Cybersecurity threatscape Q1 2022

Positive Technologies

ptsecurity.com

Содержание

Summary

Q1 2022 highlights:

- Compared to Q4 2021, the number of attacks rose by 14.8%. The share of mass attacks also increased, to 33% of the total.

- The share of attacks on individuals remains the same, amounting to 15% of the total. Attack methods and motives have not changed significantly.

- Most often, attacks on companies cause leakage of confidential information (45%) and disruption of core business (30%). In attacks on individuals, confidential data (55%) was compromised most often, and users could also suffer financial losses (25%).

- Interest in web resources is up: the share of attacks on them increased to 22% of the total against 13% in Q4 2021.

- Among the top five most-attacked industries was mass media, accounting for 5% of attacks. But it was government agencies that were most frequently hit: the number of attacks on them almost doubled compared to the previous quarter.

- Attackers are actively spreading spyware aimed at stealing credentials. In attacks on individuals, credentials were compromised in 46% of cases of data stealing. Of particular interest are credentials for VPN services, which are subsequently sold on dark web forums.

- The share of ransomware fell slightly against Q4 2021, from 53 to 44%. This change is partly the result of some ransomware groups switching to industrial espionage without encrypting devices. Some ransomware attackers, meanwhile, do not send decryption keys, aiming instead to wreck the target infrastructure. Also on the rise are attacks involving data-destroying wipers.

- Malware continues to worm its way into official app stores: many seemingly legitimate apps targeting Android users were spotted this quarter. Most of these apps are banking trojans and loaders, while the number of downloads by users in some cases runs into the hundreds of thousands.

- Major attacks affected IT companies: industry giants such as Nvidia and Samsung suffered data leaks. Cybercriminals also launch mass attacks on developers by embedding malicious code in open packages and libraries of popular platforms and frameworks.

To protect against cyberattacks, we first and foremost recommend following our general guidelines on personal and corporate cybersecurity. Given the specifics of Q1, we advise software developers to carefully test libraries before using them, ensure that all development environments are configured securely, and check the robustness of their own code. You can strengthen security at the corporate perimeter by using cutting-edge security tools, such as web application firewalls. To prevent malware infection, we recommend using sandboxes that analyze file behavior in a virtual environment and detect malicious activity.

Statistics

Compared to Q4 2021, the number of attacks in Q1 2022 rose by 14.8%. We put this down to the escalation of confrontation in cyberspace. The most frequently attacked organizations were government agencies, medical institutions, and industrial companies. However, there have been changes in the list of top five most-attacked sectors, which now includes mass media. The number of attacks not related to any sector of the economy also increased—from 18 to 23%.

The second half of the quarter saw multiple attacks on web resources, with their share climbing to 22% against last quarter's 13%. The share of credential compromise and brute-force attacks also increased. The majority of these attacks were carried out against companies' websites and social media accounts.

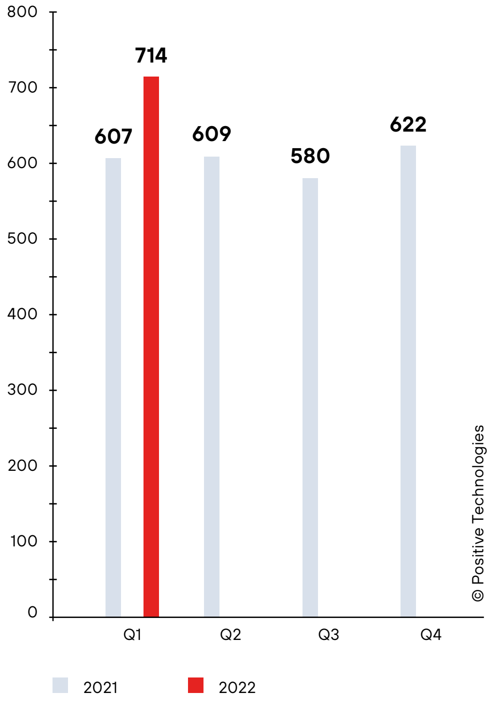


Figure 1. Number of attacks in 2021 and 2022 (by quarter)

67% of attacks were targeted

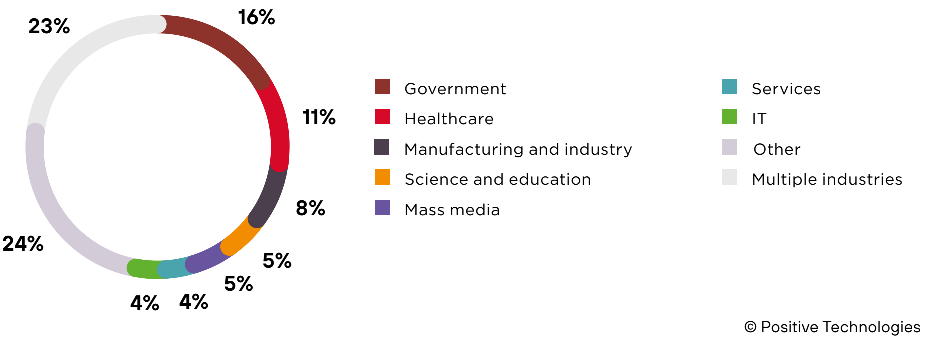


Figure 2. Victim categories among organizations

15% of attacks targeted individuals

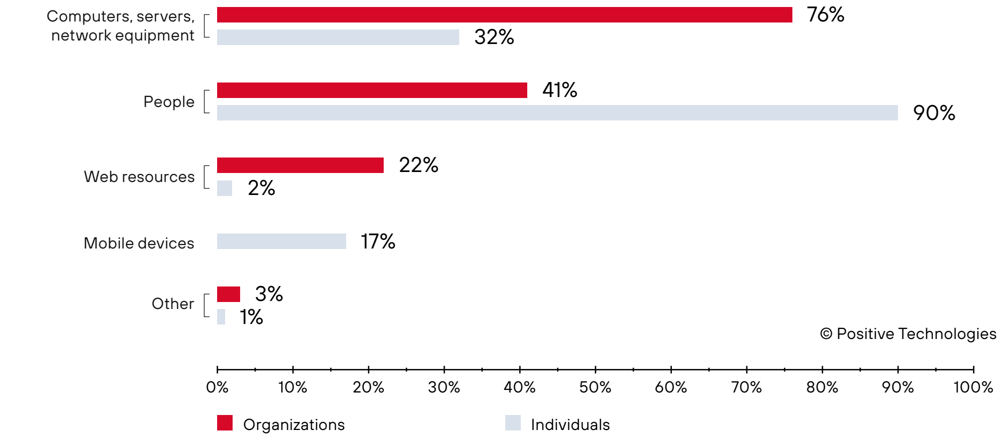


Figure 3. Attack targets (share of attacks)

