APT trends report Q1 2024

Authors

- Expert GReAT

For more than six years, the Global Research and Analysis Team (GReAT) at Kaspersky has been publishing quarterly summaries of advanced persistent threat (APT) activity. These summaries are based on our threat intelligence research. They provide a representative snapshot of what we have published and discussed in greater detail in our private APT reports. They are designed to highlight the significant events and findings that we feel people should be aware of.

This is our latest installment, focusing on activities that we observed during Q1 2024.

Readers who would like to learn more about our intelligence reports or request more information about a specific report, are encouraged to contact intelreports@kaspersky.com.

The most remarkable findings

The Gelsemium group performs server-side exploitation that effectively leads to a webshell, and uses various custom and public tools deployed with stealth techniques and technologies. The two main implants, SessionManager and OwlProxy, were first detected in 2022 in the aftermath of the ProxyLogon-type exploitations of Exchange Servers. Our latest investigation was prompted by the discovery of suspicious activity on a server located in Palestine in mid-November 2023, with traces of a previous breach attempt on October 12, 2023. The payloads were distinctively served, veiled as font files, in compressed and encrypted fashion. This characteristic led us to highly similar incidents in Tajikistan and Kyrgyzstan.

Careto is a highly sophisticated threat actor that has been seen targeting various high-profile organizations since at least 2007. However, the last operations conducted by this threat actor were observed in 2013. Since then, no information about Careto's activity has been published. Recent threat hunting enabled us to gain an insight into campaigns run by Careto in 2024, 2022 and 2019. Our private report provided a detailed description of these activities, focusing on how the actor performed the initial infections, lateral movement, malware execution, and data exfiltration activities. It is notable that the Careto actor used custom techniques, such as employing the MDaemon email server to maintain a foothold inside the organization or leveraging the HitmanPro Alert driver for persistence. In total, we have seen Careto use three complex implants for malicious activities, which we dubbed "FakeHMP", "Careto2", and "Goreto". The capabilities of these implants were also described in our private report.

Middle East

In March, a new malware campaign was discovered, targeting government entities in the Middle East. We dubbed it "DuneQuixote". Our investigation uncovered more than 30 DuneQuixote dropper samples actively employed in this campaign. The droppers represent tampered with installer files for a legitimate tool named "Total Commander". These carry malicious code for downloading further payloads, at least some of which are backdoor samples dubbed "CR4T". At the time of discovery, we identified only two such implants, yet we strongly suspect the existence of others that may come in the form of completely different malware. The group prioritized the prevention of collection and analysis of their implants – the DuneQuixote campaigns display practical and well-designed evasion methods, both in network communications and malware code.

Our last report on the Oilrig APT discussed how IT service providers were potentially used as a pivot point to reach their clients as an end-target, and we kept tracking the threat actor's activity to identify relevant infection attempts. We detected another activity in the process, likely by the same threat actor, but this time targeting an internet service provider in the Middle East. This new activity saw the actor using a .NET-based implant, which is staged using VB and PowerShell. The implant, which we named "SKYCOOK" for its function names, is a remote command execution and infostealer utility. The actor also used an autohotkey-based (AHK) keylogger similar to the one used in a previous intrusion.

Southeast Asia and Korean Peninsula

We have been tracking the activities of DroppingElephant in the past few years and recently detected several samples of the Spyder backdloor in its operations, as well as the Remcos RAT and, in a smaller number of cases, other malicious RAT tools. We observed that the threat actor abuses the DISCORD CDN network and leverages malicious .DOC and .LNK files to deliver these remote access tools to victims in South Asia. The Spyder backdoor has been detailed by QiAnXin, along with its use in targeting multiple entities in South Asia. In our report, we shared newly discovered IoCs and the type of targeted organizations based on our telemetry.

At the end of 2023, we discovered a striking malware variant orchestrated by the Kimsuky group, delivered by exploiting legitimate software exclusive to South Korea. While the precise method used to manipulate this legitimate program as the initial infection vector remains unclear, we confirmed that the legitimate software established a connection to the attacker’s server. Subsequently, it retrieved a malicious file, thereby initiating the first stage of the malware.

The initial-stage malware serves as a conventional installer designed to introduce supplementary malware and establish a persistence mechanism. Upon execution of the installer, it generates a subsequent stage loader and adds it to the Windows service for automatic execution. The culminating payload in this sequence is previously unknown Golang-based malware dubbed “Durian”. Durian boasts comprehensive backdoor functionality, enabling the execution of delivered commands, additional file downloads and exfiltration of files.

