POSITIVE TECHNOLOGIES

Hack at all costs

Putting a price on APT attacks

Contents

Introduction

The assets of well-off companies and governments have always attracted attackers. That's why potential targets commit considerable resources to securing their information. Gartner estimates that worldwide expenditures on digital security will exceed $124 billion this year. But attackers rarely give up on a target even if their first attempts are unsuccessful. According to FireEye statistics, 64 percent of companies attacked in 2018 were attacked again in the following 19 months.

A cyberattack against a company with well-organized protection system is time-consuming, expensive, and requires special knowledge and tools. Multistage, well-planned, and organized attacks targeting a specific industry or company are called advanced persistent threats (APTs). To conduct such attacks, hackers form criminal groups, known as APT groups.

It's extremely difficult to detect an APT attack when it is underway. After obtaining a foothold in a company's infrastructure, criminals can stay there unnoticed for years. For example, the cybersecurity team at German pharmaceutical giant Bayer observed malware activity for over a year. The longest presence of attackers on a network, as measured by the PT Expert Security Center (PT ESC), was over eight years. However, profit-driven cybercriminals prefer to act quickly. Cosmos Bank fell victim to a cyberattack by the Lazarus Group, which stole $13.5 million in just three days. In other words, criminals' behavior, techniques, and tools depend on their target.

In this research, we will try to assess the cost of tools used for APT attacks and how easily these tools can be obtained. We will also analyze how attackers choose their tools based on their target. We hope that our study will assist security decision-makers to better protect their systems from industry-specific attacks.

Executive summary

It is impossible to make an exact estimate of how much an APT attack costs. One reason is the difficulty of putting a value on the unique software used by criminal groups. All amounts stated in this report are approximate; actual APT expenses may be significantly higher.

- Spear phishing is an effective way to penetrate a company's internal network and is used by 90 percent of APT groups. Tools for creating malicious attachments, not including the cost of exploits for zero-day vulnerabilities, cost around $2,000.
- After penetrating the internal network, half of APT groups use legitimate administration tools and commercial penetration testing software costing from $8,000 to $40,000.
- By our estimates, the cost of the tools needed for a banking attack would start at $55,000. A cyberespionage campaign would be much more expensive, running at least $500,000 to start.

About the research

We have analyzed the tools used by 29 APT groups conducting attacks worldwide with activity during the last two years and threatening key sectors such as government, finance, and industrial companies.

Data is based on our incident response expertise and retrospective analysis of security events on corporate infrastructure, as well as on constant monitoring of active APT groups by PT ESC. We have also drawn upon publicly available reports on APT groups from reputable security companies.

We identified two main categories of APT groups based on attack motive. The first category includes financially motivated groups, which attack banks and other organizations to steal money. Cyberespionage groups, by contrast, target valuable information and seek long-term control over infrastructure.

Tools used to obtain initial access to a company's local network are different from those used during the later stages of the attack. However, the two types of groups tend to use similar tools when gaining a foothold in the system and performing lateral movement. Therefore, we have split APT tools into two categories:

- Tools used to break into the organization's network ("Initial access")
- Tools used to develop the attack on the internal network ("Attack development")

We analyzed postings on 190 darkweb sites and venues about purchase or sale of APT tools, as well as custom malware development. We focused on forums, specialized marketplaces, and chats. On average, over 70 million people visit them each month.

APT tools

Initial access

Expenses at the initial compromise stage depend on how exactly attackers deliver malware to the company's infrastructure. The method depends on the attackers' motives and the victim's level of protection.

Spear phishing is the main tool of financially motivated attackers. To conduct a phishing attack, a hacker prepares a document containing malware and a loader (dropper).

Documents containing malicious code can be created using special programs known as exploit builders. These programs generate a file with malicious code, which runs when the file is opened. This code downloads and runs the loader (a small program responsible for downloading the main malware module). The loader is normally used just once: running the loader again, even if it is obfuscated, can be detected by antivirus software.

