Acronis

Report 2020

Acronis Cyberthreats Report 2020

Cybersecurity trends of 2021, the year of extortion

Acronis Cyberthreats Report 2020

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 to implement complete integrated cyber protection to protect all data, applications and systems. Cyber protection requires researching and monitoring of threats, as well as abiding by the Five Vectors of Cyber Protection – safety, accessibility, privacy, authenticity, and security (SAPAS). As part of the strategy, we've established three Cyber Protection Operation Centers (CPOC) around the world to monitor and research cyberthreats 24/7.

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

This report covers the threat landscape, as per encountered by our sensors and analysts in 2020.

The general malware data presented in the report is gathered from June to October this year, after the launch of Acronis Cyber Protect in May 2020, and reflects the threats targeting endpoints that we detected during these past months.

This report represents a global outlook and is based on more than 100,000 unique endpoints distributed around the world. Only threats for Windows operating systems are reflected in this report because they are much more prevalent than those targeting macOS. We will continue to watch how the situation develops and may include data on macOS threats in the next year's report.

THE TOP FIVE NUMBERS OF 2020:

- **31%** of global companies are attacked by cybercriminals at least once a day
- Maze ransomware accounted for almost **50%** of all known ransomware cases
- More than **1000** companies had their data leaked after ransomware attacks
- Microsoft patched close to **1,000** flaws in its products in just nine months.
- The average life-time of a malware sample is **3.4** days

CYBERSECURITY TRENDS WE IDENTIFY AS KEY IN 2021:

- Attacks on remote workers will only increase.
- Data exfiltration will become bigger than data encryption
- More attacks on MSPs, small business, and cloud
- Ransomware will be looking at new targets
- Attackers will use more automation and the number of malware samples will rise

WHAT YOU WILL FIND IN THIS REPORT:

- Top security/threat trends we observed in 2020
- General malware statistics and key families reviewed
- Ransomware statistics with a deep-dive analysis of the most dangerous threats
- Why confidential data exposure is stage two in most successful ransomware attacks
- Which vulnerabilities contribute to the success of attacks
- Why MSPs are increasingly under threat
- Our security forecast and recommendations for 2021

Part 1

Key cyberthreats and trends of 2020

1. COVID-19 themed exploitations
2. Remote workers under attack
3. Cybercriminals focus on MSPs
4. Ransomware is still the number one threat
5. Simple backup and security are not enough anymore

The COVID-19 pandemic, which started at the very end of 2019, had a dramatic effect on our lives around the world. But apart from the obvious dangers to human health and a huge economic impact, the pandemic changed the digital world, the way we work, and the way we spend our free time online.

As travel ceased, most businesses and services had to switch to online operations. The ones who already were online had to expand, others had to introduce completely new processes. Government, medical, and service organizations had to adopt new means to meet everyday needs.

Business meetings migrated to telecommunication apps like Zoom, Webex, and Microsoft Teams, which became the new standard. Office workers were sent home, often in a rush and without proper support, resorting to their own equipment to perform their work.

Unfortunately, cybercriminals saw clear opportunities in these challenges and actively increased their attacks, leaving human compassion and mercy behind.

1. COVID-19 themed exploitations

As expected, people rushed online to get information about the new pandemic: how they can protect themselves, what the latest news is, what assistance they can count on, and so on. This interest resulted in a huge number of scams and other kinds of exploits.

Cybercriminals continue to use old tricks to exploit the COVID-19 theme in their cyberattacks, tricking victims to enter their credentials or personal information on a phishing web page, or loading malicious payloads into documents that pretend to contain essential information related to the pandemic. There are other notable approaches, and the following examples are some of the COVID-19 themed scams that we have encountered.

Fake free testing

The latest version of Trickbot/Qakbot/Qbot malware was spread in numerous phishing emails that offered free COVID-19 testing. Victims were asked to fill out an attached form, which turned out to be a fake document embedded with a malicious script. To avoid revealing its payload in malware sandboxes, the script wouldn't start downloading its payload until after some time had passed.

The lure document uses a standard gimmick to trick users into clicking 'Enable content' which allows the execution of the malicious VBA script that is embedded.

Fake financial support

In many cases, cyberattacks stayed local based on how the country was hit by COVID-19. For instance, the state of North Rhine-Westphalia (NRW) in Germany fell victim to a phishing campaign. Attackers created rogue copies of the NRW Ministry of Economic Affairs' website for requesting COVID-19 financial aid. The fraudsters collected the personal data submitted by victims and then submitted their own requests to the

legitimate website using the victims' information but the criminals' bank account. NRW officials reported that up to 4,000 fake requests had been granted, resulting in up to $109 million being sent to the scammers.

Scams around remote education

Criminals also focused on exploiting based on remote education. A new pandemic-themed phishing email delivered a Formbook Trojan embedded into a bogus grading application for school teachers. Formbook is a type of infostealer malware capable of stealing login credentials from internet browsers. It has been promoted on hacking forums since February 2016.

Interestingly, the attackers employed several anti-analysis and anti-detection techniques such as sandbox detection and virtual machine detection, steganography, and XOR encryption to hide the payload, thereby effectively evading Windows Defender.

The criminals behind Formbook campaigns have also been known to attack biomedical firms to steal financial resources, sensitive personal data, and intellectual property.

Fake medical leave documents

The Trickbot campaign also exploited COVID-19 pandemic fears to spread a malicious document entitled: "Family and Medical Leave of Act 22.04.doc" (SHA256: 875d0b66ab7252cf8fe6ab23e31926 b43c1af6dfad6d196f311e64ed65e7c0ce).

The authentic Family Medical Leave Act (FMLA) provides employees the right to have medical leave benefits. However, once the user activates the macro in these fraudulent documents, malicious script starts downloading additional malware onto the computer.

A new type of sextortion

We came across a new variation of sextortion scam. The cybercriminals still use a previously leaked password as a convincing element, but instead of threatening to release a recorded video, they threaten the life of the user. The cybercriminals claim to know the exact location and daily routines of the victim. They further declare that they "could even infect your whole family with the coronavirus". To stop them from doing so, they demand that $4,000 in bitcoins be transferred.

It's not the first time that scammers have threatened the life of users. In the past, we had seen examples where they threatened to send hooligans to beat people up – but the COVID-19 threat brings it to a new level.

Most of these emails are sent from randomly spoofed email addresses or real email accounts. Of course, the message itself should be a clear indication that it is a scam and that you can simply delete the email.

Chasing governments' and private companies' COVID-19 secrets

Certain valuable data related to the COVID-19 pandemic and suspected by some analysts to have been kept secret by the Chinese government is attracting hackers from around the world. For example, the Vietnamese state-sponsored hacking group APT32 (also known as the OceanLotus Group) reportedly attacked Chinese state organizations hoping to steal virus control measures, medical research, and statistics revealing the number of infections that allegedly have not been disclosed by China. Vietnam is a neighbor of China and its interest in part appears to be motivated by its desire to control the spread of the pandemic around the region.

The Chinese company Huiying Medical, which is purported to have developed AI that can diagnose COVID-19 based on computed tomography (CT) scanning images with 96% accuracy, was allegedly hacked. According to cybersecurity firm Cyble, a hacker dubbed "THE0TIME" put Huiying Medical data up for sale on the Dark Web that may contain user information, source code, and reports on experiments at an asking price of four bitcoin (approx. $30,000 at the time).

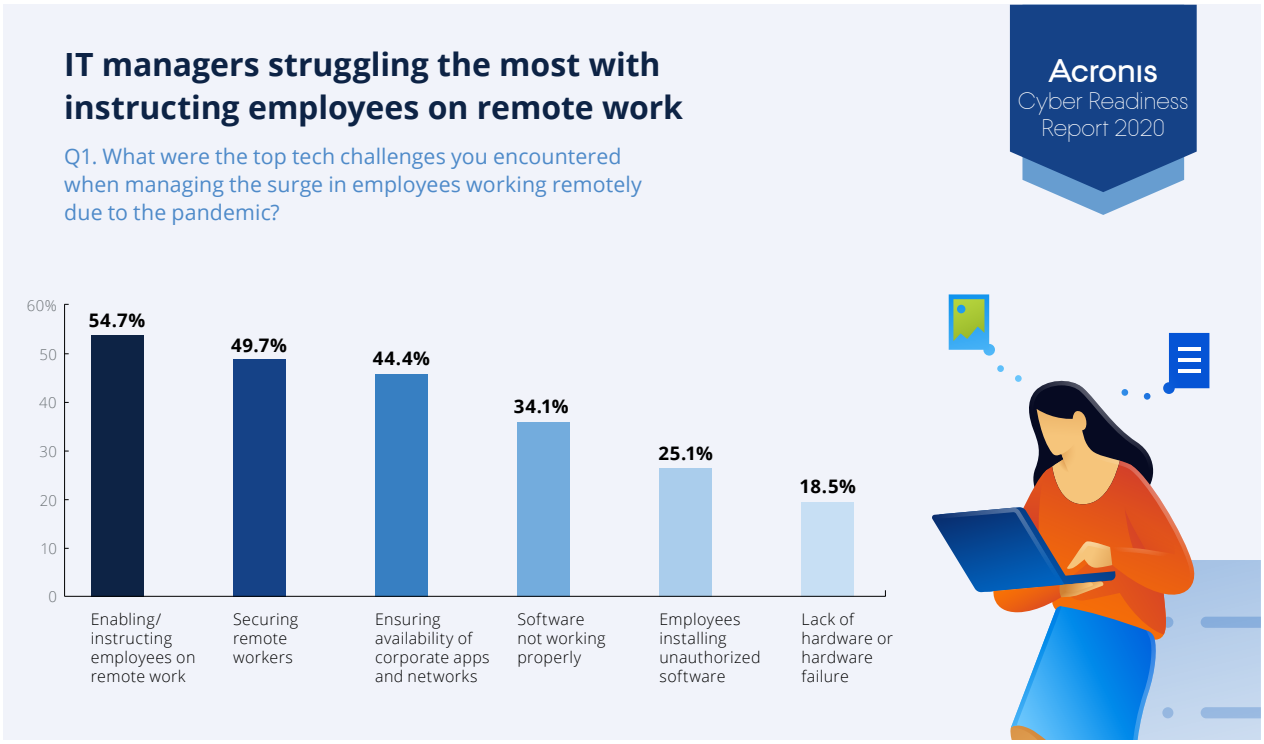
Other ATP groups attacked pharmaceutical companies and vaccination laboratories in order to steal relevant data.

