Acronis

Report
2022

Acronis Cyberthreats Report 2022

At war with ransomware gangs: a year in review

Acronis Cyberthreats Report 2022

Table of contents

Authors:

Alexander Ivanyuk

Senior Director, Product and Technology Positioning, Acronis

Candid Wuest

Vice President of Cyber Protection Research, Acronis

Introduction and Summary

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

Since its founding in 2003, Acronis has been a recognized leader in data protection. In response to the rise of cyberthreats targeting backup files, agents, and software, the company introduced its innovative Acronis Active Protection anti-ransomware technology in 2016, making it the first data protection vendor to integrate a native anti-ransomware defense in its backup solutions. That machine-intelligence- and behavior-based detection technology has since been expanded to address all forms of malware and other potential cyberthreats.

Our flagship product, Acronis Cyber Protect Cloud, empowers service providers with integrated backup, disaster recovery, antivirus, anti-malware, email security, URL filtering services, and endpoint protection management capabilities – enabling them to deliver comprehensive cyber protection services to their clients. The same technology is available directly to businesses as Acronis Cyber Protect 15.

This report covers the threat landscape, as encountered by our sensors and analysts during the second half of 2021.

Check out the findings for the first half of 2021 in our **Acronis Cyberthreats Report: Mid-year 2021**.

This report represents a global outlook and is based on over 650,000 unique endpoints distributed around the world. The main focus here is on threats for Windows operating systems, as they are much more prevalent when compared with macOS. We will see how the situation develops and may include data on macOS threats in the next report, as there has been a recent spike in these threats.

The top five numbers of H2 2021:

- The most attacked countries by malware in Q3 2021 were the U.S., Germany, and Canada.
- 376,000 URLs were blocked on the endpoint by Acronis in October alone.
- Blocked phishing emails increased by 23% and blocked malware emails increased by 40% from Q2 to Q3, 2021.
- Damages from ransomware are expected to be more than $20 billion U.S. by the end of 2021 (**Cybercrime Magazine**).
- Only 20% of companies reported that they didn't get attacked — as opposed to 32% last year, as attacks are increasing in frequency.

Among the cybersecurity trends we saw in H2 2021:

- Ransomware continues to be the number one threat to big and medium businesses, including government, healthcare, and other critical organizations.
- MSPs are under attack, and liability questions have been raised.
- Vulnerabilities are being widely exploited.
- Linux and macOS have been getting more and more attention from cybercriminals.

What you will find in this report:

- Top security/threat trends we observed in H2 2021.
- Why do we see more and more threats to cryptocurrencies.
- Why MSPs and alternative operating systems are increasingly under threat.
- General malware statistics and key families reviewed.
- Ransomware statistics with a deep-dive analysis of the most dangerous threats.
- Which vulnerabilities contribute to the success of attacks.
- Our security recommendations and threat forecast for 2022.

Key cyberthreats and trends of 2021

Part 1

1. Ransomware is at all-time high

The second half of 2021 was rich in ransomware gang activities, and the whole industry was overwhelmed with a number of big cases. These ransomware gangs were not only very active, but started to become much more aggressive. For instance, Ragnar Locker ransomware group announced that they would publish all stolen data immediately if the victim talks to the police or involves any kind of professional help. These cybercriminals claim that professional ransom negotiators make it worse for the victim. If the victims still decide to involve these ransom negotiators, the attackers are confident they will find out one way or another. Last year, Ragnar Locker compromised Campari, and then paid for Facebook ads in order to publicly pressure their victim to pay a $15 million U.S. ransom, or else 2TB of their stolen data would be published.

However, industry and law enforcement officials have put up a real fight. With the aid of Europol, the French National Gendarmerie, the Ukrainian National Police, and the United States Federal Bureau of Investigation, two ransomware operators have been arrested. These two operators are responsible for extorting up to €70 million in ransom demands. Police seized $375,000 U.S. in cash, two luxury cars, and $1.3 million U.S. in cryptocurrency. While it is not currently known who the duo ran ransomware operations for, they are suspected of carrying out coordinated attacks against industrial groups in both Europe and North America. The United States Department of Justice announced charges against the REvil ransomware affiliate responsible for the attack against Kaseya MSP platform on July 2nd, and seizing more than $6 million U.S. from another REvil partner. The DOJ also announced that law enforcement seized $6.1 million U.S. from yet another REvil ransomware affiliate. These are just some of the law enforcement operations that were carried out against ransomware groups. While members of two operators have been arrested, after a couple of months they either resurfaced or changed their names, and this is besides the hundreds of ransomware operators that continue to steal and encrypt data.

In fact, it has become so bad, that in November, the U.S. announced a bounty reward program that would reward up to $10 million U.S. for each of these REvil (Sodinokibi) and Darkside ransomware members. This bounty was being offered as part of the Department of State's Transnational Organized Crime Rewards Program (TOCRP), which expects to get information that will lead to the arrest or conviction of individuals in transnational organized crime groups. A reward of $5,000,000 U.S. is also being offered for information leading to the arrest of any individual who attempts to participate in both of these ransomware gangs.

The **FBI recently announced** some surprising numbers regarding the Ako or ThunderX ransomware gang, also known as Ranzy Locker, following a recent rebranding. According to the FBI, the gang was responsible for 30 U.S. companies, across multiple industries, being compromised this past year. The alert shows that regardless of whether your company is in construction, manufacturing, academia, information technology, transportation, or any other sector, everyone is at risk. The gang uses brute force against RDP credentials and Microsoft Exchange exploits to gain access to their victims' infrastructure.

Old gangs

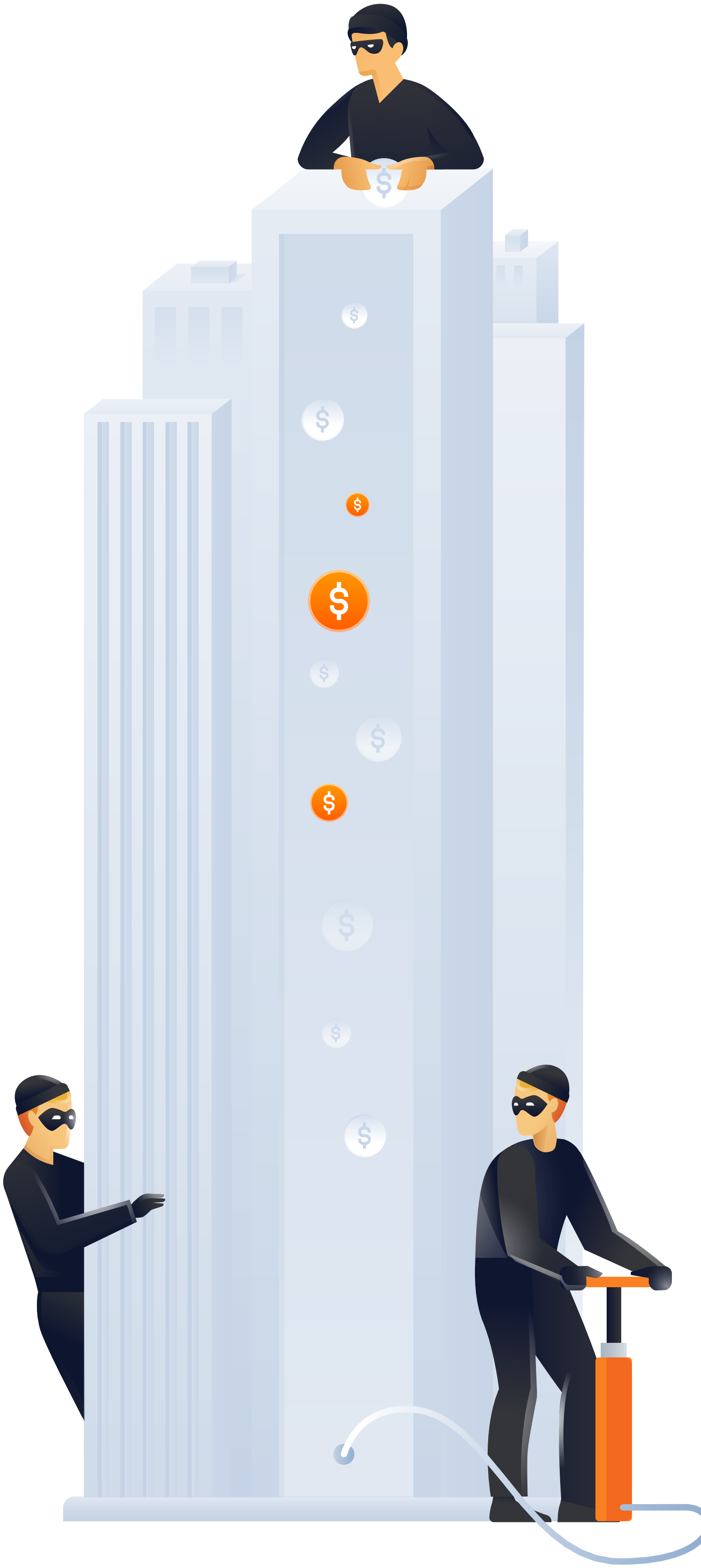
Let's take a look at **some of the big cases** we saw from July to November. CISA issued an advisory after more than 400 incidents involving Conti had occurred. Conti's ransomware first appeared sometime in May of 2020, and they continue to be a successful extortionist.

For instance, Japan-based electronics multinationals JVCKenwood and Sandhills Global have been hit with Conti ransomware. Conti is claiming to have stolen 1.7TB of data and is demanding $7 million U.S. in ransom. Conti was also ransoming Graff Jewelers data, comprising of 11,000 clients, for "tens of millions of pounds." Graff has annual revenue of over $600 million U.S. To date, Conti has already leaked 69,000 of Graff's confidential documents, including invoices, receipts, and credit notes. And one of Europe's largest customer care and call center providers, GSS, and iconic wedding dress designer Vera Wang Group have been hit by Conti ransomware as well.

A recent research by Prodaft uncovered some interesting details about the backend servers used by the Conti group. This helped to discover that the Conti group received payments of $10 million U.S. in September and already more than $7.5 million U.S. in November.

The multinational tech consulting firm Accenture has become the latest victim of the LockBit ransomware gang. With more than half a million employees and annual revenue of over $44 billion U.S., Accenture is a Fortune Global 500 company that provides services to major clients including Cisco, Alibaba, and Google. LockBit appears to have gotten away with as much as 6TB of data in the attack and is demanding a ransom of $50 million U.S. Accenture has since restored data from backups and has stated that there was no significant impact to normal operations.

Another big victim of the LockBit extortion gang is Bangkok Airways, which employs more than 3,000 people in 11 countries, and has an annual revenue of over $685 million U.S. LockBit claims to have published 200GB of Bangkok Airways' data to a legitimate file sharing service, and the airline has confirmed that the stolen data includes passengers' full names, nationalities, genders, phone numbers, email addresses, passport information, and other sensitive data.



New actors

The relatively new Hive ransomware gang just hit electronics retail giant MediaMarkt with an initial ransom demand of $240 million U.S. in November, causing IT systems to shut down and store operations to be disrupted in both the Netherlands and Germany. The demanded ransom is not a surprise when keeping in mind that MediaMarkt is Europe's largest consumer electronics retailer, with over 1,000 stores in 13 countries. MediaMarkt has approximately 53,000 employees and total annual sales of €20.8 billion.

Prior to that attack, the Hive gang developed specific versions of its ransomware to encrypt both Linux and FreeBSD. As 96.3% of the world's top 1 million servers now run on Linux, and 90% of all cloud infrastructure operates on Linux, this is a very logical move for the bad guys. Babuk, DarkSide, HelloKitty, and other ransomware gangs all have all created Linux encryptors.

The Hive gang has also attacked the Missouri Delta Medical Center. With that attack, they stole 95,000 patient records — 400GB in total — including confidential information such as patient names, social security numbers, medical records, and phone numbers. Another of their victims from the health industry was the non-profit Memorial Health System. Memorial Health System has 64 clinics, over 3,000 employees, and all evidence indicates that over 200,000 patients' data was stolen.

Another newcomer that started operations in July was BlackMatter ransomware group, which is believed to have emerged out of the DarkSide group — although at the beginning of November, they announced they were allegedly shutting down due to "pressure from the authorities." The project had a short lifespan, but did a lot of damage during that time. For example, The BlackMatter ransomware group compromised the agriculture company New Cooperative in Iowa. According to New Cooperative, 40% of America's grain production runs through their software, and they are a farm service provider having an estimated annual revenue of between $500 million and $1 billion U.S., and are part of the "16 critical sectors" outlined by the Biden administration. They had 1,000 GB of data stolen, which is being ransomed for $5.9 million U.S.

BlackMatter also attacked Japan-based tech manufacturer Olympus, which had been compromised twice during September and October. In response to the attack, affected systems were taken offline, and external partners were notified. This attack affected systems in the U.S., Canada, and Latin America.

Yet another of BlackMatter's victims was Marketron. Marketron maintains servers for more than 6,000 customers in the media industry and has an estimated revenue of $25.5 million U.S.

At some point during these past few months, BlackMatter added a module to encrypt Linux VMware ESXi servers. Their ransomware added a VMware ESXi library to their ELF 64-bit encryptor. This has enabled them to list all VM hosts and then shut them down before encrypting their images. The group was also openly seeking people who could provide access to corporate networks of companies with more than $100 million U.S. in revenue.

All told, the BlackMatter group has compromised at least 40 companies since July, though most likely a number of others that have not yet been disclosed publicly.

AVOS Locker ransomware, which we have analyzed in detail in another section of this report, was another prominent newcomer to the crime scene. During this reporting period, their operators claimed to have stolen sensitive data from Pacific City Bank. Pacific City Bank is the third-largest bank focusing on the Korean-American community, with an estimated revenue of $67.2 million U.S.

AVOS Locker also compromised the Taiwanese hardware manufacturer Gigabyte, known for its computer motherboards. This was the second incident within three months for the company. The AVOS Locker group then published 15MB of stolen data as proof of their attack, which contained passwords and usernames, employee payroll details, passport scans, signed NDAs with customers, and other confidential information.

