BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session No: 02

Agenda

- Tools & Techniques
  - Rootkits
  - Covert-channels
  - Sniffing
  - MITM
  - Botnets
  - Covering the traces
  - Camouflage
  - Defeat forensics
  - Use cases and discussions

Introduction

What is a Rootkit?

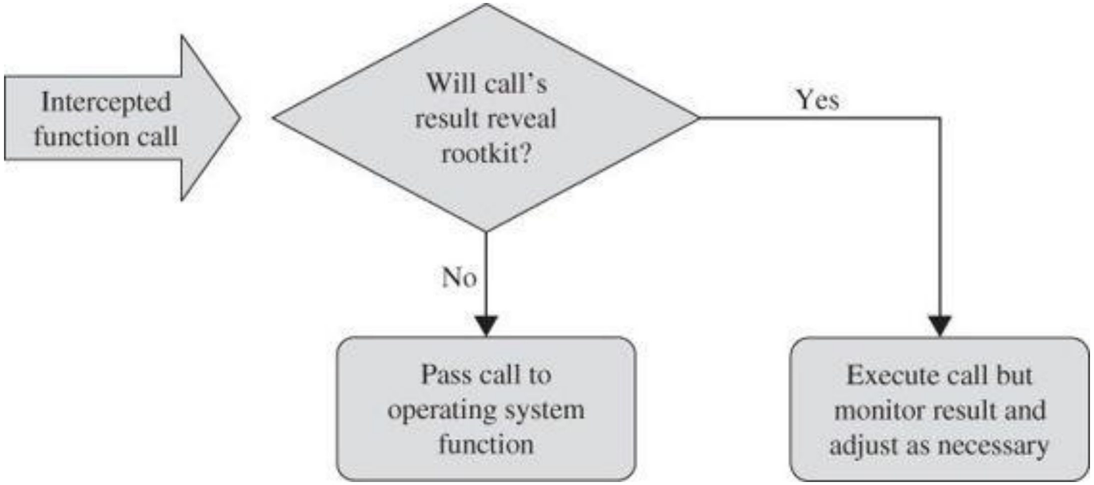
- ROOTKIT is a piece of designed to hide itself (so that it remains undetected) and its processes, data and/or activities on the system.
- ROOTKIT is used to open a backdoor so that the attacker can have uninterrupted access to the compromised machine
-
- Q: Is a rootkit virus or worm?

Rootkit Capabilities

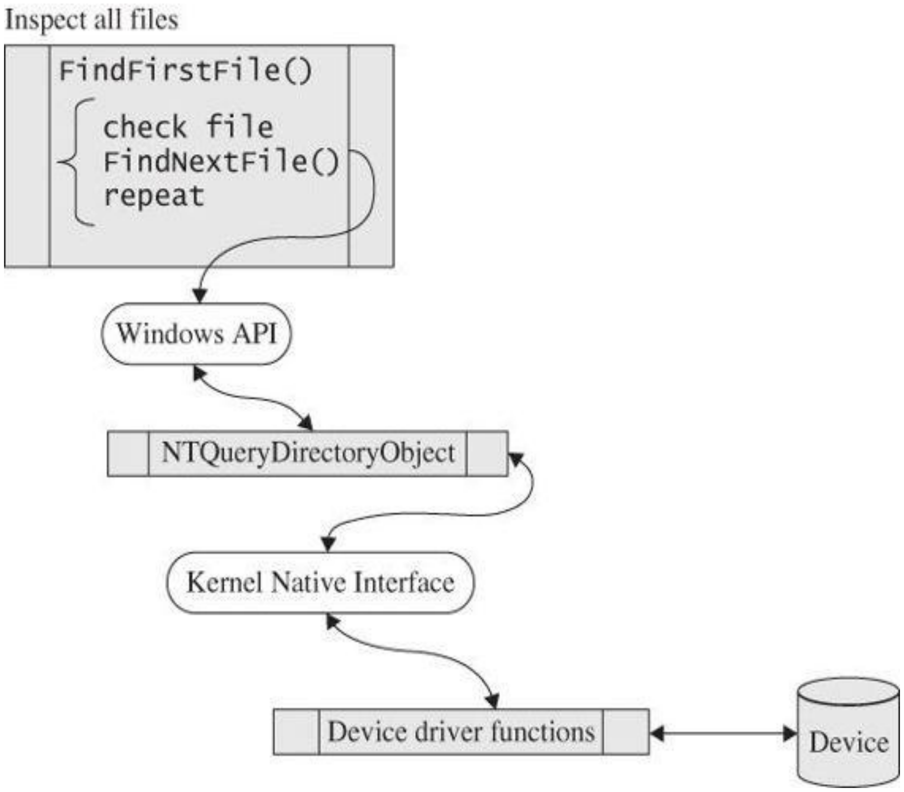
- Hides processes
- Hides files
- Hides registry entry
- Hides services
- Bypasses personal firewalls
- Undetectable by anti-virus software
- Can create covert channels – undetectable on network
- Defeats cryptographic hash checking
- Installs silently – no logs etc