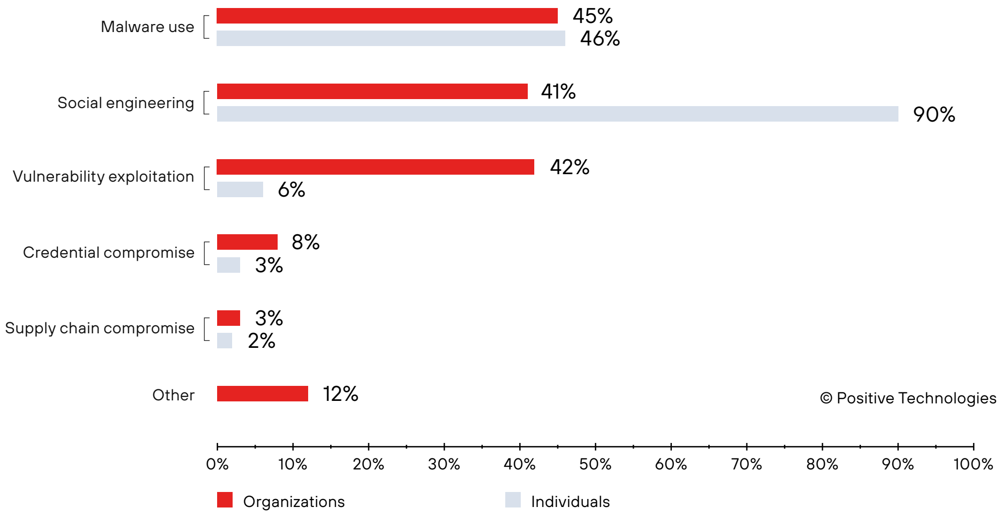


Figure 4. Attack methods (share of attacks)

© Positive Technologies

Per-industry classification of cyberincidents by motive, method, target, and victim category

Victim categories

		Government	Manufacturing and industry	Healthcare	IT	Science and education	Mass media	Services	Other	Multiple industries	Individuals
	Total	**100**	**49**	**69**	**23**	**32**	**31**	**25**	**140**	**140**	**105**
Target	Computers, servers, network equipment	51	45	61	19	28	15	18	105	119	34
	Web resources	44	4	4	5	3	15	3	41	14	2
	People	39	21	37	4	15	7	13	43	69	95
	Mobile devices	1					1		1		18
	Other	2		1	1				10	3	1
Method	Malware use	38	30	29	12	18	6	9	56	79	48
	Social engineering	39	21	37	4	15	7	13	43	69	95
	Vulnerabilities exploitation	34	25	23	14	12	18	12	61	55	6
	Supply chain compromise	6	3	10	5	4	2	1	10	8	3
	Credential compromise	10	1	4					2	3	2
	Other	17	1	1	2	1	5		32	16	
Consequences	Leak of confidential information	39	23	59	12	18	5	18	56	42	58
	Disruption of core activity	40	17	12	6	13	16	3	51	22	1
	Direct financial losses		2	5	1	1	1		20	10	26
	Damage to national interests	26					18		6	3	2
	Use of company or individual resources to carry out attacks	5	1	2	5	2	1	5	7	12	6
	Other		1		1	1			1	3	3
	Unknown	28	20	3	4	7	1	2	26	66	24

Darker colors indicate a greater proportion of attacks within a particular victim category

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

Attack consequences

Attack consequences are diverse and can vary from impacting one individual to an entire industry or region. Most often, attackers target confidential information. But their actions also cause company downtime and disruption of core business.

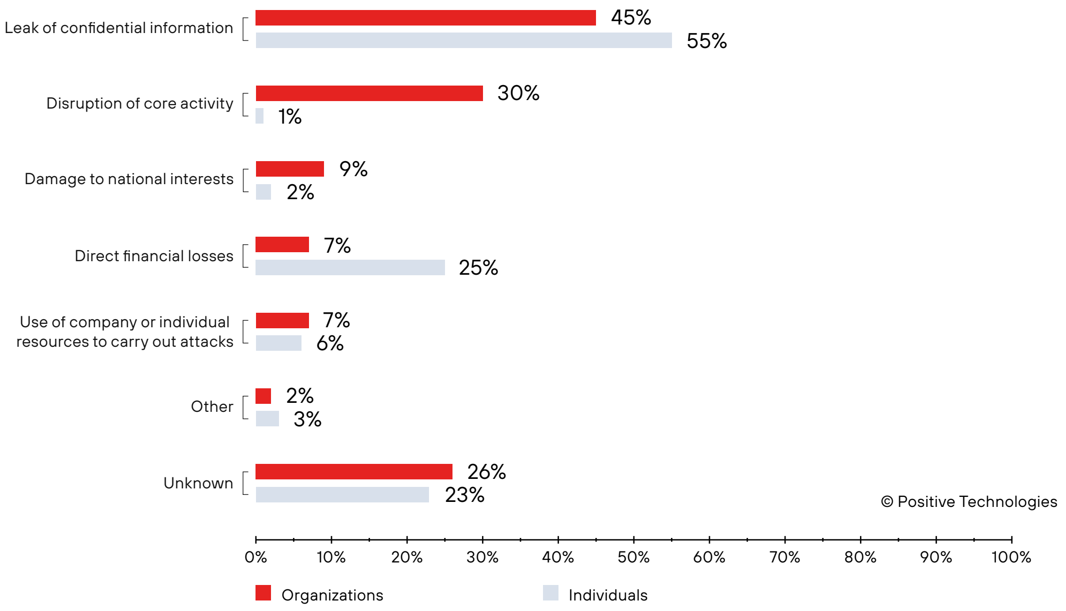
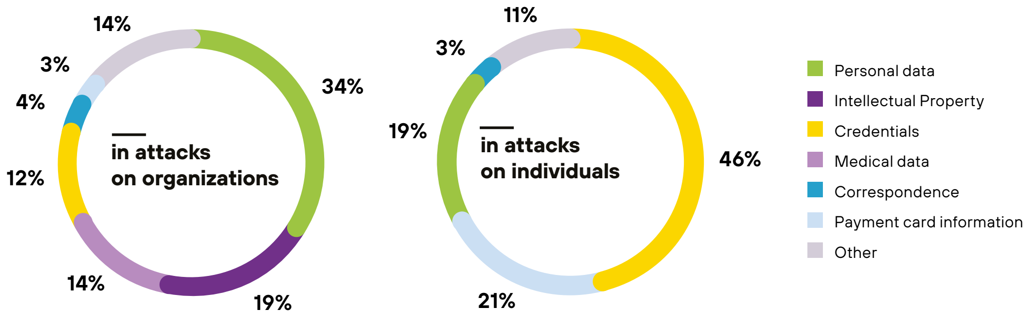


Figure 5. Attack consequences (share of attacks)

Data first

In Q1, attackers primarily aimed at stealing confidential information; for organizations, this was mostly personal data (34%) and information constituting trade secrets (19%). Medical information (14%) and credentials (12%) were also in high demand. As for attacks against individuals, attacker interest was focused on credentials (46%), personal data (19%), and payment card information (21%).



