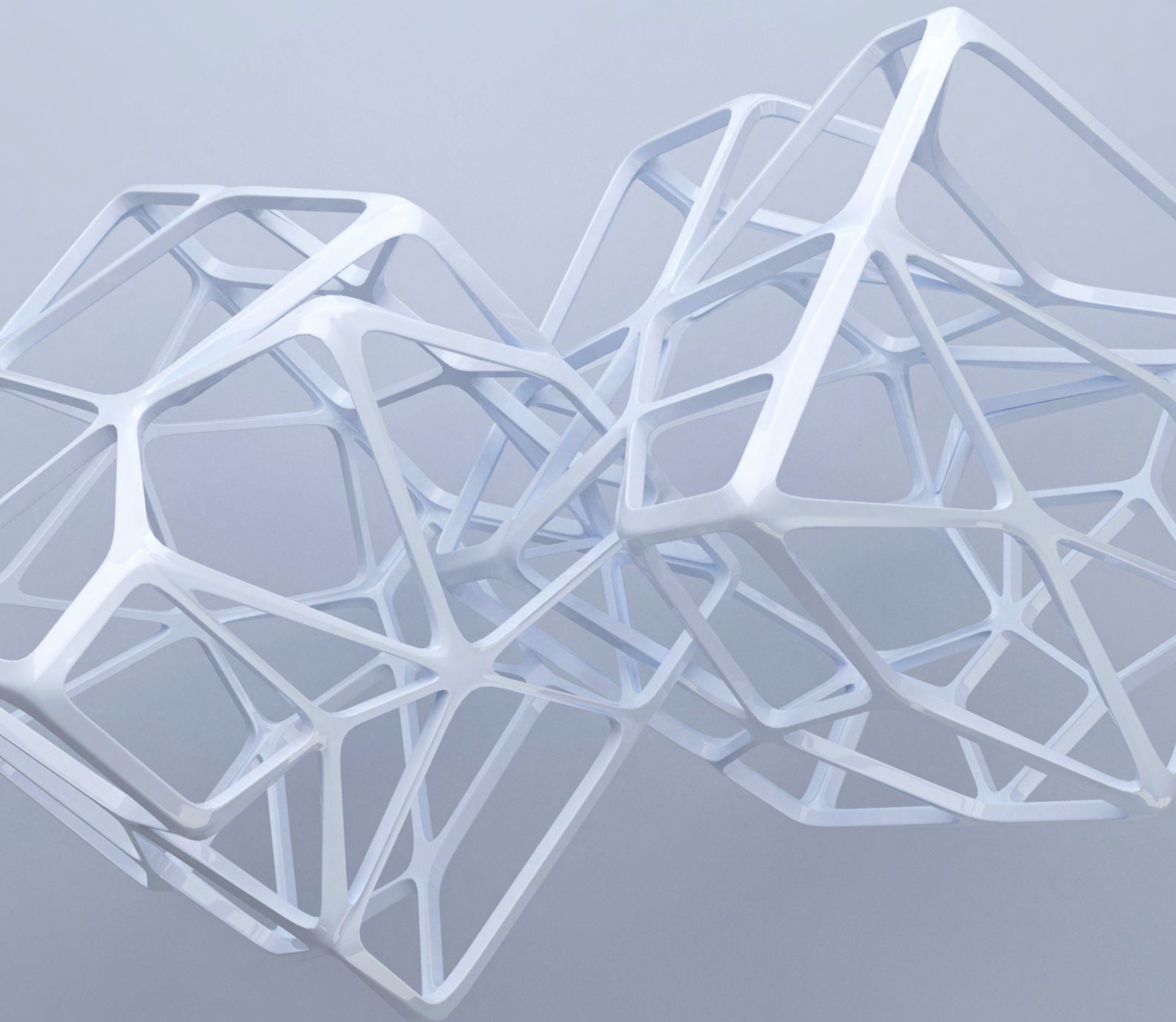


Rootkits: evolution and detection methods



Contents

Introduction	3
What is a rootkit?	4
Evolution of rootkits	5
Who is behind the attacks?	9
What the dark web offers	10
Methods of detection	13
The future of rootkits	14

