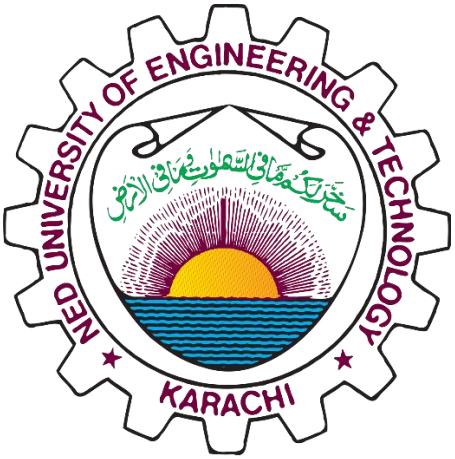
CT-541 – NETWORK SECURITY

MS-IS 004 2019/20 – Evening Fall 2019

NS Assignment-01

Internet Security Threat Report, Summary Report



STUDENT NAME: MUHAMMAD UMAR TARIQ

STUDENT ID: IS 004 2019/20

COURSE INSTRUCTOR: Dr. MUBASHIR M KHAN

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

NED UNIVERSITY, KARACHI CAMPUS

Contents

Internet Security Threat Report v2018:

Ransomware – WannaCry(May 2017) And Petya/NotPetya(June 2017) [EternalBlue Vulnerability] on Microsoft Windows OS:

In a ransomware attack, the target is victim's data, and the attackers either block access to this data or threaten to publish it online unless a ransom amount is paid. The EternalBlue Vulnerability was used to develop WannaCry and Petya/NotPetya.

Petya/NotPetya:

This attack used an Accounting Software as entry point, it infected the windows master boot record to execute a payload (the malware portion of the code) to encrypt hard drives and prevent windows from booting.

Both ransomwares spread quickly through supply chain softwares, hospitals, banks and corporate networks and enterprises.

Reasons why ransomware spreads:

- much of WannaCry's spread was from organizations that had not applied latest patches for MS Windows, or were using older Windows systems that were past their end-of-life.
- Controlled folder access is not enabled in Microsoft Windows Defender.

How ransomware gets installed:

- It is considered as a **network worm** as it has a transport and installing mechanism, the code first transports it to vulnerable devices, then it uses **EternalBlue** to gain access and **Double Pulsar** to install and execute a copy of itself.

How to protect against this attack and mitigation techniques:

- Regularly make offline backups to hard drives.
- Make sure that backup devices are not connected to any networking devices.
- **Make backups of Operating Systems Installations (Image Installations such as Acronis True Image) and verify whether the backups did not get corrupted. (keep backups separate from production systems).**
- Restrict code execution through OS Permissions.
- Restrict administrative and system access through Domains and Group Policies.

Protecting Emails and System Softwares from Ransomware:

- Apply Filters (not to be confused with spams) , in Gmail done through Filters and Blocked Addresses.

- Block Attachment Files in Emails.
- Remove Adminstrative Access Locally, and Restrict Access to critical system-level resources.
- Prevent Write Permissions
- Prevent Executions from User DIRS
- Whitelist / BlackList Applications
- Limit Access to network storage / shares.
- If we cannot prevent write, then limit write permission to just user/downloads and user/documents.

Preventing At Network Level:

- Firewall should completely disable Remote Desktop Protocol (RDP)
- Spam Lists and Spam Detection to detect spam emails.
- Limit type of file extensions that can be delivered through email
- Incase backup was enabled on the infected PC, disable automatic backup on the PC.

COINMINING / CRYPTOJACKING:

There are browser based coinminers, advanced fileless miners and the basic executables.

Reasons Cryptojacking spreads in a Computer:

- Users click legitimate emails link that are infact phishing emails, the link runs a javascript that runs in the background as victim continues to browse websites.
- **Another way is** to spread the infected script through a website or advertisement that loads in / pops up in browser, so that the script automatically executes and sends the complex mathematical operations and results to the hackers server.
- The code is designed for separate network architectures, so that when it loads it tries every architecture until one works and then infects the machine.

Indications that a computer is affected by coinminers:

- **High CPU, GPU, Network Resource Usage.**
- **Overheating, slower response times and crashes**
- **Unusual amount of connections to cryptomining websites open.**

The Threat Reports tell us that hackers have shifted towards ransomware, as cryptomining became illegal in some countries and some mining platforms got banned / closed. E.g **Coinhive.**

In 2018, this cryptojacking attack resurfaced, in form of botnet, botnets are internet connected devices that are used for network traffic obfuscation and Distributed DoS Attacks.