© Positive Technologies

Figure 6. Types of stolen data

High-profile leaks mostly affected IT companies; their consequences are examined in more detail in the Attacks on developers section below.

Note that the most valued prize in attacks on both organizations and individuals was credentials, which can later be sold on the dark web or used to develop an attack inside a corporate network. The hunt for them is ongoing: in mid-March, for example, PT Expert Security Center (PT ESC) detected a phishing email seemingly from Gosuslugi (Public Services Portal of the Russian Federation) aimed at harvesting domain accounts from Russian organizations. The message body contained a curious-looking link to a fake page: the cybercriminals only had a few domains at their disposal, but made the link look genuine by inserting the target company's domain into the third level. The link was structured as follows: *mail.[company_domain].[phishing_domain].ru.*

Service disruptions: from a single district to a whole country

The February attack on mobile operator Vodafone Portugal caused service disruptions across the country, including 4G and 5G networks, as well as SMS and television services. Vodafone Portugal serves more than four million mobile subscribers nationwide, and another 3.4 million Internet users, so the attack was felt by many Portuguese citizens. What's more, it took a long time for the company to restore its systems; its websites, for example, were down for almost a month.

Another case occurred in the U.S. state of New Mexico. An attack on the infrastructure of Bernalillo County shut down many government offices for several days and disrupted services to the general public. The attack affected 675,000 residents of the county, and work to restore the core systems lasted 12 days.

Transport in the crosshairs

In Q1, the transport industry also saw its fair share of attacks. As a result, passengers suffered delays, and there were interruptions in the supply of products and raw materials. And while an attack on the Italian railway company Ferrovie dello Stato Italiane suspended ticket sales, Belarusian Railway, the national rail company of Belarus, faced more serious consequences. In the first attack, cybercriminals encrypted the servers of the Belarusian Railway, which caused the online ticket office to malfunction. Another attack paralyzed train traffic in Minsk and Orsha, and messages appeared on Belarusian forums about service disruptions in Minsk.

The transport chaos was not limited to the railways: attackers also targeted air traffic. In Q1, the airport services company Swissport International reported a ransomware attack that resulted in flight delays.

Cyberattacks on the transport industry can impact raw materials supply chains: for example, the targeting of the major oil terminal operators SEA-invest (Belgium) and Evos (Netherlands) affected ports throughout Europe and Africa, causing delays in the supply of fuel.

Malware: spies and wipers

As before, the top positions belong to ransomware, which is used in almost one in two malware attacks, as well as malicious tools for remote control. Q1 also saw some campaigns focused on spreading wipers and DDoS tools.

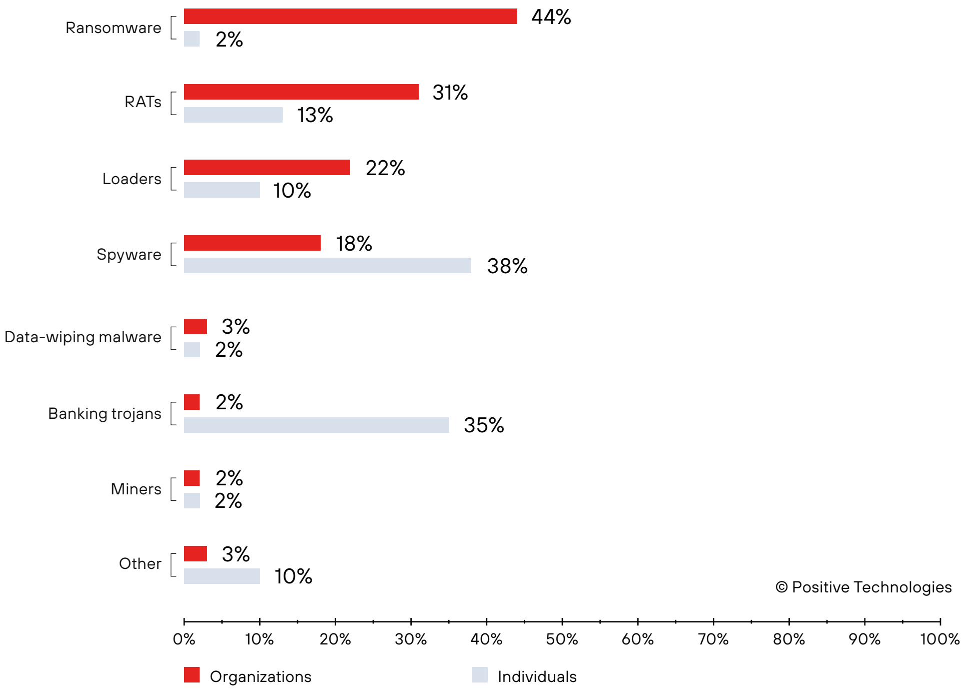


Figure 7. Types of malware (share of malware attacks)

A wave of wipers

In Q1, the number of wiper attacks increased: for organizations, they accounted for 3%, and for individuals 2%. Among the data wipers that became widespread in Q1 are WhisperGate, HermeticWiper, IsaacWiper, DoubleZero, and CaddyWiper. Interestingly, in some cases (especially WhisperGate), this malware impersonated ransomware attacks: victims even received ransom notes, but no decryption keys were provided, and the data was irrecoverably corrupted.

Also worth noting is the CaddyWiper malware, which checked whether the device was a domain controller: if it was, data was not wiped. This tactic was presumably employed to maintain access to the infected system.

Wipers can be spread in various ways: for example, HermeticWiper was propagated using a network worm, while DoubleZero was hidden in archives distributed in targeted phishing attacks. In the case of CaddyWiper, attackers usually had access to the compromised organizations' networks in advance.

> To guard against wiper attacks, first scan all received files in a sandbox—a special virtual environment. Make sure that the network is properly segmented: this will make it harder for malware to spread through the infrastructure. Pay special attention to isolating critical systems and protecting data backup storages to avoid unacceptable consequences for the organization.

Reselling access: VPN and then some

Cybercriminals exploit a variety of infection techniques to distribute infostealers and harvest information about the user and the system. Spyware made up 18% of attacks on organizations, and 38% on ordinary users.

Attackers are particularly drawn to user credentials for VPN services, which are collected by infostealers such as: RedLine, Phoenix, Jester Stealer, Saintstealer. The Phoenix stealer, for instance, can collect data from browsers, VPN tools, Discord, file system locations, and crypto wallets, and then send it to a remote server. Curiously, this malware was disguised as another, equally illegal type: what users initially downloaded was a program to conduct DDoS attacks.

RedLine, another widely used piece of malware, aims to steal browser credentials, VPN passwords, payment card and crypto wallet data, cookies, and other information. User data is often sold later on dark web forums: for example, more than half of the credentials up for sale on one such platform was obtained by the sellers using RedLine. What's more, the price for access to one account starts at five dollars, but the subsequent damage to the target organization can run into the millions of dollars if attackers compromise an employee's credentials for remote connection to the corporate network.

