securelist.com /apt-report-q3-2024/114623/

APT trends report Q3 2024

GReAT ⁝⁝ 11/28/2024

Authors

- Expert GReAT

Kaspersky's Global Research and Analysis Team (GReAT) has been releasing quarterly summaries of advanced persistent threat (APT) activity for over seven years now. Based on our threat intelligence research, these summaries offer a representative overview of what we've published and discussed in more detail in our private APT reports. They are intended to highlight the significant events and findings that we think are important for people to know about. This is our latest roundup, covering activity we observed during Q3 2024.

If you'd like to learn more about our intelligence reports or request more information about a specific report, please contact intelreports@kaspersky.com.

The most remarkable findings

In the second half of 2022, a wave of attacks from an unknown threat actor targeted victims with a new type of attack framework that we dubbed P8. The campaign targeted Vietnamese victims, mostly from the financial sector, with some from the real estate sector. Later, in 2023, Elastic Lab published a report about an OceanLotus APT (aka APT32) attack that leveraged a new set of malicious tools called Spectral Viper. Although the campaigns are the same, we cannot conclusively attribute P8 to OceanLotus.

The P8 framework includes a loader and multiple plugins. Except for the first-stage loader and the PipeShell plugin, all plugins are downloaded from the C2 and then loaded into memory, leaving no trace on disk. After a thorough analysis of the framework and its modules, we believe P8 was developed based on the open source project C2Implant, which is a red teaming C2 framework. However, P8 contains many built-in functions and redesigns of the communication protocol and encryption algorithm, making it a well-designed and powerful espionage platform. Based on the implemented supported commands, we suspect the goal is to implement another Cobalt Strike-like post-exploitation platform. Methods to gain persistence on affected systems are not built in and depend on commands received from the C2.

Unfortunately, we were unable to obtain any bait files or initial infection vectors. Based on limited telemetry, we believe with medium to low confidence that some of the initial infections were spear-phishing emails. Notably, these attacks use an obsolete version of the Kaspersky Removal Tool to side-load the P8 beacon. We also observed SMB and printer driver vulnerabilities being used to move laterally through the network.

We published a follow-up report on P8 that describes the plugins used in the attacks. Each time the system restarts, or as required by the operation, P8 downloads additional plugins from the C2 or loads them from disk into memory. So far, we have collected 12 plugins or modules that are used to support the operation by adding functionality for lateral movement, exfiltration, file management, credential stealing, taking screenshots or custom loading capabilities. In particular, two plugins are used to upload files of interest; one plugin is used for small files, while a second is used to upload large files to another server, presumably to reduce the network load on the C2.

We subsequently detected new attacks from this threat actor. While carrying out these attacks, the actor changed its TTPs from those outlined in our previous reports. For example, new persistence mechanisms were detected and we found that the loading mechanism of the final payload, the P8 beacon, also changed. In terms of victimology, there was little change. Most of the infections were still at financial institutions in Vietnam, with one victim active in the manufacturing industry. The infection vector has still not been found, nor have we been able to link these attacks to OceanLotus (APT32).

Earlier in 2024, a secure USB drive was found to be compromised and malicious code was injected into the access management software installed on the USB drive. The secure USB drive was developed by a government entity in Southeast Asia to securely store and transfer files between machines in sensitive environments. The access management software facilitates access to the encrypted partition of the drive. A Trojanized version of the software module was found to be used in these attacks. The malicious code injected into it is designed to steal sensitive files saved on the secure partition of the drive, while also acting as a USB worm and spreading the infection to USB drives of the same type.

Last year we investigated attacks against another different type of secure USB drive. Similarly, the attacks were delivered via a Trojanized USB management software called UTetris. We are tracking the threat actor behind the UTetris software attack as TetrisPhantom. In addition to the Trojanized UTetris software, TetrisPhantom uses a number of other malicious tools that have been in use for a few years. TetrisPhantom is still active and new samples of its tools have recently been detected.

