APT trends report Q2 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 Q2 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.

The most remarkable findings

On January 24, a hash for sophisticated Solaris SPARC malware was posted on Twitter. The complex, modular cyber-espionage platform rivals EquationDrug, Remsec, and Regin in complexity. We identified a Windows variant of this sample using the same string encryption algorithm, internal modules, and functionalities. The implant is a complex framework internally called SBZ. It supports multiple exfiltration methods and complicated networking infrastructure, including addressing, redirection, and routing. SBZ probably refers to STRAITBIZZARE, a cyber-espionage platform used by the Equation Group. It is also interesting to note the overlap between the Interface IDs from the DanderSpritz samples from the ShadowBrokers' dump "Lost in Translation" and the Interface IDs in the framework we were able to correlate. Our two private reports provided technical information on the Windows and SPARC variants respectively.

In late 2021, we encountered a malicious DXE driver incorporated into several UEFI firmware images that were flagged by our firmware scanner (integrated into Kaspersky products at the start of 2019). The malicious driver corresponded to the Compatibility Support Module (CSM), used to facilitate a legacy boot sequence from the Master Boot Record (MBR). This module was modified in such a way as to spawn an infection chain alongside the benign execution logic, culminating in the deployment of malicious kernel mode shellcode intended to stage the execution of an additional payload from an external server, which we were unable to fully retrieve. An investigation into the malicious UEFI component, which we named CosmicStrand, showed that a variant of it was in fact previously described by another security vendor. The samples that we found initially seemed to have used a different infrastructure and only contained slight modifications, constituting a newer variant of the malware. Our telemetry indicates that both variants were found in a limited set of PCs and were probably receiving a response from the respective C2 servers within limited timeframes, allowing us to assess with low-to-medium confidence that the implant was used in a targeted manner and could have been leveraged by an advanced actor for an undetermined purpose. The set of targets was limited and appeared to be computers belonging to victims in China, Vietnam, Russia and Iran.

Russian-speaking activity

In March, Proofpoint published a blog post about a new spear-phishing campaign related to the war in Ukraine, tentatively attributed to the Russian-speaking actor UNC1151 (aka TA445 and Ghostwriter). Based on their findings, the attack was related to the current

situation in Ukraine. The attackers sent spear-phishing emails to European government workers responsible for managing transportation and population movement in Europe, with the aim of infecting them with the Sunseed Trojan. Our investigation of this activity led us to discover other related campaigns targeting a wide range of entities located in Central Asia, Europe and the Americas since at least May 2020. We found links to previously observed cybercrime activities, new, formerly unknown samples used by the attackers during post-exploitation activities, a wealth of recent information about C2 infrastructure and the latest samples distributed to compromise victims.

Chinese-speaking activity

On March 22, Volexity released a blog post related to new activity targeting a Tibetan minority, attributed to Storm Cloud, a threat actor we track under the name Holy Water. The post described a multi-platform malware family dubbed GIMMICK, affecting both Windows and macOS machines, with variants developed in multiple programming languages (.NET, Delphi, ObjectiveC), all using an identical C2 protocol based on Google Drive. After looking at this campaign, we provided additional IoCs and analysis of the components used in these attacks.

We detected new activity, starting in March, from the threat actor behind ExCone and DexCone. We observed artefacts related to a new wave of spear-phishing attacks against targets in Russia that use information about the crisis in Ukraine to lure victims into opening a malicious document. The email is just the first step of a multi-stage infection process that leads to the installation of a new tiny variant of the Pangolin Trojan. Pangolin is private malware we discovered in 2021, exclusively used by ZexCone, the threat actor behind ExCone and DexCone. We also found a fully-fledged version of the Pangolin Trojan, including new commands.

Middle East

Recently, researchers at SEKOIA.IO released a report covering a cluster of domains they believe to be part of a malicious infrastructure they dubbed BananaSulfate. This infrastructure is of particular interest as it appears to be rapidly expanding and changing, with dozens of domains registered so far, and is active for short periods of time only. Moreover, as pointed out by SEKOIA.IO, the domain names suggest they may be part of an attack targeting multiple platforms, since the domains masquerade as legitimate services in Windows, iOS and Android operating systems. Lastly, certain similarities between this infrastructure and those we observed in previous reports suggest tthis may be renewed activity by the threat actor we call Karkadann/Piwiks.