Malware distribution methods

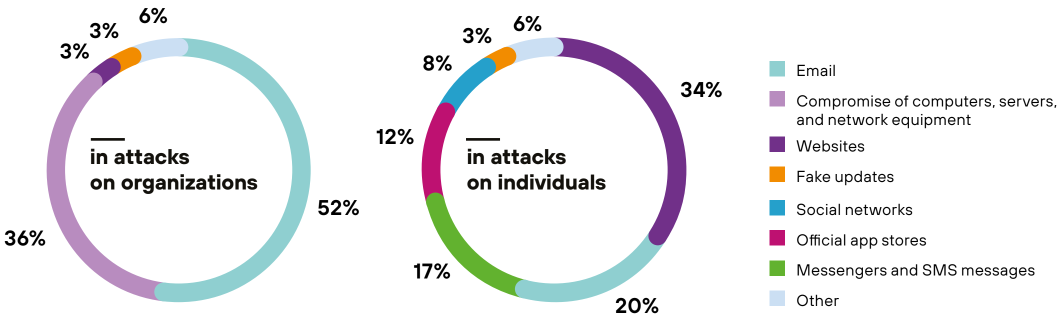


Figure 8. Malware distribution methods in attacks

Email is still the most common malware delivery method, used in 52% of attacks on organizations. For instance, PT ESC registered a mailing with an attachment containing information about events supposedly held by Roskomnadzor (the agency responsible for monitoring Russian mass media). In actual fact, the attackers exploited the CVE-2021-40444 vulnerability and downloaded Cobalt Strike Beacon to the victim device.

Mass mailings were used in attacks on Russian scientific enterprises in March too. Users were invited to open an attachment to view a list of sanctioned individuals, but the template itself contained a malicious macro to get a loader onto the device.

In attacks on individuals, attackers most often used fake or compromised websites, email, instant messengers, and social networks. For instance, the above-mentioned RedLine stealer targeted Valorant players and spread through YouTube: users were prompted to follow a link in the video description to download an auto-targeting bot.

Ways to conceal malicious activity

To hide their activities, attackers adapt methods and techniques to counter detection. For example, the BazarBackdoor malware is distributed via contact forms on corporate websites instead of regular phishing emails, so that the malicious attachment is not detected.

Cybercriminals also continue to abuse features of legitimate services and software. For example, in attacks on users with Google accounts, attackers leveraged the mention feature in Google Docs: after being notified of a mention by email, victims were prompted to click a malicious link left in the comments. Meanwhile, Raccoon Stealer used Telegram as a C2 server, making it possible to hide suspicious traffic in the networks of companies that used this messenger. As this app becomes more popular, attackers are increasingly using it.

To resist analysis, some malicious programs have special embedded functions that execute if detected. For example, the latest version of the BRATA, malware for Android includes functionality for resetting the device settings to remove all traces of malicious activity.

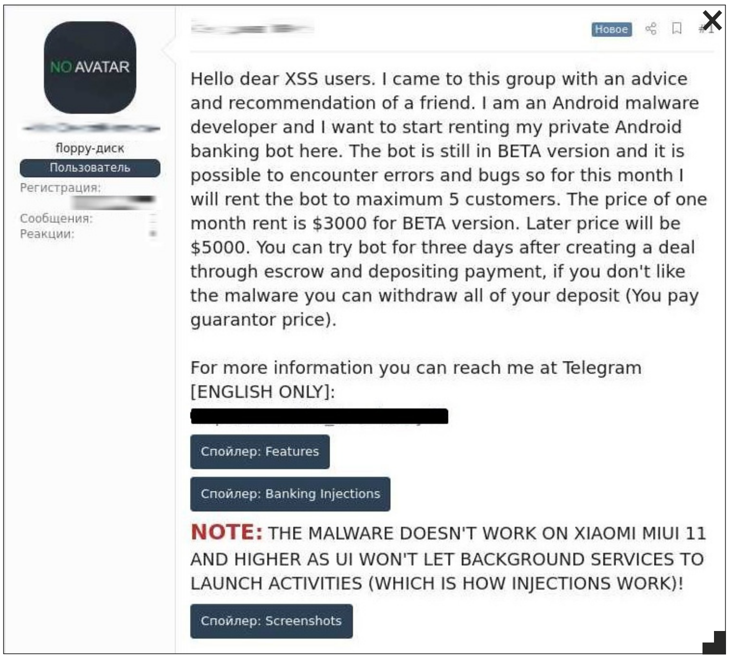
We also note the emergence of new cybercriminals yet to realize their potential. Researchers at Symantec report the use of the sophisticated and powerful new malware loader Verblecon by an unknown perpetrator in relatively simple cryptocurrency mining attacks. This Java-based malware uses server-side polymorphism to evade detection: using encryption and obfuscation, Verblecon can change form for security scanners each time it is loaded.

Focus on Android users

Malicious programs worm their way into official app stores time and again, bypassing protection. In Q1, programs containing malicious apps (FluBot, TeaBot, SharkBot, Escobar, Vultur) were slipped onto and removed from Google Play.

Earlier, we predicted a rise in the number of attacks on online banking users. Most of the infostealers being spread are banking trojans, and their share of all malware used in attacks on individuals is 35%. We advise you to be careful when installing new apps and take time to read the reviews: malware can be lurking inside even seemingly harmless programs. For example, the FluBot banking trojan was distributed as Flash Player, but once on the victim device and armed with the necessary permissions, it could steal online banking credentials and intercept text messages and one-time passwords. Another banking trojan, TeaBot, has appeared repeatedly on Google Play since December 2021 under the guise of QR code readers, weather apps, and data-cleaning tools, infecting more than 140,000 devices. Some malware, such as SharkBot, can even pass itself off as antivirus software.

Cybercriminals are increasingly furnishing their creations with the ability to intercept multifactor authentication codes (some malware poses as MFA applications, such as the Vultur banking trojan) and expanding the number of embedded functions. For instance, the Escobar banking trojan features a wide range of capabilities: control over infected devices through VNC Viewer; audio recording; screenshots; intercepting text messages; reading/writing to storage; getting a list of accounts; disabling keypad lock; making calls; and accessing device location. And this, it seems, is not the final version of the malware: the author leased the beta version of the program for $3,000 a month, while other attackers could test the bot for free for three days.



Hello dear XSS users. I came to this group with an advice and recommendation of a friend. I am an Android malware developer and I want to start renting my private Android banking bot here. The bot is still in BETA version and it is possible to encounter errors and bugs so for this month I will rent the bot to maximum 5 customers. The price of one month rent is $3000 for BETA version. Later price will be $5000. You can try bot for three days after creating a deal through escrow and depositing payment, if you don't like the malware you can withdraw all of your deposit (You pay guarantor price).