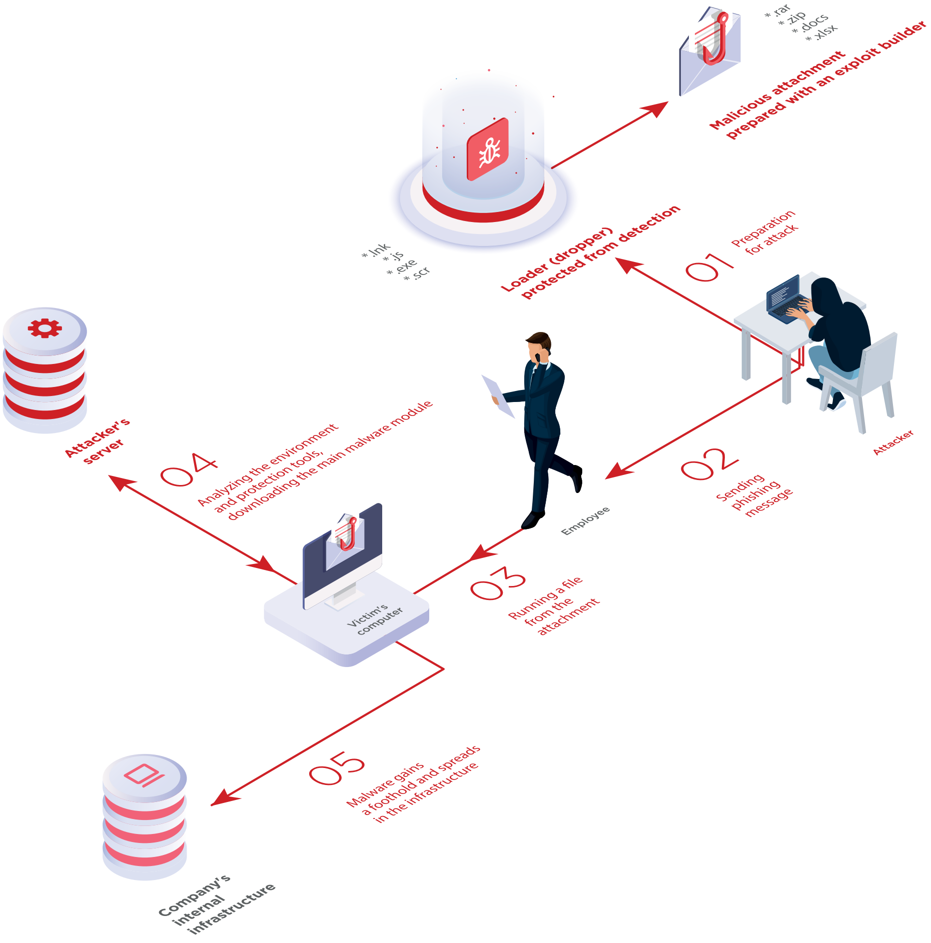

* .rar
* .zip
* .docs
* .xlsx
Malicious attachment prepared with an exploit builder
* .lnk
* .js
* .exe
* .scr
Loader (dropper) protected from detection
01
Preparation for attack
Attacker
02
Sending phishing message
Employee
03
Running a file from the attachment
Victim's computer
04
Analyzing the environment and protection tools, downloading the main malware module
Attacker's server
05
Malware gains a foothold and spreads in the infrastructure
Company's internal infrastructure

Figure 1. Phishing: malware preparation and delivery to local network

The cost of tools used to create malicious documents depends heavily on whether the malware has the ability to persist on the target system undetected by antivirus software. Malware source code costs much higher than a ready-to-use utility. For example, a ready-to-use loader costs only $25, but the source code costs at least $1,500, plus time and expenses for further modifications.

57%

of regional companies were hit by phishing attacks on employees in 2018

Spear phishing is the most common method used as an entry point

90%

of active APT groups use phishing at the initial access stage

Examples of groups:
Cobalt, APT29, Lazarus

$300+

cost of tool to create malicious files

$ 2,500

monthly subscription fee for a service to create documents with malicious content

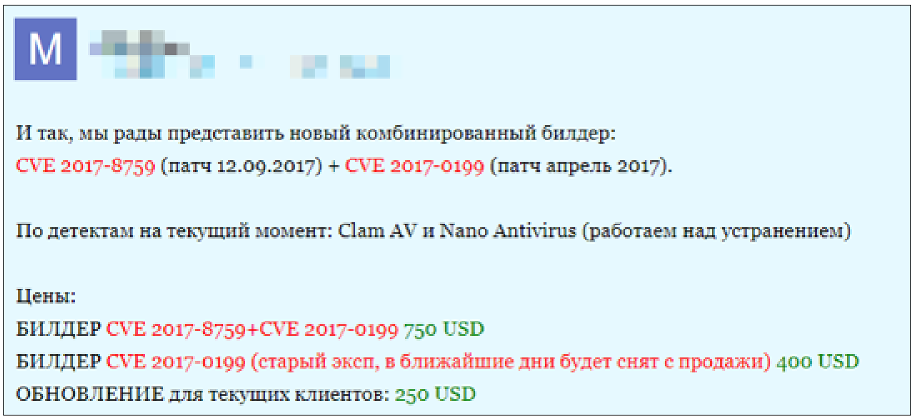
$1,500+

cost of loader source code

Spear phishing is widely used by the Cobalt group. The group constantly refines its techniques to exploit the latest vulnerabilities. In 2017, Cobalt obtained an exploit builder for vulnerability CVE-2017-0199, which at the time was being sold for $10,000. Today, exploit builders for the vulnerability can be bought for just $400.

$10,000

cost of the exploit builder used by Cobalt

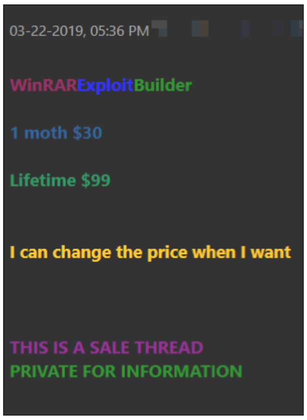


И так, мы рады представить новый комбинированный билдер:
CVE 2017-8759 (патч 12.09.2017) + CVE 2017-0199 (патч апрель 2017).

По детектам на текущий момент: Clam AV и Nano Antivirus (работаем над устранением)

Цены:
БИЛДЕР CVE 2017-8759+CVE 2017-0199 750 USD
БИЛДЕР CVE 2017-0199 (старый эксп, в ближайшие дни будет снят с продажи) 400 USD
ОБНОВЛЕНИЕ для текущих клиентов: 250 USD

Figure 3. Prices of exploits for vulnerabilities found in 2017



03-22-2019, 05:36 PM

WinRARExploitBuilder

1 moth $30

Lifetime $99

I can change the price when I want

THIS IS A SALE THREAD
PRIVATE FOR INFORMATION

Figure 2. Exploit builders for sale

The financially motivated Silence group also uses spear phishing, exploiting vulnerabilities such as CVE-2018-0802 and CVE-2018-8174. Exploits for these vulnerabilities can be bought on the darkweb for as little as $1,600.

