Cybersecurity threatscape

Q3 2020

ptsecurity.com

Contents

Executive summary

Highlights of Q3 2020 include:

- The number of incidents grew by just 2.7 percentage points compared to the previous quarter. Growth in attacks has slowed after a rapid ascent in the first two quarters of the year. Targeted attacks have increased, from 63 to 70 percent.
- Ransomware is hitting companies with increasing frequency. In Q2, ransomware accounted for 39 percent of all attacks involving malware. This figure jumped to 51 percent in Q3. In other words, more than half of malware attacks in the outgoing quarter saw use of ransomware. This is closely tied to the increasing prevalence of direct financial gain as a motivation (42% of attacks).
- The number of attacks on manufacturing and industrial companies has remained high since the start of the year: This category come in second place across all industries as measured by total incidents. Such attacks were performed primarily by APT groups and ransomware operators (with ransomware attacks making up 45%).
- Healthcare institutions were once again targeted by criminals. Half of healthcare incidents related to ransomware, with which attackers cash in on patient data and make hospitals unable to function by cutting off access to information systems, prescriptions, and exam records. Attackers are also targeting research centers active in developing a coronavirus vaccine.
- The percentage of social engineering attacks using COVID-19 as a lure fell from 16 percent in Q2 to 4 percent in Q3. We believe that this is primarily due to people gradually becoming used to the new reality and the topic of COVID-19 no longer producing quite the same effect as before. Generally speaking, attackers previously would offer personal protective equipment. Now they exploit interest in a vaccine instead.
- Compared to the prior quarter, hacking as an attack method on companies grew by 12 percentage points (to 30%). The likely cause is that criminals continue to search for vulnerabilities in services on the perimeter of corporate systems. Due to the pandemic and the mass transition to working from home, many companies have made additional services available on the perimeter for the first time. Weak protection in many cases has given more opportunities to attackers. Moreover, the systems used to provide remote access themselves may contain known vulnerabilities, of which we have seen active exploitation in practice.
- The Emotet trojan resurfaced in July and has become a pressing threat. Over 500,000 emails containing Emotet are sent on weekdays. The malware steals information of interest and provides internal network access to the operators of ransomware and banking trojans.

To protect from cyberattacks, we recommend following our guidelines for ensuring personal and corporate cybersecurity. Considering recent trends, a well-organized vulnerability management process becomes more than just a response to regulatory requirements or industry standards: it increasingly forms a key requirement for any corporate security team. With new tools for automated collection and analysis of vulnerability data, deploying such a process in real-world corporate conditions has become much easier. A vulnerability management process must be complemented by up-to-date security solutions including a web application firewall (WAF) plus traffic analysis and SIEM systems. To prevent delivery of malware in emails, verify attachments in a sandbox specially designed to perform behavioral analysis in a safe environment.

Statistics

In Q3 2020, we saw a slowdown in the explosive growth in attacker activity that had accompanied the beginning of the COVID-19 pandemic earlier in the year. But the number of attacks remains persistently high and quarter-over-quarter growth in the number of incidents continues. In Q3 2020, the number of attacks grew by comparison to both Q2 (by 2.7%) and Q3 2019 (by 54%).

2.7% more cyberattacks than in Q2 2020

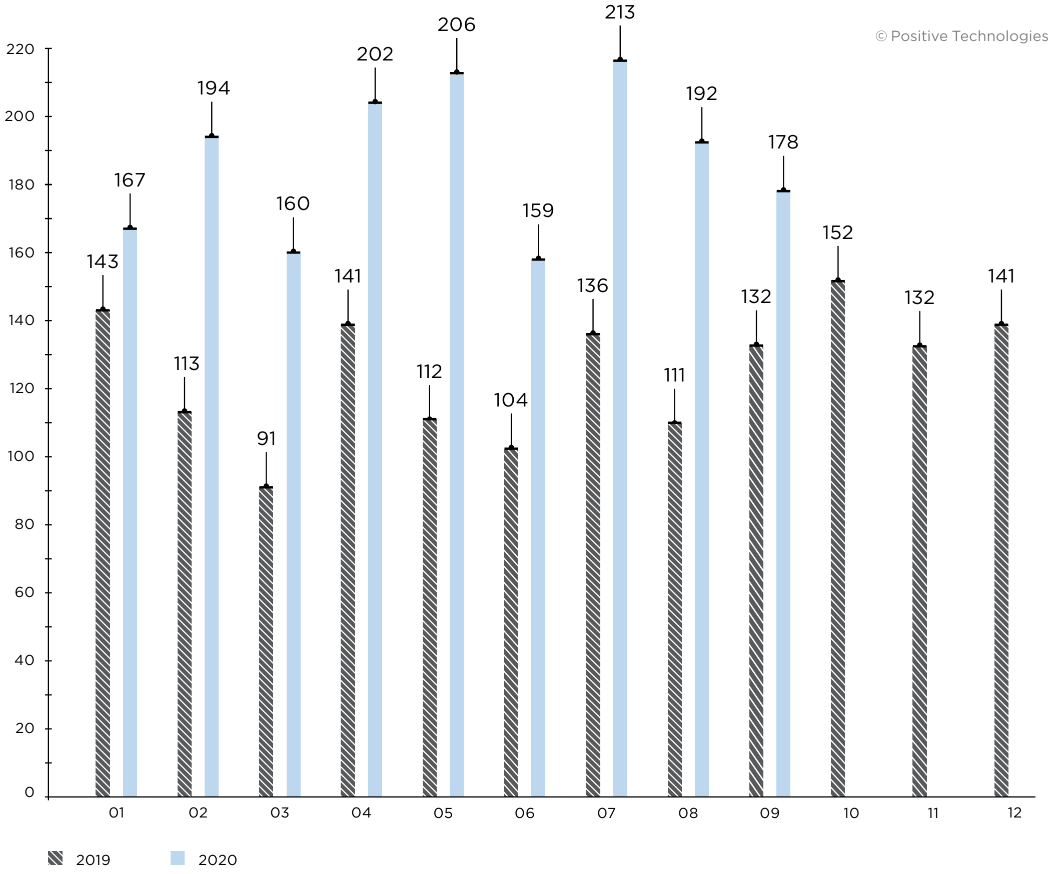
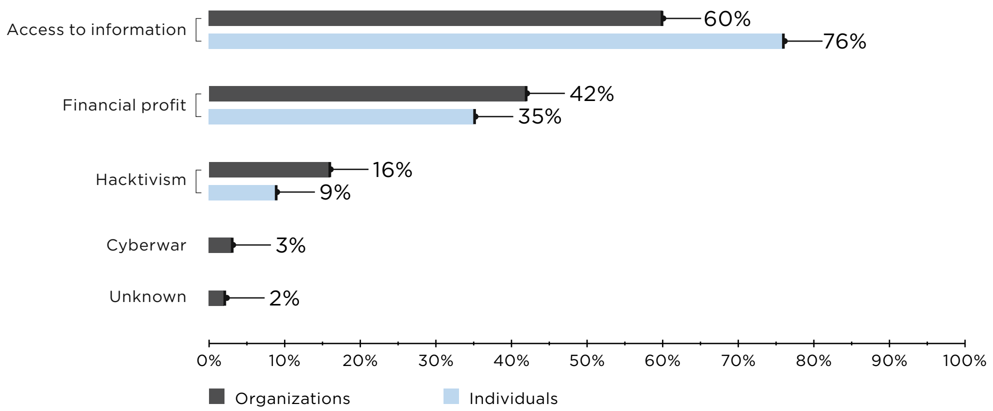
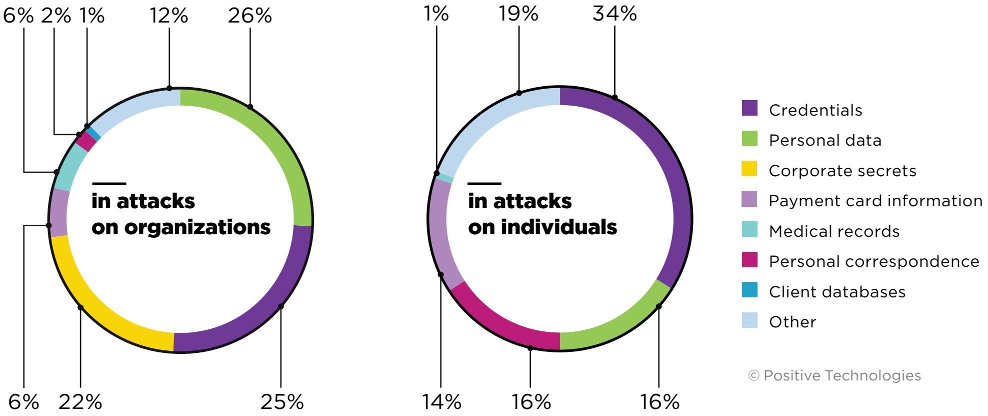


