Acronis

Acronis Cyber Protection Operation Center Report:

Cyberthreats in the second half of 2022 – Data under attack

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 Artioli

Cyber Protection Evangelist,
Acronis

Introduction and summary

Acronis was the first company to start implementing complete, integrated cyber protection to protect all data, applications and systems. Cyber protection requires active researching and monitoring of threats, as well as abiding by the five vectors of "SAPAS" — safety, accessibility, privacy, authenticity, and security. As part of the strategy, we've established four Cyber Protection Operation Centers 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 was a leader in the data protection market with its innovative Acronis Active Protection anti-ransomware technology, which evolved over time to demonstrate the company's unique expertise at stopping threats aiming at data. However, it's important to note that the artificial intelligence (AI)- and behavior-based detection technologies that Acronis 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 in the second half of 2022. General malware data presented in the report was gathered from July–November of this year, and reflects threats targeting endpoints that we observed in these months.

This report represents a global outlook, and is based on data from over 750,000 unique endpoints distributed around the world. Most of the statistics discussed focus on threats for Windows operating systems, as they are much more prevalent than macOS and Linux.

The top five numbers of this report:

- The most-attacked countries (in terms of malware per user) in Q3 2022 were South Korea, Jordan and China.
- Around 40 million URLs were blocked on the endpoint by Acronis from July–November 2022, with a significant increase over summer months figures in the last two months.
- 30.6% of all received emails were spam and 1.6% contained malware or phishing links.
- The average cost of a data breach is expected to reach $5 million in 2023.
- An average of 7.7% of endpoints tried to access some malicious URLs in Q3 2022, slightly reduced from 8.3% in Q2.

Among the cybersecurity trends we saw in the second half of 2022:

- Ransomware continues to be the number-one threat to big 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.

- 475 out of 12,985 reported vulnerabilities were being actively exploited in the first half of 2022.

- Between July and October 2022, the proportion of phishing attacks has risen by 1.3x, now representing 76% of all attacks (up from 58% in H1 2022).

What you will find in this report:

- The top security/threat trends we observed in the second half of 2022

- Why we see more and more data breaches

- General malware statistics and key families reviewed

- Ransomware statistics, with deep-dive analyses of some of the most dangerous threats

- Which vulnerabilities contribute to the success of attacks

- Our security recommendations

- Our security forecast for 2023

Key cyberthreats and trends for the second half of 2022

1. Ransomware volume is down, but the threat is bigger than ever

Unfortunately, the ransomware threat continues to worsen. Although we see lower numbers of attacks, samples and new families, the existing families are doing very well for the cybercriminals that operate them. Each month in the second half on this year, ransomware gangs were adding 200–300 new victims to their combined list. By the end of Q3, the total number of compromised targets published for the main operators were as follows:

> ↘ **LockBit: 1157**
> ↘ **Hive: 192**
> ↘ **BlackCat: 177**
> ↘ **Black Basta: 89**

While some families, or rather "ransomware brands," left the scene — such as as Egregor, REvil, BlackMatter and DoppelPaymer — the people behind them simply rebranded and began new operations. This tactic allows them to avoid law enforcement (or at least slow down their progress) and can buy additional months, if not years, of successful criminal activity.

We've seen examples of this before: WastedLocker reappeared as Hades ransomware or Cryptolocker, later changing to PayloadBin and Macaw during autumn. DarkSide ransomware was rebranded to DarkSide 2.0, and then again to BlackMatter. Earlier this year, the BlackCat ransomware gang confirmed that they are former members of the DarkSide/BlackMatter operation.

While law enforcement had some big success stories in 2022 in their fight with ransomware operators, cybercriminals are still winning. The Dutch National Police, in collaboration with cybersecurity firm Responders.NU, tricked the DeadBolt ransomware gang into handing over 155 decryption keys by faking ransom payments. Unfortunately, after realizing they were tricked and won't get paid, the DeadBolt gang switched up their tactics, and now require double confirmation before releasing decryption keys.

The big win of the "light side" was the recent arrest of a Russian national LockBit member in Canada, who was responsible for making ransom demands. However,

according to Europol he is likely an affiliate rather than a manager of the whole cybercrime operation. The main actors are still out there doing harm.

The big four of the ransomware world in 2022

As we already mentioned above, the market of ransomware operators actually dominated by 4-5 players only. The four most-active in 2022 were LockBit, Black Basta, Hive and BlackCat.

Of course, other players are still around, just causing much less damage. Groups like STOP, Inlock, Dharma, Xorist, Venus, Cuba, Pendragon, Chaos, Killnet, Zeppelin, and others still actively release new samples and infect users as well.

Let's take a look at some cases that were caused by the main threats actors in the ransomware space:

LockBit 3.0

LockBit is one of the most advanced ransomware families on the scene. It employs heavy anti-debugging, anti-detection mechanisms, and can disable Windows Defender and deletes backups. In September 2022, a leaked LockBit 3.0 builder was posted on Twitter. Group spokesman "LockBitSupp" alleged that the gang was not hacked, instead blaming a former developer for the leak. In any case, we expect to see the consequences of this incident later on, as other groups utilize the leaked code to weaponize their own attacks.

At the same time, unfortunately, we must say that LockBit operators are doing very well for themselves. They are by far leading the market — taking as much as 40-50% of it, according to various experts' estimations — and they continue to add more and more high profile victims to their list.

In July, LockBit hit the FAAC (Fabbrica Automatismi Apertura Cancelli) group, whose consolidated sales tally more than €600 million within 53 companies on five continents, and who employ over 3,600 individuals across the globe. This was followed by an attack on La Poste Mobile, which has 2,740 employees and an annual revenue of over $513 million.

LockBit continued with the Canadian town of St. Marys, Ontario with 7,500 residents, and the town of Frederick,

Colorado, with a population of 15,000 people. The group demanded a ransom of $200,000 in order to not publish the stolen data.

IHG, which currently operates 6,028 hotels in more than 100 countries, has suffered a cyberattack. It is unknown who's behind this attack, but recently the Lockbit ransomware gang claimed an attack on Holiday Inn Istanbul Kadıköy.

Japanese tech company Oomiya was hit as well. Oomiya has an annual revenue of $50 million and around 500 employees. The business is focused on designing and manufacturing microelectronics and facility system equipment. This incident could have a significant impact on third-party organizations, because Oomiya is in the supply chain of major organizations worldwide in multiple industries, including manufacturing, semiconductors, automotive, communications and healthcare.

The Bank of Brasilia (BRB) was asked for about 50 Bitcoins not to leak what was accessed to the public. Pendragon Group, which has more than 200 car dealerships in the U.K. and an annual revenue of over $ 3.9 billion, was asked for $60 million to decrypt the files and keep them private. Pendragon notified U.K. authorities about the incident, and the report has been transferred to law enforcement agencies for investigation. Interestingly, LockBit attacked them when Sweden-based company Hedin Mobility Group offered to acquire Pendragon for over $450 million.

Black Basta

Black Basta appeared around April of 2022, as we've previously reported, and was formed by former members of the Conti and REvil ransomware gangs — with which it shares similar tactics, techniques and procedures. Just recently, security researchers at SentinelLabs have uncovered evidence that links the Black Basta ransomware gang to the financially motivated hacking group FIN7, also known as "Carbanak." We will see how this develops, but Black Basta already managed to make some big hits.

The Knauf Group, with annual revenue of over $11 billion, has fallen victim to Black Basta. Knauf is a leading manufacturer of construction materials, and employs more than 35,000 people and operates 150 production sites worldwide.

In November, Canadian food retail giant Sobeys was hit over the weekend. The chain employs over 134,000 workers serving 1,500 grocery shops and pharmacies across all 10 Canadian provinces. Sobeys is one of only two major grocery merchants in the country, operating under the Sobeys, Safeway, IGA, Foodland, FreshCo, Thrifty Foods and Lawtons Drugs retail banners. Black Basta ransomware encrypted Sobeys' computers, and at the time of this report's publication, the attackers were engaged in negotiation with company representatives.

Hive

The Hive ransomware gang also scored big. Among their recent victims was Tata Power, India's largest power generation company, which serves more than 12 million customers through its distributors and has revenue of over $5 billion. Hive's operators posted the stolen data on their leak website; files included contracts, financial and business documents, engineering projects, and employees' personally identifiable information (PII) such as Aadhaar card numbers. Additionally, the data dump contains engineering drawings, financial and banking records, as well as client information.

Before that, Hive added Eurocell to its victims list, demanding $6 million. Eurocell is a building products distributor from the UK with an annual revenue of $420 million.

Hive ransomware also hit the systems of Bell Canada subsidiary Bell Technical Solutions (BTS). BTS is an independent subsidiary with more than 4,500 employees, specializing in installing Bell services across the Ontario and Québec provinces.

Damart, a French clothing company with over 130 stores across the world, has been hit as well with an attack that impacted 92 stores. Hive operators demanded a ransom of $2 million.

BlackCat/ALPHV

The BlackCat group is known for its triple extortion tactics, in which after the theft of company data, the victim is threatened with leaks and with a threat of a distributed denial of service (DDoS) attack if the demands are not met. BlackCat had a variety of big targets in the second half of 2022.

They claim to have stolen more than 150 GB from European gas pipeline operator Creos Luxembourg S.A. The company has an annual revenue of €290 million and over 800 employees.

The famous Japanese video game company Bandai Namco, known for publishing numerous video games including Elden Ring, Pac-Man and Tekken, was hit as well. The company has an annual revenue of around $7.3 billion.

BlackCat/ALPHV ransomware was behind an attack on the Italian energy services organization Gestore dei Servizi Energetici SpA (GSE); cybercriminals exfiltrated approximately 700 GB of data from their IT infrastructure.

Record TV, the second-largest TV station in Brazil, SBT and TV Cultura suffered a cyberattack recently. It's still unclear whether these actions were coordinated, but ransomware was involved — and BlackCat is suspected to be responsible. This incident impacted the internal network, telephone services, mail and transmission of local TV channels. The broadcasters have not issued a public comment, but they did have to suspend the transmission of live programming.

Other notable cases

Of course, other groups were active as well, compromising large and medium-sized businesses around the globe.

German electronics manufacturer Semikron was hit by the LV ransomware group. Semikron has over 3,000 employees in 24 global offices, and an annual revenue of $460 million.

Argentina's Judiciary of Córdoba fell victim to the PLAY ransomware group. It is unknown exactly how PLAY breached the judiciary's network, but a list of employees' email addresses was leaked in March as part of the Lapsus$ breach of Globant.

The Clop ransomware gang claims to have stolen 5 TB of data from South Staffs Water, an organization with an annual revenue of $335 million and which supplies 330 million liters of drinking water to 1.6 million consumers daily.

Greece's largest natural gas distributor, DESFA — which has an annual revenue of €270 million — confirmed that they suffered a limited-scope data breach and IT system outage following a cyberattack by the Ragnar Locker ransomware. The Ragnar Locker gang also claimed credit for an attack on TAP Air Portugal. The gang posted a new entry on their data leak site that contains personal information of more than 9,000 customers.

Cybercrime group RansomHouse claims to have compromised eight Italian districts and published the entire 2.1 TB of data exfiltrated from the IT infrastructures of the union of Tuscan municipalities, in the metropolitan city of Florence. In the message, RansomHouse announced that their attacks against government infrastructure in Italy were taking advantage of weak password practices, such as the use of "12345678" to secure sensitive data.

The Center Hospitalier Sud Francilien (CHSF), a 1000-bed hospital located 28 km from the center of Paris, suffered a cyberattack. The medical center, which serves an area of 600,000 residents, was forced to refer patients to other establishments and postpone appointments for surgeries. Attackers demanded a $10 million ransom in exchange for the decryption key.

The RansomEXX ransomware gang has claimed responsibility for a cyberattack against Bombardier Recreational Products (BRP), disclosed by the company on August 8, 2022. BRP employs over 20,000 people, counts close to $6 billion in annual sales, and distributes various products in more than 120 countries. RansomEXX listed Bombardier Recreational Products on its leak site along with almost 30 GB of files allegedly stolen from the firm. These files include non-disclosure agreements, passports and IDs, material supply agreements, contract renewals and more. In the statement, the company presented the first results of its internal investigation, saying that the attackers breached its systems via a supply-chain attack.

The Consorci Sanitari Integral (CSI) was another victim of RansomEXX. The incident affected all the organization's healthcare centers in Barcelona and Baix Llobregat, leaving workers without access to patient information or procedures. The CSI is a public entity with about 3,500

employees, and is owned by the Department of Health, the municipalities of Sant Joan Despí and l'Hospitalet de Llobregat, the Consell Comarcal del Baix Llobregat and the Creu Roja. It includes 13 centers, which serve patients in public health and primary care, hospitals, and social health centers (two residences); the CSI also manages the dependency and disability assessment services in Barcelona and l'Hospitalet. Management of the health group hasn't provided any further details, but the economic impact of this incident is greater than that of drug trafficking.

The Vice Society ransomware gang claims to have stolen more than 500 GB from the Los Angeles Unified School District (LAUSD). The district enrolls more than 640,000 students.

The Everest ransomware group claims to have access to all of the servers of South African public utility Eskom

Hld SOC Ltd. Attackers demanded $200,000 (payable in Bitcoin or Monero) for the package, which includes servers with administrator, root, and sysadmin passwords for Linux and Windows servers. Eskom is a state-owned electricity company, and provides more than 90% of the energy to customers in South Africa and the Southern African Development Community (SADC) region. Everest's operators had previously announced the sale of "South Africa Electricity company's root access" for $125,000 in March 2022, but at that time Eskom denied any security breach had occurred. When the Everest group posted again recently about a breach of Eskom, security experts noted that the utility was experiencing some server issues.

And because we simply cannot go by without talking about the elephant in the room, Cisco recently announced that its infrastructure was breached by the Yanluowang ransomware gang. The ensuing investigation revealed that nothing was taken nor leaked.

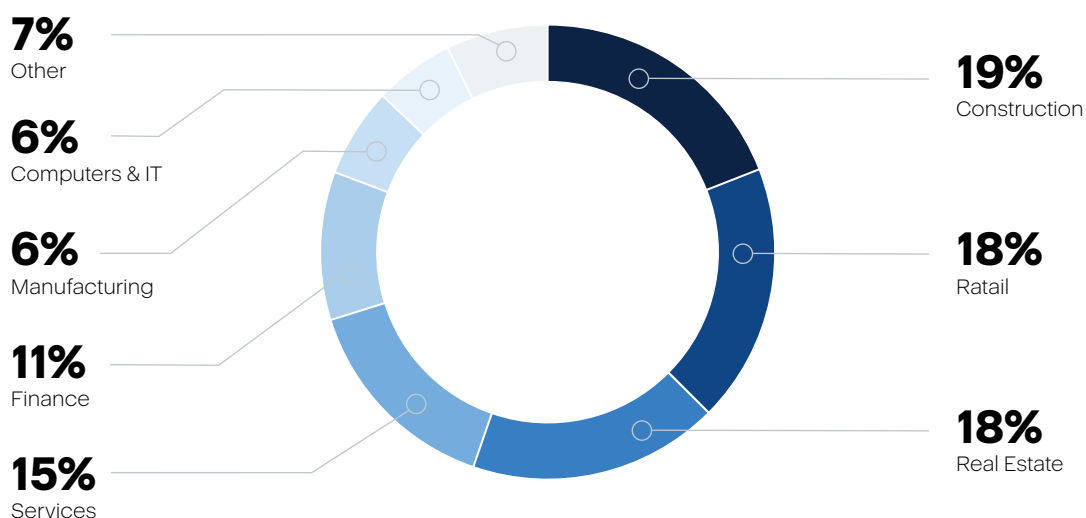# 2. Phishing and malicious emails remain the main vector of infection

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

During the period in question, we saw a significant growth in the amount of email-borne threats. The rate of malicious messages rose by 0.6 points in just 4 months

(a 60% increase). Spam rates have also increased in the same period — by over 15% — and now constitute 30.6% of all inbound traffic. It's worth noting that Acronis customers are more prone to spam attacks in comparison to Perception Point's benchmark of other customers, where they recorded spam rates of 19.3%. This is not the end though: we expect to see another rise in December due to the holiday season.

