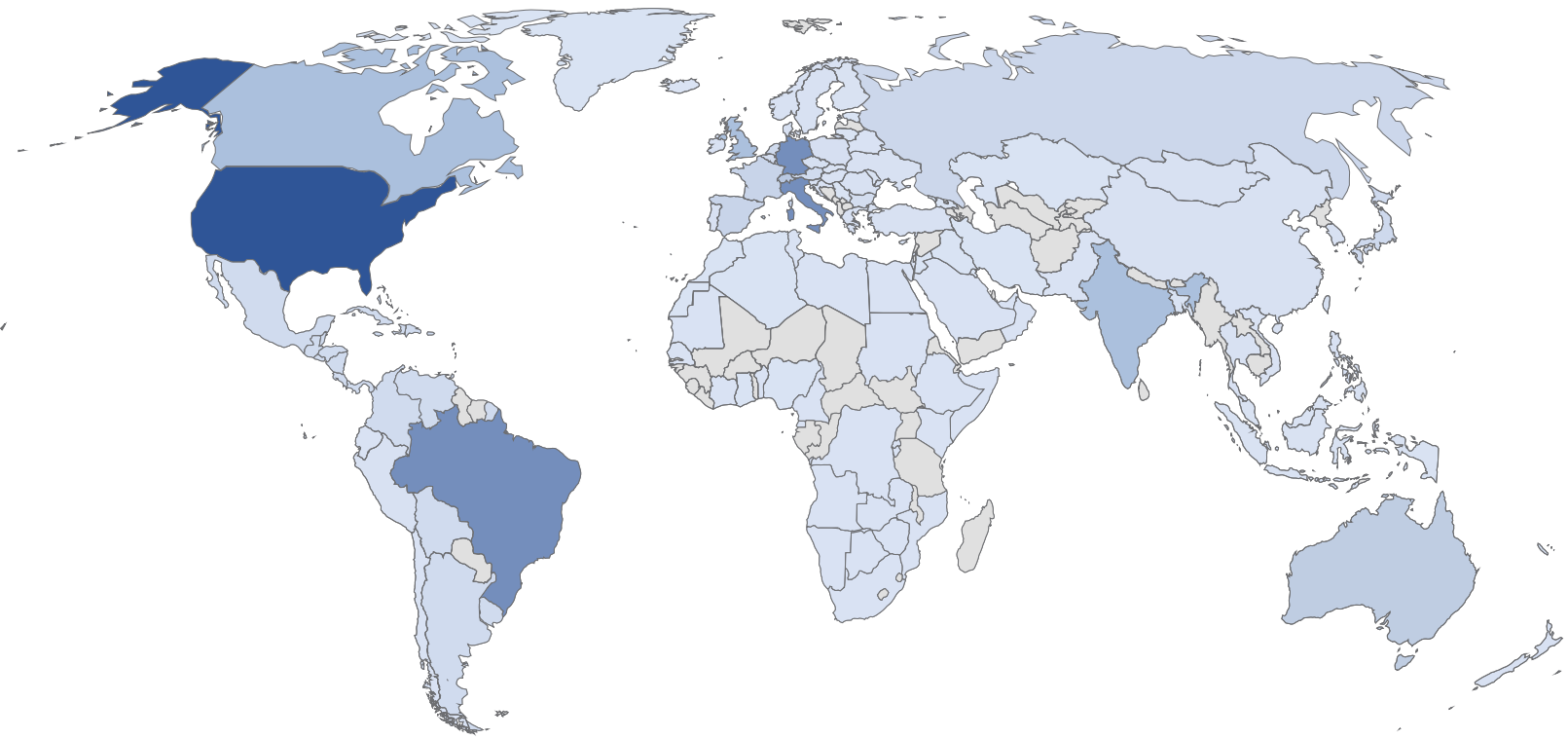
The country with the highest percentage of clients experiencing malware detections in June 2022 was the United States with 21.8%, followed by Germany with 8.9% and Brazil with 7.8%. These are very similar to the Q1 numbers, except for Brazil, which had an significant increase — especially with financial trojans.



Monthly percentage of global detections by country in 2022

Country	January	February	March	April	May	June
United States	24.4	25.4	24.6	23.7	22.8	21.8
Germany	13.2	12.7	11.2	11	9.4	8.9
Brazil	4.7	3.6	3.9	4.5	7.2	7.8
Italy	4.8	4.3	5.1	5.7	6.6	6
Canada	7.1	7.2	7.3	6.5	6.2	5.6
United Kingdom	5	5.4	5.4	5.3	5.3	4.9
Singapore	4.2	5	4.9	4.9	3.9	4.8
Switzerland	3	2.8	2.9	2.6	2.4	4.1
Japan	2.6	3	3.1	3	2.8	3.1
France	2.8	2.9	2.9	2.9	2.9	2.5

Malware detection June 2022



Percentage

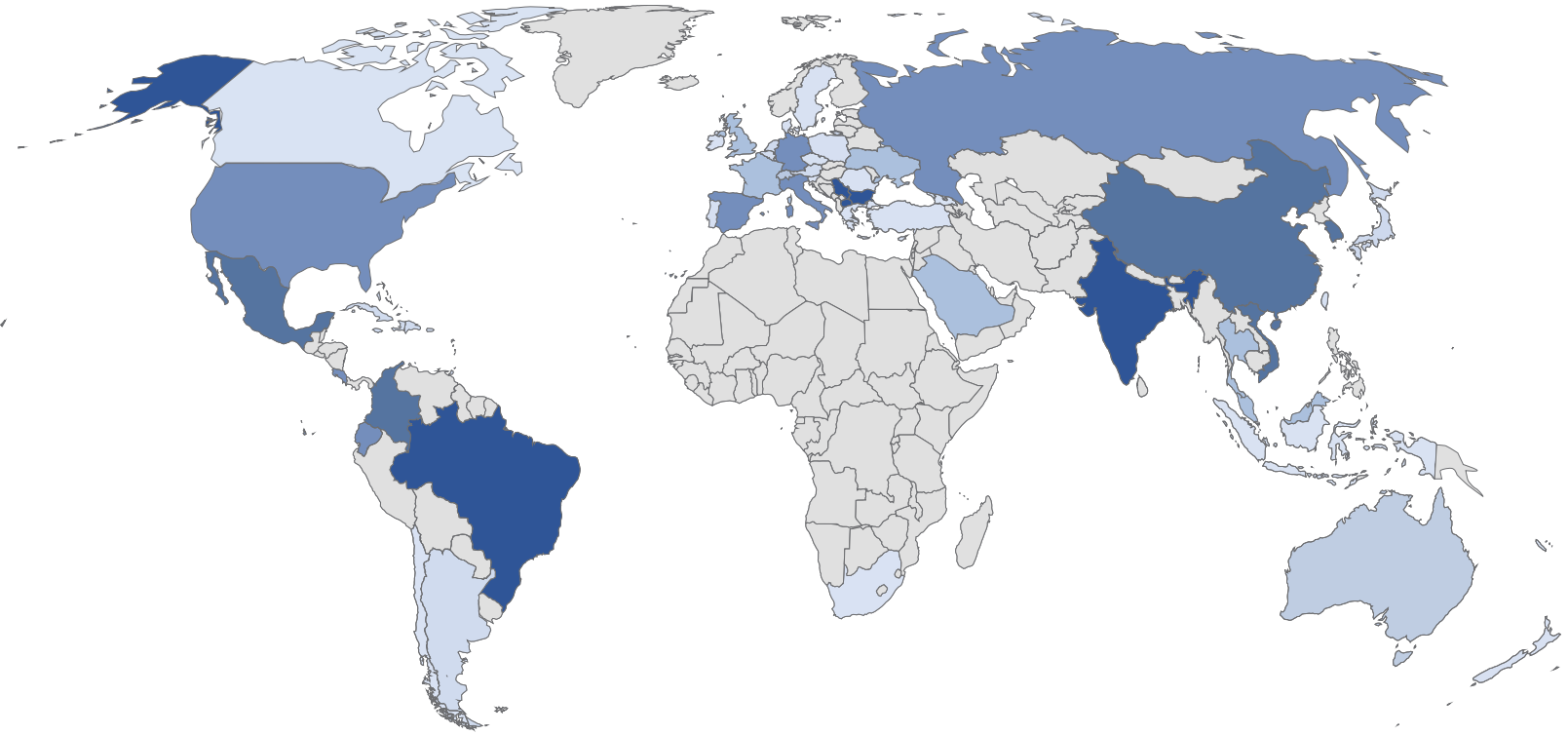
0% 21.8%

If we normalize the number of detections per active client per country, then we get a slightly different distribution. The following table shows the normalized percentage of clients with at least 25 malware detections per country in June 2022.

Monthly percentage of global detections by country in 2022

Rank	Country	Percentage of clients with malware detections in June 2022
1	Singapore	17.4
2	Brazil	15.7
3	Taiwan	15.7
4	Serbia	14.7
5	Colombia	14
6	India	13.9
7	Turkey	13.7
8	Bulgaria	13.6
9	China	13
10	South Korea	12.9
11	North Macedonia	12.7
12	Vietnam	12.7
13	Israel	11.4
14	United Arab Emirates	11.2
15	Mexico	10.8
16	Ecuador	10
17	Thailand	9.7
18	Malaysia	9.7
19	Japan	9.5
20	Argentina	9.1
21	Spain	9
22	Chile	8.9
23	Indonesia	8.7
24	New Zealand	8.7
25	Poland	8.5

Normalized number of detections in June 2022



Percentage

2.1% 17.4%

Regional normalized malware detection numbers

Top ten countries: normalized malware detection numbers by region

Asia

Rank	Country	Regional normalized malware detections percentage in June 2022
1	Singapore	17.4
2	Taiwan	15.7
3	India	13.9
4	Turkey	13.7
5	China	13
6	South Korea	12.9
7	Vietnam	12.1
8	Israel	11.4
9	United Arab Emirates	11.2
10	Thailand	9.7

EMEA

Rank	Country	Regional normalized malware detections percentage in June 2022
1	Serbia	14.7
2	Bulgaria	13.6
3	North Macedonia	12.7
4	Spain	9
5	Poland	8.5
6	Italy	8.3
7	Switzerland	7.9
8	Greece	7.7
9	South Africa	7
10	France	6.2

Americas

Rank	Country	Regional normalized malware detections percentage in June 2022
1	Brazil	15.7
2	Colombia	14
3	Mexico	10.8
4	Ecuador	10
5	Argentina	9.1
6	Chile	8.9
7	Peru	9.5
8	Costa Rica	8
9	United States	6.3
10	Canada	2.8

Ransomware threats

As we mentioned in the key trends section, ransomware is still the top cyberthreat for businesses. In this section, we're focusing on data from January–June 2022, including ransomware variants blocked by our threat-agnostic Acronis Active Protection and those that have published on underground leak sites.

