Tampere University

Akseli Piilola

ZERO DAYS

A small study into the usage of zero-day vulnerabilities and exploits by law-enforcement agencies

Faculty of Information Technology and Communication Sciences
May 2021

ABSTRACT

Akseli Piilola: Zero Days
Tampere University
May 2021

A Zero-day vulnerability or exploit, or just a zero-day, is a previously unknown and therefore unfixed security vulnerability in software or hardware. Since there is little or no way to prepare for zero-days, using them is usually an extremely effective way to compromise a system. Using zero-days can also provide governments and law enforcement agencies a meaningful way to access seized devices, intercept communications and bypass data protections. However, these vulnerabilities can be found and exploited by other, non-intended actors. Therefore, it should be in the interests of the general public to be able to construct an up-to-date situational image about the current state of such exploits in government control, and to be able to reflect that against each one's own threat model. By combining leaked information from various known hacks & whistleblowers with previous academic research, public documents, and field observations I tried to combine a somewhat reliable situational image and provide meaningful results of the capabilities and usage of such tools by government level actors. The study shows clearly that almost any sophisticated government can have access to zero-day exploits for at least the most popular commercial software & hardware. However, exploits affecting open-source projects seem to be less common and therefore more expensive. While law enforcement agencies might be cracking mobile phone protections on a daily basis, they can also save the more serious exploits for high profile targets. This is controlled by supply and demand, since no agency wants to find themselves in a situation where they have burned through all their exploits and a high-profile target needs to be taken down. It should always be assumed that an unknown exploit exists for any given system, but the exploits are very specific to certain system and/or versions, and the adversary is much more unlikely to have exploits ready for multiple different targets. Therefore, I recommend using at least two or three separate security controls and a system that will not be compromised unless all the controls are bypassed. Reflecting the key results, every individual's and organization's own threat model can give them a very good indicator whether they should need to worry about being targeted or not.

Key words and terms: Backdoors, zero-days, vulnerabilities, exploitation, governments, advanced persistence threat

1. Introduction

Throughout the history governments have always tried to find ways to break into the secrets of both their citizens and other governments. In the information era this usually means breaking into digital devices and data. Of course, most manufacturers and developers try to make their products secure – just because they are professionals who want to deliver a quality product, or at least to gain an edge against their competitors. This makes the breaking in process more difficult and requires governments to acquire technology specifically meant to break the built-in defenses of the target systems. This technology is not only developed by governments themselves, but also bought from private companies. By combining the capabilities of both the private sector and the government's own research, most governments are able to acquire a useful toolkit for breaking into digital devices.

Even though the methods are usually kept as secret as possible, at least a few people working with the tools need to have an in-depth knowledge about their capabilities and usage. Some of these people have voluntarily chosen to break the rules and reveal the details in to public. Private sector companies in turn are usually just trying to make profit, which means that they are eager to advertise their capabilities for potential buyers. Finally, in accordance with the rule of law, some documents during criminal investigations and prosecutions are to be made public. The material provided from these three separate fields of information can then be combined with prior academic research to form a meaningful conclusion.

Dozens of hacking tools and technologies available to both NSA and its allies were revealed when the agency's so called "ANT Catalog" was leaked to the public by Edward Snowden. Most of the tools used zero-day (previously unknown) security vulnerabilities to compromise target systems. Tools such as firewall & router backdoors were persistent enough to survive full OS reinstallation ["ANT Catalog" 2007]. Subsequent information leaks have also revealed details about tools produced by the private sector and sold to the government agencies ["Hacking Team" 2021; "Gamma Group" 2021]. Many private companies also market their tools and capabilities very prominently, even though they try not to disclose technical details about the actual exploitation [Magnet Forensics 2021; Cellebrite 2020].

Public records involving criminal cases and prosecutions reveal concrete observations about the technology used in practice. Even though this is something that government officials are understandably trying not to write down, by researching these cases carefully we can draw assumptions, which are then backed up by other available material to form conclusions. For example, studying a criminal case can reveal us which devices the in-

vestigators were able to break in to, and which tools they used. We can then cross reference this with other available data to draw assumptions whether an exploit was used, or if the target of the investigation just gave up the password voluntarily or used a bad password.