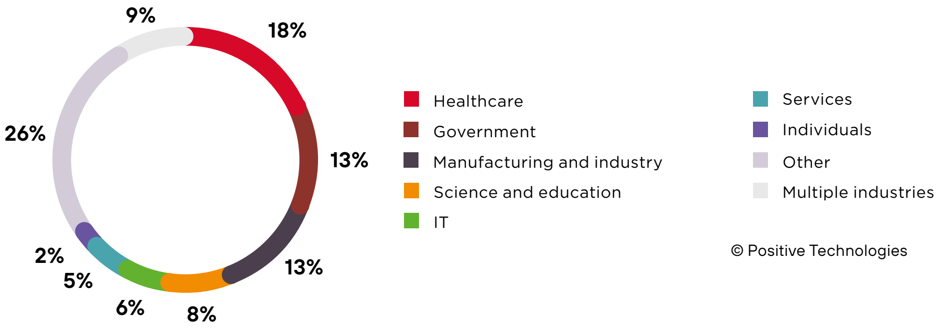
For more information you can reach me at Telegram [ENGLISH ONLY]:
[redacted]

NOTE: THE MALWARE DOESN'T WORK ON XIAOMI MIUI 11 AND HIGHER AS UI WON'T LET BACKGROUND SERVICES TO LAUNCH ACTIVITIES (WHICH IS HOW INJECTIONS WORK)!

Figure 9. Ad offering lease of Escobar banking trojan

Adaptation of ransomware

In Q1, ransomware was still active, with the lion's share of attacks aimed, as before, at medical institutions: cybercriminals were tempted by the sheer volume of information in the systems, combined with poor infrastructure security. The share of the attacks targeting government agencies rose from 8 to 13%. We again observed high-profile attacks on industrial enterprises and IT companies.



© Positive Technologies

Figure 10. Share of ransomware attacks by target

Continued attacks on QNAP devices

Owners of NAS drives still need to keep their finger on the pulse with timely security updates: January saw the start of a new Qlocker ransomware campaign. Ransom notes began appearing en masse on hacked devices.

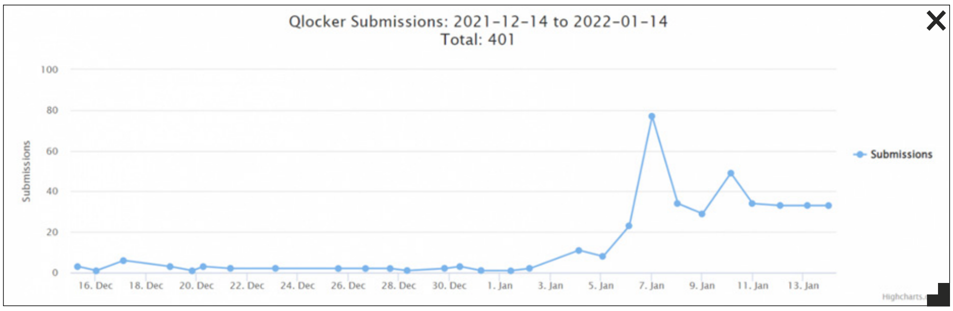


Figure 11. Number of Qlocker attacks

Later, also in January, a new ransomware group called DeadBolt encrypted multiple QNAP NAS devices worldwide, exploiting a zero-day vulnerability in the software. DeadBolt also left a ransom note for the victim company, offering to provide details of the vulnerability or send a universal decryption master key for 50 BTC.

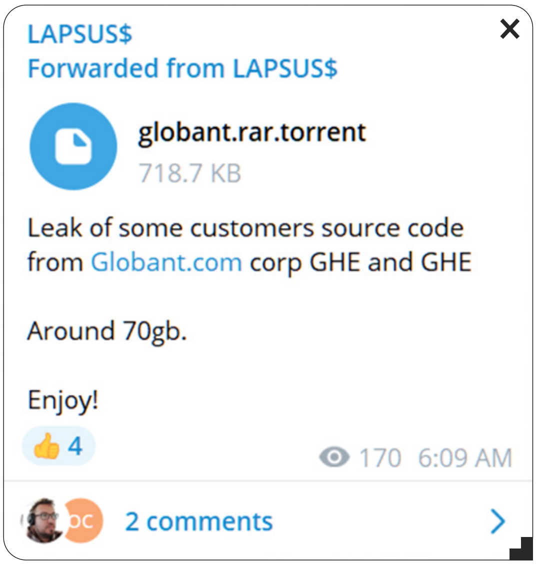
Adapting to different systems and cross-platforming

To adapt ransomware to different systems, cybercriminals rewrite their creations in other languages: for example, the BlackCat group (former members of BlackMatter, aka Darkside) is developing a new multi-platform malware program in Rust. The Hive group rewrote its malware in this same language.

Virtualization systems continue to be attacked. In early Q1, attackers made active use of a high-profile vulnerability in the Log4j library to attack VMware servers; at the same time, ransomware operators are adapting programs for different operating systems. For example, the AvosLocker ransomware has migrated to Linux and now targets VMware ESXi servers.

What next

The slight drop in the share of ransomware attacks is due to the fact that some attackers are switching to data theft, and not all attacks involve infrastructure encryption. A case in point is the Lapsus$ group, which sought to reassert itself with attacks on major companies, such as Nvidia, Samsung, Microsoft, and Globant. Compromised data was made public, but no systems were encrypted.



LAPSUS$
Forwarded from LAPSUS$

globant.rar.torrent
718.7 KB

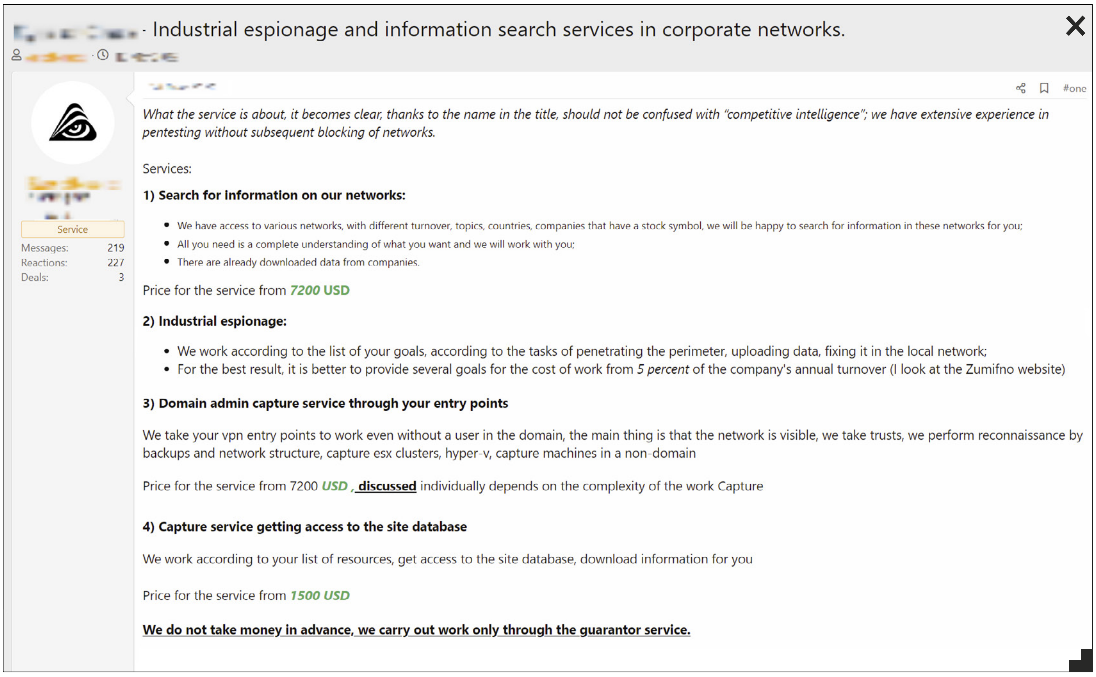
Leak of some customers source code from Globant.com corp GHE and GHE

