Advanced threat predictions for 2024

By GReAT

Published: 2023-11-14 · Archived: 2026-04-05 18:53:42 UTC

Advanced persistent threats (APTs) are the most dangerous threats, as they employ complex tools and techniques, and often are highly targeted and hard to detect. Amid the global crisis and escalating geopolitical confrontations, these sophisticated cyberattacks are even more dangerous, as there is often more at stake.

At Kaspersky's Global Research and Analysis Team (GReAT), we monitor a number of APT groups, analyze trends and try to anticipate their future developments to keep ahead of the evolving threat landscape and keep our customers safe. In this article, we will review the past year's trends to see which of our 2023 predictions have come true, and try to predict what is to come in 2024.

A review of last year's predictions

1. The rise of destructive attacks

In December of last year, shortly after we released our predictions for 2023, Russian government agencies were reported to have been targeted by a data wiper called CryWiper. The malware posed as ransomware, demanding money from the victims for "decrypting" their data. However, instead of encrypting the data, it purposefully destroyed it in the affected systems.

In January, ESET discovered a new wiper, deployed in an attack in Ukraine via the Active Directory GPO. They attribute the wiper, named SwiftSlicer, to Sandworm (aka Hades).

In June, Microsoft published a report on a threat actor named Cadet Blizzard, responsible for WhisperGate and other wipers targeting Ukrainian government agencies early in 2022. In addition to government agencies, law enforcement, IT services and emergency services in Ukraine, the threat actor has also targeted organizations in Europe, Central Asia and Latin America.

To sum up, although we did not see the same volume as we had in 2022, clearly there were some significant attacks.

Verdict: partially fulfilled 🆗

2. Mail servers become priority targets

In June, Recorded Future warned that BlueDelta (aka Sofacy, APT28, Fancy Bear and Sednit) exploited vulnerabilities in Roundcube Webmail to hack multiple organizations including government institutions and military entities involved in aviation infrastructure. The threat actor used news about the Russo-Ukrainian conflict to trick targets into opening harmful emails that exploited the vulnerabilities (CVE-2020-35730, CVE-2020-12641

and CVE-2021-44026). Using a malicious script, the attackers redirected their targets' incoming email to an email address controlled by the attackers, gathering data from the compromised accounts.

In July, we reported an updated variant of Owowa used against targets in Russia. We were able to associate the deployment of Owowa with a mail-based intrusion chain that looked like known CloudAtlas activities in a campaign we call GOFFEE.

In August, TeamT5 and Mandiant, following up on earlier research into exploitation of a remote command injection vulnerability affecting the Barracuda Email Security Gateway (ESG) appliance (CVE-2023-2868) by UNC4841, provided further detail on TTPs used by the threat actor. UNC4841 deployed new malware designed to maintain presence on a small subset of high-priority targets compromised either before the patch was released or shortly afterwards. This includes use of the SKIPJACK and DEPTHCHARGE backdoors and the FOXTROT/FOXGLOVE launcher. The threat actor targeted a wide variety of verticals. The US Cybersecurity and Infrastructure Security Agency (CISA) provided additional IoCs associated with exploitation of CVE-2023-2868.

Verdict: prediction fulfilled ✅

3. The next WannaCry

Fortunately for us, a new cyber epidemic did not happen.

Verdict: prediction not fulfilled ❌

4. APT targeting turns toward satellite technologies, producers and operators

The only known case of an attack utilizing satellite technologies that happened in recent years was the KA-SAT network hack of 2022. We have not seen anything of the kind in 2023.

Verdict: prediction not fulfilled ❌

5. Hack-and-leak is the new black (and bleak)

In April, we reported KelvinSecurity, a hacktivist and black hat Spanish-speaking group. The group's motivations are socio-political and monetary but inconsistent. Attacks are directed at public or private organizations around the globe. Leaks are often sold on the dark web, message groups or the group's own platforms, and some are given away for free.

In May, Ars Technica reported that BootGuard private keys had been stolen following a ransomware attack on Micro-Star International (MSI) in March this year (firmware on PCs with Intel chips and BootGuard enabled will only run if it is digitally signed using the appropriate keys). If an attacker is able to obtain these private keys, they could sign their malware, so that the code is trusted and run by MSI computers.