No one is safe — email-borne attacks are targeting virtually all industries. But analysis of the top 50 most-attacked organizations suggests that the following industries are at particular risk:

↘ **Construction**   ↘ **Professional services, including IT**

↘ **Retail**   ↘ **Finance**

↘ **Real estate**

7% Other

6% Computers & IT

6% Manufacturing

11% Finance

15% Services

19% Construction

18% Ratail

18% Real Estate

Most attacked industries from July to November 2022

Phishing — including specialized forms like spear phishing and whaling — continues to be the top threat facing organizations. Between July and November 2022, phishing activity rose by 130%; it now represents 76% of all email-based attacks (up from 58% in H1 2022). With this rise, the percentage of malware-delivering email attacks has fallen accordingly. Social engineering threats also saw an uptick in the last 4 months, and now account for 3% of all attacks (compared to 2% in our previous report).

Phishing — including specialized forms like spear phishing and whaling — continues to be the top threat facing organizations. Between July and November 2022, phishing activity rose by 130%; it now represents 76% of all email-based attacks (up from 58% in H1 2022). With this rise, the percentage of malware-delivering email attacks has fallen accordingly. Social engineering threats also saw an uptick in the last four months, and now account for 3% of all attacks (compared to 2% in our previous report).

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
July	5,619,052
August	7,096,120
September	4,785,525
October	13,025,443
November	15,202,217

3%
BEC

3%
Advanced Attack

18%
Malware

76%
Phishing

Phishing and malicious ratios, over time (Excluding spam)

The Acronis CPOCs blocked 17,500,697 phishing and malicious URLs in Q3 2022. This is 17% fewer than in Q2 (21,150,710) and 8% fewer than in Q1 (19,151,211).
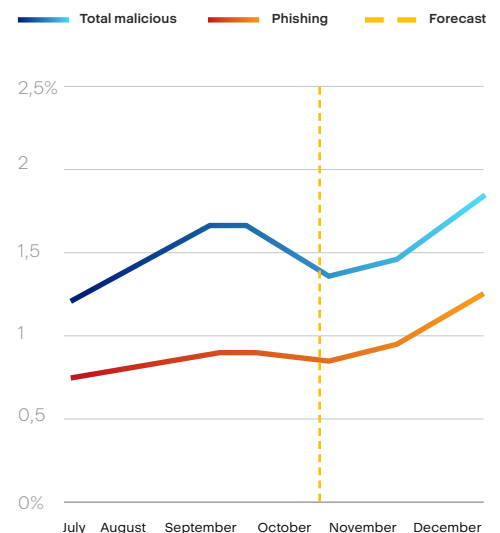
Unfortunately, many emails with malicious content — especially URLs — still get through basic email filters and reach users' endpoints. The malicious attachments often feature multiple layers as well, such as password-protected ZIP archives containing LNK files that download the final payload. This is another reason why it is important to have a multi-layered defense approach.

- 229k malicious events were observed during October
- 128k of them were phishing

As phishing constitutes a significant chunk of the overall number of attacks, it alters the trend of malicious rates over the year. Based on our analysis, after taking into consideration seasonality (e.g., the upcoming holidays) we expect to see an additional rise in attack rates towards December — reaching a yearly peak of over 2% of all traffic.

In order to bypass security measures, attackers are trying to conceal the malicious payloads within the files. Thanks to Recursive Unpacker functionality — the anti-evasion layer in the platform — we identified over 235,000 malicious events that were hidden in sub files and URLs. This constitutes six out of 10 attacks identified by the platform. A deep dive into the concealed attacks shows that this technique is mainly used to hide phishing threats, which account for 40% of all attempted attacks.

60%
Sub

40%
Root

39%
Phishing

18%
Malware

3%
Advanced attacks

Big cases and phishing trends

Phishing continues to be one of cybercriminals' favorite tools to penetrate systems. Let's take a look at some big cases discovered by Acronis and other cybersecurity reserchers between July and November.

A new attack technique called 'GIFShell' is used by attackers to launch phishing attacks through Microsoft Teams by executing commands to steal data using GIFs. The numerous vulnerabilities and flaws in Microsoft Teams, which has more than 270 million monthly active users, can be chained together for command execution, security control bypasses, phishing attacks and exfiltrating data via GIFs. GIFShell allows an attacker to create a reverse shell that delivers malicious commands via base64-encoded GIFs in Teams, and exfiltrates the output through GIFs retrieved by Microsoft's own infrastructure. GIFShell requires the installation of an executable that executes commands received within the GIFs. All received messages are saved to these logs and are readable by all Windows user groups, meaning any malware on the device can access them.

Another phishing campaign targeting Microsoft actually impersonated "the Microsoft team" and tried to bait recipients into adding their memo text onto an online memorial board "in memory of Her Majesty Queen Elizabeth II" after she passed away in September. The attackers stole Microsoft account details and attempted to get their victims' multi-factor authentication (MFA) codes to take over their accounts. The phishing page was created with the EvilProxy phishing kit. This is a typical example of

utilizing hot news as a lure, which frequently works.

Another large-scale phishing campaign was spotted targeting credentials for Microsoft's M365 email services. It is aimed at fintech, lending, accounting, insurance, and federal credit union organizations in the U.S., U.K., New Zealand and Australia. This campaign stands out as the threat actors are using a custom proxy-based phishing kit to bypass multi-factor authentication. The kit can easily modify legitimate login pages pulled from corporate logins and add their own phishing elements. Threat actors are turning to tools like Evilginx2, Muraena, and Modlishka to side-step MFA. Using these reverse proxies, the adversaries can sit in the middle between the victim and the server of the email provider, hence why they are called "AitM" (adversary in the middle).

Other popular companies and services were abused as well. For instance, the LinkedIn feature "Smart Links" was misused to bypass some security filters. This feature allows customers to create landing pages that contain up to 15 documents, and send others access to these pages via a trackable links. Unfortunately, this can be used as a redirector, allowing attackers to create links that will send the recipient to phishing pages. One recent theme was package delivery messages which mimic the Slovakian postal service. Another phishing actor is currently going after government contractors in the U.S. The email promises access to government portals that allow the bidding for lucrative government projects, but in actuality the emails link to a PDF which redirects to a malicious phishing site.

A new Instagram phishing campaign attempted to scam users of the popular social media platform by luring

them with a blue-badge offer. In the process, the users are asked to reveal personal information including their password, which of course is then directly sent to the attacker. The campaign sent upwards of 1,000 emails per day and was active for several weeks. Attackers created a sense of urgency and the illusion of a limited opportunity by warning users that if they ignore the message, the submission form for the blue badge will be permanently deleted in 48 hours. Enabling MFA can help minimize the risk and safeguard your account, but it's not a silver bullet.

Dropbox was utilized to drop the payload in a new two-step phishing campaign. Users were first directed to a clean site with a button or clickable text. After clicking, they are led to a malicious site and asked to log into their account. The user unknowingly falls for the attacker's scam — hook, line and credentials. What makes two-step phishing attacks unique is that they are usually delivered by email accounts that have already been compromised by the same technique, and can be spread by sending more phishing emails to the victim's contacts.

We should not forget about the local phishing campaigns that are unique to a specific region.

The volume of COVID-19-themed phishing messages doubled in September in the U.S. These emails typically impersonate the U.S. Small Business Administration (SBA) agency, and abuse Google Forms to host phishing pages that steal the personal details of business owners. As the SBA previously ran COVID-19 financial recovery programs, the lures used in the phishing emails promise pandemic financial support through programs like the "Paycheck Protection Program," "Revitalization Fund" and "COVID Economic Injury Disaster Loan." The supposed application for these programs requires clicking an embedded button which leads to a Google Form that mimics legitimate forms from SBA, and requests Google account credentials, SSNs, EINs, State ID and driver's license details, and bank account numbers.

Researchers discovered a new phishing campaign targeting U.S. and New Zealand job seekers. The malicious emails present recipients with a supposed lucrative job offer but actually include malicious documents. In some cases, opening the document triggers the exploit and leads to the downloading of a Word template hosted on a Bitbucket repository. In other cases, Cobalt Strike beacons are installed for remote

access to victims' devices. The Cobalt Strike beacon enables threat actors to execute commands remotely on the infected device, allowing them to steal data or spread laterally through the network. The current phishing campaign has several stages, with most steps relying on executing obfuscated scripts from the host's memory and abusing the Bitbucket service to evade detection.

A new phishing campaign is spreading Warzone RAT in Hungary. The campaign consists of a well-crafted fake government email that lures the users to execute the attached malware. The recipient gets an email impersonating a Hungarian government portal, which is used to conduct official business operations online such as submitting documents and ordering IDs. The email informs the recipient that new credentials to access the portal are in an attached ZIP file. Once the attachment is opened, it extracts the Warzone RAT and runs it. Warzone is a prevalent trojan operating under the malware-as-a-service (MaaS) model. It can be bought on a subscription basis for $37 per month. Cybercriminals may use this trojan to download and upload various files, execute and delete them, send commands to the infected computer's CMD (Command Prompt), view and kill processes via Task Manager, and browse the web using the computer's IP address. Warzone can be used to access victims' webcams and to steal saved passwords from browsers and email clients.

Another example is the Lampion malware that was distributed in greater volumes lately, with threat actors abusing WeTransfer as part of their phishing campaigns. WeTransfer is a legitimate file-sharing service that can be used free of charge. The service has 87 million monthly active users in 190 countries. In a new campaign, Lampion operators are sending phishing emails from compromised company accounts urging users to download a "Proof of Payment" document from WeTransfer. The targets receive a ZIP archive containing a VBS (Virtual Basic script) file. The victim must launch the file for the attack to begin. At this point, the contained DLL payloads are loaded into memory, allowing Lampion to stealthily execute on compromised systems. Lampion steals data from the computer, targeting bank accounts by fetching injections from the C2 and overlaying its own forms on login pages. When users enter their credentials, these fake login forms will be stolen and sent to the attacker.

To summarize:

A multi-layered cyber defense approach, including anti-phishing tech, is very important. Even if phishing attempts aren't neutralized right away, other detection tools can stop malware from executing.

3. Data breaches at a new all-time high

The global average total cost of a data breach now sits at $4.35 million — an increase of $0.11 million this year — according to IBM Cost of a Data Breach Report 2022. More than 100 million accounts were breached in the third quarter of 2022, as found in a recent Surfshark survey.

Unsurprisingly, cyberattacks made up 88 percent of data breaches, according to Identity Theft's Q3 2022 Data Breach Analysis. IT Governance identified 285 publicly disclosed security incidents between July and September 2022, which accounted for 232,266,148 compromised records. In the latest report, ENISA (the EU's cybersecurity agency) reported that more than 10 TBs of data are stolen monthly in ransomware attacks. A new report by KELA shows that initial access brokers (IABs) are selling access to 576 corporate networks worldwide for a total cumulative sales price of $4,000,000, motivating other cybercriminals to attack businesses.

While numbers may slightly differ depending on the source, we at Acronis can confirm that data breaches are growing in second half of 2022 — and for the whole year as well. More and more attackers utilize so-called "MFA fatigue" attacks, which work well in high-profile breaches. This type of social engineering technique has proven to be very successful by the Lapsus$ and Yanluowang threat actors when breaching large and well-known organizations. But data breaches are not only associated with ransomware. Traditional data exfiltration is still very popular, and we saw a number of huge breaches in Q3 2022 (measured in users below):

- ↘ **Neopets (69 million)**
- ↘ **Shanghai COVID-19 app (48.5 million)**
- ↘ **Mangatoon (23 million)**
- ↘ **Swachh City platform (16.4 million)**

The crypto industry, despite its fall, is still an attractive target for cybercriminals. The cryptocurrency bridge Nomad lost almost $200 million of its funds in a attack. Nomad is a cross-chain bridge between Ethereum, Moonbeam, Avalanche, Evmos and Milkomeda. Twitter user 'foobar' pointed out that the issue allegedly involved

in the cyber heist was discovered along with tens of other issues during an audit conducted this year by blockchain security firm Quantstamp. However, Nomad believes that the attack was not executed by a single attacker; in addition, many white hat hackers or security researchers may have transferred tokens into their own addresses to protect the funds. If true, the white hat hackers will likely return the funds — Nomad has provided a wallet address for this purpose.

Another recent crypto case was the QANplatform hack. The cryptocurrency bridge said it lost an estimated $2 million worth of cryptocurrency after an attacker manipulated one of its smart contracts.

Big businesses also continue to be under attack. Medibank — one of the largest Australian private health insurance providers, with about 3.9 million customers — disclosed that customers' personal information had been accessed without authorization following a recent ransomware attack. After an investigation, the firm reported that personal data belonging to its ahm health insurance subsidiary and international students have been breached, though it is unclear how many customers in total were affected. The compromised data includes first names and surnames, addresses, dates of birth, Medicare numbers, policy numbers, phone numbers and passport numbers. Medibank stressed that it found no evidence that direct debit details have been accessed. The company notified Australian Federal Police (AFP), acknowledging that they have been contacted by a criminal actor claiming to have obtained 200 GB of data. Medibank estimated the costs incurred by the incident to be between $16–22 million.

Two other major incidents also happened in Australia. Retail giant Woolworths disclosed a data breach that impacted approximately 2.2 million MyDeal customers. Optus, a subsidiary of Singtel with over 10.5 million subscribers and Australia's second-largest mobile operator, disclosed a security breach as well. The attacker claimed to have stolen the data of 11 million customers. A small sample of the stolen data was published on the breached forum with a ransom demand of $1 million. In response, Optus engaged with law enforcement

authorities to investigate the incident. Since no ransom was paid, the attackers published a larger sample of stolen data, allowing other threat actors to download and abuse it for their campaigns. Finally, the threat actor withdrew the extortion demands after facing increased attention from law enforcement. The attackers also apologized to over 10,000 people whose personal data was already leaked.