How rootkit evades detection

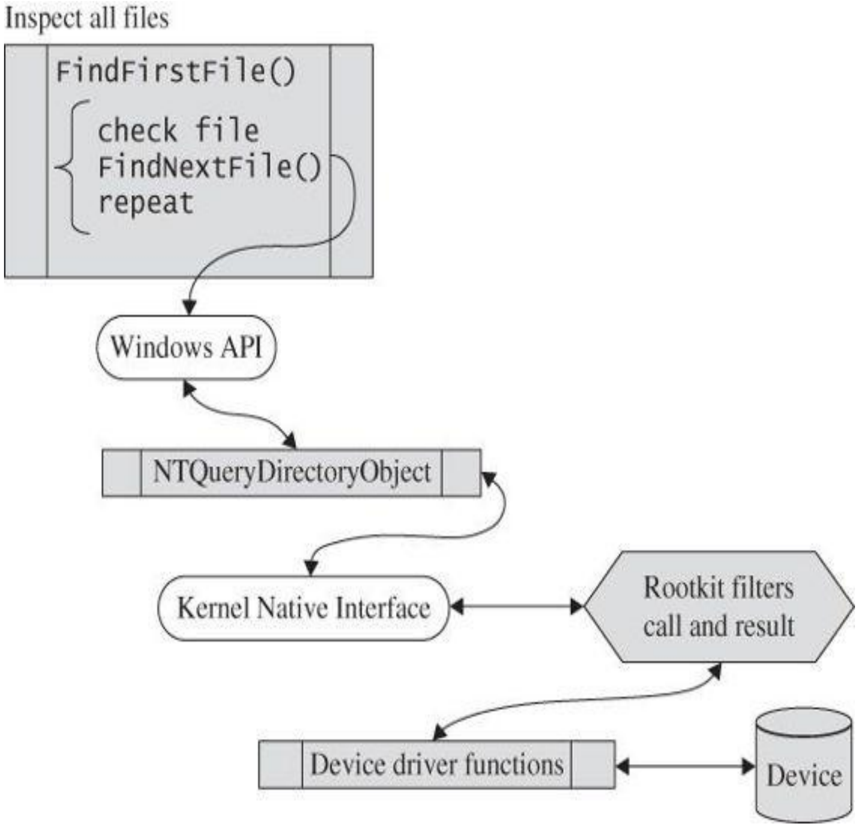
- Rootkits intercept the operating systems calls then alter results of the call if required. This allows rootkit to evade it’s detection – antivirus tools or operating system tools


Intercepted function call
Will call’s result reveal rootkit?
Yes
No
Pass call to operating system function
Execute call but monitor result and adjust as necessary

How rootkit evades detection…



Normal OS call execution



Rootkit controlled OS call execution

Rootkit Revealer Tools

- Ice Sword
- F-Secure Black Light
- Rootkit Revealer
- Dark Spy
- System Virginity Verifier
- RK Detector

Covert Channel

- A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy.
- Covert channels transfer information using non-standard methods against the system design.
- Covert channel allows the communication of information by transferring objects through existing information channels or networks using the structure of the existing medium to convey the data in small parts.
- Covert channels have been used to steal data from highly secure systems

Covert Channel Examples

- Jeremiah Denton, a prisoner of war during the Vietnam War, used a covert channel to communicate without his captors' knowledge. Denton was interviewed by a Japanese TV reporter, and eventually a videotape of the interview made its way to the United States. As American intelligence agents viewed the tape, one of them noticed Denton was blinking in an unusual manner. They discovered he was blinking letters in Morse code. The letters were T-O-R-T-U-R-E, and Denton was blinking them over and over. This is a real-world example of how a covert channel can be used to send a communication message undetected.
- In computers, a property of a file can be used to deliver information rather than the file itself. An example can be creation of a seemingly innocent computer file 16 bytes in size. The file can contain any data as that is not the important information. The file can then be emailed to another person. Again, it seems innocent enough but the real communication is of the number 16. The file size is the important data, not the contents of the file.