LockFile ransomware has also emerged, taking advantage of vulnerabilities like PetitPotam and ProxyShell. LockFile was first spotted attacking a U.S. financial organization and has quickly set itself apart from the other ransomware gangs. It has been largely targeting organizations in the U.S. and Asia, but has also been seen around the world, targeting victims in the finance, manufacturing, legal, travel, engineering, and business services sectors. The ransomware uses an intermittent file encryption technique to evade detection similar to BlackMatter, LockBit 2.0, and DarkSide; but LockFile encrypts only every other 16 bytes of a file.

2. Phishing and malicious emails remain the main infection vector

The Acronis CPOCs blocked 376,000 phishing and malicious URLs in October 2021. This constitutes a massive spike over a lower Q3 with an average of 58,000 per month.

Unfortunately many emails with malicious content, especially URLs, still get through basic email filters and end up at the user's endpoint. We have also seen attackers embedding QR codes to malicious URLs into phishing emails. Many security solutions can not handle QR codes yet, but end users are conditioned to use their smartphones to follow the links. This is another reason why it is important to have a multi-layered defense approach.

Month	Blocked URLs
July	57,588
August	33,012
September	83,804
October	376,451

With Acronis Advanced Email Security, powered by Perception Point, we saw an increase of 23% of phishing emails being blocked in Q3 as compared to Q2, while the number of malware emails increased by 40% in the third quarter.

A recent study for the **Acronis Cyber Readiness Report 2021** showed that IT administrators ranked phishing as the top threat they encounter, with 58% of respondents saying that they have received such attacks. Still, only 20% of them prioritized URL filtering solutions for their IT security stack.

Also, a recent study by the Ponemon Institute has revealed some alarming statistics about the costs of phishing attacks. The study takes a look into all costs associated with these attacks, including recovery and loss of productivity — which actually cost more than payouts made to cybercriminals. The cost of a phishing attack has risen sharply over the past six years — now costing large U.S. companies $14.8 million U.S. annually, which works out to about $1,500 U.S. per employee. By comparison, in 2015, this figure was $3.8 million U.S. annually. This means that in just six years, the cost of phishing attacks has nearly quadrupled. During 2020, business email compromise (BEC) attacks costs rose significantly, with more than $1.8 billion U.S. stolen from U.S. organizations by impersonating employees, partners, or vendors — among other common tactics.

Big cases

A **large credential phishing campaign** using open redirector links to bypass security software is currently underway. This latest campaign couples well-known branding such as Zoom, with open redirect links to lure individuals into interacting with those links. These links further redirect users to CAPTCHA verification pages, which adds an air of legitimacy and makes automated security analysis more difficult, before it then prompts users for credentials.

A phishing operation dubbed BulletProofLink has been discovered to be providing attackers with everything they need for phishing attacks. This operation provides everything from phishing kits and templates to hosting services and other useful tools. The service provides more than 100 phishing templates that copy known brands such as Microsoft, and even creates unique subdomains to associate with their campaigns — over 300,000 of which were generated in a single run. BulletProofLink provides services for as much as $800 per month, while individual services can cost much less. For instance, a one-time hosting link may only cost $50, and first-time customers even receive a 10% discount.

Another brand new phishing attack is disguising itself as a UPS email that appears legitimate, but instead exploits a vulnerability in UPS's main website. All of the links in the email are legitimate except for the button that opens the track package page. It contains a malicious payload that takes advantage of an XSS vulnerability in order to eventually download a malicious Word document that in turn delivers another malicious payload. Attacks like this demonstrate just how crafty attackers can be, and how tricky it can be to spot a phishing email.

A malware group known for pushing TeamTNT malware has a new campaign dubbed Chimaera, which has been indiscriminently attacking multiple operating systems. TeamTNT has added a number of tools to their arsenal, including shell scripts, a cryptominer, IRC, open-source tools, and more. More than 5,000 infections globally have been attributed to the group, and open source tools are now being used by TeamTNT to steal usernames and passwords, and have been attacking Windows and multiple Linux distributions, as well as AWS, Docker, and Kubernetes. In the past, they had also been observed attacking MacOS systems.

Phishing does not need to be that advanced in order to be successful. A British teen earned more than $2.7 million U.S. with a fraudulent replica of the popular Love2Shop gift card online shop. The site was being run as a phishing site, collecting all payment card details and other private data entered on the site, while victims did not receive their promised gift cards. Law enforcement subsequently found details of 12,000 payment cards and around 200 PayPal accounts in the teen's possession. The teen earned $440,000 U.S. from the website within a few weeks, which he then invested in Bitcoin that grew 10 times to a value of around $3 million U.S.

As cryptocurrencies become more and more popular, we see and will see more attacks on crypto exchanges and cryptocurrencies owners. For example, the crypto exchange Coinbase has recently disclosed that at least 6,000 customers had fallen victim to a phishing campaign earlier this year — resulting in funds being stolen from their accounts. The attacker obtained the email addresses, passwords, and phone numbers of Coinbase customers, and the company believes this was due to social engineering, such as an email phishing attack. Once logged in to customer accounts, the attacker was able to steal funds from these accounts. While Coinbase requires two-factor authentication, accounts using SMS for that verification were vulnerable due to a flaw in the SMS Account Recovery process. The flaw has since been patched, but not before funds were removed from accounts. Coinbase has chosen to reimburse customers, but most victims of phishing aren't so fortunate. Acronis Advanced Email Security scans all emails coming into your inbox and blocks phishing and other malicious emails from even being seen. This keeps your accounts and data safe by stopping an attack before it can even begin.

3. Linux and macOS under attack

We have already mentioned some Linux ransomware, but this is not the only emerging threat for this operating system. Bad guys have been paying more and more attention to Linux, as there are dozens of millions of machines connected to the internet — primarily servers — which provides more than enough motivation to develop new malware. And in addition to ransomware, cybercriminals are focusing on cryptominers, trojans, and more sophisticated malware, like rootkits.

Currently, a previously unrecognized Linux malware family is targeting organizations in Southeast Asia. The threat is being tracked as FontOnLake or HCRootkit. FontOnLake is a modular rootkit that appears to be in active development, and includes abilities like remote access enablement, credential theft, and acting as a proxy server. Attacks using FontOnLake appear to be targeted and are designed to collect data, among other malicious actions. The malware can evade detection from many traditional antivirus solutions and replaces common legitimate binaries with modified ones on infected systems. Though this rootkit has managed to stay largely out of sight since as early as May 2020, it can now be detected by the multi-layered detection engines included in Acronis Cyber Protect for Linux — keeping your data and systems safe from this and other Linux malware.

Cobalt Strike, a legitimate tool used by security researchers for penetration testing, has been found in the wild supporting Linux-based attacks. Year-over-year, Cobalt Strike has seen 161% increased use by cybercriminals. The tool has been used to target tens of thousands of organizations and was used in the SolarWinds attack. Until recently, Cobalt Strike suffered from the fact that it didn't work on anything but Windows. But since August, attackers have utilized an implementation named Vermilion Strike that targets 90% of all cloud servers. This ELF-formatted malware follows in the footsteps of Geacon, an open-source, Golang-based version of Beacon.

As with any other operating system, Linux distributives have vulnerabilities that have been actively exploited by malware. And new ones have been regularly discovered — for instance, in October, a major security flaw in the Linux Kernel's Transparent Inter Process Communication (TIPC) module had been disclosed and a patch made available. This vulnerability (marked as CVE-2021-43267) can be exploited either locally or remotely to gain kernel privileges — thus allowing an attacker to compromise the entire system. The TIPC module exists within a kernel module packaged with all major Linux distributions, but it is not loaded automatically by the system.

Apple's macOS has also been a target for cybercriminals, as Macs' market share is growing. Some Windows malware has been ported to work on Macs, as well as some specific malware created for utilizing macOS vulnerabilities. And new vulnerabilities are regularly being discovered and patched; for instance, at the end of October, Apple patched a vulnerability in the macOS Big Sur and Monterey operating systems that could be abused to bypass the SIP security feature and install kernel rootkits. Ironically, a vulnerability codenamed Shrootless has been found by a Microsoft researcher — according to whom the vulnerability resides in system_installd, the macOS software installation daemon.

Summary

As we can see, main threats and malware strains continue their malicious work in the second half of 2021.

Ransomware tactics in particular are undergoing a lot of transformation due to the heavy focus of law enforcement as well as the millions of profits that are at stake. In addition, more and more attacks are targeted to alternative OSes — especially Linux versions that are run on server hardware. In this constant state of emergency, it is very important to have proper multilayered cyber protection, which will cover as many verticals and operating systems as possible, but that will also be able to restore machines and data if something slips through. **Acronis Cyber Protect** is exactly this type of solution: aimed to provide an excellent level of protection along with best in the industry recovery time for both machines and data.

General malware threats

Part 2

In Q3 2021, an average of 13.6% of Acronis' clients had at least one malware attack successfully blocked on their endpoints. The numbers nearly doubled in October to 25.3%, indicating a spike for Q4. These high percentages show that many threats still make it to the endpoint, despite awareness training and patching performed by organizations.

Month	Percentage of clients with blocked malware
January	16.1%
February	13.7%
March	15.9%
April	16.1%
May	13.6%
June	12.1%
July	13.2%
August	11.7%
September	15.9%
October	25.3%
November*	20.5%

One recent study by Acronis for our **Cyber Readiness Report 2021** showed that 37% of responding IT administrators acknowledged they had encountered malware attacks in the last year — ranking malware attacks at number three behind phishing and DDoS attacks. This survey result is surprising in that although the number grew from 22% last year to 37%, it still appears low and suggests that companies either have very good filtering — such as email filtering — in place to keep most malware out; or, more likely, that they are missing full visibility about all attacks.

The number of new malware samples appearing in the wild decreased slightly in 2021. For instance, the independent malware testing lab AV-Test recorded over 600,000 new malware samples per day in Q1 2021, but in Q2 this decreased by 17% to 507,000 per day. And in Q3, the number decreased by another 28% to 363,000 per day. These decreases could be either the result of some groups shifting to a bit more targeted deployment, or the arrests of active email malware groups such as Emotet — though Emotet made a comeback in November and will most likely drive up Q4 numbers.

The country with the most clients experiencing malware detections in Q3 2021 was the **United States with 27.2%**, followed by **Germany with 11.5%**, and **Canada with 5.9%**, which are very similar to the Q2 numbers.

The following are the top 10 malware families we observed and tracked in H2 2021:

Family name	Percentage
Trickbot	7%
AgentTesla	6%
NJrat	5%
Remcos	5%
Formbook	4%
Jupyter	3%
RedLineStealer	3%
XMRig	3%
Zloader	2%
Qbot	2%

Trojans and Illicit cryptomining

On the general malware side, we've encountered some interesting and alarming developments as well. For instance, one of the world's largest botnets, with over 1.6 million infected devices, has been discovered in the wild. The botnet has been dubbed 'Pink' due to the number of function names in its code that begin with the word. The primary goals of the Pink botnet are to launch denial-of-service (DoS) attacks and to insert advertisements to be viewed by unsuspecting victims who are just browsing HTTP websites. The botnet uses encrypted communications with a number of services, like GitHub, command-and-control (C2) servers, and peer-to-peer (P2P) networks to control the bots.

Another botnet, MyKings, has been around for at least five years and is as active now as it ever has been. New research has shown just how busy the botnet has been and has uncovered its use of infected computers to mine or steal cryptocurrency through one of two techniques. One such technique is to install a cryptominer on the system to use victim computers to mine cryptocurrency maliciously, while the other tactic is to use their clipboard stealer trojan to detect when crypto wallets are copied and replace the clipboard contents with a crypto wallet under the attacker's control. As a result, MyKings has raked in at least $24.7 million U.S., and reports as far back as 2017 showed them earning $2.3 million U.S. in Monero each month, with over 500,000 infected computers.

With the growth of crypto rates, cybercriminals started to improve and develop new malware aimed to steal cryptocurrencies. Researchers have identified a new strain of the Golang crypto-worm that is now 15% faster and more efficient. Attackers using this worm are scanning for vulnerabilities in XML-RPC provided by WordPress, and Oracle WebLogic Servers. Upon successful exploitation, XMRig is then installed along with a worm that spreads it to other sensitive directories.

Another example is HolesWarm malware, which exploits more than 20 known vulnerabilities in Linux and Windows servers in order to spread. Over 1,000 servers have already been compromised in 2021, especially in cloud environments, and the numbers are still increasing. In this case, once a server is compromised, a Monero cryptocurrency miner is installed to generate profits for the cybercriminals.