Figure 1. Number of incidents per month in 2019 and 2020 (1 = January, 12 = December)



© Positive Technologies

Figure 2. Attackers' motives (percentage of attacks)

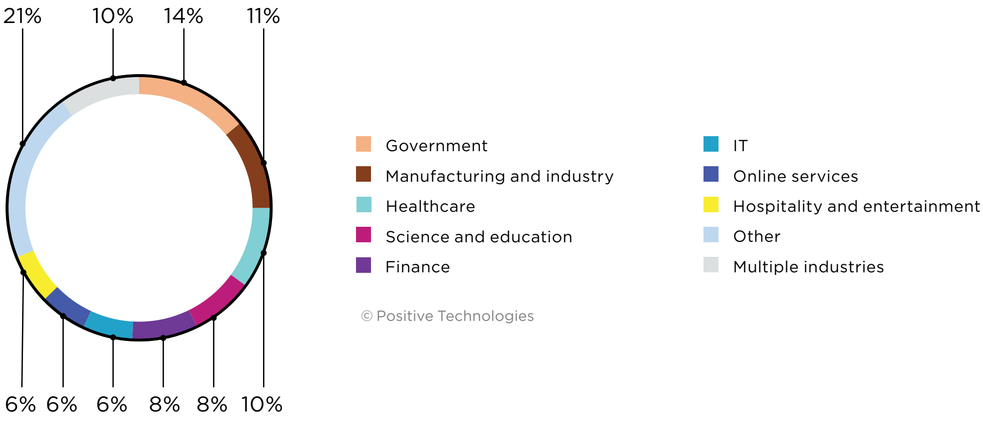


© Positive Technologies

Figure 3. Types of data stolen

70% of attacks are targeted

18% of attacks are directed against individuals



© Positive Technologies

Figure 4. Victim categories among organizations

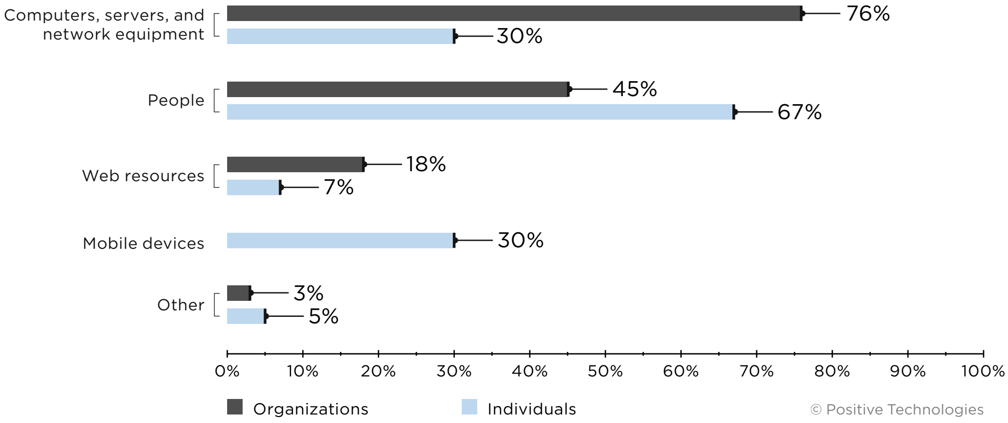


Figure 5. Attack targets (percentage of attacks)

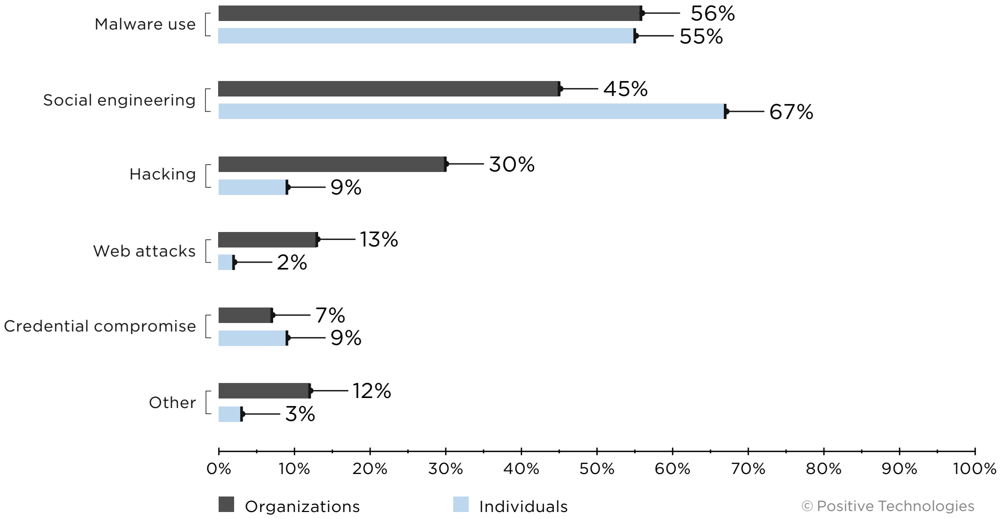


Figure 6. Attack methods (percentage of attacks)

© Positive Technologies

Per-industry classification of cyber-incidents by motive, method, target, and victim categories