2. Remote workers under attack

The COVID-19 pandemic has significantly changed the threat landscape, highlighting numerous security and privacy risks associated with remote work operations – including remote access to internal company servers, virtual conferencing, and security training among employees.

To assess how well IT teams faced this experience – where they were best able to transition to remote environments and where there was a clear opportunity for improvement – we developed our first-ever Acronis Cyber Readiness Report. For this report, we surveyed 3,400 companies and remote workers from around the world in June and July 2020 about the threats, challenges, and trends they've seen since switching to remote work. Results are alarming:

- Nearly half of all IT managers struggled to instruct and secure remote workers.
- 31% of global companies are attacked by cybercriminals at least once a day. The most common attack types were phishing attempts, DDoS attacks, and videoconferencing attacks.
- 92% of global organizations had to adopt new technologies to complete the switch to remote work. As a result, 72% of global organizations saw their IT costs increase during the pandemic.
- Successful attacks remain frequent, despite increased tech spending, because organizations aren't prioritizing defensive capabilities properly.
- 39% of all companies reported video conferencing attacks during the pandemic.



Coronavirus increases Zoom attacks

The onset of the COVID-19 pandemic saw the Zoom virtual conferencing platform attracting unwanted attention from cybercriminals. With the increased user base, more and more people started analyzing the Zoom code for weaknesses and raising privacy concerns.

For example, Vice.com reported that two zero-day vulnerabilities - security holes that vendors were not aware of and thus had no patches for - were available on the Dark Web market: one for Windows and another for macOS. The Zoom Windows RCE (Remote Code Execution) exploit was for sale for $500,000.

Zoom also became the target of a phishing campaign aimed at stealing service credentials. Phishing emails were delivered to more than 50,000 mailboxes, targeting Microsoft 365 users with a fake email invitation to an upcoming Zoom call with the human resources department to discuss a performance review (a topic designed to induce anxiety in the victim that might crowd out their normal wariness of clicking on an email link). Such phishing attacks, in combination with credential stuffing attacks where attackers check if the user shared the same password on multiple services, led to over 500,000 Zoom user credentials floating around on underground forums.

The fact that many Zoom videoconferences didn't have a password set also attracted cybercriminals. People started trying out all possible meeting ID numbers, till they found an ongoing meeting call. They then joined the call and disturbed the participants by playing videos, loud music, or other inappropriate materials. These Zoom-bombing attacks led to many schools stopping their remote teaching programs.

Not only Zoom: Microsoft 365 users attacked as well

Of course, Zoom was not the only collaboration tool in the crosshairs of the attackers. Similar attacks happened to Microsoft Teams and Webex. For example, up to 50,000 Microsoft 365 users were attacked within a week with

phishing emails containing fake Microsoft Teams notifications that redirect victims to a fake Microsoft 365 login page.

Microsoft file-sharing services such as Sway, SharePoint, and OneNote were attacked via several small phishing campaigns that targeted financial service companies, law firms, and real estate groups. One attack, named PerSwaysion for its abuse of Sway services, executed in three steps. It starts by sending phishing emails that contain a malicious PDF attachment, purporting to be a Microsoft 365 file sharing notification with a "Read Now" hyperlink. Clicking on the link opens another decoy document in Microsoft file-sharing services (notably Sway) with another "Read Now" link that takes the victim to a bogus Microsoft sign-in page that steals their credentials.

Lack of security for work-from-home staff

Now that some people have to work from home on their own computers security threats are rampant. Not only do those home machines often lack effective cyber protection, but many users also don't regularly apply the latest security patches for their operating system and popular third-party software, leaving their machines vulnerable. Many of these private machines are not managed by the IT department and therefore no company policies are applied to them.

Covering these vulnerabilities and patch management issues on the edge became a headache for admins and technicians that provide the IT support to help small businesses survive during this emergency.

In addition to this, home networks are often exposed to other unprotected devices, often from kids and other members of the family. Furthermore, the broadband router is often outdated, allowing attackers to hijack the router and potentially redirect specific traffic.

3. Cybercriminals focus on MSPs

Since a lot of small- and medium-sized businesses are serviced by managed service providers (MSPs), many MSPs became victims of cyberattacks. The logic is straightforward: instead of compromising 100 different companies, the criminals only need to hack one MSP to get access to 100 clients. Attacks in 2020 showed that MSPs can be compromised via a variety of techniques, with poorly configured remote access software being among the top attack vectors. Cybercriminals used vulnerabilities, the lack of two-factor authentication (2FA), and phishing to get access to MSPs management tools and eventually to their clients' machines.

The global IT services and solutions provider DXC Technology announced a ransomware attack on systems from its Xchanging subsidiary, for example. Xchanging primarily services businesses in the insurance industry but its list of customers includes companies from other fields: financial

services, aerospace, defense, automotive, education, consumer packaged goods, healthcare, and manufacturing. Another example was Canadian MSP Pivot Technology Solutions, which disclosed a cyberattack on its IT infrastructure. Pivot Technology suffered a data breach following a ransomware attack and the incident might have affected the personal information of customers. This scenario is typical for 2020 and we expect more of these cases to emerge.

4. Ransomware is still the number one threat

Clearly, 2020 has been a year of ransomware with more attacks, higher losses, and new extortion techniques being implemented by cybercriminals. Big cases become public practically every week. According to a report published by Coalition, one of the largest providers of cyberinsurance services in North America, ransomware cases have accounted for 41% of cyberinsurance claims filed in the first half of 2020. "Ransomware doesn't discriminate by industry. We've seen an increase in ransom attacks across almost every industry we serve," reports Coalition. We at Acronis can confirm that fact.

See the detailed statistics from our Cyber Protection Operation Centers in further sections of this report, here we outline the grim trends on a high level.

Big targets bring big ransoms

On July 18, Argentina's largest telecom provider was hit by a ransomware attack — likely by the Sodinokibi group — demanding a $7.5 million ransom. As is typical of many attackers who want to force a quick decision from the victim, this demand was set to double if not paid within 48 hours. The ransomware allegedly infected more than 18,000 workstations, including terminals with highly sensitive data.

Garmin, one of the world's largest wearable device companies, confirmed that the major outage that began on July 24 was due to a WastedLocker ransomware attack. This attack forced Garmin to halt contact center operations, Garmin Connect, and even production lines in Taiwan. With an estimated $4 billion in annual revenue, Garmin is certainly a high-value target. The requested ransom amount is believed to be $10 million. Other recent WastedLocker attacks have demanded amounts ranging from $500,000 to millions.

The list of high-ransom victims goes on. In February, the FBI published estimates for the profits of some ransomware groups. The list indicated that groups like Ryuk made about $3 million per month in 2019. With paydays like that, it's unlikely that the threat will decrease anytime soon.

What's more, modern ransomware families not only demand a ransom for decrypting data but also for not disclosing stolen confidential data to the public, which increases their chances of a payout even more.

Demanding ransom for non-disclosure

The REvil/Sodinokibi ransomware group announced on August 14 that they had compromised the Kentucky-based Brown-Forman — the parent company of whiskey brands Jack Daniels, Old Forester, The Glendronach, and various other wines and spirits. With a 2020 annual report showing gross profits of more than $2 billion and a net income of $872 million, Brown-Forman is an undeniably high-value target for ransomware operators.

The REvil group claimed to have stolen 1TB of data, including confidential employee information, financial data, internal communications, and company agreements. Images posted on their leak site indicate that they possess data dating back at least as far as 2009.

