.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Braganca, Maschenka

Pocket Spies. Advanced Persistent Espionage Campaigns Go Mobile

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3/2018), 19-29.

doi: 10.7396/2018_3_B

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Braganca, Maschenka (2018). Pocket Spies. Advanced Persistent Espionage Campaigns Go Mobile, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 19-29, Online: http://dx.doi.org/10.7396/2018_3_B.

Online publiziert: 12/2018

Pocket Spies

Advanced Persistent Espionage Campaigns Go Mobile

Mobile advanced persistent threat (APT) campaigns are simply the natural evolution of an attack type. It was just a matter of time before attackers would focus on exploiting a device that is so critical to our digital life. Threat actors always try to be ahead of the game, and advancements in tactics, techniques and procedures (TTPs) used shouldn't come as a surprise. While we notice massive changes in the way malware is written, developed and new techniques pioneered that help leave infiltration unnoticed (hardware embedded malware or fileless malware, etc.), little attention has been paid to the mobile front, although it certainly is the one electronic device no one can function without. Over the past year, we have been observing how attackers use a device that is so ubiquitous in everyone's daily life, together with the sophistication of serious malware authors that aren't just trying to siphon off a few bucks. This has given rise to what some security research classify as a new category of advanced attacks that some even call "Mobile APTs" with a clear nation-state component. APT actors have traditionally operated on PC platforms, but are now rediscovering the mobile segment through evolving tactics. This article will explore these "mobile APTs" and place them in the context of recent changes in the general threat landscape.

MASCHENKA BRAGANCA,
Sr. Program Manager of threat research communications with a security firm.

UNINTENTIONAL SPY GADGETS

Our entire private and professional digital life is happening on the mobile device, from emails to contact lists to mobile banking and security tokens that are required for accessing sensitive information on our primary device, such as the work PC. We carry it around everywhere and read and hear about cyber-related intrusions every day. And we still barely use proper cybersecurity[1] on our mobile devices, even at the executive level.

Threat actors are evolving their tactics and exploiting less-expected avenues for maximum effect. The examples that will be discussed in this article illustrate the introduction of mobile as a key component of the APT world these days, and show how threat actors are moving toward multi-platform APTs. With so-called "mobile APTs", mobile devices are becoming not just targets for espionage campaigns with a political context, but will also very likely become the primary target for any type of intrusion for enterprises as well.

Infiltrating an individual's device or a company's doesn't just serve the purpose of stealing data or intellectual property. Many of these highly resourceful, sophisticated threat actors utilize this to leverage a foothold in any company's infrastructure to later target government organizations and/

or critical infrastructure. Leveraging the mobile devices of the individuals targeted is now an additional or even quicker pathway to accessing the enterprise environment.

As the threat landscape changes and evolves, it simultaneously creates a dynamic of overlap between threat actors and a blurring of lines between traditional roles and modi operandi. Espionage (or more broadly, intelligence) in its essence used to refer to the ways in which "sovereign powers create, exploit and protect secret advantages against other sovereignties" (Warner 2014, 4). The tools of the trade used for this purpose used to be the nation-state actor's prerogative. Now these same tools are suddenly widely available to a number of threat actors with various – in part, conflicting – agendas.

THE DAWN OF THE MOBILE ESPIONAGE CAMPAIGNS

Researchers have been observing mobile malware campaigns that are highly targeted, using social network services and popular apps to deploy the malware (typically spyware) onto the mobile device. The trojanised apps function like the legitimate apps and fulfil their regular functions, but they will divert the user to download a payload. The difficulty lies in figuring out whether an app is legitimate or masquerading. How do you establish anomalous behaviour? How did the mobile apps make it into an official app store? The malicious apps are designed to pass the initial screening and be available in the official app store by bundling most of the malicious functionality into second-stage components that are downloaded only after victims have installed the rogue apps and interacted with them.