Uber disclosed a security breach in September. Threat actors gained access to its network and stole internal documents. According to the New York Times, the threat actors hacked an employee's Slack account and used it to inform internal personnel that the company had "suffered a data breach" and provided a list of allegedly hacked internal databases. The company was forced to take its internal communications and engineering systems offline to mitigate the attack and investigate the intrusion. Attackers allegedly compromised several internal systems and provided images of email, cloud storage and code repositories to the New York Times and some cybersecurity researchers. The hacker claims to be 18 years old and added that Uber had weak security; in a message sent via Slack, he also said Uber drivers should receive higher pay. This is not the first time that the company suffered a security breach. In 2017, another data breach that apparently took place in 2016 made headlines. Uber blames a threat actor allegedly affiliated with the Lapsus$ hacking group.

Electronics giant Samsung confirmed a new data breach after some of its U.S. systems were compromised in July. The electronics giant discovered on August 4 that threat actors had gained access to its systems and exfiltrated customer personal information.

The Shangri-La hotel group disclosed a data breach in which threat actors had access to a database containing the personal information of customers at eight of its Asian properties between May and July. This incident impacted hotels in Hong Kong, Singapore, Chiang Mai, Taipei and Tokyo. The company launched an investigation to determine what data had been stolen by the attackers, and has also notified authorities and any potentially impacted guests.

American Airlines disclosed a data breach in which threat actors gained access to an undisclosed number of employee email accounts. Exposed data includes names, dates of birth, mailing addresses, phone numbers, email

addresses, driver's license numbers, passport numbers and/or certain medical info provided by the impacted individuals. The security breach was discovered on July 5, after which the airline promptly adopted measures to mitigate the incident and secure the impacted email accounts. American Airlines launched an investigation with the help of a leading cybersecurity forensic firm.

British fintech firm Revolut suffered a cyberattack in which threat actors gained access to the personal information of tens of thousands of customers. The authority confirmed that the data of 50,150 customers around the world (including 20,687 in the European Economic Area) were compromised. Exposed data include names, addresses, emails, postal addresses, telephone numbers, parts of payment card data (according to the information provided by the company, the card numbers were masked), account data and more. The attackers did not access users' funds.
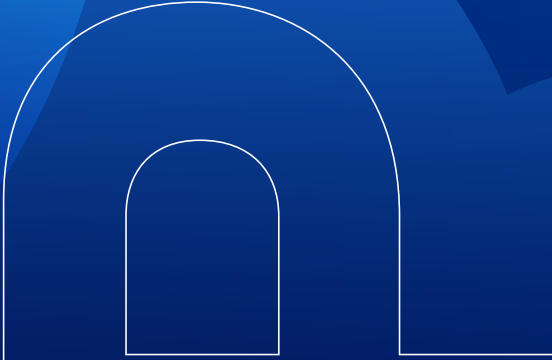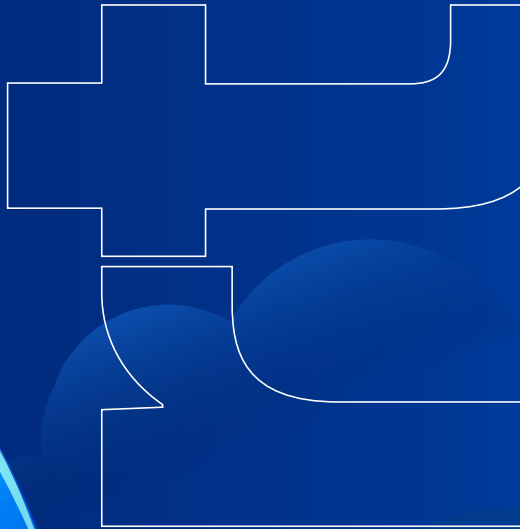

Threat actors leaked source code and gameplay videos for upcoming video game Grand Theft Auto 6 (GTA6) after they have allegedly breached the developer, Rockstar Games. The attackers appear to have compromised Rockstar Game's Slack server and Confluence wiki to do so.

The Singapore division of Starbucks suffered a data breach incident impacting over 219,000 of its customers. A data seller on the forums claims to have already sold one copy of the stolen data for $3,500, and is willing to offer at least four more copies to interested buyers.

Last but not least: never forget that consequences of the data breach is not only lost data, money and time, but also potential regulatory fines. The example case of 2022 is SHEIN: The New York Attorney General's Office has fined the retailer $1.9 million for a 2018 data breach, during which hackers stole details of 6.42 million customers.
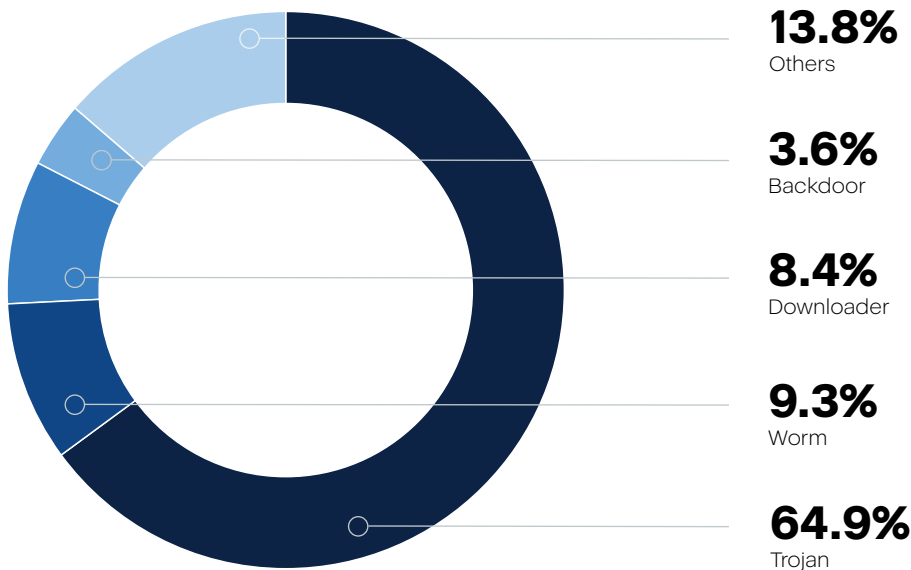
General
malware threat

In Q3 2022, an average of 11.7% of our clients had at least one malware attack successfully blocked on their endpoints. This is a slight increase from 9.4% in Q2 2022. These high percentages show that one out of 10 threats still make it to the endpoint, despite organizations' best efforts at awareness training and patching. As these numbers are from detections on endpoints, this also means that any proxy or email security that was deployed did not block these threats.

AV-TEST Malware types detected in the first 2 weeks of November 2022 (source: av-test.org)

13.8%
Others

3.6%
Backdoor

8.4%
Downloader

9.3%
Worm

64.9%
Trojan

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
July	8.7
August	8.4
September	17.9
October	9.6
November	10.4

The number of new malware samples appearing in the wild has grown slightly since 2021, but the growth per year is slowing. Sources indicate that the rate is still nearly 9 million new samples per month. This proportion matches the number of new samples seen by the Acronis CPOCs.

The average lifetime of malware samples in November 2022 was 1.7 days, after which a threat would disappear and never be seen again. In Q2 2022, this figure was at 2.3 days, showing that malware is even more short-lived today as attackers use automation to create new and personalized malware with a frequency that overwhelms traditional signature-based detection. Seventy-four percent of the samples observed were seen only once across our customer base.

The most commonly seen malware families for Q3 were as follows, showing a clear focus on bots and information stealers:

- FormBook
- AgentTesla
- LokiBot
- Snake Keylogger
- Remcos
- RedLine Stealer
- Emotet
- Raccoon Stealer
- njRAT
- AsyncRAT

The country with the most clients experiencing malware detections in October 2022 was the United States with 22.1%, followed by Germany with 8.8%, and Brazil with 7.8%. These figures are very similar to the Q2 numbers, except for the U.S. and Germany (which had a small increase, especially in financial trojans).

In these countries, MSPs and big enterprises were of the most interest to cybercriminals.

For instance, United Kingdom's National Health Service (NHS) 111 emergency services were affected by a significant and ongoing outage. This was triggered by a cyberattack that hit the systems of Advanced, a British MSP that supplies software for about 85% of the hotline's services. Advanced provides business software to more than 22,000 global customers in various industry verticals, from healthcare and education to non-profits. The MSP's list of customers includes the NHS, the UK Department for Work and Pensions (DWP) and the London City Airport. The National Crime Agency (NCA) and National Cyber Security Centre (NCSC) are both involved in the investigations.

Another example is SHI, one of the world's 15 largest IT service providers, with over 5,000 employees and annual sales that surged by 10% in 2021 to $12.3 billion. SHI fell victim to a "coordinated and professional malware attack," though there is no evidence suggesting that any of their 15,000 corporate, enterprise, public sector or academic customers had their data exfiltrated — or that any of the third-party systems in its supply chain were affected during the attack. The fact that systems were taken offline and that restoration efforts are still ongoing suggests that ransomware might have been involved. The New Jersey-based reseller is working with U.S. bodies such as the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency to probe the attack.
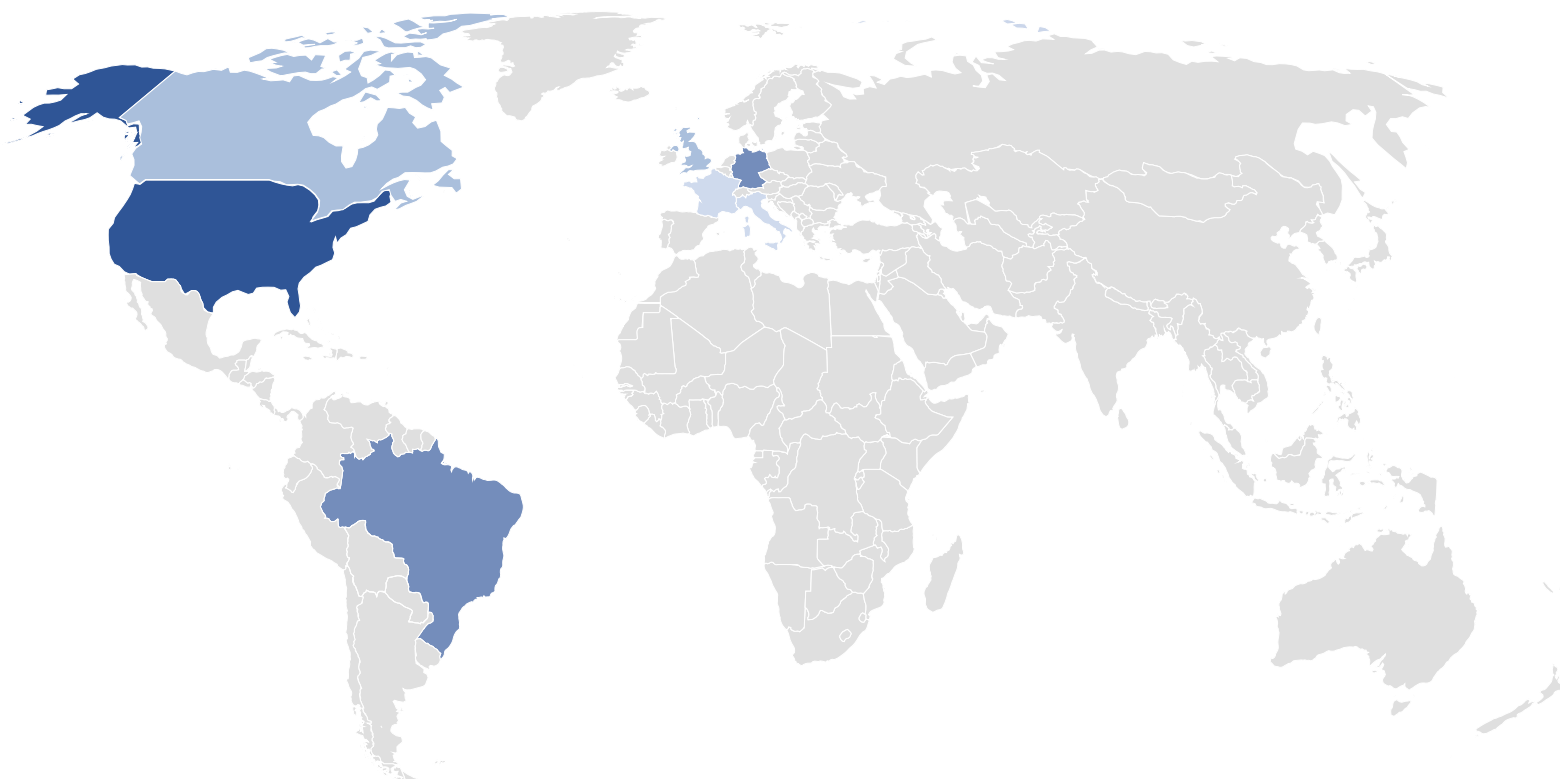
The banking industry continue to be a prime target as well, and threats there are evolving. The European Association of Secure Transactions (EAST), an industry group of banks and ATM vendors, said it's aware of at least 501 cases of ATM thefts where attackers used a new type of ATM MitM/relay attack to intercept and steal customer funds.

Monthly percentage of global detections by country, 2022

Country	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
United States	24.4	25.4	24.6	23.7	22.8	21.8	20.1	22.6	21.9	22.1	21.5
Germany	13.2	12.7	11.2	11	9.4	8.9	8.2	8.5	9.1	8.8	8.9
Brazil	4.7	3.6	3.9	4.5	7.2	7.8	9.6	9.5	7.7	7.3	6.9
Italy	4.8	4.3	5.1	5.7	6.6	6	6.2	4.5	5.9	5	5.1
Canada	7.1	7.2	7.3	6.5	6.2	5.6	4.9	6	4.7	5.5	5.8
United Kingdom	5	5.4	5.4	5.3	5.3	4.9	4.8	5	6.7	5.2	4.9
Singapore	4.2	5	4.9	4.9	3.9	4.8	5.4	4.6	3.5	4.3	4.5
Japan	2.6	3	3.1	3	2.8	3.1	3.2	3	3.1	3.7	3.4
France	2.8	2.9	2.8	2.9	2.9	2.5	2.7	2.5	3.5	3	3.2
Switzerland	3	2.8	2.9	2.6	2.4	4.1	2.3	2.7	2.9	2.7	3.2