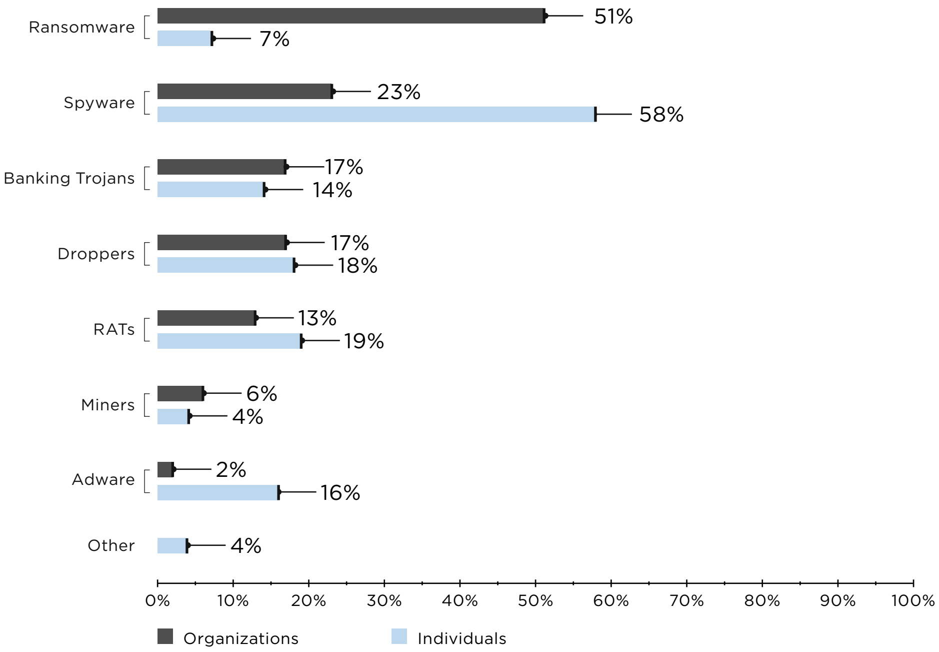
		Victim categories										
		Government	Finance	Manufacturing and industry	Healthcare	Online services	IT	Science and education	Hospitality and entertainment	Other	Multiple industrie	Individuals
	Total	**67**	**39**	**51**	**46**	**29**	**30**	**38**	**31**	**102**	**47**	**103**
Target	Computers, servers, and network equipment	42	31	49	41	15	27	28	27	76	31	31
	Web resources	21	5	1	3	16	2	4	3	18	10	7
	People	38	19	34	21	2	13	19	13	36	18	69
	Mobile devices											31
	Other	1	3					4	2	7		5
Method	Malware use	38	20	48	28	1	20	22	20	50	25	57
	Social engineering	38	19	34	21	2	13	19	13	36	18	69
	Credential compromise	7	2	2	8	2		1	1	6	4	9
	Hacking	11	9	14	14	11	13	12	16	33	16	9
	Web attacks	15	1	1	3	13	1	3	2	15	7	2
	Other	3	10	4	1	2	5	5	1	17	6	3
Motive	Access to information	39	25	47	29	20	21	19	28	46	25	78
	Financial profit	17	20	26	24	2	16	18	12	51	16	36
	Hacktivism	15	4		5	9	4	11	3	16	10	9
	Cyberwar	7		2	1				1	4	1	
	Unknown	2					1	1	1	3	4	

Darker colors indicate a higher proportion of attacks within a particular victim category.

0% 10% 20% 30% 40% 100%

Attacks involving malware

One of the year's consistent trends is a rise in use of ransomware against organizations. By contrast, individuals are getting hit with spyware, which has increased by 18 percentage points since Q2 to 58 percent of all malware attacks.

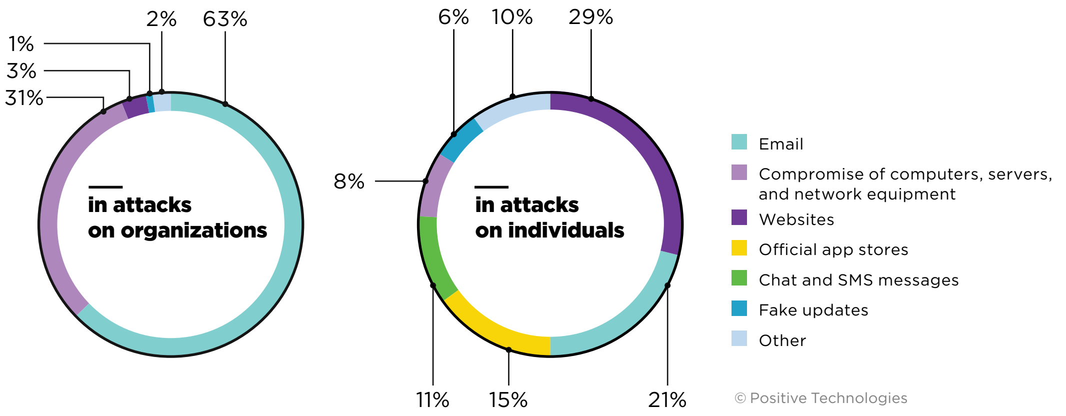


© Positive Technologies

Figure 7. Malware types (percentage of attacks involving malware)

As before, email is the main vector used to breach internal corporate networks and deliver malware. But we see a consistent quarterly uptick in exploitation of vulnerabilities on the corporate network perimeter for spreading malware. For example, as noted by Heimdal researchers, the operators of Netwalker delivered the ransomware to victims via phishing emails until April 2020. That's when they changed approaches and started to exploit vulnerabilities in unpatched VPN solutions, bruteforce RDP passwords for remote access, and search for vulnerabilities in web applications.

This trend was boosted by the pandemic, since companies urgently made services available on the perimeter that previously had been limited to the local network only. The perimeter changed quickly and many companies failed to sufficiently secure these services or simply did not have enough time to do so. Most companies are partially or fully remote, making inventories of externally accessible resources and an effective vulnerability management process more important than ever.



© Positive Technologies

Figure 8. Methods for distributing malware

Inventive attackers are getting ever more creative about hiding their tracks to maintain stealth, even against sandboxes. One such incident affected an international architectural firm in August. The attackers were after information: desktop screenshots, user passwords, and files with certain extensions. To reach the internal network, the hackers created a special malicious plugin (PhysXPluginMfx) for Autodesk 3ds Max. Bitdefender researchers found an interesting property of the malware: it checks whether Task Manager or Process Monitor is running, and if either of them is active, it remains inactive, which makes detecting the malware much more difficult.

An equally interesting incident involved old Zeppelin ransomware, which recently returned with a new downloader. Zeppelin already has more than 60 victims to its name. It is spread via phishing emails containing attachments with the .doc extension. By opening the attachment, the user runs macros and then triggers a mechanism for installing the downloader. Researchers at Juniper Threat Labs discovered that Zeppelin had learned how to evade dynamic analysis in a sandbox: after the downloader performs its work (by downloading an executable file containing the ransomware), malicious activity stops for 26 seconds. The developers presumably believed this would be enough time for automated sandbox checks to be completed. After this delay, the Zeppelin ransomware is launched.