Southeast Asia and Korean Peninsula

In January, Kimsuky, a prolific and active Korean-speaking threat actor, attacked a media company and a think-tank in South Korea. Based on our telemetry, the actor initiated the attack by sending a spear-phishing email containing a macro-embedded Word document. Various examples of different Word documents were uncovered, each showing different decoy content related to geo-political issues on the Korean Peninsula. The actor also took advantage of the HTML application file format to infect the victim using a Hangeul decoy document. After the initial infection, a Visual Basic script was delivered to the victim. As part of this process, the actor abused a legitimate blog service to host a malicious script with an encoded format. The implanted VBS file is capable of reporting information about infected computers and downloading additional payloads with an encoded format. The final stage is an infected Windows executable. Finally, the delivered malware is capable of stealing information from the victim, such as file lists, user keystrokes, and login credentials stored in web browsers. The actor apparently stole sensitive information to leverage its attack. We discovered log files from the attacker’s infrastructure containing

numerous IP addresses of more potential victims. Our research revealed multiple overlaps with old Kimsuky malware: this group has used its original malware code and scripts for a long time. However, the infection scheme has been evolving continuously. In this instance, a legitimate blog service was used to reduce suspicion; and infection stages were added to verify the victims. One interesting thing we observed in our research is that the actor used a compromised computer in a victim's network as its malware testing environment.
Lazarus is currently one of the most active groups, with the defense industry and financial institutions being the primary targets. As a result of our continuous endeavors to track this actor's activity, we have now discovered two additional operations from the group.
DeathNote, which is under the Lazarus umbrella, is a sophisticated malware cluster actively used by this group, and most recently observed when the Lazarus group attacked a software vendor and think-tank. Since then, we have discovered several entities in South Korea that were infected with similar malware in February. However, the infection scheme was slightly updated in these cases as the actor added wAgent malware in its delivery procedure.
Since late 2021, we have been detecting new attack campaigns from the SideCopy threat actor, which we believe to be a subgroup of TransparentTribe. The attacks targeted Indian and Afghan victims and, while some of the attacks had a more complicated attack chain, they all involved sophisticated techniques, such as different stages of HTA scripts with encrypted/obfuscated malicious payloads, memory-resident malware and, in most cases, DLL side-loading to execute the NightFury backdoor. We have identified a number of scenarios among these attacks that either started from a ZIP archive containing a malicious LNK file or a Word document with a malicious VBA macro. The final payloads of these attacks include Crimson RAT, ReverseRAT and the NightFury backdoor. The attackers used compromised websites to host the initial HTA scripts and their own servers as C2 for different backdoor and RAT samples, as well as download servers for downloader modules. Our private report provides an analysis of the attack infrastructure and the malware components involved in these attacks.
We discovered a highly active campaign, starting in March 2022, targeting stock and cryptocurrency investors in South Korea. Based on the domain naming scheme, we call this campaign NaiveCopy. The actor used cryptocurrency-related contents or complaints from law enforcement as lure themes. The infection chains involved remote template injection, spawning a malicious macro which starts a multi-stage infection procedure making use of Dropbox. Finally, after beaconing the victim's host information, the malware attempts to fetch the final stage payload. Luckily, we had a chance to acquire the final stage payload, which consists of several modules for exfiltrating sensitive information from the victim. As a result of analyzing the final payload, we found additional samples used a year ago. At that time, the threat actor used an Excel document and Windows executable file for the initial infection vector. The final payload used in 2021 had different structures, but it had many overlaps with previous versions. Based on this finding, we confirmed that this campaign had lasted for at least a year. We worked closely with KrCERT and ISP vendors to shut down the attacker's infrastructure, preventing additional infections. In terms of attribution, we can't find any precise connection to known threat actors, though we do believe that they are familiar with the Korean language and utilized a similar tactic to steal the login credentials for a renowned Korean portal that has been used by the Konni group.
Starting from January 2022, TransparentTribe (aka PROJECTM and MYTHIC LEOPARD) started new waves of attacks against government workers in India to perform espionage activities. The threat actor launched different attacks in which targets were lured into visiting fake websites designed to appear as official repositories for Kavach, a two-factor

authentication application mandatory for some government employees in India. People were typically tricked into downloading and executing fake installers that validate the victims and download a new Trojan that we have dubbed AREA51. This Trojan is used to perform another validation and recognize relevant victims to infect with other malware. During our investigation, we saw the attacker use AREA51 to deploy a new version of MumbaiRAT, a new CrimsonRAT variant and PeppyRAT. We also discovered a fake website used to distribute a fake Kavach installer for Linux. The implant is a simple downloader that downloads and executes Poseidon, a post-exploitation tool for Linux and macOS that can be used with the Mythic post-exploitation framework.

Other interesting discoveries

The malicious disruption of KA-SAT-based internet services in February may have been an attempt to specifically hinder communications of Ukrainian military forces and security services. We were able to identify several configuration and sensitive information disclosure vulnerabilities that would have allowed an attacker to gain access to private Viasat management network segments, as well as to remotely execute code or change configuration on CPE systems. We analyzed the publicly available wiper malware, CosmosWiper, that was submitted to an online multi-scanner service on March 15; and we believe with medium-to-high confidence that it has been leveraged to disrupt some KA-SAT customer CPE systems. Researchers believe that the malware used to wipe the Viasat satellite broadband modems could be linked to VPNFilter10.

