How active and passive cyber reconnaissance are used to perform a cyber attack

Science, Computer Science

ASSIGN BUSTER

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Reconnaissance

A designation Often associated with the military, reconnaissance in the cyber and computing world means analyze and detect weaknesses in the targets network, systems, and defenses such as firewalls, incorrect WAP setups or open network holes. The actor or Nation and State will find the information they need to access the network and systems connected. Perhaps a port is open, or the firewall allows all VPN's to access the network. Reconnaissance is a very resource heavy step, but also a key step to gain access and intrude on a target.

Passive reconnaissance

This type of Reconnaissance relies on subtle less intrusive approach, meaning this type of APT attempts to gather critical data and info without actually tapping into the targets network. Some examples of this is trying to acquire PC's or Hard drives that have been thrown out or discarded.

Appearing to be an authorized user, or even implementing Access Point Mapping (APM) or also known as ‘ War Driving’. This is when an actor patrols a town or city or even a corporation and actively looks for holes and weaknesses in AP’s. Once a weakness is found, it is then exploited. This type of exploitation can leave a very minimal footprint and is harder to trace or raise awareness of an intruder. Other types of Passive Reconnaissance includes Spear-Phishing associated with emails containing the virus. Social Media, which provide information about users for the targets they work for or are associated with. Such sites give even more information, such as LinkedIn or even Facebook. Both sites provide detailed search capabilities as well, which can further assist in Passive Reconnaissance.

Another method is to use nslookup once a weakness in the AP has been isolated and access has been granted. Some files and group policies may prevent certain accesses, but nslookup or even Kali Linux can give a basic map of the network, further assisting the actor or nation and state. In fact, even mobile devices can be used to assist in this type of reconnaissance. Android and Apple have apps that help scan ALL wireless networks, even hidden ones, that show the MAC of the device, how far and close they are in distance of meters. (Uni Developers, 2018)

With Active Reconnaissance, the intruder will directly interact and connect to the targets system. Once directly connected, then the Reconnaissance will look for weaknesses and vulnerabilities within the network. An example of Active Reconnaissance would be port scanning. In this scenario, port scanning is used to find holes or open ports to help the actor gain access to a vital system. Another example is Packet sniffing or packet manipulation with tools like Scapy powerful tools that can scan networks, saturation attacks (DDoS), scan, probe an traceroute. (Scapy, 2018) The hacker can also Telnet into a port, and start gaining access, if a port is not securely locked down. FTP Port, HTTP ports (21 and 80) and also SMTP port (25) can all be exploited to gain access to a target network. This type of APT, Active Reconnaissance, is much more intrusive and can leave a trail if not properly cleaned up.

Weaponization and Delivery

Once the APT’s Passive and Active Reconnaissance is completed (Accessed via open ports, and email vulnerabilities) the next phase will be to implement a worm that contains a payload to the target. This payload will then exploit the system, and start allowing access to the systems controls. This worm will then retrieve more information from the network, such as IP’s, run keylogging scripts and commands to various stations, stations and even mobile devices once it replicates and spreads. As stated in the previous report (C688 Task1) actors and users with little knowledge can create malware with little to no coding or networking experience.

Programs such as T2W (Trojan 2 Worm) allows an actor or even a state or nation to create a trojan that infiltrates then spreads like a worm unleashing havoc. It can create executable files to be ran once activated. (Higgins, 2008) Russia can very well create their onw, or use programs and software like these to access the power grid. In fact, Kali Linux, an OS called an “ ethical Hacking” OS, is free, and open distributed to assist with hacking issues. However, unethical hackers can also use this OS, and countries like

Russia currently use this OS, rebranded as Astra Linux. Astra Linux is used by the Russian Army and armed forces. (http://astralinux. ru, 2016)

Russia not only has the funds and resources to implement Passive and Active Reconnaissance, Russia has their own cyber team, that can create, or just download and use readily available programs and tech to assist them, helping them save time and even money, while finding the same results. Russia can easily look up employees of the power grid on LinkedIn, Facebook, Instagram, Google+ and Twitter, and see information that could lead to exploiting; which is another low footprint APT.

Exploitation and Installation

Two methods, Email attachment, and USB drive, are both considered to be the strongest way to gain access to a facilities networks and workstations. The first method, email, requires only an email to be sent to a user within the power grid facility. The user opens the email and attachment, and the bot or worm is activated and start infiltrating the facility network. This can be done via the reconnaissance done, where information retrieved from social media is used. Social media such as LinkedIn or Facebook, as previously stated early. Once information Is retrieved from social sites, an email depicting legitimacy can then be created and executed. The user within the facility at the power grid unwittingly opens the attachment thinking it is from within the corporation or is in regards to the corporation perhaps with a company they frequently do business with. The second method uses the USB drive method, where the user is influenced, knowingly or unknowingly to use a USB flash drive on their PC or another’s PC or like device.

Once the USB has been plugged in, the bot, or work is now able to be active, and spread within the facilities network. The work can then unload payloads, where these payloads will look for even more holes and breaches to exploit, and can rewrite, delete, and copy critical and sensitive data. The worm can even bring the entire network down once the program runs its course. However, before the network is brought down, the actor can also use the worm to secretly VPN into the devices or networks systems such as routers or servers. They are undetected, and can mirror other users screens and workplaces. To summarize, the worm deployed a payload, which was deployed using one of the two methods given above, email or USB via Social Media manipulation which was installed via a workstation internally. This payload installed a backdoor trojan which allowed visual and physical access to the network, workstations, servers and switches (including the Firewall).