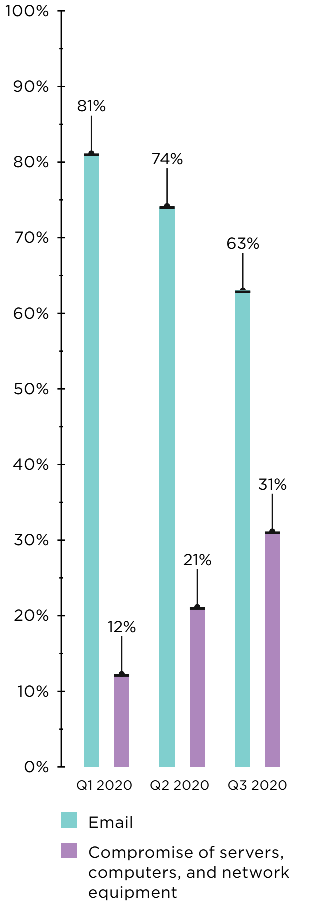
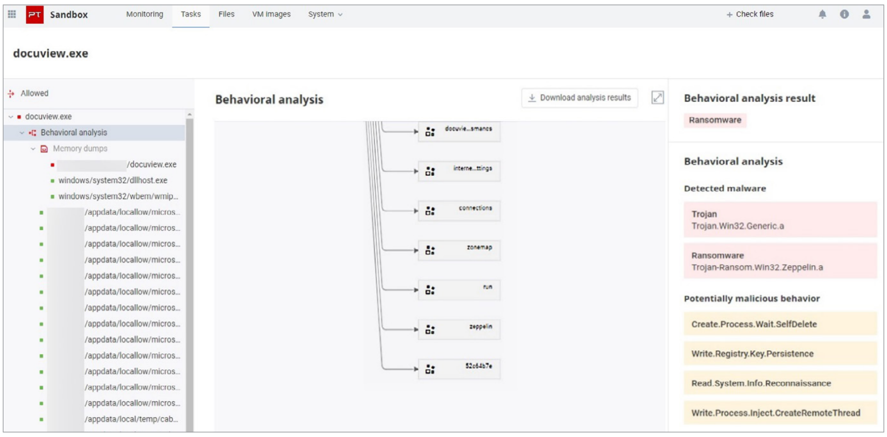


Figure 9. Main methods used for malware distribution (percentage of attacks on organizations)



docuview.exe

- docuview.exe
  - Behavioral analysis
    - Memory dumps
      - /docuview.exe
      - windows/system32/dllhost.exe
      - windows/system32/wbem/wmip...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/locallow/micros...
      - /appdata/local/temp/cab...

Behavioral analysis

Behavioral analysis result

Ransomware

Behavioral analysis

Detected malware

Trojan
Trojan.Win32.Generic.a

Ransomware
Trojan-Ransom.Win32.Zeppelin.a

Potentially malicious behavior

Create.Process.Wait.SelfDelete

Write.Registry.Key.Persistence

Read.System.Info.Reconnaissance

Write.Process.Inject.CreateRemoteThread

Figure 10. Process of detecting Zeppelin malware in a sandbox

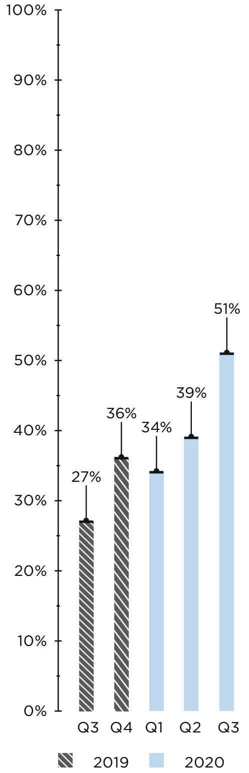


Figure 11. Ransomware attacks (percentage of attacks involving malware)

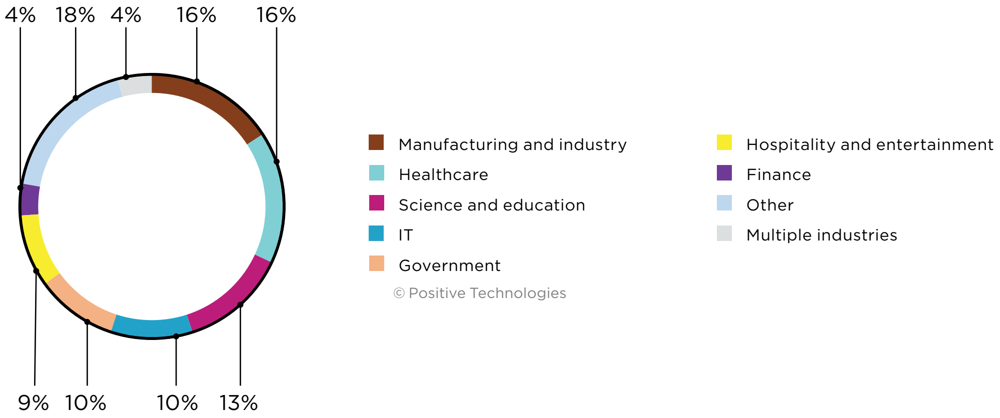
More than half of malware attacks on individuals involved spyware. One such case is FakeSpy. This spyware was spread through phishing SMS messages, which contained links supposedly from a mail or delivery service. After being downloaded to a mobile device, FakeSpy began to collect contact lists and banking app credentials, monitor SMS messages, and spread itself by sending phishing messages to all of the victim's contacts.

Notably, the share of adware doubled: in the prior quarter, it had been implicated in 8 percent of malware attacks on individuals. RainbowMix programs, which are usually made to look like a Nintendo emulator, are one example. The purpose of these programs is to show ads supposedly from legitimate apps. Total RainbowMix downloads exceed 14 million, with up to 15 million ad impressions in a single day.

Ransomware booming

The third quarter brought a record rise in the number of ransomware attacks, which accounted for over half of all malware attacks.

Instead of mass attacks, ransomware operators by and large are striking very selectively as they target major companies able to provide a large payday, or else organizations ill-able to afford any disruptions. In Q3, ransomware was particularly active against manufacturing and industry, as well as healthcare.



