Case study on cyber attacks

-Amit yadav

Introduction

The historical landscape of how wars are fought changed drastically when Technology was used by developed countries to attack one another, critical websites, organizations, or the common peoples are hacked or defaced to display the power of IT.
In this case study, top cyber attacks would be discussed to enable people understand the nature, power and threats caused by cyber attacks.
The primary objective of this case study is to introduce people about effect caused by the cyber attacks and the main reason for the attack.To cover various fields of cyber attacks we are taking examples from every possible field, and then going to divide them in LOCKHEED MARTIN KILL CHAIN format so that readers can understand and relate how hacks are actually carried out.
Below is little description about the hacks that is covered in this project:

1. Stuxnet (2010)

Stuxnet is a malicious computer worm , first uncovered in 2010. Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Exploiting four zero-day flaws, stuxnet functions by targeting machines using the Microsoft Windows system and networks, then seeking out Siemens Step7 software.

2. Pune's Cosmos Bank (2018)

India's banking sector was rudely shaken up after an international gang of hackers siphoned off Rs 94.42 crore from the Cosmos Cooperative Bank Ltd, through multiple ATM swipes in 28 countries worldwide.

3.DDos attack on - Github (2018)

On Feb. 28, 2018, GitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking.
According to GitHub, the traffic was traced back to ―over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints.

4. Mirai Botnet (2016)

Mirai is a malware that turns networked devices running Linux into remotely controlled that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.

Table of Contents

List Of Figures

.

References

https://en.wikipedia.org/wiki/Stuxnet

https://www.pcmag.com/article2/0,2817,2370107,00.asp

https://krebsonsecurity.com/tag/stuxnet/

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

https://github.blog/2018-03-01-ddos-incident-report/

Stuxnet

Stuxnet changed the meaning of malwares and their goals, it was not only a new virus but it‘s a new era of malware. It was an extremely sophisticated computer worm that exploits multiple previously unknown Windows zero-day vulnerabilities to infect computers and spread. Its purpose was not just to infect PCs but to cause real-world physical effects. Specifically, it targets centrifuges used to produce the enriched uranium that powers nuclear weapons and reactors.

This complex threat uses up to four zero-day vulnerabilities(MS10-046,MS10-061,MS08-067,0-day) in windows OS and includes many tricks to avoid being detected by the behavioral-blocking antivirus programs. This attack makes additional use of a further vulnerability categorized as CVE-2010-2772, relating to the use of a hard-coded password in those systems allowing a local user to access a back-end database and gain privileged access to the system. It damaged the Iranian nuclear reactor and its machines by infecting the PLCs (Programmable Logic Controller) that control the machines there. That makes it modify the control program which changes the behavior of the machine.

It is predicted that there were probably a number of participants in the Stuxnet development project who may have very different backgrounds. However, some of the code looks as if it originated with a "regular" software developer with extensive knowledge of SCADA systems and/or Siemens control systems, rather than with the criminal gangs responsible for most malcode, or even the freelance hacker groups, sometimes thought to be funded by governments and the military.

Flow of stuxnet

This worm was created mainly to sabotage the Iranian Nuclear Program. Once installed on a PC, Stuxnet uses Siemens' default passwords to gain access to the systems that run the WinCC and PCS 7 programs which control and modify the code of the PLCs (programmable logic controller) which control the machines themselves.

Stuxnet operates in two stages after infection, according to Symantec Security Response Supervisor Liam O'Murchu. First it uploads configuration information about the Siemens system to a command-and-control server. Then the attackers are able to pick a target and actually reprogram the way it works. "They decide how they want the PLCs to work for them, and then they send code to the infected machines that will change how the PLCs work," O'Murchu said.It managed to infect facilities tied to Iran's controversial nuclear programme before reprogramming control systems to spin up high-speed centrifuges and slow them down.

Infected countries: According to security vendor Symantec it is found that infected systems are in between 90,000 and 100,000. And infected countries are more than 100 where India is at number 3 with over 5,000 infections and Iran has been considered as the major target with the number of infections in the country at about 33,000,where Indonesia has infected systems around 10,000.

Country	Share of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

Fig 1 – Infected Countries

Suspects

Israel is an obvious suspect. Israel considers a nuclear Iran to be a direct existential threat. But, until now, there‘s no real evidence that says it was Israel who really created this worm. There are some theories said that there are evidences on Israel as the creator depending on some dates and words found inside the malware and also there‘s an analysis from the industrial control-systems maker ―Siemens‖ reportedly backs speculation that Iran may have been the target of Stuxnet's attack and that Israel may have been involved. A report by the New York Times suggested Stuxnet was a joint US-Israeli operation that was tested by Israel on industrial control systems at the Dimona nuclear complex during 2008 prior to its release a year later, around June 2009. The worm wasn't detected by anyone until a year later, suggesting that for all its possible shortcomings the worm was effective at escaping detection on compromised systems. But these evidences aren‘t real evidences in the court and the worm_s still a perfect crime.

