









Advanced threat predictions for 2025

Igor Kuznetsov :: 11/25/2024

Authors

-  [Igor Kuznetsov](#)
-  [Giampaolo Dedola](#)
-  [Georgy Kucherin](#)
-  [Maher Yamout](#)
-  [Vasily Berdnikov](#)
-  [Isabel Manjarrez](#)
-  [Ilya Savelyev](#)
-  [Joao Godinho](#)

We at Kaspersky's Global Research and Analysis Team monitor over 900 APT (advanced persistent threat) groups and operations. At the end of each year, we take a step back to assess the most complex and sophisticated attacks that have shaped the threat landscape. These insights enable us to anticipate emerging trends and build a clearer picture of what the APT landscape may look like in the year ahead.

In this article in the KSB series, we review the trends of the past year, reflect on the [predictions we made for 2024](#), and offer insights into what we can expect in 2025.

Review of last year's predictions

The rise of creative exploits for mobile, wearables and smart devices

Our discovery of [Operation Triangulation](#) last year shed light on a unique attack chain involving exploits for Apple devices, including those operating on iOS and watchOS. These exploits were leveraging multiple vulnerabilities involving components such as WebKit and the XNU kernel, as well as the Apple processor.

As expected, we continued to observe attacks in 2024 involving exploits for Apple devices. For instance, in January, Apple shared that [CVE-2024-23222](#), a remote code execution vulnerability in Safari's browsing engine, may have been used in cyberattacks. In addition, this fall, Apple disclosed [two more exploits](#) that have most likely been used in the wild: CVE-2024-23225 for the XNU kernel and CVE-2024-23296 for RTKit.

As for Android devices, they also remain lucrative targets for sophisticated threat actors. In November, Google published information on two vulnerabilities that “may be under limited, targeted exploitation”: [CVE-2024-43093](#) and [CVE-2024-43047](#). Interestingly, the latter, just like one of the exploits used in Operation Triangulation, leverages a flaw involving a hardware processor. As we can see, targeted threat actors are becoming more and more interested in exploiting vulnerabilities involving hardware components of mobile devices.

Verdict: prediction fulfilled ✓

Building new botnets with consumer and corporate software and appliances

The international cybersecurity community has begun to put significant efforts into disrupting command and control servers, making it more difficult for threat actors, including advanced ones, to conduct malicious activities from their infrastructure over prolonged periods. To counter the efforts of these researchers, several advanced threat actors recently began building their own botnets and using them to launch cyberattacks.

For example, in January of this year, the US government [disrupted a botnet](#) composed of compromised Ubiquiti Edge OS routers operated by the Sofacy (aka APT28) threat actor. The devices were initially infected with Moobot, a Mirai-based malware, which was then used to deploy additional scripts and facilitate targeted attacks against various entities, collect credentials, proxy network traffic, establish reverse SSH tunnels, host spoofed landing pages, and control other remote systems infected with a Python backdoor.

Additionally, in 2024, we observed multiple Chinese-speaking actors using botnets to conduct targeted attacks. One of these botnets was [Quad7](#), which was installed on compromised routers by the [Storm-0940 actor](#) to conduct password spraying. Another example seen this year was [KV-Botnet](#), which was deployed on vulnerable firewalls, routers and IP cameras and used to conceal the malicious activities of Volt Typhoon, the actor behind it.

Verdict: prediction fulfilled ✓

Barriers to kernel-level code execution increasingly evaded (kernel rootkits hot again)

Whenever a threat actor successfully breaks into a machine, they always want to escalate their privileges as much as possible. Specifically, one privilege targeted actors often want to achieve is access to the kernel. This allows adversaries to disable or tamper with security solutions, as well as install rootkit implants to stealthily carry out malicious activities.

In 2024, BYOVD (bring your own vulnerable driver) has remained the most popular technique for gaining access to the kernel, and is even more widely used than in previous years. For instance, in Q2 2024, we saw a 23% [increase in BYOVD usage](#). This increase is most likely due to the fact that there are currently no effective methods built into operating systems to combat this technique. While Windows implements a blocklist of vulnerable drivers, it is rarely updated (only 1-2 times per year), making it extremely easy for actors to exploit known vulnerable drivers.

