COMP2216 Principles of Cyber Security - Cyber Attack Analysis

Username: tgp1u16

Task 1: Attack Summary

To summarise the attack I will divide it into two parts from a timeline point of view:

1. the events leading up to the release of the stolen data on the 5th of July, 2015
2. the events after and including the release

The attack itself is included in the first part. However, apart from the attacker's disclosure[1] we do not have an explicit timeline of the attack. It is stated in the perpetrator's report that roughly 100 hours of work were put into the attack. The main phases of the attack were:

- information gathering
- creating a zero-day exploit for an embedded device (the attacker spent several weeks reverse engineering and testing it)
- lateral movement inside Hacking Team's network
- stealing credentials
- data exfiltration
- acquiring persistence

The timeline of the second part is more elucidating. On the 5th of July 2015, 400GB of data belonging to Hacking Team was uploaded to BitTorrent and their Twitter account got hacked[2]. After a few hours an employee named Christian Pozzi twitted that "what the attackers are claiming regarding our company is not true", and that the leaked archive "contains a virus". Pozzi's Twitter account was compromised shortly after. On the 6th of July their Twitter account was compromised and Phineas Phisher came forward as the attacker.

Hacking Team's response consists of several press releases posted on their website the following days. They stated that:

- they condemn the attacker for releasing the malware into the wild where everyone can access it[3]
- the use of the RCS[40] was suspended until new updates which would allow clients to resume criminal ad intelligence investigations[3]
- they are working on a new internal infrastructure as well as on a completely new version of Galileo RCS[4]
- they blaim the media for showing a biased and inaccurate version of the events[5]

The attack had a major impact on both Hacking Team and their clients as well as on the hacking environment. The data uploaded by the attacker included source code, documentation, emails[6], invoices and audio recordings. Sensitive information was found such as a list of clients including oppressive regimes which Hacking Team previously denied having ties to. A fully fledged Android spying tool[11] was discovered. In addition, several exploits were found targeting:

- Flash Player[7, 8, 12, 13]
- Internet Explorer[14]

- Windows kernel[8]
- UEFI BIOS[10]

Following the leak, this exploits started being used by other hackers until being patched.

Task 2: Attack Analysis

The attack analysis is mainly based on the attacker's report[1] where we can find explanations on the technical details and steps taken to conduct the attack. The techniques and tools used are also discussed and enumerated in the report. In the analysis I will explain the techniques but will keep the tools to a minimum since they are not so important.

Reconnaissance

The Reconnaissance steps are not clearly stated in the disclosure. However, several methods of gathering information are enumerated. We can assume that some or all of these methods were used.

For the collection of technical information the attacker mentions:

- subdomain enumeration[15] which can be done by querying the company's DNS server, permutation scanning, finding public SSL/TLS certificates or by using specific tools like fierce[16], theHarvester[17] and recon-ng[18]
- whois lookups to find information about who owns a specific domain or IP address
- reverse lookups using the domain or IP range of a company to find related domains and IP addresses
- port scanning[19] and fingerprinting using the IP range of a company to check which ports are open, what services are running on an open port and other important details about the machine like the TCP/IP configuration and OS. The way it works is it sends different types of requests to a range of ports at a specified IP and it analyses the response to determine the state of the scanned port

To gather social information about the company the hacker refers to public information on websites like Google and LinkedIn. Other methods are extracting the metadata in files published by the company and using specific tools[17, 18].

During the Reconnaissance phase the attacker realised that Hacking Team had little infrastructure exposed to the internet and no known vulnerabilities were found. The devices exposed were the main website running a Joomla blog, a mail server, routers, VPN devices and a spam filtering appliance.

Weaponization

For the Weaponization phase the attacker chose to create a zero-day exploit for one of the embedded devices. A remote root exploit was eventually found after some reverse engineering[20]. The exploit is not disclosed since it was not yet patched. Along with the exploit a backdoored firmware (the payload) was written and a number of post-exploitation tools were compiled. They were tested on other companies' vulnerable networks before being used.

Delivery

The Delivery phase is not documented but we can assume that it was through one of the embedded device's open ports.