While both the tactic of targeting a secure USB drive by compromising the software module installed on the drive and the victim profile in the recent attacks are similar to TetrisPhantom attacks, the malicious code implanted in the drive bears little similarity to the code injected into the *utetris.exe* program.

Our report provided an initial analysis of the Trojanized USB management program.

Chinese-speaking activity

In July 2021, we detected a campaign called ExCone targeting government entities in Russia. The attackers leveraged the VLC media player to deploy the FourteenHi backdoor after exploiting MS Exchange vulnerabilities. We also found Cobalt Strike beacons and several traces tying this actor to the ShadowPad malware and UNC2643 activity, which is in turn associated with the HAFNIUM threat actor.

Later that year, we discovered a new set of activities. This time the victimology changed: victims were also found in Europe, Central Asia and Southeast Asia. We also found new samples that we linked to Microcin, a Trojan used exclusively by SixLittleMonkeys. Shortly after, another campaign called DexCone was discovered, with similar TTPs to the ExCone campaign. Several new backdoors such as Pangolin and Iguania were discovered, both of which have similarities to FourteenHi.

Then, in 2022, we discovered another campaign by the same threat actor targeting Russia, with a special interest in government institutions, using spear-phishing emails as an infection vector and deploying an updated version of the Pangolin Trojan.

After that, we did not observe any new activity related to this actor until mid-July 2024. In this most recent campaign, the actor uses spear-phishing emails, embedding a JavaScript loader as the initial infection vector. The JavaScript loader loads yet another loader from a ZIP file, which in turn downloads a BMP image containing shellcode and an embedded PE file, which is the final payload. This is a new backdoor with limited functionality, reading and writing to files and injecting code into the *msiexec.exe* process. In this campaign, the actor decided to attack Russian educational institutions instead of government entities as it had previously.

The Scieron backdoor, a tool commonly used in cyber-espionage campaigns by the Scarab group, was detected in a new campaign. This campaign introduces novel decoders and loaders that use machine-specific information to decode and decrypt the Scieron backdoor and run it in memory. The campaign has specifically targeted a government entity in an African country and a telecoms provider in Central Asia. Notably, the infections within the telecoms provider have been traced back to 2022.

More recently, in June 2024, an updated infection chain was identified, with an updated set of decoders and loaders designed to run the Scieron backdoor and make it persistent. Our private report also provides a detailed description of the attackers' post-compromise activities.

Europe

Awaken Likho is an APT campaign, active since at least July 2021, primarily targeting government organizations and contractors. To date, we have detected more than 120 targets in Russia, but there are also targets in other countries and territories such as India, China, Vietnam, Taiwan, Turkey, Slovakia, the Philippines, Australia, Switzerland and the Czech Republic, among others. Based on our findings, we would like to highlight two specific features of this campaign: all attacks are well prepared, and the hackers rely on the use of the legitimate remote administration tool UltraVNC. While this approach is rather simplistic, the attackers have been using this technique successfully for years.

We discovered a new Awaken Likho campaign that emerged in May 2024, in which the threat actor adjusted its TTPs slightly. The threat actor cleaned up its Golang SFX-based archives by removing unused files and also switched to executing AutoIT scripts after file extraction. UltraVNC remained the final payload, but in this campaign it was made to look like a OneDrive update utility. The targeting remained the same as in the earlier campaign – mainly government organizations and their contractors located in Russia.

Awaken Likho then adjusted its TTPs again, in a campaign uncovered in June 2024 that is still ongoing. The threat actor continued to favor the use of AutoIT scripts and also began using protectors such as Themida to protect its samples. While most of the samples we found still deployed the UltraVNC module, the attackers changed the final payload from UltraVNC to MeshAgent in several samples. Unlike previous campaigns, we did not observe the Golang SFX droppers this time. The nature of the threat actor, leveraging open source and free tools, allows it to quickly change its arsenal during active campaigns.

