UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

SERLAB
Software Engineering Research
UNIVERSITÀ DEGLI STUDI DI BARI

PROGETTO SICUREZZA INFORMATICA

Prof. Danilo Caivano – Dott.sa Vita Santa Barletta

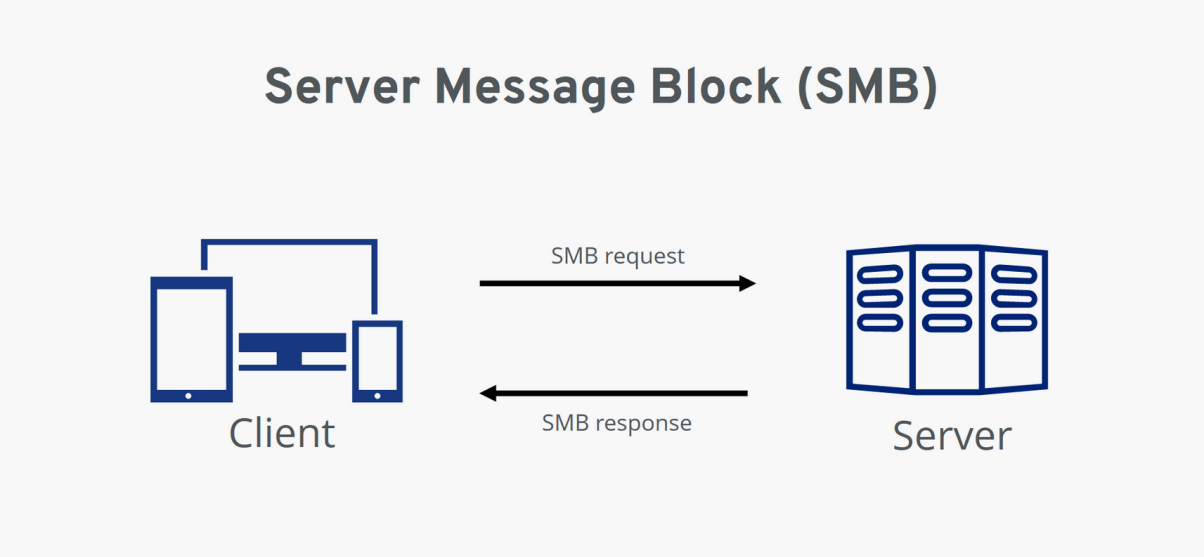
ENCRYPT

di Musciacchio Cosimo Marco, Matricola 739395
c.musciacchio2@studenti.uniba.it

Sommario

INTRODUZIONE

CONTESTO



L'attacco sfrutta un difetto del protocollo SMB 3.1.1(Server Message Block) presente in alcune versioni di Windows 10 e Windows Server:

- Windows 10 Version 1903 (32-bit, ARM64, x64)
- Windows 10 Version 1909 (32-bit, ARM64, x64)
- Windows Server, version 1903
- Windows Server, version 1909

Questa vulnerabilità consente a un pacchetto di dati, creato appositamente per sfruttare la vulnerabilità, di funzionare sul server SMB centrale ed eseguire codice casuale sul sistema.
Questa vulnerabilità è stata registrata come CVE 2020-0796 e ha ricevuto un punteggio di pericolosità di 10 su 10.
In questo attacco si andrà a sfruttare questa vulnerabilità per creare una reverse-shell sulla macchina della vittima. Si andrà poi a trasferire su di essa un file eseguibile malevolo e, tramite una ulteriore powershell reverse-shell, si andrà ad eseguirlo, andando a criptare tutti i file presenti sulla macchina.
L'attacco risulterà molto simile ad un attacco Ransomware, con la sola differenza che non ci sarà nessuna richiesta di denaro per avere i propri file decriptati.

