BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session No: 15 (Wannacry Ransomware)

Agenda

innovate achieve lead

- Case Study: WannaCry Ransomware
  - Overview
  - Technical Details
- Metasploit Framework Introduction

WannaCry Ransomware

Overview

- Known as “WannaCry,” “WCry” or “WanaCrypt0r” (based on strings in the binary and encrypted files).
- Was released in early Mar 2017 and spreads automatically (worm).
- Started at UK NHS and the quickly spread through world.
- Exploits a remote code vulnerability in Windows XP using SMB.
- Encrypts user files and demands a fee of $300 to $600 worth of bitcoins to an address specified in the instructions displayed after infection.
  - $ 300 for payment within 3 days
  - $ 600 for payment between 3 to 6 days
  - Files deleted after 6 days if payment not done

Overview

- WannaCry has 3 key components:
  - Dropper
  - Encrypter
  - Decrypter
- Dropper contains the Encrypter as an embedded resource
- Encrypter contains:
  - A Decrypter (“Wana Decrypt0r 2.0”),
  - A password-protected zip containing a copy of Tor,
  - Multiple individual files with configuration information and encryption keys
- SHA256 Hash values:
  - Dropper 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
  - Encrypter 01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
  - Decrypter b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Overview

- WannaCry primarily utilizes the ETERNALBLUE modules and the DOUBLEPULSAR backdoor.
- ETERNALBLUE is used for the initial exploitation of the SMB vulnerability.
- If successful, DOUBLEPULSAR backdoor is planted to install the malware and future communication.
- If the DOUBLEPULSAR backdoor is already installed, WannaCry leverages it to install the ransomware payload.
- This makes WannaCry as a worm and spread across the internet.

Execution Flow

- The high level flow is as follows:
  - Begins with an initial beacon which is basically a kill switch function
  - If it makes it past that step, then it looks to exploit the ETERNALBLUE/MS17-010 vulnerability and propagate to other hosts
  - Then it lays the foundations for doing the damage and getting paid for recovery
  - Then it starts encrypting files on the system
  - Finally exits the system with payment note display and ransomware file cleanup.

High Level Analysis

- Initially a file "mssecsvc.exe" is dropped which executes "tasksche.exe", this exe tests the kill switch domains.
- If Kill switch domain is not present, a service “mssecsvc2.0” is created as a method of persistence for WannaCry.
- “mssecsvc2.0” executes "mssecsvc.exe" with a different entry point than the initial execution.
  - This second execution executes 2 threads.
  - First thread checks the IP address of the infected machine and attempts to connect to TCP445 (SMB) of each host/IP address in the same subnet.
  - Second thread generates random IP address on Internet to perform same action.
  - When the malware successfully connects to a machine, a connection is initiated and data is transferred.
  - WannaCry exploits the SMB vulnerability addressed by Microsoft in the bulletin MS17-010 (ETERNALBLUE) to implant the DOUBLEPULSAR backdoor.
  - Backdoor is used to execute WannaCry on the new compromised system.

High Level Analysis

- “tasksche.exe” checks for disk drives, network shares and removable storage devices mapped to a letter, such as 'C:/', 'D:/' etc.
- WannaCry then checks for files with supported file extensions and encrypts these using 2048-bit RSA encryption.
- While the files are being encrypted, it creates a new file directory 'Tor/' into which it drops tor.exe and nine dll files used by tor.exe.
- Additionally, it drops two further files: taskdl.exe & taskse.exe.
  - “taskdl.exe” deletes temporary files while “taskse.exe” launches @wanadecryptor@.exe to display the ransom note on the desktop
  - @wanadecryptor@.exe is not a ransomware itself but only the ransom note
  - Encryption is performed in the background by tasksche.exe
  - “tor.exe” file is executed by @wanadecryptor@.exe
  - This execution process initiates network connections to Tor nodes
  - This allows WannaCry to attempt to preserve anonymity by proxying their traffic through the Tor network