In August, Insikt Group, a Recorded Future threat research division, reported BlueCharlie (formerly tracked as TAG-53, also known as Blue Callisto, Callisto (or Calisto), COLDRIVER, Star Blizzard (formerly SEABORGIUM) and TA446) linked by researchers to 94 new domains, starting in March this year, suggesting

that the group is actively modifying its infrastructure in response to public disclosures about its activities. The threat actor focuses on information gathering for espionage and hack-and-leak operations, targeting organizations in various industries, such as government, higher education, defense, and political sectors, non-governmental organizations (NGOs), activists, journalists, think-tanks and national laboratories.

Verdict: prediction fulfilled ✅

6. More APT groups will move from Cobalt Strike to other alternatives

We are closely monitoring similar tools, one of which is BruteRatel, but Cobalt Strike is still used as the go-to framework for attacks.

Verdict: prediction not fulfilled ❌

7. SIGINT-delivered malware

In September, the Citizen Lab released a report concerning the prominent Egyptian opposition figure Ahmed Eltantawy. This politician became the target of a previously undiscovered “zero-day” attack aimed at infecting his phone with spyware.

During the months of August and September, the Citizen Lab reported that Eltantawy experienced a more perilous form of network injection attacks, which did not require any action on his part, such as clicking anything.

The Citizen Lab’s report conducted an examination to ascertain the precise location of the injection within the network. It determined that the injection point was situated within the connection between two Egyptian telecommunication providers. By relying solely on technical data, the lab could not ascertain which connection side the middlebox was positioned on. Nonetheless, the Citizen Lab researchers suspected that the attack likely involved integration with one of the providers’ subscriber databases.

According to the Citizen Lab, executing the attack on Eltantawy would have necessitated the installation of the PacketLogic system on the network of Eltantawy’s communication service provider in Egypt, though the researchers did not accuse the ISP of complicity in the attack.

Verdict: prediction fulfilled ✅

8. Drone hacking!

Although there was a public report of drones used to hack a Wi-Fi network in 2022, there are no accounts of similar events happening in 2023.

Verdict: prediction not fulfilled ❌

APT predictions for 2024

Now, let us take a look at a possible future of the advanced persistent threat landscape.

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

The past year marked a significant discovery: "Operation Triangulation", a new, remarkably stealthy espionage campaign targeting iOS devices, including those of our colleagues. During the investigation, our team identified five vulnerabilities in iOS, including four zero-days. These vulnerabilities did not just affect smartphones and tablets but also extended to laptops, wearable devices and smart home gadgets including Apple TV and Apple Watch. As we look ahead, we might anticipate more occasional cases of advanced attacks to leverage consumer devices and smart home technology. iOS devices may not be the only targets: other devices and operating systems could also face risks.

A creative avenue for threat actors is to expand their surveillance efforts to include devices such as smart home cameras, connected car systems and beyond. Many of these gadgets, both new and old, are susceptible due to vulnerabilities, misconfigurations or outdated software, making them attractive and easy targets for attackers.

Another notable aspect of this emerging trend is the "silent" exploit delivery method. In "Operation Triangulation", exploits were discreetly delivered through iMessage and activated without user interaction. In the upcoming year, we may see alternative delivery methods for exploits, such as:

- Zero-clicks through popular cross-platform messengers, allowing attacks without interaction with the potential victim
- One-clicks with malicious link delivery via SMS or messaging apps, where victims may unknowingly trigger attacks by opening these links
- Malicious actors intercepting network traffic, for instance, exploiting Wi-Fi networks – a less common yet potentially effective method

To protect against complex attacks and targeted threats, protection of both personal and corporate devices is vital. Solutions like XDR, SIEM, and MDM platforms, apart from traditional anti-virus products, enable centralized data collection, accelerate analysis, and correlate security events from various sources, facilitating swift response to complex incidents.

Building new botnets with consumer and corporate software and appliances

It is a well-known fact: vulnerabilities persist in commonly used software and appliances, whether for corporate or personal use. New high and critical severity vulnerabilities are discovered every now and then. According to Statista, in 2022, a record number of vulnerabilities — more than 25,000 — were discovered. Often, limited resources are dedicated to researching vulnerabilities, and they are not always fixed in a timely manner. This raises concerns about the potential emergence of new, large-scale and stealthily established botnets capable of conducting targeted attacks.