With the help of Durian, the operator implemented various preliminary methods to sustain a connection with the victim. First, they introduced additional malware named “AppleSeed”, an HTTP-based backdoor commonly employed by the Kimsuky group. Furthermore, they incorporated legitimate tools, including ngrok and Chrome Remote Desktop, along with a custom proxy tool, to access target machines. Ultimately, the actor implanted the malware to pilfer browser-stored data including cookies and login credentials.

Based on our telemetry, we pinpointed two victims within the South Korean cryptocurrency sector. The first compromise occurred in August 2023, followed by a second in November 2023. Notably, our investigation did not uncover any additional victims during these instances, indicating a highly focused targeting approach by the actor.

Given that the actor exclusively employed the AppleSeed malware, a tool historically associated with the Kimsuky group, we have a high level of confidence in attributing these attacks to Kimsuky. However, intriguingly, we have detected a tenuous connection with the Andariel group. Andariel, known for adopting a custom proxy tool named “LazyLoad”, appears to share similarities with the actor in this attack, who also utilized LazyLoad, as observed during our research. This nuanced connection warrants further exploration into the potential collaboration or tactics shared between these two threat actors.

ViolentParody is a backdoor detected inside a South Korean gaming company, with the latest deployments observed in January this year. The threat actor distributed this backdoor over the organization’s network by infecting a batch file located on an internal network share. The execution of said infected .BAT file results in the launch of an MSI installer that in turn drops the backdoor on the machine and configures it to persist through scheduled tasks and COM objects. Analysis of this backdoor revealed that couldcollect reconnaissance data on the infected machine, perform file system operations and inject various payloads. We additionally observed the threat actor behind this backdoor launching penetration testing tools, such as Ligolo-ng, Inveigh and Impacket. We attribute the activity described in our report to Winnti with low confidence.

The threat actor SideWinder launched hundreds of attacks in recent months against high-profile entities in Asia and Africa. Most of the attacks start with a spear-phishing email containing a Microsoft Word document or a ZIP archive with an LNK file inside. The attachment kicks off a chain of events that lead to the execution of multiple intermediate stages with different JavaScript and .NET loaders, and finally ends with a malicious implant developed in .NET that runs only in memory.

During the investigation, we observed a rather large infrastructure composed of many different virtual private servers and dozens of subdomains. Many subdomains are assumed to be created for specific victims, and the naming scheme indicated that the attacker had tried to disguise malicious communications as legitimate traffic from websites related to governmental entities or logistics companies.

SideWinder has historically targeted governmental and military entities in South Asia, but in this case, we observed an expanded range of targets. The actor also compromised victims located in Southeast Asia and Africa. Moreover, we saw different diplomatic entities in Europe, Asia and Africa that were compromised. The expansion in targeting also includes new industries, proven by the discoveries of new targets in the logistics sector, more specifically in maritime logistics.

The Lazarus group has various malware clusters in its arsenal and continues to update its functionalities and techniques to evade detection. However, the actor can also be observed employing its old malware on occasion. We recently discovered that this notorious actor was testing its old and familiar tool, ThreatNeedle. The malware author utilized a binder tool to create initial-stage malware for delivering and implanting the final payload. The main objective of the binder tool is assembling the malware installer, actual payload and configuration. In addition, we discovered various malicious files from an affected machine fetching the next-stage payload after sending the victim's profile. This kind of downloader malware is typical of Lazarus's modus operandi. However, the group adopted a more complex HTTP communication format at this time to evade detection at the network level. By investigating the Command-and-Control (C2) resources used by the actor, we discovered NPM packages that contain malicious JavaScript code to deliver malware without user notification. Most of them are disguised as cryptocurrency-related programs and capable of downloading an additional payload from the actor-controlled server. This is a highly similar strategy to the scheme that we have observed and reported in the past.

Hacktivism

Hacktivism, a marriage of hacking and activism, is often excluded from a company's threat profile. This type of threat actor is commonly active in all types of crises, conflicts, wars and protests, among other events. The goal is to send a political, social or ideological message using digital means.

SiegedSec stepped up its hacktivist intrusions and activities internationally throughout 2023. This small group, active since 2022, mainly performs hack-and-leak operations. As with past hacktivist groups like LulzSec, what started as hack-and-leak and disruptive operations "just for lulz", evolved into multiple offensive efforts in pursuit of social justice-related goals across the globe. The activities also led to coordination with other cybercriminal groups as part of the Five Families hacktivist collective, although SiegedSec were later expelled for alleged improper conduct.