SCENARIO

Un nostro amico stretto, ex dipendente di un'azienda, è stato vittima di un licenziamento illegittimo, nonostante abbia provato a "difendersi" tramite contestazione e difesa. Data la sua rabbia, si è rivolto a noi per chiederci aiuto ad effettuare una piccola "vendetta".
Essendo un ex dipendente, egli ci ha fornito varie informazioni riguardo l'azienda, e soprattutto riguardo le macchine utilizzate, ossia:

- Versione del Sistema Operativo utilizzato dalle macchine.
- Password per usufruire del wi-fi.
- Informazioni su Firewall

La vittima in questo caso è l'azienda stessa (con tutte le sue macchine), ma in questa simulazione verrà attaccata una sola di queste macchine. Essendo una piccola azienda, molto probabilmente considera la cybersecurity un *dipiù* non necessario ai fini dell'operatività del business e per questo risulta molto probabilmente un soggetto vulnerabile.
L'attaccante utilizzerà una macchina **Kali Linux** per accedere al sistema della vittima. Quest'ultima, invece, utilizzerà la versione di **Windows 10 19.03 V2.**
Poiché si tratta solo di una simulazione di attacco, sono state utilizzate sulla stessa rete due macchine virtuali aventi i sistemi operativi sopra citati.

Entrambe le macchine virtuali saranno collegate ad una rete con NAT, in modo da poter interagire tra di loro.

CYBER KILL CHAIN

RED TEAM	CYBER KILL CHAIN	BLUE TEAM
Individuazione della vittima da attaccare, controllo delle porte e scansione della vulnerabilità	**RECONNAISSANCE**	Bloccare tentativi di accesso malevoli o disabilitare/negare l'accesso a software non necessario per prevenire abusi.
Dopo aver individuato il target si ottengono le funzionalità per effettuare l'attacco	**WEAPONIZATION**	Monitorare il repository di codice in cui sono archiviati i payload per scoprire quelli più utilizzati e, quindi, creare firme per rilevarlo.
Si stabilisce una connessione con la macchina della vittima e si invia un payload per permettere l'exploit	**DELIVERY**	Adoperarsi a chiudere eventuali porte aperte e mitigare l'attività a livello di Network.
Il Payload viene eseguito e viene sfruttata la vulnerabilità per creare una reverse-shell	**EXPLOIT**	Effettuare costanti aggiornamenti del sistema operativo per ridurre il rischio di vulnerabilità o limitare l'esecuzione di codice a dei virtual environment..
L'attacco non prevede installazione.	**INSTALLATION**	L'attacco non prevede installazione.
Viene trasferito sulla macchina della vittima un file malevolo in grado di criptare tutti i file presenti e in seguito viene aperta una Powershell Reverse-Shell.	**COMMAND AND CONTROL**	Installare/aggiornare antivirus e/o ridurre al minimo la possibilità di esecuzione di codice e script tramite interpreter.
L'eseguibile malevolo viene eseguito e tutti i file sulla macchina della vittima vengono criptati.	**ACTION**	Data backup e behaviour prevention.

RECONNAISSANCE

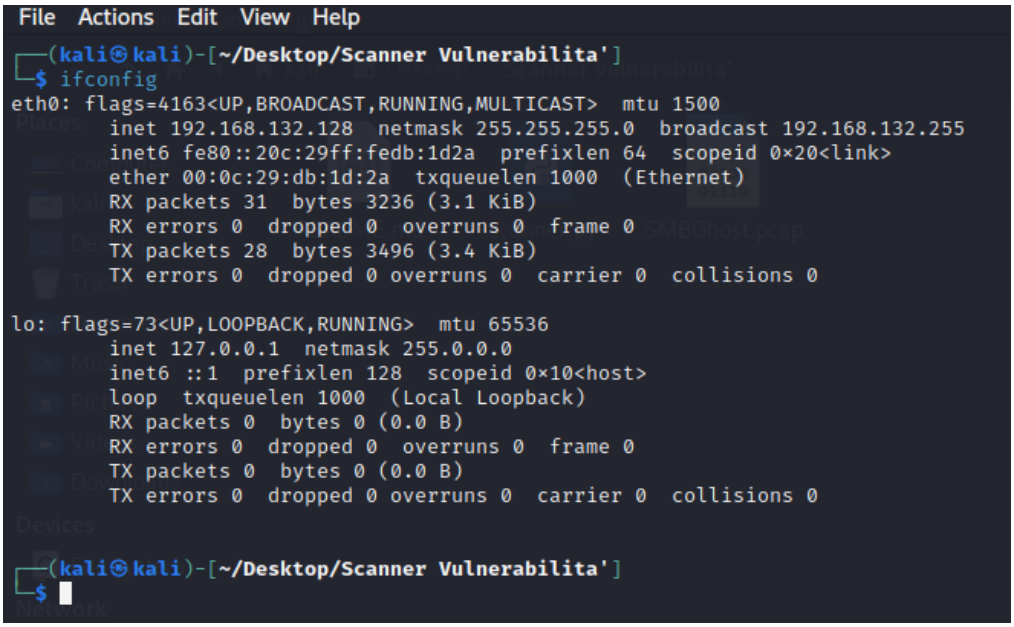
È la fase in cui l'intero attacco viene pianificato, determinante per il successo dell'attacco. L'attaccante cerca l'obiettivo e, una volta trovato, tenta di identificarne le vulnerabilità.