Malware detections, November 2022

Percentage

3%   22%
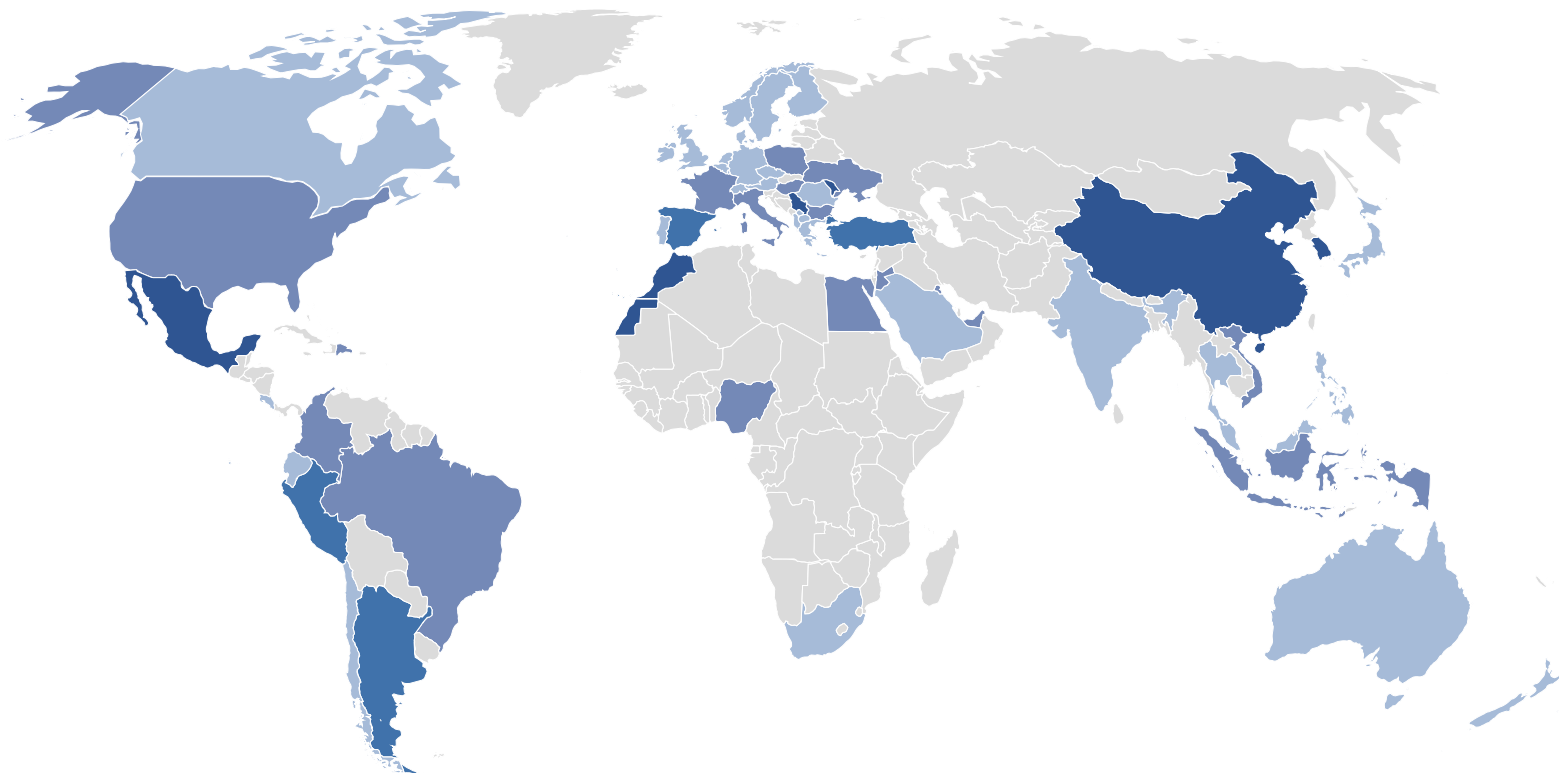
If we normalize the number of detections per active client per country, then we get a slightly different distribution. The following table shows the normalized percentage of clients with at least 25 active machines and at least 25 malware detections per country in November 2022. The percentage means that out of all actively protected workloads in that country that specicifc amount had at least one malware attack blocked.

Monthly percentage of global detections by country in 2022

Rank	Country	Percentage of clients with malware detections in November 2022
1	Egypt	32.3
2	China	27.6
3	Nigeria	26.3
4	Morocco	25.2
5	Thailand	25
6	South Korea	24.5
7	Turkey	23.9
8	Vietnam	22.5
9	India	22.5
10	Singapore	21.7
11	Taiwan	21.5
12	Republic of Moldova	21.3
13	Dominican Republic	21.2
14	Serbia	19
15	Bulgaria	18.6
16	Hungary	18
17	Peru	17.9
18	Israel	17.7
19	Argentina	16.6
20	Kingdom of Jordan	16.5
21	Philippines	15.9
22	Indonesia	15.6
23	Brazil	15
24	Spain	14.6
25	United Arab Emirates	14.5
26	Ukraine	14.2
27	Ecuador	14
28	Kuwait	13.8
29	Mexico	13.7
30	North Macedonia	13.3

Normalized malware detections, November 2022

Percentage

4%   32%

Regional normalized malware detection numbers

Top 10 countries: normalized malware detection numbers by region

Asia

Rank	Country	Regional normalized malware detection percentage in November 2022
1	China	27.6
2	Thailand	25
3	South Korea	24.5
4	Vietnam	22.5
5	India	22.5
6	Singapore	21.7
7	Taiwan	21.5
8	Philippines	15.9
9	Indonesia	15.6
10	Japan	12.2

EMEA

Rank	Country	Regional normalized malware detection percentage in November 2022
1	Egypt	32.3
2	Nigeria	26.3
3	Morocco	25.2
4	Turkey	23.9
5	Republic of Moldova	21.3
6	Serbia	19
7	Bulgaria	18.6
8	Hungary	18
9	Israel	17.7
10	Kingdom of Jordan	16.5

Americas

Rank	Country	Regional normalized malware detection percentage in November 2022
1	Dominican Republic	21.2
2	Peru	17.9
3	Argentina	16.6
4	Brazil	15
5	Ecuador	14
6	Mexico	13.7
7	Colombia	12
8	Costa Rica	11.5
9	United States	10.1
10	Chile	8.8

Ransomware threats

As we already mentioned in the key trends section, ransomware is still the number one cyberthreat for businesses. In this section, we're focusing on activity from July to November of 2022, including from attacks blocked by our threat-agnostic Acronis Active Protection and from data published on the underground leak sites of ransomware operators.

These are the top 10 most active ransomware families we observed and tracked in Q3–Q4 2022.

- Lockbit
- Black Basta
- LV
- Ragnar Locker
- STOP
- BlackCat/ALPHV
- Vice Society
- Hive
- Everest
- Royal

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, where they only attempt a handful of infections but strive for a high payout. Hence the volume of threat detection alone is not an indication of how dangerous the threat truly is. In addition, many groups operate ransomware-as-a-service businesses, and attackers might be using multiple threat families during similar attacks.

We have seen 576 publicly mentioned ransomware compromises in Q3, a slight increase from Q2. Of course, this is only a subset of the actual victims, as some do negotiate and ultimately pay the ransomware groups in order to avoid being mentioned publicly. Also, some groups have shifted towards data exfiltration only; such attacks might not be named as ransomware incidents, but simply as data breaches.
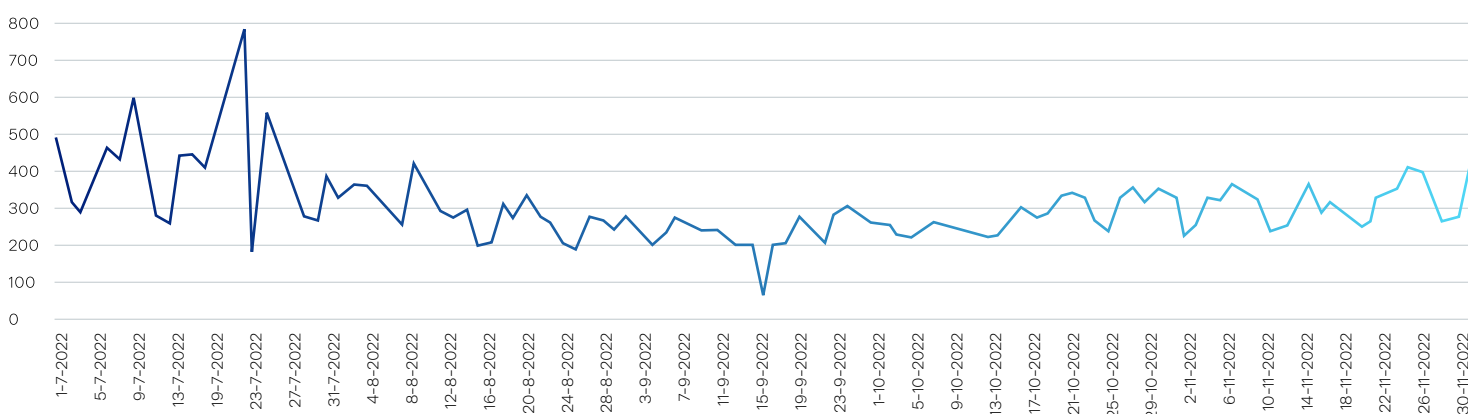
Daily ransomware detections

The number of ransomware incidents has decreased slightly in Q3, after a high during the summer months. From July to August, we had an increase of 49% of blocked ransomware attacks globally, followed by a decrease of 12.9% in September and 4.1% in October.

Changes in the number of ransomware detections per quarter per region:

Month	EMEA	America	Asia	Global
July–August	36.3	23.3	28.6	49
August–September	-11.7	-5.9	-21.2	-12
September–October	-23.2	5.8	-6	-4.1

Daily ransomware detections globally:

Ransomware detections per day:

Month	Ransomware detections per day
January	540
February	335
March	201
April	237
May	566
June	329
July	272
August	242
September	237
October	295
November	307

Top 10 countries: ransomware detections by region

Asia

Country	Regional ransomware detection percentage in Q3 2022	Regional ransomware detection percentage in Q2 2022	Regional ransomware detection percentage in Q1 2022
Japan	26.6	37.3	34.3
China	9.8	12	13.1
Philippines	2.4	5.8	4
Taiwan	3.9	5.1	4.9
India	2.5	4.2	5.9
South Korea	2.9	4.1	4.5
Turkey	2.6	4	5.1
Singapore	0.6	3	1.8
Vietnam	1.4	2.6	1.4
Thailand	1.5	2.1	2.7

EMEA

Country	Regional ransomware detection percentage in Q3 2022	Regional ransomware detection percentage in Q2 2022	Regional ransomware detection percentage in Q1 2022
Germany	54.2	44	48.1
United Kingdom	11.1	8.7	7.7
France	9.3	8.1	7.1
Italy	7.6	6.2	5.3
Switzerland	6.5	4.7	5
Spain	4.1	4.6	3.5
Netherlands	3.7	2.9	3
Austria	3.3	2.6	2.8
Czechia	2.5	1.8	2
Ukraine	1.8	1.8	1.9

Americas

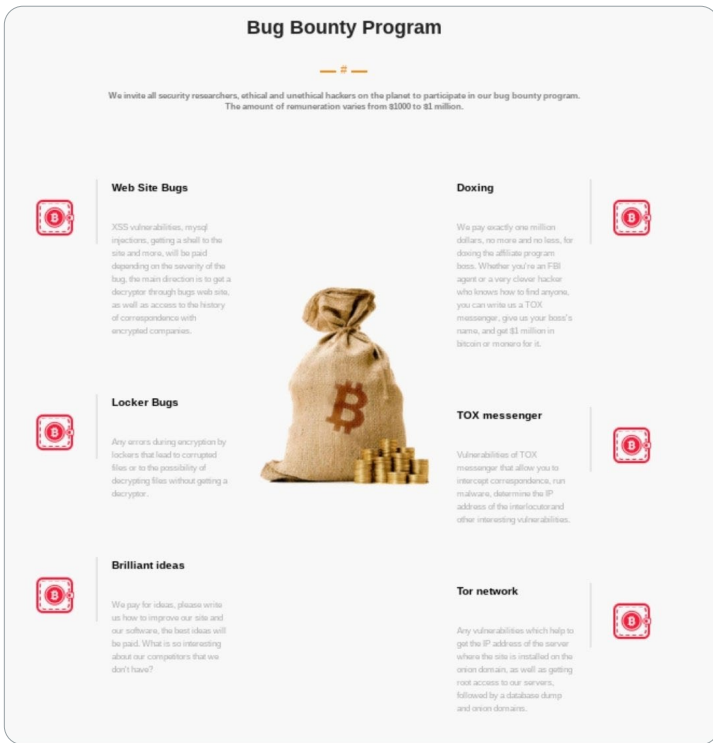| Country	Regional ransomware detection percentage in Q3 2022	Regional ransomware detection percentage in Q2 2022	Regional ransomware detection percentage in Q1 2022
United States	60	62.7	65
Canada	19.7	23.9	25.1
Mexico	2.7	3.8	2.8
Brazil	1.4	1.7	1.6
Argentina	1.2	1.4	0.9
Colombia	0.5	1.1	0.6
Peru	0.4	0.9	0.5
Chile	0.5	0.8	0.6
Guatemala	0.1	0.6	0.4
Ecuador	1.2	0.4	0.3

Ransomware groups in the spotlight

LockBit 3.0: Ransomware with bug bounty program

On May 17, 2022, LockBit spokesman "LockBitSupp" announced that a new version of the infamous ransomware would be released in the near future.

Later, on Twitter, **vx-underground** shared pictures of the LockBit 3.0 site, generated ransomware files and encryption results. Version 3.0 was named "LockBit Black" by threat actors, and cybersecurity analytics found similarities with BlackMatter/DarkSide ransomware.
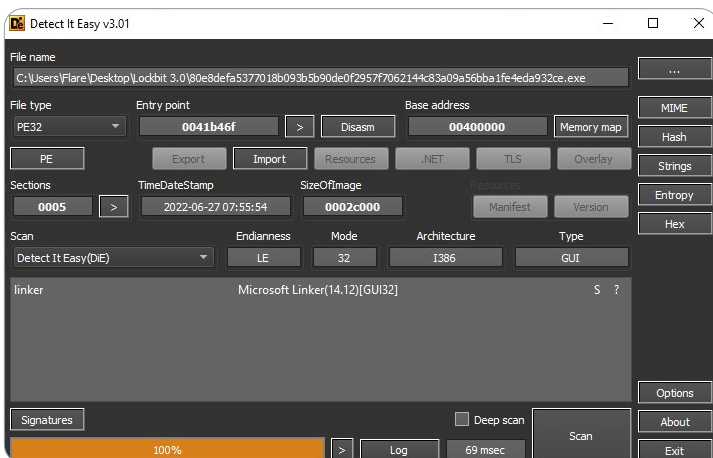
Version 3.0 has encoded functionality in the '.text' section that can be decrypted only with a key, which must be given as '-pass' argument in the command prompt. It encrypts files, changing their icon, filename and extension, changes the desktop background and drops a ransom note in each encrypted folder. Notably, LockBit 3.0 introduced the first ransomware bug bounty program, offering money to users who submit bug reports. There have already been multiple such submissions, and at least one payout.

Bug Bounty Program

— # —

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program.
The amount of remuneration varies from $1000 to $1 million.

Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decrypter through bugs web site, as well as access to the history of correspondence with encrypted companies.

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

Locker Bugs

Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decrypter.

TOX messenger

Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutor and other interesting vulnerabilities.

Brilliant ideas

We pay for ideas, please write us how to improve our site and our software, the best ideas will be paid. What is so interesting about our competitors that we don't have?

Tor network

Any vulnerabilities which help to get the IP address of the server where the site is installed on the onion domain, as well as getting root access to our servers, followed by a database dump and onion domains.

Overview of Lockbit 3.0

Nearly all found samples are PE32 executables and are similar in size. In fact, each uses the same logic, and Detect It Easy can't define what language they were written in.

