APT trends report Q1 2022

For five 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; and 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 2022. Readers who would like to learn more about our intelligence reports or request more information on a specific report, are encouraged to contact intelreports@kaspersky.com.
Disclaimer: when referring to APT groups as Russian-speaking, Chinese-speaking or other-"speaking" languages, 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 we obtained directly or which is otherwise publicly known and reported widely. 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.

The most remarkable findings

On January 14, 70 Ukrainian websites were defaced: the attackers posted the message "be afraid and expect the worst". The defacement message on the Ministry of Foreign Affairs website, written in Ukrainian, Russian and Polish, suggested that personal data uploaded to the site had been destroyed. Subsequently, DDoS attacks hit several government websites. The following day, Microsoft reported that it had found destructive malware, dubbed WhisperGate, on the systems of government bodies and agencies that work closely with the Ukrainian government. We analyzed the associated samples and concluded that the deployed malware was not comparable in complexity or code similarity to malware leveraged in previous destruction campaigns such as NotPetya or BadRabbit; but was much more reminiscent of that typically used by cybercriminals. We also identified two samples developed in December 2021 containing test strings and preceding revisions of the ransom note observed in Microsoft's shared samples. It remains unclear who is behind the attack, although Serhiy Demedyuk, deputy secretary of Ukraine's National Security and Defense Council, stated that it was the work of UNC1151, a threat actor believed to be linked to Belarus. Throughout our investigation, we identified two samples developed in December 2021 containing test strings and earlier revisions of the ransom note observed in Microsoft's shared samples. We concluded with high confidence that these samples were earlier iterations of the wiper reportedly used in Ukraine. Additionally, we suspect that the MBR wiper was initially developed at that time and repurposed more recently for the above campaign. This could have been done either by an advanced actor with the intention of conveying the false notion that the operation was being conducted by criminals; or in cooperation with lower-tier threat actors who contributed their own resources.
On January 26, CERT-UA published a report showing code similarity between WhisperKill (the file wiper used during the WhisperGate campaign) and WhiteBlackCrypt, a wiper used in the first quarter of 2021. While we were unable to obtain the same results by analyzing

the CERT-UA samples, we subsequently identified a different WhiteBlackCrypt sample matching the WhisperKill architecture and sharing similar code. We also investigated the Bitcoin wallets used by both WhisperGate and WhiteBlackCrypt, but were unable to uncover any link between the two.

On February 23, ESET published a tweet announcing new wiper malware targeting Ukraine. The malware was more advanced than the samples identified earlier in the year that we documented in two of our private reports. This wiper, named HermeticWiper by the research community, abuses legitimate drivers from EaseUS Partition Master to corrupt the drivers of the compromised system. One of the identified samples was compiled on December 28, 2021, suggesting that this destructive campaign had been planned for months. At the time of publication, we had not identified any similarities between HermeticWiper and other known malware.

The following day, Avast Threat Research announced the discovery of new Golang ransomware in Ukraine, which they dubbed HermeticRansom. This malware was found around the same time as HermeticWiper; and publicly available information from the security community indicated that it was used in recent cyberattacks in Ukraine. Due to its unsophisticated style and poor implementation, this new ransomware was probably only a smokescreen for the HermeticWiper attack, due to its non-sophisticated style and poor implementation. We named this malware Elections GoRansom.

In late February 2022, we identified two archives submitted from network addresses in Ukraine to an online multi-scanner service. Both archives leveraged the name of the Security Service of Ukraine (SBU or СБУ) to trick targets into executing a Remote Access Tool (RAT). We were unable to determine the ultimate goal of deploying such RATs, or associate the campaigns with any known threat actor, but the two archives appear linked together and may have been deployed by the same operators. Such threats pose a risk to Ukrainian organizations and their partners, as well as foreign organizations with premises in Ukraine. The RAT deployment campaigns look like they are targeted at developing access at scale in Ukraine, which could match activities from criminal groups that pledged allegiance to Russia, and may enable further destructive activities.