Creating a botnet involves stealthy installation of malware on a multitude of devices without the device owners' knowledge. APT groups may find this tactic intriguing for several reasons. To begin with, it allows threat actors to obscure the targeted nature of their attacks behind seemingly widespread assaults, making it challenging for defenders to ascertain the attackers' identity and motives. Furthermore, botnets rooted in consumer devices or software, or those belonging to legitimate organizations, conveniently mask the attackers' true infrastructure. They can function as proxy servers, intermediate C2 (Command and Control) hubs and, in cases of network misconfiguration, potential entry points into organizations.

Botnets themselves are not a new attack tool. For example, a few years ago, a botnet of more than 65,000 home routers was used to proxy malicious traffic for other botnets and APTs. Another example, which has risen in the wake of remote work becoming widespread, is related to APT campaigns targeting remote workers via small office/home office routers infected with a botnet-like remote access trojan (RAT). Given the significant number of recently disclosed vulnerabilities, we expect to see new attacks of this kind in the coming year.

Botnet-driven attacks will not be confined to APT groups and may also be adopted by cybercriminals. The covert nature of these attacks presents detection challenges while offering attackers ample opportunities to infiltrate and establish a presence within the organization's infrastructure.

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

With the introduction of modern security measures like KMCS (Kernel Mode Code Signing), PatchGuard, HVCI (Hypervisor-Protected Code Integrity) and the Secure Kernel architecture in recent Windows releases, Microsoft aimed to reduce the prevalence of rootkits and similar low-level attacks. These classical attack methods were prevalent during an earlier era characterized by a multitude of rootkit variants. Over the past few years, we have witnessed numerous APT actors and cybercrime groups successfully execute their code in the kernel-mode of targeted systems, despite the presence of these new protection mechanisms. Several Windows Hardware Compatibility Program (WHCP) abuses reported this year led to compromises of the Windows kernel trust model. In June 2021, the Netfilter rootkit was reported, after which Microsoft published an advisory detailing that it was used as a means of geo-location cheating within the gaming community in China. Bitdefender then disclosed FiveSys in October 2021, a rootkit that was mainly used to target online gamers with the main goal of credential theft and in-game-purchase hijacking. Then Mandiant reported the last known abuse that revealed the Poortry malware, which had been used in a number of cyberattacks including ransomware-based incidents. In July 2023, we privately reported new FiveSys signed variants.

We anticipate a rise in three key vectors that will further empower threat actors with this capability:

- Increased underground market for EV certificates and stolen code signing certificates
- More abuse of the developer accounts to get the malicious code signed through Microsoft code signing services like WHCP
- Continuous increase in BYOVD (Bring Your Own Vulnerable Driver) in current threat actors' TTP arsenal

Last year, the world saw well over 50 ongoing real-world conflicts, with the highest level of violent conflicts since World War II, as estimated by the UN. Any political confrontation now inherently includes cyber-elements, as they have become a default part of any conflict, and this trend is to evolve further. BlackEnergy APT attacks in Ukraine are a prominent example from the last decade, known for destructive actions against media companies, compromising industrial control systems and engaging in cyber-espionage. The current landscape of potential actors involved in cyber-warfare is extensive, ranging from the CloudWizard APT campaign activities in the Russo-Ukrainian conflict area to a string of cyberattacks sparked by the recent attacks within the Israeli-Hamas conflict. These include, for example, cyberattacks on Israeli energy, defense and telecoms organizations by a threat actor dubbed "Storm-1133" (reported by Microsoft) and the targeting of Android users in Israel with a malicious version of the RedAlert – Rocket Alerts app. A hacking group dubbed Predatory Sparrow has resurfaced following an almost year-long break amidst the ongoing conflict, according to CyberScoop reports.

As we look ahead, we anticipate a surge in state-sponsored cyberattacks as geopolitical tensions strengthen. It will not be limited to critical infrastructure, government sectors or defense companies across the globe; media organizations will also increasingly be at risk. In the current climate of heightened geopolitical tensions, media organizations may be chosen as targets by those seeking to use them for counterpropaganda or disinformation purposes.