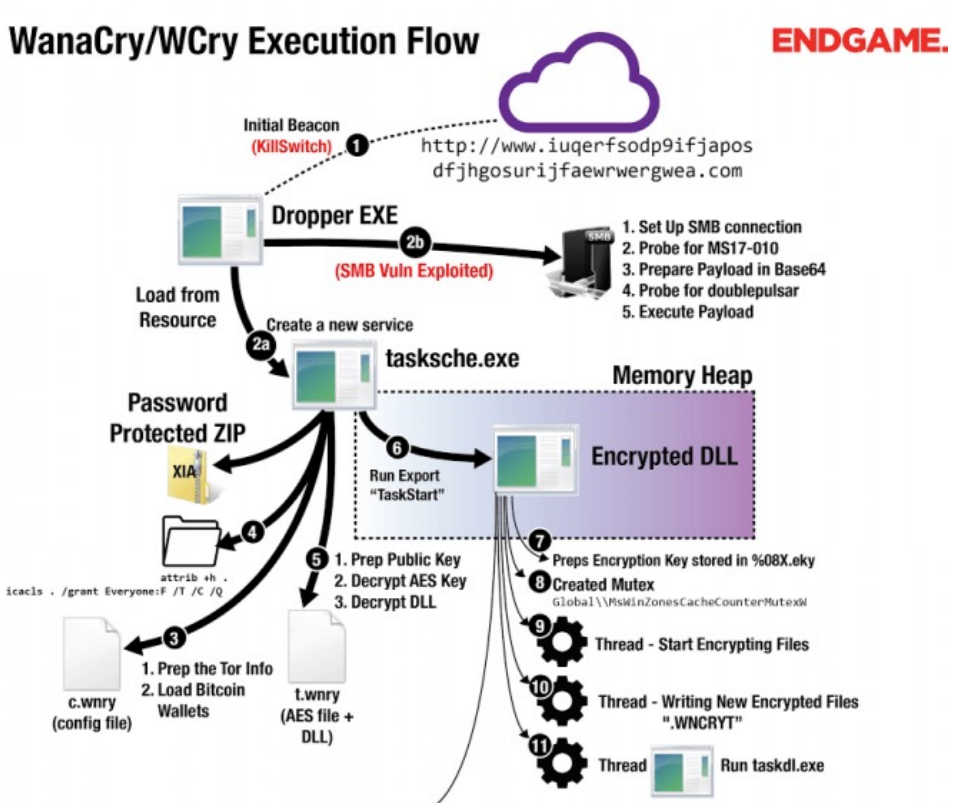
High Level Analysis

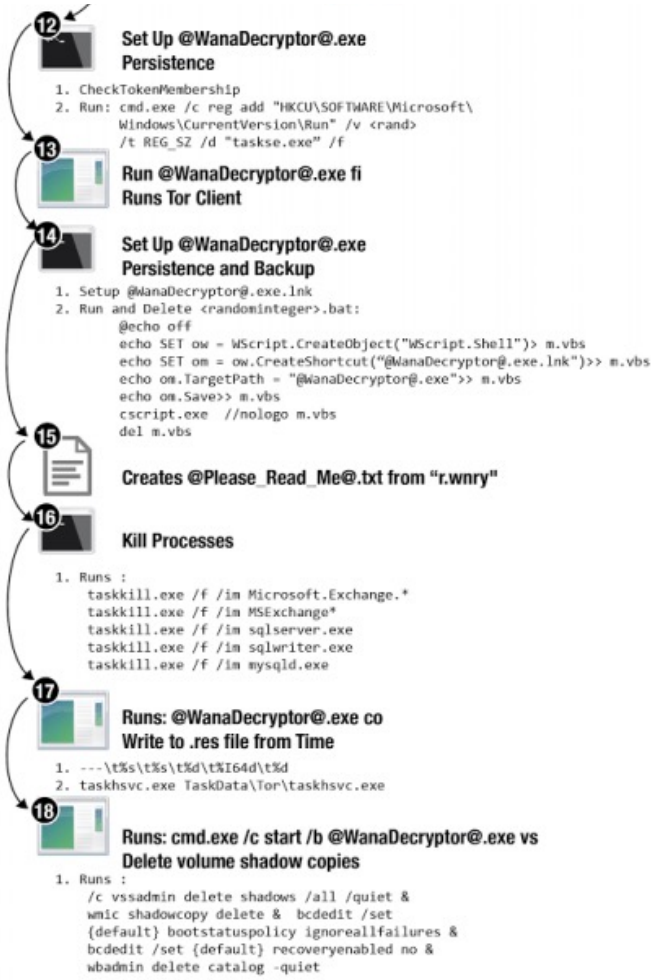
- WannaCry deletes any shadow copies on the victim's machine in order to make recovery more difficult. It uses WMIC.exe, vssadmin.exe and cmd.exe for this.