Introduction

In this research, we will tell you how rootkits evolved, by whom and for what they are used now, how to detect them and predict their future



15 minutes
to read

Compared to other tools in the attacker's arsenal, rootkits are less common than other types of malware. For example, according to Bitdefender, rootkits account for less than 1% of the total malware detected. That said, all instances of detection are associated with high-profile attacks. These include, for instance, the cyberespionage campaign of the APT group Strider (also known as ProjectSauron, or G0041), in which the cybercriminals distributed the Remsec rootkit. The group collected information about encryption methods—in attacks on government agencies, attackers stole encryption keys, configuration files, and collected the IP addresses of encryption key infrastructure servers. Cybercriminals targeted organizations in Russia, Belgium, China, Iran, Sweden, and Rwanda.

Due to the complexity of development, rootkits are not used often, but they pose a threat because they can hide malicious activity on devices and make the timely detection of a compromise difficult. Rootkits are still successfully used in attacks, despite the introduction of protection against them in modern operating systems. In preparing this study, we analyzed the 16 most well-known rootkit families discovered by experts over the past 10 years. We will tell you how rootkits evolved, by whom and for what they are used now, how to detect them, and ultimately make a prediction whether attackers will persist in their usage in the future.

What is a rootkit?

A rootkit is a program (or set of programs) that allows you to hide the presence of malware in the system.

Rootkits are often part of multifunctional malware that could have multiple abilities, such as providing attackers with remote access to compromised hosts, intercepting network traffic, spying on users, recording keystrokes, stealing authentication information, or using the host as a base to mine cryptocurrencies and aid in DDoS attacks. The task of the rootkit is to mask this illegitimate activity on the compromised machine.

Types of rootkits by level of privileges obtained:

- **Kernel-mode rootkits.** Such rootkits have the same privileges as the operating system, operating at kernel level. They are designed as device drivers or loadable modules. Such rootkits are difficult to develop, because any errors in the source code can affect the stability of the system, which will be an immediate clue to the malware. These rootkits made up 38% of our sample.
- **User-mode rootkits.** They are easier to develop than kernel-mode rootkits, making them more commonly used in mass attacks, as the design requires less precision and knowledge. User-mode rootkits operate with the same privileges as most applications. They can intercept system calls and replace values returned by APIs and applications to gain control of the machine. The share of such rootkits was 31 percent.

Some rootkits, such as Necurs, Flame, and DirtyMoe, are designed to combine both modes of operation and thus work at both levels. They accounted for 31 percent of the sample.

Switching to user-mode rootkits is a trend often used by rootkit developers. For example, [Sophos researchers found](#) that developers of the ZeroAccess rootkit had completely switched to using this mode. In our opinion, such actions might be down to the following:

- As previously mentioned, a kernel-mode rootkit is difficult to develop and implement in a system unnoticed, so attackers might not have a sufficient level of competence and instead opt for an easier route.
- It takes a lot of time to develop or modify such a rootkit, and this can make working to time constraints difficult; you must be quick to exploit a vulnerability in a company's perimeter before it is noticed and security updates are installed, or another group takes advantage of it. That is why, attackers are used to acting quickly: it can take less than a day from the moment the exploit is identified to the first attempts to make use of it, and if a group does not have a reliable, ready-to-use tool, this time is clearly not enough to work on it.
- Any errors in the source code of a kernel-mode rootkit might cause irreparable changes to the OS, which will reveal the intrusion and allow the attack to be thwarted.

- In addition, there is no point over-complicating an attack if there is confidence that the defense system is ineffective. If a point of entry to the company is found, and intelligence has shown that the perimeter is weakly protected and there are significant flaws in the security system, it is irrational and excessive to use a kernel-level rootkit, which requires a lot of effort to develop and can lead to complications.