These are the top 10 active ransomware families we observed and tracked in Q2 2022. Keep in mind that some groups try to infect as many end users as possible with a broad approach, while others focus on high-value targets, attempting only a handful of infections but striving for a high payout. Hence, the volume of threat detection alone is not an indication of the gravity of the threat. In addition, many groups operate ransomware-as-a-service businesses, so attackers might be using multiple threat families during similar attacks.

- LockBit
- Black Basta
- Vice Society
- Quantum
- Karakurt
- BlackCat/ALPHV
- Conti
- Industrial Spy
- Hive
- AvosLocker

We have seen 572 publicly mentioned ransomware compromises in Q2 — that's a 3% decline from Q1. Of course, this is only a subset, as some victims do negotiate and ultimately pay the ransomware groups in exchange for public silence. Also, some groups have shifted towards data exfiltration only; their targets might not appear as ransomware victims, but rather as data breach victims.

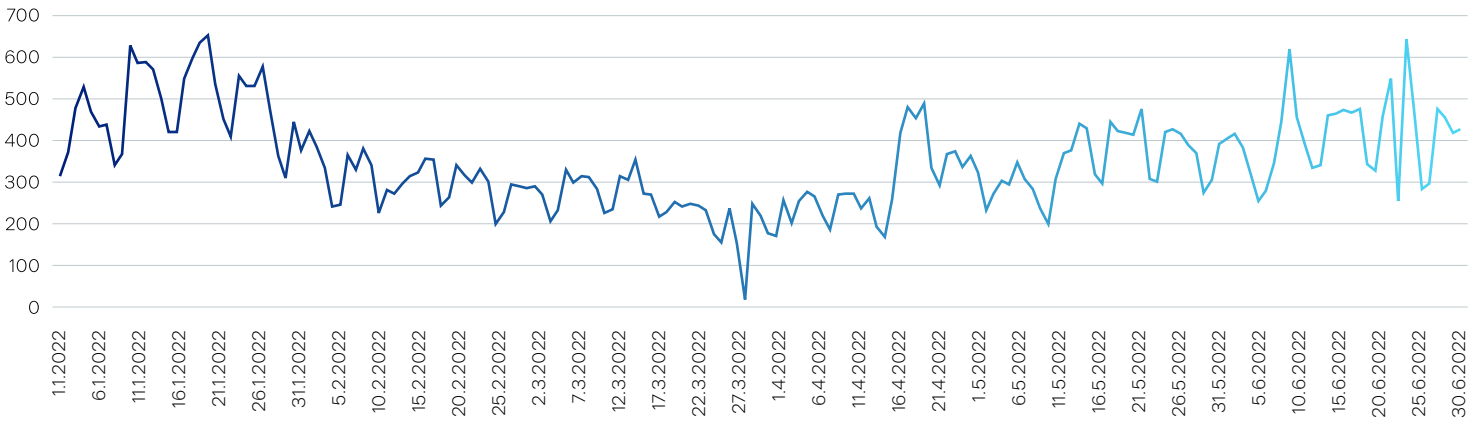
Daily ransomware detections

The number of ransomware incidents has increased only slightly — by 1% — in Q2. There have been a few arrests and more pressure from law enforcement against ransomware groups; on the other hand, some attacks are getting blocked earlier in the chain (for example, at the email lure or the malicious URL). In such events, the final payload is never downloaded and therefore not counted in this graph.

Changes in the number of ransomware detections per quarter per region

Quarter	EMEA	America	Asia	Global
Q1-Q2	-6%	-1%	+17%	+1%

Daily ransomware detections globally



Top ten countries: ransomware detections by region ↘

Asia

Country	Regional ransomware detections percentage in Q1 2022	Regional ransomware detections percentage in Q2 2022
Japan	34.3	33.7
China	13.1	12
Philippines	4	5.8
Taiwan	4.9	5.1
India	5.9	4.2
South Korea	4.5	4.1
Turkey	5.1	4
Singapore	1.8	3
Vietnam	1.4	2.6
Thailand	2.7	2.1

EMEA

Country	Regional ransomware detections percentage in Q1 2022	Regional ransomware detections percentage in Q2 2022
Germany	48.1	44
United Kingdom	7.7	8.7
France	7.1	8.1
Italy	5.3	6.2
Switzerland	5	4.7
Spain	3.5	4.6
Netherlands	3	2.9
Austria	2.8	2.6
Czechia	2	1.8
Ukraine	1.9	1.8

Americas

Country	Regional ransomware detections percentage in Q1 2022	Regional ransomware detections percentage in Q2 2022
United States	65	62.7
Canada	25.1	23.9
Mexico	2.8	3.8
Brazil	1.6	1.7
Argentina	0.9	1.4
Colombia	0.6	1.1
Peru	0.5	0.9
Chile	0.6	0.8
Guatemala	0.4	0.6
Ecuador	0.3	0.4

Ransomware groups in the spotlight

NightSky ransomware delivered via Log4j vulnerability

At the start of December 2021, the whole IT community shuddered after the discovery of the critical Apache Log4j vulnerability (CVE-2021-44228), which made it possible to perform remote code execution on victims' machines. Log4j is an open-source, Java-based login utility, and it's present in a wide range of software. Exploiting the bug to gain access to victims' systems requires minimal effort, which makes this attack vector very attractive to criminals. The NightSky ransomware gang quickly started exploiting this vulnerability to gain access to victims' VMware Horizon systems, located in corporate networks, to download and execute the ransomware.

Overview

NightSky sample (SHA256:8c1a72991fb04dc3a8cf89605fb85150ef0e742472a0c58b8fa942a1f04877b0) is a PE32+ (64 bit) file written in C++ and packed with VMProtect.

At the start of the main function, the malware calls the sub_7FF63BBA10F0() function. This function contains the initialization of the RSA2048 public key, which is hardcoded in the sample code. This key will be used to encrypt the RSA2048 private key and AES key.

```
.text:00007FF63BBA11D4 test    rax, rax
.text:00007FF63BBA11D7 mov     qword ptr cs:xmmword_7FF63BBF4210+8, rax
.text:00007FF63BBA11DE lea     rcx, unk_7FF63BBE3F90
.text:00007FF63BBA11E5 mov     r8, rbx
.text:00007FF63BBA11E8 cmovz   rcx, qword ptr cs:xmmword_7FF63BBF4210
.text:00007FF63BBA11F0 lea     rdx, aBeginPublicKey            ; "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgk"...
.text:00007FF63BBA11F7 mov     qword ptr cs:xmmword_7FF63BBF4210, rcx
.text:00007FF63BBA11FE xchg    ax, ax
.text:00007FF63BBA1200
.text:00007FF63BBA1200 loc_7FF63BBA1200:                       ; CODE XREF
.text:00007FF63BBA1200 inc     r8
.text:00007FF63BBA1203 cmp     byte ptr [rdx+r8], 0
.text:00007FF63BBA1208 jnz     short loc_7FF63BBA1200
.text:00007FF63BBA120A inc     r8
.text:00007FF63BBA120D lea     rcx, xmmword_7FF63BBF5220
.text:00007FF63BBA1214 call    sub_7FF63BBAB2F0
.text:00007FF63BBA1219 mov     rax, qword ptr cs:xmmword_7FF63BBF4210+8
```

```
aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
                                        ; DATA XREF: sub_7FF63BBA10F0+100↑o
                db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwetDt+9kp5JJGCb3YrqH',0Ah
                db '48g0rxFIaj5/NjMBvxtpa+7nO/lS0FQXxWJO78dTT6xW/UgVLPK4MvbGeIj17aQF',0Ah
                db 'SqGHbRxTeoPrHufp4sM4J2IQYLc6YLYZMS6XT02rHOjumBJpEKyROQ+df5KU/06o',0Ah
                db 'Rrhljc0Qco+qW8q/xYJQ9VFa87IJM6WM3wsydHVDDeGuWi4/PMUT4/GAa8/WMUYW',0Ah
                db '9Ebw7/hXd/aNX5LykeonN+nkJfbj1fZNTU81tc8Kx4rykLvMVE1H3AaT5ssCBt7p',0Ah
                db 'AFkLLjplOXz3XmhH+J5vm5Ifi7T85j4D6O03qocO2gwezIikCDU2YAOOpJzkb5Ab',0Ah
                db '+wIDAQAB',0Ah
                db '-----END PUBLIC KEY-----',0Ah,0
```

The malware then creates new threads and checks for the presence of a mutex (“tset123155465463213”) to see if the program is already running; if it’s missing, NightSky will create it. It also checks for available drives by calling the GetLogicalDrives() function.

```
.text:00007FF63BBA24B7 xor     edx, edx                        ; dwStackSize
.text:00007FF63BBA24B9 xor     ecx, ecx                        ; lpThreadAttributes
.text:00007FF63BBA24BB call    cs:CreateThread
.text:00007FF63BBA24C1 xor     r9d, r9d                        ; lpParameter
.text:00007FF63BBA24C4 mov     [rsp+98h+lpThreadId], r13       ; lpThreadId
.text:00007FF63BBA24C9 lea     r8, StartAddress                ; lpStartAddress
.text:00007FF63BBA24D0 mov     [rdi+rbx], rax
.text:00007FF63BBA24D4 xor     edx, edx                        ; dwStackSize
.text:00007FF63BBA24D6 mov     [rsp+98h+dwCreationFlags], r13d ; dwCreationFlags
.text:00007FF63BBA24DB xor     ecx, ecx                        ; lpThreadAttributes
.text:00007FF63BBA24DD call    cs:CreateThread
.text:00007FF63BBA24E3 mov     [rbx], rax
.text:00007FF63BBA24E6 lea     rbx, [rbx+8]
.text:00007FF63BBA24EA sub     rbp, 1
.text:00007FF63BBA24EE jnz     short loc_7FF63BBA24A0
.text:00007FF63BBA24F0
.text:00007FF63BBA24F0 loc_7FF63BBA24F0:                       ; CODE XREF: main+222↑j
.text:00007FF63BBA24F0 lea     r8, Name                        ; "tset123155465463213"
.text:00007FF63BBA24F7 xor     edx, edx                        ; bInheritHandle
.text:00007FF63BBA24F9 mov     ecx, 1F0001h                    ; dwDesiredAccess
.text:00007FF63BBA24FE call    cs:OpenMutexA
.text:00007FF63BBA2504 test    rax, rax
.text:00007FF63BBA2507 jnz     loc_7FF63BBA25C1
.text:00007FF63BBA250D lea     r8, Name                        ; "tset123155465463213"
.text:00007FF63BBA2514 xor     edx, edx                        ; bInitialOwner
.text:00007FF63BBA2516 xor     ecx, ecx                        ; lpMutexAttributes
.text:00007FF63BBA2518 call    cs:CreateMutexA
.text:00007FF63BBA251E call    cs:GetLogicalDrives
.text:00007FF63BBA2524 mov     ebp, eax
```