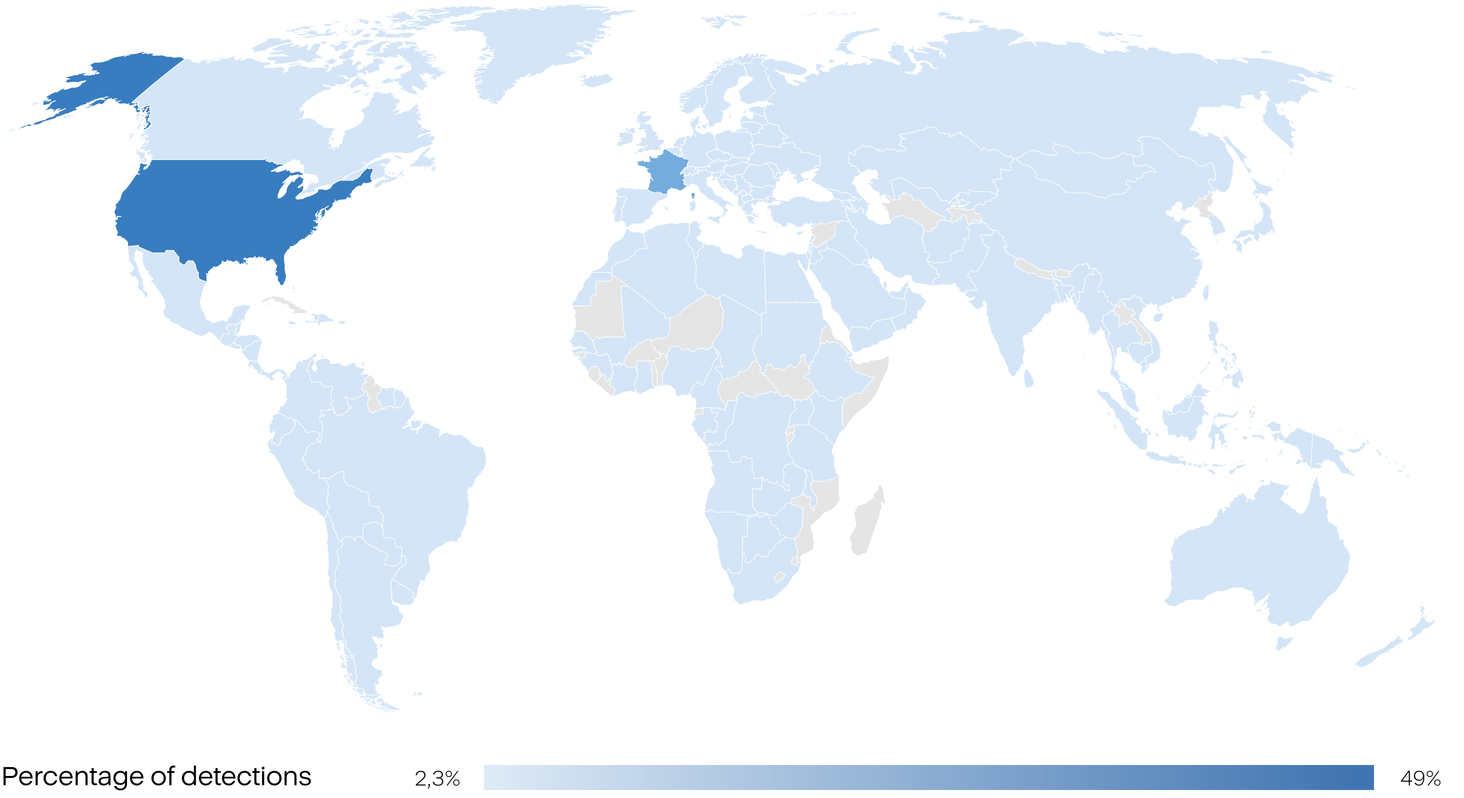
More sophisticated threats were also spotted in the second half of 2021. The North Korean APT group known as Lazarus, responsible for the infamous WannaCry ransomware attack and the 2014 attack on Sony Pictures, has been targeting the IT supply chain, according to recent research. A new variant of the BLINDINGCAN remote access trojan (RAT) has been used in recent attacks, which have been targeting both a Latvian IT company and a South Korean think tank. BLINDINGCAN allows the attacker to capture information about installed disks, the computer's operating system and processor information, and other data, as well as to create and run processes and files, among other functions.

A new fileless malware campaign known as Water Basilisk is using a new variant of HCrypt to install several remote access trojans (RATs) onto victim computers. HCrypt is a popular crypter-as-a-service, used by attackers to install RATs, because its fileless nature makes it more difficult to detect. The crypter relies primarily on VBScript and Powershell commands to download and install malicious payloads onto victims' systems. The final stage of this particular attack installs common RATs, such as NjRat, Nanocore, and QuasarRat, among others. Some instances have also seen a Bitcoin or Ethereum hijacker installed, which replaces Bitcoin or Ethereum wallet addresses in the clipboard with a wallet address controlled by the attacker.

Monthly percentage of global detections by country

Country	July 2021	August 2021	September 2021	October 2021
United States	44.4%	65.2%	23.9%	25.4%
France	14.7%	18.2%	19.5%	14.4%
Greece	0.1%	0.1%	2.7%	6.3%
United Kingdom	0.7%	0.9%	1.6%	6.2%
Spain	2.7%	0.2%	0.6%	6.1%
Japan	2.5%	2.1%	6.1%	5.9%
Germany	13.4%	1.7%	6.3%	5.8%
Israel	0.1%	0.1%	0.1%	4.7%
Turkey	0.8%	0.5%	0.9%	3.2%
Canada	0.7%	0.5%	8.3%	2.6%

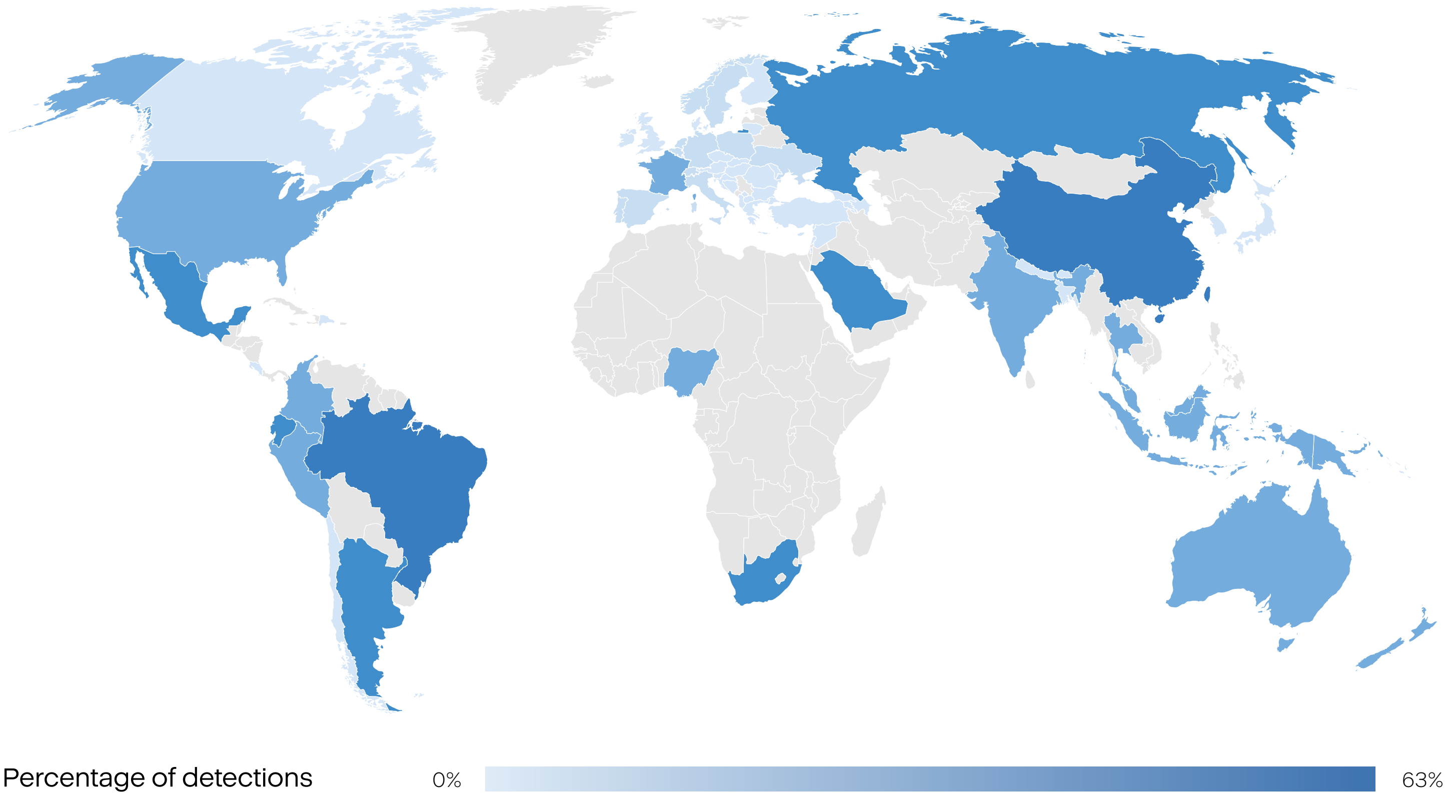
Malware detections Q3 2021



If we normalize the number of detections per active client per country, we then get a slightly different distribution. The following table shows the normalized percentage of clients with at least one malware detection per country in Q3 2021.

Rank	Country	Percentage of clients with malware detections in Q3 2021, normalized
1	Taiwan	63.6%
2	Singapore	57.4%
3	China	55.5%
4	Brazil	55.2%
5	Republic of Moldova	50.5%
6	Russia	49.5%
7	Greece	43.3%
8	Bulgaria	41.3%
9	South Korea	40.6%
10	Israel	39.7%
11	Turkey	39.4%
12	Ecuador	37.8%
13	Argentina	37.8%
14	United Arab Emirates	37.5%
15	Thailand	37.1%
16	South Africa	35.9%
17	Mexico	35.2%
18	Hungary	32.5%
19	Slovakia	32.0%
20	Portugal	30.5%
21	Haiti	30.2%
22	Spain	29.4%
23	Indonesia	28.9%
24	Saudi Arabia	28.6%
25	Slovenia	28.2%

Normalized numbers of detection in Q3 2021



Ransomware threat

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 data from July 1 to October 31, 2021, blocked by our threat agnostic Acronis Active Protection.

Below are the top 10 active ransomware families we observed and tracked in 2021. 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 the dangerousness of a threat. In addition, many groups operate ransomware as a service businesses, so that attackers might be using multiple threat families during similar attacks.

It should also be noted that in Q3, many ransomware groups disappeared, re-grouped under new names, or lost some of their members and infrastructure to law enforcement operations — which makes tracking under unique names even more challenging.

1. Lockbit
2. Conti
3. Pysa
4. Grief
5. Hive
6. CIOP
7. Marketo
8. Everest
9. LV
10. Revil

Daily ransomware detections

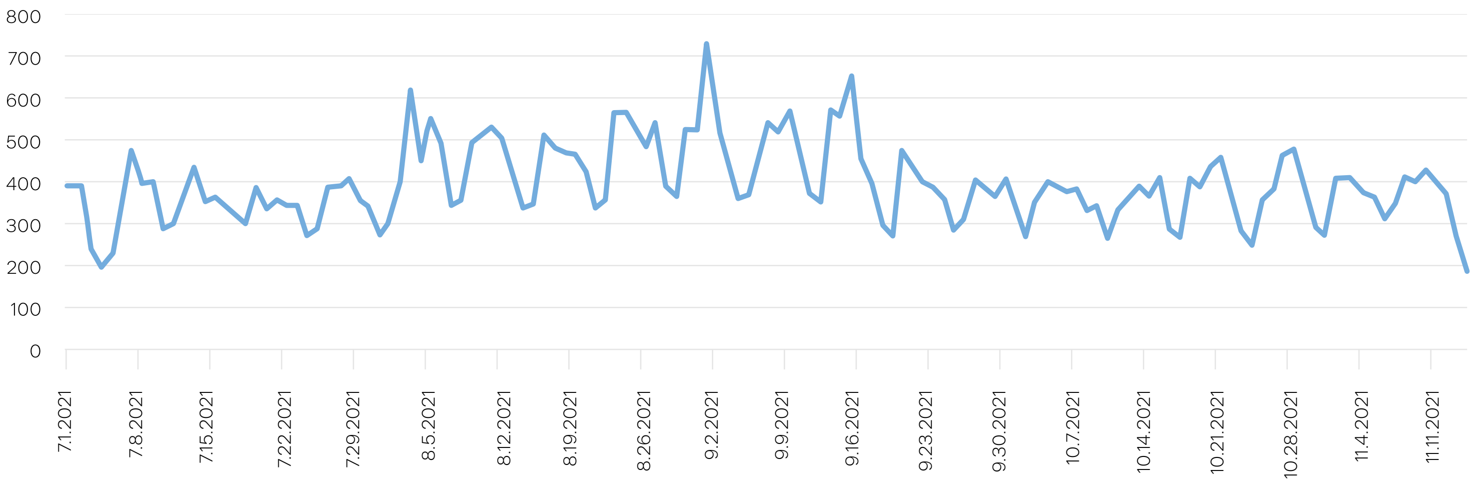
The number of ransomware incidents has decreased slightly in Q3, after a high during the summer months. From July to August, we had an increase of 32.7% of blocked ransomware attacks globally, followed by a decrease by 7% in September and 16% in October.

The reasons behind such fluctuations can be manifold. On one hand, there have been a few arrests and more pressure from law enforcement against ransomware groups. But on the other hand, some attacks are getting blocked earlier in the chain; for example, at the email lure or the malicious URL, so that the final ransomware is never downloaded and therefore cannot be counted in this graph.