If rootkits, especially at the kernel level, are so difficult to develop, then who continues to use them and why? The answer is clear: those groups for which the result of the attack exceeds all the efforts spent organizing it, strategic groups that have sufficient technical qualifications and financial capabilities. These could be APT groups that extract information or carry out destructive actions in infrastructure in the interests of customers, regardless of cost, or financially motivated criminals who steal large sums of money, while covering the costs of preparation.

Evolution of rootkits



For chronology of rootkits appearance since 2011, see [page 8](#)

Rootkits were originally used in attacks on Unix systems to gain maximum privileges and execute commands as the root user, hence their name. But in 1999, the first rootkit designed for the Windows operating system appeared—NTRootkit. Later, rootkits also appeared that could be used in attacks on macOS.

The most famous use case of a rootkit in attacks is the 2010 campaign to spread the Stuxnet malware. Using Stuxnet, attackers secretly collected data and downloaded executable files to compromised nodes. An investigation revealed the involvement of both the intelligence services of the United States and Israel in the creation of this malware, and the main purpose of such collaboration was to halt the development of Iran's nuclear system and physically destroy its infrastructure.

In the last decade, cybercriminals seeking data have been the most likely to use rootkits. As part of one of the cyberespionage campaigns in the Middle East, attackers used [the Flame rootkit](#), which helped them track victims' network traffic, performed keylogger functions, and take screenshots.

Using rootkits, you can not only secretly extract information and gain remote access. Attackers may also use them for direct financial gain, such as to hide cryptomining modules, as in the case of the DirtyMoe rootkit. [According to Avast](#), in 2021, cybercriminals distributing this rootkit infected more than 100,000 computers, although in 2020 the number of victims did not exceed 10,000. The addition of a new module that facilitates distribution on Windows computers led to a sharp increase in the number of victims. The module scanned the Internet for computers with an open SMB port, and then bruteforced credentials for remote access.



Interesting fact

In the source code of the DirtyMoe rootkit driver, Avast specialists identified many errors, which might indicate that code fragments were borrowed from across the Internet. Malware modules are written in Delphi, which makes them easy to detect by antivirus tools, so DirtyMoe developers used VMProtect to obfuscate the source code.

There are cases of inadvertently creating rootkits, such as an incident that occurred in 2016 with the developers of Street Fighter V by Capcom. The company released an update that disabled kernel-level protection against third-party code execution (SMEP) and thus allowed attackers to gain remote access to players' computers. Attentive users aborted the installation of this update because system-level privileges were requested during the installation process.

The Moriya rootkit has been used in TunnelSnake's targeted cyberespionage campaign since at least 2018. The list of victims includes, among others, two diplomatic organizations in Southeast Asia and Africa. The main goal of the malware is to provide cybercriminals with remote access to the IT infrastructure of victims, as well as to make it possible to download and run further destructive code. The rootkit is focused on Windows machines and combines user mode and kernel mode. As an initial line of assault, the attackers took advantage of vulnerabilities on servers accessible from the Internet, presumably the CVE-2017-7269 vulnerability. The rootkit developers have utilized a mechanism to bypass the mandatory signature verification of drivers and the PatchGuard module. The latter technology, when trying to penetrate the core of the system, causes BSoD (Blue Screen of Death). To do this, they used a driver for the VirtualBox virtual machine. In addition, the rootkit does not initiate a connection to the command and control server, which helps to hide it.

Remsec (Cremes) rootkit is a modular malware used by the Strider group (ProjectSauron, G0041) for the purpose of cyberespionage. Attackers are interested in information about software that protects traffic using cryptographic methods. They carefully select victims, including government agencies, research centers, and telecommunications companies. Zero-day vulnerabilities are then used to penetrate the infrastructure. The Remsec rootkit runs in kernel mode and is focused on Windows. Its modules allow attackers to gain remote access, download malware, tap network traffic, record keystrokes on the keyboard, and transmit the received data to the attacker's server. Most of the modules are written in the Lua language. ESET researchers found that legitimate antivirus kernel-mode drivers were used to deploy the rootkit. It is noteworthy that Remsec does not intercept and hijack API calls or system operations in order to hide its activity in the system; instead, the malware developers simply needed elevated privileges to execute their code.