File encryption

The main encryption function is sub_7FF63BBA19F0(). At the start, it creates a ransom note file named “NightSkyReadme.hta” using hard-coded HTML and writes it to the current search folder.

```
.text:00007FF63BBA1A26 call    cs:RtlAllocateHeap
.text:00007FF63BBA1A2C mov     rsi, rax
.text:00007FF63BBA1A2F test    rax, rax
.text:00007FF63BBA1A32 jz      short loc_7FF63BBA1A14
.text:00007FF63BBA1A34 mov     rdx, r14                        ; lpString2
.text:00007FF63BBA1A37 mov     rcx, rax                        ; lpString1
.text:00007FF63BBA1A3A call    cs:lstrcpyW
.text:00007FF63BBA1A40 lea     rdx, aNightskyreadme            ; "\\NightSkyReadMe.hta"
.text:00007FF63BBA1A47 mov     rcx, rsi                        ; lpString1
.text:00007FF63BBA1A4A call    cs:lstrcatW
.text:00007FF63BBA1A50 xor     r15d, r15d
.text:00007FF63BBA1A53 xor     r9d, r9d                        ; lpSecurityAttributes
.text:00007FF63BBA1A56 mov     [rsp+2D8h+hTemplateFile], r15   ; hTemplateFile
.text:00007FF63BBA1A5B mov     edx, 40000000h                  ; dwDesiredAccess
.text:00007FF63BBA1A60 mov     [rsp+2D8h+dwFlagsAndAttributes], r15d ; dwFlagsAndAttributes
.text:00007FF63BBA1A65 mov     rcx, rsi                        ; lpFileName
.text:00007FF63BBA1A68 mov     [rsp+2D8h+dwCreationDisposition], 1 ; dwCreationDisposition
.text:00007FF63BBA1A70 lea     r8d, [r15+1]                    ; dwShareMode
.text:00007FF63BBA1A74 call    cs:CreateFileW
.text:00007FF63BBA1A7A mov     rbx, rax
.text:00007FF63BBA1A7D cmp     rax, 0FFFFFFFFFFFFFFFFh
.text:00007FF63BBA1A81 jz      short loc_7FF63BBA1AB6
.text:00007FF63BBA1A83 lea     rcx, Buffer                     ; lpString
.text:00007FF63BBA1A8A call    cs:lstrlenA
.text:00007FF63BBA1A90 lea     r9, [rsp+2D8h+NumberOfBytesWritten] ; lpNumberOfBytesWritten
.text:00007FF63BBA1A95 mov     qword ptr [rsp+2D8h+dwCreationDisposition], r15 ; lpOverlapped
.text:00007FF63BBA1A9A mov     r8d, eax                        ; nNumberOfBytesToWrite
.text:00007FF63BBA1A9D lea     rdx, Buffer                     ; lpBuffer
.text:00007FF63BBA1AA4 mov     rcx, rbx                        ; hFile
.text:00007FF63BBA1AA7 call    cs:WriteFile
.text:00007FF63BBA1AAD mov     rcx, rbx                        ; hObject
.text:00007FF63BBA1AB0 call    cs:CloseHandle
```

Then it starts to find and encrypt files across the victims’ folders. NightSky malware has a list of ignored file extensions which include ‘.exe’ and ‘.dll’. It also skips already-encrypted files.

```
.text:00007FF63BBA1BB5 loc_7FF63BBA1BB5:                       ; CODE XREF: sub_7FF63BBA19F0+1B9↑j
.text:00007FF63BBA1BB5 cdqe
.text:00007FF63BBA1BB7 lea     rbx, [rsp+2D8h+FindFileData.cFileName]
.text:00007FF63BBA1BBC lea     rdx, aExe                       ; ".exe"
.text:00007FF63BBA1BC3 lea     rbx, [rbx+rax*2]
.text:00007FF63BBA1BC7 mov     rcx, rbx                        ; String1
.text:00007FF63BBA1BCA call    cs:uaw_lstrcmpiW
.text:00007FF63BBA1BD0 test    eax, eax
.text:00007FF63BBA1BD2 jz      loc_7FF63BBA1D79
.text:00007FF63BBA1BD8 lea     rdx, aDll                       ; ".dll"
.text:00007FF63BBA1BDF mov     rcx, rbx                        ; String1
.text:00007FF63BBA1BE2 call    cs:uaw_lstrcmpiW
```

Additionally, the following files and folders will be skipped during encryption:

AppData	Mozilla Firefox	bootmgfw.efi
Boot	$Recycle.Bin	desktop.ini
Windows	ProgramData	iconcache.db
Windows.old	All Users	ntldr
Tor Browser	autorun.inf	ntuser.dat
Internet Explorer	boot.ini	ntuser.dat.log
Google	bootfont.bin	ntuser.ini
Opera	bootsect.bak	thumbs.db
Opera Software	bootmgr	Program Files
Mozilla	bootmgr.efi	Program Files (x86)

If the file being examined doesn’t match any of these exclusions, the program will read it and call the sub_7FF63BBA1000() function, which will then encrypt the file with the AES-128-CBC algorithm. The maximum encrypted block size is 524288*3 bytes, or approximately 1.57 MB.

```
.text:00007FF63BBA1830 loc_7FF63BBA1830:                       ; CODE XREF: sub_7FF63BBA1400+4B1↓j
.text:00007FF63BBA1830 lea     r9, [rsp+2540h+NumberOfBytesRead] ; lpNumberOfBytesRead
.text:00007FF63BBA1835 mov     qword ptr [rsp+2540h+dwCreationDisposition], rbx ; lpOverlapped
.text:00007FF63BBA183A mov     r8d, 80000h                     ; nNumberOfBytesToRead
.text:00007FF63BBA1840 mov     rdx, r14                        ; lpBuffer
.text:00007FF63BBA1843 mov     rcx, r12                        ; hFile
.text:00007FF63BBA1846 call    cs:ReadFile
.text:00007FF63BBA184C mov     r8d, 80000h
.text:00007FF63BBA1852 lea     rcx, [rbp+2440h+Src]
.text:00007FF63BBA1859 mov     rdx, r14
.text:00007FF63BBA185C call    sub_7FF63BBA1000                ; eas_128_CBC_enctyption
.text:00007FF63BBA1861 xor     r9d, r9d                        ; dwMoveMethod
.text:00007FF63BBA1864 xor     r8d, r8d                        ; lpNewFilePointer
.text:00007FF63BBA1867 mov     rdx, rdi                        ; liDistanceToMove
.text:00007FF63BBA186A mov     rcx, r12                        ; hFile
.text:00007FF63BBA186D call    cs:SetFilePointerEx
.text:00007FF63BBA1873 lea     r9, [rsp+2540h+NumberOfBytesWritten] ; lpNumberOfBytesWritten
.text:00007FF63BBA1878 mov     qword ptr [rsp+2540h+dwCreationDisposition], rbx ; lpOverlapped
.text:00007FF63BBA187D mov     r8d, 80000h                     ; nNumberOfBytesToWrite
.text:00007FF63BBA1883 mov     rdx, r14                        ; lpBuffer
.text:00007FF63BBA1886 mov     rcx, r12                        ; hFile
.text:00007FF63BBA1889 call    cs:WriteFile
```

This function contains a hardcoded IV key of ‘4030201h’ in hexadecimal, which is ‘67305985’ in decimal. It will then call the sub_7FF63BBA63D0() function which takes aes_context, aes_encrypt, 16ui64 converter, the IV key and two buffers as parameters. It will then encrypt the data.

```
.text:00007FF63BBA1000                 mov     r11, rsp
.text:00007FF63BBA1003                 mov     [r11+8], rbx
.text:00007FF63BBA1007                 mov     [r11+18h], rsi
.text:00007FF63BBA100B                 push    rdi
.text:00007FF63BBA100C                 sub     rsp, 170h
.text:00007FF63BBA1013                 mov     rax, cs:__security_cookie
.text:00007FF63BBA101A                 xor     rax, rsp
.text:00007FF63BBA101D                 mov     [rsp+178h+var_18], rax
.text:00007FF63BBA1025                 movsxd  rsi, r8d
.text:00007FF63BBA1028                 mov     rbx, rdx
.text:00007FF63BBA102B                 mov     rdi, rcx
.text:00007FF63BBA102E                 mov     dword ptr [r11-28h], 4030201h ; IV_key
.text:00007FF63BBA1036                 xor     edx, edx        ; Val
.text:00007FF63BBA1038                 mov     dword ptr [r11-24h], 4030201h ; IV_key
.text:00007FF63BBA1040                 mov     r8d, 120h       ; Size
.text:00007FF63BBA1046                 mov     dword ptr [r11-20h], 4030201h ; IV_key
.text:00007FF63BBA104E
.text:00007FF63BBA104E loc_7FF63BBA104E:                       ; DATA XREF: .2fU0:00007FF63BD05DA
.text:00007FF63BBA104E                 lea     rcx, [rsp+178h+var_148] ; void *
.text:00007FF63BBA1053                 mov     dword ptr [r11-1Ch], 4030201h ; IV_key
.text:00007FF63BBA105B                 call    memset
```

In the end, the encrypted file will be rewritten with the .nightsky extension and the malware will proceed to search the next file.

Obfuscation

This malware sample is packed with VMProtect software, which makes it very hard to analyze. The packed file contains only 17 functions, a count which grows to 986 after unpacking.