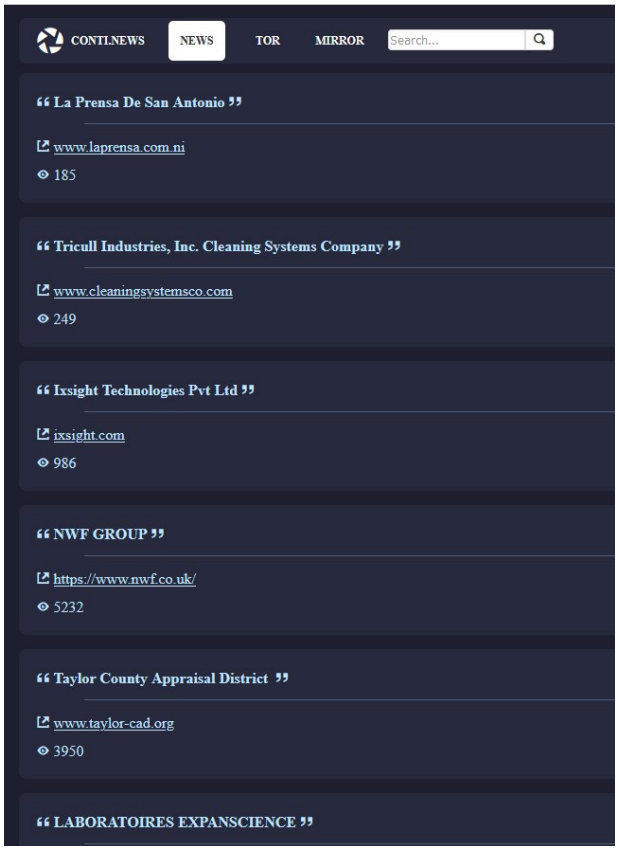
Canon, the multinational corporation specializing in optical and imaging products, fell victim to a Maze ransomware attack that impacted their email system, Microsoft Teams, their U.S. website, and other internal applications. The Maze ransomware operators stated that they stole more than 10TB of data from Canon, including private databases. Canon acknowledged the attack in an internal message sent to employees.

CWT, one of the world's largest travel and event management companies, was compromised by the Ragnar Locker ransomware. The attackers allegedly stole 2TB of sensitive corporate data and claim to have compromised more than 30,000 systems. While the attackers initially demanded $10 million for the safe return of stolen data, CWT entered negotiations and eventually agreed to pay a ransom of 414 bitcoin — equal to more than $4 million at the time of writing.

Conti, a new ransomware as a service (RaaS) and the successor of the notorious Ryuk variant, released a data leak website as part of its extortion strategy to force victims into paying a ransom. While Conti has been active for several months, it wasn't until recently that the cybercriminals publicly released a data leak site where they threaten to publish victims' stolen data if the demanded ransom is not paid. "Conti.News" currently lists 112 victims, including large and well-known companies.

In total, about 20 different ransomware groups have created dedicated pages for data leaks, hosted on the Tor underground network. More than 700 companies have had their data published – 37% of leaks came from Maze ransomware infections, followed by Conti with 15%, and Sodinokibi with 12%.

These data breaches can result in reputation loss, follow-up attacks, and various fines. Plus, the leak of customer data might be punishable under privacy regulations such as GDPR or CCPA, and paying the ransom could be an offense under the U.S. OFAC regulation.



5. Simple backup and security are not enough anymore

We have been predicting that ransomware will attack backup solutions since 2016. That projection was made because initiatives like No More Ransom, which Acronis has been a proud member of since 2017, motivate people and companies to not pay ransoms and, instead, properly protect machines from ransomware. If you have a backup, you don't need to pay a ransom, since you can restore from it. That was the key idea, but cybercriminals quickly caught on. Since 2017, practically every ransomware strain began deleting or disabling Windows volume shadow copies and tried to disable traditional backup solutions. As many of these backup solutions have very basic self-protection capabilities - or none at all - this was easy. The test made by AMTSO member laboratory NioGuard is a good reflection of this grim situation.

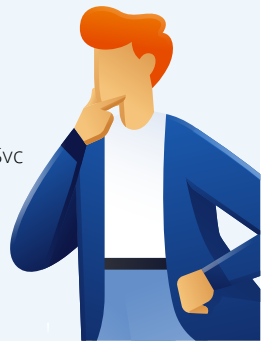
Let's take a look at some recent ransomware examples.

CONTI RANSOMWARE:

- The average demand for this ransomware is under $100,000
- Uses Windows Restart Manager to close any open or unsaved files before encryption
- Contains more than 250 strings decryption routines and about 150 services to be terminated
- Performs fast file encryption in 32 simultaneous threads using Windows I/O Completion Ports
- Follows the trend and recently has launched the 'Conti.News' data leak site

What's more, the ransomware deletes shadow copies of the files and resizes shadow storages for disks from C: to H: that may also result in shadow copies disappearing. It also stops services that belong to SQL, antivirus, cybersecurity, and backup solutions such as BackupExec and Veeam. It also tries to terminate the Acronis Cyber Protect solution but fails due to our self-protection feature. The list contains about 150 services, including:

Acronis VSS Provider	BackupExecRPCService	VeeamDeploySvc
Veeam Backup Catalog Data Service	BackupExecVSSProvider	VeeamEnterpriseManagerSvc
AcronisAgent	EPSecurityService	VeeamMountSvc
AcrSch2Svc	EPUpdateService	VeeamNFSSvc
Antivirus	mozyprobackup	VeeamRESTSvc
BackupExecAgentAccelerator	VeeamBackupSvc	VeeamTransportSvc
BackupExecAgentBrowser	VeeamBrokerSvc	VeeamHvIntegrationSvc
BackupExecDeviceMediaService	VeeamCatalogSvc	Zoolz 2 Service
BackupExecJobEngine	VeeamCloudSvc	AVP
BackupExecManagementService	VeeamDeploymentService	



NETWALKER RANSOMWARE:

Another example is Netwalker ransomware, which was discovered in the wild in August 2019. It implements the RaaS model and targets organizations as well as individual users. Since March 2020, they managed to extort approximately $25 million. The distinguishing trait of the most recent version of Netwalker is the usage of the heavily obfuscated PowerShell loader to start ransomware on an infected system. The use of PowerShell script, or in general the abuse of any preinstalled tools under the tactic of living off the land, remains popular among cybercriminals.

Similar to many other ransomware strains, Netwalker deletes Windows shadow copies of the files.

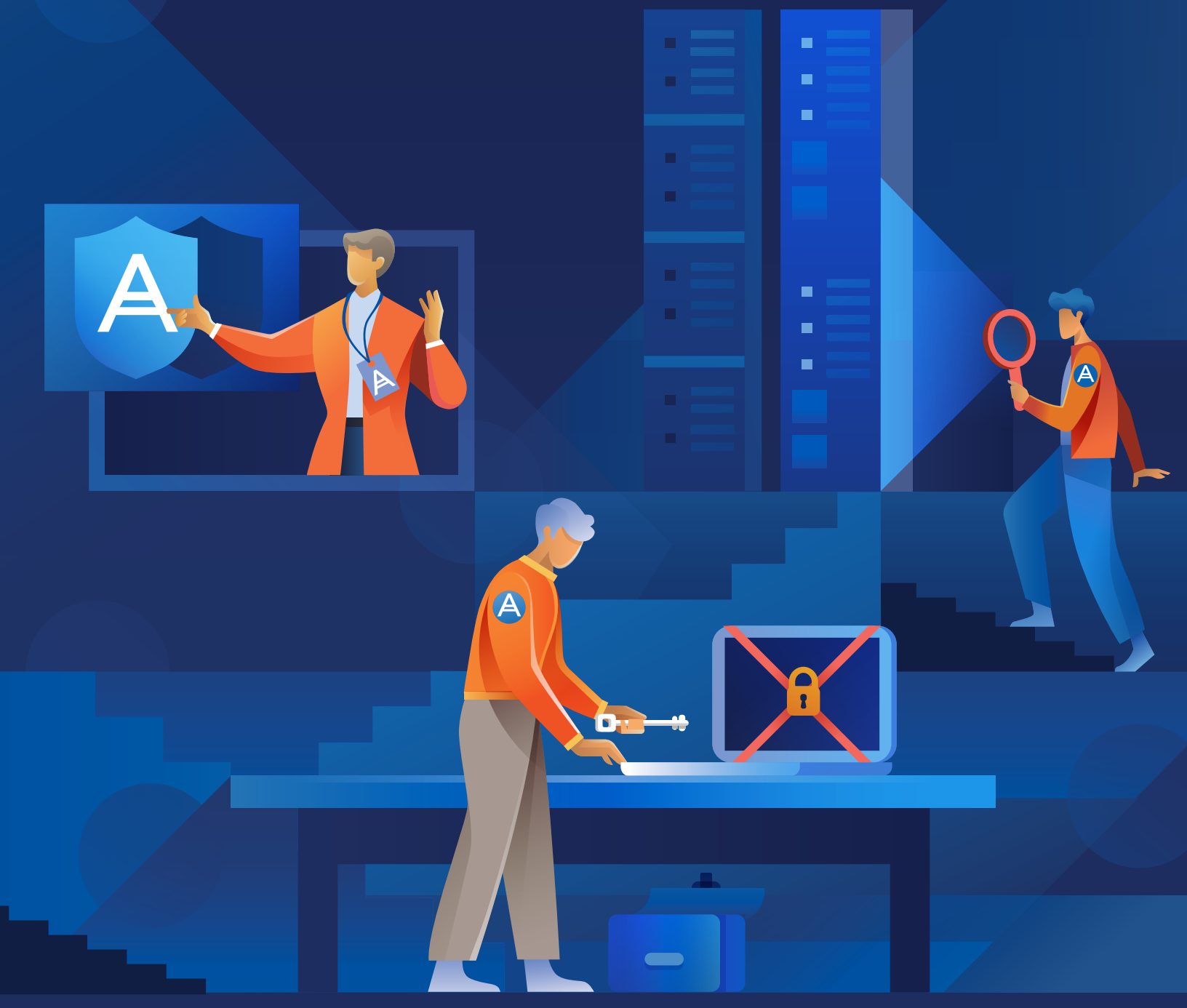
```
Get-Wmiobject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null
```