© Positive Technologies

Figure 12. Ransomware attacks by industry

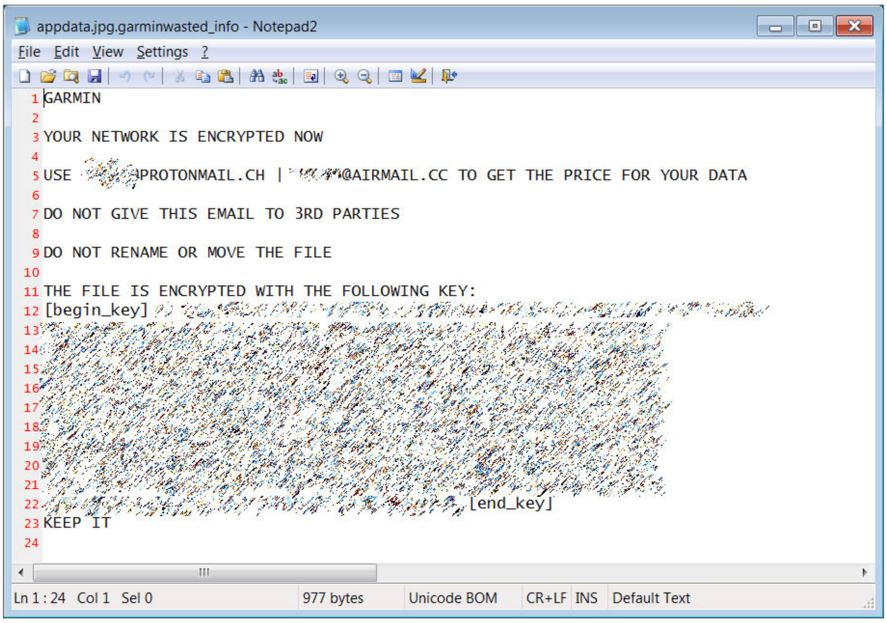
Top five most used ransomware families in Q3 2020

1. Netwalker
2. REvil
3. Maze
4. DoppelPaymer
5. RansomEXX

In mid-July, the operators of REvil infected the internal network of Telecom Argentina, one of the South American country's largest Internet providers. The hackers infected more than 18,000 workstations. They requested a ransom of $7.5 million. Another high-profile incident in Argentina occurred in late August, this time involving the country's immigration service. A Netwalker ransomware attack brought the country's border crossings to a halt. For restoration of access, the attackers requested $4 million.

New DarkSide ransomware was publicly noted for the first time in August as well. The operators of DarkSide are requesting ransoms from $200,000 to $2 million. They select their victims with great care, based on whether they believe whether a particular company will be able to pay. They have pledged to not attack healthcare, education, governments, and non-profits. According to Advanced Intelligence, the malware avoids ending certain processes during attacks. Since TeamViewer is one of the processes in question, it may be that the attackers are using TeamViewer for remotely connecting to victim computers. One of the first victims was Brookfield Residential in North America, from which the DarkSide operators stole more than 200 GB of data including corporate secrets, financial information, and employee records.

The operators of WastedLocker are no less thorough when selecting their victims. In late July, they struck Garmin, the manufacturer of GPS navigation equipment and smart watches. Garmin clients lost access to connected services and applications for several days. The attackers' initial ransom demand was for $10 million. Four days after the attack, Garmin began to bring its services back online. It is suspected that the company reached a deal with the hackers and paid a ransom, although the precise amount, if any, remains unknown.



```
GARMIN

YOUR NETWORK IS ENCRYPTED NOW

USE [redacted]PROTONMAIL.CH | [redacted]@AIRMAIL.CC TO GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
[begin_key][redacted][end_key]
KEEP IT
```

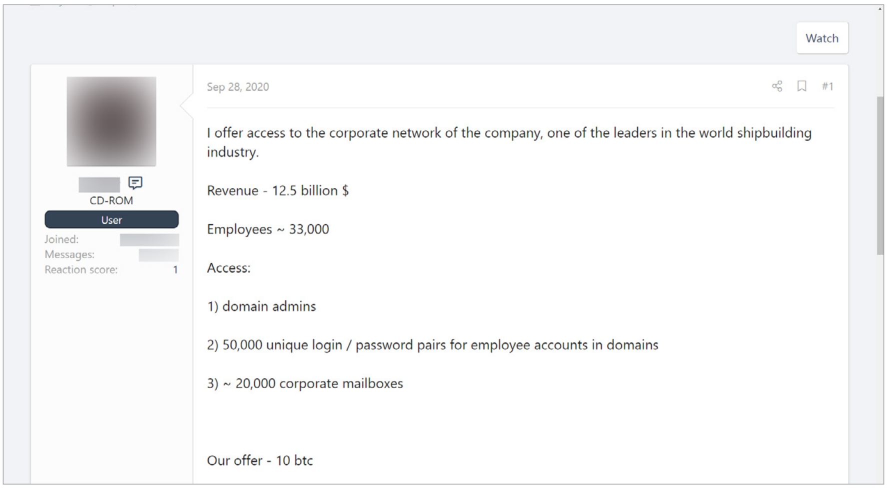
Figure 13. Ransom demand addressed to Garmin

In late July, RansomEXX ransomware brought down the Konica Minolta site, making it inaccessible for around a week. During the same time period, Maze was striking Canon: the group claimed to have stolen 10 TB of the company's data.

Chinese offices of French shipping giant CMA CGM also fell victim. At the end of the third quarter, they were attacked by the operators of Ragnar Locker ransomware. The company's container reservation system, sites, and applications were inaccessible for around 24 hours.

Data processing provider Equinix was compromised by Netwalker ransomware in early September. The stolen data included financial information, data center audits and reports, salaries, and accounting documents. The ransom demanded for decryption and non-disclosure of the stolen data was $4.5 million. In their ransom note, the hackers also threatened to double the amount if it was not paid quickly. Equinix has not publicized how the attackers breached its network, but researchers at Advanced Intelligence discovered sale postings on the darknet for credentials for 74 of the company's servers.

The market for criminal cyberservices has been a topic in our previous reports. A division of labor can be seen in the cybercrime world. Less-skilled hackers find ways in to corporate networks. They sell this access on to more experienced hackers who can monetize it most effectively. The case of Equinix is far from the only one, even among major companies. For example, a posting offering to sell access to the corporate network of a leading global shipbuilding company was put on the darkweb in September. The price was 10 bitcoins, which at current valuations exceeds $100,000.



Sep 28, 2020

I offer access to the corporate network of the company, one of the leaders in the world shipbuilding industry.

Revenue - 12.5 billion $

Employees ~ 33,000

Access:

1) domain admins

2) 50,000 unique login / password pairs for employee accounts in domains

3) ~ 20,000 corporate mailboxes

Our offer - 10 btc

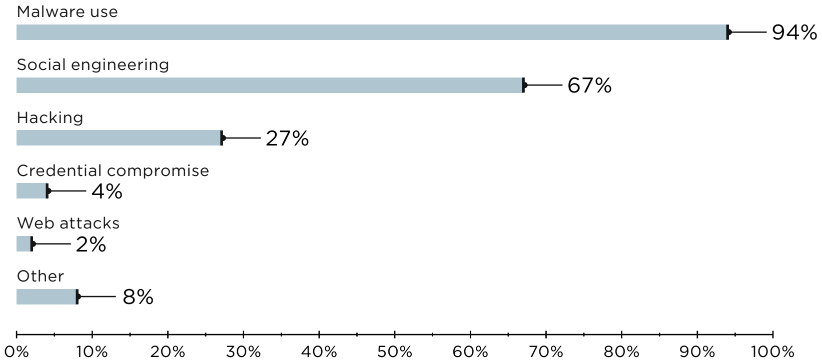
Figure 14. For sale: access to a global shipbuilding giant

As noted already, some attackers steal data before encrypting the victim's copy. If no ransom is forthcoming, they publish this high-value content on their own sites. Such sites appeared in the last quarter among SunCrypt, DarkSide, and Conti.