How it works

1. **Infection:** Stuxnet enters a system via a USB and proceeds to infect all machines running Microsoft windows operating system. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. **Search:** Stuxnet then check whether a give machine is part of the targeted industry machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. **Update:** If the system isn‘t a target, Stuxnet does nothing; if it is, the worm attempts to access the internet and download a more recent version of it.

4.**Compromise:**The worm then compromises the target system‘s logic controllers(PLC‘s) exploiting ―zero-day‖ vulnerabilities software weakness that haven‘t been identified by security experts.

5. **Control**: In the beginning, stuxnet on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spins themselves to failure.

6. **Deceive and Destroy**: Meanwhile, it provides false feed-back to outside controllers, ensuring that they won‘t know what‘s going wrong until it‘s too late to do anything about it.

Cosmos Bank

Cosmos Bank became the latest victim of a major cyber-attack in August 11 and 13 in year(2018), a group of international hackers broke into the servers of the Bank. About Rs 78 crore was withdrawn through various ATMs located in 28 countries through 12,000 VISA transactions and another Rs 2.5 crore was withdrawn through 2,800 debit card transactions at various locations in India, and on August 13th, in another malware attack on the bank‘s server, a SWIFT transaction was initiated – transferring funds to the account of ALM Trading Limited in Hanseng Bank, Hong Kong.

The total losses from the attack stand at INR 94 crore, or 13.5 million USD. Cosmos Bank was forced to close its ATM operations and suspend online and mobile banking facilities.

How did the breach take place?

The breach involved an ATM switch and related SWIFT environment compromise that created two routes through which hackers cashed out, according to Securonix.

Either targeted spear phishing and/or a hack against a remote administration/third-party interface allowed hackers to gain an initial foothold in the Indian bank's network. Following subsequent lateral movement, the bank's internal and ATM infrastructure was compromised.

After the initial break-in, attackers most likely either leveraged the vendor ATM test software or made changes to the deployed ATM payment switch software to create a malicious proxy switch.

Hackers were then in a position to establish a malicious ATM/POS switch in parallel with the existing (legit) system before breaking the connection to the backend/Core Banking System (CBS) and substituting their own counterfeit system in its place.

How did the attack happen?

- Malware attack: The core banking system (CBS) of the bank receives debit card payment requests via a ‗switching system‘. During the malware attack, a proxy switch was created and all the fraudulent payment approvals were passed by the proxy switching system.
- Details sent from a payment switch to authorise transactions were never forwarded to backend systems so the checks on card number, card status, PIN, and more were never performed. Requests were handled by

the shadow systems deployed by the attackers sending fake responses authorising transactions.Attackers using MC(a malicious ATM/POS switch) were able to send fake transaction reply messages in response to transaction request messages generated from cardholders or end points.

- ATMs compromised: When depositors withdraw money at ATMs, a request is transferred to the respective bank‘s CBS. If the account has sufficient balance, CBS will allow the transaction. In the case of Cosmos Bank, the malware created a proxy system that bypassed the CBS. While cloning the cards and using a parallel or proxy switch system, the hackers were able to approve the requests – withdrawing over INR 80.5 crore in approximately 15,000 transactions.

How was it detected?

- Suspicious Transaction activity
- Suspicious ATM activity
- Suspicious Network activity

Cyber kill chain

Reconnaissance: Cosmos bank where attackers are able to find and understand how the banking systems work , its customers, the protocols being used and other information.The attackers also consider the possibility of the phishing campaigns where spear phishing can be done on selected targets to gain access to the network.They were also able to gain information about ATM machines and how it is communicating to the Central Banking System

Weaponization: Attackers was able to identify the vulnerability that was present in the switch that plays a vital role in the transaction management for the banking system.Attackers were successfully able to craft malicious script to exploit vulnerable points.

Delivery: Attackers were able to deliver malicious using multiple techniques one of them is spear phishing. And the malware was able to affect the switching system

Exploitation:.

Malware was able to make a proxy system that was placed between ATM and CBS.

Malware was able to transfer all transactions to the proxy system which authenticated all the unauthorized transactions.