Epeius is a commercial spyware tool developed by an Italian company that claims to provide intelligence solutions to law enforcement agencies and governments. In recent years, the malware attracted the attention of the community due to the publication of two articles. The first, published in 2021 by Motherboard and Citizen Lab, shared the first evidence and indicators related to the software. The second, an article published in 2024 by the Google Threat Analysis Group, described the business model of various companies that provide commercial surveillance solutions. Knowledge of this threat is sparse and the Epeius malware has never been publicly described in detail. Our own threat hunting efforts to obtain related samples started in 2021, and last year we discovered a DEX file that we attribute with medium to high confidence to Epeius. Our private report describes what we know about Epeius and provides a technical description of its main Android component.

Middle East

In September 2023, our colleagues at ESET published a report on a newly discovered and sophisticated backdoor used by the FruityArmor threat actor, which they named DeadGlyph. The same month, we released an APT report detailing the ShadowWhisperer and NightmareLoader tools used in conjunction with the DeadGlyph malware. More recently, we identified what appears to be the latest version of the native DeadGlyph Executor backdoor module, with changes to both its architecture and workflow components.

MuddyWater is an APT actor that surfaced in 2017 and has traditionally targeted countries in the Middle East, Europe and the USA. The actor typically uses multi-stage PowerShell execution in its attacks, probably to obfuscate the attacks, evade defenses and hinder analysis.

Recently we uncovered VBS/DLL-based implants used in intrusions by the MuddyWater APT group that are still active today. The implants were found at multiple government and telecoms entities in Egypt, Kazakhstan, Kuwait, Morocco, Oman, Syria and the UAE. The threat actor achieves persistence through scheduled tasks that execute a malicious VBS file with the wscript.exe utility.

The TTPs and infrastructure we analyzed for the current intrusions are similar to previously reported intrusions by the MuddyWater APT group.

Southeast Asia and Korean Peninsula

Gh0st RAT, an open source RAT created about 15 years ago, is used by various groups, including state-sponsored actors. One of them is Dragon Breath (aka APT-Q-27 and Golden Eye Dog), first discussed in 2020 in connection with a watering hole campaign aimed at tricking users into installing a Trojanized version of Telegram. By 2022, the group was still using Trojanized Telegram applications as an infection vector, but had changed the final payload to Gh0st RAT.

A year later, Sophos published a blog post describing the latest change in the group's TTPs, which included double side-loading DLLs. Since then, the Gh0st RAT payload has remained the same, but the attackers have again slightly adjusted their TTPs. DLL side-loading was abandoned and replaced by leveraging a logical flaw in a version of the TrueUpdate application, while more recently the group began to run the malware via a Python-based infection chain executed by the installer package.

Historically, Dragon Breath has targeted the online gaming and gambling industry. Given the nature of the infection vector, we're not yet able to determine the target audience for this campaign. The attack begins by tricking users into downloading a malicious MSI installer. Once the installer is started, the malware is installed alongside the legitimate application. We believe the victim is prompted to download and launch it from a fake site while searching for a Chinese version of the legitimate TrueUpdate MSI installer.

Bitter APT has been active for over a decade. Since late 2023, this threat actor has used and continues to use CHM (compiled HTML) files, LNK shortcuts and DOC files as the first stage of infection. These files carry malicious scripts to connect to a remote server and download the next stage of the attacks, and appear to be used as attachments to spear-phishing emails. The payloads delivered via these malicious scripts represent new samples of backdoor modules described in previous private reports. However, in several cases, the final payloads can only be downloaded by pre-selected system configurations authorized by the threat actor after the initial reconnaissance phase. In a recent report, we discussed the workflow of the initial LNK, DOC and CHM files, their progress through the next stages of the attack, as well as the updates to the final backdoor modules and corresponding infrastructure.

Tropic Trooper (aka KeyBoy and Pirate Panda) is an APT group operating since 2011. The group's targets have traditionally been in government, as well as the healthcare, transportation and high-tech industries located in Taiwan, the Philippines, and Hong Kong. Our most recent investigation revealed that in 2024, the group conducted persistent campaigns against a government entity in Egypt, which began in June 2023.