In the following passage, a few recent examples of mobile espionage campaigns will be described to illustrate the methods and tactics being used by the various threat actors that have been transitioning and/or expanding into "mobile APTs". Most of these cases use a combination of run-of-the-mill phishing techniques (either via social media, straightforward text messaging or chat apps) to drop the payload on the victim's device, mostly by prompting the user to download an app. Looking through indicators of compromise (IOCs) and malware analysis, the different research teams often thought what they were seeing were low-level threat actors employing relatively simple cyber-espionage tactics probably for criminal endeavours, but were surprised to discover more purposeful and persistent behaviours in most threat actors. Also, while some incidents initially seemed incidental, some of the campaigns were operational for a lot longer than initially expected.[2]

Pegasus

Profile:

- Discovered in: August 2016.
- Functionality: It's functionality can be broken down as follows: Starting with a phishing scheme via SMS, the attack relies on the human weakness. Through SMS, the user is prompted to click on a link, which starts the browser and loads a page. Pegasus exploits three critical iOS zero-day[3] vulnerabilities that form an attack chain that subverts even the tightly controlled security of the Apple Store and environment.[4] Once in the device, malware is installed in order to perform the assigned tasks (gathering information, etc.) and maintains persistence to ensure that it stays installed. Pegasus uses encryption to remain stealthy and fly under the radar of traditional security detection tools.
- Threat Actor: The security researchers identified NSO Group behind these operations, connecting it to a product that

NSO Group sold as "Pegasus solution". NSO Group sells surveillance technology like weaponized software that targets mobile phones and is often characterized as a "cyber-arms dealer". NSO Group was operating on behalf of various clients, among whom were also nation-state clients.

- Victims and Targets: The goal of Pegasus was espionage with large-scale geographical reach. Among the victims identified in early reports on this attack were political dissidents and human rights defenders based in UAE, Mexico, Uzbekistan and other countries across the world, but the type of malware used here indicates that any high-value victim could be targeted, in political and corporate settings alike.

Security firm Lookout describes the Pegasus campaign, discovered in 2016, as "the most sophisticated attack" (Citizen Lab and Lookout 2016) they have yet seen on any endpoint (not just on mobile). Like other similar mobile spyware, it takes advantage of the combination of the unique features available with a mobile device (such as 24/7 WiFi, 5G, microphone, video, contact lists, applications, email, SMS, messaging, GPS, etc.). What is special in this case is that in this attack the adversary can effectively jailbreak an iOS device, exploiting three iOS zero-days, and then remain under the radar spying on its victim. A tailor-made exploit sequence for iOS devices (like this one based on not one but three zero-days) is typically very costly because it is relatively difficult to achieve. Threat actors will typically use this kind of targeted and expensive spyware to attack "high-value" individuals who give them access to sensitive information. In political and corporate settings alike, the amount of sensitive information that is being carried on or accessed from mobile devices clearly highlights the susceptibility to high-level (corporate) espionage.

ViperRAT

Profile:

- Discovered in: February 2017.
- Functionality: ViperRAT has been specifically designed to exfiltrate information of high value from compromised devices. It comes in two variants. As is often the case, social engineering is at the beginning of this attack. The victims were contacted via social media by good-looking women from Western countries to lure the user into downloading a trojanised app disguised as a chat or game app. This app will do some basic profiling of the device and then download the second component/variant of ViperRAT that has a more comprehensive surveillance and intelligence gathering function. It includes a dropper which, in order to be installed, requires the user to grant permissions and can then exfiltrate image data and audio content and use the device camera. In 2018, samples belonging to this mobile malware family resurfaced as chat apps in the Google app store (Flossman 2018; Flossman 2017). ViperRAT has been operating since late 2015 and was likely used a test application at first.
- Threat Actor: There are many theories about potential threat actors, but no conclusive evidence that could point toward one specific actor with a fair amount of certainty. What can be said is that research indicates the actor behind it has a well-developed cyber-capability as well as an active interest in the geopolitics of the Middle East.
- Victim and Targets: Likely espionage against Israeli Defense Force (IDF) personnel.