Netwalker also attempts to stop the backup services that begin with the following strings – in order to prevent restoration:

veeam*	ShadowProtectSvc	StorageCraft ImageManager
backup*	AcronisAgent	acrsch2svc*
backup	AcrSch2Svc	

Part 2

General malware threat

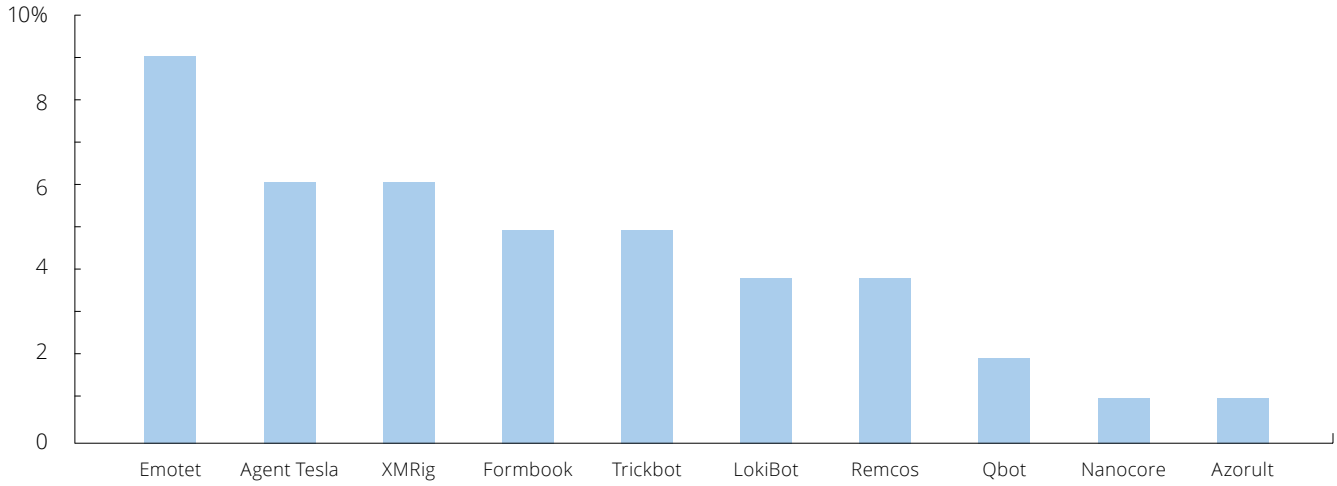


In Q3 2020, an average of 11% of our clients had at least one malware attack successfully blocked. The numbers declined slightly back to normal levels since the beginning of the pandemic. In July, it was still 14.7%, followed by 10.1% in August, 8.9% in September, and 6.7% in October.

The country with the most clients experiencing malware detections in Q3 2020 was the United States with 27.9%, followed by Germany with 16.7%, and the United Kingdom with 6.1%.

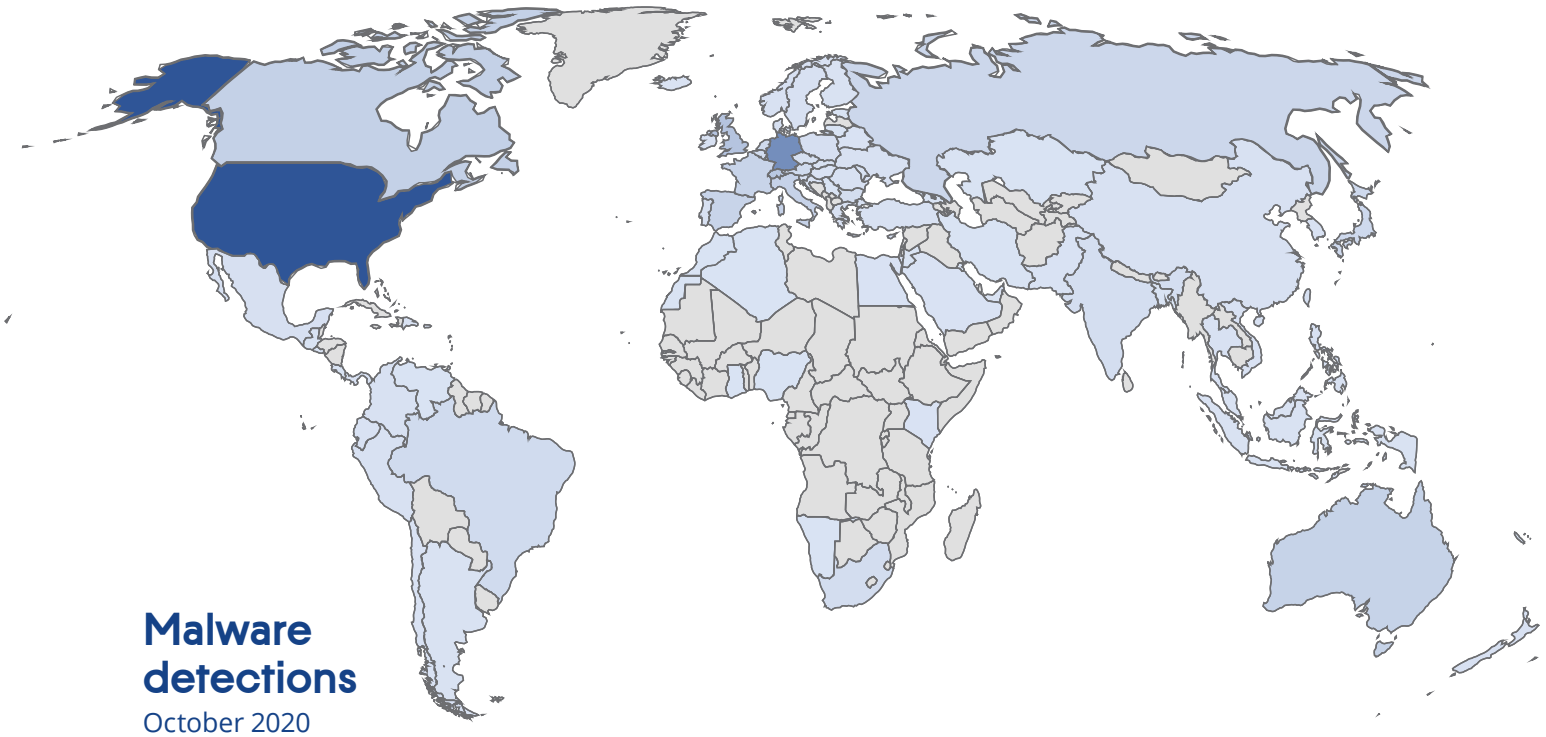
The independent malware testing lab AV-Test recorded 400,000 new malware samples per day in Q3 2020, which clearly indicates that cybercriminals are automating their process and generating a flood of new malware threats. However, most of these threats are only used for a handful of attacks in a very short time period. Of the samples that we encountered, 19% were only seen once. The average lifetime of a malicious sample was 3.4 days, before it disappeared and was never seen again.

These are the top 10 malware families we observed and tracked in 2020:



Monthly percentage of global detections per country

COUNTRY	OCT 2020	SEPT 2020	AUG 2020	JULY 2020
United States	27.5%	27.9%	29.3%	16.4%
Germany	18.4%	16.7%	16.8%	4.3%
Switzerland	7.2%	5.4%	3.6%	3.2%
United Kingdom	5.9%	6.1%	6.4%	4.5%
Canada	3.0%	3.6%	3.6%	1.5%
France	3.0%	2.9%	3.3%	2.3%
Italy	3.0%	3.2%	3.3%	1.7%
Australia	3.0%	3.3%	3.1%	2.0%
Spain	2.6%	3.0%	2.8%	4.2%
Japan	2.0%	2.3%	3.2%	15.7%