On March 1, ESET published a blog post related to wipers used in Ukraine and to the ongoing conflict: in addition to HermeticWiper, this post introduced IsaacWiper, used to target specific machines previously compromised with another remote administration tool named RemCom, commonly used by attackers for lateral movement within compromised networks. Contrary to reporting from other vendors, this wiper does not leverage the Isaac PRNG.

On March 10, researchers from the Global Research and Analysis Team shared their insights into past and present cyberattacks in Ukraine. You can find the recording of the webinar here and a summary/Q&A here.

On March 22, the Ukraine CERT published a new alert about the DoubleZero wiper targeting the country. This is a new wiper, written in .NET, with no similarities to previously discovered wipers targeting Ukrainian entities. According to the CERT public statement, the campaign took place on March 17, when several targets in Ukraine received a ZIP archive with the filename “Вирус… крайне опасно!!!.zip” (translation: “Virus… extremely dangerous!!!.zip”).

Russian-speaking activity

In December 2021, as a result of our continued monitoring of the activities of the DustSquad threat actor, we observed new infrastructure and tools being used alongside the already known Octopus Trojan. We had initially analyzed this Delphi malware in April 2018. Since then, the actor has continued to target diplomatic entities of several Central Asian countries; and, according to our telemetry, their consulates in APAC and the Middle

East are also affected by recent campaigns. Octopus is only one of DustSquad's tools, along with other Windows and Android malware such as Zaka, Akinak and Harpoon. For Windows development, Delphi has been the group's traditional programming language of choice. The actor maintains a two-layered communication scheme, with relays and real C2s, utilizing a JSON-formatted base64-encoded network communication protocol, via the use of a third-party IndyProject library. We have previously seen DustSquad use third-party post-exploitation tools, such as the password dumping utility fgdump; but we have now observed new custom C modules, a first for DustSquad, and Delphi downloaders acting as post-exploitation facilitators, able to gather documents of interest for the actor. Malicious Windows executables have also been compiled with GCC under the MinGW environment.

Chinese-speaking activity

While hunting for malicious IIS modules, following our earlier reports about the mass exploitation of ProxyLogon and the Owowa module, we identified another backdoor module that has been widely deployed since at least June 2021. We named it BlackMoule, as we believe it is an update of BlackMould, a malicious tool that was briefly mentioned by Microsoft in late 2019 as part of GALLIUM activities against telecoms companies (aka Operation SoftCell).

In May 2021, we reported on Websiic, a cluster of activities that formed a set of attacks against high-profile targets in Europe and Asia. The attackers used the infamous ProxyLogon exploit to compromise Exchange servers and deploy a China Chopper web shell, which was in turn used to start a sophisticated infection scheme leading to the execution of a new backdoor that we dubbed Samurai. The toolset includes several unique loaders and installers that had not previously been observed and can be used to load malicious payloads directly into memory, usually in the context of a legitimate process such as svchost.exe. We discovered continued activity involving multiple new loaders and installers, which were supposedly used to deploy different malicious payloads. We also observed that the malware was exclusively used against servers until August 2021; but starting from September, similar samples were also observed targeting desktop environments via messaging applications such as Telegram. Despite the discovery of weak ties to the FunnyDream cluster, we were unable to confidently attribute this new campaign to an existing group, so we dubbed the threat actor behind these attack clusters ToddyCat. Our private report on the matter takes a closer look at the available evidence: we concluded that the overlaps are weak but unlikely to be coincidental, leading us to believe that the actor behind Websiic might be part of the Chinese-speaking nebulae.

At the end of January, the BfV (Federal Office for the Protection of the Constitution of Germany) issued a report detailing activity by the APT27 group (aka LuckyMouse) targeting German commercial companies. Their analysis outlines the usage of a common infection triad leveraged by the group, whereby a legitimate executable (mempeng.exe or vfhost.exe) side-loads a malicious DLL (vftrace.dll), which in turn invokes the execution of the HyperBro malware from position-independent code found within a third file (thumb.dat). By investigating this threat through the lens of Kaspersky's telemetry, we found an identical intrusion set targeting an enterprise in Taiwan that deals with the manufacture of smart city technology, which may suggest an intent to steal intellectual property, possibly as a means of leveraging the same technology as an instrument of surveillance. Another victim in which the same chain was exhibited is a computer game manufacturer in Cambodia, where the attack could have been used for a different purpose, possibly to infiltrate the company's supply chain. We determined that the attackers were able to spread across the network and remain active within it for months, while making use of various tools. In addition to the infection chain outlined above, we found post-exploitation tools that were not mentioned by the BfV, including a custom-written keylogger and a publicly available