Not only the developers of security tools, but also OS manufacturers are actively fighting against rootkits. For example, the massive transition to Windows 10 affected already existing rootkits. This version of the OS provides for a whole range of measures to counter rootkits. This is discussed in more detail in section "What the dark web offers". However, cybercriminals also develop new technologies. For example, the relatively new Moriya rootkit already provides mechanisms for bypassing the security tools built into the OS—checking the mandatory signature of drivers and the PatchGuard module. The development of rootkits involves highly qualified specialists who understand the targeted operating system and who have knowledge and experience in reverse engineering and programming.



Previously, the task of rootkits was to get the maximum privileges on the system (either administrator or system privileges). Now they are more focused on avoiding the detection by security tools.

Using reverse engineering methods, malware developers identify operating system features that could allow the implementation of a rootkit. Despite all the difficulties associated with their creation, new rootkits appear regularly.

From the above, it follows that rootkits are extremely dangerous because:

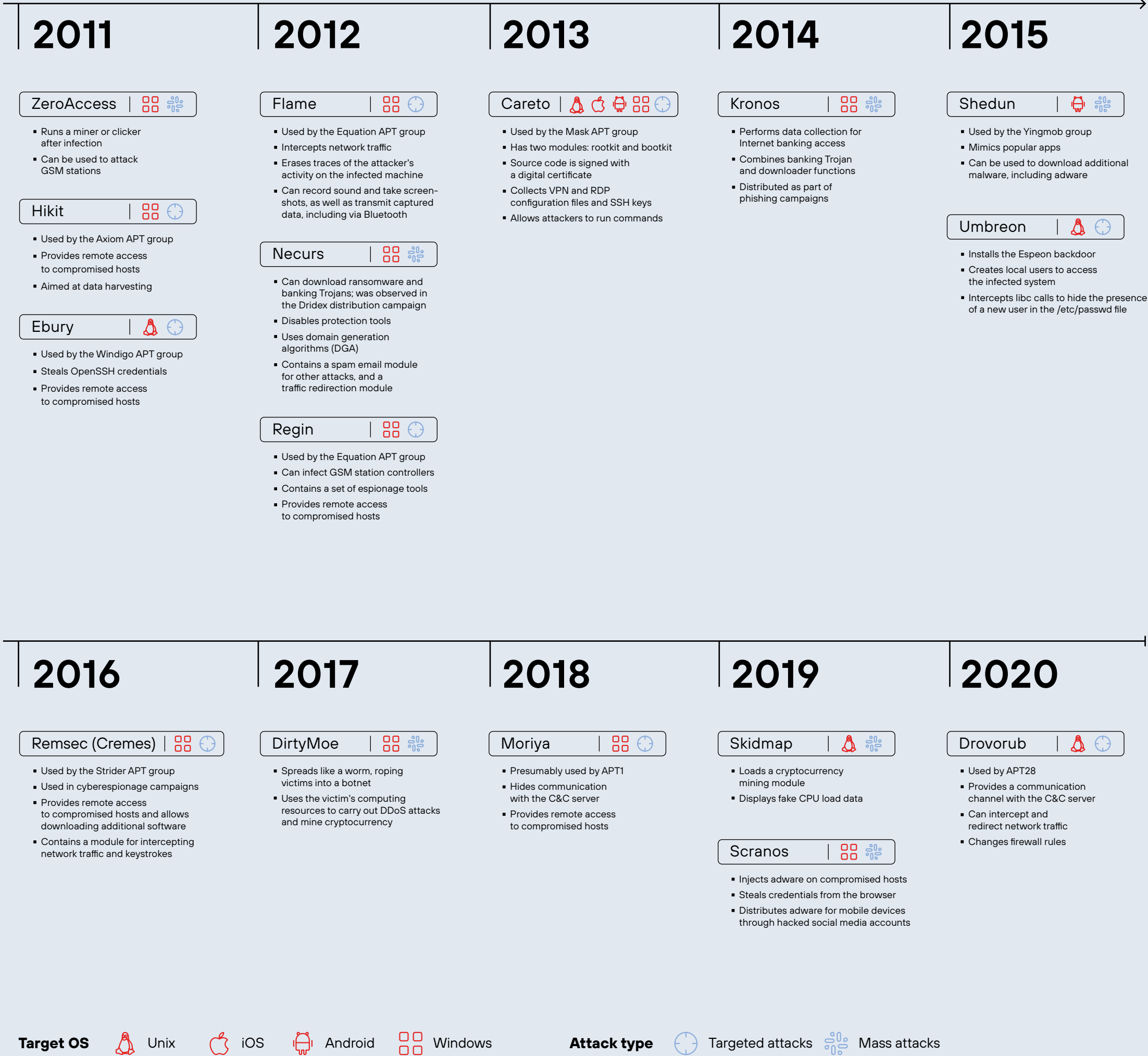
- They provide attackers with elevated privileges in the system.
- They make it much more difficult to detect malicious activity.
- They are difficult to detect and remove.
- Their presence often indicates a targeted attack by a well-prepared cyber-group, which means that while the attack is unnoticed, the company's infrastructure can be under the full control of the attackers.