Function name	Segment
sub_1403B4672	.2fU2
nullsub_3	.2fU2
sub_1407FD2CF	.2fU2
sub_1407FD458	.2fU2
sub_1407FD719	.2fU2
sub_1407FD725	.2fU2
sub_1407FD73D	.2fU2
sub_140945A19	.2fU2
sub_140945A32	.2fU2
sub_140945A4B	.2fU2
sub_140945A64	.2fU2
sub_140945A7D	.2fU2
sub_140945A96	.2fU2
sub_140945AAF	.2fU2
sub_140945AC8	.2fU2

Line 17 of 17

Function name	Segment
sub_7FF63BBA1000	.text
sub_7FF63BBA10F0	.text
sub_7FF63BBA1400	.text
sub_7FF63BBA19F0	.text
sub_7FF63BBA1DE0	.text
StartAddress	.text
main	**.text**
sub_7FF63BBA2780	.text
sub_7FF63BBA2790	.text
sub_7FF63BBA2890	.text
sub_7FF63BBA2A30	.text
sub_7FF63BBA2B70	.text
sub_7FF63BBA2E00	.text
std::_Future_error_map(int)	.text
sub_7FF63BBA2E80	.text
sub_7FF63BBA2EE0	.text
sub_7FF63BBA3180	.text
sub_7FF63BBA32C0	.text
sub_7FF63BBA3400	.text
sub_7FF63BBA34E0	.text
sub_7FF63BBA3640	.text
sub_7FF63BBA3650	.text
sub_7FF63BBA38A0	.text
sub_7FF63BBA3980	.text
sub_7FF63BBA3AC0	.text
sub_7FF63BBA3D00	.text
sub_7FF63BBA4B60	.text
sub_7FF63BBA4C20	.text
sub_7FF63BBA4F00	.text
sub_7FF63BBA5480	.text

Line 6 of 986

Ransom note

The ransom note NightSkyReadme is an '.hta' file (HTML application). It contains information stating that the victim has been hacked and their data has been stolen. The attackers provide a link, username and password to contact them via web chat, as well as an email address and a .onion URL to the data leak site. They promise the victim that their data will remain safe so long as the attackers' demands are met.

NIGHT SKY

WARNING!

Your company has been hacked by us.

Internal files have been stolen and encrypted by us.

But don't worry, we didn't destroy them, and we won't leak data right away.

If your company is willing to meet our requirements,

we will decrypt the data and destroy the stolen data without data leakage.

Contact information

- Web Chat:

```
You can use the username and password provided by us to login to the chat room to communicate with us.
URL:https://contact.nightsky.cyou
username:user-kdwckln
password:kdjfikerjjsjJHDUFIGjk3289
```

- Email:

```
You can contact us by email.
EMAIL ADDRESS:akij@nightsky.cyou
```

Data release website

- Where we use to disclose the data of customers who do not pay

```
http://gg5ryfgogainisskdvh4y373ap3b2mxafcibeh21vq5x7fx76ygcosad.onion
```

The data leak site includes two additional pages with previous victims' data. If a new target is attacked with NightSky ransomware, there will be a new page with information about leaked data and further instructions regarding payment.

Conclusion

NightSky ransomware appeared in late December 2021 and started attacking corporate networks using the Apache Log4j vulnerability. Some cybersecurity researchers have found that the sample code has similarities with Rook ransomware. This sample is packed with VMProtect, which makes it more difficult to analyze. NightSky uses the RSA-2048 public key and the AES-128-CBC algorithm for file encryption. It can read computer names, users' languages and countries, and view the registry. Encrypted files have the '.nightsky' extension, while the ransom note with instructions and URLs is in '.hta' format.

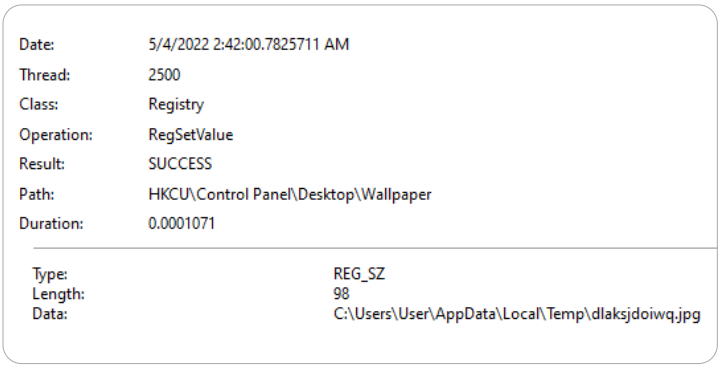
Black Basta ransomware: a successor of Conti?

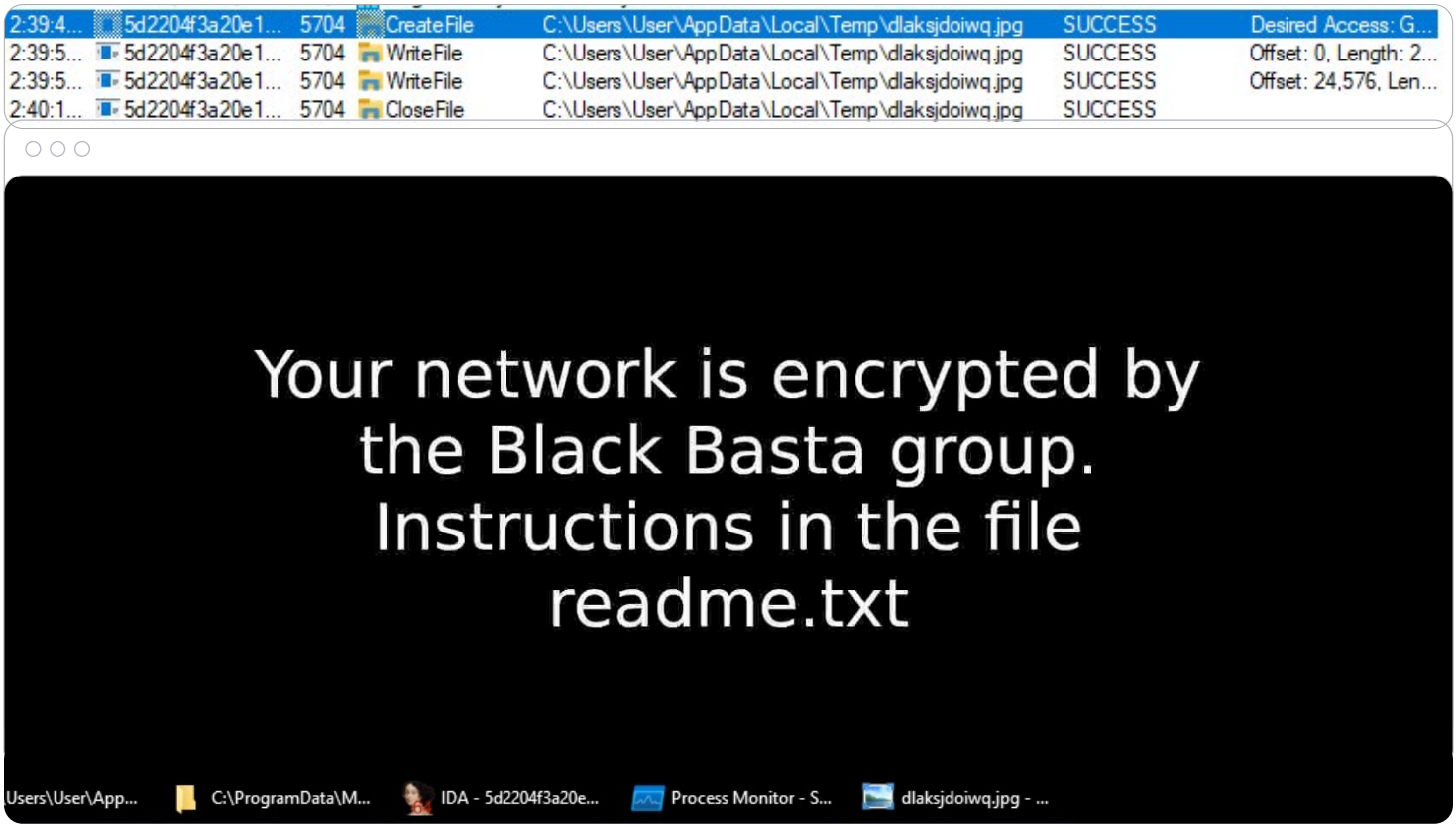
A new ransomware gang by the name of Black Basta started operations in April 2022, and in just a few weeks had breached at least 12 companies. In May, the group increased their activity. Based on ransom notes and information from the gang's data leak site, Black Basta not only encrypts data but also downloads it — an example of double-extortion tactics — giving the threat actors additional leverage in their demands for a ransom; if not paid, they may publish sensitive data online. As Black Basta doesn't advertise their existence, little is known about the group. There are some similarities with Conti ransomware, however.

Overview

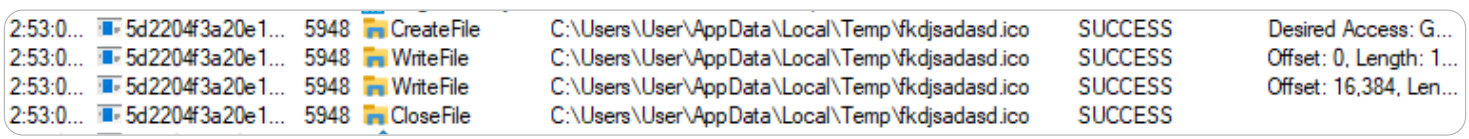
This Black Basta sample is a PE32 file and written in C++. It doesn't have any digital signature.

Before starting the file encryption process, Black Basta takes some preparatory steps. First, it creates and drops the file 'dlaksjdoiwq.jpg' to the '%Temp' folder. This file is a picture, which will change the victim's desktop background. To do this, the malware overwrites the path to the wallpaper in the registry.