The Goal of Cryptojacking and Coinmining attacks is to use CPU resources and Cloud CPU usage from enterprises and consumers.

Cryptojacking spreads through Docker containers, Networked Windows Computers to steal windows credentials, through P2P software and rTorrent clients, some routers that do not have updated patches e.g carrier-grade routers were also affected.

The number of these attacks using IoT devices as Botnets have increased by upto 70 %.

Some potentially unwanted applications and Grayware (Spyware, adware etc.) affect the performance of computer, they also get installed in older Mobile Operating System versions.

Security Companies identify many variants of these malwares, in variants the professional hacker disassembles, reassembles and/or slightly changes the code to be either:

1. Bugfree
2. Containing Bugs

If it contains bugs, intentionally it inhibits and restricts the spread of virus, so that it remains undetected for longer periods.

When the bugfree version is released, this spreads quickly through networks. So when other hackers obtain their own copies, they modify these viruses and then it becomes separate variants. So we need to identify each variant.

We can stop the spread of these viruses by constantly upgrading our softwares and creating mitigation strategies for each variants.

Stopping Spread of Cryptojacking Cryptoviruses:

- **Enable PUA Detection and** Install Verified Ad-Blocking Addons and Tools.
- **Intrusion Prevention and Machine Learning and Email Filtering.**
- Add Web Filters
- Install Antivirus softwares with anti-cryptojacking capabilities.
- **Mobile Device Management Softwares, with corporate policies, certificates and on-device configuration settings in addition to backend infrastructure can help reduce cryptojacking viruses.**
- **Over The Air Updates of softwares.**
- **Constantly Monitor Network and CPU Performance Metrics.**

Increase in Targeted Attack Groups (State-Sponsored / Political or Money/Data Gathering) Motivations :

- **Large operational groups like Butterfly, Turla and Dragonfly** use various tools, some are for gaining access to servers, some tools are used to compromise email servers or other network resources.
- These groups gather information about other groups / organizations / geographical areas
- Then these groups observe the network traffic patterns
- Then the malware is deployed on vulnerable websites / desktop machines / networked machines.
- These attack groups hide their operations through carefully designed networks / servers and virtual machines with encryption as well as mechanisms to hide server locations.
- They relocate the servers very often after and during the attacks. To remain undetected
- They use different tools, and they upgrade their tools with newer source codes.
- Some of their activites over networks can be traced, through which Antivirus vendors detect which tools , codes they use for their attacks.
- They only launch attacks on targets of interest to them: i.e those people who have some data,money, resources etc. and then they launch their attacks. These can be launched on multiple groups with multiple servers.
- They also target energy companies and the critical infrastructure of governments (since most of these groups are also state sponsored)

INFECTION / ATTACK VECTORS:

A Vector: is a method/path/procedure that the Attacking Group uses to execute Malicious code on a computer (due to which it spreads to many computers)

Common attack vectors include malware, viruses, email attachments, web pages, pop-ups, instant messages, text messages and social engineering.

- Attackers first identify the vulnerable computers in an organization / network
- Then they move on to specific computers of interest by mapping and traversing organizations network
- Groups with good operational security clean-up after they attack and thus remain undetected.
- IP Attribution and Digital Forensics can be done, but since IP Addresses change frequently, we can't detect in some cases who was using the machine with source-ip.
- IP Addresses are spoofable.
- Hosts use a single IP Address for multiple clients, e.g subnets, CIDR, and NAT.
- Social Engineering, Phishing and Typosquatting is employed.
- Active attacks include MITM Attacks, software vulnerabilities, email spoofing, domain hijacking and ransomware, compromised/trojanized software update packages.
- **Lateral Movement, in which** attackers compromise 1 computer on a network, and use it to attack other computers on the network. By exploring the network first and then identifying their targets.
- **Examples of Lateral Movements are: Stolen Credentials,** pass the hash, exploiting open network sharing centers.
- **Attackers also disguise viruses as other viruses, such as a network was compromised through spear-phishing emails and watering-hole attacks, then five months later a virus disguised as ransomware, (but it was actually a Disk Wiper), it deleted all files of victim but was disguised as a ransomware virus was used.**
- Sandworm group created a Disakil Trojan that was disguised as ransomware that encrypted key operating system files used by Linux.
- BadRabbit virus spread through SMB and Mimikatz (a tool capable of stealing passwords). It also used a hardcoded list of commonly used credentials to attempt to guess the passwords. This was a ransomware attack.
- The trends are either **Disruptive Attacks / Decoy Attacks vs Short-Term or Long-Term Trends** Attack groups focus on these ways and either create copycat versions of viruses or they modify a virus and name it something else, but after research it is found out that it was another virus.