Changes in the number of ransomware detections per month per region

Month	EMEA	Americas	Asia	Global
July-August	26.5%	19.4%	64.7%	32.7%
August-September	-6.2%	-2.9%	-9.1%	-7.0%
September-October	-13.2%	-21.0%	-17.2%	-16.0%

Daily ransomware detections globally



Top 10 countries: ransomware detections by region

Asia

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021
Japan	31.61%	38.09%
Israel	8.49%	2.55%
China	7.92%	8.59%
India	7.34%	3.65%
South Korea	5.50%	5.51%
Turkey	5.44%	5.51%
Taiwan	4.91%	5.43%
Philippines	4.70%	4.16%
Thailand	2.95%	2.55%
Indonesia	2.75%	2.06%

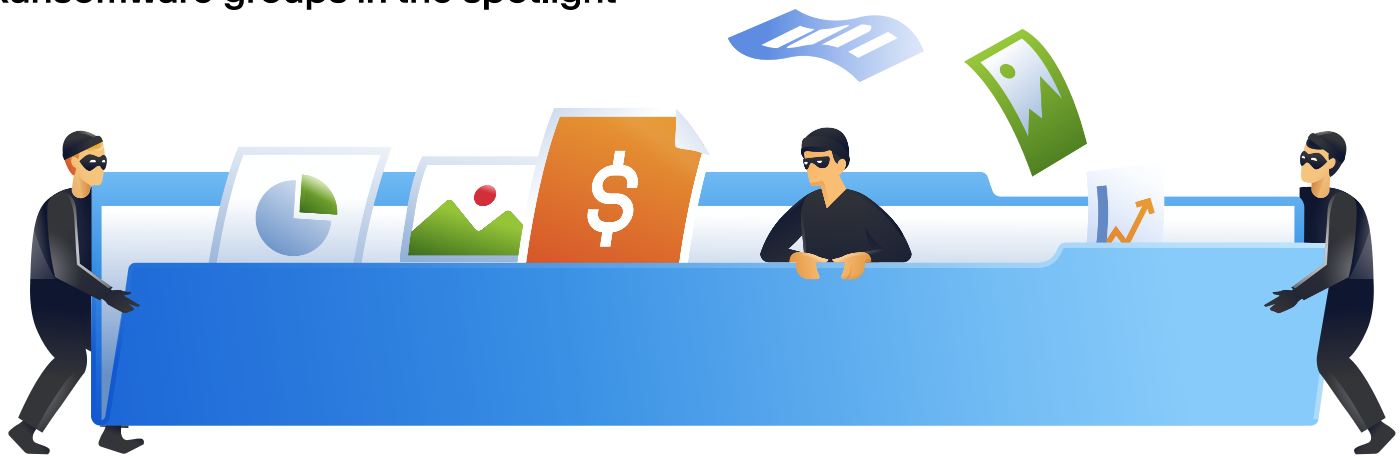
EMEA

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021
Germany	43.37%	45.17%
United Kingdom	9.64%	9.46%
France	9.00%	9.37%
Switzerland	7.98%	8.45%
Italy	5.65%	5.50%
Netherlands	3.28%	4.04%
Spain	3.07%	2.85%
Austria	3.01%	3.13%
Belgium	2.31%	2.33%
Czech Republic	1.65%	1.38%

Americas

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021
United States	79.03%	79.64%
Canada	12.05%	12.14%
Mexico	2.20%	2.15%
Brazil	1.73%	2.09%
Argentina	0.93%	0.49%
Colombia	0.86%	0.64%
Chile	0.44%	0.48%
Peru	0.39%	0.46%
Bolivia	0.29%	0.11%
Guatemala	0.26%	0.22%

Ransomware groups in the spotlight

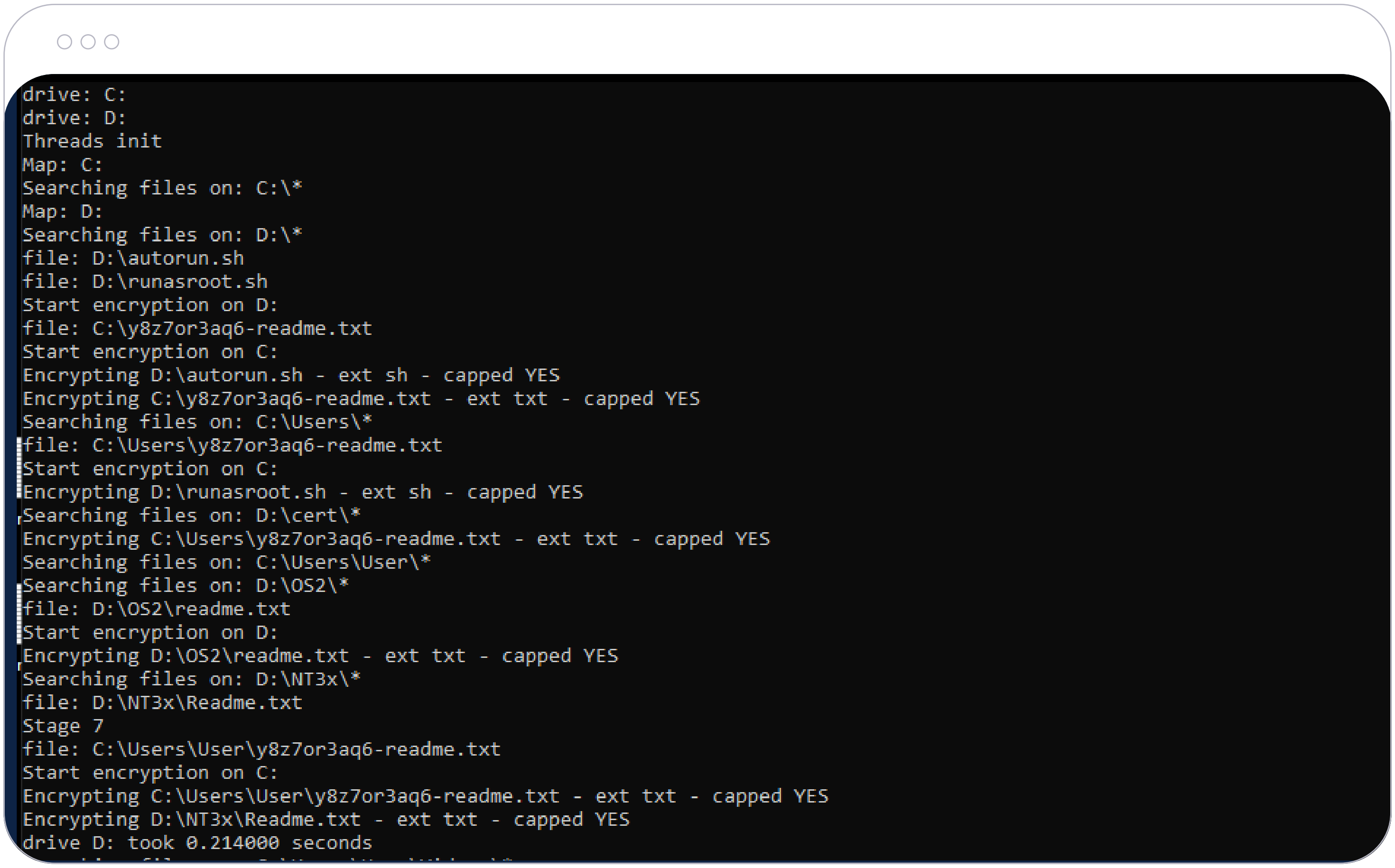


AvosLocker ransomware

The ransomware AvosLocker was discovered in late June of 2021. The criminals started searching for affiliates through various DarkWeb forums, as was revealed in a Twitter post. They also announced recruitment for penetration testers who have worked with Active Directory and “access brokers” who have remote access to hacked infrastructure. In another post, they offered ransomware-as-a-service — providing a piece of malware written in C++ with the multithreading capability that overwrites victims’ files — with encrypted content instead of through the creation of file copies. AvosLocker was distributed as spam emails targeting Windows machines and uses AES-256-CBC for file encryption, and RSA-1024 for file keys encryption. It encrypts network shares, and terminates associated processes that may be blocking access.

Execution

By default, the ransomware works as a console application, printing the execution log to the console. It is typically run manually by an attacker who remotely has accessed the machine.



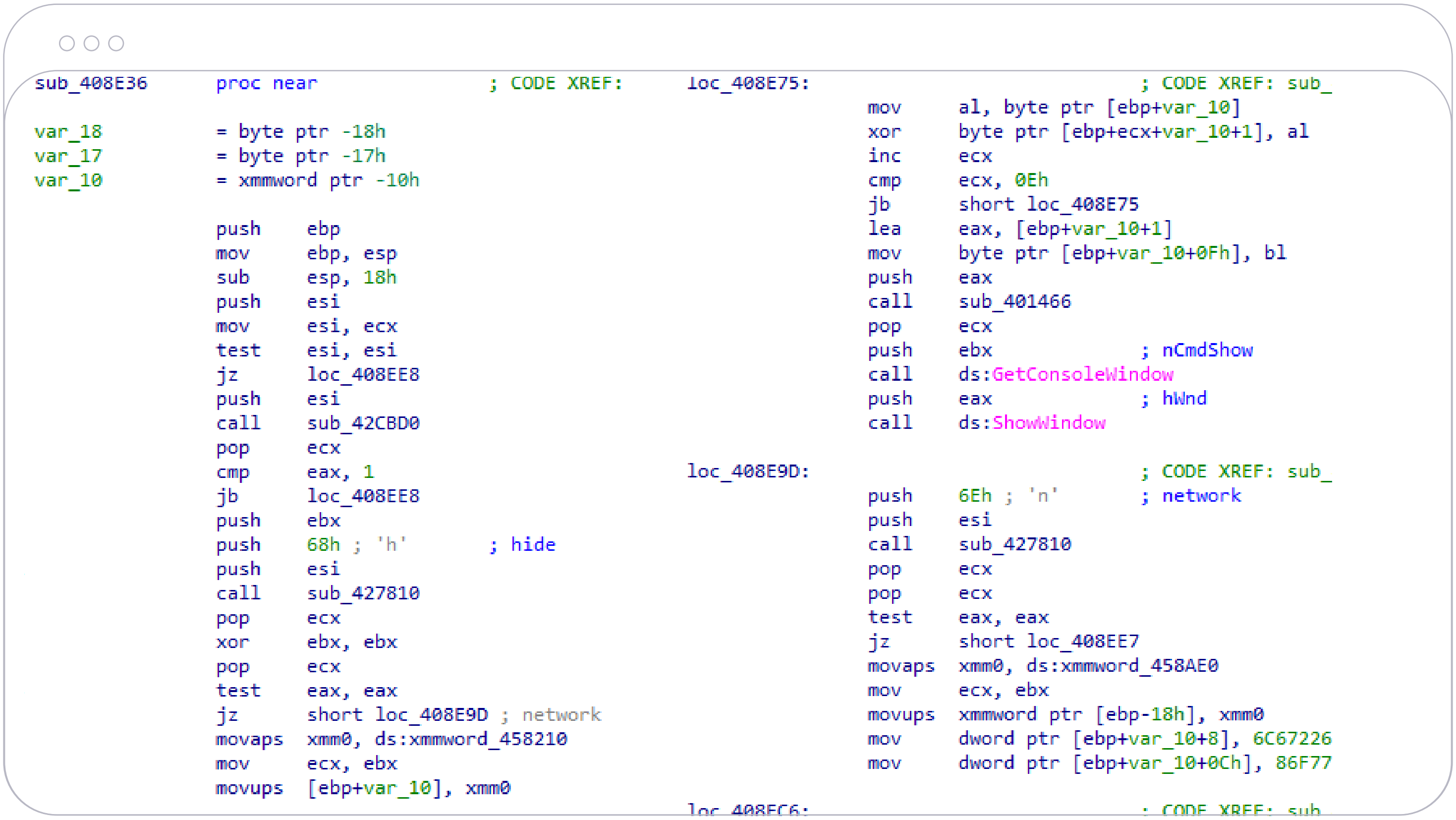
```
drive: C:
drive: D:
Threads init
Map: C:
Searching files on: C:\*
Map: D:
Searching files on: D:\*
file: D:\autorun.sh
file: D:\runasroot.sh
Start encryption on D:
file: C:\y8z7or3aq6-readme.txt
Start encryption on C:
Encrypting D:\autorun.sh - ext sh - capped YES
Encrypting C:\y8z7or3aq6-readme.txt - ext txt - capped YES
Searching files on: C:\Users\*
file: C:\Users\y8z7or3aq6-readme.txt
Start encryption on C:
Encrypting D:\runasroot.sh - ext sh - capped YES
Searching files on: D:\cert\*
Encrypting C:\Users\y8z7or3aq6-readme.txt - ext txt - capped YES
Searching files on: C:\Users\User\*
Searching files on: D:\OS2\*
file: D:\OS2\readme.txt
Start encryption on D:
Encrypting D:\OS2\readme.txt - ext txt - capped YES
Searching files on: D:\NT3x\*
file: D:\NT3x\Readme.txt
Stage 7
file: C:\Users\User\y8z7or3aq6-readme.txt
Start encryption on C:
Encrypting C:\Users\User\y8z7or3aq6-readme.txt - ext txt - capped YES
Encrypting D:\NT3x\Readme.txt - ext txt - capped YES
drive D: took 0.214000 seconds
```

The log shows that AvosLocker first looks for accessible drivers and lists all their files filtered by extensions that will be encrypted later. The encrypted files will get the '.avos' or '.avos2' extension appended to the original file name.

As mentioned before, the ransomware is deployed by the attacker manually on machines. During execution, it will generate logs about performed actions, so that the attacker can observe in real time what the program is doing. To evade signature-based detection, ransomware uses string obfuscation. The AvosLocker does not use any packer or cryptor to hide its content.