Besides the new wallpaper, it drops one more file named 'fkdjsadasd.ico'. Black Basta then creates a new registry key 'HKCR\.basta\DefaultIcon' and writes a path to the file. This setting will change the icons for all files with a '.basta' extension.



```
00000000006301B8 push    offset aDefaulticon ; "\\DefaultIcon"
00000000006301BD push    offset aBasta_0 ; ".basta"
00000000006301C2 push    eax
00000000006301C3 call    sub_622E70
00000000006301C8 add     esp, 0Ch
00000000006301CB mov     byte ptr [ebp+var_4], 1
00000000006301CF lea     ecx, [ebp+dwDisposition]
00000000006301A5 cmp     [ebp+var_DC], 8
00000000006301AC lea     eax, [ebp+lpSubKey]
00000000006301B2 push    ecx             ; lpdwDisposition
00000000006301B3 cmovnb  eax, [ebp+lpSubKey]
00000000006301BA lea     ecx, [ebp+phkResult]
00000000006301C0 push    ecx             ; phkResult
00000000006301C1 push    0               ; lpSecurityAttributes
00000000006301C3 push    103h            ; samDesired
00000000006301C8 push    0               ; dwOptions
00000000006301CA push    0               ; lpClass
00000000006301CC push    0               ; Reserved
00000000006301CE push    eax             ; lpSubKey
00000000006301CF push    80000000h       ; hKey
00000000006301D4 call    ds:RegCreateKeyExW
00000000006301DA test    eax, eax
```

Names of these files are not generated randomly; they are stored in the memory.

```
.rdata:006911B0 aDlaksjdoiwqJpg:                ; DATA XREF: sub_62EAA0+2CD↑o
.rdata:006911B0                                 ; sub_62FCB0+5C↑o
.rdata:006911B0                 text "UTF-16LE", 'dlaksjdoiwq.jpg',0
.rdata:006911D0 aNtuserDat:                     ; DATA XREF: sub_62EAA0+2FC↑o
.rdata:006911D0                 text "UTF-16LE", 'NTUSER.DAT',0
.rdata:006911E6                 align 4
.rdata:006911E8 aFkdjsadasdIco:                 ; DATA XREF: sub_62EAA0+32B↑o
.rdata:006911E8                                 ; sub_62FB60+5C↑o
.rdata:006911E8                 text "UTF-16LE", 'fkdjsadasd.ico',0
```

Next, Black Basta opens the service 'Fax' and obtains control of it. Service hijacking is used to avoid detection by antivirus software. To do this, the ransomware must be executed by the administrator.

```
.text:00D2C924 push    10020h                   ; dwDesiredAccess
.text:00D2C929 cmovnb  eax, [ebp+lpServiceName]
.text:00D2C92D push    eax                      ; lpServiceName
.text:00D2C92E push    ecx
.text:00D2C92F mov     [ebp+var_268], e
.text:00D2C935 call    ds:OpenServiceW
.text:00D2C93B mov     edi, eax
.text:00D2C93D lea     ecx, [ebp+lpDisp
.text:00D2C943 lea     eax, [ebp+lpServ
.text:00D2C946 push    eax
.text:00D2C947 call    sub_D26BD0
.text:00D2C94C mov     byte ptr [ebp+va
```

```
[ebp+lpServiceName]=[debug010:008FF7E0]
db  46h ; F
db    0
db  61h ; a
db    0
db  78h ; x
db    0
db    0
db    0
```

```
.text:00D2C98C lea     eax, [ebp+ServiceStatus]
.text:00D2C992 push    eax                      ; lpServiceStatus
.text:00D2C993 push    1                        ; dwControl
.text:00D2C995 push    edi                      ; hService
.text:00D2C996 call    ds:ControlService
.text:00D2C99C mov     eax, [ebp+ServiceStatus.dwCurrentState]
```

After successfully obtaining control of this service, it copies its name and deletes it.

```
.text:00D2CB96 loc_D2CB96:                      ; CODE XREF:
.text:00D2CB96 push    edi                      ; hService
.text:00D2CB97 call    ds:DeleteService
```

Once the original service is deleted, Black Basta can create its own service with the same name. It may use other parameters in this process, but the main parameter of concern is 'lpBinaryPathName'. Black Basta assigns this value with its own pathname.

```
.text:00D2CC45 loc_D2CC45:                      ; CODE XREF: sub_D2C8E0+328↑j
.text:00D2CC45 cmp     [ebp+arg_30], 8
.text:00D2CC49 lea     edx, [ebp+lpBinaryPathName]
.text:00D2CC4C push    0                        ; lpPassword
.text:00D2CC4E cmovnb  edx, [ebp+lpBinaryPathName]
.text:00D2CC52 lea     ecx, [ebp+lpDisplayName]
.text:00D2CC58 cmp     dword ptr [ebp+var_218+4], 8
.text:00D2CC5F lea     eax, [ebp+lpServiceName]
.text:00D2CC62 push    0                        ; lpServiceStartName
.text:00D2CC64 cmovnb  ecx, [ebp+lpDisplayName]
.text:00D2CC6B cmp     [ebp+arg_18], 8
.text:00D2CC6F push    0                        ; lpDependencies
.text:00D2CC71 cmovnb  eax, [ebp+lpServiceName]
.text:00D2CC75 push    0                        ; lpdwTagId
.text:00D2CC77 push    0                        ; lpLoadOrderGroup
.text:00D2CC79 push    edx                      ; lpBinaryPathName
.text:00D2CC7A push    1                        ; dwErrorControl
.text:00D2CC7C push    2                        ; dwStartType
.text:00D2CC7E push    10h                      ; dwServiceType
.text:00D2CC80 push    0F01FFh                  ; dwDesiredAccess
.text:00D2CC85 push    ecx                      ; lpDisplayName
.text:00D2CC86 push    eax                      ; lpServiceName
.text:00D2CC87 push    [ebp+var_270]            ; hSCManager
.text:00D2CC8D call    ds:CreateServiceW
```

When a modified service is created, Black Basta will reboot the computer. After the system restarts, the malicious service will automatically execute the ransomware, which then proceeds to encrypt files.

```
.text:00D2C7F8 call    sub_D30280
.text:00D2C7FD add     esp, 18h
.text:00D2C800 push    edi                      ; nShowCmd
.text:00D2C801 push    edi                      ; lpDirectory
.text:00D2C802 push    offset Parameters        ; "/C shutdown -r -f -t 0"
.text:00D2C807 push    offset File              ; "cmd.exe"
.text:00D2C80C push    offset Operation         ; "open"
.text:00D2C811 push    edi                      ; hwnd
.text:00D2C812 call    ds:ShellExecuteA
.text:00D2C818 push    edi                      ; uExitCode
```

Black Basta also changes boot settings before rebooting the system, using the 'bcdedit.exe' utility to start the device in Safe Mode with Networking.

```
.text:00D2C73B push    eax                      ; int
.text:00D2C73C push    103h                     ; int
.text:00D2C741 push    edi                      ; int
.text:00D2C742 push    offset SubKey            ; "SYSTEM\\CurrentControlSet\\Control\\Saf"...
.text:00D2C747 push    80000002h                ; int
.text:00D2C74C call    ds:RegOpenKeyExW
.text:00D2C752 test    eax, eax
.text:00D2C754 jnz     loc_D2C843
.text:00D2C75A sub     esp, 18h
.text:00D2C75D mov     ecx, esp
.text:00D2C75F mov     [ebp+var_30], esp
.text:00D2C762 push    offset lpServiceName
.text:00D2C767 call    sub_D26BD0
.text:00D2C76C mov     [ebp+var_4], 2
.text:00D2C773 push    [ebp+phkResult]          ; hKey
.text:00D2C776 mov     [ebp+var_4], 0FFFFFFFFh
.text:00D2C77D call    sub_D2CEE0
.text:00D2C782 add     esp, 1Ch
.text:00D2C785 test    al, al
.text:00D2C787 jz      loc_D2C81E
.text:00D2C78D push    offset aBcdeditSetSafe   ; "bcdedit /set safeboot network"
.text:00D2C792 call    sub_D5DC04
.text:00D2C797 push    offset aCWindowsSystem   ; "C:\\Windows\\System32\\bcdedit.exe /set"...
.text:00D2C79C call    sub_D5DC04
.text:00D2C7A1 push    offset aCWindowsSysnat   ; "C:\\Windows\\SysNative\\bcdedit.exe /se"...
.text:00D2C7A6 call    sub_D5DC04
.text:00D2C7AB lea     eax, [ebp+var_28]
```

File encryption

Before starting the file encryption process, Black Basta deletes all shadow copies using the 'vssadmin.exe' utility to make system recovery impossible.

```
000000000062F6AF call    ds:GetCurrentProcessId
000000000062F6B5 mov     dword_6A9278, eax
000000000062F6BA call    ds:FreeConsole
000000000062F6C0 push    offset aCWindowsSysnat_0 ; "C:\\Windows\\SysNative\\vssadmin.exe de"...
000000000062F6C5 call    sub_65DC04
000000000062F6CA push    offset aCWindowsSystem_0 ; "C:\\Windows\\System32\\vssadmin.exe del"...
000000000062F6CF call    sub_65DC04
000000000062F6D4 mov     [ebp
000000000062F6DB mov     [ebp
000000000062F6E2 mov     [ebp+var_20], 0
000000000062F6E9 mov     [ebp+var_24], 0
000000000062F6F0 mov     [ebp+var_20], 0Fh
000000000062F6F7 mov     byte ptr [ebp+var_34], 0
```

```
aCWindowsSystem_0 db 'C:\Windows\System32\vssadmin.exe delete shadows /all /quiet',0
                                                ; DATA XREF: sub_62F650+7A↑o
```

Black Basta searches files with the 'FindFirstFile' and 'FindNextFile' functions and then encrypts them with the ChaCha20 algorithm.