GnatSpy

Profile:

- Discovered in: December 2017.
- Functionality: The distribution vector starts with sending malicious files containing the malware directly to users with legitimate sounding titles such as "Android Setting" or "Facebook Update". The goal is to steal images, messages, contact information, call history, and other sensitive data from infected devices. The research (like shared C2 domains) suggests that GnatSpy is likely an improved version of the so-called VAMP malware by the same threat actor, indicating that these threats are connected.[5] However, GnatSpy has a much more modular set-up as opposed to VAMP, which suggests that the developer must have knowledge in good software design compared to previous authors. GnatSpy uses Java annotations and reflection methods to evade detection and encrypts its C2 server (Xu 2017) and can, in addition to the images, text messages, contacts and call history that VAMP would remove, also pull information from the infected device, such as battery, memory and storage usage, and SIM card status.
- Threat Actor: APT-C-23 (also known as "Two-Tailed-Scorpion").
- Victim and Targets: Mainly countries in the Middle East.

GnatSpy, detected by Trend Micro in 2017, was likely developed by the threat actor APT-C-23 (or "Two-Tailed-Scorpion") that was also behind the VAMP malware. GnatSpy is evidence to the fact that some threat actors are remarkably persistent even if their activities have been exposed and documented by researchers in the past. The threat actor is not just continuing its activities, but really improving their technical capabilities.

AnubisSpy

Profile:

- Discovered in: December 2017.
- Functionality: AnubisSpy uses a "watering hole" technique. It comes disguised as an app, published on Google Play and third-party app stores, and was even signed with fake certificates.[6] It uses socio-political themes as social-engineering hooks for phishing attacks with the goal of stealing messages (SMS), photos, videos, contacts, location, email accounts, calendar events and browser histories, and to take screenshots and record audio, including calls. The collected data is encrypted and sent back to the C2 server. It is also constructed to self-destruct to cover its tracks.[7] The research suggests that it might be linked to the Sphinx threat actor group that also employs PC/desktop-targeting malware, based on shared file structures and C2 server and seemingly has expanded the platform being served (Xu/Guo 2017). AnubisSpy's first activity dates back as early as April 2015.
- Threat Actor: APT-C-15 (also known as "Sphinx").
- Victim and Targets: Mostly, the victims have been linked to countries in the Middle East. The treat actor is likely Sphinx, targeting government and military organizations.

AnubisSpy is one of the more devious mobile espionage malware types, coming disguised as a legitimate app, and was available on the Google app store.[8] It also marks the current trend of a transition in threat actor tactics from the PC to the mobile platform.

DarkCaracal

Profile:

- Discovered in: January 2018.
- Functionality: DarkCaracal also starts with a simple phishing message like "How are you?" or trojanised Android apps disguised as secure chat apps to direct potential victims to the watering hole. It retains full functionality, exfiltrating sensitive data without the victim noticing. Victims granted attackers the right to access the private data by granting permissions when they installed the app. DarkCaracal's attack profile shows that the threat actor is operating on multiple platforms. The mobile component of DarkCaracal was one of first observed glb espionage campaigns with global reach, according to security researchers (Electronic Frontier Foundation and Lookout 2018).
- Threat Actor: The first attack using DarkCaracal that was identified and analysed seems to emanate from the Lebanese General Directorate of General Security (GDGS) according to security researchers. The malware has been around since early 2012.
- Victims and Targets: Among the targets connected to DarkCaracal were journalists, activists, government officials, military personnel, financial institutions, defence contractors and other individuals and groups in the US, China, Germany, India, Russia, Saudi Arabia, South Korea and within Lebanon. The goal seems to have been acquiring enterprise intellectual property as well as personally identifiable information.