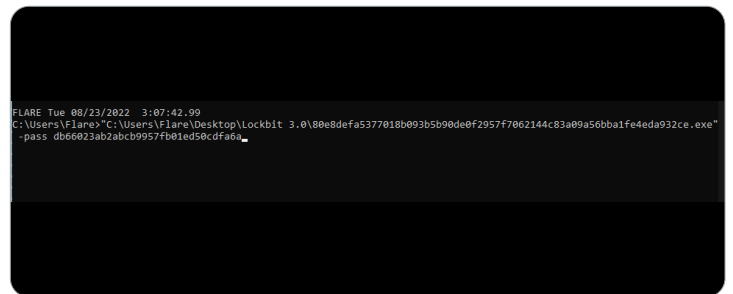|			
80e8defa5377018b093b5b90de0f2957f706...	8/23/2022 1:44 AM	Application	162 KB
391a97a2fe6beb675fe350eb3ca0bc3a995f...	8/23/2022 1:45 AM	File	162 KB
a56b41a6023f828cccaaef470874571d169f...	8/23/2022 1:46 AM	BIN File	162 KB
b951e30e29d530b4ce998c505f1cb0b8adc...	8/23/2022 1:47 AM	File	155 KB
c6cf5fd8f71abaf5645b8423f404183b3dea1...	8/23/2022 1:48 AM	File	162 KB
d61af007f6c792b8fb6c677143b7d0e25333...	8/23/2022 1:49 AM	BIN File	162 KB
fd98e75b65d992e0ccc64e512e4e3e78cb2...	8/23/2022 1:51 AM	File	176 KB
Lockbit 3.0-2	8/23/2022 1:35 AM	0-2 File	162 KB
unknown.bin	8/23/2022 1:51 AM	BIN File	163 KB

On first look in the IDA disassembler, these samples don't have a lot of functions, strings and imports, but there is an encrypted '.text' segment with execution permission, which takes more than half the weight of the file.

```
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Write/Execute
.text:00401000 _text          segment para public 'CODE' use32
.text:00401000                assume cs:_text
.text:00401000                ;org 401000h
.text:00401000                assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000                dd 0C0F27AB8h, 2EA22129h, 6B5528ADh, 6527AEC1h, 42BEEBCh
.text:00401000                dd 0C095781Dh, 83B4EE71h, 2876FFDDh, 5D75F015h, 9EDF05CAh
.text:00401000                dd 0E43E0913h, 17E91307h, 74B1022Fh, 0EC57EBE5h, 0BD836E32h
.text:00401000                dd 0F2729048h, 7AE0E5F9h, 19393CB4h, 94D842B9h, 0EAF2E78Ch
.text:00401000                dd 9601D830h, 0E31E34D3h, 14765DA6h, 84C3D797h, 4D2488D3h
.text:00401000                dd 47709FBDh, 0F61FE9C4h, 7CDEF68Dh, 6488B55Ch, 0EDDB31C0h
.text:00401000                dd 46FF2BD7h, 0E406FD17h, 7FC3252h, 3EFD6000h, 3A2E92BAh
.text:00401000                dd 43056EEAh, 0EFCF5F16h, 0C0C74850h, 73845053h, 94191E8Dh
.text:00401000                dd 9EF130CFh, 24409943h, 0FB7866B3h, 0EFF2F30Eh, 934B3B0Ch
.text:00401000                dd 6A2D0348h, 0DA8AC3D0h, 0F95FCD39h, 73D7019Ah, 585EA3EDh
```

Execution

LockBit 3.0 must be executed via command prompt with the '-pass' argument. This is similar to the ALPHV ransomware, which uses an access token to start executing. In the case of LockBit, this argument is a key, which is used to decrypt the '.text' segment; the keys are different for different samples. For example, for the sha256:80e8defa5377018b093b5b90de0f29 57f7062144c83a09a56bba1fe4eda932ce sample the key will be next: db66023ab2abcb9957fb01ed50cdfa6a

```
FLARE Tue 08/23/2022  3:07:42.99
C:\Users\Flare>"C:\Users\Flare\Desktop\Lockbit 3.0\80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce.exe"
 -pass db66023ab2abcb9957fb01ed50cdfa6a_
```

At the start of execution, LockBit will call the "sub41B000" function, which takes the given key and loads the '.text' segment to the 'sub_41B41C' function.

Detect It Easy v3.01

File name
C:\Users\Flare\Desktop\Lockbit 3.0\80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce.exe

File type	Entry point	Base address	
PE32	0041b46f	>	Disasm	00400000	Memory map

PE | Export | Import | Resources | .NET | TLS | Overlay

| Sections | TimeDateStamp | SizeOfImage | |
| 0005 | > | 2022-06-27 07:55:54 | 0002c000 |

Scan: Detect It Easy(DiE)
Endianness: LE Mode: 32 Architecture: I386 Type: GUI

linker   Microsoft Linker(14.12)[GUI32]   S ?

```
.itext:0041B082 loc_41B082:              ; CODE XREF: sub_41B000+72↑j
.itext:0041B082                          ; sub_41B000+79↑j
.itext:0041B082 mov    ecx, [esi+0Ch]
.itext:0041B085 add    ecx, ebx
.itext:0041B087 push   [ebp+var_64]
.itext:0041B08A lea    eax, [ebp+var_174]
.itext:0041B090 push   eax
.itext:0041B091 push   dword ptr [esi+10h]
.itext:0041B094 push   ecx
.itext:0041B095 call   sub_41B41C
.itext:0041B09A
.itext:0041B09A loc_41B09A:
.itext:0041B09A add    esi, 2
.itext:0041B09D dec    edi
```

Output window
747C0000: loaded C:\Windows\SysWOW6
66640000: loaded C:\Windows\SysWOW6
75D70000: loaded C:\Windows\SysWOW6

LockBit divides loaded segments on smaller sections and decrypts them with 'sub_41B41C' decryption function.

```
.itext:0041B41C push    ebp
.itext:0041B41D mov     ebp, esp
.itext:0041B41F push    ebx
.itext:0041B420 push    esi
.itext:0041B421 push    edi
.itext:0041B422 xor     eax, eax
.itext:0041B424 mov     ebx, [ebp+arg_C]
.itext:0041B427 xor     ecx, ecx
.itext:0041B429 xor     edx, edx
.itext:0041B42B mov     esi, [ebp+arg_4]
.itext:0041B42E mov     edi, [ebp+arg_0]
.itext:0041B431 test    esi, esi
.itext:0041B433 jz      short loc_41B468
.itext:0041B435 push    ebp
.itext:0041B436 mov     ebp, [ebp+arg_8]
.itext:0041B439
.itext:0041B439 loc_41B439:                      ; CODE XREF: sub_41B41C+49↓j
.itext:0041B439 mov     dl, [ebp+ecx+var_s0]
.itext:0041B43D add     dl, bl
.itext:0041B43F mov     bl, [ebp+edx+var_s0]
.itext:0041B443 mov     dl, [ebp+ebx+var_s0]
.itext:0041B447 mov     dl, [ebp+edx+var_s0]
.itext:0041B44B inc     dl
.itext:0041B44D mov     al, [ebp+edx+var_s0]
.itext:0041B451 xor     [edi], al
.itext:0041B453 mov     dl, [ebp+ebx+var_s0]
.itext:0041B457 xchg    dl, [ebp+ecx+var_s0]
.itext:0041B45B mov     [ebp+ebx+var_s0], dl
.itext:0041B45F inc     cl
.itext:0041B461 inc     edi
.itext:0041B462 dec     esi
.itext:0041B463 test    esi, esi
.itext:0041B465 jnz     short loc_41B439
.itext:0041B467 pop     ebp
```

After that, it will call the function from the decrypted segment:

```
.itext:0041B46F public start
.itext:0041B46F start:
.itext:0041B46F nop
.itext:0041B470 nop     dword ptr [eax+eax+00000000h]
.itext:0041B478 call    sub_41B000              ; decrypt
.itext:0041B47D nop     dword ptr [eax+00h]
.itext:0041B481 call    loc_408254              ; decrypted segment
.itext:0041B486 xchg    ax, ax
.itext:0041B488 call    sub_40B804
.itext:0041B48D nop     dword ptr [eax+eax+00h]
.itext:0041B492 call    loc_418F78              ; decrypted segment
.itext:0041B497 nop     dword ptr [eax+eax+00000000h]
.itext:0041B49F push    0
.itext:0041B4A1 call    dword 4275C0
```
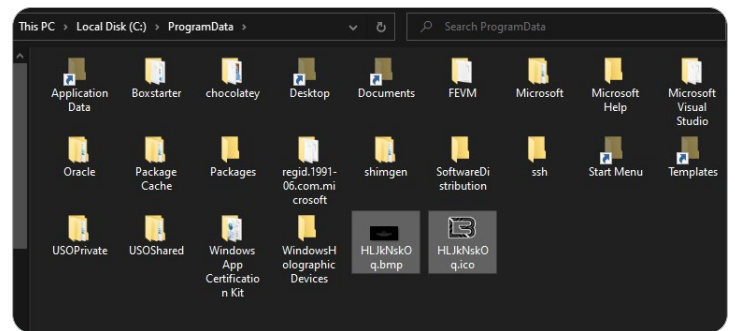
In the decrypted section, LockBit hides its WinAPI functions, calls and strings. It uses the 'sub_407C5C' function to resolve actual APIs. This technique is also used by the BlackMatter ransomware.

```
.text:004082B1 push    offset unk_407DA4
.text:004082B6 push    offset unk_427408
.text:004082BB call    sub_407C5C
.text:004082C0 push    edi
.text:004082C1 push    esi
.text:004082C2 push    offset unk_407E94
.text:004082C7 push    offset unk_4274F4
.text:004082CC call    sub_407C5C
.text:004082D1 push    edi
.text:004082D2 push    esi
.text:004082D3 push    offset unk_407F88
.text:004082D8 push    4275E4h
.text:004082DD call    sub_407C5C
.text:004082E2 push    edi
.text:004082E3 push    esi
.text:004082E4 push    40802Ch
.text:004082E9 push    427684h
.text:004082EE call    sub_407C5C
.text:004082F3 push    edi
.text:004082F4 push    esi
.text:004082F5 push    408040h
.text:004082FA push    427694h
.text:004082FF call    sub_407C5C
.text:00408304 push    edi
.text:00408305 push    esi
.text:00408306 push    40807Ch
.text:0040830B push    4276CCh
.text:00408310 call    sub_407C5C
.text:00408315 push    edi
.text:00408316 push    esi
.text:00408317 push    4080D4h
.text:0040831C push    427720h
.text:00408321 call    sub_407C5C
```

This function loads an obfuscated string and performs an XOR operation with '4506DFCA' as the key. The result will be the WinAPI name.

```
.text:00407C62 mov     esi, [ebp+arg_4]
.text:00407C65 lodsd
.text:00407C66 xor     eax, 4506DFCAh
.text:00407C6B push    eax
.text:00407C6C call    sub_407AE0
.text:00407C71 test    eax, eax
.text:00407C73 jz      loc_407D9C
.text:00407C79 mov     edi, [ebp+arg_0]
.text:00407C7C add     edi, 4
```

During execution, LockBit dropped two files in the 'C:\ProgramData' folder. The first file ('.bmp') will be used to change desktop background, and the second ('.ico') will be used to change encrypted files icons.

To evade detection, LockBit modifies all subkeys in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\ path after execution. These keys are related to the Windows Event Log, and LockBit will change two values in all of them:

ChannelAccess – O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)
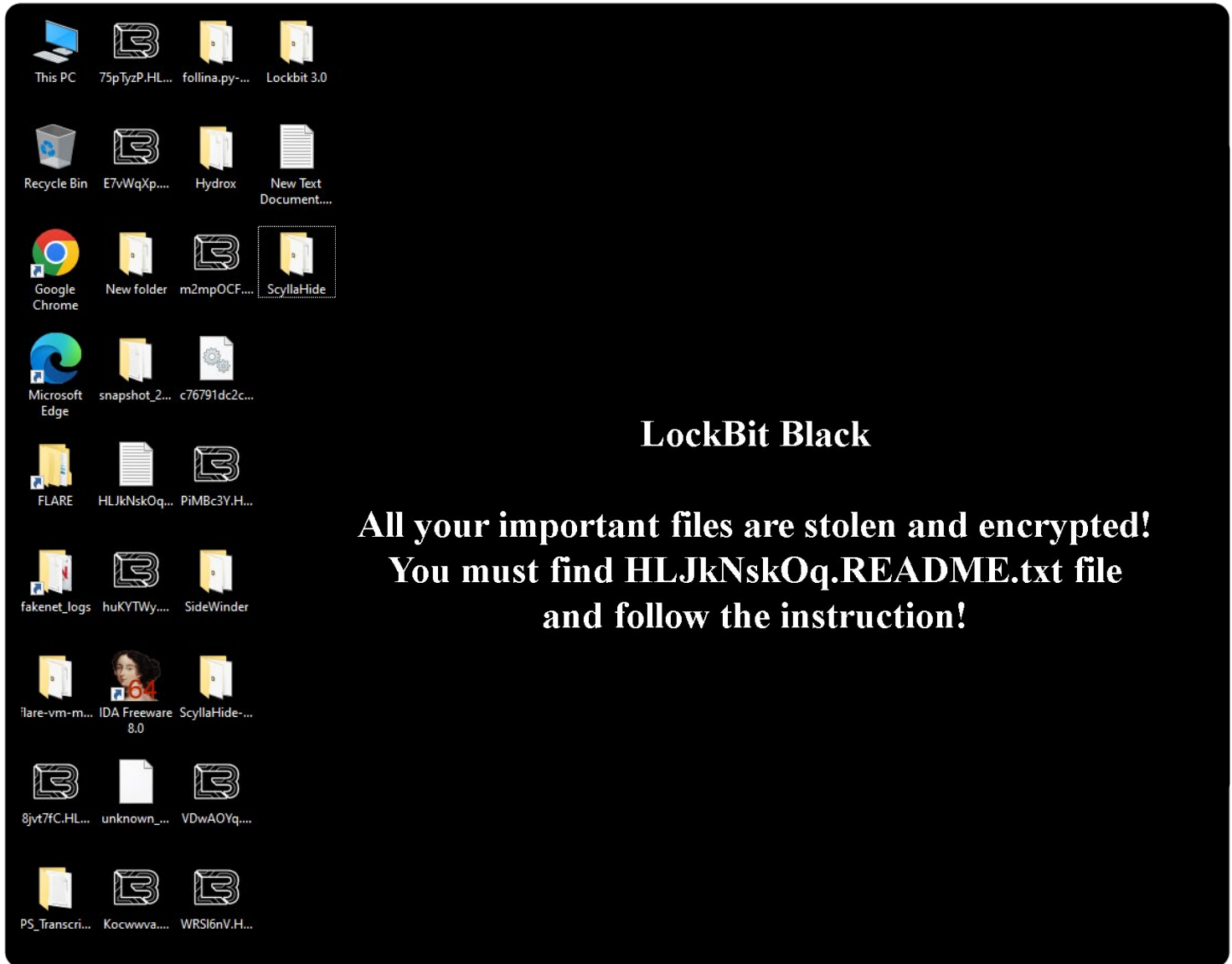
Enabled – 0

Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelAccess	REG_SZ	O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)
Enabled	REG_DWORD	0x00000000 (0)
Isolation	REG_DWORD	0x00000001 (1)
MaxSize	REG_DWORD	0x00040000 (262144)
MaxSizeUpper	REG_DWORD	0x00000000 (0)
OwningPublisher	REG_SZ	{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Type	REG_DWORD	0x00000001 (1)

Encrypted files will have the '.HLJkNskOq' extension, a new randomly generated name and a changed icon. All encrypted files also have 133 bytes appended at the end of the file, which are used as a decryption ID.
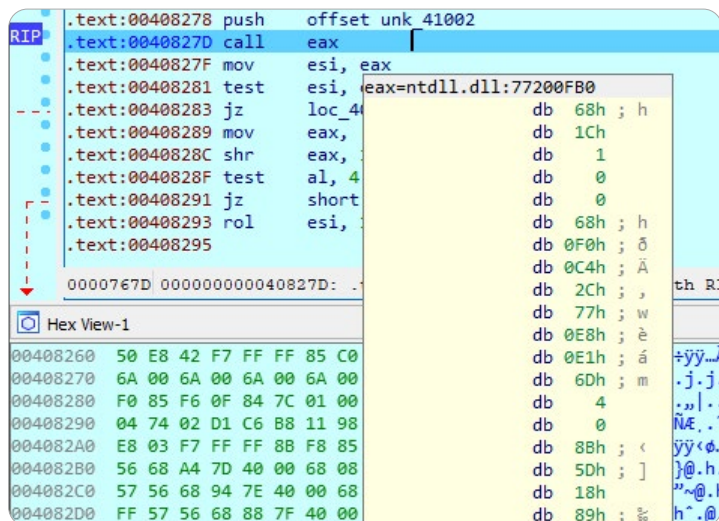

Once execution has completed, LockBit deletes itself.