Covert Channel Example

- Some covert channels rely on a technique called tunneling, which lets one protocol be carried over another protocol.
- Internet Control Message Protocol (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system.
  - Ping command is a generally accepted troubleshooting tool using ICMP protocol.
  - For that reason, many router, switches, firewalls, and other packet filtering devices allow the ICMP protocol to be passed through the device.
- Loki is a hacking tool that provides shell access over ICMP, making it much more difficult to detect than TCP or UDP based backdoors.
  - The network thinks, a series of ICMP packets are being sent across the network.
  - Hacker sends commands from Loki client and executing them on the server.
  - https://www.skillset.com/questions/the-hacking-tool-loki-provides-shell-access-to-the-attacker-over-6083
- Reference: https://www.hackingarticles.in/covert-channel-the-hidden-network/

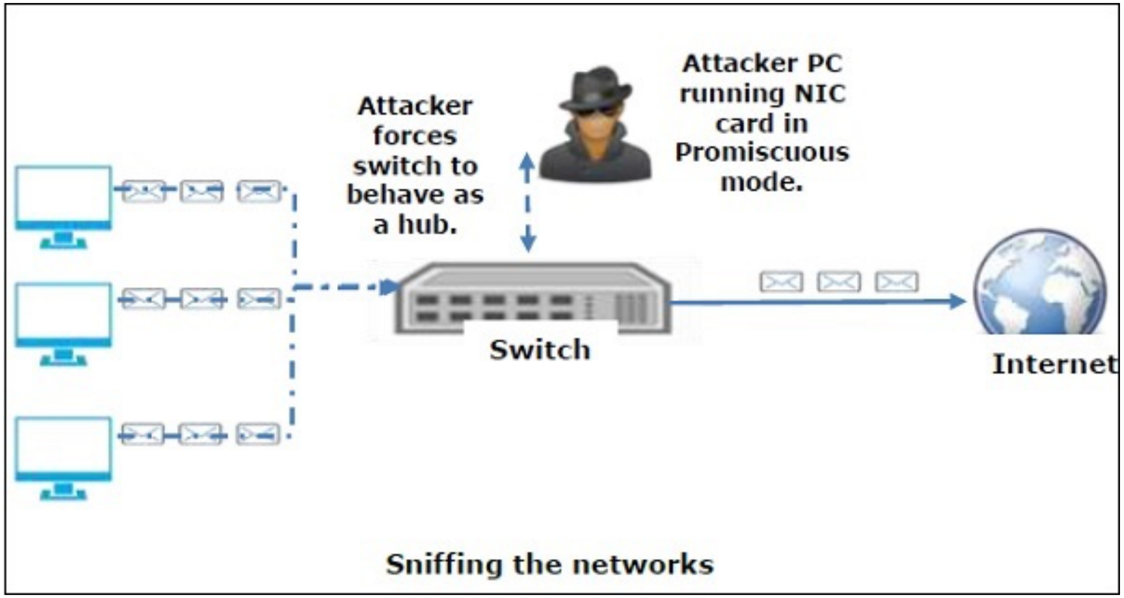
Exercise

- http://www.spammimic.com

Sniffing

- Sniffing is the process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers.
- Packet Sniffers (network protocol analysers) are used by network administrators to keep track of data traffic passing through their network.
- **Active Sniffing:**
  - Conducted on a switched network.
  - Switch is a device that connects two network devices together.
  - Switches use the media access control (MAC) address to forward information to their intended destination ports.
  - Attackers take advantage of this by injecting traffic into the LAN to enable sniffing.
- **Passive Sniffing:**
  - Uses hubs instead of switches.
  - Hubs perform the same way as switches only that they do use MAC address to read the destination ports of data.
  - All an attacker needs to do is to simply connect to LAN and they are able to sniff data traffic in that network.

How does Sniffing Work?


Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet
Sniffing the networks

- Sniffing is similar to that of “tapping phone wires” and try to know the conversation details (**wiretapping**).
- Information sniffed normally includes:
  - Email traffic
  - FTP passwords
  - Web traffics
  - Telnet passwords
  - Router configuration
  - Chat sessions
  - DNS traffic

Sniffing Tools

- **BetterCAP:** Perform various types of MITM attacks, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials etc.
- **Ettercap:** Comprehensive suite for MITM attacks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
- **Wireshark:** One of the widely used packet sniffers. It offers many features to analyse traffic.
- **Tcpdump:** Well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network.
- **WinDump:** A Windows port of the tcpdump.
- **OmniPeek:** A commercial product that is the evolution of the product EtherPeek.
- **Dsniff:** A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords on Unix & Linux platforms.
- **EtherApe:** Linux/Unix tool with graphical display of incoming and outgoing connections.
- **MSN Sniffer:** Sniffing utility specifically designed for sniffing MSN Messenger traffic.
- **NetWitness NextGen:** It includes a hardware-based sniffer to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.