In most cases, an attack leads not only to data compromise, but also to real financial damage, which is very difficult to assess for several reasons:

- The consequences of an attack involving highly skilled attackers can manifest themselves over a long period of time, especially if the attackers have been on the company's network for years.
- It is required to calculate all the costs of eliminating the consequences of the attack, and, in some cases, the rootkit cannot be removed and infected IT infrastructure hardware must be upgraded.
- If the attack was aimed at obtaining data, it is necessary to estimate in monetary terms the value of said stolen data and the damage that the company will suffer from such data being leaked.

ROOTKITS

chronology of appearance



Who is behind the attacks?

56%

of the investigated root-kits were used in targeted attacks

Given the full range of possibilities and the difficulties associated with the development of rootkits, they are most often used by APT groups. The main motive for attackers at this level is data acquisition and cyberespionage. For example, Equation Group actively used the Flame rootkit in their cyberespionage campaigns in the Middle East. Incidentally, among all the families of rootkits we studied, in 77 percent of cases, the attackers distributing them were aiming to obtain data. In about a third of the cases (31%), the criminals sought financial gain, such as Yingmob and TA505. Their attacks were massive and not industry-specific, with Yingmob targeting private individuals. The rarest motive, reported in only 15 percent of cases, is to infect and reuse the infrastructure of the victim company to carry out subsequent attacks.

By way of the main method of spreading rootkits (85% of cases), cybercriminals use social engineering methods, such as sending phishing messages, creating fake websites and applications that mimic legitimate sites. For example, the attackers distributing the Scranos rootkit targeted individuals, so they opted for hacked software and phishing mailings as distribution methods. This malware was particularly active in 2019. Victims of this campaign were found in China, India, Romania, France, Italy, Brazil, and Indonesia. The cybercriminals were motivated by financial gain and data acquisition. They were primarily interested in cookies and credentials for access to Internet banking and authentication for social networks and other resources of interest to criminals. The malware not only provided cybercriminals with remote access and the ability to collect data, but also injected a bootloader into the legitimate svchost.exe process. Most often, cybercriminals download adware, so to ascertain if you have been infected with this malware, analyze your activity on Facebook and similar social networks and on the video hosting site YouTube. If you find actions that you did not initiate, this is a sign that someone is controlling your account, and you should check the system for malware. Another interesting point: Scranos overwrites itself to disk before shutting down the computer and creates a key in the registry for startup.