Command and Control

Below is a visual breakdown of the Command and Control method that is executed via the APT. You can see that after the passive/active reconnaissance, the system was then exploit and then infiltrated. Once connected, the attacker is now completely connected and has full access to the system and network without any alarms or red flags being raised. (Zorabedian, 2014) As we can see in the infograph above, once the hacker establishes a solid and encrypted connection to the power grid, commands, programs, copying and deletion of files, sensitive data, personal information, and other types of encrypted information can be manipulated. The attacker can use different ports to go undetected, such as port 443 (http) or port 135

(Windows Remote Desktop) or as previously mentioned, port 23, telnet. Port 80 could also be executed, but many companies and corporations know 80 is widely used now, and that is usually locked down. So the other ports that are rarely used seem more likely, but port 80 is still going to be monitored.

Actions

APT’s are not always easily detected due to network traffic and packet movement. Since packets or coming and going constantly at an almost nonstop rate, APT’s actions can go unnoticed, as it look like regular packet traffic. While bandwidth can be some indicator of something odd happening on the network, it is not always a clear cut sine. IP’s can be masked, or a hacker can piggyback onto a user watching a youtube video, and the bandwidth stream can look like someone is watching large video requiring large bandwidth. Or an update for Windows could be in progress, and the actor can use this as another option to stay fully connected without raising suspicion. (Goodin, 2015) This is a great example of Command and Control in action, as piggybacking, whether a signal, or bandwidth or even stealing a remote login, it shows that these are hard to monitor and detect and stop.

Staying undetected is the key setup hackers try to maintain. It allows them to stay connected for long periods of time, stealing, changing and copying data. Changing settings, stealing settings, deleting setups and records little by little until the systems are crashing. A new RAT (Remote Access Trojan) was recently found that mostly attacked the automotive industry. This RAT was sent via email, the attachment looked to be an email within the company domain, and users opened the attachment to find they were then hacked and files encrypted. The following was also discovered to be part of the payload that intruded the network and systems:

Remote Desktop Manipulation

File system manager

Proxy support

Audio Chat Access

This malware, FlawedAmmyy, is based on Ammyy Admin, and is a remote desktop program. Since this clone, a malicious clone, it contains all the resources and accesses that the remote desktop software contains. (www. cyberdefensemagazine. com, 2018)

We can see how data is not pulled and extracted from exploited targets. Web applications, such as browsers, websites, web enhanced programs, emails. We also have Backdoor trojans and malware that uses ports, which can include the DNS port 53. We also can see the use of FTP (File Transfer Protocol), which allows users both internal and external to share files, documents, media and pics.

Defense in Depth Recommendations:

People End users, company employees, managers, engineer, even IT tech, and IT admins are all parts of security risk because of the aptly known issue of user error. People are by far the most critical part of security for corporations, Armed forces, government and public systems and networks.

Safeguards must be implemented and strictly followed by all peoples associated with the technology. Below, we will discuss this in greater detail:

Security Training and Practices: Setup and implement security policy protocols to deter cyber-attacks. We recommend policies and procedures that show proper procedures and practices when it comes to data sharing, email attachments, using external devices such as USB or external hard drives. Limit personal devices like laptops or personal smartphones. Design a more secure network by locating known issues, test for holes and vulnerabilities in both hard line and AP setups. Ethernet ports that are open and never used should be turned off, and AP's should either be upgraded via firmware or hardware to implement stronger firewalls and security protocols. Raise awareness of how social media (spear phishing) can be used to hack systems. These training sessions should be frequent, and informative, to help the employees retain the information. Being diligent and repetitive with this type of awareness and training will help keep the security protocols up to date and fresh in the minds of employees. This will raise information assurance level based on the repetition of training sessions that help solidify the information to help better retain and use it on a daily basis.

Physical and Cloud protection: We highly recommended data and file backup using both physical and virtual formats. Sensitive data and information should be backed up via redundant systems, both physical and virtual in the cloud. Physical can be both on location hard drive back up and physically written data. The cloud back up can be setup and protected off site to help protect any data loss, corrupted or deleted due to a malware intrusion. We can simply retrieve the backed up file and repair some of the damage done.

System Admins: Most networks are controlled and monitored by the system admins. there can be a network admin, systems admin, domain admin and etc. These Admins are crucial to maintaining network, system, and domain stability. We recommended that new procedures and policies be created and put into effect. These new policies will help to protect and enhance security for facilities. It should be a requirement that these admins obtain, keep and maintain certifications in relation to network security. Higher training should be implemented, and admins must make sure accountability is noted. Who logs into what, when and where and was it authorized. This will raise information assurance level by making admins more goal oriented and responsible for the first level of security. Giving them more tools to fight with and a better understanding of real world cyber-attacks. .

Passwords: Passwords safety needs to be implemented within the facility. Secure passwords where they are not personally used outside of the facility. Policies need to be put in place where passwords should be changed frequently, and even have machines with fingerprint security, as passwords can be hacked, and fingerprint readers are harder to bypass. System admins should not use default usernames and passwords. Each admin should use their own credentials, this also helps with pinpointing who accessed a device last, and helps in alleviating a tedious search of who logged into the server last and made changes. If admin is the default username for all admins, it is hard to shows who actually accessed the device. Both admins and users need to train on proper password and login procedures to ensure a high level of security. This will raise information assurance level because employees and admins who are now trained properly in password protection and implementation will be better equipped to give a higher level of security.

Access Restrictions: It is recommended that access restrictions be setup and implemented. Only personal who has been given access to certain rooms, servers, files, and data both shared and unshared need to have strict protocols enabled that limit who can access and if can access, have limited control or are monitored. Many user can easily access items they have no need nor business accessing. System admins needs to design and execute stricter access procedures. This will greatly help keep many items within the network secure.