Hackers will primarily focus on data theft, IT infrastructure destruction and long-term espionage. Cyber-sabotage campaigns will likely be on the rise, too. The attackers will not just encrypt data; they will destroy it, posing a significant threat to organizations vulnerable to politically driven attacks. This will also include specific targeted attacks against individuals or groups. These attacks may involve compromising the devices of individuals to gain access to the organization they work for, using drones to locate specific targets, using malware for eavesdropping, and beyond.

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

Another instance of digital integration in conflicts is hacktivism. It is hard to imagine any future conflict without hacktivist involvement. There are several ways hacktivists may influence cybersecurity. First, they can carry out actual cyberattacks, including DDoS attacks, data theft or destruction, website defacement, and so on. Second, hacktivists can make false hack claims leading to unnecessary investigations and subsequent alert fatigue for SOC analysts and cybersecurity researchers. For example, in the ongoing Israeli-Hamas conflict, a hacktivist group claimed that they attacked the Israeli Dorad private power station in the beginning of October. Although the subsequent research revealed that the data they posted online was leaked by another group in June 2022, it took time and resources to find out that no new leak occurred. Deepfakes are also in use, easily accessible tools employed for impersonation and to throw in disinformation, as well as other high-profile cases, such as hackers interrupting Iranian state TV broadcasts during protests. All in all, as geopolitical tensions rise with no prospects of abating any time soon, we expect to see an increase in hacktivist activity, both destructive and aimed at disinformation.

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

There is a growing trend where attackers meet their objectives through suppliers, integrators or developers. This means small and medium-sized companies, often lacking robust protection against APT attacks, are becoming gateways for hackers to access the data and infrastructure of major players, their ultimate targets. To illustrate the magnitude of supply chain attacks, as we witness them now, one might recall the widely-discussed breaches through Okta in 2022 and 2023. This identity management company serves over 18,000 customers worldwide, and each of these could potentially be compromised.

The motivation behind these attacks may vary, ranging from financial gain to cyber-espionage, intensifying the concerning nature of this threat. For example, the notorious APT group Lazarus has been honing its supply chain attack capabilities. What is even more remarkable is the discovery that the notorious Gopuram backdoor, deployed through the infamous 3CX hack affecting victims worldwide, was found to coexist on victim machines alongside AppleJeus, a backdoor attributed to Lazarus. This attack was highly targeted and showed particular interest in cryptocurrency companies, which may indicate that the ultimate goal of the attackers was financial gain.

As supply chain attacks become more popular among threat actors, 2024 might usher in a new phase in related activities. The trend may evolve in various ways. First, popular open-source software could be employed to target specific enterprise developers. Additionally, the shadow market could introduce new offerings, including access packages targeting various software vendors and IT service suppliers. Consequently, those interested in orchestrating supply chain attacks, armed with access to an extensive pool of potential victims, can then carefully select their preferred targets for large-scale assaults. By doing this, threat actors are potentially taking the efficiency of supply chain attacks to a new level.

Spear-phishing to expand with accessible generative AI

Chatbots and generative AI tools are now widespread and easily accessible. This trend has not gone unnoticed by threat actors who are developing their own black-hat chatbots based on legitimate solutions. For instance, WormGPT, a language model explicitly designed for malicious use, claimed to be based on the open-source language model GPTJ. Other models, like xxxGPT, WolfGPT, FraudGPT, DarkBERT, and more, lack the content restrictions present in legitimate solutions, making them attractive to attackers that exploit these models for malicious purposes.

The emergence of these tools is likely to facilitate the mass production of spear-phishing messages, often serving as the initial step in APT and other attacks. The significance extends beyond the ability to craft persuasive and well-written messages quickly. It also encompasses the capability to generate documents for impersonation and mimic the style of specific individuals, such as a business partner or a colleague of the victim. In the upcoming year, attackers are expected to develop new methods for automating espionage on their targets. This may include automatic data collection from the victim's online presence, such as social media posts, media comments, or authored columns: any content associated with the victim's identity. This information will be processed using generative tools to create various text or audio messages in the specific individual's style and voice.