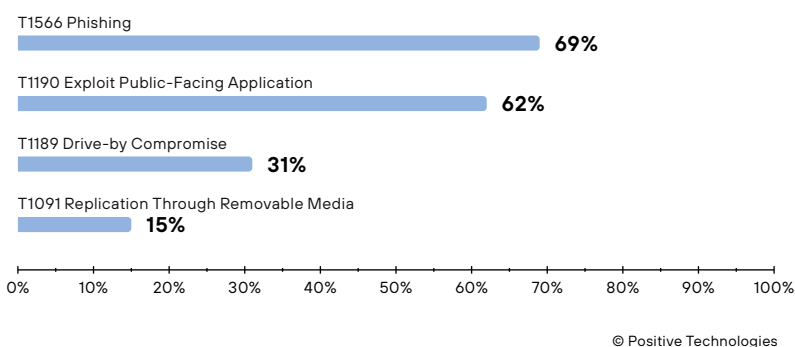
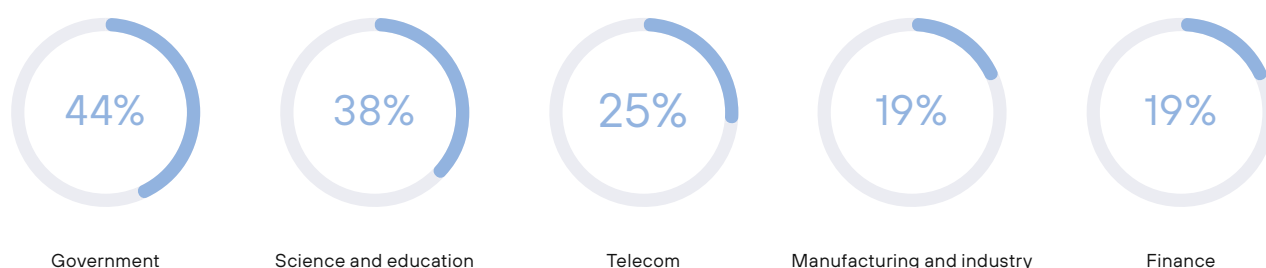


Figure 1. Rootkit distribution methods according to the MITRE ATT&CK classification (share of rootkits)

Top five most attacked industries (by share of rootkit attacks)

© Positive Technologies



An analysis of rootkit families showed that in 44 percent of cases cybercriminals used this malware to attack government agencies, while such attacks were slightly less common on scientific and educational institutions. This is primarily due to the key criminal motive, in that information processed by organizations from these industries is of great value to attackers.

19 percent of rootkits were used in attacks against financial institutions. One example of bank-targeted rootkits is [Kronos](#). Victims included banks in the UK and India.

More than half of rootkits (56%) are also used in attacks on individuals. These targeted hacks mostly consist of attacks against high-ranking officials, diplomats, or employees of organizations of interest to cybercriminals, as a component of larger cyberespionage campaigns.

What the dark web offers

Expert Bill Demirkapi at the Defcon conference in 2020 [joked](#) that it is very easy to write a high-quality rootkit for Windows; all you need is to know how to program in C or C++ and build projects, be able to develop exploits, do reverse engineering, and have a deep knowledge of the architecture of devices on the Windows platform. For a successful attack, you just need to find and use a vulnerable driver for your destructive objectives, then quietly inject and install the rootkit itself.

Rootkit development is a complex process, but there is a lot of information on the topic across the Internet, especially on the dark web. In addition to reference data, you can find both ready-made variants of malware "for any budget," as well as developers who will finish the code or the whole project, and even find "clients."

The average
cost of a rootkit
on the dark web is

\$ 2,800

We analyzed ten of the most popular Russian-language and English-language forums on the dark web, with offers to buy and sell rootkits, as well as advertisements seeking malware developers. Most of the advertisements for sale feature custom rootkits. The cost of a complete rootkit ranges from USD 45,000 to USD 100,000 and depends on the operating mode, target OS, conditions of use, and additional features.

For example, for USD 100-200, the buyer gets a rootkit for temporary use, meaning it can be used for, say, no more than a month.