The modes of operation can be selected using the following command line arguments:

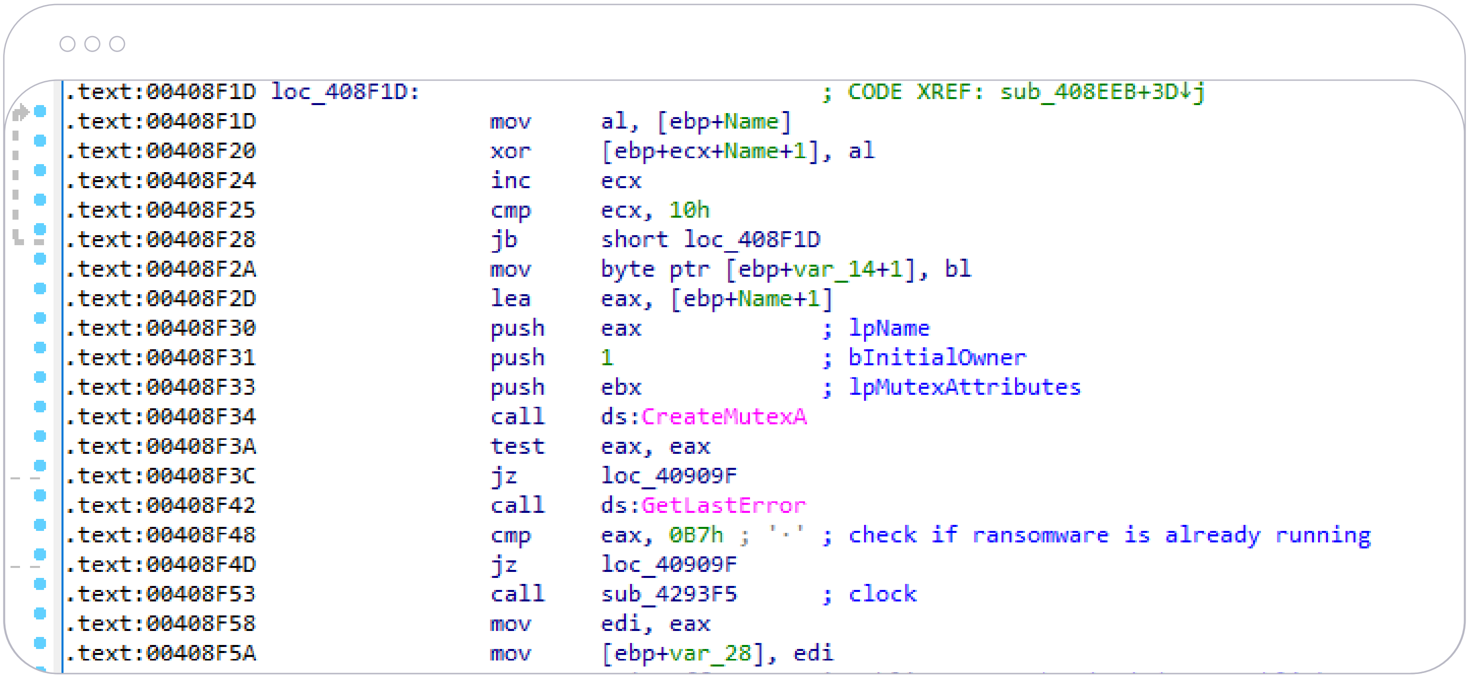
- **'h'** – enables the hide mode.
- **'n**' – enables encryption of network shared folders and drives.



```
sub_408E36      proc near               ; CODE XREF:

var_18          = byte ptr -18h
var_17          = byte ptr -17h
var_10          = xmmword ptr -10h

                push    ebp
                mov     ebp, esp
                sub     esp, 18h
                push    esi
                mov     esi, ecx
                test    esi, esi
                jz      loc_408EE8
                push    esi
                call    sub_42CBD0
                pop     ecx
                cmp     eax, 1
                jb      loc_408EE8
                push    ebx
                push    68h ; 'h'       ; hide
                push    esi
                call    sub_427810
                pop     ecx
                xor     ebx, ebx
                pop     ecx
                test    eax, eax
                jz      short loc_408E9D ; network
                movaps  xmm0, ds:xmmword_458210
                mov     ecx, ebx
                movups  [ebp+var_10], xmm0
```

```
loc_408E75:                             ; CODE XREF: sub_
                mov     al, byte ptr [ebp+var_10]
                xor     byte ptr [ebp+ecx+var_10+1], al
                inc     ecx
                cmp     ecx, 0Eh
                jb      short loc_408E75
                lea     eax, [ebp+var_10+1]
                mov     byte ptr [ebp+var_10+0Fh], bl
                push    eax
                call    sub_401466
                pop     ecx
                push    ebx             ; nCmdShow
                call    ds:GetConsoleWindow
                push    eax             ; hWnd
                call    ds:ShowWindow

loc_408E9D:                             ; CODE XREF: sub_
                push    6Eh ; 'n'       ; network
                push    esi
                call    sub_427810
                pop     ecx
                pop     ecx
                test    eax, eax
                jz      short loc_408EE7
                movaps  xmm0, ds:xmmword_458AE0
                mov     ecx, ebx
                movups  xmmword ptr [ebp-18h], xmm0
                mov     dword ptr [ebp+var_10+8], 6C67226
                mov     dword ptr [ebp+var_10+0Ch], 86F77

loc_408EC6:                             ; CODE XREF: sub
```

The ransomware checks for the Mutex 'ievah8eVki3Ho4oo' to prevent the ransomware from executing more than one instance at a time. If the Mutex already exists, the ransomware quits.



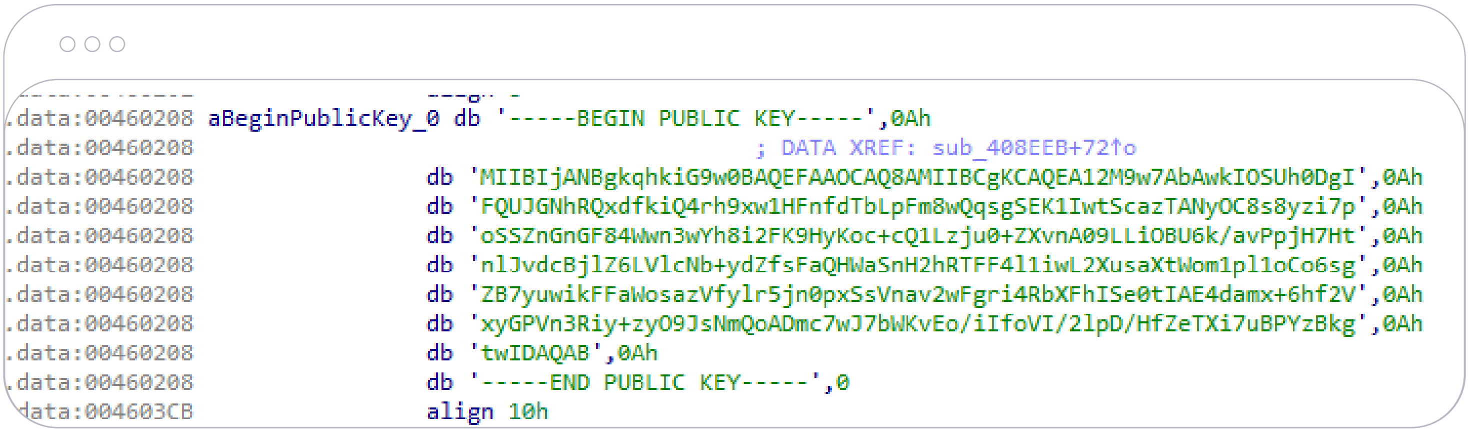
```
.text:00408F1D loc_408F1D:                             ; CODE XREF: sub_408EEB+3D↓j
.text:00408F1D                 mov     al, [ebp+Name]
.text:00408F20                 xor     [ebp+ecx+Name+1], al
.text:00408F24                 inc     ecx
.text:00408F25                 cmp     ecx, 10h
.text:00408F28                 jb      short loc_408F1D
.text:00408F2A                 mov     byte ptr [ebp+var_14+1], bl
.text:00408F2D                 lea     eax, [ebp+Name+1]
.text:00408F30                 push    eax             ; lpName
.text:00408F31                 push    1               ; bInitialOwner
.text:00408F33                 push    ebx             ; lpMutexAttributes
.text:00408F34                 call    ds:CreateMutexA
.text:00408F3A                 test    eax, eax
.text:00408F3C                 jz      loc_40909F
.text:00408F42                 call    ds:GetLastError
.text:00408F48                 cmp     eax, 0B7h ; '·' ; check if ransomware is already running
.text:00408F4D                 jz      loc_40909F
.text:00408F53                 call    sub_4293F5      ; clock
.text:00408F58                 mov     edi, eax
.text:00408F5A                 mov     [ebp+var_28], edi
```

This makes the malicious code more difficult to analyse and detect.

File encryption

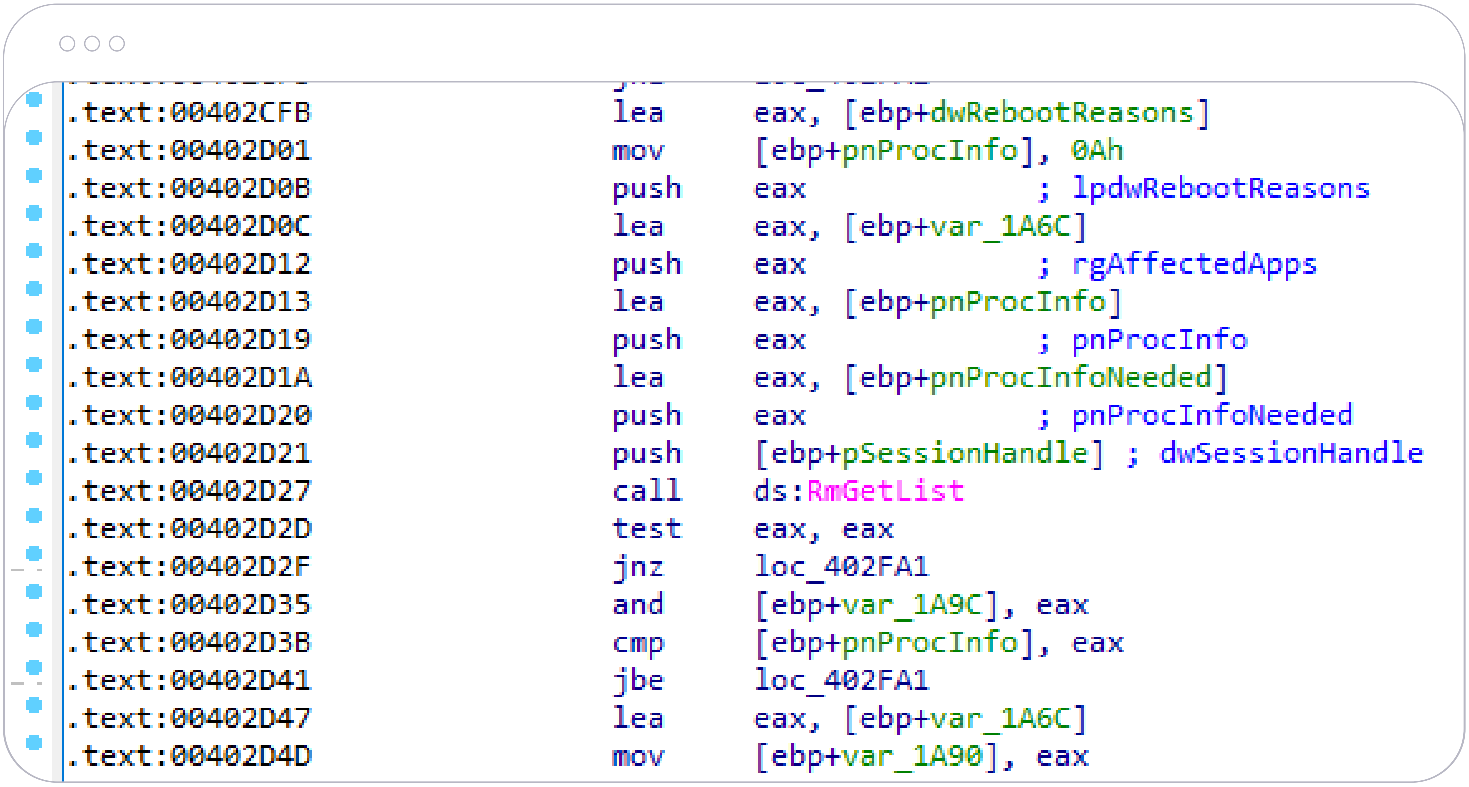
For data encryption, AvosLocker uses AES-256-CBC for file encryption, and RSA-1024 to encrypt the generated file keys. This scheme seems to be quite popular among ransomware groups as this makes it impossible for a victim to restore their files without buying a decryptor.

The master RSA public key is hardcoded in the binary:



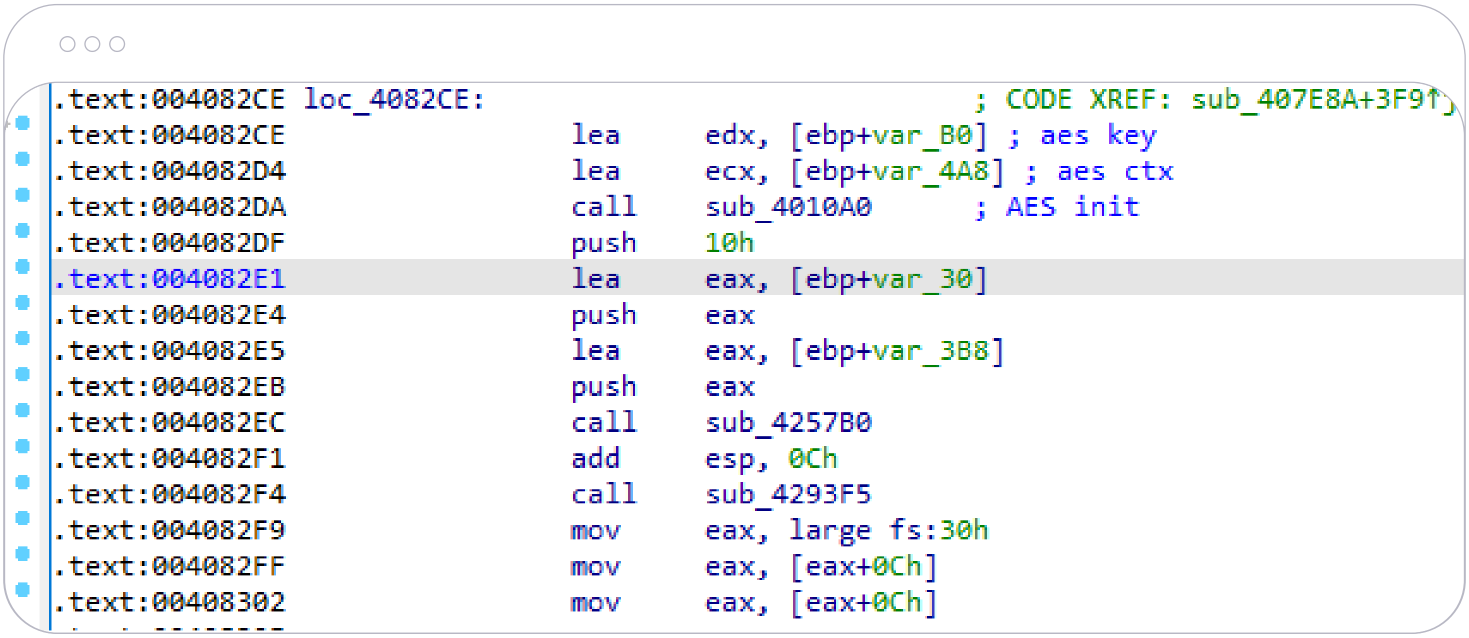
```
.data:00460208 aBeginPublicKey_0 db '-----BEGIN PUBLIC KEY-----',0Ah
.data:00460208                                         ; DATA XREF: sub_408EEB+72↑o
.data:00460208                db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA12M9w7AbAwkIOSUh0DgI',0Ah
.data:00460208                db 'FQUJGNhRQxdfkiQ4rh9xw1HFnfdTbLpFm8wQqsgSEK1IwtScazTANyOC8s8yzi7p',0Ah
.data:00460208                db 'oSSZnGnGF84Wwn3wYh8i2FK9HyKoc+cQ1Lzju0+ZXvnA09LLiOBU6k/avPpjH7Ht',0Ah
.data:00460208                db 'nlJvdcBjlZ6LVlcNb+ydZfsFaQHWaSnH2hRTFF4l1iwL2XusaXtWom1pl1oCo6sg',0Ah
.data:00460208                db 'ZB7yuwikFFaWosazVfylr5jn0pxSsVnav2wFgri4RbXFhISe0tIAE4damx+6hf2V',0Ah
.data:00460208                db 'xyGPVn3Riy+zyO9JsNmQoADmc7wJ7bWKvEo/iIfoVI/2lpD/HfZeTXi7uBPYzBkg',0Ah
.data:00460208                db 'twIDAQAB',0Ah
.data:00460208                db '-----END PUBLIC KEY-----',0
.data:004603CB                align 10h
```