Exploitation

We only know that the exploit was triggered to take advantage of the vulnerability.

Installation

The embedded device's firmware was replaced with the backdoored one containing the post-exploitation tools.

Command & Control

For the C&C phase the perpetrator has set up an infrastructure consisting of:

- domain names to resolve hostnames into IP addresses and for DNS tunneling[21] which allows for data exfiltration and C&C while using the data payload such as TXT records
- stable servers used to receive reverse shell (the target machine initiates the connection while the server listens), to launch attacks and to store stolen data
- hacked servers to hide the IP addresses of stable servers and to connect to the rest of the internet and perform malicious activity like scanning ports and downloading compromised data

The connection to the infrastructure was made through Tor[22] which allows for online anonymity by encrypting and randomly bouncing connections through a network of relays.

One of the post-exploitation tools is a SOCKS[23] proxy server which allows the attacker to access Hacking Team's local network from the outside. It works by setting up an IP tunnel with a firewall and the protocol requests are initiated from the firewall[24]. The attacker communicates with the embedded device and it forwards the packets to devices on the local network as if it were the attacker. Also, the hacker set up a service for port forwarding through the firewall.

Actions on Objectives

This phase is the most relevant due to the fact that the attacker's goal was to completely gain control over Hacking Team's internal networks. To accomplish this, lateral movement techniques were used in combination with data exfiltration until acquiring the administrators credentials. Most of the actions in this phase were performed using access through the proxy server.

After entering the network the perpetrator started to slow scan it to avoid detection and also fired a tool to analyse the traffic.

During the scan a few iSCSI[25] devices with no authentication required were found (according to their documentation they were supposed to be on a separate network). iSCSI allows for linking of data storage facilities over IP. It provides block-level access to storage devices by carrying commands over a TCP/IP network. Therefore, the disks of the connected machines appear as being locally attached to each machine.

To mount one of the devices the attacker:

- used a VPS[26] by doing port forwarding
- added a firewall rule to the VPS to redirect the outgoing traffic to the actual address of the device on the Hacking Team network back to localhost
- mounted the iSCSI device
- mounted the device file
- mounted one of the virtual machines which was the Exchange server

- finally mounted the server's hard disk

Following, the attacker started looking for cached and hashed passwords and trying to dump them using several tools:

- pwdump[27]
- cachedump[28]
- mimikatz[29] with lsadump[30]

lsadump found the password to a BES[31] which had local administrator permission.

On the BES server the attacker used the psexec_psh exploit[33] in combination with a Powershell payload. Powershell[34] is a command-line shell and scripting language similar to Linux's Terminal. The commands and scripts that run in Powershell are executed in memory so the risk of detection by Antivirus decreases significantly. After retrieving a Meterpreter [36] (payload that uses in-memory DLL injection and is extended over the network at runtime) shell the perpetrator retrieved passwords from the LSA[35] memory by setting UseLogonCredential registry setting to 1 and using creds_wdigest[37] in Metasploit.

One of the passwords belonged to the Domain Administrator. Having access to the email the attacker starts downloading it by using Powershell. In addition, files from different servers have been downloaded by using a tool for accessing SMB/CIFS resources on servers[38].

To acquire persistence the attacker used Duqu 2 style "persistence", meaning that it wouldnt modify any disk files or system settings and instead it would use processes that run into memory. In the unlikely event that all the servers would reboot at the same time the hacker held a Kerberos[39] golden ticket[41] (which is valid for 10 years even if the user it's tied to changes password) and also the stolen passwords.

The final piece of the hack was getting access to an isolated network with the source code for the RCS[40]. To achieve this the attacker found a Truecrypt[42] volume on one of the sysadmins' computer, waited until he mounted it and then copied the files. Within the volume there was a file with a password to a server which had access to the isolated network. Since the password only allowed access to the web interface he used a public code execution exploit. In the end the attacker used the "forgot my password" feature to retrieve the password for Hacking Team's Twitter account and GitLab server.