We noticed the infection in June 2024, when our telemetry showed recurring alerts for a new China Chopper web shell variant (China Chopper is used by many Chinese-speaking actors) found on a public web server. The server hosted a Content Management System (CMS) called Umbraco, an open source CMS platform for publishing content written in C#. The observed web shell component was compiled as a .NET module of Umbraco CMS.

During our subsequent investigation, we looked for other suspicious detections on this public server and identified several related malware sets. These include post-exploitation tools that we believe with medium confidence are related and being used as part of this intrusion.

We also identified new DLL search-order hijacking implants that are loaded from a legitimate vulnerable executable because it lacks the full path to the required DLL. This attack chain attempted to load the Crowdoor loader, named after SparrowDoor described by ESET. During the attack, the security agent blocked the first Crowdoor loader, which prompted the attackers to switch to a new, as yet unreported variant, with almost the same effect.

We investigated the attribution of this activity to the Chinese-language threat actor known as Tropic Trooper. Our findings show an overlap in capabilities reported in recent Tropic Trooper campaigns. The samples we found also show a high degree of overlap with samples previously attributed to Tropic Trooper.

PhantomNet is a RAT first described by ESET in late 2020. In 2021, we released our analysis of the PhantomNet malware, which at the time was being used in attacks against the Vietnamese government sector. Our report discussed in detail the plugins we found and the commands it supported.

We rediscovered PhantomNet during a recent investigation into a cyberattack on the Brazilian education and government sectors that occurred in April. This time we were able to recover several scripts, commands executed by the attackers, and the PhantomNet builder tool. The threat actor has changed the persistence mechanism so that the payload is now stored in an encrypted manner in the Windows registry and with an associated loader to retrieve the payload from the registry. There are also some changes to the victimology. Previously, PhantomNet infections were found in Asia, but now the infections have been found in many regions around the world and affect a wide variety of industries.

We discussed these findings in our private report, filling in the gaps from our previous report.

We have observed that the Kimsuky group uses a strategy of registering malware as a service for reliable persistence. The so-called ServiceChanger malware drops a malicious DLL file and registers a service disguised as a legitimate service. In the case we analyzed, ServiceChanger installed the TOGREASE malware, which is an evolved version of GREASE that adds the ability to toggle RDP activation when necessary by the operator; and in another instance, it was observed installing the XMRig miner.

In addition, this year’s updated version of the GREASE malware creates backdoor accounts to use RDP connections under the names “Guest” and “IIS_USER”, respectively. They borrow code from the publicly available UACME, allowing them to bypass UAC and execute commands with escalated privileges. Uniquely, the resources section within the GREASE malware includes a Zoom Opener installer vulnerable to DLL hijacking, which has not been observed in use by Kimsuky. However, it is possible that they may create malware that exploits this vulnerability in the future.

The updated GREASE malware is thought to be connected to the RandomQuery malware also used by Kimsuky, as it communicates with the C2 in a similar manner. The similarity and the overlap between the TOGREASE and GREASE malware used by the Kimsuky group suggests that this group is behind the malware.

Hacktivism

In the course of our research on hacktivist groups targeting organizations based in Russia, we have identified similarities among several of these groups. This suggests either that these clusters of activity share at least a subset of the same individuals, or that the groups are working closely together in their attacks. Our report details the tools, malware, and procedures of the BlackJack group and links it to the previously known group Twelve. In addition, further examination of its preferred wiper and ransomware tools uncovered samples that cannot be definitively attributed to either group.