Malware detections

October 2020

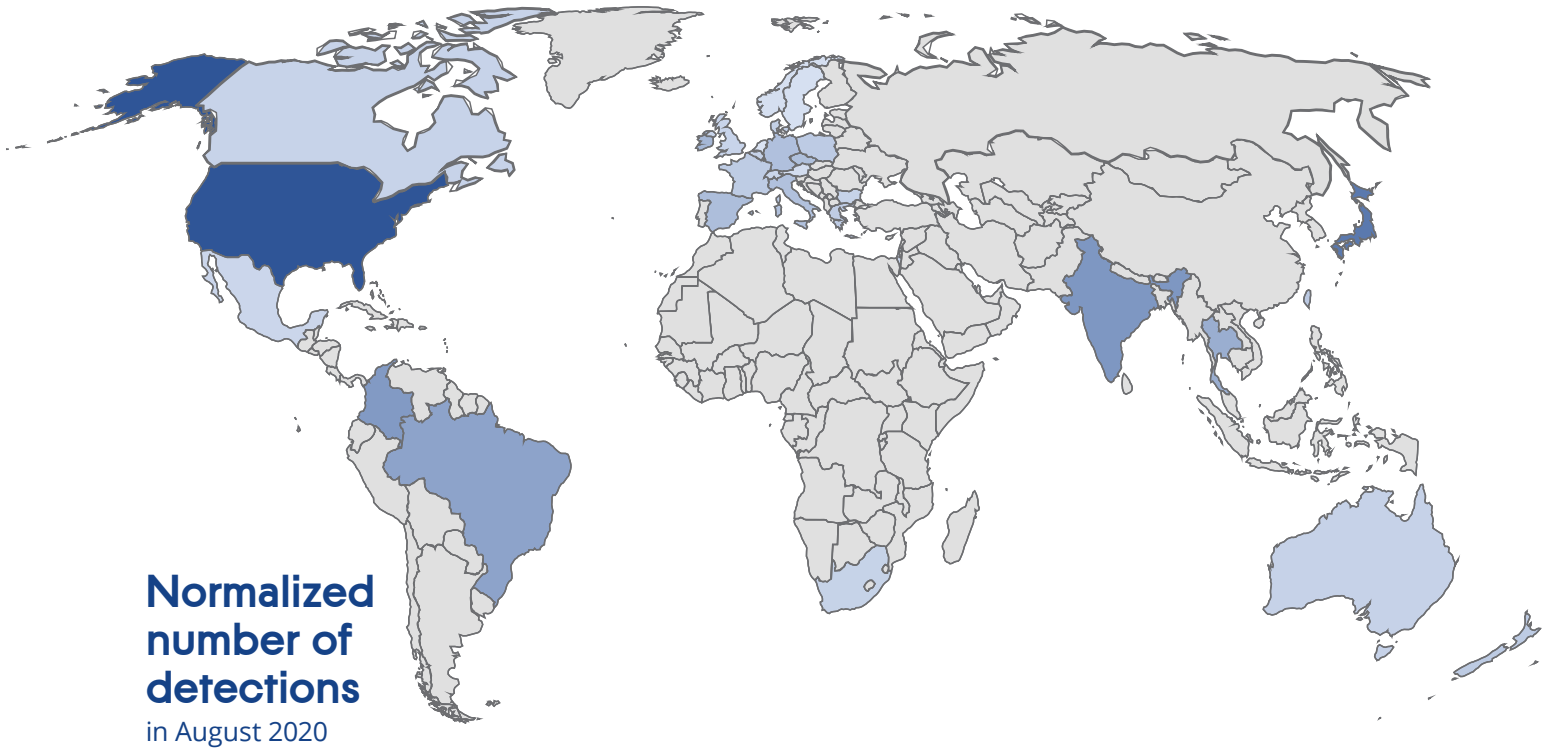
Percentage

0% 0,27%

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	MALWARE DETECTION per 1,000 clients seen in August
1	United States	2,059
2	Japan	1,571
3	India	1,168
4	Colombia	1,123
5	Brazil	994
6	Thailand	856
7	Ireland	729
8	Spain	634
9	Czech Republic	611
10	Germany	601
11	Italy	589

RANK	COUNTRY	MALWARE DETECTION per 1,000 clients seen in August
12	Hong Kong	518
13	Taiwan	480
14	New Zealand	462
15	Poland	453
16	France	444
17	Greece	437
18	Denmark	375
19	Australia	361
20	Belgium	358
21	South Africa	351
22	Bulgaria	351
23	Canada	347
24	United Kingdom	329
25	Switzerland	311



Normalized number of detections
in August 2020

Number of detections per 1,000 clients

131 2,059

Ransomware threat

As we already mentioned in the key trends section, ransomware is still the number one cyberthreat for businesses. While we observed ransomware from 2017 when Acronis Active Protection was first developed, in this section we're focusing on data from January 1 to October 31, 2020.

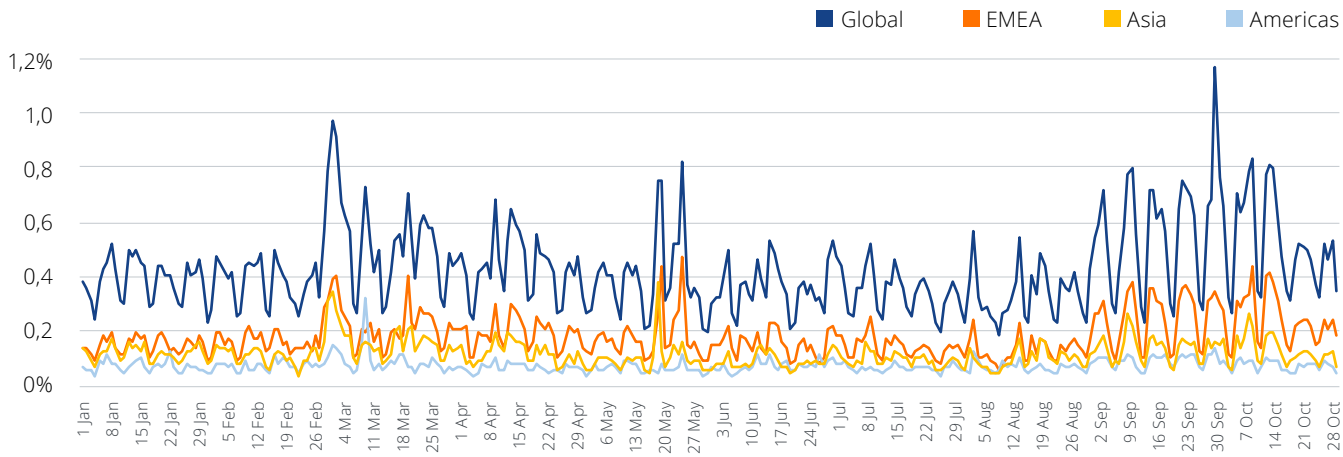
These are the top 10 ransomware families we observed and tracked in 2020. Keep in mind that some groups try to infect as many end users as possible with a broad approach, while others focus on high value targets, where they only attempt a handful of infections but strive for a high payout. Hence the volume of threat detection alone is not an indication of how dangerous a threat is.

1. Maze
2. REvil/Sodinokibi
3. SNAKE (EKANS)
4. Nemty
5. NetWalker (aka Mailto)
6. Ragnar Locker
7. MegaCortex
8. CLOP
9. DoppelPaymer
10. Thanos

For the last nine months, we saw around 50 new ransomware families emerge. Some are smaller groups focusing on consumers, but the trend with new groups like Avaddon, Mount Locker, and Suncrypt is to go after the more profitable corporations. More and more of 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

This year we observed a clear global spike at the start of the COVID-19 lockdown in March. Since that time, ransomware activity stayed at higher than normal levels. Regarding the attacked sectors or geographical regions, we have seen that there are no exemptions – all sectors are targeted by attackers. In September, we started to see another wave of ransomware attacks, especially against education and manufacturing companies in North America.



Top 10 countries: ransomware detections by region

Asia:

COUNTRY	Regional ransomware detections percentage in Q3 2020
Japan	17.7%
Philippines	13.3%
Taiwan	9.6%
China	8.6%
India	7.8%
Turkey	5.4%
Iran	5.3%
South Korea	3.9%
Indonesia	3.7%
Thailand	3.6%

EMEA:

COUNTRY	Regional ransomware detections percentage in Q3 2020
Germany	17.7%
France	13.3%
Italy	9.6%
United Kingdom	8.6%
Switzerland	7.8%
Spain	5.4%
Austria	5.3%
Netherlands	3.9%
Belgium	3.7%
Czech Republic	3.6%

Americas:

COUNTRY	Regional ransomware detections percentage in Q3 2020
United States	67.3%
Canada	15.9%
Chile	4.7%
Brazil	3.0%
Mexico	2.7%
Colombia	1.7%
Peru	1.0%
Argentina	0.8%
Bolivia	0.4%
Ecuador	0.3%

Ransomware groups in the spotlight

Evasive Maze ransomware encrypts and steals terabytes of private data in targeted attacks

Maze ransomware has been seen in targeted attacks since at least May 2019 and is allegedly responsible for the latest attack against Canon on July 30, 2020, resulting in the outage of the image.canon cloud storage service. Moreover, the Maze ransomware operator claimed to steal 10TB of private data as a part of the attack on Canon. The Maze operators already published the data from Xerox and LG that have been stolen during successful attack in June 2020, as the companies refused to pay a ransom.

- **Not only encrypts but also steals data to publish it later if a ransom is not paid**
- **Canon, Xerox, and LG are among the biggest victims of Maze**
- **Employs anti-disassembly and anti-debugging techniques**
- **Does not encrypt systems with a Russian default locale**
- **wmic.exe call to delete shadow copies is obfuscated**
- **Sends an HTTP check-in request to C&C server located in '91.218.114.0' network in Moscow, Russia**
- **Uses Mimikatz, Procdump, and Cobalt Strike hacking tools for proliferation**

Maze ransomware is typically delivered as the result of a targeted attack against an organization that starts with a spear-phishing email, getting access via compromised RDP or VDI (the credentials are usually bought on the Dark Web), and exploiting vulnerabilities in VPNs.