The criminal cases used as the source material of this study are from USA and Finland. Finland is used both for practical reasons (I live in Finland and the Finnish material is more easily accessible for me), and for legislative reasons. Finland is known for its high respect for individual's data protection laws and highly transparent public sector. In fact, according to Finnish law anyone can order just about any document from any public sector agency, excluding classified documents of course. Finland is also a financially stable and highly developed country with excellent technical competence. Lastly, Finland is in good terms with leading intelligence agencies in the USA and has been confirmed to cooperate with them in both ways ["R/0006083/13" 2013]. This makes Finnish criminal investigation a highly competent one, which in turn means that the documents obtained from such cases give us valuable and reliable information about the surveillance capabilities of modern law enforcement agencies in general.

Since almost all exploits are fixed sooner or later after they are made public, most of the actual techniques in source materials used are of course already outdated. However, we can still use the material to reflect the situation in early 2010's and form a clear picture of at least the interests, objectives and behavior of the exploit business. While old exploits are rendered useless and new are constantly developed, without any impactful legislative changes, the business itself is likely to stay the same, or follow the trend of other information technology businesses and grow even bigger.

2. Methods

Hacking Team was an Italian based information security company selling offensive intrusion and surveillance capabilities to governments & law enforcement agencies. In July 2015, the company was compromised by a hacker called "Phineas Phisher". Over 400GB of data was leaked online and made publicly available. Among that data was the source code of some of the company's products plus a comprehensive amount of email conversations between company's representatives and their clients ["Hacking Team" 2021]. Earlier the same hacker had compromised Hacking Team's competitor, the Gamma Group, leaking over 40GB of data ["Gamma Group" 2021]. These leaks offered a unique view into a private sector exploit business and its capabilities. They revealed some of the methods the groups used to obtain knowledge of previously unknown vulnerabilities, which were later developed into exploits. Besides the actual documents retrieved from Wikileaks' Hacking Team Email Archive [2015], multiple independent summaries of the leaks were analyzed to make sure that the source material and results are reliable. The

information in the above-mentioned summaries was also verified from the original data leaks wherever possible. Some of the summaries analyzed were the works of Boire [2012], Tsyrklevich [2015], Marquis-Boire at al [2014], and Hacked Team [2015] GitHub repository, which apparently contains at least some of the leaked source codes.

A 50-page classified document listing surveillance and exploitation technology available to United States National Security Agency (NSA) was made public in December 2013 in files leaked by NSA's former contractor Edward Snowden ["ANT Catalog" 2021]. This in turn revealed some of the capabilities of arguably the leading offensive cyber intelligence unit in the world, NSA's TAO (Tailored Access Operations). ["Tailored Access Operations" 2021]. Furthermore, the Snowden leak also revealed NSA's and other Five Eyes countries' capabilities at the time in numerous other documents. I retrieved the copies of the files from Snowden Archive [2021], an archive of all the documents leaked by Edward Snowden that have subsequently made public, and analyzed the technologies described in them to form a picture of a nation level actor's capabilities at the time.

To complete the results and form a reliable image of the situation today, I contacted multiple private companies known for developing and providing digital surveillance technology for law enforcement agencies. After all, the nature of a private company is to make money, which makes many of them eager to advertise their capabilities to potential buyers. Among the companies contacted were Cellebrite, Magnet Forensics and Grayshift. All known for developing digital forensics tools utilizing previously unknown vulnerabilities and exploits ["Cellebrite" 2021; "Grayshift" 2021; "Magnet Forensics" 2021].

Existing academic research on the capabilities of law-enforcement agencies regarding the usage of zero-day exploits is naturally limited. There is, however, case studies closely related to the subject. For example, Schmeh [2016] studied dozens of cases where law enforcement was up against encrypted devices. Even if the studies are not directly related to the subject, it is possible to draw credible and useful conclusions from the results. Earlier academic research has thus been taken into account, whereas the results would of course be more concrete if I also had access to restricted studies and material, other than almost a decade-old leaks. As far as I know, no existing public research compiling all these aspects to draw direct conclusions of the exploitation capabilities of the law enforcement agencies have been made.