Obfuscation

LockBit uses encoded fragments of code, which can be accessed only during debugging. It uses function call obfuscation, loading them to one of the general purpose registers.
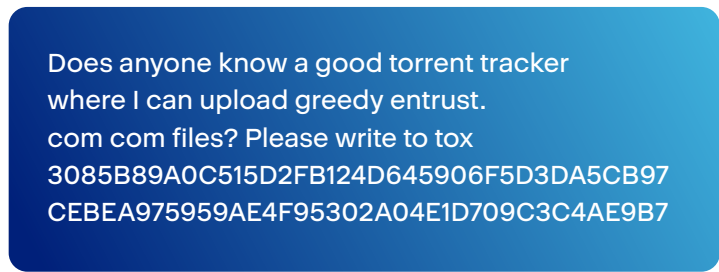

The malware also has functions to dynamically resolve WinAPI functions' names. This is done to hide its real import table from static analysis.
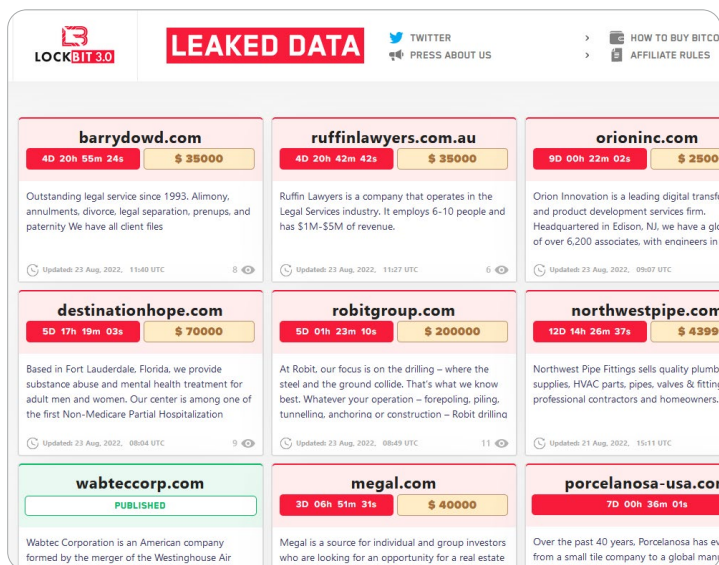
Ransom note

LockBit 3.0 drops the ransom note 'HLJkNskOq.README. txt' in each folder whose contents are encrypted. This file is very long and contains the victim's ID as well as links to the data leak site and chat (both for Tor and for normal browsers). The note warns victims about what will happen to their files if they fail to pay the ransom, go to the police or try to otherwise recover their own data.

Data leak site

While the data leak is loading, it prints the following text:

> Does anyone know a good torrent tracker where I can upload greedy entrust. com com files? Please write to tox 3085B89A0C515D2FB124D645906F5D3DA5CB97 CEBEA975959AE4F95302A04E1D709C3C4AE9B7

The data leak page contains a collection of victims. Each victim has a timer and a price, which they must pay to the threat actors to decrypt their data (and to prevent its publishing). The site also lists victims who didn't pay the ransom and had their data published as a result.

Conclusion

Lockbit 3.0, or LockBit Black, now uses a key to begin execution — a similar tactic to that of ALPHV ransomware, which uses an access token.

Initial samples have not many strings, imports and functions; instead, a '.text' section takes more than half of the file weight. This section is decoded using a given key during runtime into the executable code, and contains functions to dynamically resolve WinAPI function names using an XOR cipher.

During the encryption process, LockBit 3.0 makes changes to the desktop background and registry. All encrypted files have an altered name, icon and extension. Compared to other ransomware, LockBit still has the fastest encryption speed — in the latest samples, this may even increase while simultaneously receiving new functionality. There is no official universal decryptor for LockBit 3.0 at this moment, but the **RansomHunter team provides help** with decrypting files.

Prestige: New ransomware to hit transportation and logistics organizations

On October 14, 2022, Microsoft Security Intelligence found a new ransomware, targeting Ukraine and Poland transportation and logistics organizations. This threat was deployed on victims' computers on October 11, 2022 and served as a way for threat actors to deploy additional malicious files to the system, with a one-hour delay between attacks. The name of the ransomware ("Prestige") was taken from the email address in the ransom note.
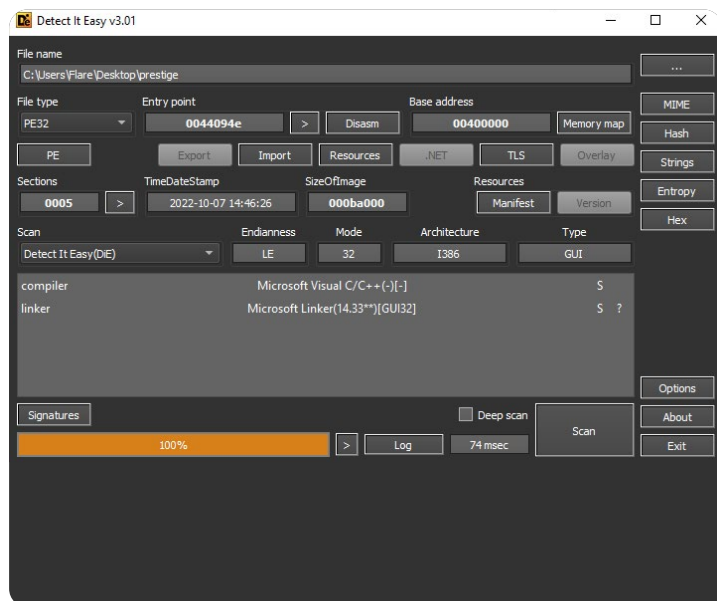
Delivery

Prestige has been deployed on remote systems using three different observed methods:

- Obtaining access and copying malicious files to the ADMIN$ share, and using the Impacket tool to create a scheduled task that will execute the ransomware

- Obtaining access and copying malicious files to the ADMIN$ share and using the Impacket tool to load and execute a PowerShell script, which will in turn execute the ransomware

- Copying the malicious files to the Active Directory Domain Controller and deploying to systems using the Default Domain Group Policy Object

Overview

The Prestige sample is a PE32 file, written in the C++ programming language, and has a compilation timestamp 07.10.2022 (four days before the observed attacks). This file is not packed or obfuscated.

Execution

At the start of execution, Prestige checks CPU information with the 'cpuid' instruction and 'IsProcessorFeaturePresent' function with an argument value of '10', which (if found) indicates that the system supports the SSE2 instruction set.

Prestige uses a lot of SSE2 instructions in the code, so to function properly it needed this feature in the processor.

SSE2 instructions usage example in the Prestige sample

To start, the Prestige ransomware must have administrative privileges. It terminates the MSSQL Windows service with a hardcoded command appending to it 'MSSQLSERVER':

To prevent system restoration after encryption, it deletes backup catalogs using WBAdmin and all volume shadow copies using VSSAdmin.

```
aCWindowsSystem_2:                          ; DATA XREF: sub_411979+3B2↑o
              text "UTF-16LE", 'C:\Windows\System32\wbadmin.exe delete catalog -qui'
              text "UTF-16LE", 'et',0
              align 10h
aCWindowsSystem_3:                          ; DATA XREF: sub_411979+3F5↑o
              text "UTF-16LE", 'C:\Windows\System32\vssadmin.exe delete shadows /al'
              text "UTF-16LE", 'l /quiet',0
```

These commands use tools located in the System32 folder and the Prestige sample is a 32-bit application. It disables file system redirection using the 'Wow64DisableWow64FsRedirection' function. After executing the commands, it calls the 'Wow64RevertWow64FsRedirection' function to restore file system redirection.

```
.text:0043194?        mov     ....
.text:00431947        call    edi ; CryptAcquireContextA
.text:00431949        test    eax, eax
.text:0043194B        jnz     short loc_43197A
.text:0043194D        push    ebx
.text:0043194E        call    ds:GetLastError
.text:00431954        push    8               ; dwFlags
.text:00431956        push    1               ; dwProvType
.text:00431958        push    0               ; szProvider
.text:0043195A        push    offset szContainer ; "Crypto++ RNG"
.text:0043195F        push    esi             ; phProv
.text:00431960        mov     ebx, eax
.text:00431962        call    edi ; CryptAcquireContextA
.text:00431964        test    eax, eax
.text:00431966        jnz     short loc_431979
.text:00431968        push    28h             ; dwFlags
.text:0043196A        push    1               ; dwProvType
.text:0043196C        push    eax             ; szProvider
.text:0043196D        push    offset szContainer ; "Crypto++ RNG"
.text:00431972        push    esi             ; phProv
.text:00431973        call    edi ; CryptAcquireContextA
.text:00431975        test    eax, eax
.text:00431977        jz      short loc_43198C
```

The ransom note is hardcoded in the code and will be dropped to the 'C/Users/Public' folder as 'README' file without an extension.

```
aPrestigeRanuso:                            ; DATA XREF: .rdata:off_49EF00↑o
              text "UTF-16LE", 'Prestige.ranusomeware@Proton.me',0
aYouPersonalFil:                            ; DATA XREF: sub_40226F+8E↑o
              text "UTF-16LE", 'YOU PERSONAL FILES HAVE BEEN ENCRYPTED.',0Dh,0Ah
              text "UTF-16LE", 0Dh,0Ah
              text "UTF-16LE", 'To decrypt all the data, you will need to purchase '
              text "UTF-16LE", 'our decryption software.',0Dh,0Ah
              text "UTF-16LE", 'Contact us {}. In the letter, type your ID = {:X}.',0Dh
              text "UTF-16LE", 0Ah
              text "UTF-16LE", 0Dh,0Ah
              text "UTF-16LE", '* ATTENTION *',0Dh,0Ah
              text "UTF-16LE", '- Do not try to decrypt your data using third party'
              text "UTF-16LE", ' software, it may cause permanent data loss.',0Dh,0Ah
              text "UTF-16LE", '- Do not modify or rename encrypted files. You will'
              text "UTF-16LE", ' lose them.',0Dh,0Ah,0
              align 10h
```

Once the ransom note is dropped, it makes two registry changes. The first one is the registration of the new file extension of encrypted files ('.enc'), and the second is used to launch the ransom note in Notepad after the user opens any encrypted file.

```
aCWindowsSystem_0:                          ; DATA XREF: sub_4112A8+14↑o
              text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\.enc /ve /t RE'
              text "UTF-16LE", 'G_SZ /d enc /f',0
              align 10h
aCWindowsSystem_1:                          ; DATA XREF: sub_4112A8+34↑o
              text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\enc\shell\open'
              text "UTF-16LE", '\command /ve /t REG_SZ /d "C:\Windows\Notepad.exe C'
```

File encryption

Before starting the encryption process, Prestige loads a list of extensions that must be encrypted:

.1cd, .7z, .abk, .accdb, .accdc, .accde, .accdr, .alz, .apk, .apng, .arc, .asd, .asf, .asm, .asx, .avhd, .avi, .avif, .bac, .backup, .bak, .bak2, .bak3, .6h, .bkp, .bkup, .bkz, .bmp, .btr, .6z, .6z2, .bzip, .bzip2, .c, .cab, .cer, .cf, .cfu, .cpp, .crt, .css, .db, .db-wal, .db3, .dbf, .der, .dmg, .dmp, .doc, .docm, .docx, .dot, .dotm, .dotx, .dpx, .dsk, .dt, .dump, .dz, .ecf, .edb, .epf, .exb, .ged, .g1f, .gpg, .gzi, .gzip, .hdd, .img, .1so, .jar, .Java, .jpeg, .jpg, .js, .json, .kdb, .key, .1z, .1z4, .1zh, .1zma, .mdmr, .mkv, .mov, .mp3, .mp4, .mpeg, .myd, .nude, .nvram, .oab, .odf, .ods, .old, .ott, .ovf, .p12, .pac, .pdf, .pem, .pfl, .pfx, .php, .pkg, .png, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .pvm, .py, .qcow, .qcow2, .r0, .rar, .raw, .rz, .s7z, .sdb, .sdc, .sdd, .sdf, .sfx, .skey, .sldm, .s1dx, .sql, .sqlite, .svd, .svg, .tar, .taz, .tbz, .tbz2, .tg, .tib, .tiff, .trn, .txt, .txz, .tz, .vb, .vbox, .vbox-old, .vbox-prev, .vdi, .vdx, .vhd, .vhdx, .vmc, .vmdk, .vmem, .vmsd, .vmsn, .vmss, .vmx, .vmxf, .vsd, .vsdx, .vss, .vst, .vsx, .vtx, .wav, .wbk, .webp, .wmdb, .wmv, .xar, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .x1w, .xz, .z, .zbf, .zip, .zipx, .z1, .zpi, .zz

Prestige uses the Crypto++ cryptographic library to perform file encryption with the AES algorithm. The RSA public key is hard-coded, and is different for each sample.

```
.rdata:0049FDC8 aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
.rdata:0049FDC8                                    ; DATA XREF: sub_40221B+5↑o
.rdata:0049FDC8              db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4mpkHWE1p0nefE0PL/Qk',0Ah
.rdata:0049FDC8              db 'gT7bjLTeJ9bpH6v41L1YGI688cwfEnjmIaDa0zwvHfbT8dn4o+Wh2iSpUZk0BYIi',0Ah
.rdata:0049FDC8              db 'Lw6u5+9nSd2UzD4sB+MY9dv6oVTHInxqp4VNLHR2nMjgIS4rFHYzNJ7Tsj/j3YJZ',0Ah
.rdata:0049FDC8              db 'dVPuPVCqbpZg5boXoSFbgLNIn6Mnr+vKc5tGh+pkGty0otyFd/ghM0b/xitowcvx',0Ah
.rdata:0049FDC8              db 'eqZezPO0YXmkjjeTi0jFa7E9IIP3Z/DMOR9r/oJR0NyEIs9HNKdFGTAjJKDAKWxu',0Ah
.rdata:0049FDC8              db '1nEPXiZoPPHgS7fxqg40+ciCjj2i7eUwqVkop5PvwjqtqQ0TkIt8EqjvkmDtMrp8',0Ah
.rdata:0049FDC8              db 'ZQIDAQAB',0Ah
.rdata:0049FDC8              db '-----END PUBLIC KEY-----',0Ah,0
```