Not every campaign necessarily utilizes sophisticated tools such as iOS zero-days such as in the case of Pegasus. There is evidence for surprisingly low-budget options as well. The same firm that discovered DarkCaracal indicated it initially looked like a criminal endeavour but turned out to be traceable to a nation-state intelligence agency. The tools employed for this campaign are not sophisticated and simply require luring the user into granting certain application permissions (Perlroth 2018). This threat actor is the exact opposite of Pegasus, which shows us the entire spectrum of the espionage game. Mobile platforms are appealing to APT actors because they have less security measures or are left unsecured by users, and are often cheaper for attackers to work around.

Zoopark

Profile:

- Discovered in: May 2012.
- Functionality: Zoopark spreads via two main distribution channels. 1) drive-by downloads (watering holes)[9] from websites and 2) it mimics the chat app Telegram. Several samples observed reportedly mimicked a voting application for Iranian Kurdistan. Zoopark has been around at least since June 2015. Four variations are claimed to have been found that also show gradual improvements in their functionalities. The latest version is the most advanced and can exfiltrate a wide range of data, including contacts, GPS location, text messages, call audio, key logs and browser data (among others); it also has backdoor functionality that allows it to make phone calls, send messages and execute shell commands. As is often the case, it begins with a watering hole attack leveraging Telegram channels and compromised legitimate websites.
- Threat Actor: The current research does not indicate a specific threat actor.
- Victims and Targets: Among the victims identified were individuals in the Middle East e.g. Iran, Morocco, Egypt, Jordan

and Lebanon, but also political organizations such as United Nations Relief and Works Agency for Palestine Refugees (UNRWA).

Zoopark trojan spyware is an example of mobile spyware that is able to remotely control a device and steal all sorts of confidential information from it. It was discovered by vendor Kaspersky Labs, who state that they found four different iterations of the Zoopark malware apparently developed between 2015 and 2017, each one expanding on the previous (Kaspersky 2018). The latest version shows massive improvement and advancement in comparison to its predecessors, which only had basic functionality[10] and incrementally added features. This leads the research team to believe that the threat actor might have outsourced development or purchased from specialist vendors. There is a huge (black) market for specialist (surveillance) tools and it is not an uncommon practice today to purchase them instead of going through the process of developing in-house.

RedDawn

Profile:

- Discovered in: May 2018.
- Functionality: RedDawn uses multi-component malware. The attackers planted three unreleased beta apps in Google Play. They have legitimate sounding content such as food and security, but behind the scenes steal data like contacts, messages, call recordings and photos, and have remote command capability and additional executable (.dex) files from a C2 server. After being installed, the malware uses e.g. Facebook to infiltrate the contact list and prompt users to install the app (through phishing techniques). RedDawn has been reportedly operating since 2017.
- Threat Actor: The attacks have been associated with threat actor "Sun Team" hacking group. Further investigation has shown that there have been multiple versions of the malware. It seems Sun Team's only goal is to extract information from devices, since all of the malwares are spyware.
- Victims and Targets: For the most part, victims are Korean-speaking users, possibly North Korean defectors and journalists.

The most recent case is RedDawn. The campaign was discovered by vendor McAfee in May 2018 (Min 2018b). It is the second campaign by this threat actor within this year; the first was targeting North Korean defectors and journalists using a chat app as a delivery vector. According to the analysis, the apps used in this campaign are multi-staged and typically use multiple components, starting with a reconnaissance phase that sets the foundation for the next steps (Min 2018a).[11] The threat actor seems to be using modified (publicly available) exploits which, according to McAfee, might indicate a lack of in-house technical expertise.

WHAT MAKES THIS NEW KIND OF MOBILE ATTACKS AN "ADVANCED" THREAT?

When it comes to describing cyber attacks or cyber operations, the word sophisticated is used very quickly. But not every operation or campaign is "advanced" or even "sophisticated". Does the anatomy of the attack classify mobile malware as an APT rather than just another piece of malware that can steal information or disrupt a system? Very often this marks a marketing tactic by vendors, but in some cases, adding this attribute tells a bit of the story of method or technique that is not entirely well understood at the time it has been discovered.