Last I obtained materials from a selected few high profile criminal investigations to try and see if/when this kind of technology is used in practice. Material included cases from both USA & Finland and was limited to only the most serious criminal offenses, like ordering assassinations [USA v. Ross Willian Ulbricht 2013; "5680/R/8414/20" 2020; "R/20/3331" 2021], running drug enterprises [USA v. Ross Willian Ulbricht 2013; "5500/R/10198/19" 2019; "5500/R/25783/19" 2019; "R/20/406" 2021], and production

or distribution of child pornography [USA v. Eric Eoin Marques 2019; USA v. Ferrell 2015]. From this material I studied the possible or confirmed use of zero-day exploits as part of the investigative process. I acknowledge that the usage of such tools is almost never written down in documents, but it is still possible to draw reliable conclusions from the written facts. For example, this material lists the devices the investigator(s) were able to break into, even though it is not shared how exactly did they do it. If there is no other plausible explanation, then the usage of such exploits must be taken into serious consideration. Dozens of cases were combed through, but only the relevant cases are listed in the references.

3. Results

By inspecting the data leaks of HackingTeam and Gamma group it can be noticed that the market for zero-days is running and hot. There seems to be a constant demand for both the tools to be sold and the vulnerabilities/exploits to be bought for, in turn, more tools to be developed and sold. Dealers and buyers negotiate sales like with any other information technology. Scope and capabilities of the tools are clearly defined beforehand, of course, since the exploits usually work only on very specific models and software versions, which makes adding new features something that no vendor can easily promise [Tsyrklevich 2015]. Although the exploits available support vast number of target systems and versions, it's still only a small percentage of systems in use worldwide, except for mobile phones where vast majority of devices & version seem to be supported [Magnet Forensics 2021; Cellebrite 2020; Hacked Team 2015; "ANT Catalog" 2007].

There is usually only a short timeframe to utilize the zero-day until the manufacturer releases an update or a new model, after which the old exploits are usually rendered useless, and the whole process of finding vulnerabilities and developing exploits must be started from the beginning ["Zero-day" 2021; Bilge and Dumitras 2012]. Capabilities of the exploits vary from bypassing certain security features to full backdoor and remote-control toolset offered as a service for monthly price. At the time of the leak most exploits were not detected by any anti-virus softwares, or they deployed sophisticated anti-detection techniques ["Remote Control System Price Scheme" 2015; Marquis-Boire et al 2014; Boire 2012; Marquis-Boire and Marczak 2012; "ANT Catalog" 2007].

The above-mentioned observation can also be confirmed by contacting some of the vendors, and by reading their current product catalogues. For example, Magnet Forensics promises that their product can "acquire images from locked and unlocked iOS devices using GrayKey" and "bypass passwords on thousands of Android models with exploits and advanced extraction capabilities" [Magnet Forensics 2021]. In turn Cellebrite states that their tool can "determine passcodes and perform unlocks for all Apple devices run-

ning the latest iOS version" and "bypass or determine locks on all flagship Samsung devices and select Android devices" [Cellebrite 2020]. This is a heavy indicator that both companies are possessing knowledge of vulnerabilities not patched by the device manufacturer. Research also shows that both Apple and Samsung have actively been patching the vulnerabilities that law enforcement uses, or otherwise denied the requisitions for backdoors ["FBI – Apple encryption dispute" 2021; Magnet Forensics 2018]. This indicates that the vulnerabilities and exploits possessed by the companies are true zero-days, and that their existence is not known to the manufacturers, or otherwise the vulnerabilities would get patched.

By inspecting the Snowden leak and NSA's ANT Catalog it can be seen that at least the bigger law enforcement agencies are also actively doing research of their own. It is now known whether all the exploits come from inside the agency, or if some are bought from private markets. It is certain, however, that the agencies have at least possessed a wide range of previously unknown exploits for numerous commercial devices & software, and that they are willing to use them against their targets ["ANT Catalog" 2007]. There is also more recent evidence of law enforcement agencies being in possession of serious exploits, for example EternalBlue in 2017, which affected almost every Windows operating system at the time ["Eternal Blue" 2021]. This means that the agencies have no problem withholding knowledge of vulnerabilities that could compromise a significant part of the information systems used worldwide. Since there has not been any significant changes in legislation, it can only be assumed that the situation inside the agencies stays the same.