Red Team

Una volta connesso alla rete dell'azienda, essendo a conoscenza della password grazie all'ex dipendente, l'attaccante si serve della tecnica **Active Scanning**(MITRE ATT&CK®ID: T1595).

Segue la tecnica utilizzata per ottenere le informazioni necessarie per attaccare la vittima, ossia **Gather Victim Host Information** (MITRE ATT&CK® ID: T1592) che permette di raccogliere informazioni sulle reti della vittima. In questo caso verrà trovato l'Indirizzo IP della vittima.

In seguito, si andrà ad utilizzare la tecnica **Vulnerability Scanning** (MITRE ATT&CK® ID: T1595.002) per verificare se la vittima è vulnerabile all'exploit della CVE 2020-0796.
Questo verrà eseguito tramite uno script che controlla i dialetti del protocollo SMB 3.1.1 e le sue capacità di compressione tramite una Negotiate request.



Check del proprio IP sulla rete

```
┌──(kali㉿kali)-[~/Desktop/Scanner Vulnerabilita']
└─$ nmap -sP 192.168.132.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 08:18 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00040s latency).
Nmap scan report for 192.168.132.128
Host is up (0.00050s latency).
Nmap scan report for 192.168.132.130
Host is up (0.00052s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.37 seconds
```

Scan della rete tramite Nmap

```
┌──(kali㉿kali)-[~/Desktop/Scanner Vulnerabilita']
└─$ sudo nmap -f 192.168.132.130
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 08:19 EDT
Nmap scan report for 192.168.132.130
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:C2:E9:F6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

Scan delle porte "più frequentemente utilizzate" della vittima