SUPPLY-CHAIN SOFTWARE ATTACKS:

Supply chain software implementations use well-guarded networks. Attackers used Software updates as the attack vectors in this case.

In this attack malware is added into a legitimate software update package. This can occur in 3 ways:

- During production at the software vendor
- At a third-party storage location
- Through Redirection

This attack may provide attackers with elevated privileges, fast distribution of the attack, and penetration of well protected organizations by leveraging trusted channels.

- Compromise Software supplier directly.
- Hijacking DNS, domains, IP Routing or network traffic.
- Hijacking third party hosting services.

TYPES OF SUPPLY-CHAIN ATTACKS:

- Account Misuse
- Watering Hole Attacks
- Process Attacks
- Deliberate malicious applications
- Collateral Infections

MOBILE THREAT LANDSCAPE:

- Social engineering used to bypass android v6 permissions model.
- Ransomware uses voice recognition, forces victims to speak unlock code instead of typing the key. (in case phone had enabled this security feature)
- Ransomware using social media applications with payment sdks to facilitate barcode payments.
- MobileSpy using reactive tools to hook into events, such as sms text received, to trigger other actions and commands remotely.
- WAP websites, in which the virus automatically makes the victim sign-up on his website and then victim subscribes to the website to the paid services without consent.
- Rootnik creates a virtual space within android device that is used to install and run APK files without constraints.
- Devices already infected with adclicker were turned into DDoS bots that were commanded to repeatedly visit specific target URLs.
- Banking malware variants found to be using StackTraceElements API to derive decryption keys at runtime.
- Fake mobile apps with embedded JavaScript-based cryptocurrency miners.
- Fakeapp variant steals credentials of online aggregate service providers, covering up the trail by launching legitimate apps by using mobile deep linking URIs.
- **Grayware such as hack tools, accessware, spyware, adware, dialers, joke programs.**

FILE TYPES, DEVICE TYPES, AND SERVICE TYPES ATTACKED USING MALWARE ATTACKS(Pre-2018):

- Visual Basic Script(.vbs) and JavaScript (.js) files are among the most common type of malicious attachments.
- .exe, .jar, .docx, .doc, .html, .htm, .wsf , .pdf , .xml , .rtf
- **Telnet, HTTP , HTTPS , SMB , SSH , UPnP , FTP , CWMP , SNMP , Modbus services are the most frequently targeted IoT Services.**
- **Router, DVR, Network, Satellite Dish, DSL / Cable Modem, SOHO Router, NAS (Network Attached Storage) , Camera, PLC (Programmable Logic Controller) , Alarm Systems are the types of devices involved in the IoT attacks against Symantec Honeypot.**

MELTDOWN AND SPECTRE(2018):

Meltdown and Spectre are critical hardware vulnerabilities in the Modern CPUs. These allow programs to steal data which is currently processed on the computer. Using this vulnerability a malicious program can get a hold of secrets and passwords stored in the memory of other running programs. This might include passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business critical documents.

In Meltdown Bug, We Read (Kernel Memory from User Space) breaks fundamental isolation between user applications and Operating system, this attack allows a program to access the memory and the secrets of other programs and OS.

Spectre breaks isolation between different applications, it allows attacker to trick error-free programs, which follow best practices, into leaking their secrets.

Internet Security & Threat Report (v. 2019):

- Malicious URLS, Formjacking , Cryptojacking and Ransomware(Both on the enterprise and the mobile threat landscap) , increased.
- Increase in Malicious Email
- Increase in Powershell Scripts.

Formjacking

The use of malicious javascript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce WebSites.

These attacks are carried out on well-guarded supply chain networks.