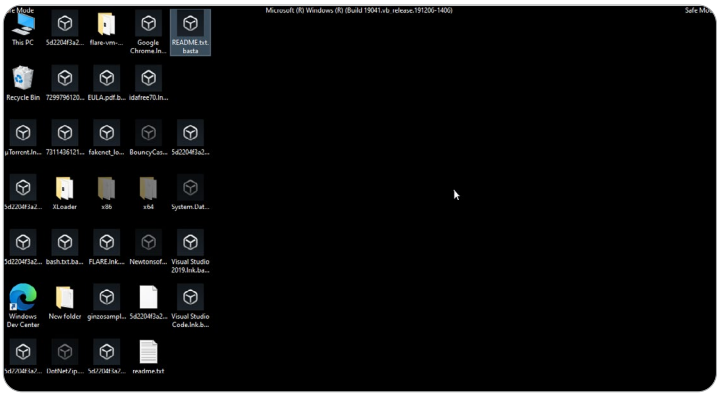
```
00000000006396E7 loc_6396E7:
00000000006396E7 add     ecx, [ebp+var_18]
00000000006396EA xor     ebx, ecx
00000000006396EC mov     edx, [ebp+var_1C]
00000000006396EF rol     ebx, 10h
00000000006396F2 add     edx, ebx
00000000006396F4 mov     esi, edx
00000000006396F6 xor     esi, [ebp+var_14]
00000000006396F9 rol     esi, 0Ch
00000000006396FC add     ecx, esi
00000000006396FE mov     [ebp+var_40], ecx
0000000000639701 xor     ecx, ebx
0000000000639703 mov     ebx, [ebp+var_34]
0000000000639706 rol     ecx, 8
0000000000639709 mov     [ebp+var_1C], ecx
000000000063970C add     ecx, edx
000000000063970E mov     edx, [ebp+var_4]
0000000000639711 mov     [ebp+var_48], ecx
0000000000639714 xor     ecx, esi
0000000000639716 rol     ecx, 7
0000000000639719 mov     [ebp+var_4C], ecx
000000000063971C mov     ecx, [ebp+var_10]
000000000063971F add     ecx, [ebp+var_20]
0000000000639722 xor     ebx, ecx
0000000000639724 rol     ebx, 10h
0000000000639727 add     edx, ebx
0000000000639729 mov     esi, edx
000000000063972B xor     esi, [ebp+var_10]
000000000063972E rol     esi, 0Ch
0000000000639731 add     ecx, esi
0000000000639733 mov     [ebp+var_34], ecx
0000000000639736 xor     ecx, ebx
0000000000639738 mov     ebx, [ebp+var_38]
```

The ChaCha20 encryption key will be encrypted with the RSA-4096 key embedded in the sample.

```
.rdata:00471550 aUagkcg5mzsQxxu db 'uaGKCG5Mzs/qXXuWAooBP4GHL60GR/Kld5rpSDwoarfCyGBQnKRzEQwJ+lxJY1BK6'
.rdata:00471550                                         ; DATA XREF: sub_40F650+1B6to
.rdata:00471550                 db 'ISgREm4SQAJWRLGzPfJOzp+lZFbnLcknd EUiOtEHgy/vpuCr2hzEzMnnmdOS5uNgi'
.rdata:00471550                 db 'sI/NmZYac3mqbKsA+kXKpFZ5MpdnFCLyYd/TqQ8DdGmdqQnDVCJWCfhrjq1KdogN9'
.rdata:00471550                 db 'mi1X1kyqoutquaT7QMNZsbVtaelokyBEBrjocYmtRFbv17zTjeEhi85BvAjtrqPJ'
.rdata:00471550                 db 'a8zYdHrIiWEDhPGUcjux7MpXeQqtDk6oLD+Q55Zy3uHJnc86sPaXCU8sAf5QY+Q1B'
.rdata:00471550                 db '84peV/LlN3Ejb1+MODp5tNbYgOvKyIe5KEBu0rA9wrPk+Bo6FOqSIG8uyfwadyNtk'
.rdata:00471550                 db '4rjl9uKAcjwTCjiLmnv5pSvG+tqp1SnQ3flYKgG+Wc8RSdNuCHMu4K6DCBsmcta3B'
.rdata:00471550                 db 'GLpQuMYE+QfN+7Wv9krtOs9pXFznTuIQmBVKh+QsijQV0R8+Q/t3ggK19cJNIQmgJ'
.rdata:00471550                 db 'oR3i8GTfegdBrY3/12PORhowEwSUFoYeUTOdvuS/zSwj6u+Tgk+BArJT2m8yPhVEY'
.rdata:00471550                 db 'xuroLOoIRMgBFH/ix0eHP3eLPMfwJsZv77+YCpboJhCCElDMQ2bXJJneOL26jc0xE'
.rdata:00471550                 db 's7kqaN6xqdEIffkMBcvccTTUDojADj7q0=',0
.rdata:004717FD                 align 10h
.rdata:00471800 aEncryption     db 'ENCRYPTION',0       ; DATA XREF: sub_40C5A0+2Ato
.rdata:0047180B                 align 4
```

After a file is encrypted, the ransomware will change its extension to '.basta'. Due to previous registry changes, the icon also will be changed.

```
0000000000621000 sub_621000 proc near
0000000000621000 push    6
0000000000621002 push    offset aBasta   ; ".basta"
0000000000621007 mov     ecx, offset aBasta_0 ; ".basta"
000000000062100C call    sub_633C90
0000000000621011 push    offset sub_685240
0000000000621016 call    sub_658777
000000000062101B pop     ecx
000000000062101C retn
```



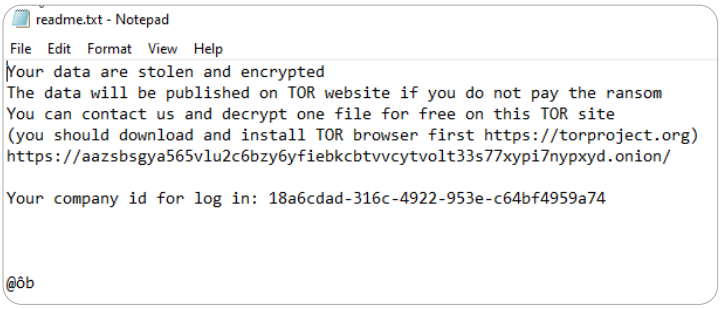
Obfuscation

Black Basta obfuscates its usage of WinAPI calls by loading a hash of the function in one of the registers.

```
.text:0062F4B3 mov     eax, [ecx]
.text:0062F4B5 mov     eax, [eax+8]
.text:0062F4B8 call    eax
.text:0062F4BA test    eax, eax
.text:0062F4BC jz      short loc_62F4C6
.text:0062F4BE mov     edx, [eax]
.text:0062F4C0 mov     ecx, eax
.text:0062F4C2 push    1
.text:0062F4C4 call    dword ptr [edx]
```

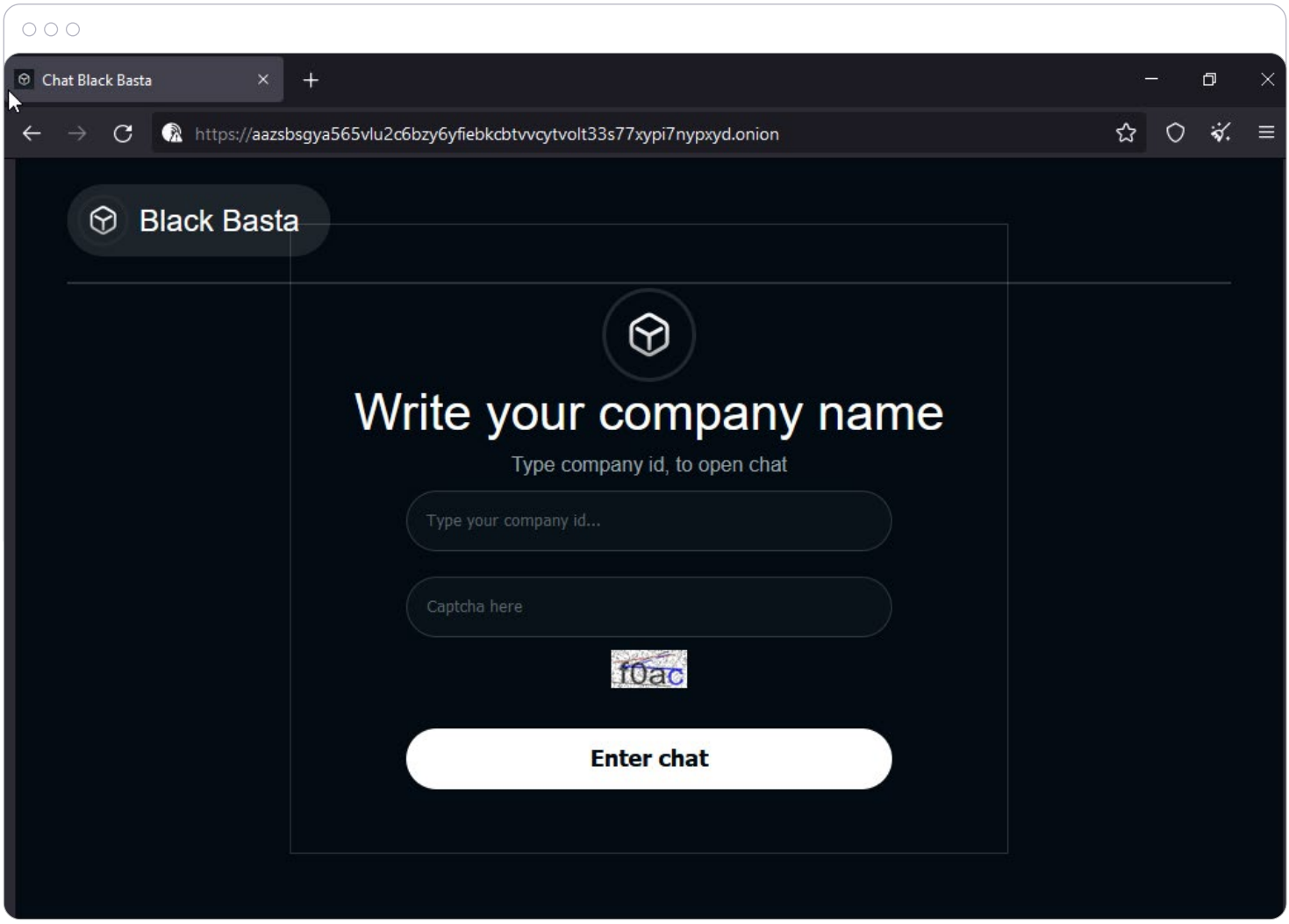
Ransom note

A ransom note named 'readme.txt' is dropped in each folder. This file contains a Tor browser link to the website and a victim ID.



Data leak site

On the data leak site, the victim must enter their ID (as specified in the ransom note) to open a chat with the threat actors.



Conclusion

Black Basta ransomware first appeared in April 2022, and quickly breached at least 12 companies. To encrypt victims' files, it uses ChaCha20 and RSA-4096 algorithms. Black Basta deletes all volume shadow copies, hijacks the 'Fax' system service and reboots the device in Safe Mode. That's why — if not detected and stopped — data will be lost and only can be recovered from a backup.

All of this makes it even more important to use the most effective anti-malware solutions possible. These solutions should be capable of identifying any cyberthreat, even those they've never seen before, so they can immediately shut the threat down before any harm can be done.