The term "Advanced Persistent Threat" has a history of its own and its use in describing specific attacks is not undisputed among security researchers (Bejtlich 2010). In very simple terms, the term "advanced persistent threat" originated from the US Air Force around 2006 and denotes an attack where the adversary systematically targets and infiltrates a system and remains there for an extended period of time without being detected. It originally and, perhaps most significantly, meant an attack by a nation state. Advanced persistent threats typically have several phases, which often leads to confusion with so-called "targeted attacks" because of the many shared attributes – such as selective targeting of victim organizations, maintaining a foothold in the environment for future use and control, technical sophistication[12] and many others (Genes 2015). Not every advanced threat or well-designed piece of malware necessarily emanates from a nation state actor. There is a host of other skilled threat actors from which to choose.

Quelle: Braganca

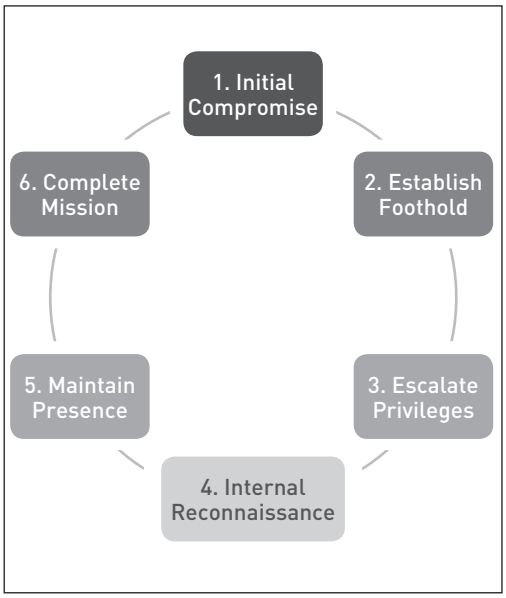

Fig. 1: Typical APT/targeted attack lifecycle

Most of the attacks that follow this pattern are targeted attacks, and this also applies to the campaigns discussed before. In some cases, the nation-state aspect might justify the APT terminology but in some cases the level of "sophistication" might be questionable. In fact, the attribution often goes the other way round – after looking at the samples, many threat actors have been identified as APT actors that have started adding the mobile vector to their previous PC-targeting operations. One example is the famous Lazarus group[13] that was found utilizing mobile operations as part of their repertoire (Han 2017), or the aforementioned Sphinx group.

When we look at the modus operandi of many of these groups, it usually begins in quite the unspectacular way with a simple email or SMS, which very often is one of the most effective malware delivery mechanisms. Only at the infiltration stage do we see what tools are really being used and what can be achieved with them. As the cases discussed show, there is a broad range of tools with varying degrees of sophistication – from low-budget trojans to pre-made toolkits to costly zero-day exploits. Perhaps the most significant factor is that these actors, who have been operating for many years while going unnoticed (and those that were discovered and reported on), continue to improve their tactics and procedures.

THREAT ACTORS AND THE EVOLUTION OF METHODS AND TACTICS

APT attacks are the handiwork of threat actors with substantial resources and specific motivation, and that description typically fits nation states with a strategic interest. APTs have been around for decades. It is not really surprising to see APT threat actors increasingly adopting the mobile platform. At the beginning stage, the mobile operations were most likely offshoots, extensions, or separate but related opera-

tions of their desktop/PC counterparts. They are now well underway to becoming the primary attack vector.

In today's threat landscape, we are faced with a plethora of threat actors, from script kiddies and hacktivists with a political motive to cybercriminal syndicates and nation states as well as combinations of these different groups that occasionally work together. A factor that is contributing to the current threat landscape is also directly related to the major leaks we have seen in past years (Vault7, Shadowbrokers, et al). Those leaks have led to a surge of cyber weaponry on the black market, which now makes very sophisticated tools available for purchase. Any threat actor can leverage advanced weaponry and doesn't need to painstakingly develop and test it. Naturally, the new market offerings also create new actor profiles and enrich these groups with capabilities that before would have been impossible. Among these are nation states previously without significant offensive or high-tech capabilities and/or resources who are now taking the stage as they are able to access the tools necessary for such (wide-ranging) espionage campaigns. As history has shown in other instances, this is a result of the proliferation of a highly unregulated type of good and introduces new dynamic geostrategic constellations.