However, some security solutions are attempting to implement mechanisms to prevent the exploitation of vulnerable drivers, forcing threat actors to adapt by finding vulnerabilities in Windows drivers already installed on the device that can be used to perform kernel space escalations. For example, this year [Lazarus exploited CVE-2024-21338](#), a vulnerability in the AppLocker driver, to deploy the FudModule rootkit.

Verdict: prediction fulfilled ✓

Growth in cyberattacks by state-sponsored actors

Year after year, we're seeing more and more attacks by sophisticated threat actors, and 2024 was no exception. For instance, this year we [reported](#) a 25% rise in APT attack detections observed from January to June. Throughout the year, we've covered the most interesting of these attacks [on our blog](#).

Notably, we also observed sophisticated actors increase not only the quantity, but also the quality of their campaigns. This is particularly notable in the case of Lazarus APT, specifically its [attacks against cryptocurrency investors](#) in May.

These attacks were extremely carefully orchestrated – to conduct them, Lazarus stole the source code of a cryptocurrency-related computer game, promoted social media accounts related to that game, and obtained access to a unique chain of zero-day exploits used to infect targets visiting the game website. All these activities must have taken months of work on the part of this actor, indicating an exceptional level of organizational effort.

Verdict: prediction fulfilled ✓

Hacktivism in cyber-warfare: the new normal in geopolitical conflicts

As we previously predicted, we observed an increase in attacks by hacktivist groups this year, specifically those operating in the context of the Russo-Ukrainian and Israeli-Hamas conflicts. In the case of the Russo-Ukrainian conflict, notable hacktivist groups we reported on included [Twelve](#), [Head Mare](#) and [Crypt Ghouls](#). In general, we've observed hacktivists in the Russo-Ukrainian conflict become more skilled and more focused on attacking large organizations such as government, manufacturing and energy entities. By focusing on these targets, hacktivist groups make the consequences of their attacks more visible to ordinary people.

We have also observed the same pattern of activity from hacktivists operating in the Israel-Hamas conflict. For instance, one recent attack observed in this area was a [DDoS attack](#) targeting Israel's credit card payment system. What is particularly interesting about the cyberattacks in this conflict is that their target range has expanded far beyond the conflict area. This year, for example, the pro-Palestinian hacktivist group BlackMeta attacked the Internet Archive website, which has nothing to do with the conflict.

Verdict: prediction fulfilled ✓

Supply chain attacks as a service: operators bulk-buying access

This year, we haven't seen any supply chain attacks that caused significant damage to their targets. However, one especially notable supply chain attack in 2024 was the XZ Utils backdoor, which we covered in a three-part [blog post](#). Given that the backdoor affected multiple popular Linux distributions, the consequences of this attack would have been much worse had it not been spotted by the community. We might have seen access to networks of compromised companies being sold to advanced actors.

Verdict: prediction not fulfilled ❌

Spear-phishing to expand with accessible generative AI

Ever since the emergence of generative AI, multiple threat actors – both financially motivated and state-sponsored – have started using this technology to make their attacks more effective. This is especially true for phishing attacks, as generative AI tools are now capable of composing well-written, illustrated phishing emails.

One notable case of AI being used in a targeted campaign was the [unsuccessful attack on the company KnowBe4](#), where a hacker, allegedly from the Lazarus threat group, used AI to trick the company's HR department when applying for a job. For example, as part of the job application, they used a stock photo manipulated with AI tools to make it more credible. With the help of AI, they were able to trick the company, get the job and gain access to the internal network; however, further hacking attempts were quickly spotted by the company's SOC.

Verdict: prediction fulfilled ✔️

Emergence of more groups offering hack-for-hire services

While we've seen new hack-for-hire groups emerge in the crimeware world, we haven't observed any new notable commercially motivated threat actors carrying out sophisticated cyberattacks similar to those commonly conducted by APTs.