In these attacks the Smaller businesses and their websites are infected with viruses, which in turn connect to the larger networks that are secure. And thus, this infection spreads.

Malware Trends in 2019 and Malware Removal Techniques:

- There is a drop in ransomware attacks, this is because of **Behaviour analysis, machine learning and email security and filters applied on Email Clients**.
- Microsoft Office files like docx,doc etc have embedded macro programs inside them. These can also include xml and/or **DDE payloads**.
- Living Off the Land attacks, in which the attacker uses pre-installed software and applications, instead of using own tools to attack the system. So that he exploits bugs in existing systems.
- Poorly secured cloud databases such as S3 Buckets.
- If any cloud databases are open, they are vulnerable to ransomware attacks, in which contents are wiped and afterwards the container deployment systems such as Kubernetes or serverless applications and other publicly exposed api services are targeted.
- Amazon Simple Storage Service(S3) recommends Bucket policies and User policies available for granting permissions to amazon s3 resources. Both use json-based access policy language.

MELTDOWN AND SPECTRE , Cloud Services, VPNFilter And Other 2019 Malware (v. 2019):

- In cloud computing, resources such as storage, processing, memory, network bandwidth and virtual machines are provided to end-users.
- The resources from individual computers are aggregated into shared pools of configurable computing resources.
- These shared pools are the target of Meltdown and Spectre vulnerability.
- **A Successful attack on even a single physical system could result in data being leaked from several cloud instances.**
- **Speculative Store Bypass, and Foreshadow were also subsequent vulnerabilities and released after meltdown and spectre.**
- **Unpatched Routers and Linux Servers were the target of DDoS attacks.**
- **Industrial Control Systems** were the target in 2018.
- **VPNFilter is an IoT Threat.** was an attack that worked even after the system rebooted, this attack had man in the middle, data exfiltration, credential theft and SCADA Communications (which in turn affects LAN, SONET, radio , modem or serial line communication) as sub-tools inside the toolkit. And also had the option to “brick” a device. Which would render the device useless if the attacker wanted to remove all traces of evidence.

ALBERT NETWORK MONITORING:

This is a cost-effective Intrusion Detection System that uses open source software combined with Signature Set:

- Commercial Signatures that are optimal for detecting standard malware and crimeware
- Advanced Persistent Threat (APT) indicators.
- CIS research and open source reporting.

NetFlow Record is a summary of data exchange between two systems, it’s based on 7 distinct characteristics:

1. Source IP
2. Destination IP
3. Source Port
4. Destination Port
5. TCP Flags
6. Number of bytes of traffic sent and received.
7. Timestamp information (start, end, and duration of connection)

Albert Service utilizes 1U server (or VM for smaller installations) by way of network tap or data aggregator (such as gigamon) . and for smaller networks this uses span port off a router or switch.

Monitoring includes Management of sensor, maintaining OS, IDS Engine, NetFlow tools , and signature sets.

2019 Threat Summary:

- Email Malware, Spear Phishing Emails and Emotet increased in 2018.
- .doc , .dot , .exe , .rtf , .xls , .xlt , .xla , .jar, .html , .htm , .docx , .vbs , .xlsx , .pdf extensions of files were most commonly used in the attacks. With scripts taking 48 % , executables taking 26 % and other files taking 25 % of the total attacks carried out.
- Mobile App categories that were targeted (In Descending Order of Attack Percentage are):
    1. Tools
    2. Lifestyle
    3. Entertainment
    4. Social & Communication
    5. Music & Audio
    6. Brain & Puzzle Games
    7. Photo & Video
    8. Arcade & Action Games
    9. Books & References
    10. Education Apps.

Top Mobile Malwares are:

1. Malapp
2. Fakeapp
3. MalDownloader
4. FakeInst
5. MobileSpy
6. HiddenAds
7. PremiumText
8. Mobilespy
9. Hiddenapp
10. Opfake

Web Attacks Domains Included:

- Dynamic DNS
- Gambling
- Hosting
- Technology
- Shopping
- Business
- Health
- Educational
- Content Delivery Networks

IoT Device Types Performing the Attacks are:

1. **Router**
2. **Connected Camera**
3. **Multimedia Device**
4. **Firewall**
5. **PBX Phone System**
6. **Network Attached Storage**
7. **VoIP Phone**
8. **Printers**
9. **Alarm Systems**
10. **VoIP Adapter.**