If the master RSA public key is not available, then the new RSA key pair is generated. In order to unlock the user's files currently opened by applications, such as databases and documents, the cryptolocker terminates the processes associated with these file types. The list of associated processes is obtained using **RmGetList() WinAPI call**:



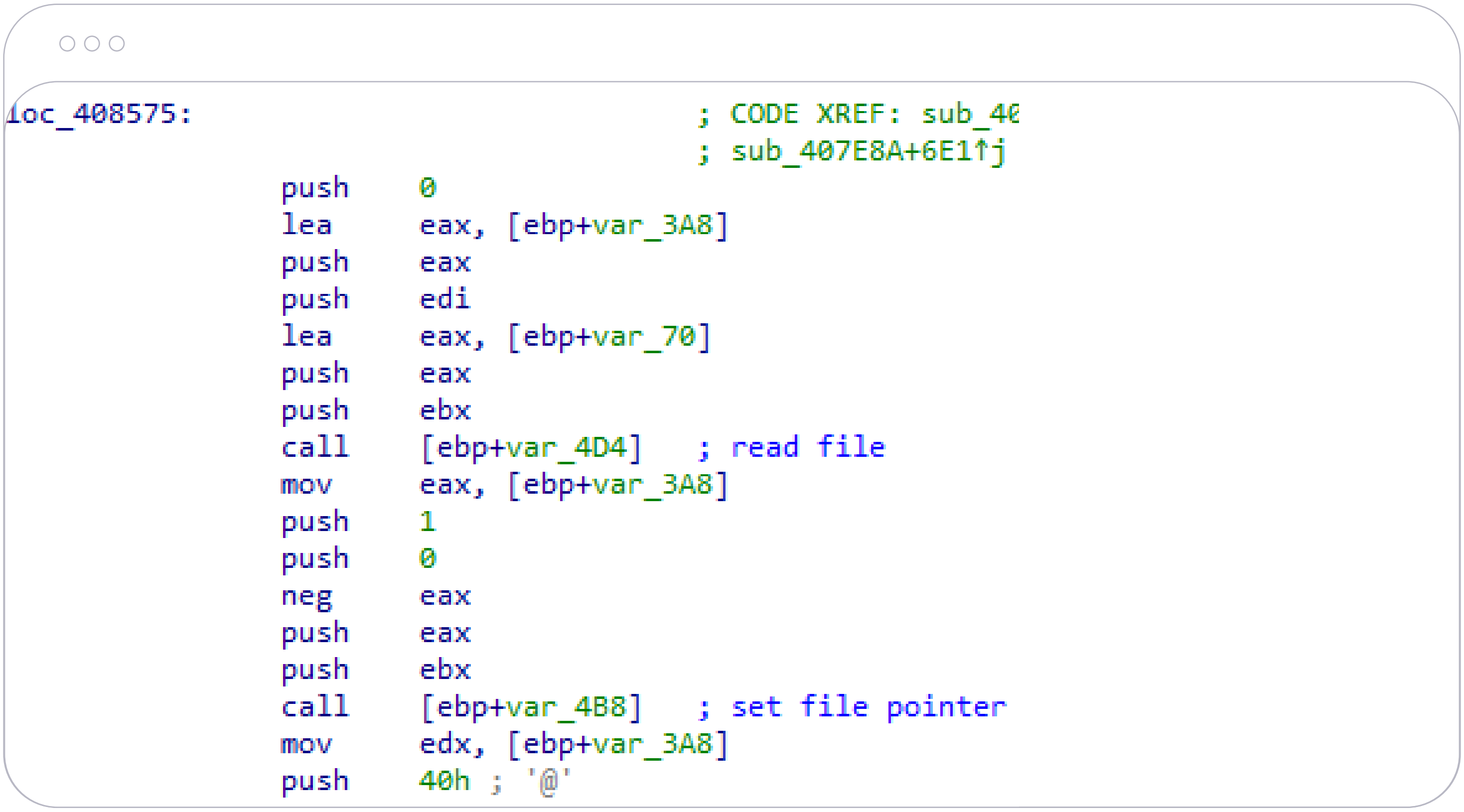
```
.text:00402CFB         lea     eax, [ebp+dwRebootReasons]
.text:00402D01         mov     [ebp+pnProcInfo], 0Ah
.text:00402D0B         push    eax             ; lpdwRebootReasons
.text:00402D0C         lea     eax, [ebp+var_1A6C]
.text:00402D12         push    eax             ; rgAffectedApps
.text:00402D13         lea     eax, [ebp+pnProcInfo]
.text:00402D19         push    eax             ; pnProcInfo
.text:00402D1A         lea     eax, [ebp+pnProcInfoNeeded]
.text:00402D20         push    eax             ; pnProcInfoNeeded
.text:00402D21         push    [ebp+pSessionHandle] ; dwSessionHandle
.text:00402D27         call    ds:RmGetList
.text:00402D2D         test    eax, eax
.text:00402D2F         jnz     loc_402FA1
.text:00402D35         and     [ebp+var_1A9C], eax
.text:00402D3B         cmp     [ebp+pnProcInfo], eax
.text:00402D41         jbe     loc_402FA1
.text:00402D47         lea     eax, [ebp+var_1A6C]
.text:00402D4D         mov     [ebp+var_1A90], eax
```

A unique **AES key** and **initialization vector (IV)** are generated for each file.

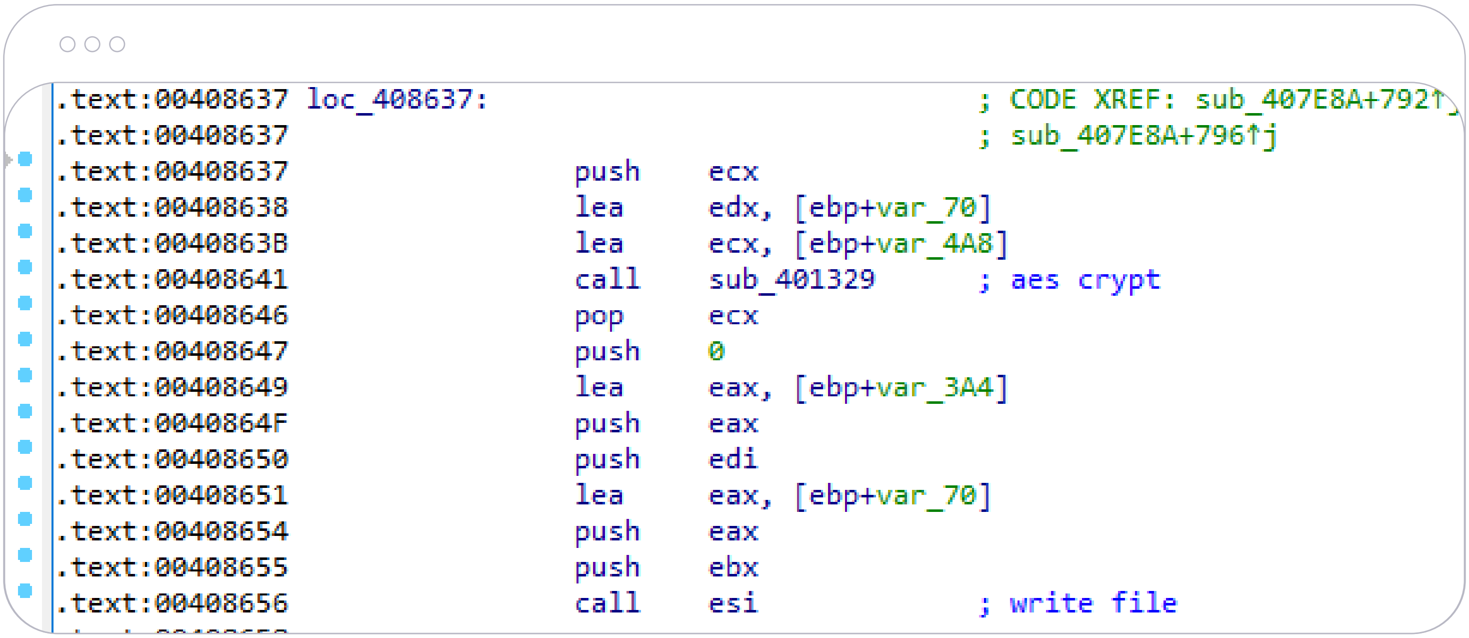


```
.text:004082CE loc_4082CE:                              ; CODE XREF: sub_407E8A+3F9↑
.text:004082CE                 lea     edx, [ebp+var_B0] ; aes key
.text:004082D4                 lea     ecx, [ebp+var_4A8] ; aes ctx
.text:004082DA                 call    sub_4010A0      ; AES init
.text:004082DF                 push    10h
.text:004082E1                 lea     eax, [ebp+var_30]
.text:004082E4                 push    eax
.text:004082E5                 lea     eax, [ebp+var_3B8]
.text:004082EB                 push    eax
.text:004082EC                 call    sub_4257B0
.text:004082F1                 add     esp, 0Ch
.text:004082F4                 call    sub_4293F5
.text:004082F9                 mov     eax, large fs:30h
.text:004082FF                 mov     eax, [eax+0Ch]
.text:00408302                 mov     eax, [eax+0Ch]
```

After that, the **file content is replaced with the encrypted data** that makes it harder to restore original files.

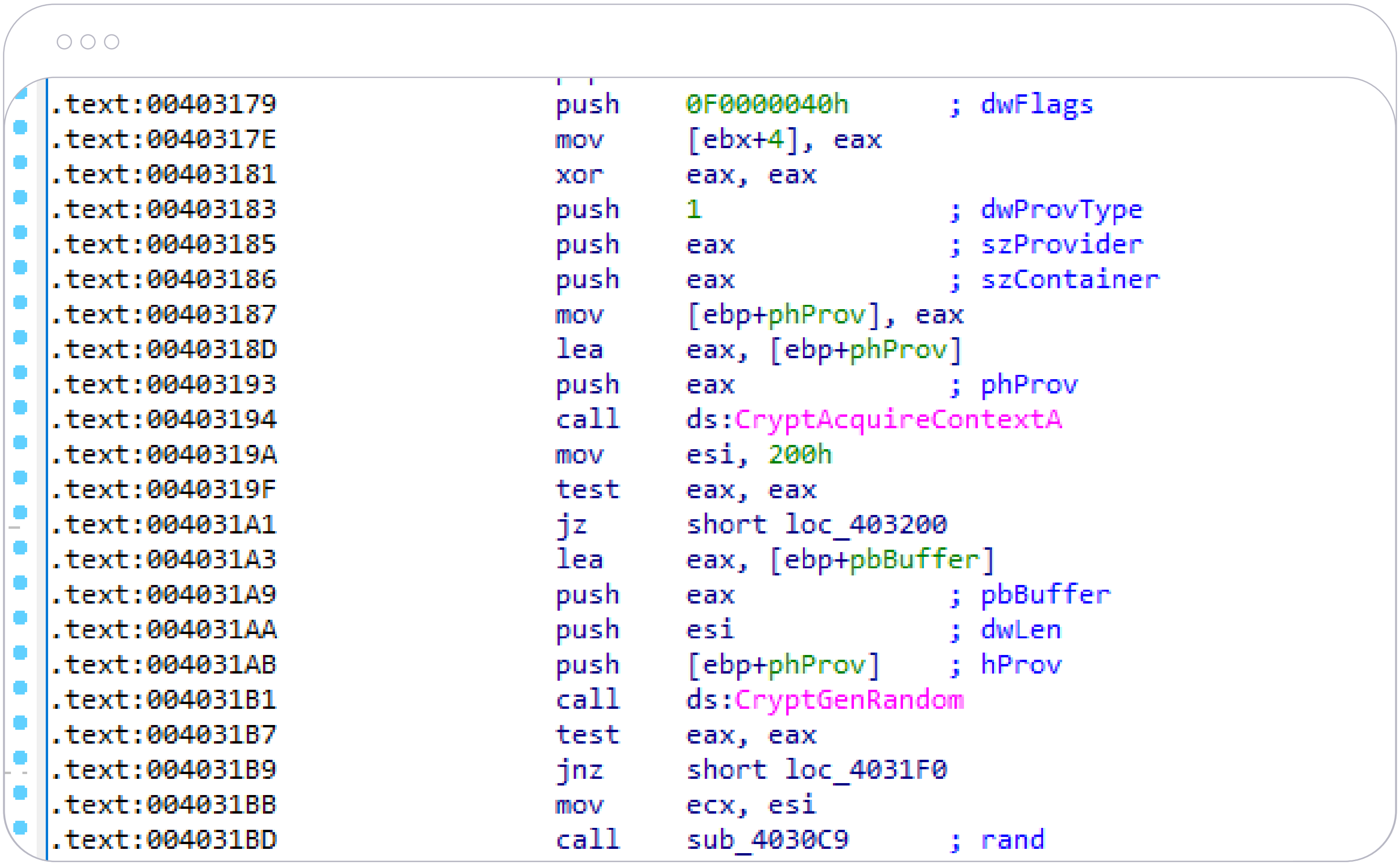


```
loc_408575:                             ; CODE XREF: sub_40
                                        ; sub_407E8A+6E1↑j
                push    0
                lea     eax, [ebp+var_3A8]
                push    eax
                push    edi
                lea     eax, [ebp+var_70]
                push    eax
                push    ebx
                call    [ebp+var_4D4]   ; read file
                mov     eax, [ebp+var_3A8]
                push    1
                push    0
                neg     eax
                push    eax
                push    ebx
                call    [ebp+var_4B8]   ; set file pointer
                mov     edx, [ebp+var_3A8]
                push    40h ; '@'
```



```
.text:00408637 loc_408637:                          ; CODE XREF: sub_407E8A+792↑
.text:00408637                                      ; sub_407E8A+796↑j
.text:00408637                push    ecx
.text:00408638                lea     edx, [ebp+var_70]
.text:0040863B                lea     ecx, [ebp+var_4A8]
.text:00408641                call    sub_401329     ; aes crypt
.text:00408646                pop     ecx
.text:00408647                push    0
.text:00408649                lea     eax, [ebp+var_3A4]
.text:0040864F                push    eax
.text:00408650                push    edi
.text:00408651                lea     eax, [ebp+var_70]
.text:00408654                push    eax
.text:00408655                push    ebx
.text:00408656                call    esi            ; write file
```