From the dozens of criminal cases I went through, in only two was it proved that an exploit utilizing previously unknown vulnerabilities was used [USA v. Eric Eoin Marques 2017; USA v. Ferrell. 2015]. In numerous other cases, however, mobile devices and laptops were opened without providing passwords. It seems that the only devices that the law enforcement was not able to break into were either from a smaller manufacturer, and not commonly used, or were using open-source protections such as TrueCrypt or LUKS -encryption [R/20/406 2021; R/20/3331 2021; 5680/R/8414/20 2020; 5500/R/10198/19 2019; 5500/R/25783/19 2019]. This is in line with the product catalogues of earlier mentioned companies providing offensive intrusion to said devices. The power of the open-source software against law enforcement was also noted in a study by Schmeh [2016], where it was concluded that TrueCrypt is the encryption software that the law enforcement is most often against to, and that they rarely succeed in breaking in. This indicates that at least the open-source software is surprisingly well protected against intrusion attempts.

4. Discussion

It is a bit of a mystery why there seems to be so many zero-days for mobile phones, while at the same time zero-days affecting a popular operating system are considered incredible rare, valuable and dangerous. It is possible be that zero-days for mobile devices are much less common than it seems, and that the actual cause of a high success rate of cracking the devices open is because people give up their devices voluntarily or use guessable passwords. The other explanation could be that the supply for new exploits for mobile devices is high and constant. Modern mobile phones are a very compelling target for exploit developers anyway since the demand for vulnerabilities/exploits is constant and global. It might just be that that's where the independent vulnerability researchers focus their resources, which in turn produces more vulnerabilities to the market.

Overall, it should always be assumed that an exploit exists for any given system, and one cannot blindly trust a single software or device to be secure. However, since the exploits target a very specific device and/or version, a meaningful protection could be achieved easily by relying on multiple individual controls. For example, one could use a somewhat modern mobile phone combined with open-sourced full disk encryption. In this case the phone itself would provide protection against hardware related attacks, while totally independent system provides protection on software level. System would have to be designed in a way where both security controls would need to be bypassed for the device to be fully compromised.

It should also be noted that the cost of the licenses to use surveillance systems developed by private companies seem to be relatively low ["Remote Control System Price Scheme" 2015]. This also makes them affordable for non-state actors, should the vendors decide to sell. Furthermore, many exploits are sold with license model where the license period and payments can be terminated early if, for example, the vulnerability is patched, and the exploit no longer works. This in turn makes the financial risk for the buyer much smaller [Tsyrklevich 2015]. This should be taken into consideration when reflecting the threat model against non-state actors.

This study could have been advanced much further by analyzing more criminal investigations, or by getting access to up-to-date restricted material. First option is difficult since many countries do not publicly disclose details in high profile investigations, and in a small country like Finland, those are quite rare to begin with. Second option is ruled out since it would make the study not accessible for general public, which it was meant to be. Maybe we will see more leaks of classified material in the future and can update the situational image based on those.

5. Conclusion

The study shows clearly that almost any sophisticated government can have access to zero-day exploits for at least the most popular commercial software & hardware. However, exploits affecting open-source projects seem to be less common and therefore more expensive. While law enforcement agencies might be cracking mobile phone protections on a daily basis, they can also save the more serious exploits for high profile targets. This is controlled by supply and demand, since no agency wants to find themselves in a situation where they have burned through all their exploits and a high-profile target needs to be taken down. It should always be assumed that an unknown exploit exists for any given system, but the exploits are very specific to certain system and/or versions, and the adversary is much more unlikely to have exploits ready for multiple different targets. Therefore, I recommend using at least two or three separate security controls and a system that will not be compromised unless all the controls are by-passed. Reflecting the key results, every individual's and organization's own threat model can give them a very good indicator whether they should need to worry about being targeted or not.