Cash-hungry criminals are interested in quick gains (on average, just one week to one month passes between sending messages and cashing out). Therefore, they are willing to buy ready-made tools and send mass phishing emails.

Just like financially motivated attacks, cyberespionage APT efforts usually start with phishing. But whereas ordinary criminals might take a scattershot approach targeting an entire industry, cyberspies act with precision and careful preparation. For example, in one penetration attempt investigated by PT ESC, the SongXY group sent a document with a link to an image on an attacker-controlled server. The link triggered automatically when the document was opened. This allowed attackers to collect additional information about the server configuration, including the Microsoft Office version in use, and choose a malicious document with the right exploit needed to compromise the system.

The exploit builders and loaders used by cyberspies are not sold on the darkweb. Even roughly estimating the cost of such tools is nearly impossible. One can only compare them with the prices for custom development. Darkweb criminals are ready to pay $20,000 or more for custom development of a single tool.

Cyberespionage APT groups may prepare malicious emails by hand. They are determined for their malicious code not to be detected by any security system, and focus above all on bypassing the protection tools used by the target organization. Identifying these protection tools is one of the key tasks at the attack reconnaissance stage. These attackers carefully choose the layout and text of their messages, making it likely that the victim will open the attachment.

To further increase the odds of phishing success, cyberespionage APT groups may even hack partners and contractors of a target organization and impersonate them in emails. In spring 2019, hackers penetrated the network of IT giant Wipro and sent phishing messages to the company's clients.

14%

of groups conduct watering hole attacks at the penetration stage

Cost: $10,000+

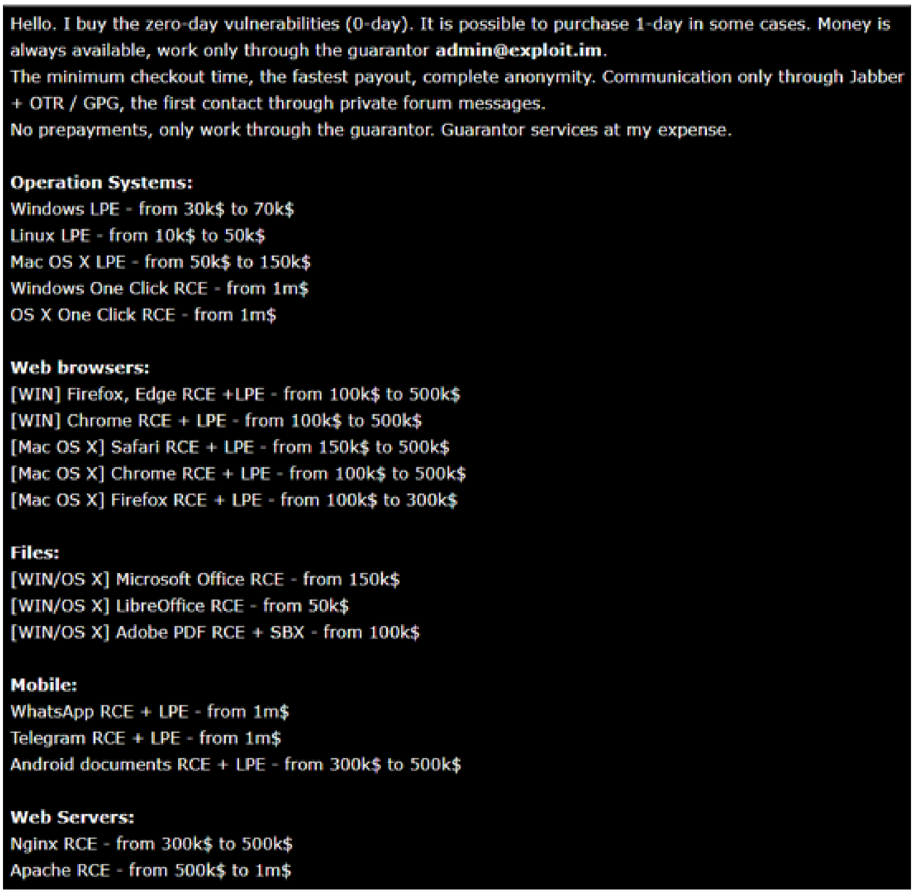
Examples of groups: APT29, APT35, TEMP.Periscope, DarkHydrus

Attackers sometimes conduct watering hole attacks. They select web pages regularly visited by a target company's employees, such as partners' websites or industry-specific portals. Attackers then hack these websites and install malware on them. If targeted employees subsequently visit the infected websites, the attackers may penetrate the company's internal network.

Cyberespionage groups do not scrimp on expensive exploits for zero-day vulnerabilities, can develop their own tools, and conduct multistage attacks that leverage other organizations to get at the ultimate target.

More than $1,000,000

a single exploit for a zero-day vulnerability can cost



Hello. I buy the zero-day vulnerabilities (0-day). It is possible to purchase 1-day in some cases. Money is always available, work only through the guarantor **admin@exploit.im**.
The minimum checkout time, the fastest payout, complete anonymity. Communication only through Jabber + OTR / GPG, the first contact through private forum messages.
No prepayments, only work through the guarantor. Guarantor services at my expense.