Curiously, some attackers are trying to piggyback on the reputation of more well-known groups. The operators of SunCrypt ransomware announced at the end of August that they had joined the Maze cartel. But Maze was unaware of this, judging by the group's denial. Maze stated that SunCrypt was pursuing a PR strategy of claiming membership in the cartel as a way to increase the pressure on victims.

Manufacturing and industry still under threat

The number of attacks on manufacturing and industrial companies has remained high since the start of the year: The culprits in Q3 were primarily APT groups (RTM, TinyScouts) and ransomware operators (Nefilim, Maze, Netwalker, RansomEXX, Conti, DoppelPaymer). Ransomware accounted for 45 percent of total attacks.

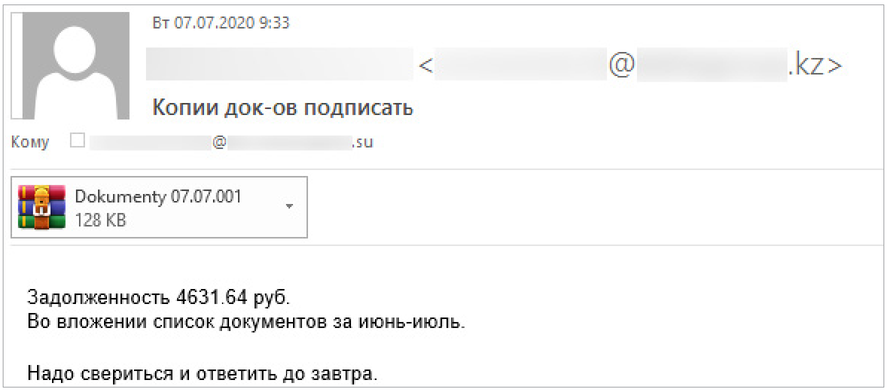


© Positive Technologies

Figure 15. Attack methods (percentage of attacks on manufacturing and industrial companies)

Nor were manufacturing and industrial companies immune to the trend of intensified exploitation of network perimeter vulnerabilities: these attacks more than doubled, in percentage terms, compared to the prior quarter. However, most of the incidents (67%) occurred in the old-school way, implying use of email as the main method of penetration. These attackers include TinyScouts, a new group that targets energy companies, among others. During the first stage of their attack, they sent phishing messages to employees at different companies. The topics were related to COVID-19 or else victim-specific. In the group's July campaign, they enclosed a file with the .lnk extension. When opened, this file launched the utility mshta.exe. The .exe file performed two roles: for the user, it opened a decoy document, while for the attackers, it ran a script that checked for TeamViewer, RDP sessions, and domain login status. What happened next depended on the target: if the company was of particular interest, the attackers ran spyware to collect information. Otherwise, ransomware set to work. Note that a similar method, involving a .link file followed by launch of mshta.exe, is used by the Gamaredon APT group against government targets. Gamaredon's activity has been monitored by the PT Expert Security Center for several quarters.

The RTM APT group, too, uses social engineering to deliver malware. During Q3, PT ESC detected 34 phishing mailings from the group.



Вт 07.07.2020 9:33

[redacted] <[redacted]@[redacted].kz>

Копии док-ов подписать

Кому □ [redacted]@[redacted].su

Dokumenty 07.07.001
128 KB

Задолженность 4631.64 руб.
Во вложении список документов за июнь-июль.

Надо свериться и ответить до завтра.

Figure 16. Message with malicious archive sent by the RTM APT group

One fifth of attacks in Q3 included spyware or malware for remote administration. In such cases, attackers are likely eying confidential data.

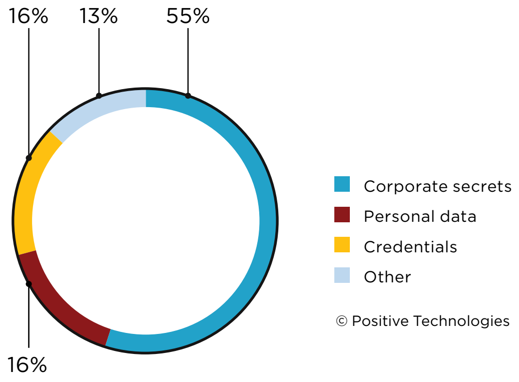


Figure 17. Data stolen in attacks on manufacturing and industrial companies

Netwalker ransomware did not spare manufacturing and industry. On September 7, the group attacked K-Electric, the sole electrical supplier in the Pakistani city of Karachi. Consequences included disruptions to online billing and other services. The attackers demanded $3.9 million for restoring access and, if not paid within seven days, threatened to raise the amount to $7.7 million.

Maze performed a successful attack on major Vietnamese steel sheet manufacturer Hoa Sen Group. They stole a range of data, including employee records, internal correspondence, and other sensitive files. To date, 1.64 GB of files (5% of the total amount stolen) has been put online. The same attackers also struck SK hynix, a major vendor of RAM and flash memory. They exfiltrated 11 GB of information, including confidential agreements for sale of NAND flash memory to Apple.

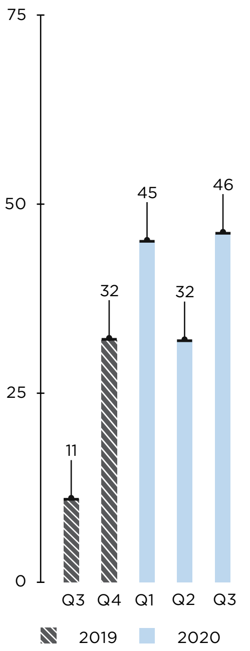


Figure 18. Number of attacks against healthcare

Healthcare: the second wave

Since February 2020, COVID-19 has been a major concern in almost every country. This is particularly true for healthcare institutions, which continue operating under colossal burdens. Cybercriminals are taking advantage of the epidemic. In the third quarter, we saw more attacks aimed at these very institutions.

Half of healthcare attacks included by ransomware, with painful consequences. In late September, American hospital network Universal Health Services was attacked by Ryuk ransomware. Doctors could not access patient test results or prescriptions, get data from diagnostic devices, or provide patient care. Computers were turned off and all the necessary data, stored electronically, had been encrypted by the attacker.

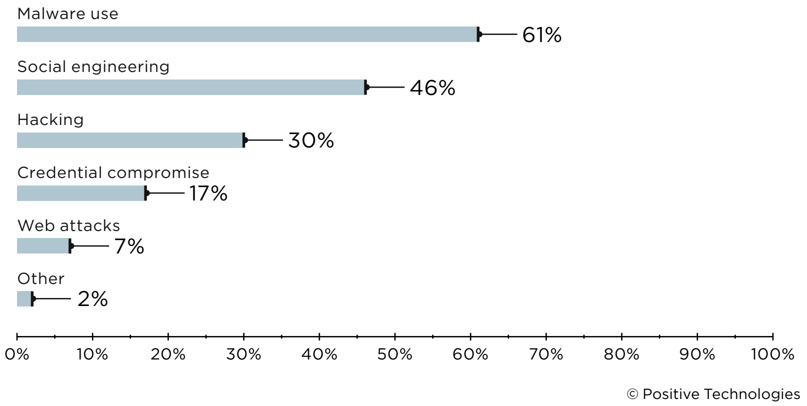


Figure 19. Attack methods (percentage of attacks on healthcare)

The trend of publishing stolen data continues to grow. In August, the operators of REvil attacked Valley Health hospitals in the U.S., from which they stole all information on the internal network before encrypting it. To prove that they had obtained access, the attackers published some of the stolen information online, including patient medical data such as prescription lists and exam records. In September, University Hospital New Jersey was struck by SunCrypt ransomware. A total of 240 GB of data, including patient records, was stolen. After 48,000 of the hospital's documents were published on the site of the ransomware operator, the hospital contacted the attackers with a request to halt further publications. In negotiations, the ransom was reduced from $1.7 million to $670,000, which the hospital paid.