SSH and SFTP credential stealer. Interestingly, we were able to observe the presence of a second malware loader on several hosts in the network that coincided with the deployment of the HyperBro implant. This loader leverages a fake Flash installer implanted with shellcode that is used to fetch a Cobalt Strike payload from a remote C2 server. At the time of writing, we can only assess with medium confidence that this tool is indeed associated with the group's activity, indicating a possible sharing of initial access to the network with an external entity, or usage of Cobalt Strike as an alternative to HyperBro in the case of unsuccessful deployment.

Middle East

While hunting for malicious modules for Microsoft IIS servers, we identified a poorly detected and widely deployed module that we call XTest. XTest is based on the publicly available IIS-Raid open source, and was identified on hundreds of servers in late February, with 95 percent of them still being compromised at the time of our report. We were not able to determine the exact purpose XTest serves the threat actors, but we believe, with low confidence, that the module may have been deployed as part of malicious activities from the APT35 actor (aka Charming Kitten and Phosphorus).

Southeast Asia and Korean Peninsula

We reported recent, ongoing malicious activity that we attribute to the threat actor Sidecopy, targeting government staff in India. In addition to the known malware types deployed in past campaigns by this actor, such as MargulasRAT, we identified a cluster of activity targeting Linux and macOS platforms, including an unknown Golang-based Linux RAT that we attribute exclusively to this group. The supporting infrastructure for this operation overlaps with an operation described in a report published by Cisco Talos in September 2021, which discusses a campaign targeting government personnel in India using Netwire and Warzone (aka AveMaria RAT) dating back to the end of 2020. According to the authors, the decoys, used in malicious documents and spread in the early stages of these operations, resemble the one used by TransparentTribe (aka APT36 and Mythic Leopard) and Sidecopy. Our private report provides additional and updated indicators of compromise (IoCs) in the context of the same campaign and a description of some Linux and macOS malware that the group behind it has recently adopted.

We identified three campaigns linked to the Konni threat actor, active since mid-2021, targeting Russian diplomatic entities. While the attackers used the same Konni RAT implant throughout the different campaigns, the infection vectors were different in each campaign: documents containing embedded macros, an installer masquerading as a COVID-19 registration application and, finally, a downloader with a new year screensaver decoy. We also identified post-exploitation tools exclusively used by Konni following a successful infection. These are capable of taking screenshots of the active window, deploying a keylogger or listing the connected USB devices and their content. The tools align with the threat actor's goal of stealing sensitive information from infected systems. We found overlaps in the infrastructure used by a tunneling tool used by the actor and several possible phishing websites set up within the above time frame. One of the registered domains shared similarities with another domain attributed to TA406 that, according to ProofPoint, incorporates the Konni APT.

Monitoring APT10 activities, we discovered new variants of its tools being used against the same targets as in previous campaigns – Japanese government agencies and diplomatic entities. We have seen versions of the LODEINFO backdoor through v0.4.7, v0.4.8, v0.4.9, v0.5.6, and v0.5.8 from January to December 2021, while Lilim RAT received an update to v1.4.1 in June 2021. In 2020, we published private reports featuring LODEINFO, a sophisticated fileless malware first mentioned in a blogpost from JPCERT/CC3. In these

reports, we mentioned new families of fileless malware known as DOWNJPIT and Lilim RAT, which replaced the existing tools of the trade. Further, we disclosed, with high confidence, that LODEINFO and its related activities were attributed to APT10, the infamous Chinese-speaking actor. Our latest report on this subject includes technical analysis of the new versions of LODEINFO and Lilim RAT and reviews updates to the malware. In particular, LODEINFO v0.5.6 and v0.5.8 introduced obfuscated backdoor command identifiers to slow down the reversing process. They also implemented the Vigenere cipher to evade detection by certain security products.