Operation Systems:
Windows LPE - from 30k$ to 70k$
Linux LPE - from 10k$ to 50k$
Mac OS X LPE - from 50k$ to 150k$
Windows One Click RCE - from 1m$
OS X One Click RCE - from 1m$

Web browsers:
[WIN] Firefox, Edge RCE +LPE - from 100k$ to 500k$
[WIN] Chrome RCE + LPE - from 100k$ to 500k$
[Mac OS X] Safari RCE + LPE - from 150k$ to 500k$
[Mac OS X] Chrome RCE + LPE - from 100k$ to 500k$
[Mac OS X] Firefox RCE + LPE - from 100k$ to 300k$

Files:
[WIN/OS X] Microsoft Office RCE - from 150k$
[WIN/OS X] LibreOffice RCE - from 50k$
[WIN/OS X] Adobe PDF RCE + SBX - from 100k$

Mobile:
WhatsApp RCE + LPE - from 1m$
Telegram RCE + LPE - from 1m$
Android documents RCE + LPE - from 300k$ to 500k$

Web Servers:
Nginx RCE - from 300k$ to 500k$
Apache RCE - from 500k$ to 1m$

Figure 4. Prices attackers are ready to pay for zero-day vulnerabilities

Attack development

48%

of APT groups use penetration testing tools

Inside the infrastructure, an attack passes through several stages: intruders execute code on hosts, escalate privileges, collect data, move among hosts, and create channels for command and control (C2). APT groups use similar tools for attack development on internal networks. Both financially motivated and cyberspy groups prefer publicly available legitimate software, using self-developed malware or buying utilities on the darkweb only when necessary.

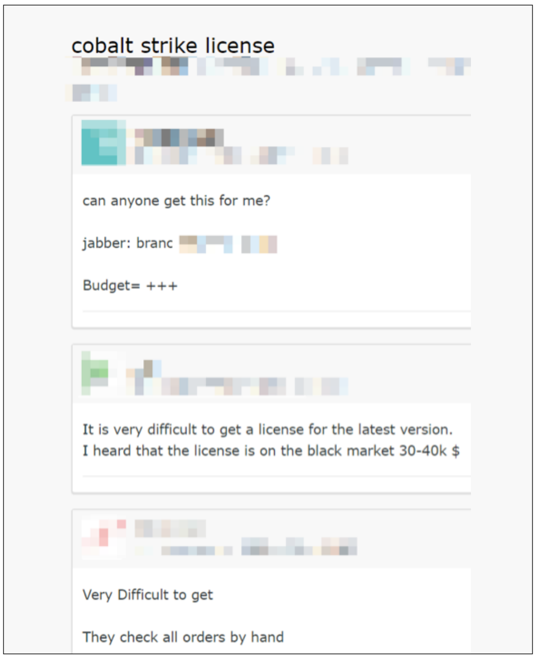
Cobalt Strike and Metasploit Pro are commercial frameworks used for penetration testing. However, they enjoy popularity among both security experts and black hats.

Cobalt Strike

Official price at the time of this study: $3,500 per year

Black market prices: $30,000–$40,000

Groups: APT10, APT29, APT32, APT40, Cobalt, DarkHydrus, Winnti



cobalt strike license

[redacted]

[redacted]

can anyone get this for me?

jabber: branc [redacted]

Budget= +++

[redacted]

It is very difficult to get a license for the latest version.
I heard that the license is on the black market 30-40k $

[redacted]

Very Difficult to get

They check all orders by hand

Figure 5. Demand for Cobalt Strike on the darkweb

The developers of Cobalt Strike, aware of their product's potentially nefarious appeal, perform strict checks on potential customers. As a result, hackers periodically express interest on the darkweb in obtaining hacked or illegally obtained official versions of Cobalt Strike.

Metasploit Pro is also sold on the darkweb. Available versions include hacked ("cracked") originals as well as modified variants containing additional features.

Metasploit Pro

Official price at the time of this study: $15,000 per year

Modified version with year of technical support: $8,000–$15,000

Groups: APT35, Carbanak, Patchwork, Silence, TreasureHunter

After penetrating a company's infrastructure, financially motivated criminals try to quickly identify hosts of interest, such as any computers responsible for outgoing financial transactions. This could be a bank workstation used for interbank transfers or the computer of an accountant at a regular company. To identify these hosts, attackers use free utilities, such as nmap or nbtscan, or more convenient commercial programs (for example, Cobalt used SoftPerfect Network Scanner, which has an official price of $3,000). The sprawling networks of major organizations are complex and have a large number of servers and workstations, which forces criminals to acquire special tools for handling such networks.

After reaching the hosts of interest, criminals are faced with yet another task—to understand the workings of specialized banking software and how to initiate and confirm transactions. (Sometimes, of course, all of this is old news to the attackers.) Whereas bank workstations tend to work in predictable ways, non-financial companies may have to use multiple bank clients on the same machine in order to work with different banks. In these situations, hackers need special tools to observe the desktop of the infected computer, monitor the user's actions in real time, and take videos and screenshots, all while remaining invisible to the employee. They can use hVNC and modified versions of TeamViewer, RMS, Ammyy Admin, and others.