Malicious websites

An average of 8.3% of endpoints tried to access some malicious URLs in Q2 2022 — slightly down from 8.5% in Q1. In March, we observed a slight increase to 9%, which coincides with the spike of malicious emails that month.

The largest percentage of blocked malicious URLs on endpoints during June 2022 was in the United States, with 20.6%. This was followed by Canada with 9.8% and Italy with 9.0%.

We have observed more groups paying attention to the browser user-agent requesting the websites. Automated scanning tools that do not mimic normal users are served clean, decoy websites instead of the real payload. A similar fate occurs with solutions that replace URL arguments, like email addresses, for privacy reasons when they are passed to the website. Some kits have a checksum that can detect this change and serve a benign website instead. There was also a small increase in the known tactic of bait-and-switch scams, in which the URL in the email points to an initially clean website — but after a few hours, the website is switched to the final malicious payload, in the hope that any initial scan of the message would already have marked the link as safe.

Month	Percentage of users that clicked on malicious URLs
January	8.5
February	8.1
March	9
April	8
May	8.1
June	8.8

Top 10 countries with the most blocked URLs in June 2022

Rank	Country	Percent of blocked URLs in June 2022
1	United States	20.6
2	Canada	9.8
3	Italy	9
4	Germany	8.3
5	United Kingdom	6
6	Brazil	4.4
7	France	3.1
8	Japan	3
9	South Africa	2.7
10	Singapore	2.6

Similar to the malware detection statistics, we normalized the numbers depending on the total of active machines in each country with at least 10 blocked URLs. These normalized breakdowns per region can be found below.

Top ten countries: normalized malware detection numbers by region

Asia

Rank	Country	Regional normalized percent of blocked URLs in June 2022
1	Kuwait	26.2
2	Thailand	15.8
3	Saudi Arabia	14.6
4	Taiwan	14.1
5	Indonesia	12.9
6	United Arab Emirates	12.3
7	Malaysia	11.9
8	Philippines	10.9
9	Singapore	8.9
10	Japan	8.8

EMEA

Rank	Country	Regional normalized percent of blocked URLs in June 2022
1	South Africa	19.5
2	Ghana	18.8
3	Bosnia and Herzegovina	12.1
4	Bulgaria	11.8
5	Italy	11.6
6	North Macedonia	9.9
7	Slovakia	9.3
8	Poland	8.9
9	Luxembourg	8.1
10	Nigeria	7.9

Americas

Rank	Country	Regional normalized percent of blocked URLs in June 2022
1	Haiti	39.8
2	Costa Rica	18.6
3	Peru	16.2
4	Colombia	12.5
5	Panama	10.7
6	Dominican Republic	9.2
7	Brazil	8.3
8	Chile	7.9
9	United States	5.6
10	Argentina	5.3

Vulnerabilities in Windows OS and software

Microsoft Patch Tuesdays

The beginning of 2022 was pretty impressive for Microsoft in terms of security patches. In January, the company released 96 security-related fixes, including updates to address six zero-day vulnerabilities. Among them, Microsoft has fixed problems including remote code execution (RCE) exploits, privilege escalation flaws, spoofing issues, and cross-site scripting (XSS) vulnerabilities. Patched flaws affected Microsoft Exchange Server, the Office product suite, Windows Defender, Windows Kernel, RDP, Cryptographic Services, Windows Certificates and Microsoft Teams. According to Microsoft, none of the zero-day flaws above are known to have been exploited in the wild.

Microsoft greatly boosted security for their Edge browser: 24 vulnerabilities were patched. January is usually a much calmer month for vulnerability fixes, but not this time.

Microsoft's February Patch Tuesday included fixes for a total of 48 bugs, including one patch for a zero-day vulnerability. While none of this month's patches are considered "critical" in severity, the zero-day bug had a CVSS rating of 7.8 out of 10, and can be exploited to escalate privileges via the kernel. The zero-day vulnerability was not assigned a critical rating because the attacker must take additional actions in order to exploit the vulnerability.

Microsoft's March Patch Tuesday brought a total of 71 security fixes to Windows and other Microsoft products, including three zero-day vulnerabilities, and three critical bugs. All three zero-day vulnerabilities were rated "important" by Microsoft and included remote code execution vulnerabilities in .NET, Visual Studio and Remote Desktop Client. The largest Microsoft Patch Tuesday in nearly 18 months was during April 2022, with 128 vulnerability patches — the largest number of patches since September 2020. Two of the patches fixed zero-day vulnerabilities that were already widely known; ten were considered critical; and 115 were considered important. The two zero-day vulnerabilities were both related to the escalation of privilege, giving attackers with basic access the potential ability to elevate their privileges to those of an administrator.

Microsoft's May 2022 Patch Tuesday brought fixes for three zero-day vulnerabilities, one of which had been actively exploited, and a total of 75 flaws. Of these, eight were classified as "critical" as they allow remote code execution or elevation of privileges. The actively exploited zero-day vulnerability fixed is for a new NTLM relay attack using an LSARPC flaw tracked as "CVE-2022-26925 — Windows LSA Spoofing Vulnerability". Using this attack, threat actors can intercept legitimate authentication requests and use them to gain elevated privileges — even going so far as to assume the identity of a domain controller.

Once again, we would like to stress that patching is very important if you want to protect yourself or your business. As recently as June, another way of utilizing Microsoft Office documents to commence an attack was discovered. The new vulnerability CVE-2022 30190 (Follina) allows an attacker to create a Word document that will execute malicious code through the MSDT protocol when the user opens the document in Preview mode. The method is gaining in popularity, as it allows attackers to deploy malware without the need for macros. Even a nation-state APT group has now been seen using this vulnerability against targets in Tibet.

Apart from malicious emails, exploiting unpatched vulnerabilities of exposed services is another common infection vector. In particular, ransomware authors exploited unpatched Exchange servers and the Log4j vulnerability to gain a foothold into corporations.

Google, Adobe and others' patching activities

Google issued a lot of important security updates in the first half of 2022. The company released Chrome 99.0.4844.51 for macOS, Linux and Windows, including 28 security patches for the browser. Google has released information on the 21 publicly submitted vulnerabilities, while internally discovered bugs have been kept undisclosed until users have an opportunity to update to the latest version of the browser. Of the released vulnerabilities, nine are considered high severity. A use-after-free vulnerability in MediaStream took the top payout, earning the researcher $15,000, while many of the other vulnerabilities had payouts in the thousands of dollars — for buffer overflow, out-of-bounds memory, and additional use-after-free vulnerabilities, among others.

Later on, Google issued an update for its Chrome browser that patched the second high-severity zero-day vulnerability this year, and they highly recommended that all 3.2 billion Chrome users update to Chrome 99.0.4844.84 for Windows, macOS or Linux immediately. The patch included in this release fixed a remote code execution vulnerability that was already being exploited in the wild. The vulnerability is being tracked as CVE-2022-1096 and is caused by a confusion weakness in the Chrome V8 JavaScript engine.

After that, we had an emergency update (Chrome 98.0.4758.102) for the Chrome browser on Windows, macOS and Linux, fixing seven high-severity vulnerabilities. Vulnerability CVE-2022-0609 has already been actively exploited in the wild, making it the first Chrome zero-day vulnerability for this year.

Google wasn't the only company to patch a popular browser — Mozilla also released Firefox 97.0.2, which included fixes for two critical use-after-free vulnerabilities that were actively being exploited, allowing attackers to run unauthorized commands on a victim's system.

Adobe was active in January, releasing five patches addressing 41 CVEs in Acrobat and Reader, Illustrator, Adobe Bridge, InCopy and InDesign. The update for Acrobat and Reader fixed a total of 26 bugs, the worst of which could lead to remote code execution (RCE) if a user opened a specially crafted PDF. The patch for InDesign corrected two critical-rated out-of-bounds (OOB) write bugs that could lead to code execution, plus a moderate use-after-free privilege escalation. The others were a mix of privilege escalations and memory leaks.

For February, Adobe released five bulletins addressing 17 CVEs in Adobe Illustrator, Creative Cloud Desktop, After Effects, Photoshop and Premiere Rush. The update for Illustrator fixed a total of 13 bugs, the most severe of which could allow arbitrary code execution through either a buffer overflow or an OOB write. The fix for After Effects addressed an OOB write bug that exists within the parsing of 3GP files.

The issue resulted from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. The final critical-rated patch from Adobe in February fixed a buffer overflow in Photoshop that could allow arbitrary code execution.

The Adobe release for March was quite small. Adobe released only three patches addressing six CVEs in Adobe Photoshop, Illustrator and After Effects. The patch for After Effects fixed four critical-rated, stacked-based buffer overflows that could result in arbitrary code execution. The fix for Illustrator was also rated critical. It addressed a single buffer overflow that could lead to arbitrary code execution. Last but not least, the update for Photoshop fixed a single "important"-rated memory leak.

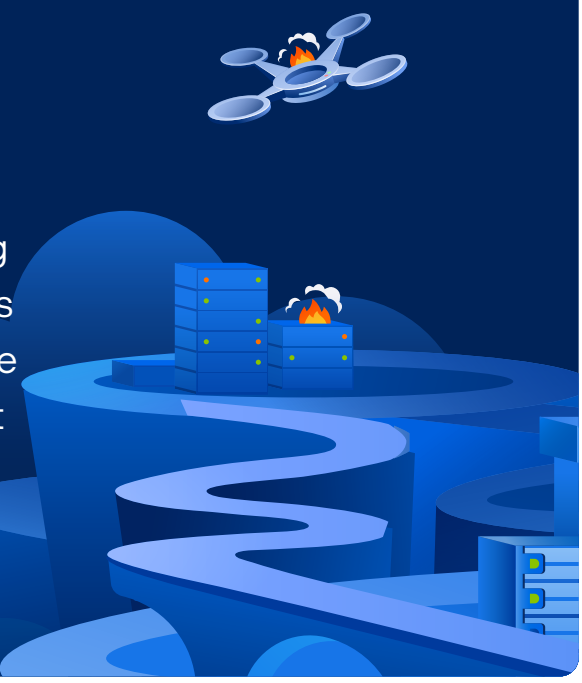
For April, Adobe released four updates addressing a whopping 70 CVEs in Acrobat and Reader, Photoshop, After Effects and Adobe Commerce. The update for Acrobat and Reader was by far the largest, with 62 CVEs being addressed. The more severe vulnerabilities fixed are the critical-rated use-after-free and OOB write bugs. These could allow an attacker to execute code on a target system if they can convince a user to open a specially crafted PDF document. There were 13 CVEs fixed in the patch for Photoshop. All the vulnerabilities addressed by this patch involved critical-rated code execution bugs.