Installation: Malware was able to place a proxy switching system where all the transactions go through the switch and is self authenticated.The connection to the Central Banking System is served and all the transactions are authorized in the switching proxy.

Command & control: In this scenario the attackers were able to manipulate the authorization by increasing the withdrawal limits of cards and also they were able to exploit the SWIFT system into sending the money to accounts in other countries

Action on objectives: Attacker's motive was to take out a lot of cash within a short span of time and make the attack complex that it could not be detected easily

The attacker were able to achieve their aim as the attack was complex and even the intrusion detection system failed to identify attack

DDoS attack on - Github

Github survived the biggest DDoS attack ever recorded on February 2018 peaking at 1.35 Terabits of traffic. It was the most powerful attack recorded to date and it used an increasingly popular DDoS method, no botnet required this time attackers performed DDoS attack via memcached server.

What is DDoS?

DDoS (distributed denial of service in full) is type of a cyber attack that aims to bring websites and web-based services down by bombarding them with so much traffic that their services and infrastructure are unable to handle it. Main objective behind DDoS is to force targets go down.

Potential motives for any DDoS attack:

Hacktivism – Hacktivists use DoS attacks as a means to express their criticism of everything from governments and politicians, including ―big business‖ and current events.

Cyber vandalism – Cyber vandals are often referred to as ―script kiddies‖—for their reliance on premade scripts and tools to cause grief to their fellow Internet citizens. These vandals are often bored teenagers looking for an adrenaline rush, or seeking to vent their anger or frustration against an institution (e.g. school/college) or person they feel has wronged them and some of them are just to gain attention, fame

Business competition – DDoS attacks are increasingly being used as a competitive business tool. Objective is to divert competitors from main goal and engage them with attack .or sometime with a goal of complete shutdown of their business.

Cyberwarfare- This kind of attack is backed by nation/states; these are well-funded and orchestrated campaigns are executed by tech-savvy professionals.

About the incident

Between 17:21 and 17:30 UTC on February 28th github identified and mitigated a significant volumetric DDoS attack. The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints. It was an amplification attack using the memcached-based approach that peaked at 1.35Tbps via 126.9 million packets per second.

The first portion of the attack peaked at 1.35Tbps and there was a second 400Gbps spike a little after 18:00 UTC.

This graph provided by Akamai shows inbound traffic in bits per second that reached their edge:

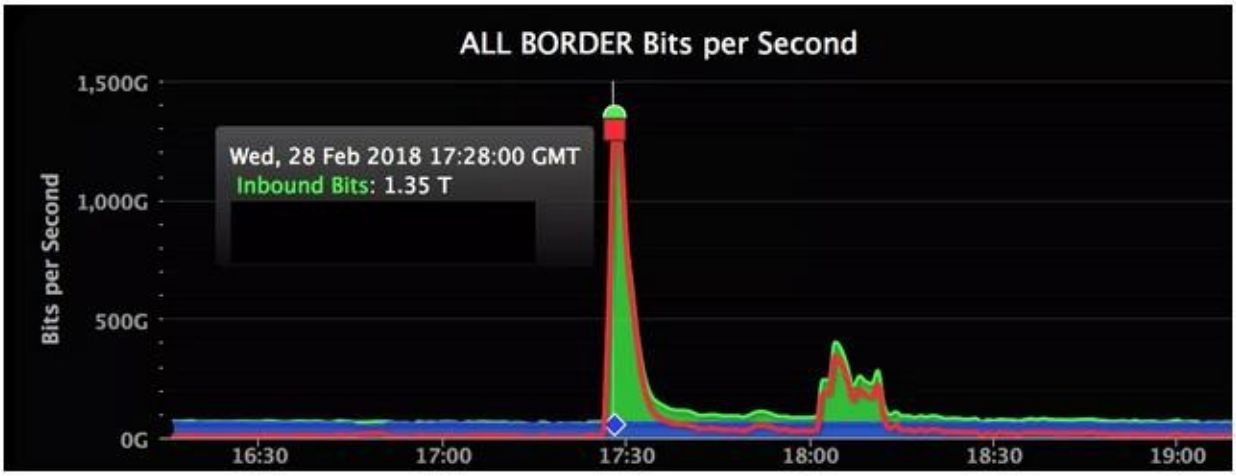

Fig -2 All border bits

How was the attack made?

To generate this much amount of traffic, one might require thousands of botnets like mirai botnets. But this case was completely different. It was found that the attack wasn‘t made by botnets. Hackers used a new method which makes this attack unique; they used - *Memcached Server* to perform the attack.