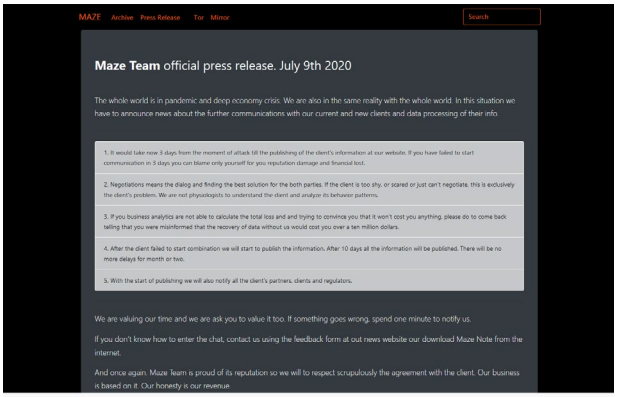
Once the Maze operator obtains access to the internal network of the organization, it runs Mimikatz and Procdump to harvest passwords stored in the memory and switch to reconnaissance using the Cobalt Strike red-teaming tool.

Maze uses anti-disassembly techniques to harden the code analysis in a disassembler.

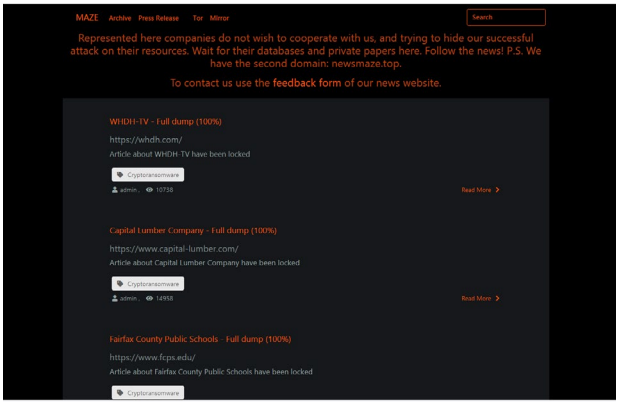
The obfuscation techniques include:

1. **Conditional jumps which redirect to the same location, replacing absolute jumps**
2. **Calls are followed by pushing the return address to the stack and jumping to the caller address.**

Additionally, Maze can detect if its code is being debugged. It checks the flag 'BeingDebugged' in the PEB structure if the process is run under a debugger. If so, the code goes into an infinite loop and does no encryption. Also, Maze kills the processes of the malware analysis tools and office tools by the hashes of the process names.



Maze ransomware is similar to recent ransomware strains such as WastedLocker, Netwalker, and REvil in that it not only encrypts, but also steals data. It uses 7zip utility to pack collected data and exfiltrate archives to the attacker's FTP server using the WinSCP client. In some incidents, it was reported that the exfiltrated data was also Base64 encoded.



All in all, this makes the Maze ransomware family one of the most dangerous we saw in 2020.

DarkSide ransomware does not attack hospitals, schools, and governments

DarkSide is a new ransomware strain. Attacks started at the beginning of August 2020, supposedly being run by the former affiliates of other ransomware campaigns that made money in the extortion business and decided to develop their own code. According to known incidents, the ransom payment is between $200,000 and $2,000,000. Like other ransomware used in targeted attacks, DarkSide not only encrypts user data but also exfiltrates data from the compromised servers.

Unlike the Maze ransomware that successfully attacked the Newhall school district and Fairfax County schools, DarkSide has a code of conduct that prohibits attacking hospitals, schools, and government organizations.

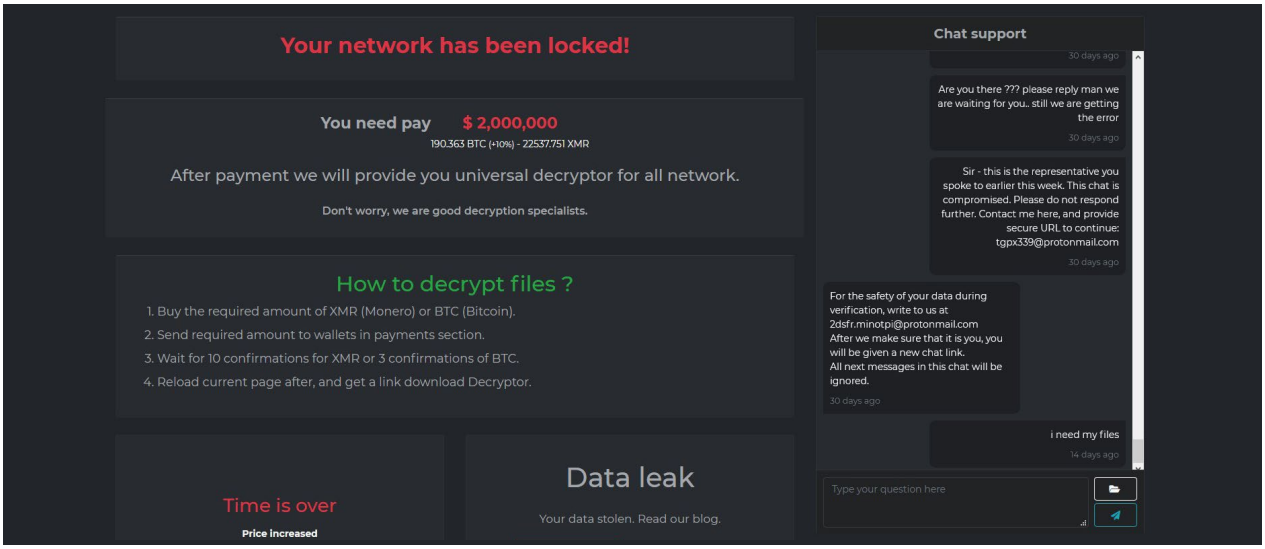
- **Discovered in August 2020**
- **Targets only English-speaking countries, avoiding former Soviet countries**
- **Does not attack hospitals, hospices, schools, universities, non-profit organizations, the government sector**
- **Uses Salsa20 with the custom matrix and RSA-1024 encryption algorithms**
- **Ransom payments vary from $200,000 to $2,000,000**

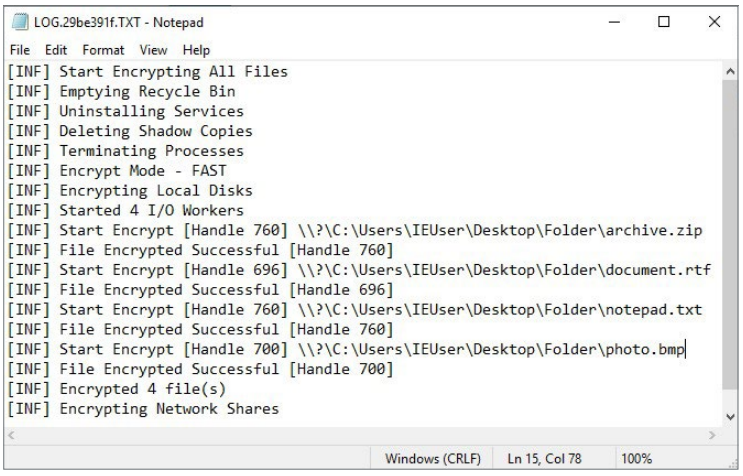
The ransomware empties the Recycle Bin without using the SHEmptyRecycleBinA() function to be stealthier. Instead, it removes files and folders thrown to the Recycle Bin one by one.

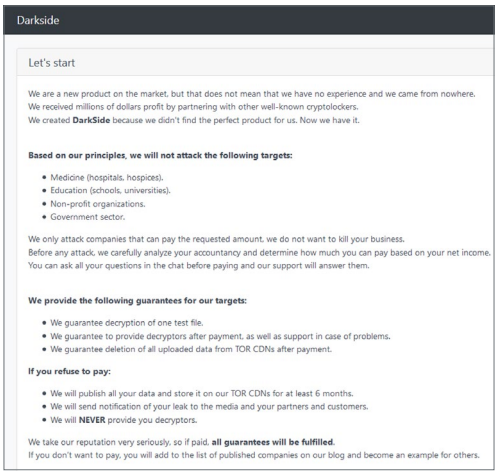
DarkSide uninstalls the following services related to security and backup solutions:

After Volume Shadow Copy Service (VSS) is uninstalled, the ransomware deletes shadow copies by launching an obfuscated PowerShell script. DarkSide also specifies a key, which needs to be entered on the first site. The key is not unique per user, but seems to be unique per sample, as the value is hardcoded and encrypted in the executable.

The conclusion here is the same: new ransomware families, even ones that aren't overly complicated, attack backups by default. Unfortunately, it's the new norm.