The 'CryptAcquireContextA' function is used to acquire a handle to the Crypto++ RNG (RandomNumberGenerator) keys container.

```
.text:00431947              call    edi ; CryptAcquireContextA
.text:00431949              test    eax, eax
.text:0043194B              jnz     short loc_43197A
.text:0043194D              push    ebx
.text:0043194E              call    ds:GetLastError
.text:00431954              push    8           ; dwFlags
.text:00431956              push    1           ; dwProvType
.text:00431958              push    0           ; szProvider
.text:0043195A              push    offset szContainer ; "Crypto++ RNG"
.text:0043195F              push    esi         ; phProv
.text:00431960              mov     ebx, eax
.text:00431962              call    edi ; CryptAcquireContextA
.text:00431964              test    eax, eax
.text:00431966              jnz     short loc_431979
.text:00431968              push    28h         ; dwFlags
.text:0043196A              push    1           ; dwProvType
.text:0043196C              push    eax         ; szProvider
.text:0043196D              push    offset szContainer ; "Crypto++ RNG"
.text:00431972              push    esi         ; phProv
.text:00431973              call    edi ; CryptAcquireContextA
.text:00431975              test    eax, eax
.text:00431977              jz      short loc_43198C
```

To perform encryption with AES, Prestige checks whether AES-NI (AES New Instructions) and SSE2 instructions are supported by the CPU.

```
cmp     byte_4AFD92, 0
push    esi
jz      short loc_432405
mov     ecx, [esp+8+arg_0]
push    offset aAesni   ; "AESNI"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

```
cmp     byte_4AFD8D, 0
jz      short loc_43242E
mov     ecx, [esp+8+arg_0]
push    offset aSse2    ; "SSE2"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

If the CPU supports these instructions, the encryption process begins. 'aesenc' instructions will perform one round of encryption, and 'aesenclast' will perform the last round of encryption.

```
sub     [esp+8+arg_4], 1
lea     edi, [edi+10h]
movups  xmm1, xmmword ptr [edi-10h]
movups  xmm0, xmmword ptr [ecx]
aesenc  xmm0, xmm1
movups  xmmword ptr [ecx], xmm0
movups  xmm0, xmmword ptr [edx]
aesenc  xmm0, xmm1
movups  xmmword ptr [edx], xmm0
movups  xmm0, xmmword ptr [esi]
aesenc  xmm0, xmm1
movups  xmmword ptr [esi], xmm0
movups  xmm0, xmmword ptr [eax]
aesenc  xmm0, xmm1
movups  xmmword ptr [eax], xmm0
jnz     short loc_43CF50
mov     edi, [esp+8+arg_14]
```

```
mov      eax, [esp+8+arg_10]
add      edi, edi
movups   xmm0, xmmword ptr [ecx]
movups   xmm1, xmmword ptr [eax+edi*8]
mov      eax, [esp+8+arg_C]
aesenclast xmm0, xmm1
movups   xmmword ptr [ecx], xmm0
movups   xmm0, xmmword ptr [edx]
aesenclast xmm0, xmm1
movups   xmm0, xmmword ptr [edx], xmm0
movups   xmm0, xmmword ptr [esi]
aesenclast xmm0, xmm1
movups   xmmword ptr [esi], xmm0
movups   xmm0, xmmword ptr [eax]
aesenclast xmm0, xmm1
pop      edi
movups   xmmword ptr [eax], xmm0
```

'aeskeygenassist' is used to assist the key generation and 'aesimc' is used to perform the invert mix column transformation.

```
call    sub_441A20
movaps  xmm1, [esp+3Ch+var_10]
mov     edx, edi
shr     edx, 2
add     esp, 0Ch
aeskeygenassist xmm0, xmm1, 0
pextrd  ecx, xmm0, 3
xor     ecx, [esi]
lea     eax, [edx+7]
mov     [esp+30h+var_24], offset unk_46FCF4
shl     eax, 4
xor     ecx, 1
add     eax, esi
mov     [esi+edx*4], ecx
mov     [esp+30h+var_20], eax
```
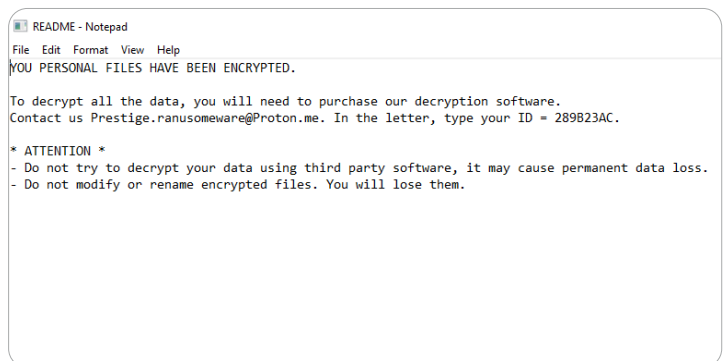
```
aesimc  xmm0, xmmword ptr [edx+ecx*4]
aesimc  xmm1, xmmword ptr [edx+eax*4]
movups  xmmword ptr [edx+eax*4], xmm0
add     eax, 4
movups  xmmword ptr [edx+ecx*4], xmm1
sub     ecx, 4
cmp     eax, ecx
jb      short loc_43D0A0
```

After encrypting the file, Prestige appends '.enc' to the file extension. It also writes the 'enc' to the end of all encrypted files.

```
00000B80   1F EB AF BE 50 2A E0 64 3C 8A 89 D7 0D B2 A6 DE    ë¯¾P*àd<Š‰×.²¦Þ
00000B90   65 36 F4 77 65 7A 60 AE 13 7A 55 2A 44 45 A0 BA    e6ôwez`®.zU*DE º
00000BA0   E3 F6 06 44 1F 51 9D 96 95 DC 6A D0 00 B0 30 10    ãö D Q ÜjÐ.°0
00000BB0   F2 61 76 85 3E 40 80 93 24 35 72 F8 DF DC F3 42    òav…>@€$5røßÜóB
00000BC0   45 81 06 07 04 75 E9 45 29 3B F3 C3 15 56 08 F5    E uéE);óÃ V õ
00000BD0   DC 63 AC FC C0 FC 90 66 AF 8B 8F C8 63 21 2A 7A    Üc¬üÀü f¯‹ Èc!*z
00000BE0   EE 08 1B 56 15 E3 26 8C 08 15 06 34 3D 22 13 C5    î V ã&Œ 4="Å
00000BF0   3C 67 31 A8 26 A7 72 85 21 0D BF 5F 29 82 68 17    <g1¨&§r…! ¿_)‚h
00000C00   C0 51 29 DE BE E9 22 3A 98 C9 17 AE 3E 8A A0 4C    ÀQ)Þ¾é":˜É ®>Š L
00000C10   50 3D 99 04 53 E7 8D 9E 59 F0 31 B7 86 EA B6 7C    P=™ Sç žYð1·†ê¶|
00000C20   B9 05 49 14 D3 89 65 6E 63                         ¹ I Óenc
```

Ransom note

The ransom note 'README' is dropped in the 'C/Users/Public' folder and launched in Notepad every time the user opens any encrypted file. This note contains a unique victim ID and an email address at which to contact the threat actor.

```
README - Notepad
File  Edit  Format  View  Help
YOU PERSONAL FILES HAVE BEEN ENCRYPTED.

To decrypt all the data, you will need to purchase our decryption software.
Contact us Prestige.ranusomeware@Proton.me. In the letter, type your ID = 289B23AC.

* ATTENTION *
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Do not modify or rename encrypted files. You will lose them.
```

Conclusion

This newly discovered ransomware called Prestige targeted transportation and logistics organizations. It may be connected to the ongoing Russian–Ukrainian conflict and aimed to disrupt operations. This ransomware can be delivered to victims in at least three ways, and the first attacks occur with a delay of one hour. In fact, all attacks against Ukraine have these similarities and use the same security weakness and vulnerabilities. This sample is relatively primitive and not secured, but still dangerous.

All found samples analyzed above are successfully detected and stopped by Acronis Cyber Protect, highlighting the importance for businesses to use modern cyber protection solutions.

Malicious websites

An average of 7.7% of endpoints tried to access malicious URLs in Q3 2022, down slightly from 8.3% in Q2.

The largest percentage of blocked malicious URLs at endpoints in November 2022 was in the United States with 20.5%. This was followed by Germany with 9.0% and Italy with 8.6%.

Malicious URLs are very common in emails, but we've also seen an increase in their use in other communication mediums, such as Slack or Teams chat. Attackers are trying to personalize the links further, in an attempt to make them harder to block for all users even if a single instance is successfully detected. Malicious links from phishing emails often contain the targets' email address as an argument. This allows the attacker to verify who clicked the links, and also allows the phishing website to dynamically adapt to the targeted user. For example, some phishing kits will use the domain from the email address and load that main page as a background to the phishing website, providing another token of distraction.

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
July	8.1
August	8.5
September	6.6
October	8.5
November	8.7

Top 10 countries with the most blocked URLs in November 2022

Rank	Country	Percent of blocked URLs in November of 2022
1	United States	20.5
2	Germany	9
3	Italy	8.6
4	Japan	5.4
5	Brazil	5.4
6	United Kingdom	5.2
7	Colombia	4.3
8	France	3.4
9	Canada	3.3
10	Singapore	2.8

Similarly to the malware detection statistics, we normalized these numbers depending on the number of active machines in each country with at least 25 blocked URLs. These normalized breakdowns per region can be found below.

Top 10 countries: normalized blocked URLs by region

Asia

Rank	Country	Regional normalized percent of blocked URLs in November 2022
1	Philippines	19
2	India	16.8
3	Japan	16.2
4	Malaysia	15.4
5	Indonesia	14.8
6	China	14.4
7	Taiwan	13.8
8	South Korea	12.4
9	Hong Kong	12.1
10	Singapore	11.4

EMEA

Rank	Country	Regional normalized percent of blocked URLs in November 2022
1	Kuwait	33.6
2	Saudi Arabia	18.7
3	Slovakia	16.7
4	Bulgaria	16.3
5	Italy	14.1
6	Greece	13.9
7	North Macedonia	13.7
8	Kingdom of Jordan	13.3
9	Portugal	12.9
10	United Arab Emirates	12.4

Americas

Rank	Country	Regional normalized percent of blocked URLs in November 2022
1	Haiti	39.9
2	Panama	36.4
3	Peru	25.6
4	Colombia	23.6
5	Costa Rica	19
6	Dominican Republic	14.4
7	Chile	11.2
8	Brazil	9.9
9	United States	8.1
10	Mexico	7.9

Vulnerabilities in Windows OS and software

We at Acronis continue to see and warn both businesses and home users that new zero-day vulnerabilities — as well as old, unpatched ones — are a top vector of system-compromising cyberattacks. While software vendors try to keep up and release patches regularly, their efforts are often not enough.

Just to take once recent case, a free unofficial patch was released for an actively exploited zero-day that allows files signed with malformed signatures to bypass Mark-of-the-Web (MotW) security warnings in Windows 10 and Windows 11.

As mentioned in our last report, Microsoft now adds a MotW flag to files downloaded from the internet, causing the operating system to display security warnings when the file is launched. But threat actors later started using stand-alone JavaScript files to install the Magniber ransomware on victims' devices, and Windows did not display any security warnings when they were launched — even though they contained an MotW. How is that possible? Because the JavaScript files were digitally signed using a malformed signature, and Windows allows signed files to run.

With this zero-day vulnerability being actively exploited in ransomware attacks, 0patch decided to release an unofficial fix that can be used until Microsoft releases an official security update. In a blog post, 0patch co-founder Mitja Kolsek explained that this bug is caused by Windows SmartScreen's inability to parse the malformed signature in a file. Microsoft later issued an official fix in November's Patch Tuesday.

Microsoft Patch Tuesdays

As always, Microsoft had a lot of work to do patching its popular products. In July, the company released 84 fixes, with four rated as critical. We've listed the most important changes below.

The most severe vulnerability fixed was a remote code execution in the Windows Graphic component. CVE-2022-30221 earned a CVSS rating of 8.8. In order to take advantage of this flaw, an attacker would need to convince the user to connect to a malicious RDP server, which may be not that easy.

Also critical, with a CVSS score of 8.1, was a Network File System RCE named CVE-2022-22029. Similar to previous RCE vulnerabilities, the attacker needs to create an unauthenticated, specially crafted call to a NFS service to trigger remote code execution.

In August, Microsoft released 123 fixes, with 17 rated

as critical. Three of the 17 critical vulnerabilities are elevation of privilege vulnerabilities in Exchange. Exchange has been routinely getting security updates this year, as more and more security flaws are discovered and beng used in cyberattacks. CVE-2022-24477, CVE-2022-24516, and CVE-2022-21980 all have a CVSS base score of 8.0. Microsoft also mentioned that in addition to installing the latest updates, customers vulnerable to this issue would need to enable Extended Protection in order to prevent such attacks.

Another critical vulnerability was exclusive to Windows 11. With a CVSS base score of 8.8, CVE-2022-35804 is likely to be exploited, according to the official advisory. An issue in the Microsoft Server Message Block 3.1.1 (SMBv3) protocol and how it handles certain requests allows attackers who successfully exploit the vulnerability to execute code on the target system.

September brought fewer fixes: 63 in total, with five rated as critical. Of these five, only one is more likely to be exploited. CVE-2022-34718 is a remote code execution vulnerability that received an inopressive and scary CVSS score of 9.8. When exploited, it would allow an unauthenticated attacker to send a specially crafted IPv6 packet to a Windows node where IPSec is enabled. This in turn could enable a remote code execution exploitation on that machine. However, this also means that only systems with the IPSec service running would be vulnerable to this attack.

Another two of the critical vulnerabilities, CVE-2022-34721 and CVE-2022-34722, enable remote code execution in the Windows Internet Key Exchange (IKEv1) protocol. All Windows Servers are affected because they accept both v1 and v2 packets. These vulnerabilities could allow an unauthenticated attacker to send a specially crafted IP packet to a target machine that is running Windows and has IPSec enabled, in turn allowing for remote code execution.

October Patch Tuesday had 89 fixes, with 13 rated as critical. This time, the most critical one was patched in a popular SharePoint site. CVE-2022-41038 received a CVSS base score of 8.8. An attacker must both be authenticated to the target site and also have permission to access and use the Manage List within Sharepoint. This vulnerability, if exploited, allow attackers to run code remotely on SharePoint servers. Additionally, three less severe vulnerabilities were also fixed for SharePoint. CVE-2022-41037, CVE-2022-41036, and CVE-2022-38053 are all RCE vulnerabilities with a CVSS score of 8.8.