How to Detect Sniffing?

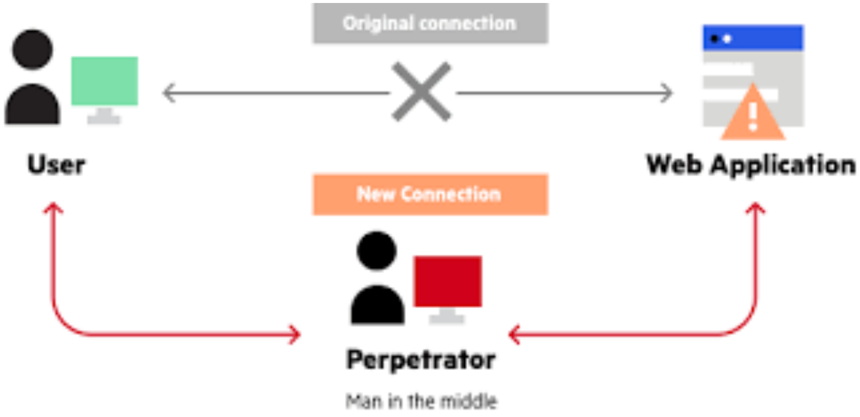
- Sniffers normally collect data and are difficult to detect.
- Easier to detect a sniffer on a switched ethernet network segment. The techniques are:
  - **Ping method:** Sniffer might respond to the ping if the suspect machine is still running. It is a not strongly reliable method.
  - **ARP method:** Machines always capture and caches ARP. Upon sending a non-broadcast ARP, the sniffer/promiscuous machine will cache the ARP and it will respond to our broadcast ping
  - **On Local Host:** Logs can be used to find if a sniffer is being used.
  - **Latency method:** Ping time is generally short. If the load is heavy by sniffer, it takes long time to reply for pings.
  - **ARP Watch:** Used to trigger alarms when it sees a duplicate cache of the ARP.
  - **Using IDS:** Intrusion detection systems monitors for ARP spoofing in the network.

Man In The Middle (MITM)

- Man-In-The-Middle attack intercepts a communication between two systems.
- The attacker splits the original connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server.
- Once the connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.
- The MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based.
- The MITM attack could also be done over an https connection. It consists in the establishment of two independent SSL sessions, one over each TCP connection.
- The browser sets a SSL connection with the attacker, and the attacker establishes another SSL connection with the web server.
- Normally, browser warns the user that the digital certificate used is not valid, but the user may ignore the warning because they don’t understand the threat.

MITM Attack Tools

- MITM attack tools are particularly efficient in LAN network environments as they implement extra functionalities, like ARP spoof capabilities to intercept communication between hosts.
- Few popular once are:
  - PacketCreator
  - Ettercap
  - Dsniff
  - Cain e Abel



MITM Attack Types

- **IP spoofing:** Spoofing of the IP address of target server which a victim wants to connect
- **DNS spoofing:** A technique that forces a user to a fake website rather than the real one the user intends to visit.
- **HTTPS spoofing:** Attacker can fool browser into believing it's visiting a trusted website when it's not. By redirecting browser to an unsecure website, the attacker can monitor your interactions with that website and possibly steal personal information.
- **SSL hijacking:** Attacker uses another computer and secure server and intercepts all the information passing between the server and the user's computer.
- **Email hijacking:** Taking over the email accounts of banks and other financial institutions and monitor transactions between the institution and its customers. The attackers can then spoof the bank's email address and send their own instructions to customers.
- **Wi-Fi eavesdropping:** Cybercriminals can set up Wi-Fi connections with legitimate sounding names. Once a user connects to the fraudster's Wi-Fi, the attacker will be able to monitor the user's online activity and be able to intercept login credentials, payment card information, and more.
- **Stealing browser cookies:** A cybercriminal can hijack browser cookies which store information from user browsing session enabling attacker to gain access to passwords, address, and other sensitive information.

MITM Attack Prevention

- Ensure “HTTPS” — with the S — is always in the URL bar of the websites you visit.
- Be wary of potential phishing emails from attackers asking to update password or any other login credentials. Instead of clicking on the link provided in the email, manually type the website address into browser.
- Never connect to public Wi-Fi routers directly, if possible. A VPN encrypts internet connection on public hotspots to protect the private data you send and receive while using public Wi-Fi, like passwords or credit card information.
- Since MITB attacks primarily use malware for execution, you should install a comprehensive internet security solution, such as Norton Security, on your computer. Always keep the security software up to date.
- Be sure that your home Wi-Fi network is secure. Update all of the default usernames and passwords on your home router and all connected devices to strong, unique passwords.