For May, Adobe released five bulletins addressing 18 CVEs in Adobe ColdFusion, InCopy, Framemaker, InDesign and Adobe Character Animator. The largest of these patches was the fix for Framemaker, with 10 CVEs in total. Nine of these are critical-rated bugs that could lead to code execution, mostly due to OOB write vulnerabilities. The patch for InDesign addressed three critical-rated bugs that could lead to code execution.

According to CISA, there were 475 vulnerabilities reported in the first half of 2022, which were exploited widely in the wild. That's a full 4% of all 12,985 reported vulnerabilities listed in VulDB, and represents an average of 79 new exploits per month. According to a research statistic by Google's Project Zero team, half of exploited zero-day vulnerabilities are just variations of previous threats. These could have been prevented if the initial software patch had more adequately addressed the root cause of the issues.

To summarize: we saw a lot of vulnerabilities being used by cybercriminals and discovered by researchers. And the number is only growing compared to last year. Many ransomware groups are exploiting vulnerabilities in order to breach their targets. This situation emphasizes the need for comprehensive vulnerability assessment and patch management solutions with exploit prevention functionality in place. Without such capabilities, the chances of becoming a victim are very high.

To summarize:
We saw a lot of vulnerabilities being used by cybercriminals and discovered by researchers. And the number is only growing compared to last year. Many ransomware groups are exploiting vulnerabilities in order to breach their targets. This situation emphasizes the need for comprehensive vulnerability assessment and patch management solutions with exploit prevention functionality in place. Without such capabilities, the chances of becoming a victim are very high.



Acronis' recommendations to stay safe in the current and future threat environment

Modern cyberattacks, data leaks, and ransomware outbreaks all reveal the same thing: traditional cybersecurity is failing. This failure is the result of weak technologies and human mistakes caused by clever social engineering. In cases where a backup solution was working well and wasn't compromised, it usually takes hours and days to restore systems (with data) to an operational state. Backup is essential for when cybersecurity solutions fail, but at the same time, backup solutions can be compromised or disabled, and may perform slowly, causing businesses to lose a lot of money due to downtime.

To solve these problems, we recommend an integrated cyber protection solution like Acronis Cyber Protect Cloud that combines anti-malware, EDR, DLP, email security, vulnerability assessment, patch management, RMM and backup capabilities into a single agent. This integration lets you maintain optimal performance, eliminate compatibility issues and ensure rapid recovery: if a threat is missed or detected while your data is being altered, the data will be restored from a backup immediately. That's the power of integration.

This approach isn't possible for those using separate agents for anti-malware protection and backup capabilities. Your anti-malware solution may stop the threat, but some data may already be lost. Your backup agent won't know about this automatically, and data will be restored slowly — if at all.

Of course, Acronis Cyber Protect Cloud strives to make data recovery unnecessary by detecting and eliminating threats before they can damage your environment. This is achieved with our enhanced, multilayered cybersecurity functionality.

That said, even those using modern solutions shouldn't forget about basic security rules.

Patch your OS and apps

This is crucial, as a lot of attacks succeed due to unpatched vulnerabilities. With a solution like Acronis Cyber Protect, you're covered with embedded vulnerability assessment and patch management functionalities. We track all discovered vulnerabilities and released patches and allow admins or technicians to easily patch all endpoints with a flexible configuration and detailed reporting. Acronis Cyber Protect supports not only all embedded Windows apps but also 300 popular third-party apps, including telecommunications tools like Zoom and Slack, and popular VPN clients used in remote work. Be sure to patch high-severity vulnerabilities first and follow the success report to check that patches were applied properly.

If you don't use software with patch management capabilities, keeping your applications up to date is much harder. At the very least, you need to be sure that Windows gets all updates it needs and that they are installed promptly — users tend to ignore system messages, especially when Windows asks for a restart. This is a big mistake. Be sure that auto-updates to popular software vendors like Adobe are enabled, and apps like PDF Reader are also updated promptly.

Be prepared for phishing attempts, and don't click on suspicious links

Phishing messages and malicious websites appear in large numbers every day. These websites are sometimes filtered out on a browser level, but with cyber protection solutions like Acronis Cyber Protect, you also gain dedicated URL filtering functionality. As a general rule, don't click on links you don't need to click — or that you didn't expect to receive.

Phishing or malicious-themed attachments can come through email — the same as the malicious links covered above. Regarding attachments: always check where they really come from and ask yourself if you're expecting them or not. In any case, before you open an attachment, it should be scanned by your anti-malware solution.

Use a VPN while working with business data

No matter whether you're connecting to remote company sources and services or just casually browsing the web, use a virtual private network (VPN). If you have a VPN procedure in your company, you'll most likely get instructions from your admin or MSP technician. If you have to secure your workplace yourself, use well-known recommended VPN apps and services, widely available in software marketplaces or directly from vendors. A VPN encrypts all your traffic, making it secure in case an attacker attempts to capture your data in transit.

Be sure your cybersecurity is running properly

Acronis Cyber Protect uses many well-balanced and tuned security technologies, including multiple detection engines. We recommend using it instead of an embedded OS-native solution.

But just having anti-malware defenses in place is not enough; they must be configured properly.

This means that ↘

- A full scan should be performed at least every day.
- The product should look for and retrieve updates on a regular basis — ideally daily or hourly.
- The product should be connected to its cloud detection mechanisms, as is the case with Acronis Cyber Protect and its connection to the Acronis Cloud Brain. Ensure that reliable internet access is available and does not accidentally block anti-malware software.
- On-demand and on-access (real-time) scans should be enabled and react on every new software installation or execution.

Additionally, don't ignore messages coming from your anti-malware solution — read them carefully and act accordingly. Always ensure that your license is legitimate.

Keep your passwords and your working space to yourself

Make sure that your passwords (and those of your employees, if applicable) are strong and private. Never share passwords with anyone, and use different and long passwords for every service. To help you remember them, use password manager software. Alternately, the easiest way to create strong passwords is to create a set of long phrases you can remember. Eight-character passwords are easily brute-forced nowadays. Where possible, use multifactor authentication.

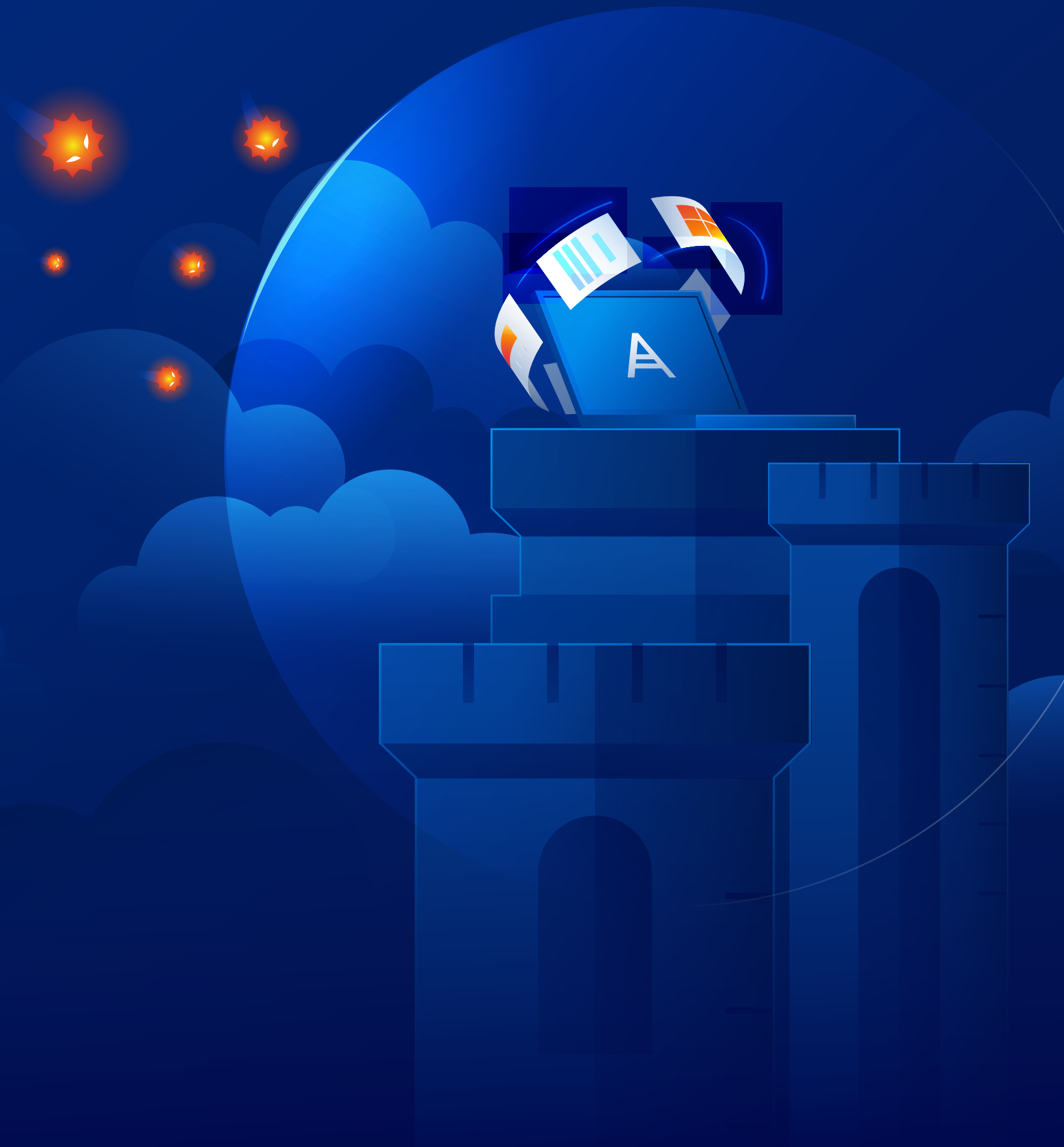
Even when working from home, do not forget to lock your laptop or desktop system and limit access to it. In many cases, people can simply steal sensitive information off an unlocked computer — even from a distance.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment — from cloud to hybrid to on premises — at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

Acronis



Learn more at
www.acronis.com