Seven of the critical vulnerabilities were patched in the Windows point-to-point tunneling protocol. All received a CVSS base score of 8.1. In order to exploit the vulnerability, an attacker would need to send a specially crafted malicious PPTP packet to a PPTP server. If successful, the attacker can then remotely execute code on the target machine.

The last major vulnerability (CVE-2022-37968) received a max CVSS base score of 10. It's in the cluster connect feature of Azure Arc-enabled Kubernetes clusters. Because the Azure Stack Edge allows users to deploy Kubernetes workloads on devices via Azure Arc, Azure Stack Edge devices are also deemed as vulnerable.

With 68 flaws fixed in total, November 2022's Patch Tuesdays brought fixes for six actively exploited

Windows vulnerabilities. This oncludes 11 critical ones which allow privilege elevation, spoofing, or remote code execution. These figures do not include two OpenSSL vulnerabilities disclosed on November 2, which we will cover later in this report.

So let's check the critical ones. CVE-2022-41128 – Windows Scripting Languages Remote Code Execution Vulnerability requires that a user with an affected version of Windows access a malicious server. An attacker would have to host a specially crafted server share or website, and then convince a user to visit it — typically by way of an enticing email or chat message.

Windows Mark of the Web Security Feature Bypass Vulnerability (named CVE-2022-41091) was fixed as well. Windows Print Spooler Elevation of Privilege Vulnerability (CVE-2022-41073) allows an attacker who successfully exploited this vulnerability to gain system privileges.

Microsoft Exchange Server Elevation of Privilege Vulnerability CVE-2022-41040) was disclosed through Zero Day initiative. If triggered, attacker would be abile to run PowerShell in the context of the system.

Another Exchange vulnerability (CVE-2022-41082) allows remote code execution. As an authenticated user, the attacker could attempt to trigger malicious code in the context of the server's account through a network call.

Google, Adobe, and others' patching activities

In the second half of the year, Google focused on its Chrome browser security fixes, as expected. The browser's recent version 107.0.5304.87/88 contains a fix for the seventh zero-day vulnerability since the start of the year. The previous six were fixed at a rate of approximately one per month, with the three most recent happening in September (CVE-2022-3075), August (CVE-2022-2856) and July (CVE-2022-2294). In some cases, these vulnerabilities were exploited by state-sponsored threat actors for several weeks before Google discovered and patched them.

The high-severity flaw (CVE-2022-3723) fixed in a new version of Chrome stated above is a type confusion bug in V8 Javascript engine. Type confusion vulnerabilities occur when the program allocates a resource, object, or variable using a type and then accesses it using a different, incompatible type, resulting in out-of-bounds memory access. By accessing forbidden memory regions from the context of the application, an attacker could read sensitive information from other apps, cause crashes or execute arbitrary code.

Adobe had a lot of work to do in the past five months. Their most recent batch of security patches included fixes for 29 documented vulnerabilities across multiple enterprise-facing products that hackers could exploit to take complete control of vulnerable machines. These vulnerabilities could expose both Windows and macOS users to arbitrary code execution, arbitrary file system write, security feature bypass and privilege escalation attacks. According to an Adobe critical-rated advisory, a total of 13 ColdFusion flaws were fixed, including some carrying a CVSS 9.8/10 severity rating.

The Adobe Commerce and Magento Open Source flaw (CVE-2022-35698) was described by vendor as a cross-site scripting (stored XSS) bug with a CVSS severity rating of 10.0.

The Adobe Dimension product also had bugs that scored a maximum severity rating. The company addressed nine documented threats, and noted that both Windows and macOS users are at risk of code execution and memory leak attacks.

Before that, Adobe released patches for 25 documented security vulnerabilities that expose users to malicious attacks. Acrobat and Reader updates addressed multiple critical and important vulnerabilities. Successful exploitation could lead to arbitrary code execution and memory leaks. Adobe also released a bulletin with details on four security defects in the Adobe Illustrator 2022 software.

In a September security update, Adobe addressed 63 vulnerabilities across seven products. All of these vulnerabilities received a CVSS base score between 5.3 and 7.8, with 35 of them being critical. Exploitation could lead to a number of problems like arbitrary code execution, security feature bypass, arbitrary file system read and memory leak.

The most critical case was Adobe Bridge (APSB22–49) for Windows and macOS, where 10 out of 12 patched vulnerabilities were marked as critical. Adobe InDesign (APSB22–50) for Windows and macOS was in a bad spot before 18 vulnerabilities were fixed, including 8 critical ones. Last but not least were Adobe Photoshop 2021 and 2022 (APSB22–52) for Windows and macOS, where 10 vulnerabilities were patched — nine of which were critical.

Other vendors also released important updates. The OpenSSL Project patched two high–severity security flaws in its open–source cryptographic library used to encrypt communication channels and HTTPS connections. The vulnerabilities (CVE–2022–3602 and CVE–2022–3786) affect OpenSSL version 3.0.0 and have been addressed in OpenSSL 3.0.7.

CVE–2022–3602 is an arbitrary 4–byte stack buffer overflow that could trigger crashes or lead to remote code execution (RCE), while CVE–2022–3786 can be exploited by attackers via malicious email addresses to trigger a denial of service state via a buffer overflow. OpenSSL also provided mitigation measures requiring admins operating TLS servers to disable TLS client authentication until the patches are applied.

Similarly, Cisco warned customers that two security vulnerabilities in the Cisco AnyConnect Secure Mobility Client for Windows are being exploited in the wild. The two security flaws (CVE–2020–3433 and CVE–2020–3153) enable local attackers to perform DLL hijacking attacks and copy files to system directories with system–level privileges. Following successful exploitation, the attackers could execute arbitrary code on the targeted Windows devices with system privileges. Both vulnerabilities require authentication, with the attackers being required to possess valid system credentials.

This was just a small glimpse into the huge number of vulnerabilities discovered and fixed in the last five months. We know that ransomware attackers have taken advantage of more than 150 vulnerabilities during this same period, emphasizing once again how important it is to patch on time and have vulnerability assessment functionalities in place to protect businesses and home users.

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

Modern cyberattacks, data leaks, and ransomware outbreaks all show the same thing: cybersecurity is failing. This failure is the dual result of weak technologies and human error, often caused by clever social engineering.

Even if your backup solution is functional and wasn't compromised, it often takes hours and days after a cyber incident to restore systems (including data) to an operational state. Backup is essential for when cybersecurity solutions fail, but at the same time these tools can be compromised, disabled or simply perform slowly — all of which causes businesses to lose a lot of money to downtime.

To solve these problems, we recommend an integrated cyber protection solution like Acronis Cyber Protect that combines anti-malware, EDR, DLP, email security, vulnerability assessment, patch management, RMM and backup capabilities into a single agent running under a family of Windows operating systems. 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. Thanks to its single agent, the solution knows when data is lost and needs to be restored.

This isn't possible with an anti-malware solution that runs a separate agent from your backup solution. Other cybersecurity products may stop the threat, but can't restore any data that's already been lost. A backup agent won't automatically know about the situation, 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, multi-layered cybersecurity functionality.

That said, companies and home users shouldn't forget about basic security rules even if they use modern solutions like Acronis Cyber Protect.

Patch your OS and apps

This is crucial, as many 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, allowing 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 have Acronis Cyber Protect and/or don't use any patch management software, the task becomes much harder. At the very least, you need to ensure that Windows gets all needed updates and that they're 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.

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

Themed phishing and malicious websites appear in large numbers every day. While these are sometimes filtered out on a browser level, cyber protection solutions like Acronis Cyber Protect also offer dedicated URL filtering functionality. Malicious links can come from anywhere — instant messenger apps, email, forum posts, etc. Never click links you don't need to click, or that you didn't expect to receive.
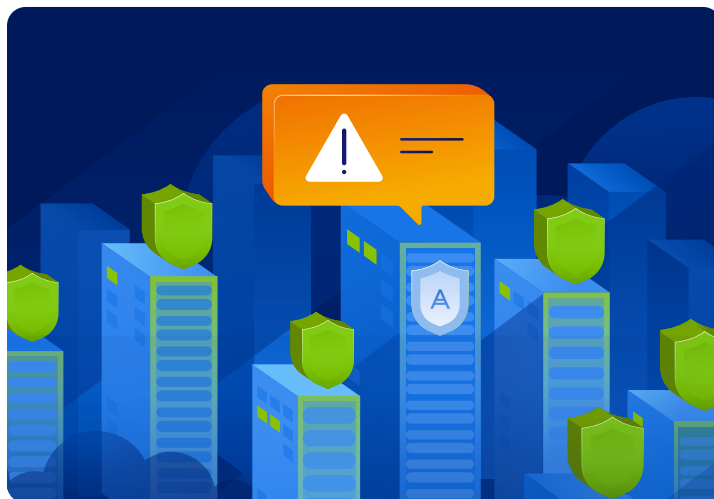
Malicious themed attachments can also be delivered by email. Always check where messages with attachments really originated from, and ask yourself if you were expecting it or not. In any case, before you open an attachment, it should be scanned by your anti-malware solution.

Use a VPN while working with business data

Whether you connect to remote company sources and services, or if your work doesn't require those activities and you just need to browse some web resources and use telecommunication tools, use a Virtual Private Network (VPN). VPNs encrypt all your traffic, making it secure against

attackers who may attempt to capture your data in transit.

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.

Ensure your cybersecurity is running properly

Acronis Cyber Protect uses many well-balanced and tuned security technologies, including multiple detection engines. We recommend using this solution in place of embedded Windows or macOS security tools.

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 needs to check for, and retrieve, updates frequently — daily or ideally hourly.

- A product should be connected to its cloud detection mechanisms, in the case of Acronis Cyber Protect to the Acronis Cloud Brain. It is on by default but you need to be sure that the internet is available and not accidentally blocked for antimalware software.

- On-demand and on-access (real-time) scans should be enabled and react on every new software installed or executed.

Additionally, don't ignore messages coming from your anti-malware solution — read them carefully, and ensure that the license is legitimate if you're using a paid version from a security vendor.

Keep your passwords and your working space to yourself

Security tip number one: make sure that your passwords — and your employees' passwords — are strong and private. Never share passwords with anyone.

Use different and long passwords for every service; password manager software can help you remember them. One way to create strong passwords is to come up with a long phrase that you can easily remember. Eight-character passwords are easily brute-forced nowadays. Where possible, use multi-factor authentication for an extra layer of security.

Even when working from home, do not forget to lock your laptop/desktop PC and limit access to it. Other individuals can easily view, steal or delete (even accidentally) sensitive files on an unlocked system.

Acronis cybersecurity trends and predictions for 2023

Today's world is more digitally dependent than ever. IT environments are becoming increasingly complex, and small flaws in resilience can have a major impact on an organization's ability to continue operating following a security incident or breach.

Here are ten trends that are likely to shape the cybersecurity landscape in 2023:

1. Authentication and identity management systems in the crosshairs

Authentication and Identity Access Management (IAM) will be successfully attacked more frequently. Many attackers have already started to steal or bypass multi-factor authentication (MFA) tokens. In other situations, overwhelming targets with MFA requests can lead to successful logins without the need of a vulnerability. Recent attacks against Okta and Twilio showed that such external services are getting breached too. This is, of course, on top of a years-long problem with users selecting (and reusing) weak passwords. It's all the more important to ensure that MFA is configured properly, and that minimum required access rights are given to all company employees.

2. Ransomware will bring even more damage

The ransomware threat is still going strong and evolving. While we are seeing a shift towards more data exfiltration, the main actors are continuing to professionalize their operations.

Most of the large players have expanded to macOS and Linux, and are also looking at the cloud environment. New programming languages like Go and Rust are becoming more common and require adjustments in the analysis tools.

The number of attacks will continue to grow as they remain profitable, especially when cyber insurance covers some of the impact. This will undoubtedly increase the cost of cyber insurance premiums even further. Attackers will increasingly focus on uninstalling security tools, deleting backups, and disabling disaster recovery plans wherever possible. Living-off-the-land techniques will play a major role in this.

3. Data breaches for the masses

Information-stealing malware, such as Raccoon and RedLine, is becoming the norm for infections. Stolen data often includes user credentials, which are then sold via initial access brokers to facilitate future attacks. The growing number of blobs of data combined with the complexity of interconnected cloud services will make it harder for organizations to keep track of their data. The requirement for multiple parties to access the data makes it harder to keep it encrypted and protected. A leaked API access key, for example on GitHub or the mobile app, can be enough to steal all data. This will lead to advances in privacy-friendly computing.

4. Phishing expands beyond email

Malicious emails and phishing attacks continue to be sent by the millions. Attackers will continue to try to automate and personalize their attacks using previously leaked data. Socially engineered scams, like Business Email Compromise (BEC) attacks, will increasingly spread to other messaging services (SMS/texting, Slack, Teams chat, etc.) to avoid filtering and detection. Phishing, on the other hand, will continue to use proxies to capture session tokens, steal MFA tokens, and use diversions like QR codes to further hide itself.

5. Not-so-smart contracts

No end is in sight to the attacks on cryptocurrency exchanges and smart contracts on various blockchains. Even nation-state attackers are trying to steal hundreds of millions in digital currencies. The more sophisticated attacks on smart contracts, algorithmic coins and DeFi solutions continue, in addition to classic phishing and malware attacks against their users.

6. Living off your infrastructure

Service providers are increasingly being attacked and compromised. The attackers then abuse the installed tools like PSA, RMM or other deployment tools to "live off that land." This threatens not only managed IT service providers, but also consulting companies, first-level support organizations and similarly connected partners. Outsourced insiders are often deployed as the weakest link in a target organization without the need to painstakingly craft software supply chain attacks.

7. Calling from within the browser

There will be more attacks in or through the browser, conducting the attacks from within sessions. Malicious browser extensions can swap target addresses of cryptocurrency transactions or steal passwords in the background. There is also a trend in hijacking the source code of such tools and adding backdoors through the GitHub repository. On the other side, websites will continue tracking users with JavaScript and oversharing session IDs across HTTP referrers to marketing services. Attackers will expand on the Formjacking/Magecart techniques, where small added snippets steal all the information in the background of the original website. With the increase of serverless computing, analysis of such attacks can become more complicated.

8. Cloud automation through APIs

There has already been a tremendous shift of data, processes and infrastructure to the cloud. This will continue with more automation between different services. Many IoT devices will be part of this large hyper-connected cloud of services. This will result in many APIs being accessible from the internet, increasing the risk of large-scale automated attacks.

9. Business process attacks

Attackers will always come up with new ideas about how to modify business processes for their own benefit/ profit — like changing the receiving bank account details in an organization's billing system template, or adding their cloud bucket as a backup destination for the email server. These attacks often don't involve malware but require close analysis of user behavior, much like the growing number of insider attacks.

10. AI everywhere

AI and ML processes will be used by corporations of all sizes and sectors. Advances in the creation of synthetic data will further fuel identity fraud and disinformation campaigns using deepfake content. A more worrisome trend will be the attacks against the AI and ML models themselves. An attacker may try to use weaknesses in the model, implant bias on purpose into data sets or simply use the triggers to flood IT operations with alerts.

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