Their recent offensive activity is contingent on current socio-political events. Their web-application-focused offensive activity targets companies and industrial and government infrastructure, and they leak stolen sensitive information. SiegedSec's social justice initiatives include demanding freedom for an arrested Colombian website defacer / hacker, U.S. state governments' involvement in instituting anti-abortion laws, the ongoing Israel-Hamas conflict and alleged human rights violations by NATO. The group's members, both past and present, are still at large.

During the Israel-Hamas conflict, there has been an uptick in activities by hacktivists from all around the world, including denial of service (DoS and DDoS), web defacements, doxing and recycling of old leaks. The targets and victims have been primarily Israeli and Palestinian infrastructure. But since there are supporters on both sides of this conflict, hacktivists also target the infrastructure of supporting countries.

To mitigate exposure to threat actors of this type, it is first important to update the threat/risk profile when similar events happen. Second, it is vital to understand the technology exposure connected to the respective country or institution, and prevent unauthorized access by ensuring secure access and updated software. Third, DoS/DDoS readiness is essential. Although these attacks are transient, merely denying access for a limited time before normal service resumes, the respective tools are widely available, and their disruptive impact on business operation may vary depending on attack duration and size. Therefore, it is essential to implement measures to mitigate against application and volumetric attacks. Finally, data leaks are almost inevitable nowadays. Hackers may merely start with stolen credentials to gain full enterprise access and leak sensitive data. The data may then get recycled in future events, to associate the hot topic of compromise with the hacktivist message, so that it can be heard widely. The best approach to mitigate against this is to prevent the data leak in the first place. Implementing ways to monitor the network flow can be helpful in identifying an unusually large outbound data flow, which could be blocked at an early stage.

Other interesting discoveries

In 2020, we reported an ongoing campaign, started in 2019, that leveraged what was at the time new Android malware named “Spyrtacus”, used against individuals in Italy. The tool exhibited similarities with HelloSpy, the infamous stalkerware used to remotely monitor infected devices. The threat actor first started distributing the malicious APK via Google Play in 2018, but switched to malicious web pages forged to imitate legitimate resources relating to the most common Italian internet service providers in 2019. We have continued to monitor this threat over the years and recently observed a previously unknown Spyrtacus agent developed for Windows. The implant communicates with a C2 resource already reported in one of our previous reports and shares similarities to the Android counterpart in both malware logic and the communication protocol. During the investigation, we discovered other subdomains, which indicate the existence of implants for iOS and macOS, and may indicate the expansion of the group’s activities to other countries in Europe, Africa and the Middle East.

Final thoughts

While the TTPs of some threat actors remain consistent over time, such as heavy reliance on social engineering as a means of gaining a foothold in a target organization or compromising an individual’s device, others have refreshed their toolsets and expanded the scope of their activities. Our regular quarterly reviews are intended to highlight the most significant developments relating to APT groups.

Here are the main trends that we saw in Q1 2024:

- The key highlights this quarter include Kimsuky’s use of the Golang-based backdoor Durian in a supply-chain attack in South Korea, and campaigns focused on the Middle East, including APTs such as Gelsemium, but also hacktivist attacks.

- The Spyrtacus malware used for targeting individuals in Italy demonstrates that threat actors continue to develop for multiple platforms, including mobile malware.
- APT campaigns continue to be very geographically dispersed. This quarter, we reported campaigns focused on Europe, the Americas, the Middle East, Asia and Africa.
- We have seen attacks targeting a variety of sectors, including government, diplomatic, gaming, maritime logistics and an ISP.
- Geopolitics remains a key driver of APT development, and cyberespionage remains a prime goal of APT campaigns.
- We also continue to see hacktivist campaigns: these have been centered mainly around the Israel-Hamas conflict, but not exclusively, as the activities of SiegedSec illustrate.

As always, we would like to note that our reports are the product of our visibility into the threat landscape. However, it should be borne in mind that, while we strive to continually improve, there is always the possibility that other sophisticated attacks may fly under our radar.

Disclaimer: when referring to APT groups as Russian-speaking, Chinese-speaking or other-language-speaking, we refer to various artefacts used by the groups (such as malware debugging strings, comments found in scripts, etc.) containing words in these languages, based on the information that we obtained directly or that is otherwise publicly known and widely reported. The use of certain languages does not necessarily indicate a specific geographic relation, but rather points to the languages that the developers behind these APT artefacts use.