TeamViewer

Legitimate remote administration tool. A modified version is invisible to users and has several additional functions, including built-in keylogger

Price on the darkweb: $100

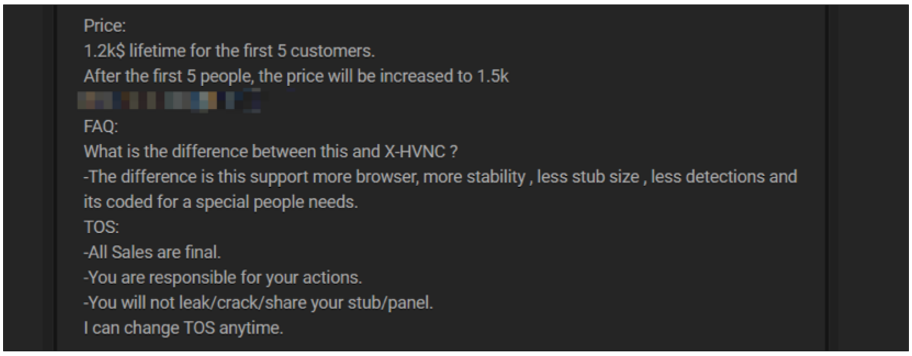
Groups: Carbanak, Cobalt

Hidden VNC

A modification of the legitimate VNC utility, allowing hackers to remotely connect to a user's workstation and stay invisible while executing commands

Price on the darkweb: $1,000 per month

Used by the Carbanak group



Price:
1.2k$ lifetime for the first 5 customers.
After the first 5 people, the price will be increased to 1.5k
[redacted]
FAQ:
What is the difference between this and X-HVNC ?
-The difference is this support more browser, more stability , less stub size , less detections and its coded for a special people needs.
TOS:
-All Sales are final.
-You are responsible for your actions.
-You will not leak/crack/share your stub/panel.
I can change TOS anytime.

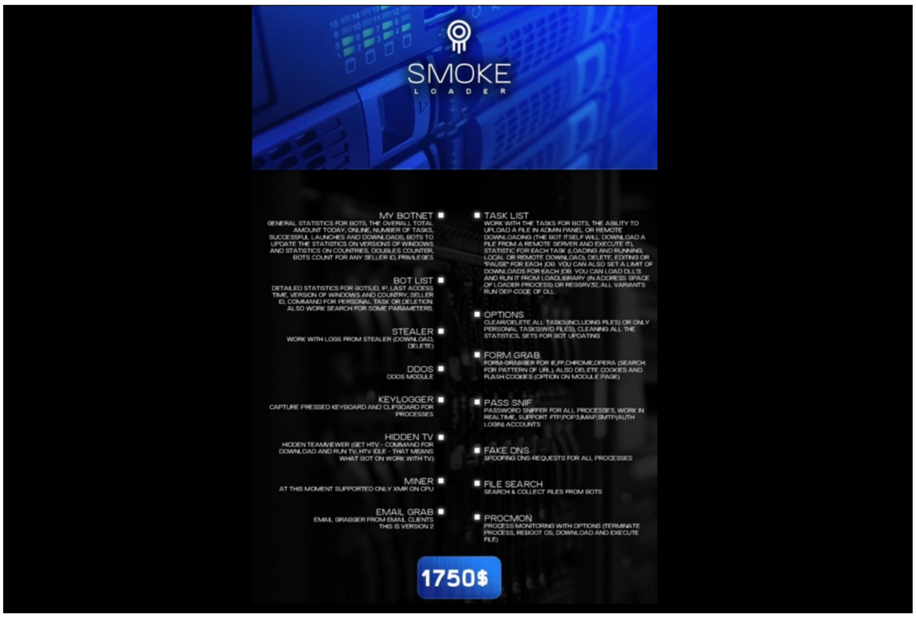
Figure 6. Hidden VNC for sale

$400+

cost of a ready-made banking bot, base configuration (downloading and execution of arbitrary files)

$1,750

cost of Smoke Bot banking malware with full set of modules



MY BOTNET
GENERAL STATISTICS FOR BOTS, THE OVERALL TOTAL AMOUNT TODAY, ONLINE, NUMBER OF TASKS, SUCCESSFUL LAUNCHES AND DOWNLOADS, BOTS TO UPDATE THE STATISTICS ON VERSIONS OF WINDOWS AND STATISTICS ON COUNTRIES, DOUBLES COUNTER, BOTS COUNT FOR ANY SELLER ID, PRIVILEGES

BOT LIST
DETAILED STATISTICS FOR BOTS,ID, IP, LAST ACCESS TIME, VERSION OF WINDOWS AND COUNTRY, SELLER ID, COMMAND FOR PERSONAL TASK OR DELETION. ALSO WORK SEARCH FOR SOME PARAMETERS.

STEALER
WORK WITH LOGS FROM STEALER (DOWNLOAD, DELETE)

DDOS
DDOS MODULE

KEYLOGGER
CAPTURE PRESSED KEYBOARD AND CLIPBOARD FOR PROCESSES

HIDDEN TV
HIDDEN TEAMVIEWER (GET HTV - COMMAND FOR DOWNLOAD AND RUN TV, HTV IDLE - THAT MEANS WHAT BOT ON WORK WITH TV)

MINER
AT THIS MOMENT SUPPORTED ONLY XMR ON CPU

EMAIL GRAB
EMAIL GRABBER FROM EMAIL CLIENTS THIS IS VERSION 2

TASK LIST
WORK WITH THE TASKS FOR BOTS, THE ABILITY TO UPLOAD A FILE IN ADMIN PANEL OR REMOTE DOWNLOADING (THE BOT ITSELF WILL DOWNLOAD A FILE FROM A REMOTE SERVER AND EXECUTE IT), STATISTIC FOR EACH TASK (LOADING AND RUNNING, LOCAL OR REMOTE DOWNLOAD), DELETE, EDITING OR "PAUSE" FOR EACH JOB. YOU CAN ALSO SET A LIMIT OF DOWNLOADS FOR EACH JOB. YOU CAN LOAD DLL'S AND RUN IT FROM LOADLIBRARY (IN ADDRESS SPACE OF LOADER PROCESS) OR REGSRV32, ALL VARIANTS RUN OEP CODE OF DLL