```
┌──(kali㉿kali)-[~/Desktop/Scanner Vulnerabilita']
└─$ python scanner.py 192.168.132.130
192.168.132.130 Vulnerable
```

Vulnerability Scan

Blue Team

Delle efficaci mitigazioni possono essere le seguenti:

- Effettuare dei cambiamenti alle password (in questo caso al wi-fi) frequenti e facendo in modo che siano sicure**,** **Password Policies**(MITRE ATT&CK® ID:M1027)
- Rimuovere o negare l'accesso al protocollo SMB 3.1.1, per prevenire eventuali abusi**,** **Disable or Remove Feature or Program**(MITRE ATT&CK® ID:M1042)
- La tecnica **Update Software** (MITRE ATT&CK® ID: M1051), in quanto un aggiornamento del sistema operativo potrebbe portare alla rimozione di possibili vulnerabilità.

- **Network Intrusion Prevention**(MITRE ATT&CK® ID:M1031) per difendersi da port scanning.

WEAPONIZATION

Red Team

L'attaccante si procura le funzionalità per eseguire l'attacco con la tecnica Obtain capabilities (MITRE ATT&CK® ID: T1588).
In particolare, per questo attacco gli strumenti sono:

- **Nmap,** per effettuare la scansione della rete
- **Metasploit,** in quanto verrà utilizzato msfvenom per il payload per la reverse shell
- **InfinityCrypt.exe**, eseguibile malevolo in grado di criptare qualsiasi file all'interno di una macchina
- **Netcat**, da usare come listener per la reverse-shell
- **Invoke-PowerShellTcp.ps1**, ossia uno script per far partire una seconda reverse-shell da powershell
- **Smbghost.py**, ossia uno script in python per sfruttare la vulnerabilità di SMB3.1.1