Process ID	Process Name	Command Line
29 (cmd.exe)	cmd.exe	cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
30 (vssadmin.exe)	vssadmin.exe	vssadmin delete shadows /all /quiet
35 (WMIC.exe)	WMIC.exe	wmic shadowcopy delete

- WannaCry uses multiple methods to aid its execution by leveraging both attrib.exe to modify the +h flag (hide) and also icacls.exe to allow full access rights for all users, "icacls . /grant Everyone:F /T /C /Q”
- WannaCry has been designed as a modular service.
  - Potentially, this structure of WannaCry can be used to deliver and run different malicious payloads.
- After encryption is over, WannaCry displays the ransomware payment note
  - Ransomware screen is an executable and not an image, HTA file, or text file.

Execution Flow





Ref: https://www.elastic.co/blog/wcrywanacry-ransomware-technical-analysis

Exploit Details

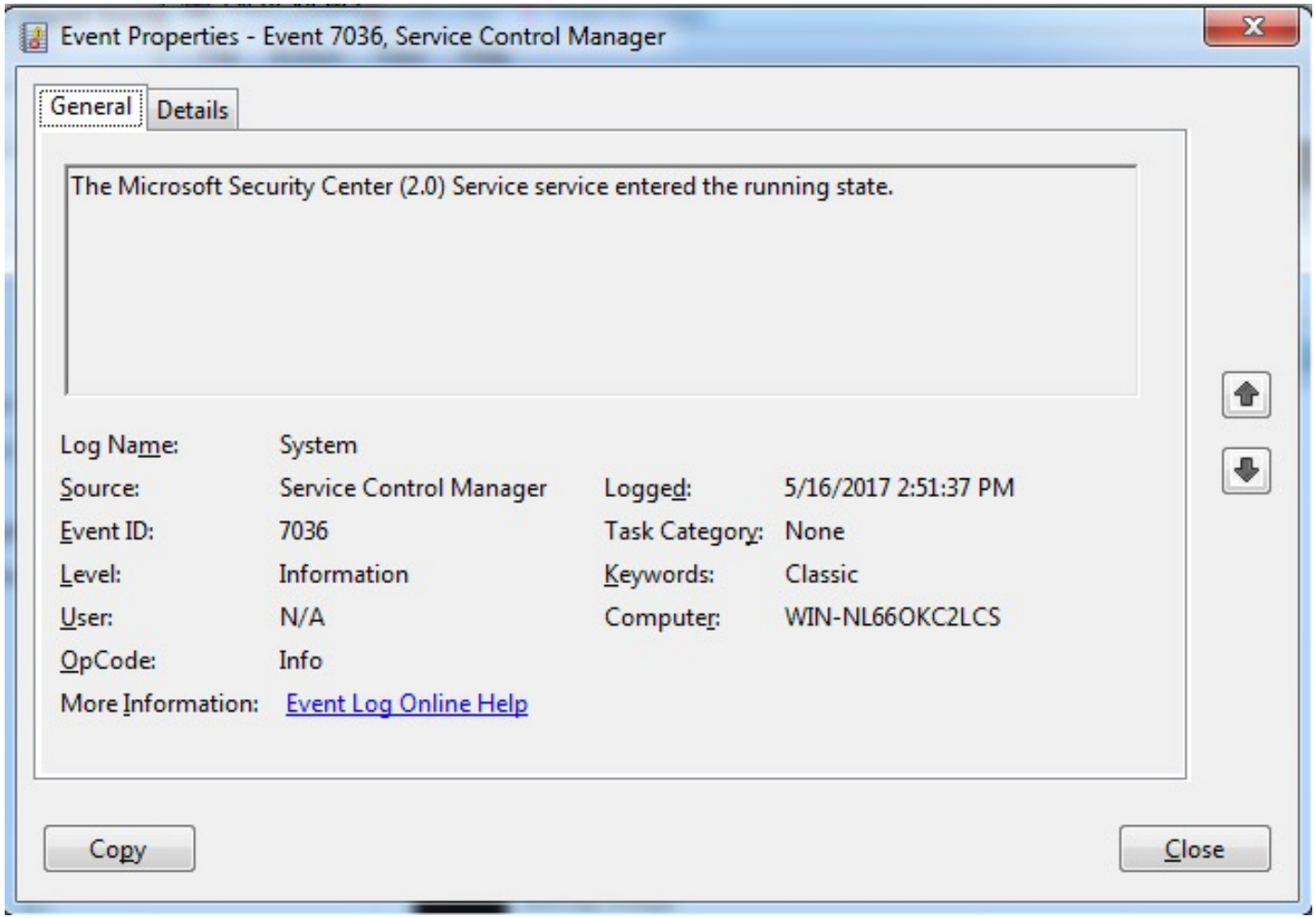
- The exploit EternalBlue, exploits a vulnerability in the Server Message Block (SMB) protocol which allows WannaCry to spread to all unpatched Windows systems from XP to 2016 on a network that have this protocol enabled.
- This vulnerability allows remote code execution over SMB v1.
- WannaCry utilizes this exploit by crafting a custom SMB session request with hard-coded values based on the target system.
- After the first SMB packet sent to the victim's IP address, WannaCry sends two additional packets to the victim containing the hard-coded IP addresses 192.168.56.20 and 172.16.99.5.