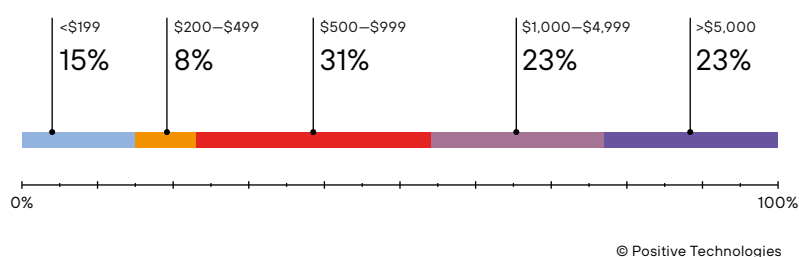


Figure 2. Ratio of cost of rootkits on sale

Rootkits without time limits are more expensive. For example, in 2014, the Kronos rootkit, which collects data for access to Internet banking, was sold for USD 7,000. Such rootkits are most often used in targeted attacks by APT groups.

In some cases, malware developers offer rootkit customization and provide service support.

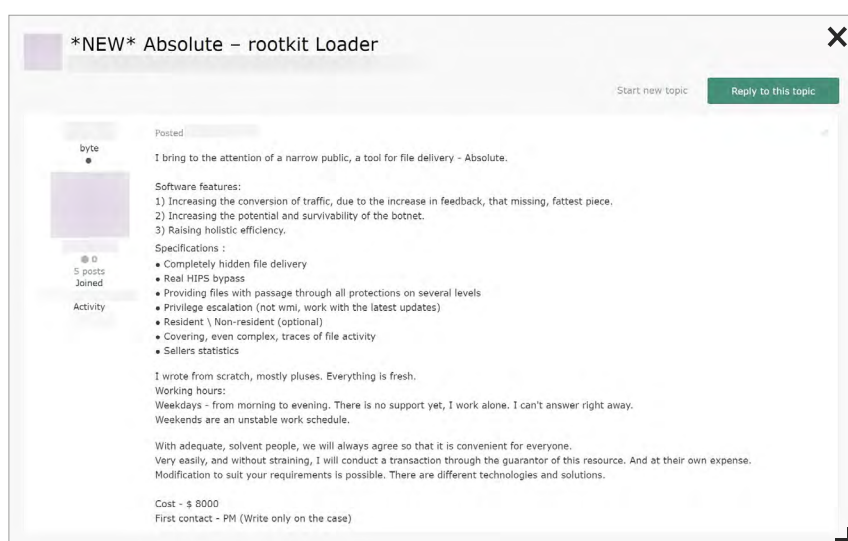


Figure 3. Announcement of the sale of a rootkit on a dark web forum

Rootkit purchase announcements generally ask for the following features: provision of remote access, hiding files, processes, and network activity.

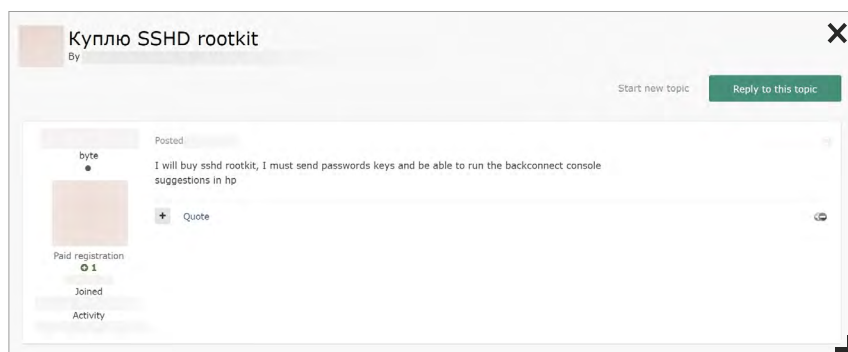


Figure 4. Announcement of the purchase of a rootkit on the dark web

In 67 percent of cases, the announcement included a requirement that the rootkit should be tailored for Windows, and in real attacks, Windows-based rootkits are also most often encountered: in the families we studied, their share was 69 percent. Note that some rootkits support multiple operating systems at once.