Verdict: prediction not fulfilled ❌

MFT systems at the forefront of cyberthreats

Last year, incidents involving MFT systems such as MOVEit and GoAnywhere caused serious damage to compromised organizations. Although these attacks took place a year ago, their impact on the affected companies is still being felt today. For instance, several days ago, personal data related to Amazon employees that was allegedly leaked over the course of the MOVEit vulnerability attack was [leaked](#) on a cybercrime forum.

This year the cybersecurity community has also discovered several vulnerabilities in MFT systems that are being exploited in the wild. One of them is CVE-2024-0204, which allows attackers to bypass authentication in the GoAnywhere MFT. Another example is CVE-2024-5806, a similar vulnerability in MOVEit Transfer. However, this year the cybersecurity community was much better prepared to counter attacks on MFT systems, so the consequences of attacks involving these vulnerabilities have not been as drastic as last year.

Verdict: prediction partially fulfilled 

APT predictions for 2025

Hacktivist alliances to escalate in 2025

In recent years, hacktivist groups have begun to closely link their operations to socio-political conflicts. While their early efforts were primarily focused on generating public attention, we're now seeing them pursue more substantial objectives with real-world impact, such as [targeting GNSS systems](#).

This year, we've watched hacktivism evolve, with groups forming alliances and forums with common motivations. These alliances are not limited to military conflicts – for example, the formation of the “Holy League,” which [claims](#) to unite 70 active hacker groups. Hacktivist alliances also emerge in response to fast-moving events, such as when hacktivists [united](#) to deface French websites in response to the arrest of Telegram CEO, Pavel Durov.

While a common goal can unite and motivate malicious acts, the sharing of tools and infrastructure is also an important part of such alliances, allowing even more ambitious goals to be achieved.

Hacktivism has grown stronger with this strategy, so we can expect to see more organized and impactful campaigns in the future, possibly even including the deployment of ransomware. In some cases, hacktivist attacks may reveal a lack of funding for the security of the structures they attack.

The IoT to become a growing attack vector for APTs in 2025

The rapid proliferation of IoT devices, predicted to [grow](#) from 18 billion today to 32 billion by 2030, brings both innovation and increased security challenges. As smart devices such as cameras, switches, and plugs become more common, they add countless new connections to the internet, each with its own potential vulnerabilities.

Many IoT devices rely on remote servers for control, but the security practices of the companies managing these servers are often unclear, resulting in new potential attack vectors on their infrastructure. Additionally, IoT devices frequently run on embedded systems with firmware that can be easily analyzed for vulnerabilities. Many older devices rely on outdated libraries with known security gaps, making them susceptible to exploitation.

The surge in mobile applications for controlling these devices adds another layer of risk. With so many apps available, it's difficult to verify the legitimacy of every single one, creating opportunities for attackers to spread fake apps to gain control of IoT devices. Supply chain risks also pose concerns; malicious actors can implant malware during the manufacturing process, as seen in [some Android TV boxes](#).

The main problem is the absence of countermeasures. Defenders are almost blind, with no visibility on these devices. Compared to last year, the situation has not improved, and we can only expect that attackers will continue to take advantage of the vast number of unprotected devices.

Increasing supply chain attacks on open-source projects

One notorious campaign this year was the [backdooring of XZ](#), a widely used open source compression tool in popular Linux distributions. The attackers employed social engineering techniques to gain persistent access to the software development environment and remained undetected for years. This

case highlights some critical aspects of the current open source ecosystem, where many significant projects are maintained by just a handful of developers – or sometimes even a single developer – who are often unable to defend against sophisticated state-sponsored APT groups.

The XZ case was nothing unexpected, but it sheds light on a real problem. It caught the attention of the cybersecurity community and various other organizations, who will likely start to improve the monitoring of open source projects. While we may not see an increase in the number of supply chain attacks, we will definitely see an increase in the number of discoveries of supply chain attacks currently underway.

C++ and Go malware to adapt to the open-source ecosystem

As open source projects increasingly adopt the latest versions of C++ and Go, threat actors will need to adapt their malware to these widely used languages. In 2025, we can expect a significant rise in APT groups and cybercriminals migrating to these languages, capitalizing on their growing prevalence in open source projects.