The generation of **random keys** is performed with the help of a **CryptGenRandom() WinAPI function**, which is a part of the Microsoft Cryptographic Provider.



```
.text:00403179                push    0F0000040h     ; dwFlags
.text:0040317E                mov     [ebx+4], eax
.text:00403181                xor     eax, eax
.text:00403183                push    1              ; dwProvType
.text:00403185                push    eax            ; szProvider
.text:00403186                push    eax            ; szContainer
.text:00403187                mov     [ebp+phProv], eax
.text:0040318D                lea     eax, [ebp+phProv]
.text:00403193                push    eax            ; phProv
.text:00403194                call    ds:CryptAcquireContextA
.text:0040319A                mov     esi, 200h
.text:0040319F                test    eax, eax
.text:004031A1                jz      short loc_403200
.text:004031A3                lea     eax, [ebp+pbBuffer]
.text:004031A9                push    eax            ; pbBuffer
.text:004031AA                push    esi            ; dwLen
.text:004031AB                push    [ebp+phProv]   ; hProv
.text:004031B1                call    ds:CryptGenRandom
.text:004031B7                test    eax, eax
.text:004031B9                jnz     short loc_4031F0
.text:004031BB                mov     ecx, esi
.text:004031BD                call    sub_4030C9     ; rand
```

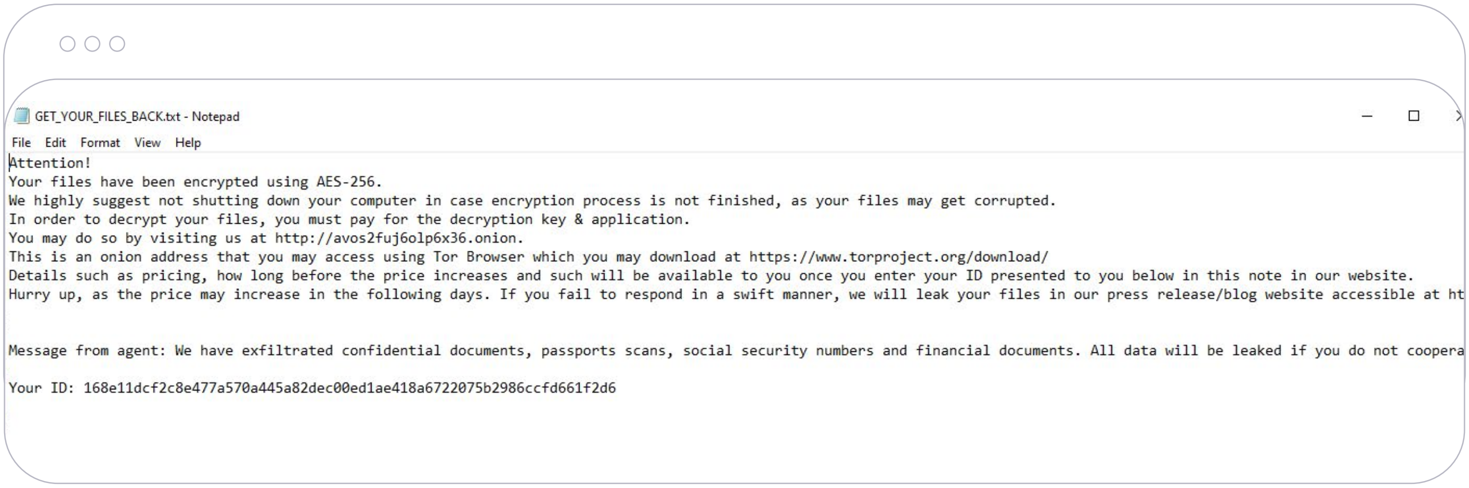
After the file is encrypted, the ransomware stores a Base64-encoded AES file key encrypted with the master RSA public key at the end of the encrypted file.

The ransomware performs file encryption in multiple threads. When the command line argument 'n' is given, it starts with encrypting network resources. The files with the following extensions are searched and stored in the list which is later submitted for encryption:

ndoc docx xls xlsx ppt pptx pst ost msg eml vsd vsdx txt csv rtf wks wk1 pdf dwg onetoc2 snt jpeg jpg docb docm dot dotm dotx xlsm xlsb xlw xlt xlm xlc xltx xltm pptm pot pps ppsm ppsx ppam potx potm edb hwp 602 sxi sti sldx sldm sldm vdi vmdk vmx gpg aes ARC PAQ bz2 tbk bak tar tgz gz 7z rar zip backup iso vcd bmp png gif raw cgm tif tiff nef psd ai svg djvu m4u m3u mid wma flv 3g2 mkv 3gp mp4 mov avi asf mpeg vob mpg wmv fla swf wav mp3 sh class jar java rb asp php jsp brd sch dch dip pl vb vbs ps1 bat cmd js asm h pas cpp c cs suo sln ldf mdf ibd myi myd frm odb dbf db mdb accdb sql sqlitedb sqlite3 asc lay6 lay mml sxm otg odg uop std sxd otp odp wb2 slk dif stc sxc ots ods 3dm max 3ds uot stw sxw ott odt pem p12 csr crt key pfx der dat

Ransom note

AvosLocker drops a ransom note **“GET_YOUR_FILES_BACK.txt”** which contains the link to the data leak site and victim’s I.D.



```
Attention!
Your files have been encrypted using AES-256.
We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key & application.
You may do so by visiting us at http://avos2fuj6olp6x36.onion.
This is an onion address that you may access using Tor Browser which you may download at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.
Hurry up, as the price may increase in the following days. If you fail to respond in a swift manner, we will leak your files in our press release/blog website accessible at ht


Message from agent: We have exfiltrated confidential documents, passports scans, social security numbers and financial documents. All data will be leaked if you do not coopera

Your ID: 168e11dcf2c8e477a570a445a82dec00ed1ae418a6722075b2986ccfd661f2d6
```

When going to the data leak site, **a victim is asked to provide the I.D. stored in the ransom note**. The data leak site then provides the customer support capability. The data leak site also has ‘press releases’ that contain exfiltrated data of the victims who refused to pay.

Conclusion

AvosLocker represents a typical example of modern ransomware-as-a-service, providing a strong encryption scheme with symmetric AES-256-CBC and asymmetric RSA1024 algorithms that can be run in multiple threads. The files are not copied for encryption but files’content is replaced with encrypted data. The ransomware is equipped with basic obfuscation algorithms to prevent the binary being detected by AV signature scanners. Also, AvosLocker can encrypt network resources together with local and mapped drives. As with other RaaS groups, AvosLocker has its own data leak site where criminals provide support for victims as well as publishing stolen data of those who hadn’t paid.

Malicious websites

An average of 1.9% of endpoints tried to access some malicious URLs in Q3 2021, up slightly from 1.8% in Q2. In October, we have seen a spike to 4.3%, which is related to the spike we saw in phishing emails reaching users' inboxes.

Month	Percentage of users that clicked on malicious URLs
January	3.2%
February	2.9%
March	2.1%
April	1.8%
May	1.9%
June	1.8%
July	1.9%
August	1.8%
September	2.1%
October	4.3%

The largest percentage of blocked malicious URLs in Q3 2021 was 26.8% in the United States, followed by 20% in Germany, and 8.7% in Canada — with 65% of these blocked URLs encrypted by HTTPS, making them more difficult to analyse and filter on the network.

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

Top 20 countries with the most blocked URLs in Q3 2021:

Rank	Country	Percent of blocked URLs in Q3 2021
1	United States	26.8%
2	Germany	20.0%
3	Canada	8.7%
4	United Kingdom	7.2%
5	Italy	5.1%
6	Netherlands	3.4%
7	Singapore	3.2%
8	Belgium	3.1%
9	France	3.0%
10	Japan	2.9%
11	Australia	2.0%
12	Switzerland	1.9%
13	Spain	1.8%
14	Thailand	1.6%
15	Austria	0.9%
16	Russia	0.8%
17	Brazil	0.7%
18	Costa Rica	0.7%
19	Peru	0.7%
20	Turkey	0.6%

Vulnerabilities in Windows OS and software

Part 3

As vulnerabilities are one of the key gates to penetrate systems, they are constantly being searched for, used, and eventually patched (unfortunately not always successfully and definitely not on time). The second half of 2021 did not bring anything groundbreaking in this sense, but rather confirmed the alarming fact that more and more critical vulnerabilities are being discovered and exploited by cybercriminals. The number of patches released by software vendors continues to be measured in dozens — if not hundreds — for every month we fully analyzed from July to October.

As has been the case previously, Google Chrome, the most popular browser, was under heavy fire. They had to release an emergency security patch for the browser for a zero-day vulnerability that is being actively exploited in the wild. Google has not provided technical details regarding the vulnerability dubbed CVE-2021-37973, but this is coming on the heels of 19 other vulnerabilities that were disclosed and patched that affectes Mac, Windows, and Linux versions of Chrome. Later on, Google released Chrome update 95.0.4638.69 for Windows, Mac, and Linux to patch seven vulnerabilities, including two actively exploited zero-days. The two zero-day vulnerabilities — CVE-2021-38000 and CVE-2021-38003 — have both been rated high severity. Both were discovered by Google's own Threat Analysis Group.

These newest discoveries bring the total number of patched zero-day vulnerabilities in the Chrome browser to 15 so far this year. That amounts to an astonishing 1.5 zero-day vulnerabilities per month.

Microsoft had been doing a good job patching vulnerabilities in its products. Let start with July: they released 117 security fixes for the software, including a remote code execution (RCE) vulnerability in the Exchange Server found by participants of the Pwn2Own competition. Thirteen were considered critical, and nine were zero-days, where four were actively used in-the-wild. However, a set of three older vulnerabilities in the Microsoft Exchange Server could be chained, thus allowing an attacker to perform unauthenticated remote code execution. This potential to run arbitrary code and commands on victims' machines had threat actors scanning for vulnerable servers. Two of the three vulnerabilities were patched as part of the April Microsoft Patch Tuesday bug fixes, and the third was patched in May. However, despite patches being available, Exchange honeypots are showing that attackers are still actively searching for and exploiting these vulnerabilities on unpatched servers as recently as the past couple of weeks.

In August, there were 44 vulnerabilities covered, with one of them being funny in a way: attackers used CVE-2021-36948, which exploited a weakness in the Windows Update Medic service. This new service lets users repair Windows update components from a damaged state so that the device can continue to receive updates. The flaw is an "elevation of privilege" vulnerability that affects Windows 10 and Windows Server 2019 — meaning it can be leveraged in combination with another vulnerability to let attackers run code of their choice as administrator on a vulnerable system.

September brought 85 patches, including one for the MSHTML vulnerability disclosed during that month, as well as a critical remote code execution vulnerability in the Open Management Infrastructure, and two other critical vulnerabilities — with the remaining vulnerabilities being considered important according to Microsoft's vulnerability ratings. Three critical vulnerabilities were being patched by Microsoft, including one for Win32k (a driver used by Windows), which can lead to elevation of privilege. It is actively being exploited. And the vulnerabilities for both office suites are still being graded in terms of severity, but could be critical.

In addition to the 85 patches for 37 products released by Microsoft, Apple patched five vulnerabilities in September. The Apple vulnerabilities patched in macOS and Safari allowed for arbitrary code execution, while the Chrome update includes patches for nine vulnerabilities — including two zero-day vulnerabilities that had already been exploited in the wild.

Microsoft's Patch Tuesday for October fixed four zero-days and 81 flaws, including one for Microsoft Edge, that is being patched. OpenOffice and LibreOffice are each receiving three separate patches for similar issues.

For November, Microsoft released patches for 55 new CVEs in Microsoft Windows and Windows Components Azure, Azure RTOS, Azure Sphere, Microsoft Dynamics, Microsoft Edge, Exchange Server, Microsoft Office and Office Components, Windows Hyper-V, Windows Defender, and Visual Studio. Six among them are rated critical and 49 are rated as important in severity. Two vulnerabilities are listed as under active exploit at the time of release.