OPTIONS
CLEAR/DELETE ALL TASKS(INCLUDING FILES) OR ONLY PERSONAL TASKS(W/O FILES), CLEANING ALL THE STATISTICS, SETS FOR BOT UPDATING

FORM GRAB
FORM-GRABBER FOR IE,FF,CHROME,OPERA (SEARCH FOR PATTERN OF URL), ALSO DELETE COOKIES AND FLASH COOKIES (OPTION ON MODULE PAGE)

PASS SNIF
PASSWORD SNIFFER FOR ALL PROCESSES, WORK IN REALTIME, SUPPORT FTP,POP3,IMAP,SMTP(AUTH LOGIN) ACCOUNTS

FAKE DNS
SPOOFING DNS-REQUESTS FOR ALL PROCESSES

FILE SEARCH
SEARCH & COLLECT FILES FROM BOTS

PROCMON
PROCESS MONITORING WITH OPTIONS (TERMINATE PROCESS, REBOOT OS, DOWNLOAD AND EXECUTE FILE)

1750$

Figure 7. Smoke Bot banking malware for sale

Sysinternals Suite

Legitimate administration toolkit

Utilities most commonly used by attackers: PsExec, ProcDump, PsList, SDelete

Examples of groups:

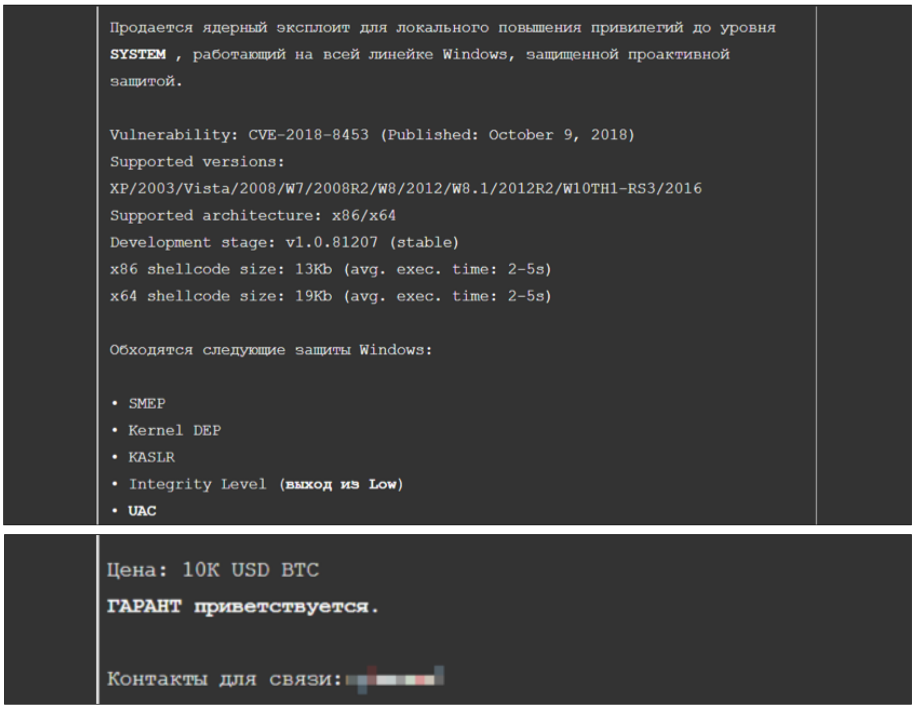
APT29, Leafminer, OilRig

Just like financially motivated criminals, cyberspies will try to entrench themselves in the system and identify key hosts after successfully penetrating the internal network. They are interested in workstations and servers that store and process valuable information, including trade secrets and intellectual property. They also target computers of top executives and other key persons, or perhaps servers that allow access to industrial control system (ICS) networks. Before collecting sensitive information, cyberspies study the business processes of the target company. In order not to attract attention or arouse suspicions, they prefer using legitimate administration tools. For example, 48 percent of studied APT groups use the free Sysinternals Suite from Microsoft.

The next important step is escalating OS privileges. On the darkweb, criminals can purchase exploits for escalating OS privileges by exploiting known or zero-day vulnerabilities.

$10,000

cost of exploit for escalating OS privileges



```
Продается ядерный эксплоит для локального повышения привилегий до уровня
SYSTEM , работающий на всей линейке Windows, защищенной проактивной
защитой.

Vulnerability: CVE-2018-8453 (Published: October 9, 2018)
Supported versions:
XP/2003/Vista/2008/W7/2008R2/W8/2012/W8.1/2012R2/W10TH1-RS3/2016
Supported architecture: x86/x64
Development stage: v1.0.81207 (stable)
x86 shellcode size: 13Kb (avg. exec. time: 2-5s)
x64 shellcode size: 19Kb (avg. exec. time: 2-5s)

Обходятся следующие защиты Windows:

• SMEP
• Kernel DEP
• KASLR
• Integrity Level (выход из Low)
• UAC
```