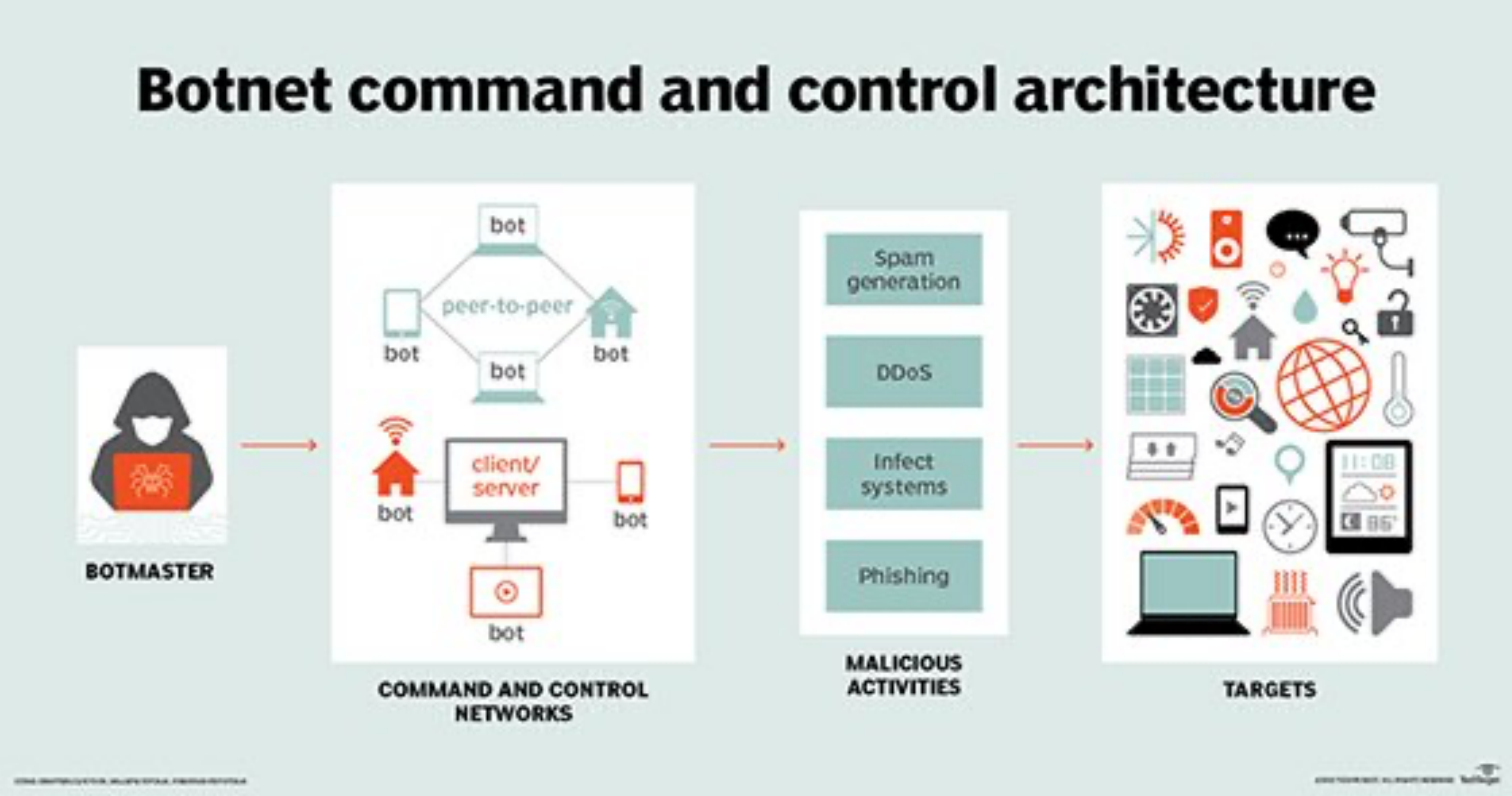
Botnets

- A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Attackers use botnets to for malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks. Common botnet actions are:
- **Email spam:** Used for sending out spam messages in huge numbers. The Cutwail botnet can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.
- **DDoS attacks:** Leverages the massive scale of the botnet to overload a target network or server with requests, rendering it inaccessible to its intended users.
- **Financial breach:** Includes botnets specifically designed for the direct theft of funds from enterprises and credit card information. ZeuS botnet is one such example.
- **Targeted intrusions:** Smaller botnets designed to compromise specific high-value systems of organizations (R&D, Financials, IP etc) from which attackers can penetrate and intrude further into the network.