Task 3: Attacker Analysis

From the disclosure it is clear that the attacker was motivated by the beliefs that Hacking Team is creating social injustice by doing something unethical like selling offensive security solutions "that helped governments hack and spy on journalists, activists, political opposition, and other threats to their power"[1]. It can be observed that no monetisation motivations were involved:

- data was released into the wild instead of being sold
- no ransomware or DDos attacks involved

The perpetrator's goals were to prove the said beliefs and also to take Hacking Team out of the business by releasing both confidential information and the code for their malware, thus making it unusable.

The skills shown are far more advanced than the ones of a script kiddie but not as developed as a nation state or cybercriminal organisation. We have seen that the attacker:

- has wide knowledge in areas like information gathering, lateral movement, data exfiltration, persistence zero-day exploits
- did not have a clear strategy
- relied on the information gathered at each step and adapted accordingly
- did not use any groundbreaking technique nor did he create an APT

All the facts mentioned above point to the attacker being a Hacktivist. His motives were purely ideological and social, revealing a person willing to put his freedom at risk to fight against unethical and immoral activity. The goal was a typical one to a Hacktivist as well involving web defacement (Twitter account hacked) and data breach. From how the attack was carried out we can draw the conclusion that most probably only one person was behind it, excluding the possibility of nation states or cybercriminal organisations.

Several clues point to the attacker being used to launching similar attacks. The most important one is the attacker's disclosure on hacking Gamma Group[43], a company similar to Hacking Team. Another clue is the ease with which the hacker moved laterally through the network knowing how to put together several pieces of data to exploit the vulnerabilities.

References

[1] http://pastebin.com/raw/0SNSvyjJ

[2] http://www.cydefe.com/podcast/2015/7/11/the-hacking-team-hack-timeline

[3] http://www.hackingteam.it/news/2015/07/08/information-attack-july6.html

[4] http://www.hackingteam.it/news/2015/07/13/statement-from-CEO.html

[5] http://www.hackingteam.it/news/2015/07/22/statement-from-hackingteam.html

[6] https://wikileaks.org/hackingteam/emails/

[7] https://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/

[8] https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/

[9] https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/

[10] https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

[11] https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/

[12] https://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/

[13] https://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/

[14] http://blog.trendmicro.com/trendlabs-security-intelligence/gifts-from-hacking-team-continue-ie-zero-day-added-to-mix/

[15] https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6

[16] https://github.com/mschwager/fierce

[17] https://github.com/laramies/theHarvester

[18] https://bitbucket.org/LaNMaSteR53/recon-ng

[19] https://en.wikipedia.org/wiki/Port_scanner

[20] https://en.wikipedia.org/wiki/Reverse_engineering

[21] https://www.plixer.com/blog/network-security-forensics/what-is-dns-tunneling/

[22] https://www.torproject.org/

[23] https://en.wikipedia.org/wiki/SOCKS

[24] http://etherealmind.com/fast-introduction-to-socks-proxy/

[25] https://en.wikipedia.org/wiki/ISCSI

[26] https://en.wikipedia.org/wiki/Virtual_private_server

[27] https://en.wikipedia.org/wiki/Pwdump

[28] http://www.securiteam.com/tools/5JP0I2KFPA.html

[29] https://github.com/gentilkiwi/mimikatz

[30] https://github.com/gentilkiwi/mimikatz/wiki/module- -lsadump

[31] https://en.wikipedia.org/wiki/BlackBerry_Enterprise_Server

[32] https://github.com/haad/proxychains

[33] https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/smb/psexec_psh.rb

[34] https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6

[35] https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service

[36] https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

[37] https://www.trustedsec.com/2015/04/dumping-wdigest-creds-with-meterpreter-mimikatzkiwi-in-windows-8-1/

[38] https://www.samba.org/samba/docs/current/man-html/smbclient.1.html

[39] https://en.wikipedia.org/wiki/Kerberos_(protocol)

[40] https://wikileaks.org/spyfiles/document/hackingteam/31_remote-control-system-v5-1/31_remote-control-system-v5-1.pdf

[41] http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi-extension-golden-ticket-howto/

[42] http://truecrypt.sourceforge.net/

[43] http://pastebin.com/raw.php?i=cRYvK4jb