The other side of the diversity in threat actors is that nation states can practically "outsource" the work to vendors that offer these tools and services. This has many advantages: A nation-state actor can on the one hand pass off the time and investment required for the development of effective espionage tools (especially smaller states), but more crucially avoid incrimination and attribution for certain interferences, and publically distance themselves from APTs.

WHAT MAKES MOBILE ESPIONAGE SO ATTRACTIVE AS A TARGET AND WHAT IS DIFFERENT?

The "smartphone" is the perfect pocket spy tool due to its features and its ubiquity in our personal and professional lives. The modern workforce is reliant on these devices to be more flexible and BYOD culture in the corporate world has brought its own set of concerns. There also is no shortage of sensitive information stored on a smartphone and it functions as a control node in our digital life, hosting not just volumes of interesting data, but options to gain access to enterprise/other sensitive networks.

Mobile espionage is not just an evolution in cyber techniques, but the logical continuation of old-school espionage techniques (wiretapping to listen in on conversations, HUMINT aspects of following individuals and their transactions, etc.) All this can be very conveniently accomplished since everyone basically volunteers to be exposed to all these options by carrying a phone with them wherever they go. Using mobile devices for longer-term espionage campaigns is a step in the natural evolution.

Using mobile platforms for cyber-crime or data theft is not new. The mobile attack vector has been known for years. But we like to forget that this little handheld device we use for everything is the easiest way to access anyone's entire digital life. In 2017, the mobile landscape was most notably riddled by a surge of (mobile) ransomware, the usual vector; banking trojans are still active, and mobile threats are joining in on cryptocurrency mining. One slightly disturbing pattern is that legitimate services such as the Google Play Store have been abused at a rapid pace. These threats are harder to detect because they hide behind legitimate and encrypted traffic and seem-

Quelle: Braganca

CAMPAIGN	DISCOVERED IN	OPERATING SINCE	VICTIM/TARGET	THREAT ACTOR	SCALE/SCOPE
Pegasus	August 2016		Various high-value individual, among the first were political dissidents in UAE, Mexico, Uzbekistan etc.	NSO Group, on behalf of various clients, among which there are nation-state clients	Worldwide
ViperRAT	February 2017	Since late 2015	Israeli Defense Force (IDF) personnel	unclear	Middle East
GnatSpy	December 2017		Countries in the Middle East	APT-C-23 (also known as "Two-Tailed-Scorpion")	Middle East
AnubisSpy	December 2017	As early as April 2015	Countries in the Middle East; it is likely Sphinx has targeted government and military organizations	APT-C-15 (also known as "Sphinx")	Middle East
DarkCaracal	January 2018	Since early 2012	From USA to China, Germany, India, Russia, Saudi Arabia, South Korea and within Lebanon; enterprise Intellectual property as well as PII are targeted	Possibly the Lebanese General Directorate of General Security (GDGS), according to the security firm	Global scale, very broad span, 21+ countries, easily 2,000 victims
Zoopark	May 2018	At least June 2015, four variations claimed found	Countries in Middle East e.g. Iran, Morocco, Egypt, Jordan and Lebanon, political organizations such as UNRWA	unclear	Middle East; up to 100 victims (the low number indicates very selective targeting)
RedDawn	May 2018	2017	Korean-speaking users, likely North Korean defectors and journalists	Possibly "Sun Team"	Korean peninsula, around 100 victims

Fig. 2: What can smartphones gather

ingly normal app functionalities and are essentially exploiting the trust people have in the official app store and their screening measures (Trend Micro 2017).