What is Memcached?

Memcached is a process running on a server at port 11211(by default) which is generally used to cache large amount of frequently accessed data in the memory so that is can boost the speed of the server/website and can response faster without sending any request to main server, by default it doesn‘t have authentication mechanism as it want to response quickly. Another feature of Memcached is that a small request query to the server is capable of returning a large amount of data, and Memcached uses UD**P.**

How is it vulnerable?

As Memcached server listens on UDP port 11211 by default. It can be exploited to produce DDoS amplification attacks by sending the memcached server a UDP packet with a spoofed IP containing a message asking for statistics, which will cause the server to return an enormous message to the victim. Exploitable DDoS amplification vectors allow attackers to deliver massive and/or many packets for each small packet they send, without the need to control a botnet of hacked devices. Amplification attacks via memcached servers result in an amplification factor of 9,000 X or more. As a comparison, NTP, a DDoS amplification vector known for its high amplification factor typically reaches an amplification factor of 557 X the original payload.

How was it mitigated?

They move the traffic to Akamai (American content delivery network and cloud service provider), which help them by providing additional network capacity. And by using DDoS scrubber center they were able to stop/block malicious packets and only sending legitimate request to Github server

Who is behind the attack?

Who committed this attack is still unknown but some links are found that shows that the attack was linked to firewalls of china. So it is doubted that china is behind the attack but it is not proved as there is no relevant proof to support.

Cyber kill chain

Reconnaissance: Attackers able to find and understand how the Memcahed server works ,and how its protocols are being used and other information.

They were also able to gain information about which types of query server is responding better.

Weaponization: Attackers were able to identify the vulnerability that was present in the server that plays a vital role in response to query, Attackers were successfully able to craft malicious script to exploit vulnerable point.Attackers were able to spoof ip address successfully.

Delivery: Attackers were able to request server using spoofed ip

Exploitation: Memcached server was responding to the github server to all the requests which was actually made by the attacker that peaked at 1.35Tbps via 126.9 million packets per second.

Installation: Attackers was able to request on behalf of github (using ip spoofing) and memcached server is listening on UDP port 11211 by default without authentication mechanism helped attacker make request without validation

Action on objectives: Attacker's motive was to take down the service, attacker were able to achieve their aim for some time

Mirai botnet

Mirai botent is a self-propagating botnet malware that infects smart devices which are using ARC processors, infection turning those devices into a network of remotely controlled bots.

Once the virus is loaded into memory on the BOT it deletes itself from the BOT‘s disk. The virus will remain active until the BOT is rebooted. Immediately after a reboot the device is free of the virus however it only takes a few minutes before its once again discovered and re-infected.

The attack vectors are highly configurable from the CnC but by default Mirai tends to randomize the various fields (port numbers, sequence numbers, ident etc) in the attack packets so they change with every packet sent.

In September 2016, the authors of the Mirai malware launched a DDoS attack on the website of a well-known security expert. A week later they released the source code into the world, possibly in an attempt to hide the origins of that attack. This code was quickly replicated by other cybercriminals, and is believed to be behind the massive attack that brought down the domain registration services provider, Dyn, in October 2016

How mirai works

The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password these devices were things like digital cameras and DVR players. There are 68 username and password pairs in the botnet source code. However, many of those are generic and used by dozens of products, including routers, security cameras, printers and digital video recorder (DVRs).

The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and co-ordinate them to mount a DDOS attack against a chosen victim. The attack was so sophisticated that it resulting in the inaccessibility of several high-profile websites such as Twitter, the Guardian, Netflix, Reddit,Airbnb ,CNN and many other.

Dyn estimated that the attack had involved 100,000 malicious endpoints‘, and the company said there had been reports of extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second.