Some hackers repurpose the official websites of healthcare institutions to publish their own content. In one case, attackers exploited vulnerabilities in CMS platforms used by the sites of the U.S. National Institutes of Health and National Cancer Institute to post articles about how to hack accounts on popular social networks. In the articles, they prompted paying for an alleged hacking tool; the attackers thus gained access to payment card data as well as money from purchasers.

Hunt for a vaccine

Clinics and hospitals are far from the only ones hit. Attackers are even targeting research centers working on a vaccine for COVID-19. This September, research centers in Spain were attacked. The attackers' main objective was to obtain information on development and testing.

COVID-19 concern is abused in attacks on individuals as well. In the prior quarter, phishing messages would tend to offer personal protective equipment or more information about the virus. But now, most often, they exploit interest in a vaccine instead. One mailing addressed to people in the United Kingdom claimed that local vaccine efforts were going slowly and offered a supposed vaccine for sale on the site of a Canadian pharmacy chain. Needless to say, the link went to a fraudulent site offering fakes.

However, the number of COVID-19 phishing mailings is decreasing quickly. The percentage of social engineering attacks using COVID-19 as a lure fell from 16 percent in Q2 to 4 percent in Q3.

Perimeter attacks picking up steam

Attackers' preferred methods for breaching internal networks are changing. Across nearly all industries, we see increasing use of hacking instead of other methods. This is unsurprising given the mass move to working from home and rapid growth in services available on the network perimeter at many companies.

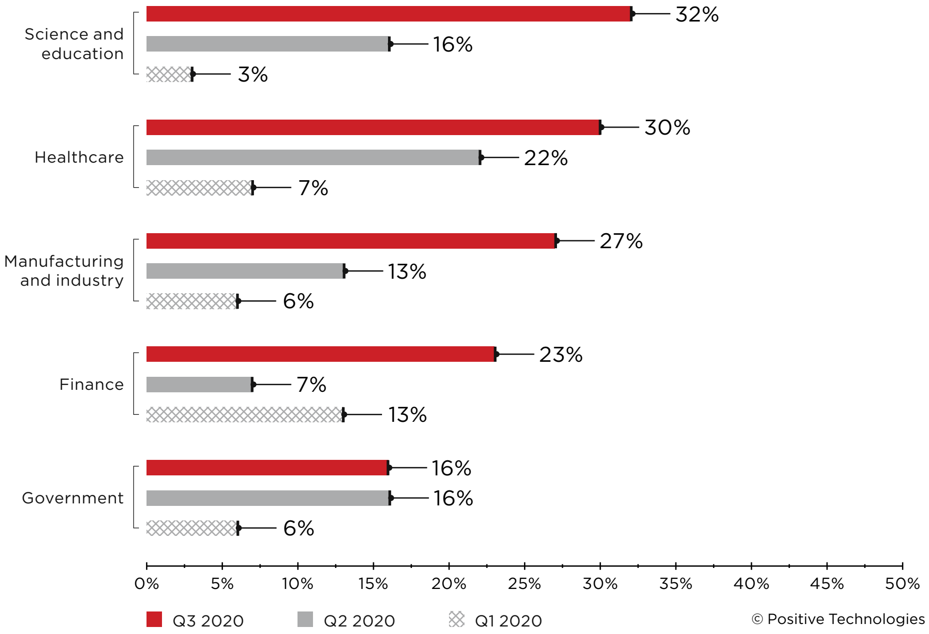


Figure 20. Percentage of hacking among attack methods used (most frequently attacked industries)

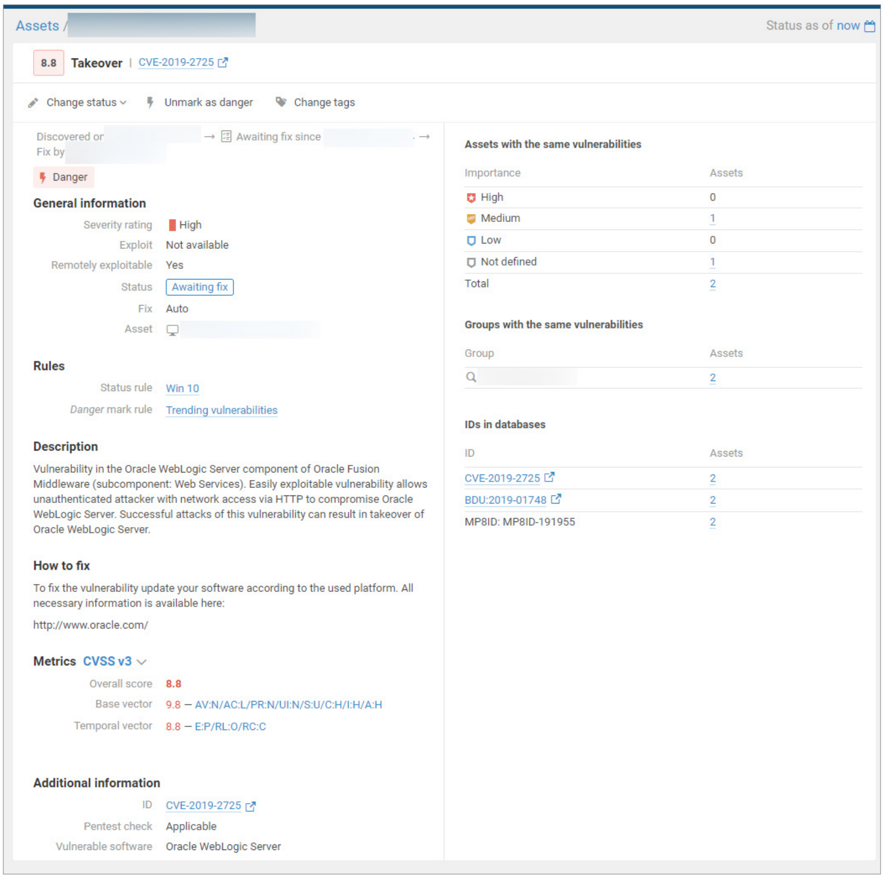
Most frequently exploited vulnerabilities in Q3 2020

- CVE-2019-19781 (Citrix NetScaler ADC, Gateway и SD-WAN)
- CVE-2019-2725 (Oracle WebLogic Server)
- CVE-2019-11510 (Pulse Secure VPN)
- CVE-2020-5902 (F5 BIG-IP)

Vulnerability names are appearing in the news with greater frequency in the context of attack vectors. For example, attackers in August exploited Remote Code Execution vulnerability CVE-2019-19781 against Italian eyewear manufacturer Luxottica. A few weeks prior, cruise company Carnival Corporation was attacked. Researchers at Bad Packets analyzed the incident and identified several vulnerable devices on the company's network perimeter. For reaching the local network, attackers could have used vulnerabilities CVE-2019-19781 in Citrix ADC or CVE-2020-2021 in a Palo Alto Networks firewall, for example.