In February, we discovered a new SilentMarten campaign targeting Kyrgyzstan government entities. This was the first time we had observed the technique of putting shellcode into Windows event logs, allowing the “fileless” last-stage Trojan to be hidden from the file system. The dropper saves the shellcode into the Key Management System (KMS) event source’s information events with a specific category ID and incremented message IDs. Another technique is the use of a C2 domain name that mimics a legitimate one. The name, “eleed”, belongs to a regional ERP/ECM product, that really is in use on target systems. The threat actor takes their initial reconnaissance into consideration when developing the next malicious stages. They provided a lot of anti-detection decryptors, using different compilers: Microsoft’s cl.exe, GCC under MinGW and a recent version of Go. They also decided not to stick to just one last-stage Trojan: there are HTTP and named pipe-based ones too. Along with the aforementioned custom modules, several commercial pen-testing tools were used, such as Cobalt Strike and NetSPI (ex-SilentBreak). In September 2021 we observed SilentBreak’s toolset, but in other regions – the Middle East and North Africa. Attention to the event logs isn’t limited to storing shellcodes. Droppers also patch Windows Native API functions to make the infection process stealthier. Also, some modules are signed with a Fast Invest digital certificate; we believe this was issued by the threat actor, because our telemetry doesn’t show any legitimate software signed with it beyond the malicious code used in this campaign.

We recently identified SessionManager, a poorly detected malicious IIS module that, starting in late March 2021, has been used against NGOs and government organizations in Africa, South America, Asia, Europe, Russia and the Middle East. We believe, with medium-to-high confidence, that the module has been deployed thanks to previous exploitation of ProxyLogon-type vulnerabilities on Exchange servers. We believe, with low confidence, that SessionManager might be used by the GELSEMIUM threat actor, based on an overlap in victimology and the use of OwlProxy.

We first reported DeathStalker’s VileRAT campaign in August 2020. While continuing to track associated activities, we noted that the threat actor still regularly updates its malware and preceding infection chains. DeathStalker’s main tactics remain consistent, but the threat actor is continuously making efforts to evade detection. We recently identified new

infection documents that ultimately deliver updated VileRAT samples, and provided fresh indicators and knowledge about these campaigns in a private report.

In recent years, the number of hack-and-leak incidents has steadily increased, with this becoming a popular tool for both APTs and cybercriminals. In the case of APTs, these leaks are mainly used to tarnish a target's image and compromise their reputation. For instance, back in 2016, Democratic National Committee chairwoman Debbie Wasserman Schultz resigned following an extensive email leak from WikiLeaks. For cybercriminals, leaks are typically used in conjunction with ransomware attacks, where a company's data is encrypted and held for ransom. Since the beginning of the war in Ukraine, various cybercriminal groups (e.g., Conti) have expressed their support for the parties involved in the conflict, muddying the separation between state-sponsored and cybercriminal operations. Similarly, we have seen a spike in the number of hacktivist activities related to the conflict, ranging from DDoS attacks to doxxing and hack-and-leak operations. We recently came upon several such operations that are interesting in the context of the Russo-Ukrainian war. This report looks at several websites likely associated with APTs and hacktivists.

In a private report that differs somewhat from our usual format, we published a comprehensive review of modern ransomware Techniques, Tactics and Procedures (TTPs). The report combined the efforts of multiple teams at Kaspersky – our Threat Research Team, the Global Emergency Response Team (GERT) and Global Research and Analysis Team (GReAT). We also used best practices from the Escal Institute of Advanced Technologies (SANS), the National Cybersecurity Centers and the National Institute of Standards and Technology (NIST). The report draws on our statistics to select the most popular groups, analyzes in detail the attacks they have perpetrated, and employs data described in MITRE ATT&CK to identify a large number of shared TTPs. By tracking all the groups and detecting attacks, we see that the core techniques remain the same throughout the cyber kill-chain. The attack patterns thus revealed are not accidental, because this class of attack requires the hackers to go through certain stages, such as penetrating the corporate network or the victim's computer, delivering malware, further discovery, account hijacking, deleting shadow copies, removing backups, and, ultimately, achieving their objective.

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 Q2 2022:

•Geo-politics continues to be one of the drivers of APT development. Unsurprisingly, we continue to see attacks centered around the war in Ukraine. We have seen a spike in "hacktivist" attacks, ranging from DDoS attacks to doxxing and hack-and-leak operations. Cybercriminals are also seeking to exploit the conflict. Moreover, we have also seen threat actors exploit the war as a theme to lure potential victims into running malicious code.

•As underlined by our report on the NaiveCopy campaign targeting stock and cryptocurrency investors in South Korea, financial gain remains one of the ongoing motives behind APT attacks.

•In our APT annual review 2021, we highlighted two cases where attackers had developed UEFI implants; and predicted the further growth of low-level attacks. This quarter we reported yet another malicious UEFI component, CosmicStrand.

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.

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.