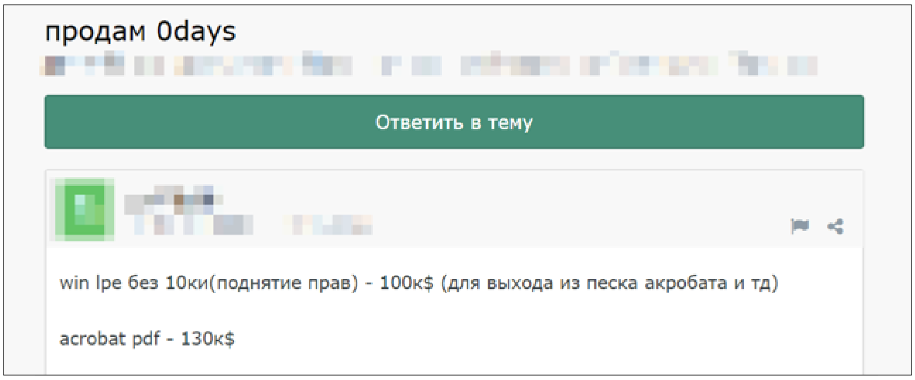
```
Цена: 10K USD BTC
ГАРАНТ приветствуется.

Контакты для связи:[redacted]
```

Figure 8. Privilege escalation exploits for sale

Exploiting zero-day vulnerabilities is a tried-and-true technique used by cyberespionage groups. In one such case, TEMP.Reaper exploited a zero-day vulnerability in Adobe Flash. The flaw, now catalogued under number CVE-2018-4878, has a publicly available exploit. Another zero-day vulnerability (CVE-2018-15982) in Adobe Flash was exploited in a cyberspy APT attack against a state-run outpatient clinic in Russia. It is difficult to estimate the cost of an exploit for an unknown vulnerability. However, the cost of an exploit for a zero-day vulnerability in Adobe Acrobat on the darkweb is rather high.

$130,000

cost of exploit for a zero-day vulnerability in Adobe Acrobat



продам 0days

win lpe без 10ки(поднятие прав) - 100к$ (для выхода из песка акробата и тд)

acrobat pdf - 130к$

Figure 9. Zero-day vulnerabilities for sale

$1.6 million

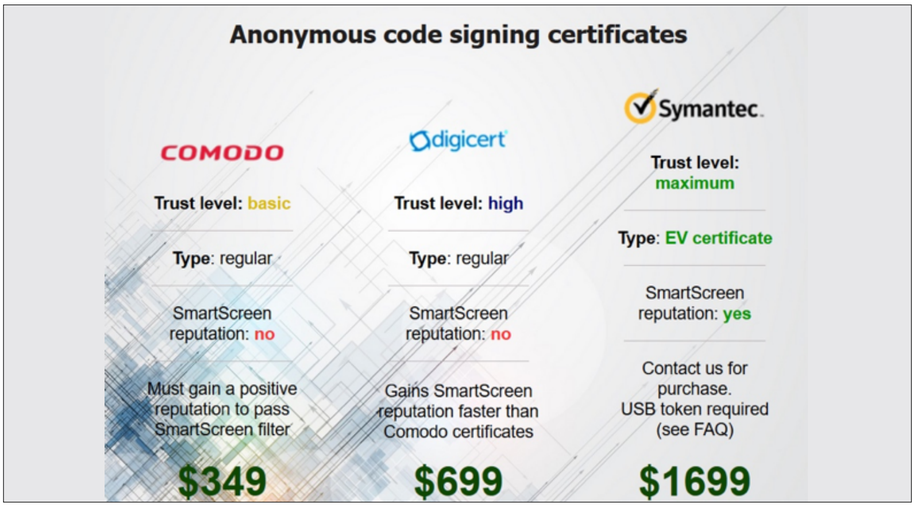
cost of the FinSpy spyware framework

Attackers can use zero-day vulnerabilities to deliver spyware Trojans. For example, one APT group used zero-day vulnerabilities in Adobe Flash Player (CVE-2017-11292) and Microsoft .NET Framework (CVE-2017-8759) to deliver FinSpy malware. Also known as FinFisher, the FinSpy framework is surveillance software able to spy on users through an infected computer's webcam and microphone, capture chat messages and emails, and steal passwords and other sensitive data. This Trojan is used by the SandCat APT group. Besides its considerable spying abilities, FinSpy employs a number of anti-analysis techniques, including code obfuscation and virtual machine detection. All this makes the work of defenders more difficult and explains why the malware costs a whopping €1.5 million.

Hackers use various techniques to bypass the protection mechanisms of network hosts. For example, they may sign malicious code with certificates in order to pass it off as legitimate. Ready-to-use certificates are also available on darkweb forums.

$1,700

cost of an extended validation (EV) code signing certificate



Anonymous code signing certificates

COMODO	digicert	Symantec.
Trust level: basic	Trust level: high	Trust level: maximum
Type: regular	Type: regular	Type: EV certificate
SmartScreen reputation: no	SmartScreen reputation: no	SmartScreen reputation: yes
Must gain a positive reputation to pass SmartScreen filter	Gains SmartScreen reputation faster than Comodo certificates	Contact us for purchase. USB token required (see FAQ)
$349	$699	$1699

Figure 10. Advertisement for signing of malware with legitimate certificates

When hackers need to access specially protected network segments, such as ICS networks, they may prefer self-developed tools. In one such case, in the TRITON attack against industrial companies, malicious actors used custom tools such as SecHack (for collecting credentials) and NetExec (for moving inside the network).

Tool sets for entrenchment and lateral movement may cost a financially motivated group from $30,000 to $35,000. These are, however, one-time expenses. Groups buy ready-made tool sets and then use them in many future attacks, significantly reducing the financial blow.

An exploit for a single zero-day vulnerability costs tens or even hundreds of thousands of dollars. High prices for exploits do not stop cyberspies. Besides buying exploits, cyberspies have the means to develop their own malware able to bypass antivirus software and detect when it is being run in a sandbox. All this complicates attacker detection and forces companies to use robust security tools and measures to protect sensitive information. Of course, protection will not be effective without around-the-clock monitoring by a skilled security operations center (SOC).