Meanwhile, the importance of cybersecurity awareness and preventative measures, including threat intelligence and proactive monitoring and detection, will continue to grow.

Emergence of more groups offering hack-for-hire services

Hacker-for-hire (or hack-for-hire) groups specialize in infiltrating systems and offering data theft services. Their clientele includes private investigators, law firms, business rivals, and those lacking the technical skills for such attacks. These cyber-mercenaries openly advertise their services and target entities of interest.

One such group, tracked by our Global Research and Analysis Team (GReAT), is DeathStalker. It focuses on law firms and financial companies, providing hacking services and acting as an information broker rather than operating as a traditional APT. They use spear-phishing emails with malicious file attachments to take control of victims' devices and steal sensitive data.

These groups consist of skilled hackers organized hierarchically, with leaders managing teams. They advertise on dark web platforms and employ various techniques, including malware, phishing, and other social engineering methods. They adapt to avoid detection by using anonymous communication and VPNs, and causing various impacts, from data breaches to reputational damage. The services of hacker-for-hire groups in general go beyond

cyber-espionage and extend to commercial espionage. They may gather data on competitors, for example, M&A transactions, expansion plans, financials, and customer information.

This approach is gaining global momentum, and we expect it to evolve in the coming year. It is possible that some APT groups may expand their operations due to the demand for such services, as they need to generate income to sustain their activities and compensate their operatives.

MFT systems at the forefront of cyberthreats

As the digital landscape continues to evolve, so does the complexity and sophistication of cyberthreats. At the heart of this evolving scenario are Managed File Transfer (MFT) systems, designed to securely ferry sensitive data between organizations. Housing a wealth of confidential information including intellectual property, financial records, and customer data, MFT solutions have become indispensable in modern business operations. They facilitate seamless data sharing both internally and externally, thereby becoming a cornerstone of organizational efficiency. However, this pivotal role also places them in the crosshairs of cyber-adversaries, particularly ransomware actors, who are on a relentless quest to exploit digital vulnerabilities for financial extortion.

The incidents involving MFT systems, such as MOVEit and GoAnywhere, in 2023, shed light on the potential vulnerabilities within these critical data transfer conduits. The MOVEit breach orchestrated by the Cl0p ransomware gang, and the exploitation of Fortra's GoAnywhere MFT platform highlighted how a single vulnerability could be leveraged to exfiltrate sensitive data, disrupt operations and demand a ransom.

Looking ahead, the threat landscape affecting MFT systems is poised for escalation. The allure of financial gain and the potential to cause substantial operational disruptions will likely fuel a surge in targeted attacks against MFT systems. The intricate architecture of MFT systems, coupled with their integration into broader business networks, potentially harbors security weaknesses that are ripe for exploitation. As cyber-adversaries continue to hone their skills, the exploitation of vulnerabilities within MFT systems is anticipated to become a more pronounced threat vector.

The trajectory of cyberthreats targeting MFT systems underscores a looming reality: the potential for significant data breaches and financial extortion will continue to rise. The incidents of 2023 serve as a stark reminder of the vulnerabilities inherent within MFT systems and the dire need for robust cybersecurity measures to safeguard these critical data transfer channels.

In light of this, organizations are strongly advised to undertake comprehensive reviews of their MFT solutions to identify and mitigate potential security weaknesses. Implementing robust Data Loss Prevention (DLP) solutions, encrypting sensitive data, and fostering a culture of cybersecurity awareness are prudent steps towards fortifying MFT systems against emerging cyberthreats. As the cyberthreat horizon continues to expand, proactive cybersecurity measures encompassing MFT systems will be paramount in safeguarding organizational data assets and ensuring operational resilience in the face of evolving cyberthreats.

The narrative of 2023 is a clarion call for organizations to bolster their cybersecurity apparatus around MFT systems. As we venture into a future where cyberthreats are bound to become more sophisticated, the onus is on organizations to stay ahead of the curve, ensuring the integrity and security of their MFT systems in a bid to thwart the nefarious designs of cyber-adversaries.

These were our predictions for the year 2024. A year from now, we shall see which ones materialized and which ones did not.