CONCLUSION

The mobile threat surface is not new, but until recently, persistent and stealthy espionageware has been and still is an underrated problem for the mobile platform. While there might have been suspicion that these techniques are being used and possible on mobile devices, the scope was unclear and the cases described in this article often have shown more activity than initially thought.

Cyber threat actors are motivated to utilize every possible angle and tool available to them. The use cases highlight not just geopolitical constellations and shifts thereof, but also the evolution of new actors that (thanks to new opportunities and available resources) can operate side by side and increasingly contribute to a blurring and blending of the "old system", in which espionage was the stronghold of only nation-state actors. Instead, we are now seeing an overlap of various actors with varying motivations and goals that exist side by side or in mutual coexistence.

The focus on the mobile device also highlights the importance of a proactive security philosophy that is agile and fortifies the mobile frontier adequately. The mobile front doesn't allow for the luxury of analysing after the event to start thinking about defences. There isn't enough time. Perhaps one somewhat comforting aspect of the mobile mouse trap, however, is that almost every attack starts with a phishing attempt/social engineering message, and that is where the education would need to begin. Organizations and enterprises alike need to put in the resources to safeguard their employees' devices and deploy an effective mobile security strategy. Mobile

threat defence (MTD) is no easy task[14], seeing as the technology must cover applications, networks and device-level threats to iOS and Android phones as well as other handheld devices to be effective.[15]

The question is not about who will be using these options and exploiting a device as ubiquitous as a smartphone that we forget to protect, or how long it will take more attackers to realize, develop and exploit our negligence. The real question is what it will take to realize the full firepower of the little handheld device. Seeing the first use cases as a part of politico-strategic espionage is only the beginning. It won't be long until the same tactics will be adopted on larger scales and in enterprise environments. Securing the mobile endpoint must become an imperative not only to executives and businesses, but any user at this point. As the reliance on devices grows, the threat landscape is evolving. Mobile will be cybersecurity's next main frontier.

[1] *Proper securing of handheld devices would mean at the bare minimum secure practices and a cybersecurity solution installed on it.*

[2] *Some were around for many years, even dating back to 2011.*

[3] *Also called "Trident Exploit Chain".*

[4] *Apple fixed these three vulnerabilities in its 9.3.5 patch.*

[5] *Shared command/control infrastructure. The structure of GnatSpy is more modular and has additions such as receivers and services. The research team thinks this it indicates that it was developed by a skilled author with good software design practices.*

[6] *According to the researchers, there were seven apps found to actually be AnubisSpy. The apps have been taken down from the Google Play Store.*

[7] *It can run commands and delete files on the device, as well as install and uninstall Android Application Packages (APKs). The self-destruct command happens when expire_team is reached or on command. The position module retrieves the device's location and uploads it to the C2 in pre-determined intervals. According to the analysis, the position module was collecting and uploading information every ten minutes.*

[8] *According to the researchers, seven apps were actually found to be AnubisSpy, and they were in Arabic.*

[9] *Watering hole attacks/tactics are very often used as stepping stones to conduct espionage attacks. In watering hole attacks, the goal is not to serve malware to as many systems possible. The attacker instead infects a specifically chosen, usually well-known and trusted resource like a website that potential victims will eventually come to. The ultimate goal is to infect a targeted user's computer and gain access to the network, a common tactic in targeted attacks.*

[10] *Such as stealing contact and accounts registered on the victim device.*

[11] *The threat actor was using a popular chat app used in South Korea called "KakaoTalk" and social engineering techniques to drop the malware. However, the would-be-victim had to go out of their way to download it outside of Google Play.*

[12] *Technical skills mean the adversary can build custom exploits or find zero-days (undisclosed vulnerabilities) to take advantage of, building a very targeted piece of code that allows him to execute very specific processes without being detected.*