Malicious websites

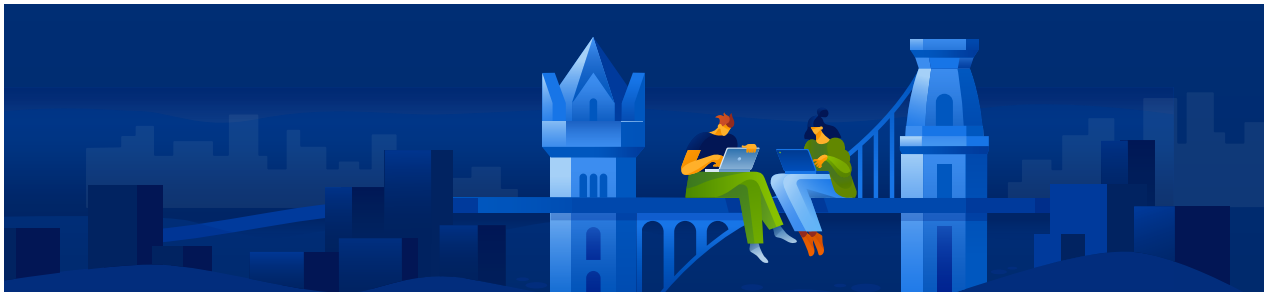
During the pandemic, we witnessed an increase in phishing attacks, especially against the collaboration tools and file sharing services that gained popularity as employees worked from home. After the initial spike in March, we observed a normalization of phishing attacks. Some of the cybercriminal groups seem to have switched back to malicious attachments. Even the notorious Emotet group returned in July after a five-month absence, sending malicious Office documents again.

MONTH	PERCENTAGE OF USERS that clicked on malicious URLs
June	5.5%
July	5.1%
August	2.3%
September	2.7%
October	3.4%

The largest percentage of blocked malicious URLs in Q3 2020 was in the United States with 16.4%. This was followed by Germany with 14.1% and the Czech Republic with 10.4%. However, 51% of the blocked URLs were encrypted HTTPS, making it more difficult to filter on the network. We have also observed more groups phishing 2FA tokens and then immediately using them with a script to log in. 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 – a tactic that can prevent automated scanning solutions from analyzing and blocking the phishing website.

Top 20 countries with the most blocked URLs in Q3

RANK	COUNTRY	PERCENT OF BLOCKED URLS IN Q3 2020
1	United States	16.4%
2	Germany	14.1%
3	Czech Republic	10.4%
4	Spain	8.3%
5	United Kingdom	6.7%
6	China	5.8%
7	South Africa	5.2%
8	Hong Kong	3.6%
9	Italy	3.4%
10	Australia	2.4%
11	France	2.1%
12	Canada	2.0%
13	Peru	1.9%
14	Norway	1.9%
15	Netherlands	1.8%
16	Japan	1.6%
17	Switzerland	1.6%
18	Bulgaria	0.9%
19	Singapore	0.8%
20	Austria	0.7%



Part 3

Vulnerabilities in Windows OS and software

1. Third-party apps are vulnerable and being used by bad guys as well
2. Most commonly exploited applications worldwide

The number of discovered vulnerabilities and released patches have skyrocketed in 2020. Risk Based Security's VulnDB team aggregated 11,121 vulnerabilities disclosed during the first half of 2020.

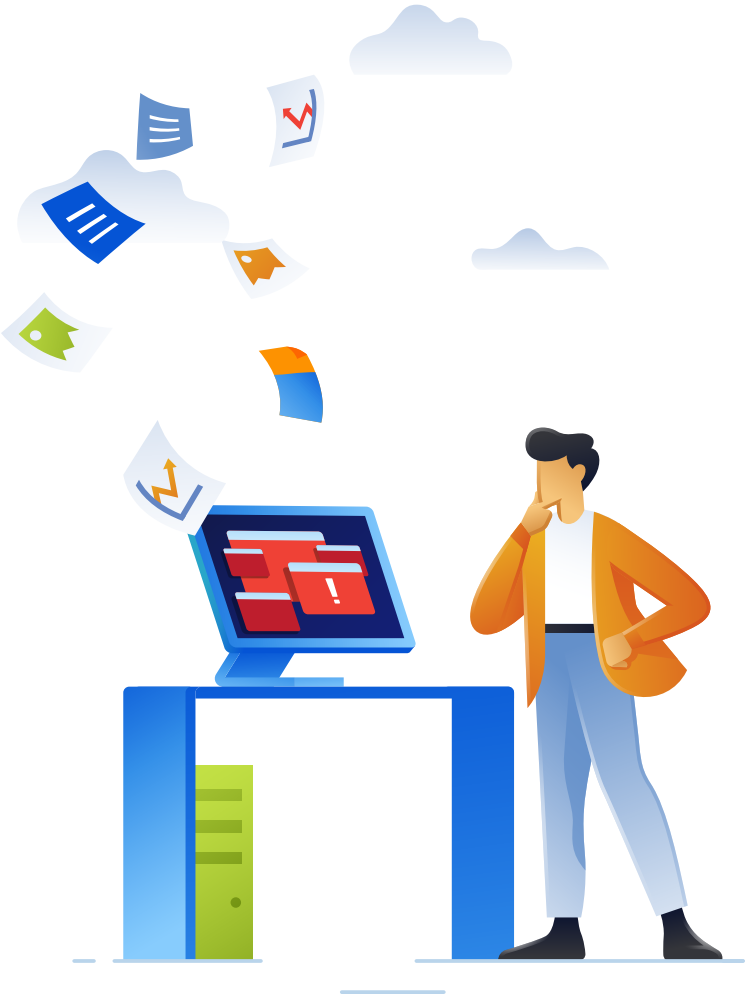
In the latest Microsoft patch in September, the company reported 129 closed security vulnerabilities, 23 of which could be exploited by malware to get complete control of Windows computers with little or no help from users. This is the seventh month in a row when Microsoft has shipped fixes for more than 100 flaws in its products, and the fourth month in a row that it fixed more than 120.

The problem is old: even if a vendor released a patch quickly, it doesn't mean it was patched everywhere. For example, CVE-2020-0796, better known today as SMBGhost, was thought so dangerous were it to be weaponized that it got the rarest of common vulnerability scoring system (CVSS) ratings: a "perfect" 10. Microsoft issued an emergency out of band fix within days. But cybersecurity firms around the globe, including Acronis, have still seen the vulnerability being used in the wild.

Similarly, the vulnerabilities indexed as CVE-2020-1425 and CVE-2020-1457, the two remote-code execution (RCE) flaws, are respectively rated as 'critical' and 'important' in severity. Both are related to Microsoft Windows Codecs Library, which handles objects in memory. An attacker who can exploit CVE-2020-1425 "could obtain information to further compromise the user's system", according to Microsoft. Successful exploitation of the second flaw, meanwhile, could enable attackers to execute arbitrary code on the targeted machine. Each flaw was given the "exploitation less likely" rating on Microsoft's Exploitability Index.

Some of these vulnerabilities are actively exploited, as we see in our data: CVE-2020-1020 and CVE-2020-0938. . As we reported on March 23, Microsoft confirmed these Windows vulnerabilities without a fix that were being actively exploited by attackers. Windows 10 users who do not get patched, when Microsoft released a fix, are at risk of an attacker being able to install programs, view or change data, and create new accounts.

Windows spoofing vulnerability CVE-2020-1464 is also widely attacked. A flaw exists when Windows incorrectly validates file signatures. An attacker who successfully exploits this could use a spoofed signature attached to a malicious executable to load any file and trick the OS into thinking it's legitimate. This vulnerability affects all supported versions of Windows and, if the patch is not yet applied, presents a major issue.



Third-party apps are vulnerable and being used by bad guys as well

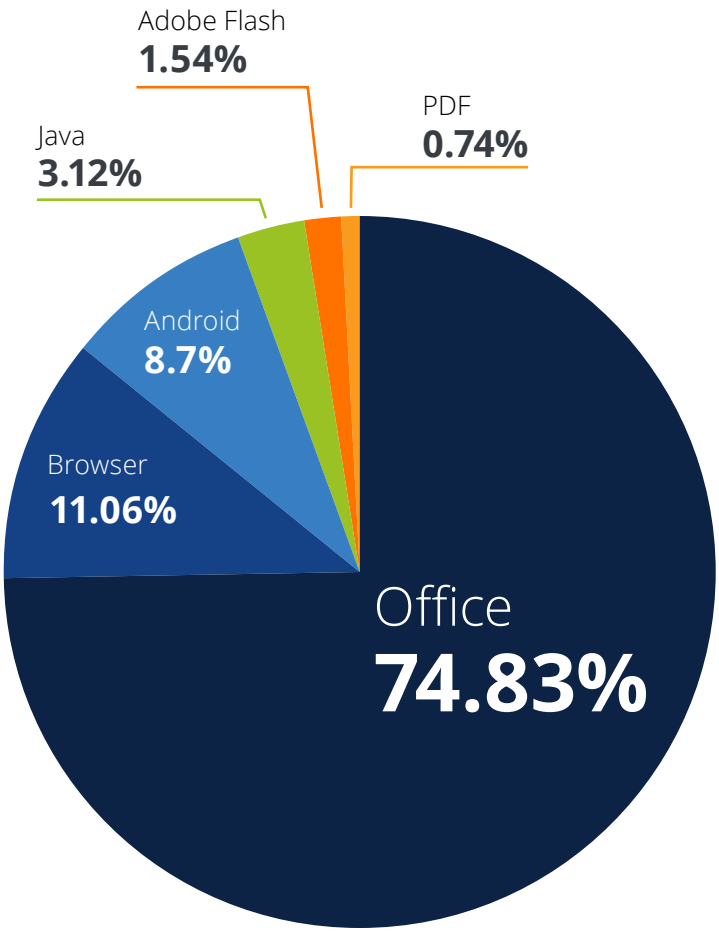
Of course, Microsoft isn't the only company to have vulnerabilities in its software. We're also seeing the following vulnerabilities being exploited in 2020.