We recently discovered a Trojanized DeFi application, compiled in November 2021. This application contains a legitimate program called DeFi Wallet, that saves and manages a cryptocurrency wallet, but also implants a malicious file when executed. This malware is a fully featured backdoor containing sufficient capabilities to control the compromised victim. After looking into the functionalities of this backdoor, we discovered numerous overlaps with other tools used by the Lazarus group. The malware operator exclusively used compromised web servers located in South Korea for this attack. To take over the servers, we worked closely with a local CERT and, as a result of this effort, we had the opportunity to investigate a Lazarus group C2 server. The threat actor configured this infrastructure with servers set up as multiple stages. The first stage is the source for the backdoor, while the purpose of the second stage server is to communicate with the implants. This represents a common scheme for Lazarus infrastructure. From the log files originating from the C2 servers, a number of infected hosts are visible. By only using IP addresses we weren't able to confirm the exact victims of this campaign, given that some may belong to researchers, but they did reveal that this attack targeted entities and/or individuals at a global level.

Since October 2021, the Sidewinder threat actor has been using new malicious JS code with recently created C2 server domains. The attack targets victims with spear-phishing emails containing malicious OOXML files. The OOXML files have an external reference to the attacker's server and download an RTF document exploiting the CVE-2017-11882 vulnerability. The RTF documents have an embedded JS script in an OLE object that is dropped onto the victim's machine. Sidewinder has been using this infection chain for over a year; we provided details of these modules and described further payloads in our previous report. Our last report, in November, showed that Sidewinder's use of the obfuscated JS script has decreased in recent months. Closer investigation of the attacks performed in that period revealed dozens of detections of a new obfuscation technique used in their JS script, while the rest of the infection chain remained fairly consistent. The new attacks use the same infection chain, targeting other victims from their traditional victim profile as well as a number of victims in countries that were not traditionally of interest to SideWinder, such as Singapore. The timestamp of the detections and the registration of the servers used by Sidewinder in these attacks suggest that they started preparing the infrastructure and registering domains for their new wave of attacks in late September. In early October they updated their toolset with new JS obfuscation techniques, and while they continued the use of their old obfuscation routine for a while, they have slowly switched completely to the new one. We described the attacks using the new obfuscated JS scripts in our most recent private report. The attackers also used a new technique to reduce the suspicion raised by some of their spear-phishing documents that had no text content. They followed their first attempt to attack the victim – a spear-phishing email containing a malicious RTF exploit file – with another similar email, but in this case the title of the malicious document was "_Apology Letter.docx", and it contained some text explaining that the previous email was sent in error and that they are reaching out to apologize for that mistake.

In January, a trusted source forwarded a suspicious email to us. This email is disguised as an invitation from the renowned PyeongChang Peace forum and contains a DropBox link in the email body. The fetched file from the DropBox link contains a malicious Windows shortcut file capable of downloading the next stage payload from the attacker's server. Fortunately, we were able to acquire the samples from the remote server. We dubbed this malware Phontena; and our analysis revealed the entire infection chain of this attack, made up of multiple stages. From our telemetry, we discovered a full-featured backdoor that is probably the final payload of this infection. After analyzing the samples from the remote server, we recognized that the actor behind this attack was associated with information published by another vendor about a threat actor named APT-C-601 or APT-Q-122. Based on the malware sample we discovered, we assess that this group has many overlaps with the DarkHotel group. Malware used in previous DarkHotel activity, as well as the samples discovered as part of this research, has very similar C2 communication and internal mechanisms. Moreover, the malware author left Korean comments in one of the stager payloads.

Two years after we first reported the activities of a threat actor we named FishingElephant, the group continues to target victims in Bangladesh and Pakistan. While we identified the use of a new keylogger by FishingElephant, it appears that the group still mainly relies on the same TTPs (such as payload and communication patterns) that were covered in our initial reports.

ToddyCat, a relatively new APT actor, is responsible for multiple attacks detected since December 2020. In the first wave of attacks, dubbed Websiic, the attackers exploited a ProxyLogon vulnerability to compromise Exchange Servers of high-profile organizations in Europe and Asia. More recently, we detected a new set of attacks against desktop machines starting in September 2021, named Ninja by the attacker. This Trojan provides a large set of commands allowing the attackers to control target computers. Some capabilities we analyzed are similar to those provided in other notorious post-exploitation toolkits.