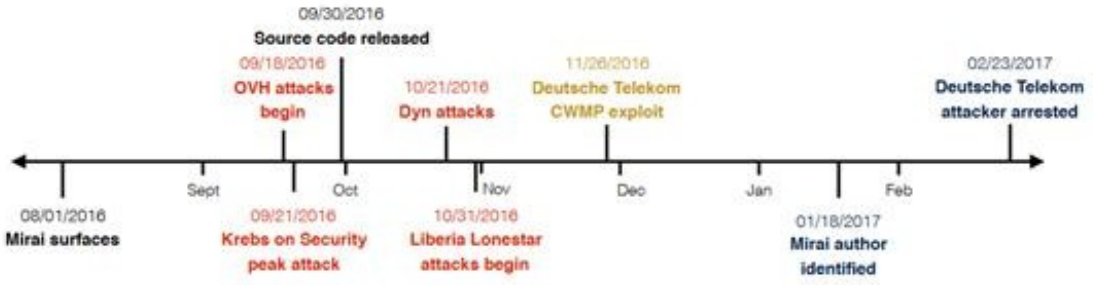

Fig. 3 – Mirai Timeline

Who created mirai

The virus is built for multiple different CPU architectures (x86, ARM, Sparc, PowerPC, Motorola) to cover the various CPUs deployed in IoT devices. The image itself is small and employs several techniques to remain undiscovered and to obscure its internal mechanisms from reverse engineering attempts.
Twenty-one-year-old Paras Jha and twenty-year-old Josiah White co-founded Protraf Solutions, a company offering mitigation services for DDoS attacks. Theirs was a classic case of racketeering: Their business offered DDoS mitigation services to the very organizations their malware attacked.

What makes mirai successful

Default username and passwords are the main reason behind the success of mirai, Mirai bot herders scan a broad range of IP addresses, trying login to devices using a list of 62 default usernames and passwords that are baked into Mirai code, according to US-CERT.

Mirai connects hijacked devices to an IRC-type service where it waits for commands. Often one of the first things a bot does is scan the internet for more vulnerable devices to infect. These devices are largely security cameras, DVRs and home routers. Brian Krebs, whose krebsonsecurit.com site was one of the first hit by a massive Mirai-based DDoS attack.

Username/Password	Manufacturer
admin/123456	ACTi IP Camera
root/anko	ANKO Products DVR
root/pass	Axis IP Camera, et. al
root/vizxv	Dahua Camera
root/888888	Dahua DVR
root/666666	Dahua DVR
root/7ujMko0vizxv	Dahua IP Camera
root/7ujMko0admin	Dahua IP Camera
666666/666666	Dahua IP Camera
root/dreambox	Dreambox TV receiver
root/zlxx	EV ZLX Two-way Speaker?
root/juantech	Guangzhou Juan Optical
root/xc3511	H.264 - Chinese DVR
root/hi3518	HiSilicon IP Camera
root/klv123	HiSilicon IP Camera
root/klv1234	HiSilicon IP Camera
root/jvbzd	HiSilicon IP Camera
root/admin	IPX-DDK Network Camera
root/system	IQinVision Cameras, et. al
admin/meinsm	Mobotix Network Camera
root/54321	Packet8 VOIP Phone, et. al
root/00000000	Panasonic Printer
root/realtek	RealTek Routers
admin/1111111	Samsung IP Camera
root/xmhdipc	Shenzhen Anran Security Camera
admin/smcadmin	SMC Routers
root/ikwb	Toshiba Network Camera
ubnt/ubnt	Ubiquiti AirOS Router
supervisor/supervisor	VideoIQ
root/<none>	Vivotek IP Camera
admin/1111	Xerox printers, et. al
root/Zte521	ZTE Router

Fig 4– Default Username & passwords

How we can secure our devices:

1. Randomizing the default passwords, Mirai botnet demonstrated that even an unsophisticated dictionary attack could com-promise hundreds of thousands of Internet-connected de-vices.
2. Set default-open ports to default-closed, apart from network security, IoT developers need to apply ASLR, isolation boundaries, and principles of least privilege into their designs

Cyber kill chain

Reconnaissance:

Mirai bots scan the IPv4 address space for devices that run telnet or SSH.Finding out all default usernames and passwords of different vendors.

Weaponization:

created a dictionary of default username and passwords to attack.

Attacker was ables to identify the vulnerability that was present in IOt devices which are using ARC processors

Delivery:

It discovers new open devices.

Exploitation:

Details of the device are sent to the command and control server. Then mirai connects hijacked devices to an IRC-type service where it waits for commands

Installation:

Once the virus is loaded into memory on the BOT it deletes itself from the BOT‘s disk.

Command & Control:

Wait for attacker commands till that copies virus into new devices

Action on Objective:

Merai attacked not only on Krebs on Security but also affected numerous game servers, telecoms and anti-DDos providers and many other unlinked/unrelated sites.

Conclusion

The purpose of this case study is to analyze and to make the general public aware of Cyber Attacks. So that they will not be the victim of these crimes by using proper security policies. Once such an attack occurred, Disaster Recovery teams should come to picture with countermeasure steps. It is difficult to stop crackers from launching attacks, but exercising defensive measures can prevent attacks. Investment on network security needs to be increased in order to increase network security and losses due to cyber attacks. These are some catastrophic attacks that have happened in past years.