Protection from Botnets

- Use a good Internet security suite that detects and removes a malware from machine and prevents future attacks.
- Always update your computer’s operating system as early as possible. Hackers often utilize known flaws in operating system security to install botnets. You can even set your computer to install updates automatically.
- The same is true of applications on your computer, phone and tablet. Once weakness are found and announced by software companies, hackers rush to create programs to exploit those weaknesses.
- Don’t download attachments or click on links from email addresses you don’t recognize.
- Use a firewall when browsing the Internet. Use pre-installed firewall on Mac while install a good third party firewall on Windows based machine.
- Don’t visit websites that are known distributors of malware. Use a full-service Internet security suite to warn you when you’re visiting such sites.

Protection from Botnets



Covering the Tracks

- Hiding of digital footprints is the final stage of penetration testing.
- Ethical hackers cover their tracks to maintain their connection in the system and to avoid detection by incident response teams or forensics teams.

Covering the Tracks

- **Using Reverse HTTP Shells**
- An ethical hacker installs reverse HTTP shells on the victim computer and uses it to send communications to the network's server. The reverse shell is designed in a way that the target device will always return commands. This is possible since port 80 is always open, and therefore, these commands are not flagged by the network's perimeter security devices like firewalls. The hacker can now gain any information from the server undetected leaving no footprint behind since all they did was send HTTP commands.
- **Using ICMP Tunnels**
- The ICMP is used by a network device to test connectivity using echo requests. Ethical hackers encapsulate these echo requests with TCP payloads and forward them to the proxy server. This request is then de-capsulated by the proxy server, which extracts the payload and sends it to the hacker. The network's security devices read this communication as simple ICMP packet transfer hence facilitating the hacker in covering their tracks.
- **Clearing Event Logs**
- By using Metasploit's Meterpreter. First, the hacker must exploit a network using Metasploit. After a successful exploit, the ethical hacker uses the Meterpreter command prompt and uses the script "clearev" to clears all the event logs. Event logs can also be cleared using the clearlog.exe file. After deleting the event logs, the hacker removes the clearlog.exe file from the system. Event logs in Linux systems can also be deleted using text editors such as "kWrite". Logs in Linux systems are stored in the "/var/logs" directory.
- **Erasing or Shredding Command History**
- If the hacker is in a hurry and does not have time to go through all the event logs, they could cover their tracks by erasing and shredding the command history. Ethical hackers delete their bash history (can store upto 500 commands) by resetting its size to zero using command "export HISTSIZE=0". The history file could also be shredded using the command "shred -zuroot/bash_history".