How much can an APT cost

Besides the software costs discussed already, hackers incur numerous other operational expenses: renting servers, buying domain names, hosting websites, and paying for VPN services, to name a few. Our estimate is that such expenses total approximately $1,000, which is well below the cost of attack tools. In this report, we will analyze the main expenses of cybercriminals and illustrate them with data for several actual APT attacks. Our conclusions are based on the cost of similar services and software on the darkweb.

Silence

$288,000
average damage from a successful attack

$55,000
cost of toolkit

In early 2019, we observed a resurgence of the financially motivated group Silence. Let's try to figure out how much an attack by this group could cost to perform. As mentioned already, a monthly subscription to a service for creating malicious attachments would typically cost $2,500. Silence uses the free Sysinternals Suite plus a number of self-developed tools, including the Silence framework, Atmosphere ATM theft toolkit, and a number of others. Incidentally, our research on the criminal cyberservices market showed that malware for ATMs is the most expensive class of ready-made malware on the darkweb, with prices averaging around $5,000. After thorough analysis of cyberservices offered on the darkweb, we come up with a ballpark figure of $55,000 for the starting price of a full set of tools for a financially motivated group like Silence.

In July 2018, hackers stole the equivalent of $930,000 from PIR Bank in Russia. How much money did the criminals invest in their attack? At the penetration stage, they sent phishing messages. In addition to self-developed malware, they actively used Metasploit Pro and Sysinternals Suite for movement inside the network. To spy on the bank's employees, they used their own tools and the legitimate NirCmd utility. We would put a price tag of at least $66,000 on this set of tools.

Attack on PIR Bank

$930,000
damage from attack

$66,000
cost of toolkit

Funds were stolen from PIR Bank via client cards at 22 banks; most of the stolen money was cashed out on the night of the attack itself. To withdraw money and cash out, criminals typically hire so-called money mules. The total cost of such services, including compensation to money mules and related expenses, is 15 to 50 percent of the total amount stolen. So in this case, the Silence organizers paid between $140,000 and $465,000 to obtain the stolen cash.

It is more difficult to evaluate the cost of a cyberespionage attack. Zero-day vulnerabilities may cost tens of thousands or even millions of dollars on the darkweb. What's more, hackers sometimes use self-developed malware, which is unique to each group. We do not know how such malware is developed in each particular case, nor how much time and effort it takes to create. Estimating the cost of development is therefore

APT38

$41,000,000
average damage from a successful attack

$500,000+
cost of an attack

extremely problematic. To put a lower bound on the cost, we took an advertisement for the cheapest custom malware development we could find on the darkweb.

FireEye experts investigated attacks conducted by APT38, another profit-driven group, and found they were similar to cyberespionage campaigns. The group's tools were the same as those used for cyberespionage by TEMP.Hermit. APT38 conducts watering hole attacks at the penetration stage and burrows into a victim network for an average of 155 days, which is atypically long for attacks aimed at stealing money. The group's arsenal contains 26 unique custom malware families. We estimate that the development cost of such tools exceeds $500,000.

Conclusions and recommendations

The tools used by hackers in APT attacks vary considerably depending on motivation. While the cost of attack tools for a financially motivated group is measured in the tens of thousands of dollars, for APT cyberespionage groups the figure is higher by an order of magnitude. At the same time, victims' losses are many times greater than the costs of APT groups. Just a few successful attacks are enough for the "investment" in purchasing or developing tools to pay off.

We recommend that financial organizations actively share information on cyberattacks and indicators of compromise at the industry level. Resources such as FS-ISAC significantly reduce the success rates of cyberattacks on financial institutions. It is also vital to quickly identify attack traces in infrastructure and constantly monitor the network for abnormal activity. This awareness enables detecting and investigating new unknown attacks, as well as sharing the results with the rest of the industry.

Today's cyberespionage groups tend to use self-developed malware and exploits for zero-day vulnerabilities. Such groups take the time to conduct reconnaissance and prepare unique tools to bypass the target's protection. They have particular targets in mind, and the smallest mistake may cause the entire operation to fail. In today's conditions, it is impossible to detect a cyberespionage attack at the stage of penetration into a local network, and very difficult to identify when it gains a foothold and spreads in the infrastructure. Worse still, the target infrastructure itself is often not conducive to detecting attacks.

Out-of-the-box protection solutions for individual servers or endpoints are hopelessly outclassed. Criminals long ago figured out how to bypass antivirus software, sandboxes, and intrusion detection systems (IDS). Companies need a sober understanding of the protection systems in place to secure their key assets. Solutions must be comprehensive, limiting criminals' space for maneuver and ensuring maximum coverage of security events in the context of system logs, traffic, and network objects. Full awareness of infrastructure events is a critical link in the threat hunting chain for detection of the actions of APT groups.

Deep analysis of network traffic, retrospective analysis of security events, user behavior profiling, and access to RAM, processes, and other forensic artifacts allow significantly reducing infrastructure dwell time, making it much harder for attackers to achieve their goals. Of course, no APT protection system can be effective without the support of skilled incident investigation experts.

Only by combining knowledge of modern techniques and tools, readiness to detect the most common industry-specific attack methods, and awareness of attacker objectives and motives can organizations build a truly effective protection system, anticipate and stay ahead of attackers, eliminate threats, and mitigate key risks.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

ptsecurity.com
info@ptsecurity.com