While other programming languages will continue to be used less frequently, C++ and Go will become the most common for malware development as attackers exploit the strengths and vulnerabilities of these languages to infiltrate systems and bypass security defenses.

Broadening the use of AI in the hands of state-affiliated actors

Last year, we predicted that APT groups would use AI to enhance spear-phishing attacks. OpenAI has since [reported](#) terminating accounts linked to state-affiliated threat actors, highlighting how APT groups are already using large language models (LLMs) for spear-phishing, text translation, script generation, and open-source research to create more targeted content. Our latest [discovery](#) showed that Lazarus leveraged AI-generated images to promote a fake gaming site that exploited a Chrome zero-day vulnerability to steal cryptocurrency.

We believe the use of LLMs will become a standard practice for attackers, much in the same way defenders have increasingly incorporated AI and machine learning tools into their cybersecurity strategies. Attackers will likely use LLMs for reconnaissance – LLMs can automate the process of identifying vulnerabilities and gathering information about specific technologies, making it easier for attackers to find weak points in their targets. They will rely more on AI when creating malicious scripts and generating commands during post-exploitation activities to increase their chances of success.

It's also likely that attackers will attempt to hide their activities from companies like OpenAI by creating local LLMs or masking their behavior on public platforms – using multiple accounts, being cautious with their inputs, and minimizing the data shared with corporate platforms like Google, OpenAI, Microsoft, and so on.

Deepfakes will be used by APT groups

Special attention must be given to the rise of deepfakes, which are rapidly evolving and pose significant risks. In the past, we've generally trusted videos, images and voices as reliable sources of information. However, as deepfake technology improves and becomes more accessible, that trust is increasingly being challenged. In 2024, deepfakes were used in high-profile scams, such as when a CEO's voice [was](#)

mimicked and used together with YouTube footage in video calls to trick employees, or when various publicly available videos and other footage were used to create a new fake video to trick an employee of a Hong Kong company into transferring approximately \$25.5 million.

The reason these attacks are so effective is rooted in human psychology: when people hear a voice they recognize, they instinctively trust the message. In the past, voice impersonation wasn't considered a major threat, which is why such scams can be so convincing. However, the advent of AI technologies has completely changed this paradigm. Today, new services mean deepfake videos and voice recordings can be generated from just a few real samples, easily collected from social media profiles or through other reconnaissance methods.

While we have seen AI voice cloning used by cybercriminals for scams, we expect APTs to increasingly incorporate this technology into their toolkit to impersonate key individuals, creating highly convincing messages or videos to deceive employees, steal sensitive information, or carry out other malicious activities.

Backdoored AI models

The widespread adoption of AI models by businesses across various industries makes these models an increasingly attractive target for cybercriminals and state-sponsored threat actors. The broad distribution of open-source and fine-tuned AI models heightens the risk of these models being trojanized or backdoored.

In 2025, we will most likely see APT groups targeting popular open-source AI models and datasets, introducing malicious code or biases that could be difficult to detect and widely shared.

The rise of BYOVD (bring your own vulnerable driver) exploits in APT campaigns

As we've already mentioned, the BYOVD (bring your own vulnerable driver) technique has become a trend in 2024. This technique allows attackers to leverage vulnerabilities in drivers to escalate privileges, bypass security measures, and deploy sophisticated payloads in both ransomware campaigns and APT attacks.

Drivers play a critical role in the communication between hardware and software, but they can also serve as a powerful gateway for attackers, especially when exploited at the kernel level. Vulnerable drivers allow attackers to execute malicious code with high levels of privilege, potentially leading to long-term espionage, data theft, and network infiltration. Although some security vendors implement various mechanisms to prevent such attacks, their sophistication is difficult to counter with traditional security measures. These drivers are legitimate software that may be necessary to facilitate normal system functionality, making it tricky to distinguish their legitimate use from malicious use. It's also no easy task to ensure that they are used solely for legitimate purposes.

Looking ahead, this trend is expected to continue into 2025. As attackers become more adept at leveraging low-level vulnerabilities, the complexity of such attacks is likely to increase, and we may see even more refined techniques, such as exploiting outdated or third-party drivers that are not typically scrutinized for security flaws.