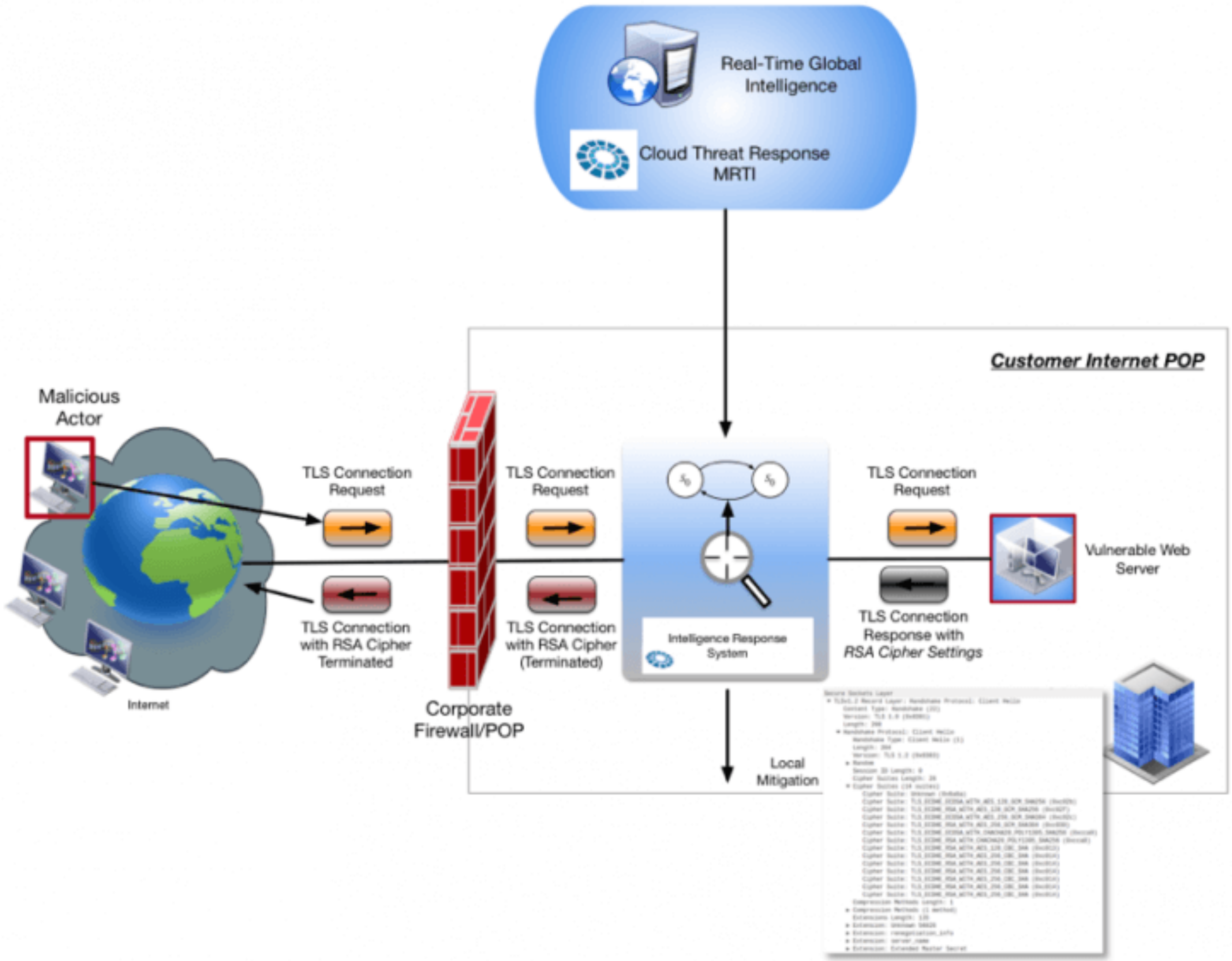
Camouflage

- **Camouflage**: the act, means, or result of obscuring things to deceive an enemy by painting or screening objects so that they are lost to view in the background, or by making up objects that from a distance have the appearance of fortifications.
- **Deception**: to mislead by a false appearance or statement.

Camouflage Defense startegy

- Predicting Attacks
  - Ability to gather low-false positive threat intelligence on adversary tactics, indicators…etc.
  - Ability to more easily understand goals, motives, intent
- Detecting Activities
  - Ability to gather more advanced detection when other protections fail
  - Early alerting and notification to operations without impact to business-critical systems
- Disrupting & Responding
  - Easily engage with attackers and their TTPs
  - Easy reconnaissance on the attacks
  - Manipulation of behaviors and interactions that confuse, delay, or interrupt attacker's activities
  - Increase the cost, expertise required, and impact on the attacker

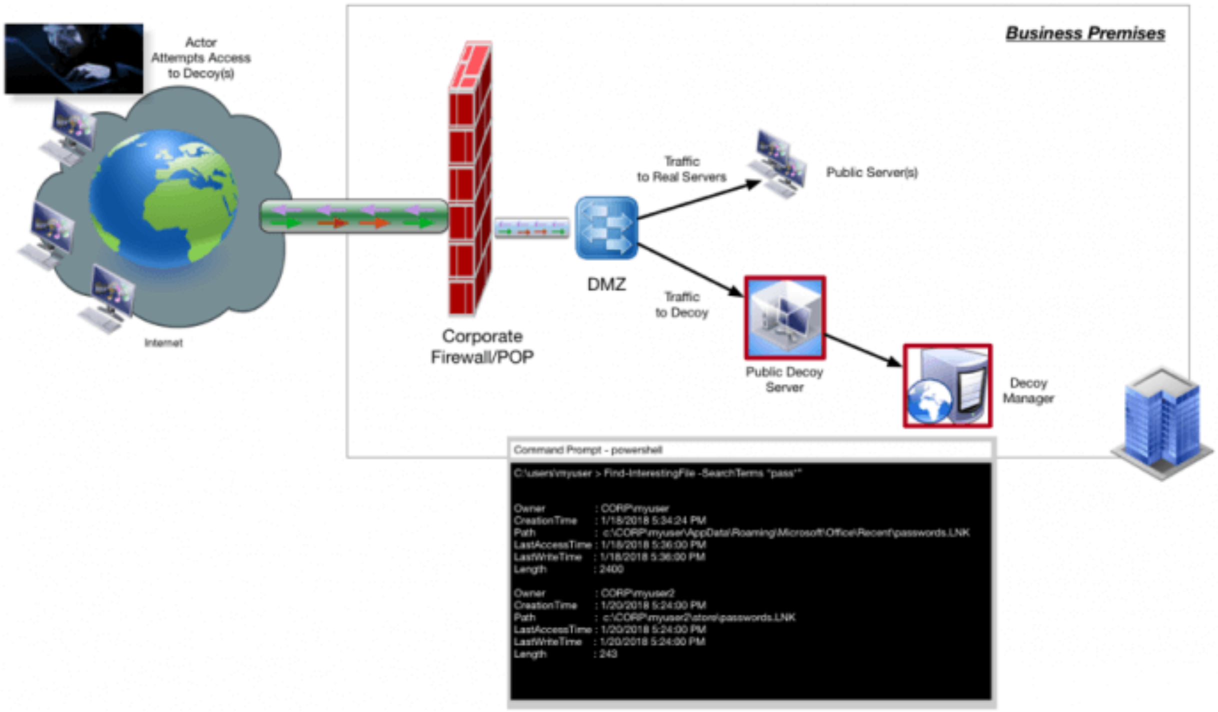
Network based – Camouflaging unpatched server