In an incident during late June to early July, vulnerability CVE-2019-11510 (which allows reading arbitrary server files) was exploited. A hacker scanned the Internet's entire IPv4 address space for Pulse Secure VPN servers and then used an exploit for CVE-2019-11510. The hacker obtained more than 900 pairs of credentials as well as IP addresses for accessing web servers, and then provided them free of charge to all comers. A Bank Security researcher who analyzed the data reached the conclusion that software versions vulnerable to CVE-2019-11510 had in fact been installed on all of the listed Pulse Secure VPN servers.

Panda Security researchers found that Remote Code Execution vulnerability CVE-2019-2725 is often used in REvil ransomware attacks. This July, REvil performed several attacks on Spanish rail company Adif. The 800 GB of stolen data included corporate secrets, accounting and personal information, and electronic correspondence.



8.8 **Takeover** | CVE-2019-2725

Discovered or [redacted] → Awaiting fix since [redacted] →
Fix by [redacted]

Danger

General information

Severity rating	🟥 High
Exploit	Not available
Remotely exploitable	Yes
Status	Awaiting fix
Fix	Auto
Asset	[redacted]

Rules

Status rule	Win 10
Danger mark rule	Trending vulnerabilities

Description

Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

How to fix

To fix the vulnerability update your software according to the used platform. All necessary information is available here:

http://www.oracle.com/

Metrics CVSS v3

Overall score	8.8
Base vector	9.8 — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Temporal vector	8.8 — E:P/RL:O/RC:C

Additional information

ID	CVE-2019-2725
Pentest check	Applicable
Vulnerable software	Oracle WebLogic Server

Assets with the same vulnerabilities

Importance	Assets
High	0
Medium	1
Low	0
Not defined	1
Total	2

Groups with the same vulnerabilities

Group	Assets
[redacted]	2

IDs in databases

ID	Assets
CVE-2019-2725	2
BDU:2019-01748	2
MP8ID: MP8ID-191955	2

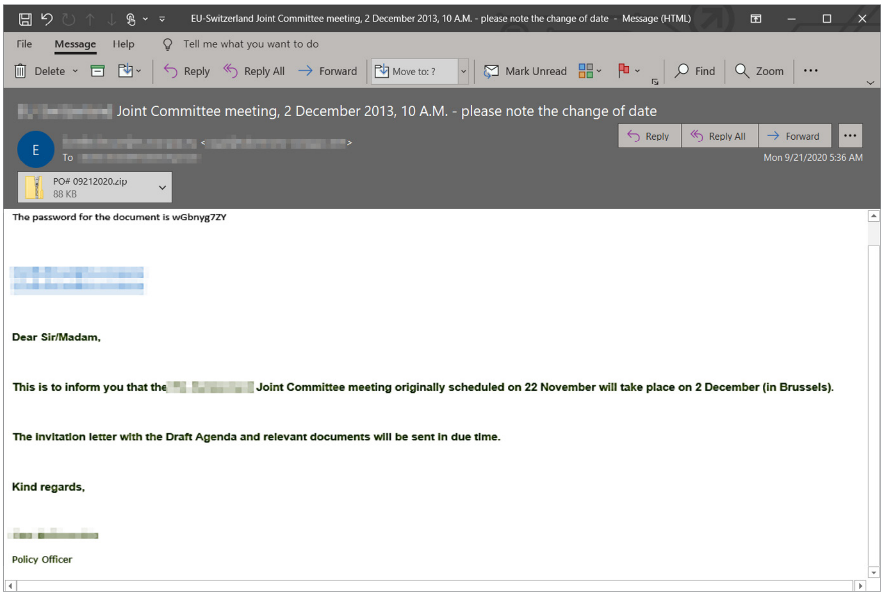
Figure 21. Detection of CVE-2019-2725 with MaxPatol VM

Some vulnerabilities make life easier for botnet operators. For instance, Trend Micro researchers have detected a new version of the Mirai IoT botnet designed to target, among other things, vulnerability CVE-2020-10173 (which involves Comtrend router commands). Experts predict that this vulnerability will also be exploited by other botnets in DDoS attacks.

What to expect from a six-year-old trojan

After a short absence from February to July, the Emotet trojan became active again. It is spread via phishing emails and has downloader functionality, which enables it to deliver other malware. At the beginning of the new wave of attacks, Emotet spread Trickbot spyware, which after collecting information opened up access to Ryuk and Conti ransomware. But this quickly changed, as noted by researchers following Emotet: now the attackers install the QakBot (QBot) banking trojan on victim computers.

CISA experts believe that Emotet is one of the most important threats today. The malicious wave affected just U.S. organizations at first, but in August and September, reports of attacks surfaced in France, Japan, New Zealand, Canada, Italy, and the Netherlands.



EU-Switzerland Joint Committee meeting, 2 December 2013, 10 A.M. - please note the change of date - Message (HTML)

[redacted] Joint Committee meeting, 2 December 2013, 10 A.M. - please note the change of date

E [redacted] <[redacted]>

To [redacted]

Mon 9/21/2020 5:36 AM

PO# 09212020.zip
88 KB

The password for the document is wGbnyg7ZY

[redacted]

Dear Sir/Madam,

This is to inform you that the [redacted] Joint Committee meeting originally scheduled on 22 November will take place on 2 December (in Brussels).

The invitation letter with the Draft Agenda and relevant documents will be sent in due time.

Kind regards,

[redacted]

Policy Officer

Figure 22. Example of phishing email from Emotet in a message thread

At the beginning of the attack, the user receives an email with a malicious attachment. After the user opens the attachment and activates macros, the Emotet executable file begins downloading. As soon as installation completes, the computer becomes a part of the botnet and starts sending emails to all of the victim's contacts. For subsequent spreading, the hackers use message threads on the infected computer: they reply to a message from a pre-existing thread, so the recipients fully trust the sender and open the attached malicious file.

In its advisory, Microsoft notes that Emotet sends more than 500,000 emails daily (excluding weekends). To slip through email security gateways, the attackers pack the attachment as a password-protected archive.

About the research

In this quarter's report, Positive Technologies shares information on the most important and emerging IT security threats. Information is drawn from our own expertise, outcomes of numerous investigations, and data from authoritative sources.

In our view, the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity by hacker groups are unable to perform a precise count. This research is conducted in order to draw the attention of companies and ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

In this report, each mass attack (in which attackers send out a phishing email to many addresses, for instance) is counted as a single incident. Definitions for terms used in this report are available in the glossary on the Positive Technologies site.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.