Blue Team

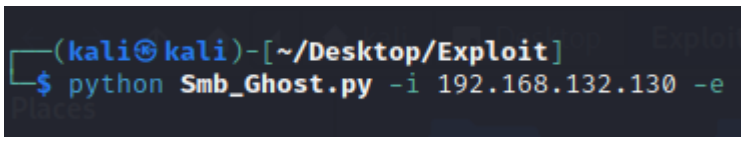
Questa tecnica non può essere facilmente mitigata con controlli preventivi poiché si basa su comportamenti eseguiti al di fuori dell'ambito delle difese e dei controlli interni. L'unica raccomandazione è quella di monitorare il repository di codice in cui sono archiviati i payload per scoprire quelli più utilizzati e, quindi, creare firme per rilevarlo.

DELIVERY

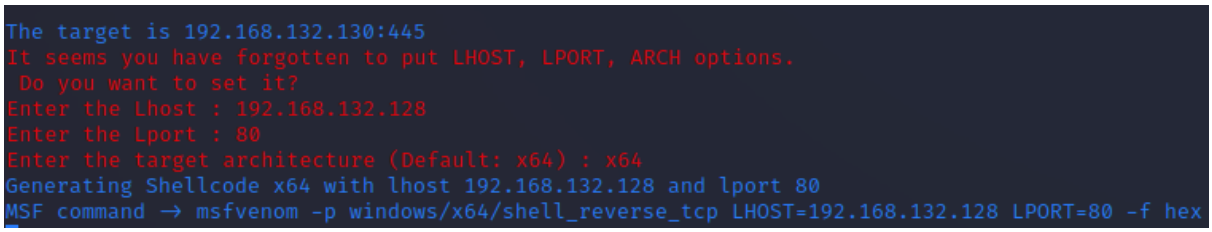
Red Team

In questo attacco il payload,creato con msfvenom, riguarda l'apertura di una reverse shell sulla macchina della vittima.
Tramite lo script **Smb_Ghost.py il** payload viene inviato e si prova a sfruttare la vulnerabilità del protocollo SBM 3.1.1 per aprire una reverse-shell. Le informazioni necessarie sono le seguenti:

- L'indirizzo IP della vittima, ossia 192.168.132.130.
- L'indirizzo IP dell'attaccante, ossia 192.168.132.128.
- La porta sulla macchina della vittima, che in questo caso è 445. Essa deve essere aperta, e come è stato visto nella fase di Reconnaissance, essa lo è.
- La porta su cui settare il listener di netcat(nel nostro caso 80).
- L'architettura del sistema operativo della vittima



Viene lanciato lo script Smb_Ghost.py con l'IP della vittima



Vengono inseriti l'indirizzo IP dell'attaccante, la porta del listener e l'architettura del sistema operativo della vittima, e viene creato il payload per la reverse-shell

Blue Team