Around 70gb.

Enjoy!

Figure 12. Archive of compromised data published by Lapsus$

We expect other groups to pick up this trend. Dark web ads offering industrial espionage and information search in corporate networks are becoming more frequent.



[redacted] · Industrial espionage and information search services in corporate networks.

[redacted] · [redacted]

[redacted]

Service

Messages: 219
Reactions: 227
Deals: 3

What the service is about, it becomes clear, thanks to the name in the title, should not be confused with "competitive intelligence"; we have extensive experience in pentesting without subsequent blocking of networks.

Services:

1) Search for information on our networks:

- We have access to various networks, with different turnover, topics, countries, companies that have a stock symbol, we will be happy to search for information in these networks for you;
- All you need is a complete understanding of what you want and we will work with you;
- There are already downloaded data from companies.

Price for the service from ***7200* USD**

2) Industrial espionage:

- We work according to the list of your goals, according to the tasks of penetrating the perimeter, uploading data, fixing it in the local network;
- For the best result, it is better to provide several goals for the cost of work from *5 percent* of the company's annual turnover (I look at the Zumifno website)

3) Domain admin capture service through your entry points

We take your vpn entry points to work even without a user in the domain, the main thing is that the network is visible, we take trusts, we perform reconnaissance by backups and network structure, capture esx clusters, hyper-v, capture machines in a non-domain

Price for the service from 7200 ***USD*** , **discussed** individually depends on the complexity of the work Capture

4) Capture service getting access to the site database

We work according to your list of resources, get access to the site database, download information for you

Price for the service from ***1500* USD**

We do not take money in advance, we carry out work only through the guarantor service.

Figure 13. Industrial espionage ad on a dark web forum

Attackers are switching their attention to insurance companies. In an interview with REvil, the group explained why they make attractive targets: their systems contain information about companies that have cyberinsurance policies and are thus more likely to pay a ransom.

More attacks on government agencies

In Q1 2022, the number of attacks on government agencies returned to its former level, almost doubling compared to Q4 2021.

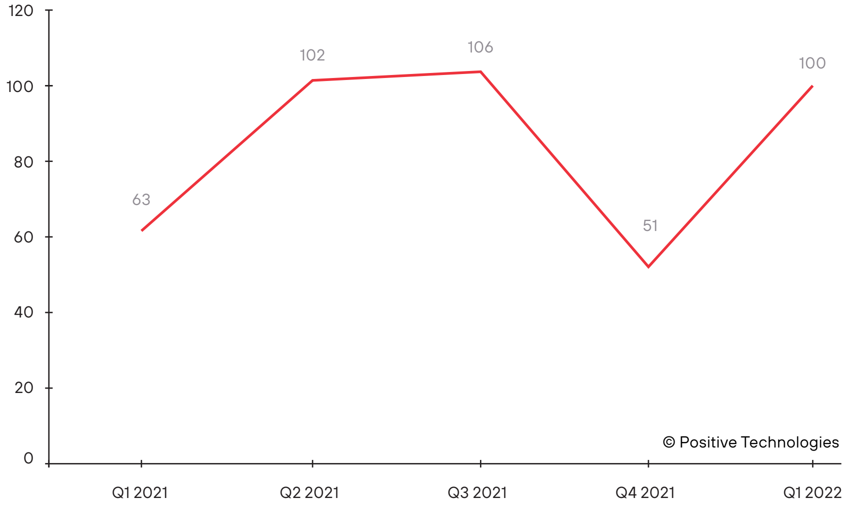


Figure 14. Number of attacks on government agencies

In most cases, the attackers' goal was to disrupt the victim's operation and steal confidential information. In the second half of the quarter, we observed a surge of attacks on various government websites.

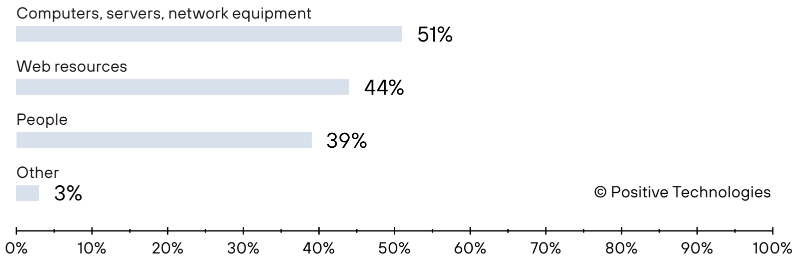


Figure 15. Targets of attacks on government agencies (share of attacks)

To disable target systems, cybercriminals aimed not only at web resources, but also at telecommunications service providers: Israel, for example, declared a state of emergency after an unprecedented cyberattack on government systems. Several Israeli government websites were taken down. A source in the country's defense establishment claimed it was the largest-ever cyberattack against Israel.

Serious consequences for industry

Q1 was not without large-scale attacks on various industries: oil and gas, energy, and agriculture. The primary goal was to steal confidential information, but the attacks also affected the core operations of victim companies, causing major damage, including shutdown of entire plants and disruption of production and business processes.