Exploit Details

innovate achieve lead

- Dropper on execution, attempts to make a connection to a domain ***http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com***
  - Execution 'exits' if the connection is successful
  - This domain was unregistered at the time of WannaCry release, hence causing this connection to fail.
- Security researcher MalwareTech found this weakness and registered and sinkholed this domain on 12-May-17 effectively acting as a "killswitch" for WannaCry and slowing the rate of infection.
- However, the above kill switch does not affect systems connecting through a proxy server, leaving those systems still vulnerable.
- If the connection fails, the dropper attempts to create a service named "mssecsvc2.0" with the DisplayName "Microsoft Security Center (2.0) Service".
  - This is logged in the System event log as event ID 7036, indicating that the service has started.

Exploit Details



Exploit Details

- The dropper then extracts the encrypter binary from its resource R/1831, writes it to the hardcoded filename %WinDir%\tasksche.exe, and then executes it.
- When executed, the encrypter checks to see if the mutex “MsWinZonesCacheCounterMutexA0” exists, and will not proceed if present.

Exploit Details

- The encrypter binary also contains a password-protected zip file (password: WNcry@2ol7) containing the following files:
  - A directory named “msg” containing Rich Text Format files with extension .wnry. These files are the “Readme” file used by the @WanaDecryptor@.exe decrypter program for each supported languages
  - b.wnry, a bitmap file displaying instructions for decryption
  - c.wnry, containing the following addresses:
    - gx7ekbenv2riucmf.onion
    - 57g7spgrzlojinas.onion
    - xxlvbrloxvriy2c5.onion
    - 76jdd2ir2embyv47.onion
    - cwwnhwhlz52maqm7.onion
    - https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
  - r.wnry, additional decryption instructions used by the decrypter tool, in English

Exploit Details

- The encrypter binary also contains a password-protected zip file (password: WNcry@2ol7) containing the following files:
  - s.wnry, a zip file containing the Tor software executable
  - t.wnry, encrypted using the WANACRY! encryption format, where “WANACRY!” is the file header
  - taskdl.exe, (hash 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79), file deletion tool
  - taskse.exe, (hash 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d), enumerates Remote Desktop Protocol (RDP) sessions and executes the malware on each session
  - u.wnry (hash b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25), “@WanaDecryptor@.exe” decrypter file

Exploit Details

- After dropping these files to its working directory, WannaCry attempts to change the attributes of all the files to “hidden” and grant full access to all files in the current directory and any directories below.
  - It does this by executing “attrib +h .”, followed by “icacls . /grant Everyone:F /T /C /Q” commands
- A registry key is written to “HKLM\SOFTWARE\Wow6432Node\WanaCrypt0r\wd” that adds a key to reference the location from where WannaCry was originally executed.