Adobe has been releasing regular security patches for its products with an out-of-band emergency security update for Photoshop, Prelude, and Bridge in July. A week after issuing the firm's standard monthly security update, Adobe published security advisories revealing a total of 13 vulnerabilities, 12 of which are deemed critical. If exploited, they can lead to arbitrary code execution.

In August, Adobe released patches to address 26 vulnerabilities in Adobe Acrobat and Adobe Reader, including 11 flaws that were rated critical. The critical flaws could be exploited to bypass security controls, with nine of the critical flaws allowing the remote execution of arbitrary code.

Software for Windows is not the only vulnerable type. Cybercriminals are increasingly targeting unpatched Virtual Private Network (VPN) vulnerabilities. An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild. An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.

Most commonly exploited applications worldwide



Part 4

What to look for in 2021

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

Attacks on remote workers will only grow

With COVID-19 infection numbers growing rapidly, it is hard to imagine that the pandemic will end this year. More likely, it will take all of next year and maybe even 2022 for a vaccine to be globally distributed. That means remote, poorly protected workers are here to stay. In 2020, cybercriminals realized that phishing still works very well and that employees are the gateway to companies' data. We expect attacks on remote workers to grow in number and sophistication as more cybercriminals strive to get to the business data and systems located in empty offices and data centers.

Data exfiltration will become bigger than data encryption

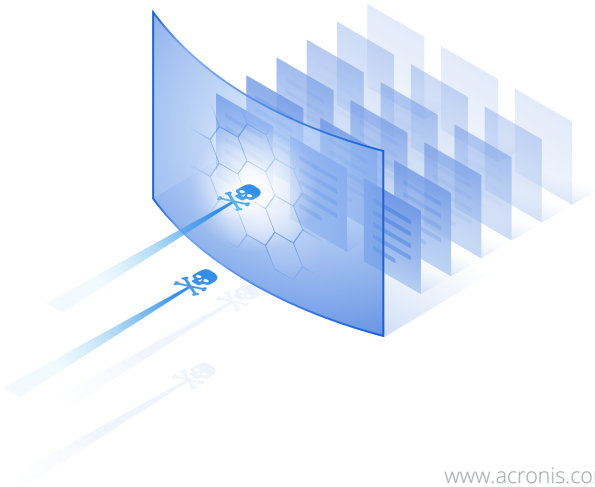
Recent ransomware cases showed that cybercriminals want to monetize every attack. More than that, they saw that extortion based on stolen confidential data is working very well, maybe even better than when they simply encrypt the same data. That is why we expect the main target in every ransomware attack will be data exfiltration. Data protection and data loss and leakage prevention solutions will be very important in the coming year because even if we see a reduced number of new ransomware families, the active ones will do huge damage and be very successful. That means next year we expect ransomware to still be the number one threat for businesses.

More attacks on MSPs and small business

With more small and medium businesses using cloud MS(S)Ps, more cybercriminals are invited to attack them. In 2019-2020, bad guys realized that attacking MSPs is very efficient, especially smaller ones who may not be prepared. By attacking MSPs, they attack the dozens of companies the MSP serves and can get more money through ransomware infections or banking Trojans. In addition, the attackers can make use of well-established tools, such as remote access and software delivery tools. These types of attacks are more likely to grow in number and geography as both small businesses and MSPs aren't ready for serious attacks and yet are still able to pay a moderate ransom.

Cloud under attack

During the lockdown, many companies moved their services to the cloud. Unfortunately, the configuration was often done in haste and is therefore not perfectly secure, leaving cloud applications and data services exposed to everyone on the internet. This scenario provides an opportunity for attackers to access and exfiltrate data, as we have already seen with data breaches on S3 data buckets and elastic search databases. Furthermore, identity and access management is still frequently overlooked, although identities are becoming the new perimeter. This situation will lead to an increase in user entity behavior monitoring and dynamic access controls.



Ransomware is looking at new targets

Ransomware attacks are expanding beyond Windows and Mac desktop machines. The attackers are trying to get a foothold in the cloud environment because cloud databases and containers are a lucrative target for them. Inside organizations, the increasingly exposed industrial control systems (ICS) of the OT side are another interesting target for extortion. For home users, the increased adoption of the internet of things (IoT), especially in connection with 5G, can yield new areas for infection – even if just to generate DDoS attacks as a way of motivating victims to pay ransom demands.

Attackers use more automation, number of malware samples grows

Cybercriminals are trying to automate their process wherever possible. Big data analytic tools and machine learning allows them to find new victims and generate personalized spam messages. The crimeware as a service and affiliate programs increase acceleration even more. However, after the initial access and execution phase, most groups still utilize manual methods to spread their malware inside the corporation's networks. Nevertheless, we will see a higher frequency of already known attack methods, with varying levels of personalization.

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

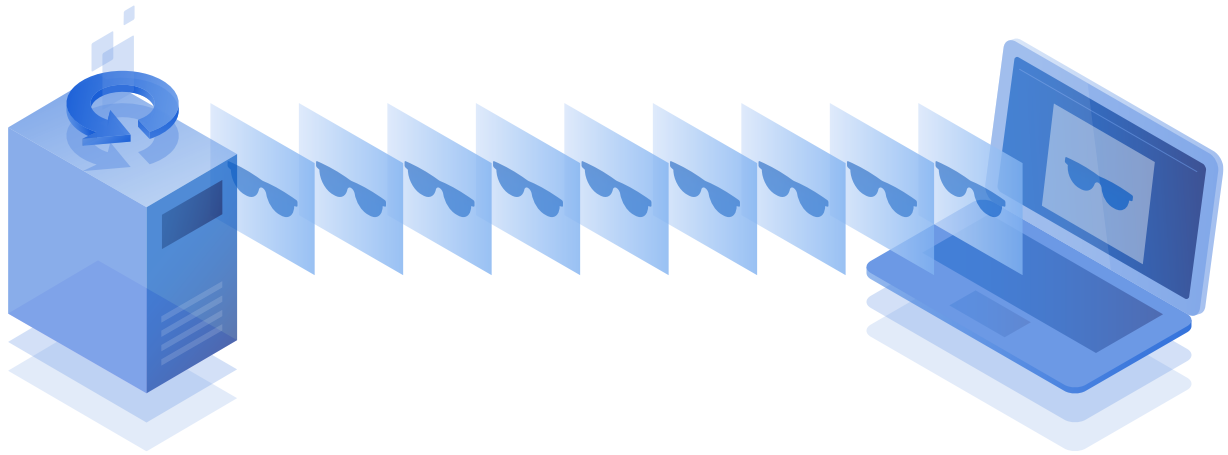
Modern cyberattacks, data leaks, and ransomware outbreaks all show the same thing: cybersecurity is failing. This failure is the result of weak technologies and human mistakes caused by clever social engineering. In cases where a backup solution was working well and wasn't compromised, it usually takes hours and days to restore systems (with data) to an operational state. Backup is essential for when cybersecurity solutions fail, but at the same time backup solutions can be compromised, 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, vulnerability assessment, patch management, RMM, and backup capabilities into a single agent running under a family of Windows operating systems. This integration enables 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 agent will immediately restore unaltered data from backup.

This kind of automated recovery isn't possible with an anti-malware 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 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 level of defense 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

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 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 100 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, which is a big mistake. Be sure that auto-updates to popular software vendors like Adobe are enabled and apps like Acrobat Reader are also updated promptly.

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

COVID-19 is now widely used in phishing attempts but the number of these malicious activities will only grow, so every remote worker needs to be prepared for it. Themed phishing and malicious websites appear in large numbers every day, these 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 Acronis Cyber Protect has a special category related to public health topics,

which is updated with greater priority. Malicious links can come from anywhere, including email, forum posts, and instant messaging apps. Don't click links you don't need to or that you didn't expect to receive.

Phishing or malicious attachments can come through email, 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

Whether 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, always use a Virtual Private Network (VPN). A VPN encrypts all your traffic, making it secure in case a hacker attempts to capture your data in transit. 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.

Be sure your cybersecurity solution is running properly

In Acronis Cyber Protect, we use many well-balanced and finely tuned security technologies, including several detection engines – recommended 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**
- **Product needs to get updates daily or hourly, depending on how often they are available**
- **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 make sure that the internet is available and not accidentally blocked by anti-malware software**
- **On-demand and on-access (real-time) scans should be enabled and react to 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

Final security tip: make sure that your passwords and your employees' passwords are strong and private. Never share passwords with anyone. Use different and long passwords for every service 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 that you can remember. Eight-character passwords are easily cracked with brute-force attacks nowadays.

In a secure product like Acronis Cyber Cloud or Acronis Cyber Backup, we never store passwords anywhere – preventing any unwarranted access to your data.

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

Additional Resources

Webinar On-demand: Cybersecurity 2021 – The Expected Threat Landscape

White Paper: Acronis Cyber Readiness Report

Free Tool: Cybersecurity Assessment Questionnaire

Acronis

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 award-winning AI-based anti-malware 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 1,500 employees in 33 locations in 18 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