[13] *The Lazarus group has been found using mobile platform.*

[14] *Within an enterprise environment, the task of protecting mobile devices is now more difficult than in a traditional setting because employees exercise more control (often using personal devices), and it's impractical to try to police every individual, their movements and traffic – the solution must cover applications, networks and device-level threats to iOS and Android phones and tablets to be effective.*

[15] *Mobile threat defense means first and foremost detecting and then mitigating attacks on mobile devices e.g. by the means of scanning for risky apps and insecure WiFi networks. At a minimum, having a security app installed on the endpoint.*

Sources of information

Bejtlich, Richard (2010). What Is APT and What Does It Want?, Tao Security Blog, Online: https://taosecurity.blogspot.

com/2010/01/what-is-apt-and-what-does-it-want.html (16.01.2010).

Citizen Lab and Lookout (2016). Sophisticated, persistent mobile attack against high-value targets on iOS, Online: https://blog.lookout.com/trident-pegasus (25.08.2016).

Electronic Frontier Foundation and Lookout (2018). Dark Caracal. Cyber-espionage at a Global Scale, Online: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf.

Flossman, Michael (2017). ViperRAT: The mobile APT targeting the Israeli Defense Force that should be on your radar, Online: https://blog.lookout.com/viperrat-mobile-apt (27.02.2017).

Flossman, Michael (2018). mAPT ViperRAT Found in Google Play, Online: https://blog.lookout.com/viperrat-google-play (16.04.2018).

Genes, Raimund (2015). Targeted Attacks versus APTs: What's The Difference?, Online: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/?_=2.203871888.1652628051.1526942729-561099954.1526149945 (14.09.2015).

Han, Inhee (2017). Android Malware Appears Linked to Lazarus Crime Group, Online: https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/ (20.11.2017).

Kaspersky Lab (2018). Who's Who in the Zoo. Cyberespionage Operation Targets Android Users in the Middle East, Online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/03114450/ZooPark_for_public_final_edit.pdf (03.05.2018).

Min, Jaewon (2018a). North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk, Online: https://securingtomorrow.mcafee.com/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/ (11.01.2018).

Min, Jaewon (2018b). Malware on Google Play Targets North Korean Defectors, Online: https://securingtomorrow.mcafee.com/mcafee-labs/malware-on-google-play-targets-north-korean-defectors/ (17.05.2018).

Perlroth, Nicole (2018). Lebanese Intelligence Turned Targets' Android Phones Into Spy Devices, Researchers Say. New York Times, Online: https://www.nytimes.com/2018/01/18/technology/lebanese-intelligence-spy-android-phones.html (18.01.2018).

Trend Micro (2017). 2017 Mobile Threats Landscape, Online: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-mobile-threat-landscape.

Warner, Michael (2014). The Rise and Fall of Intelligence. An International Security History, Georgetown.

Xu, Ecular (2017). New GnatSpy Mobile Malware Family Discovered. Dec 18. https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/?_ga=2.252235849.1355112915.1526149945-561099954.1526149945.

Xu, Ecular/Guo, Grey (2017). Cyberespionage Campaign Sphinx Goes Mobile with AnubisSpy. Technical Brief, Online: https://documents.trendmicro.com/assets/tech-brief-cyberespionage-campaign-sphinx-goes-mobile-with-anubisspy.pdf (19.12.2017).

Further literature and links

Goodman, Marc (2015). Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, New York.

Johnson, Loch/Wirtz, James (2011). Intelligence. The Secret World of Spies, New York.

Laqueur, Walter (1985). A World of Secrets. The Uses and Limits of Intelligence, New York.

Krebs, Brian (2014). Spam Nation. The Inside Story of Organized Cybercrime – from Global Epidemic to your Front Door, Naperville, IL.

Naor, Ido (2017). Breaking The Weakest Link Of The Strongest Chain, Online: https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/ (16.02.2017).

Washington Post (2012). Zero Day – The Threat in Cyberspace. A Washington Post Special Report, Online: http://www.washingtonpost.com/investigations/zero-day.