Other interesting discoveries

In June, we identified an active campaign called “PassiveNeuron”, targeting government entities in Latin America and East Asia using previously unknown malware. The servers were compromised before security products were installed, and the method of infection is still unknown. The implants used in this operation were dubbed “Neursite” and “NeuralExecutor”. They do not share any code similarities with known malware, so attribution to a known threat actor is not possible at this time. The campaign shows a high level of sophistication, with the threat actor using compromised internal servers as an intermediate C2 infrastructure. The threat actor is able to move laterally through the infrastructure and exfiltrate data, optionally creating virtual networks that allow attackers to steal files of interest even from machines isolated from the internet. A plugin-based approach provides dynamic adaptation to the attacker’s needs.

In mid-April, we discovered a suspicious domain which, upon further investigation, revealed two backdoors written in Golang. During analysis, another backdoor was discovered that was used earlier in the attack timeline and protected using VMProtect. As well as the backdoors, an unknown keylogger and the use of the SOCAT tool were observed in this attack. The campaign exhibits a few peculiarities. First, the Golang backdoor uses Google Translate services as a proxy to communicate with the C2. Second, the threat actor tries to imitate Kaspersky software in terms of file names and names of scheduled tasks. Thirdly, we found only one infection, targeting a telecoms research center in India. We were unable to attribute this campaign to any known threat actor based on code similarity or TTPs.

In early April, we decided to take a closer look at the Windows Desktop Window Manager (DWM) Core Library Elevation of Privilege vulnerability (CVE-2023-36033), which was previously discovered as a zero-day and exploited in the wild. While searching for samples related to this exploit and attacks using it, we found a document of note that was uploaded to a multi-scanner service on April 1, 2024. This document had a rather descriptive file name, indicating that it contained information about a vulnerability in the Windows operating system. Inside the document we found a brief description of a Windows Desktop Window Manager vulnerability and how it could be exploited to gain system privileges.

The exploitation process described in the document was identical to that used in the previously mentioned zero-day exploit for CVE-2023-36033. However, the vulnerability was different. Judging by the quality of the writing and the fact that the document was missing critical details about how to actually trigger the vulnerability, there was a high probability that the vulnerability described was made up or was present in code that could not be accessed or controlled by the attackers. The subsequent investigation revealed a zero-day vulnerability that can be used to escalate privileges. After reporting the findings to Microsoft, the vulnerability was designated CVE-2024-30051 and a patch was released as part of Patch Tuesday on May 14, 2024.

After closely monitoring our statistics for related exploits and attacks, it became clear that there were several exploits for this zero-day vulnerability. Our discoveries showed that it was being used in conjunction with QakBot and other malware such as NewBot, leading us to believe that multiple threat actors have access to it. While previous findings of in-the-wild exploitation of CVE-2024-30051 showed financial motivation, it is possible that it could be leveraged in future APT activity.

An updated set of intrusions, possibly related to the Deathstalker cyber-mercenary group, employs an updated DarkMe VB6 OCX/DLL implant and stealthier TTPs, such as a more sophisticated infection chain.

In the intrusions we reported previously, the threat actor typically delivered the initial dropper through instant messaging (IM) apps such as Skype. In more recent intrusions, the actor typically delivered the initial dropper through Telegram. We assess with medium confidence that the threat actor delivered the initial droppers via Telegram channels related to e-trading and fintech news.

Apart from the delivery method, the attackers also increased their level of OPSEC and post-compromise cleanup by deleting post-exploitation files, tools, and registry keys after the operators achieve their objectives. Such actions, in turn, make the infection harder to detect and complicate post-compromise investigation.

Final thoughts

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

Here are the key trends we observed in Q3 2024:

- This quarter, we saw threat actors broaden their targeting, both in terms of verticals and geography.
- The purpose of most APT activity is cyber-espionage, although hacktivist attacks remain a feature of the threat landscape this quarter, mirroring areas of real-world conflict.
- Even more open source tools have been employed by APT threat actors, mostly to manage network connectivity with C2s.
- We continue to see threat actors using LOTL (Living off the Land) techniques in their campaigns.

As always, we would like to point out that our reports are the product of our visibility into the threat landscape. However, it is important to remember that while we strive for continuous improvement, there is always the possibility that other sophisticated attacks may fly under our radar.

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