Exploit Details

- WannaCry Encrypter launches the embedded Decrypter binary "@WanaDecryptor@.exe,"
  - Displays two timers and instructions for sending the ransom in the configured language of the infected system
  - A payment of $300 / $600 equivalent in bitcoins to a specified address is demanded
- Following addresses are hardcoded in the binary, although only the first was observed to be used by the analyzed sample:
  - 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
  - 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
  - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WannaCry Activity List

innovate achieve lead

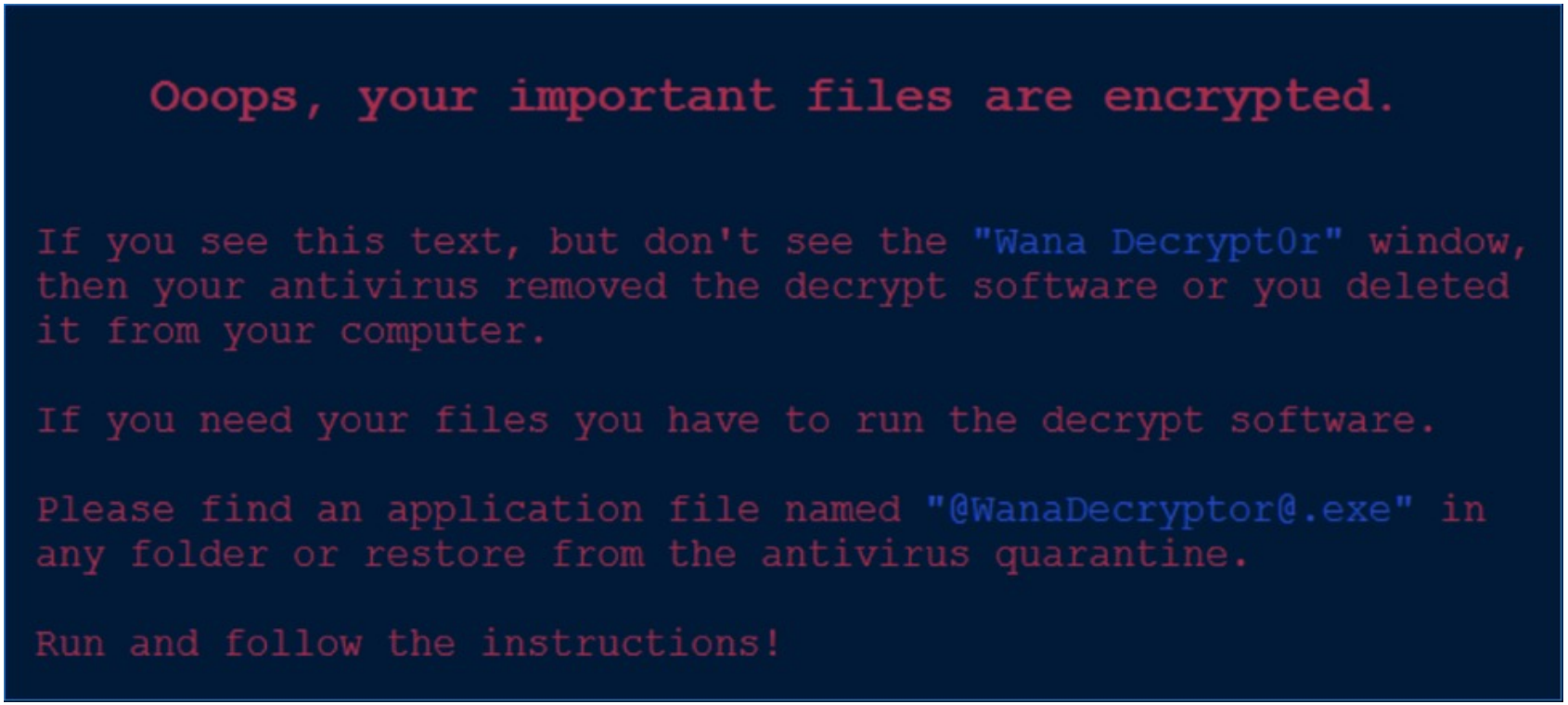
WannaCry file system activity

STEP	OPERATION	PURPOSE
1	SetSecurityFile	Modify discretionary access control list (DACL) of original document to Full for group Everyone, via the Windows application ICACLS.EXE.
2	CreateFile	Check if encrypted document with '.WNCRY' file extension exists.
3	CreateFile (Generic Read)	Open original document for read only.
4	QueryBasicInformationFile	Record timestamps on original document.
5	ReadFile	Read first 8 bytes of original document.
6	CreateFile (Generic Write)	Create encrypted file with '.WNCRYT' file extension, for write only.
7	WriteFile	Write 'WANACRY!' string (8 bytes) in encrypted file.
8	WriteFile	Write 4 bytes, at offset 8 bytes, in encrypted file.
9	WriteFile	Write 256 bytes, at offset 12 bytes, in encrypted file.
10	WriteFile	Write 4 bytes, at offset 268 bytes, in encrypted file.
11	WriteFile	Write 8 bytes, at offset 272 bytes, in encrypted file.
12	ReadFile	Read original document, entirely (0 bytes to EndOfFile).
13	WriteFile	Write encrypted file, entirely, at offset 280 bytes.
14	SetBasicInformationFile	Give encrypted file same timestamps as original document.
15	CloseFile	Close original document.
16	CloseFile	Close encrypted file.
17	SetRenameInformationFile	Change file extension of encrypted file from '.WNCRYT' to '.WNCRY'.
18	CreateFile (Generic Write)	Open original document for write only.
20	WriteFile	Write 1,024 bytes (1 KB) in original document. **At offset EndOfFile -1,024 bytes.**
21	FlushBuffersFile	Commit all buffered data to be written to disk.
21	WriteFile (Non-cached)	Write 4,096 bytes (4 KB) in original document, at offset AllocationSize on disk -4,096 bytes.
22	WriteFile	Write in chunks of 262,144 bytes (256 KB) in original document.
23	CloseFile	Close original document, now encrypted file.
24	OpenFile (Read Attributes)	Open encrypted file.
25	SetRenameInformationFile	Rename file to %temp%\<num>.WNCRYT. ReplaceIfExists: True.
26	CloseFile	Close encrypted file.