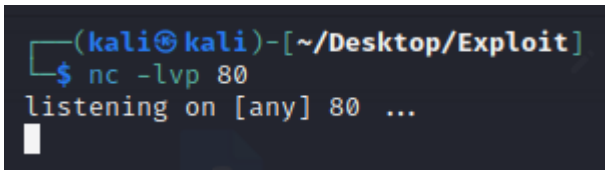
In quanto la comunicazione tra l'attaccante e la vittima avviene sulla porta 445, una buona mitigazione consiste nel chiudere quella porta, secondo la tecnica **Filter Network Traffic** (MITRE ATT&CK® ID:M1037), oppure potrebbe utilizzare

la tecnica **Network Intrusion Prevention**(MITRE ATT&CK® ID:M1031), in modo da mitigare l'attività a livello di network.

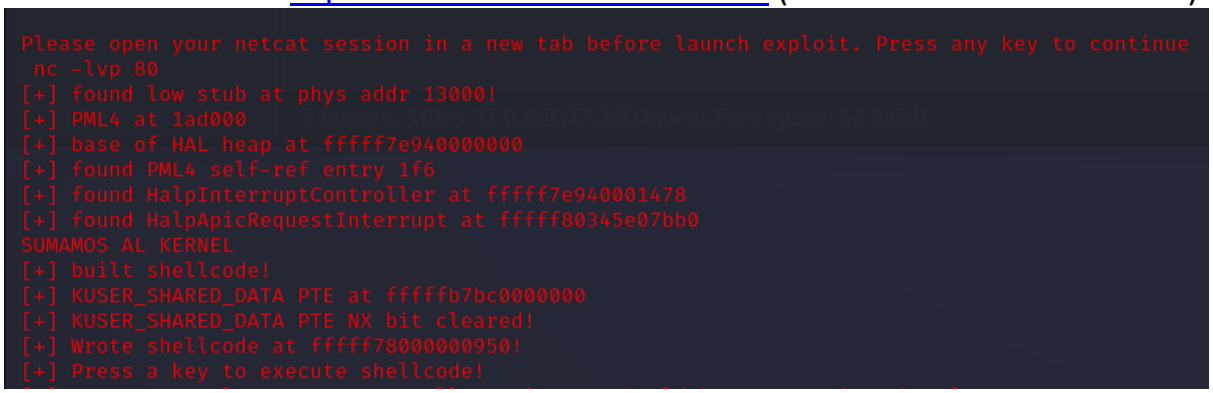
EXPLOIT

Red Team

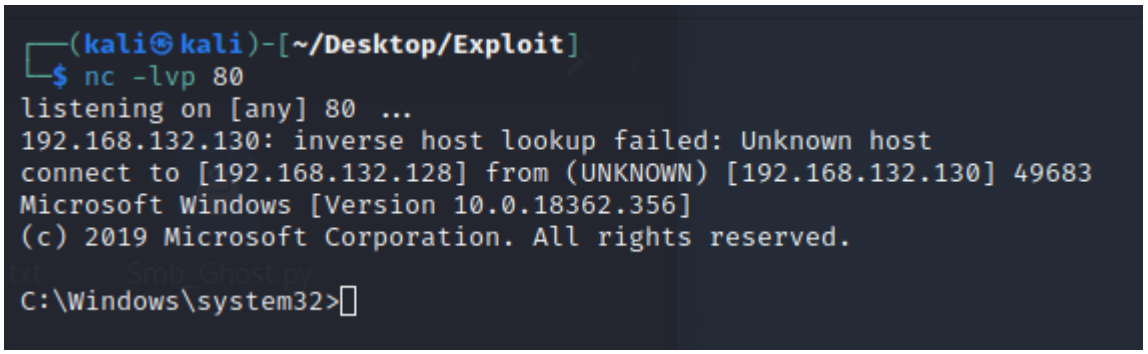
Dopo aver settato il listener con netcat sulla porta 80



Si procede a far partire il payload per sfruttare la vulnerabilità di SMB 3.1.1, secondo la tecnica Exploitation of Remote Services (MITRE ATT&CK® ID: T1210).



Lo shellcode presente nel payload viene lanciato



Reverse shell

Blue Team

Anche in questo caso una buona mitigazione consiste nella tecnica **Disable or Remove Feature or Program** (MITRE ATT&CK® ID: M1402) per disabilitare il Protocollo SBM 3.1.1
Altre mitigazioni efficaci possono essere:

- la tecnica **Update Software** (MITRE ATT&CK® ID: M1051), in quanto un aggiornamento del sistema operativo potrebbe portare alla rimozione della vulnerabilità.
- **Application Isolation and Sandboxing** (MITRE ATT&CK® ID: M1408), in modo da limitare l'esecuzione di codice a dei virtual environment.
- **Vulnerability Scanning** (MITRE ATT&CK® ID: M1051), ossia effettuare una scansione delle vulnerabilità per identificare quelle presenti prima che vengano sfruttate.