References

ANT Catalog. 2007. Part of the leaked documents by Edward Snowden. Archived: *http://web.archive.org/web/20201120095058/https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHe2cc.dir/doc.pdf*

Bilge, Leyla and Tudor Dumitras. 2012. Before we knew it: An empirical study of zero-day attacks in the real world. Archived: *https://web.archive.org/web/20210520203 246/http://users.umiacs.umd.edu/~tdumitra/papers/CCS-2012.pdf*

Boire, Morgan. 2012. Backdoors are forever: Hacking team and the Targeting of Dissent. Archived: *https://web.archive.org/web/20210308025832/https://citizenlab.ca/wp-content/uploads/2015/03/Backdoors-are-Forever-Hacking-Team-and-the-Targeting-of-Dissent_websitepdf.pdf*

Cellebrite. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210516060443/https://en.wikipedia.org/wiki/Cellebrite*

Cellebrite. 2020. Product overview. Archived: *http://web.archive.org/web/20201126005043/https://cf-media.cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf*

Eternal Blue. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210428054914/https://en.wikipedia.org/wiki/EternalBlue*

FBI – Apple encryption dispute. 2021. Wikipedia. Archived: *http://web.archive.org/web/20210225002135/https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute*

Gamma Group. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210506023248/https://en.wikipedia.org/wiki/Gamma_Group*

Grayshit. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210311100854/https://en.wikipedia.org/wiki/Grayshift*

Hacked Team. 2015. GitHub [Accessed 2021 May 12]. Online at: *https://github.com/hackedteam.*

Hacking Team. 2021. Wikipedia. Archived: https://web.archive.org/web/20210506185653/*https://en.wikipedia.org/wiki/Hacking_Team*

Hacking Team Email Archive. 2015. Wikileaks. Online at: *https://wikileaks.org/hacking-team/emails/*

Magnet Forensics. 2018. An In-depth Look at Different Password Bypass Options [Webinar; Accessed 2021 May 11]. Online at: *https://www.youtube.com/watch?v= FvJAF3SQ9b4*

Magnet Forensics. 2021. Magnet Forensics homepage. Archived: *https://web.archive.org/web/20210513165150/https://www.magnetforensics.com/*

Magnet Forensics. 2021. Axiom for law enforcement [Accessed 2021 May 17]. Online at: *https://go.magnetforensics.com/AXIOM-LE-Overview*

Marquis-Boire, Morgan and Bill Marczak. 2012. From Bahrain With Love. Archived: *https://web.archive.org/web/20210322191728/https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/*

Marquis-Boire, Morgan, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola. 2014. Police Story: Hacking Team's Government Surveillance Malware. Archived: *https://web.archive.org/web/20210502012600/https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/*

Remote Control System Price Scheme. 2015. Hacking Team [Accessed 2021 May 17]. Online at: *https://drive.google.com/file/d/0B2q69Ncu9Fp_TF9XeFF3VFUwa2s/ view.*

Schmeh, Klaus. 2016. Do Backdoors Actually Help Law Enforcement Catch Bad Guys? [Conference presentation; Accessed 2021 May 11]. RSA Conference 2016. Online at: *https://www.you-tube.com/watch?v=cYRlnyDOHDQ*

Snowden Archive. 2021. Canadian Journalists For Free Expression [Accessed 2021 May 12]. Online at: *https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi.*

Tailored Access Operations. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210501234716/https://en.wikipedia.org/wiki/Tailored_Access_Operations*

Tsyrklevich, Vlad. 2015. Hacking Team: a zero-day market case study. Archived: *https://web.archive.org/web/20210426085224/https://tsyrklevich.net/2015/07/22/* hacking-team-0day-market/

USA v. Eric Eoin Marques. 2019. Criminal Complaint. Archived: *https://web.archive.org/web/20201221142956/https://www.courtlistener.com/recap/gov.uscourts.mdd.247657/gov.uscourts.mdd.247657.13.1.pdf*

USA v. Ferrell. 2015. Search Warrant. Archived: *https://assets.documentcloud.org/documents/2165971/us-v-ferrell-affidavit-in-support-of-search.pdf*

USA v. Ross Willian Ulbricht. 2013. Criminal Complaint. Archived: *https://web.archive.org/web/20160505034302/https://info.publicintelligence.net/SilkRoadComplaint.pdf*

Zero-day. 2021. Wikipedia. Archived: *https://web.archive.org/web/20210519202127/https://en.wiki pedia.org/wiki/Zero-day_(computing)*

List of Finnish criminal cases & court decisions used in the study:

R/0006083/13. 2013. Oulu Police Department.

R/10198/19. 2019. Helsinki Police Department.

R/20/3331. 2021. District court of Pirkanmaa.

R/20/406. 2021. District court of Helsinki.

R/25783/19. 2019. Helsinki Police Department.

R/8414/20. 2020. Central Finland Police Department.