#	SetDispositionInformationFile	Once all documents on the disk are encrypted, a separate application TASKDL. EXE is run to delete %temp%*.WNCRYT (i.e. all '.WNCRYT' files).

Payment Notice

Payment Notice

The malware also displays the following bitmap image contained in “b.wnry” on the desktop, in case the “Wana Decrypt0r” program failed to execute:



Exploit Details

innovate achieve lead

- WannaCry uses the Microsoft Enhanced RSA and AES Cryptographic Provider libraries to perform the encryption.
- After the files are encrypted, the Decrypter program delete any Windows Shadow Copies via this command:
  - cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet

Metasploit Framework

Understanding Exploits

- An exploit is a security attack on a vulnerability
  - An exploit attacks a system vulnerability and generates an event that the application/program/OS is not designed to handle successfully
  - This results in a system that discontinues to function correctly
- Exploit can be designed to meet the methodology of attack
  - Ex: An attacker exploits an IDS to reboot it or crash it before he/she launches a further attack to avoid detection.
- However, Exploits have more potential
  - They are commonly used to install system malware or gain system access or recruit client machines into an existing 'botnet'.
  - This is accomplished with the help of a ***payload***
  - **Payload** is a sequence of code that is executed when the vulnerability is triggered
  - An Exploit can be broken up into two parts:
  - EXPLOIT = Vulnerability + Payload;

Understanding Payloads

- The payload is usually written in Assembly Language
- Platform and OS dependent
  - A Win32 payload will not work in Linux (even if exploiting the same bug)
    - Big Endian, Small Endian Architectures

- Different payload types exist and they accomplish different tasks
  - exec : Execute a command or program on remote system
  - download_exec : Download a file from a URL and execute
  - upload_exec : Upload a local file and execute
  - adduser : Add user to system accounts

Understanding Payloads

- The most common payload type used with exploits are **shellcodes or aka shell payloads**
  - These payloads are very useful because they provide the attacker an interactive shell that can be used to completely control the system remotely
  - The term is inherited from Unix → /bin/sh
  - For Win OS's, shells actually refer to command prompt → cmd.exe

- There are two different types of shell payloads
  - Bind Shells → A socket is created, a port is bound to it and when a connection is established to it, it will spawn a shell.
  - Reverse Shells → Instead of creating a listening socket, a connection is created to a predefined IP and Port and a shell is then shoveled to the Attacker.