Other interesting discoveries

In December we were made aware of a UEFI firmware-level compromise through logs from our firmware scanning technology. Further analysis showed that the attackers modified a single component within the firmware to append a payload to one of its sections and incorporate inline hooks within particular functions. These changes allowed the attackers to intercept the original flow of the firmware code and have it executed alongside a sophisticated infection chain. The introduced malicious flow, in turn, is in charge of persistently executing a malware stager from a Windows service once the operating system is running. By examining other IoCs from the same network, we gathered a trove of evidence that led us to assess, with medium-to-high confidence, that the threat actor involved is closely tied to the APT41 group. More specifically, we inspected communication of other nodes in the same network to infrastructure related to the server from which the payload is retrieved by the malicious stager. This traffic originated from an in-memory modular implant dubbed ScrambleCross, known to be in use by APT41 or a closely affiliated actor. Although we have covered several UEFI-based infections in APT reports in the last few months, those were cases operating through modifications introduced to the Windows boot loader image, which resides on the ESP partition on disk and can be remediated through a reinstallation of the operating system. In this case, however, the malware was found in an image typically based in the SPI flash, which is outside the hard disk and therefore withstands formatting or disk replacement. To the best of our knowledge, this is only the third known case found in the wild of a comparable UEFI implant, following LowJax and MosaicRegressor.

While hunting for recent Deathstalker intrusions, we identified a new Janicab variant used in targeting legal entities in the Middle East during 2020, possibly active into early 2021 and potentially extending an extensive campaign that can be traced back to early 2015 targeting legal, financial and travel organizations in the Middle East and Europe. Janicab was first introduced in 2013 as malware able to run on macOS and Windows operating systems. The Windows version has a VBS script-based implant as the final stage, instead of the C#/PowerShell combination observed previously in Powersing samples. The VBS-based implant samples we have identified to date have a range of version numbers, meaning it was, and still is, in development. Overall, Janicab shows the same functionalities as its counterpart malware families, but instead of downloading several tools later in the intrusion lifecycle, as the group used to do with EVILNUM and Powersing intrusions, the analyzed samples have most of the tools embedded and obfuscated within the dropper. Interestingly, the threat actor continues to use YouTube, Google+, and WordPress web services as Dead Drop Resolvers (DDRs). However, some of the YouTube links observed are unlisted and go back to 2015, indicating possible re-use of infrastructure. Law firms and financial institutions remain the sectors most affected by DeathStalker. However, in the intrusions we analyzed recently, we suspect that travel agencies are a new vertical that we haven't previously seen this threat actor targeting.
We recently identified additional malicious activities, conducted by Tomiris operators since at least October 2021, against government, telecoms and engineering organizations in Kyrgyzstan, Afghanistan and Russia. In July 2021, we reported the previously unknown Tomiris Golang backdoor, deployed against government organizations within a CIS country through DNS hijacking. We exposed similarities between DarkHalo's SunShuttle backdoor and the Tomiris implant. Later in 2021, we uncovered associated malicious activities that also used the open-source RATel implant to target several government organizations within Russia and Central Asia, while drawing an additional possible link between Tomiris operators and UNC1514.

Final thoughts

While the TTPs of some threat actors remain consistent over time, relying heavily on social engineering as a means of gaining a foothold in a target organization or compromising an individual's device, others refresh their toolsets and extend the scope of their activities. Our regular quarterly reviews are intended to highlight the key developments of APT groups.
Here are the main trends that we've seen in Q1 2022:

- Geopolitics has always been a key driver of APT developments; never more so than during a period of open warfare, as illustrated by the various cyberattacks related to the conflict in Ukraine. We have, of course, seen other activity centered around geopolitics, including the Konni and APT10 campaigns.
- One of the trends we discussed in our 2021 APT review and predictions for 2022 was the further development of low-level implants. Moonbounce provides a striking example of this trend.

As always, we would 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.