Adobe was doing a lot of patching job as well. For July, it released five patches addressing 29 CVEs in Adobe Dimension, Illustrator, Framemaker, Acrobat and Reader, and Adobe Bridge. In August, 29 CVEs were addressed again, closing vulnerabilities in Adobe Connect and Magento. The critical-rated patch for Magento fixed a wide range of bugs, the worst of which could allow remote code execution. For September, Adobe released 15 patches covering 59 CVEs, and in October, there were 10 CVEs in Adobe Reader, Acrobat Reader for Android, Adobe Campaign Standard, Commerce, Ops-CLI, and Adobe Connect. It's important though, that in the two weeks following this October set of security patches, Adobe issued another 14 security bulletins covering 92 CVE-listed bugs. These patches include 61 critical bugs, many of which allow arbitrary code execution.

Threat actors are constantly exploiting vulnerabilities and zero-days, so it's important to stay up-to-date on patches. Acronis Cyber Protect has made this simple with its patch management solution, which enables updating both quickly and easily.

Security forecast for 2022

Part 4

As the COVID-19 pandemic spread, everyone had to adapt to a very different routine full of challenges that few were prepared for. This completely changed the security landscape in 2021. Here are key trends that are likely to define the cybersecurity landscape going into 2022.

1. Ransomware continues to grow and evolve despite U.S. and Interpol/Europol efforts

Ransomware is one of the most profitable cyberattacks at the moment. Despite some recent arrests, there is no end in sight. Ransomware will expand further to macOS and Linux, as well as to new environments such as virtual systems, cloud, and OT/IoT. Anything that is connected to a reachable network is a potential target. This will increasingly lead to consequences and impacts in the real world, and thus also to more demand for official regulations and sanctions. Stealing data for double extortion as well as disabling security tools will be the norm; but it will also become more personal with insider threats and personal data.

The chaos will continue as groups continue rebranding to defy investigations, and ransomware-as-a-service will acquire smaller tier groups, allowing for overlapping usage of different families. Going forward, we can expect this resilience and flexibility to continue, and as such, ransomware operations by the end of 2022 may be unrecognizable compared to what we see today.

2. Cryptocurrency will become the attackers' favorite

With the price of Bitcoin at an all-time high, attacks are increasing with threat actors following profits. End users have struggled with phishing attacks, infostealers and malware that swap wallet addresses in memory for quite some time. We expect to see more of these attacks waged directly against smart contracts —attacking the programs at the heart of cryptocurrencies. We also expect attacks against Web 3.0 apps to occur more frequently in 2022. These new markets open new opportunities for sophisticated attacks (e.g., flash loan attack), which may allow attackers to drain millions of dollars from cryptocurrency liquidity pools.

3. Phishing will continue to be the main infection vector

Malicious emails and phishing in all variations are still at an all-time high. Despite constant awareness campaigns, users still fall for them and enable the attacker to compromise their organization. We don't expect AI to fully take over phishing emails in 2022, but instead expect increased automation and personalized information with these various data breaches, making them more effective. New tricks against OAuth and MFA will continue to generate profit for attackers, allowing them to take over accounts, despite plans from companies such as Google to auto-enroll 150 million users to 2FA. In order to bypass common anti-phishing tools, attacks such as business email compromise (BEC) will make use of alternative messaging services, such as text messages, Slack, or Teams chat. This goes hand-in-hand with the hijacking of legitimate email distribution services, as for example in Novemeber, when the FBI's own email service was compromised and started sending spam emails.

4. MSPs will be targeted via the tools they use

Attackers are going after the trusted connections that allow them to gain access to company networks. Software supply chain attacks are one of these methods, but even without full compromise of a vendor, there are similar ways to get in. Attackers are going after management tools used by the administrators, like professional services automation software (PSA), or remote monitoring and management (RMM) tools. They are the keys to the kingdom, and cybercriminals will use them against you. Service providers in particular will be targeted more frequently, as they often have many automation tools in place for the efficient rollout of new software. Unfortunately, this is now being done by the attackers in order to distribute malware. This can go together or in parallel with supply-chain attacks on a source code level. We expect more and more attacks when the source code of used apps or libraries are modified with malicious intent.

5. Trust will be compromised on a cloud level: API attacks

Cloud services are booming and so are serverless computing, edge computing, and API services. In combination with container orchestrations like Kubernetes, processes can be efficiently automated and dynamically adapted to various circumstances. Attackers are trying to disrupt this hyper-automation by going after such APIs, which can seriously impact the business processes of a company.

6. Data breaches for everyone

Despite the increase in data privacy regulations, the number of reported data breaches will also continue to increase. This is not just because they have to be reported, but because of the complex interactions and IT systems. Many companies have lost the overview of where all their data is and how it can be accessed. And automated data exchange from IoT devices and M2M communications increases the spread of data further. Unfortunately, we expect to see many large-scale data breaches in 2022. These data leaks will enable attackers to enrich their target profiles easily.

7. Adversarial attacks in AI

As AI is more frequently used to detect anomalies in IT systems and automatically configure and protect any valuable assets in them, it is understandable that attackers increasingly will try to attack the logic within the AI model. Being successful at reversing the decisions inside the AI model can allow an attacker to remain undetected or generate a denial of service attack with an undesired state. It may also allow them to identify timing issues, whereas slow changes are not seen as anomalies and thus are not blocked.

8. Security products unification: One vendor paradigm

To be better prepared for all these threats mentioned above, businesses must favor security vendors who provide wider security coverage under one product or umbrella of products. This helps to minimize supply-chain attacks, and allows faster reaction and recovery, which are crucial for keeping businesses up and running. Cybercriminals are profit-driven and will try to maximize their gains by automating their business and attacking companies where they are most exposed. They aggressively pursue each opportunity that they can find, and so it is therefore key to have strong authentication with MFA, timely patching of vulnerabilities, and visibility in place across the whole infrastructure.

Staying safe in 2022

Unfortunately, businesses are still struggling to effectively protect their entire workloads across the complex ecosystem of cloud, office, and home office. Doing so requires efficient solutions that integrate cybersecurity with data protection, as well as management and monitoring of endpoints. This holistic approach to cyber protection allows for an automated response against the flood of cyberthreats.

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

Part 5

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

To solve these problems, we recommend an integrated cyber protection solution like Acronis Cyber Protect, that combines antimalware, 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 – because of its one agent, it knows that data was lost and needed to be restored.

This isn't possible with an antimalware agent separate from a backup product with its own agent. Your antimalware solution may stop the threat, but some data may already be lost. A backup agent won't know about it automatically and, in the best case scenario, data will be restored slowly — if at all.

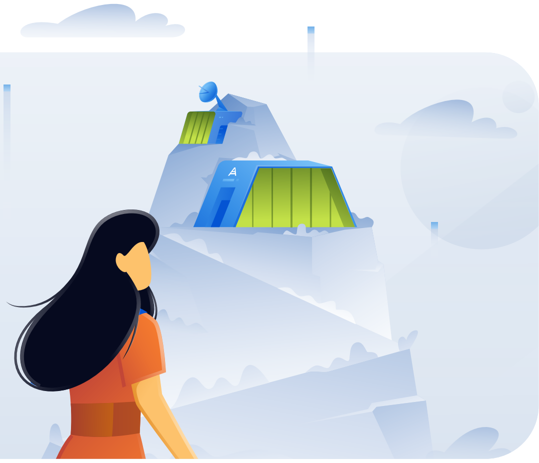
Of course, Acronis Cyber Protect Cloud strives to make data recoveries unnecessary by detecting and eliminating threats before they can damage your environment. This is achieved with our enhanced, multilayered cybersecurity functionality.

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 a lot of attacks succeed due to unpatched vulnerabilities. With a solution like Acronis Cyber Protect, you're covered with embedded vulnerability assessment and patch management functionalities. We track all discovered vulnerabilities and released patches, and allow admins or technicians to easily patch all endpoints with a flexible configuration and detailed reporting. Acronis Cyber Protect supports not only all embedded Windows apps, but also more than 230 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, things become much harder. At the very least, you will need to be sure that Windows gets all updates it needs and that they are installed promptly. Users tend to ignore system messages, especially when Windows asks for a restart. This is a big mistake. Be sure that auto updates to popular software vendors like Adobe are enabled and apps like PDF Reader are also updated promptly.



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

Themed phishing and malicious websites appear in large numbers every day, and are typically filtered out on a browser level; but with cyber protection solutions like Acronis Cyber Protect, you also gain dedicated URL filtering functionality. The same functionality is available in endpoint protection solutions, although in Acronis Cyber Protect we have a special category related to public health topics, which is updated with greater priority. Remember that malicious links typically come from somewhere: your instant messenger, email, forum posts, etc. Don't click on links you don't need to click, or that you don't expect to receive.

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

Use VPN while working with business data

No matter if you connect to remote company sources and services, or if your work doesn't require those activities and you just browse some web resources and use telecommunication tools, always use a Virtual Private Network (VPN). If you have a VPN procedure in your company, you most likely will get instructions from your admin or MSP technician. If you have to secure your workplace yourself, use well-known recommended VPN apps and services that are widely available in software marketplaces, or directly from vendors. A VPN encrypts all your traffic, making it secure in case a hacker attempts to capture your data in transit.

Be sure your cybersecurity is running properly

In **Acronis Cyber Protect**, we use many well-balanced and tuned security technologies, including several detection engines. We recommend using it instead of an embedded Windows solution.

But just having an antimalware defense in place is not enough; it should be configured properly. This means that:

- A full scan should be performed at least once every day.
- A product needs to get updates daily or hourly, depending on how often they are available.
- 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 upon every new software installed or executed.

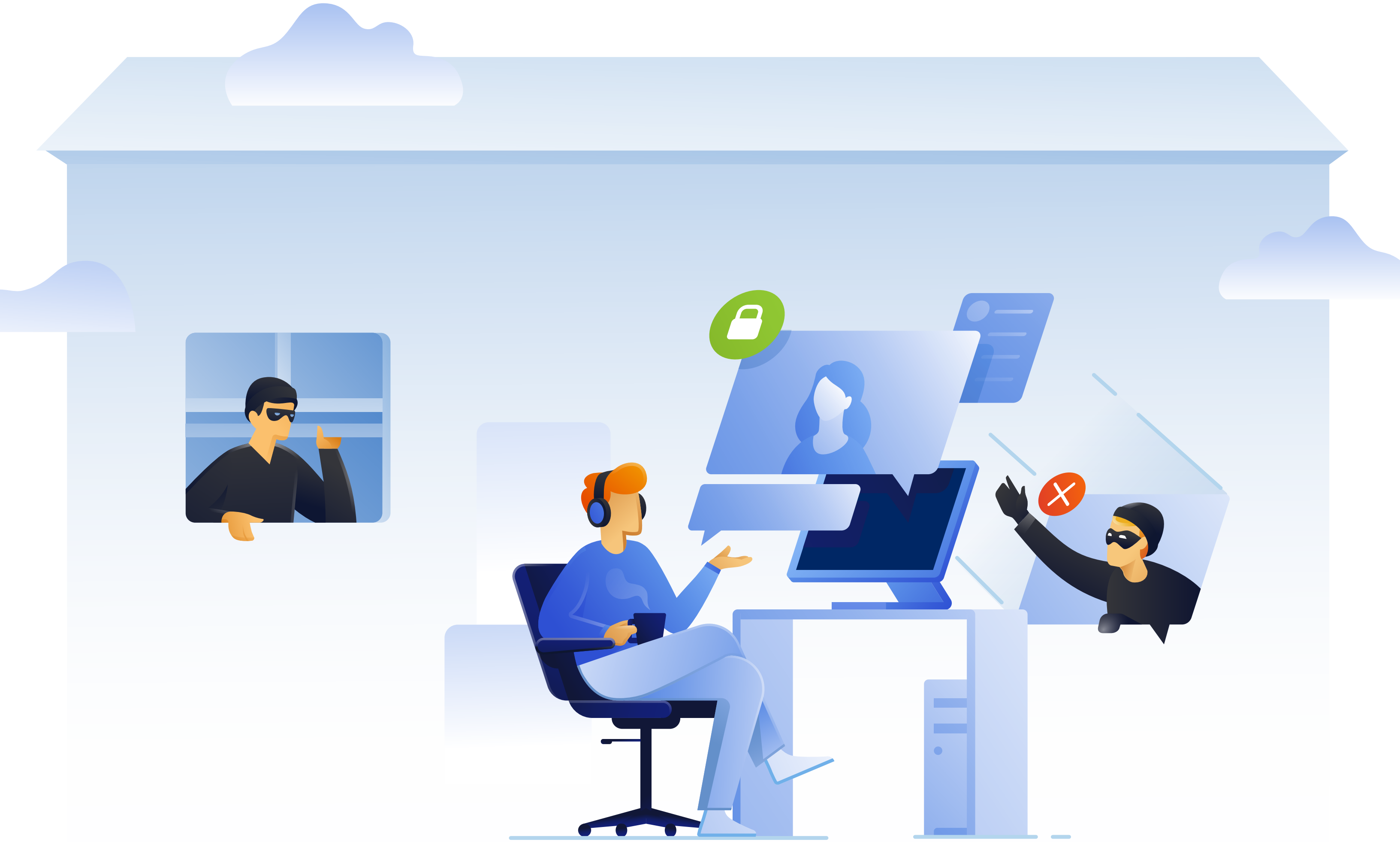
Additionally, **don't ignore messages coming from your antimalware solution.** Read them carefully and be sure that the license is legitimate if you're using a paid version from a security vendor.

Keep your passwords and your working space to yourself

Security tip number one: make sure that your passwords and your employee passwords are strong and private. Never share passwords with anyone, and use different and long passwords for every service you use. To help you remember them, use password manager software. Alternately, the easiest way to create strong passwords is through a set of long phrases you can remember. Eight character passwords are easily brute-forced nowadays.

In a secure product like Acronis Cyber Cloud or Acronis Cyber Backup, we never store passwords anywhere, so once forgotten, it will put an end to access to your data.

Also, even when working from home, do not forget to lock your laptop or desktop and limit access to it. There have been many cases where people could simply steal sensitive information off a non-locked PC, even from a distance.



About Acronis

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

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. 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 25 languages. For more information, visit www.acronis.com