Metasploit Framework

"The Metasploit Framework (MSF) is a platform for writing, testing, and using exploit code. The primary users of the Framework are professionals performing penetration testing, shellcode development, and vulnerability research."

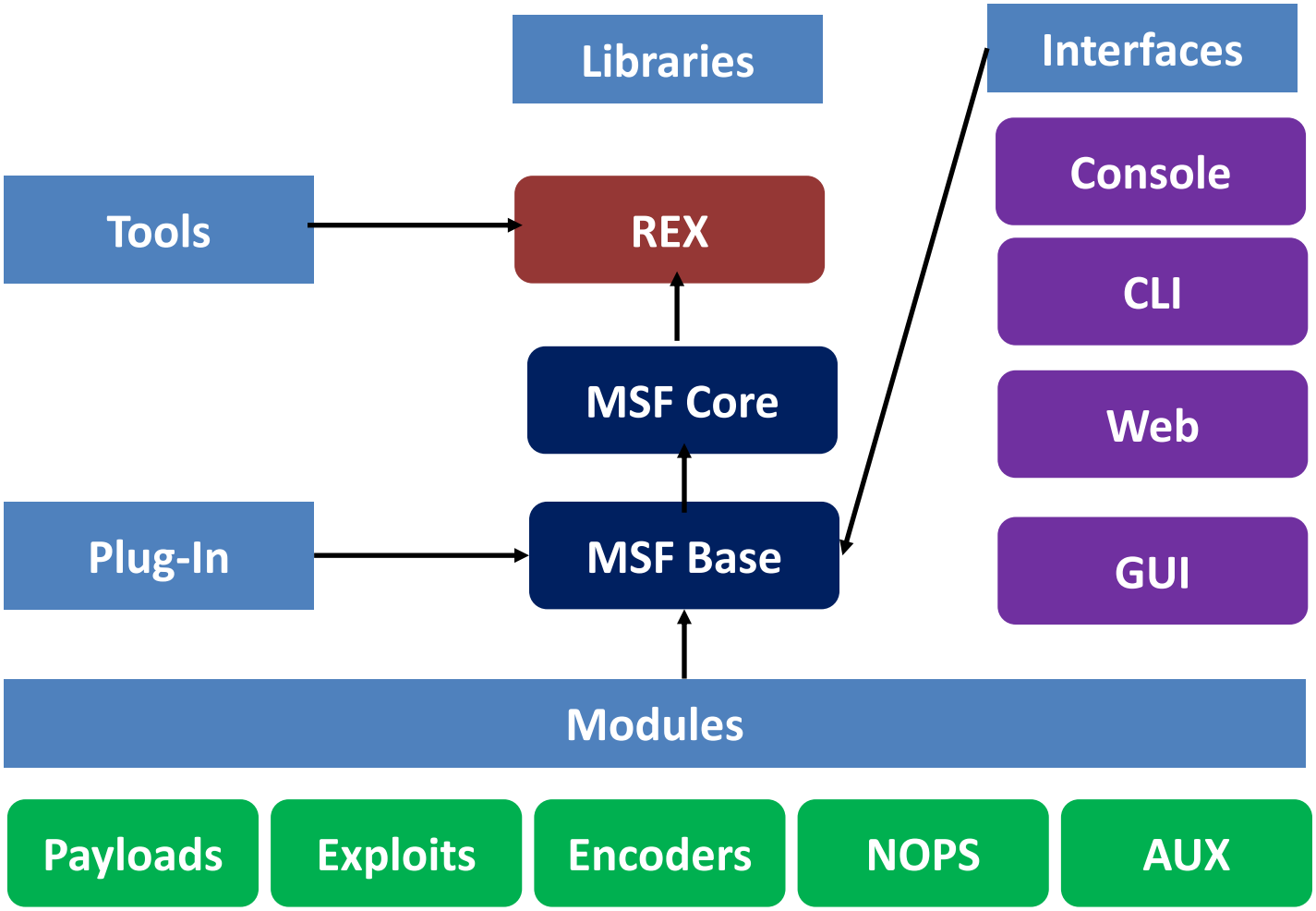
- MSF is not only an environment for exploit development but also a platform for launching exploits on real-world applications. It is packaged with real exploits that can provide real damage if not used professionally.