Real-Time Global Intelligence
Cloud Threat Response MRTI
Customer Internet POP
Malicious Actor
TLS Connection Request
TLS Connection Request
TLS Connection Request
Vulnerable Web Server
TLS Connection with RSA Cipher Terminated
TLS Connection with RSA Cipher (Terminated)
TLS Connection Response with RSA Cipher Settings
Intelligence Response System
Internet
Corporate Firewall/POP
Local Mitigation

```
Secure Sockets Layer
▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 200
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: [illegible]
      Version: TLS 1.2 (0x0303)
    ▸ Random
      Session ID Length: 0
      Cipher Suites Length: 28
    ▾ Cipher Suites (14 suites)
        Cipher Suite: Unknown ([illegible])
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Compression Methods Length: 1
    ▸ Compression Methods (1 method)
      Extensions Length: [illegible]
    ▸ Extension: Unknown [illegible]
    ▸ Extension: renegotiation_info
    ▸ Extension: server_name
    ▸ Extension: Extended Master Secret
```

- IT & security teams are often unable to keep up with the continuous challenge of maintaining software patch levels on all servers.
- Unpatched servers remain vulnerable to being exploited.
- Network-based camouflage is another way to protects against certain types of vulnerabilities.
- This involves obfuscation and camouflage by an intermediary network system configured to do so based on threat intelligence on the vulnerabilities.

Server Decoys



```
C:\users\myuser > Find-InterestingFile -SearchTerms "pass*"

Owner          : CORP\myuser
CreationTime   : 1/18/2018 5:34:24 PM
Path           :  c:\CORP\myuser\AppData\Roaming\Microsoft\Office\Recent\passwords.LNK
LastAccessTime : 1/18/2018 5:36:00 PM
LastWriteTime  : 1/18/2018 5:36:00 PM
Length         : 2400

Owner          : CORP\myuser2
CreationTime   : 1/20/2018 5:24:00 PM
Path           :  c:\CORP\myuser2\store\passwords.LNK
LastAccessTime : 1/20/2018 5:24:00 PM
LastWriteTime  : 1/20/2018 5:24:00 PM
Length         : 243
```

- Deception techniques are alternative or addition to camouflage.
- Use of decoy systems that impersonate legitimate systems that can act as an enticement to attackers.
- The endpoint decoy can provide vital insight to the TTPs performed by those actors.
- Decoys engage an attacker to explore/ spend time to analyse false data provided by the decoy.
- This increases the time the attacker is under watch and provides useful intelligence on their objectives.

What is Anti-Forensics

- Approach to criminal hacking with an objective – Make it hard for them to find you and even harder for them to prove they found you.
  - Data hiding – encryption, steganography, hardware/software based concealment
  - Artifact hiding – Disk cleaning utilities (Cyber scrub, CyberCide, KillDisk), File wiping utilities (BC wipe, Eraser Cyber scrub)
  - Trail obfuscation – log cleaners, timestamp modification, misinformation, spoofing, trojan command
  - Attacks against computer forensics
  - Counter forensic tools

Defeat Forensics

- Techniques for anti-forensics
  - Encryption
  - Steganography
  - Tunnelling
  - Onion routing
  - Obfuscation
  - Spoofing: IP. & MAC spoofing

Understand Trust Boundaries

- **BetterCAP** – BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.

Stuxnet: Rootkit for Industrial Control Systems

- Stuxnet: Destroyed Iranian nuclear facility

  http://virus.wikidot.com/stuxnet

- What is a root kit

  https://www.varonis.com/blog/rootkit/

Thank You