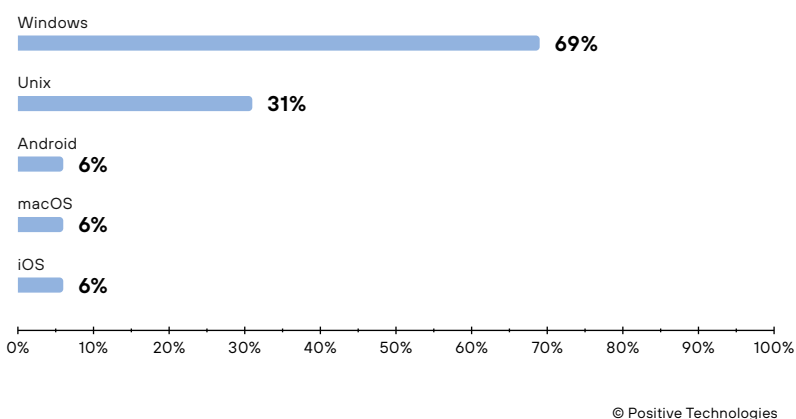


Figure 5. The share of OS-specific rootkits among the studied sample

In 2006, Windows developers, after assessing the damage caused by rootkits and the extent of their distribution, added the Kernel Patch Protection (KPP) component to the new version of Windows Vista. This module obligated hardware and software vendors to digitally sign their drivers. Later, cybercriminals managed to bypass this check, so a number of features were provided in Windows 10 that are designed to prevent rootkits from starting by checking drivers, component integrity, configuring reliable bootloaders, as well as recording and evaluating the boot process. Nevertheless, these innovations also do not guarantee protection.

Methods of detection

To detect a rootkit in the system, specialists resort to signature and behavioral analysis of the system, as well as checking its integrity. According to the European Agency for Network and Information Security (ENISA), in most cases a rootkit can only be removed by performing a clean installation on a compromised system.

To detect a rootkit, you can:

- Check the integrity of the system.
- Analyze network traffic for anomalies.
- Use a rootkit scanner.
- Use tools for detecting malicious activity on end nodes, which will help to detect a rootkit at the stage of its installation.
- Use sandbox solutions for rootkit detection at the installation stage and during operation.

The sandbox will help identify a rootkit at the stage of its installation in the system, since at this time the attacker performs a number of malicious or at least suspicious actions. Agentless sandboxes do not prevent the rootkit from loading, and built-in analyzers alert you of a potentially dangerous third-party load. Since the malicious process runs without interruption, and the checks for any presence of protection tools do not detect the sandbox, the attacker does not have any suspicions that they have already been detected. Incidentally, PT ESC experts will release a detailed study in October 2021, when you can learn in more detail about all the techniques for detecting rootkits using the sandbox.

In order to minimize the possibility of rootkit infections, you should monitor and install security updates regularly, install programs only from trusted sources and check digital signatures and certificates before installation, and regularly update the signatures of antivirus tools, because they are able to detect most of the "old" rootkits.

The future of rootkits

We believe that rootkits will not disappear from cybercriminals' toolkits any time soon. PT ESC specialists note the emergence of new versions of rootkits, whose mechanism of operation differs from the already known malware, and this indicates that attackers are not standing still and instead are inventing new techniques to bypass protection. The advantages of using rootkits—executing code in privileged mode, being able to hide from security tools, and being online for long periods of time—are too important for criminals to reject such a tool. At the same time, rootkits will continue to be used primarily by highly qualified groups that have the skills to develop such a tool, as well as groups that have sufficient financial resources to buy rootkits on the dark web. This means that the main danger of rootkits will be to conceal complex targeted attacks right up until an actual assault or set of events that will be most damaging for the target organization.



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

For 19 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](#).