- MSF is an open-source tool and provides such a simplified method for launching dangerous attacks, it attracts wannabe hackers and script kiddies to a great extent.

Understanding Metasploit

- It is not just a single tool but collection of several
- Used mostly for Penetration Testing, Research, Creating and Testing new exploits
- It provides infrastructure to automate mundane and complex tasks.
- Created by HD Moore in 2003 in Perl
- Metasploit 2.0 in 2004 and Metasploit 3.0 in 2007
- Many developers worldwide
- URL: http://www.metasploit.com/ - Community version
- Acquired by security form Rapid7 in 2009
  - Metasploit Pro and Metasploit Express paid versions besides community version

Metasploit Architecture



Encoders

innovate achieve lead

- Encoders are used to evade the anti- virus Softwares and firewall
- However it has no effect on the functionality of out exploit
- Popular encoders are
  - shikata_ga_nai
  - base64
  - powershell_base64

NOPS

- NOP is short for No Operation
- NOPs keep the payload sizes consistent ensuring that validly executable by the processor
- Basically makes payload stable

AUXILIARY

- Provides additional functionality like scanning, fuzzing, Information gathering

Payloads

- Singles Usually standalone
- Fire and forget type
- Stagers Payload is divided into stages
- Stages Components of stager module.

- Bind TCP Shell
  - In case of bind tcp an exploit opens a vulnerable port in victim machine. And then it waits for connection from attacker
- Bind Reverse TCP Shell
  - In case of bind reverse tcp the target machine communicate back to attacker machine. Attacker machine has listening port open on which it receives connection

MSFVENOM

- It is a standalone payload generator and encoder
- Msfvenom replaced msfpayload and msfencoder in 2015
- It allows use to create playloads in c, exe, python, java formats
- Basically, allow us to create malicious files.
- MSFVENOM STEPS
  - Create a malicious file
  - Start the payload handler
  - Get victim to run the malicious file.

ARMITAGE

- Armitage is an attack manager tool that automates Metasploit in a graphical way
- Created by Raphael Mudge
- Written in java

PIVOTING

innovate achieve lead

- Pivoting is a technique that allows attackers to use a compromised system to attack other machines in the same network
- Basically hack another machine through already compromised machine

Basic Steps

- Identify which Exploit to use
- Configure the Exploit
- Pick a Payload
- Configure the Payload
- Execute the Exploit

Terminology

- Vulnerability: A method of interaction which allows for an unintended action to occur in response to an unexpected, invalid, or otherwise unaccounted for input of some form.
- Exploit: A piece of code that is designed to exploit a vulnerability to allow for an unintended action.
- Types: There are three key module types in Metasploit: exploit modules, post-exploit modules, and auxiliary modules.
  - Exploit modules take advantage of vulnerabilities to gain an initial foothold on the system.
  - Post-exploit modules collect information, escalate privileges, or otherwise expand upon the foothold achieved through an exploit module.
  - Auxiliary modules perform functions unrelated to exploitation.

Terminology

- Meterpreter: A Swiss army knife payload that allows for modular enhancement, routing, secondary exploitation, and control. A solid first-choice.
- Session: An open connection to a remote system through which commands, modules, or network traffic may be directed or routed.
- Pivoting: Using one system to bridge between two networks, typically to move into a more privileged or restricted area.

Demo

- SUNBURST SolarWinds 2020 Exploit
  https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- SMB Exploitation
  https://www.youtube.com/watch?v=eedTXtYiOK4
- Nmap SMB Enumeration
  https://www.youtube.com/watch?v=5kLPfVsOxzY
- Metasploit Framework
  https://www.youtube.com/watch?v=8lR27r8Y_ik

Thank You