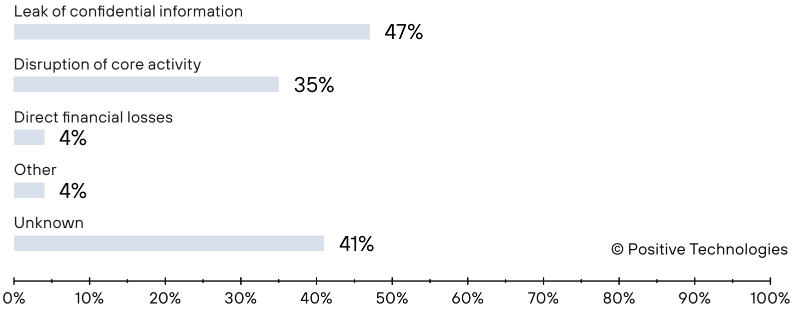


Figure 16. Consequences of attacks on industry sectors

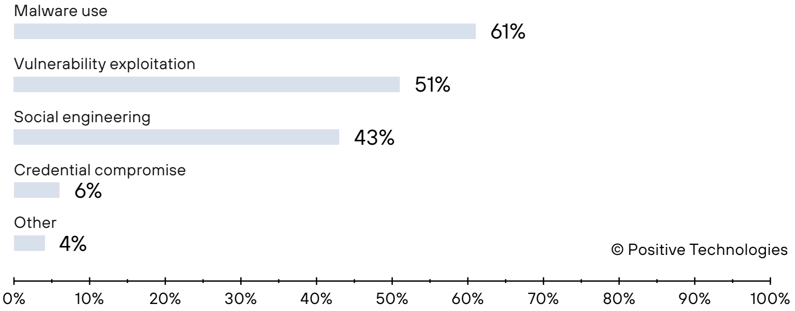


Figure 17. Methods of attacks on industry sectors

In late January, two subsidiaries of Marquard & Bahls AG, a German energy and chemicals group, fell victim to cyberattacks: gasoline distributor Oiltanking and oil supplier Mabanaft. They are believed to have been hit by a ransomware attack, with Marquard & Bahls being the likely breach point in both cases. The attack consequences are significant not only for the entities involved, but for ordinary citizens too: these companies supply fuel to many gas stations across Germany, and a shortage of gasoline could impact the country's entire economy. The clean-up costs are also substantial: many automated production processes (such as loading/unloading tanks) depend entirely upon computer systems that were disabled for some time.

Once again, the energy sector came under attack: a March advisory from the FBI warned of attacks using the specialized TRITON malware aimed at safety instrumented systems. Embedded malicious code can cause damage to facilities, system downtime, and even fatalities if the system fails to correctly initiate safety shutdown procedures.

An attack on Kojima Industries, a Japanese manufacturer of plastic components for cars, also had serious consequences and led to Toyota suspending operations at 14 plants in Japan. According to Kojima Industries, ransomware was again to blame for the system failure.

Cryptocurrencies and blockchain

Cryptocurrencies are, quite literally, gaining currency. Their increased popularity is being exploited by cybercriminals who probe cryptocurrency exchanges and transfer protocols for vulnerabilities, as well as adapt fraudulent schemes to individuals and cryptoinvestors.

Cryptoinvestors and cryptowallet owners in the crosshairs

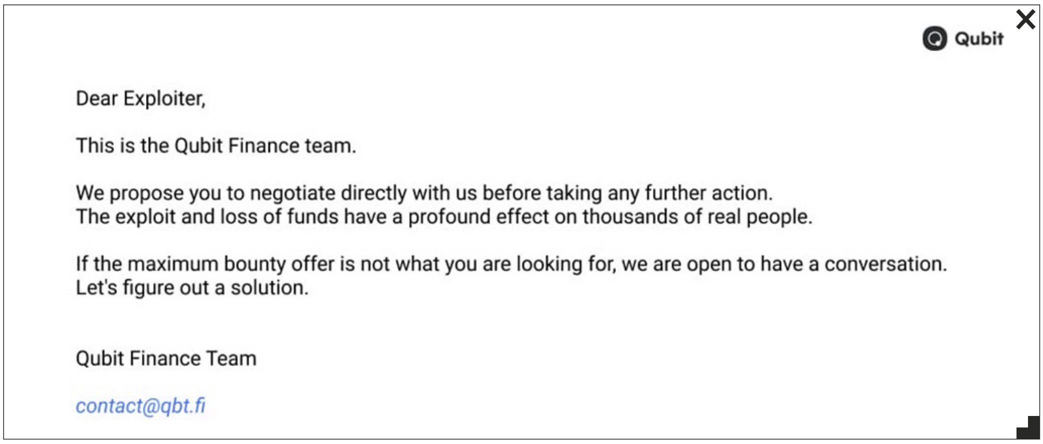
Many infostealers are focusing more on cryptowallets and less on bank card details. For example, Bitdefender researchers discovered the new modular BHUNT malware, designed to hijack cryptowallets by stealing passwords and passphrases.

Attacks on cryptoinvestors continue: researchers at Akamai described the actions of attackers exploiting the Amazon brand to squeeze bitcoins out of potential investors. Cybercriminals are also leveraging the growing popularity of NFTs. In January, for instance, the CryptoBatz project hosted an NFT sale on its Discord channel, but accidentally left a discarded URL active, along with old tweets linking to it. Scammers set up a fake server, and users who clicked on the legitimate link, instead of buying NFTs, transferred money to the cybercriminals' wallet.

Big financial losses

In Q1, we noted an increase in attacks on blockchain projects and cryptocurrency exchanges. What's more, March witnessed an attack on Axie Infinity's Ronin sidechain, believed to be the largest cryptoheist to date. The perpetrator attempted to withdraw nearly 620 million U.S. dollars in Ethereum and USDC tokens after gaining access to most of the validator nodes needed to drain the funds.

In the wake of an attack, companies often offer monetary rewards for disclosure of found and exploited vulnerabilities. In January, Qubit Finance's DeFi platform was hacked and about 80 million U.S. dollars in cryptocurrency stolen. Qubit was unable to recover the funds on its own, so at first the company offered the attacker a reward for describing the vulnerability using the Private Note feature. After that, Qubit additionally published an appeal on Twitter.



Dear Exploiter,

This is the Qubit Finance team.

We propose you to negotiate directly with us before taking any further action.
The exploit and loss of funds have a profound effect on thousands of real people.

If the maximum bounty offer is not what you are looking for, we are open to have a conversation.
Let's figure out a solution.

Qubit Finance Team

contact@qbt.fi

Figure 18. Qubit's Twitter appeal

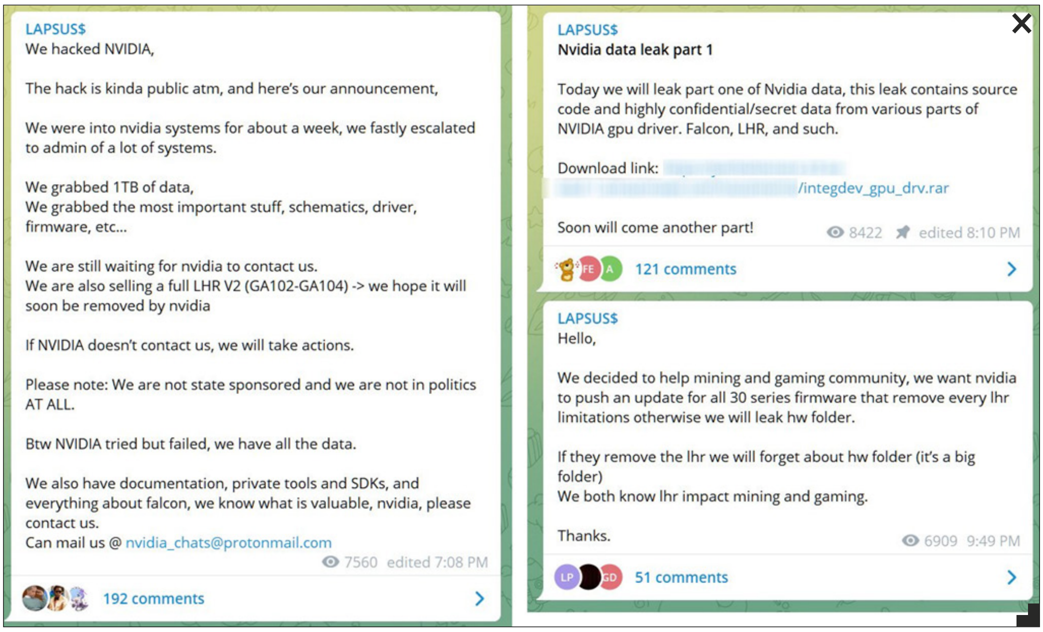
Another case is related to a bug in the Multichain network protocol, whose exploitation has already caused damage to the tune of 1.5 million U.S. dollars. One of the hackers who used this vulnerability to steal $200,000 later claimed to be a white hatter, and offered to return 80% of the funds.

Attacks on developers

Theft of source code and certificates for signatures

In Q1, we observed some large-scale attacks aimed at IT companies: in February, Lapsus$ attacked U.S. graphics card developer Nvidia, and in early March, Samsung suffered a breach of the Samsung Galaxy source code.

The attack on Nvidia resulted in the theft of 1 TB of data. The group also published a nearly 20 GB archive reportedly containing source code for video card drivers. Later, through an open chat, Lapsus$ offered its mining tool for Nvidia GPUs, which allows a bypass of internal restrictions.



LAPSUS$
We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.
Can mail us @ nvidia_chats@protonmail.com

7560 edited 7:08 PM

192 comments

LAPSUS$
Nvidia data leak part 1

Today we will leak part one of Nvidia data, this leak contains source code and highly confidential/secret data from various parts of NVIDIA gpu driver. Falcon, LHR, and such.

Download link: [redacted]/integdev_gpu_drv.rar

Soon will come another part!

8422 edited 8:10 PM

121 comments

LAPSUS$
Hello,

We decided to help mining and gaming community, we want nvidia to push an update for all 30 series firmware that remove every lhr limitations otherwise we will leak hw folder.

If they remove the lhr we will forget about hw folder (it's a big folder)
We both know lhr impact mining and gaming.

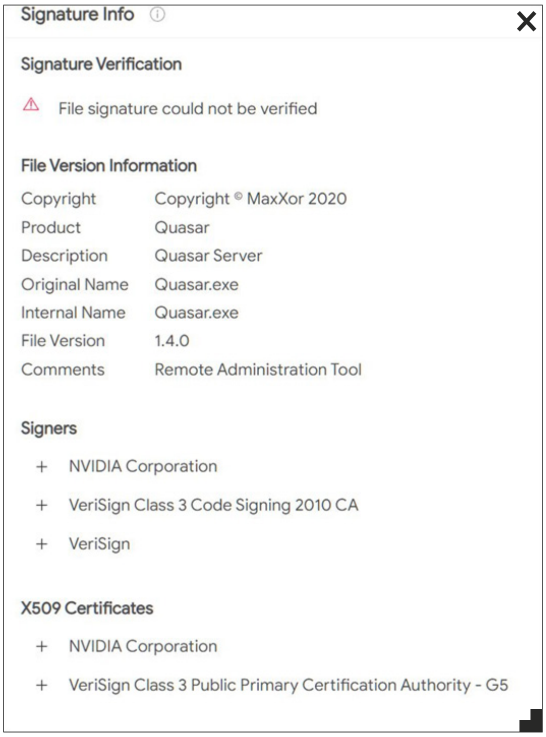
Thanks.

6909 9:49 PM

51 comments

Figure 19. Lapsus$ messages posted on Telegram

And still that's not all the attack consequences: later, the cybercriminals used the stolen Nvidia certificates to sign their malware to create the appearance of a legitimate program. According to samples uploaded to the VirusTotal malware scan engine, the stolen certificates were used to sign Cobalt Strike Beacon and Mimikatz, plus various backdoors and remote access trojans.



Signature Info

Signature Verification

⚠ File signature could not be verified

File Version Information

Copyright	Copyright © MaxXor 2020
Product	Quasar
Description	Quasar Server
Original Name	Quasar.exe
Internal Name	Quasar.exe
File Version	1.4.0
Comments	Remote Administration Tool

Signers

- NVIDIA Corporation
- VeriSign Class 3 Code Signing 2010 CA
- VeriSign

X509 Certificates

- NVIDIA Corporation
- VeriSign Class 3 Public Primary Certification Authority - G5

Figure 20. Quasar RAT signed by NVIDIA certificate

This case was not the only one seen in Q1. AhnLab researchers discovered a new Magniber ransomware campaign under the guise of fake Chrome and Firefox updates signed with valid Microsoft certificates.

Malware in open-source libraries

Many developers in Q1 were caught off guard by the mass distribution of malware embedded in the code of open-source libraries.

In March, the developer of node-ipc, a popular npm package, released versions of the library which, if run, would delete and overwrite all data on users' computers. Such an attack could potentially do a lot of harm to users: node-ipc is an important package that is used by major development libraries and gets more than a million downloads per week. For example, Vue.js, a JavaScript framework, also uses node-ipc as a dependency, so many users asked the project developers to bind the node-ipc dependency to a secure version after some systems became corrupted.

Attackers often use typosquatting—an attack method in which the victim is tricked using packages with names similar to legitimate ones. Also in March, JFrog analysts detected 218 malicious packages targeting npm developers using the @azure scope, as well as @azure-rest, @azure-tests, @azure-tools, and @cadl-lang. This set of legitimate packages is downloaded tens of millions of times every week, so the probability of typing errors and downloading spyware among some users is quite high.

Developers must keep specialized development environments secure. In late March, Aqua Security researchers discovered Python ransomware targeting vulnerable misconfigured Jupyter Notebook environments. Since this development environment is used to analyze and build data models, such an attack can cause significant damage to organizations.

About the research

This report contains information on current global information security threats based on Positive Technologies' own expertise, investigations, and reputable sources.

We believe that 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 do a precise threat count. Our research seeks to draw the attention of companies and individuals who care about information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies glossary.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

Positive Technologies is a leading global provider of cybersecurity solutions. Over 2,300 organizations worldwide use technologies and services developed by our company. For more than 20 years, our mission has been to safeguard businesses and entire industries against the threat of cyberattacks.

Positive Technologies is the first and only cybersecurity company in Russia to go public on the Moscow Exchange (MOEX: POSI).

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