INSTALLATION

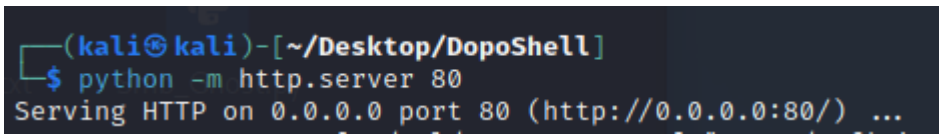
L'attacco non prevede alcuna installazione.

COMMAND AND CONTROL

Red team

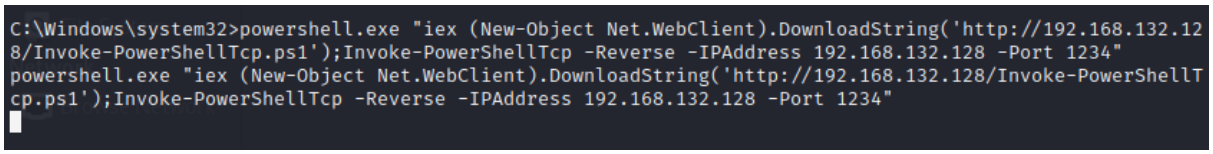
In questa fase dell'attacco, grazie alla reverse-shell, sarà possibile eseguire comandi sulla macchina della vittima con la tecnica **Command and Scripting Interpreter** (MITRE ATT&CK® ID: T1059), in particolare **Windows Command shell** (ATT&CK® ID: T1059.003). Il prossimo passo è creare un webserver sulla macchina dell'attaccante tramite la funzionalità di python in modo da poter trasferire dei file sul pc della vittima, secondo la **tecnica** **Ingress Tool Transfer**(MITRE ATT&CK® ID: T1105),

Il primo file che verrà trasferito è **InfinityCrypt.exe**, ossia l'eseguibile malevolo che verrà eseguito prossimamente. Il secondo è **Invoke-PowerShellTcp.ps1**, che permetterà di aprire una nuova reverse-shell con powershell. Quest'ultimo verrà subito eseguito e sull macchina dell'attaccante verrà aperto un listener sulla porta 1234.

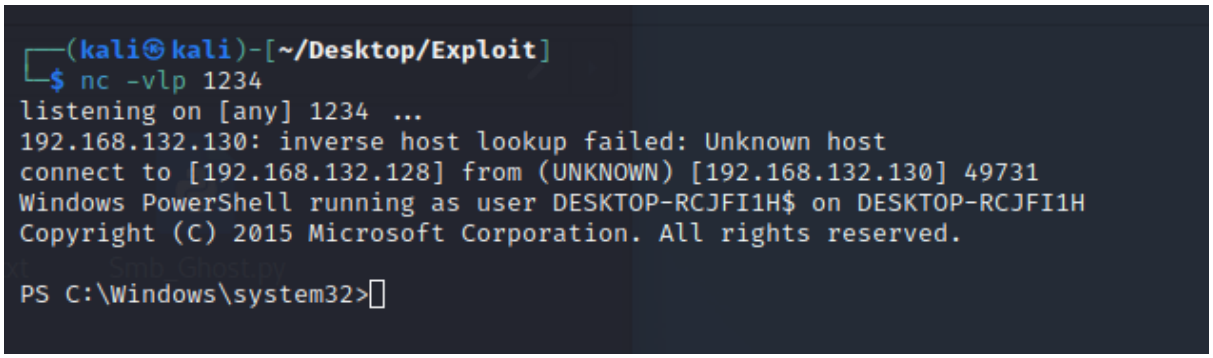


Creazione del webserver

Trasferimento del file InfinityCrypt.exe



Trasferimento ed esecuzione del file Invoke-PowerShellTcp.ps1



PowerShell Reverse-Shell

Blue Team

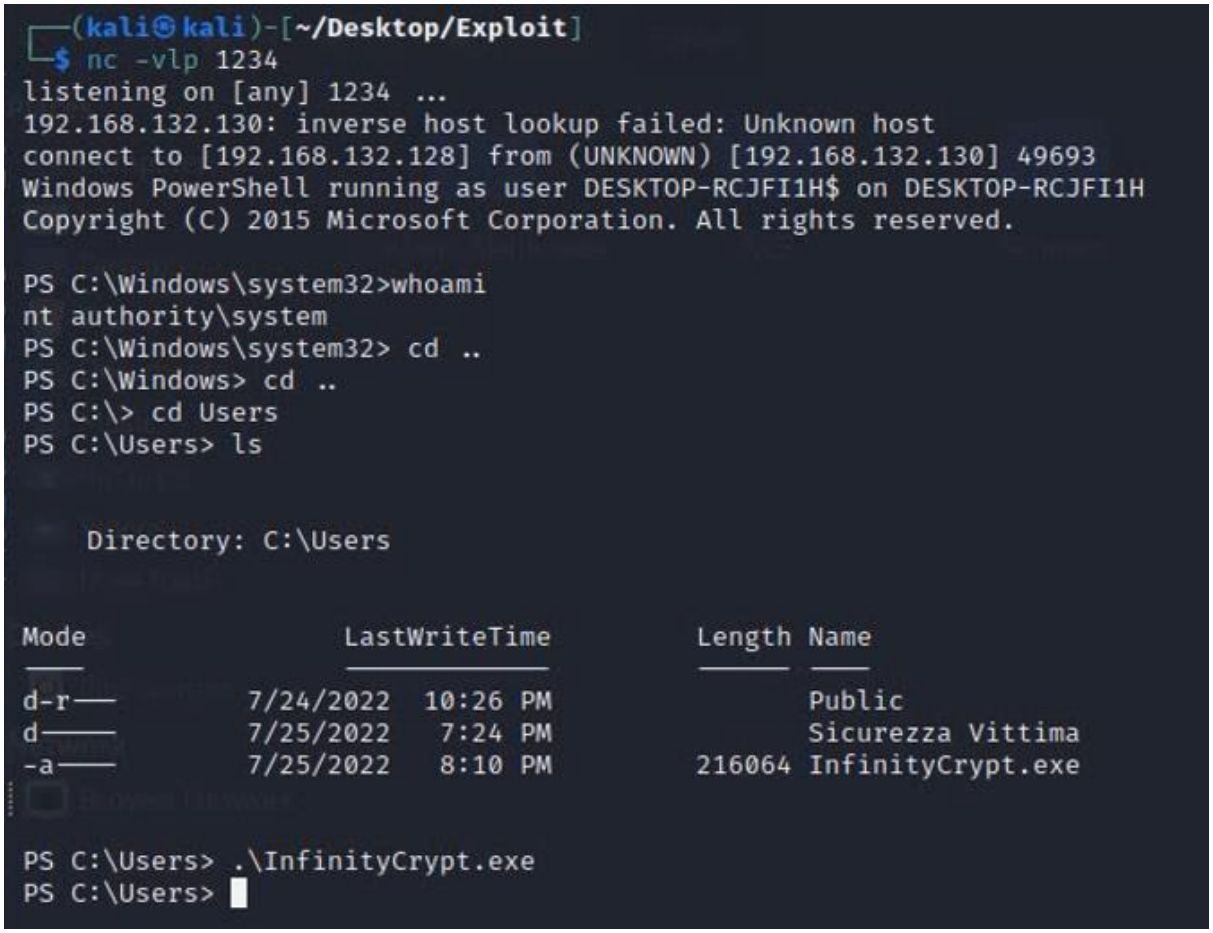
Le mitigazioni in questa fase sono le seguenti:

- Antivirus/Antimalware (MITRE ATT&CK® ID: M1049), per poter rilevare e rimuovere eventuali file malevoli
- Disable or Remove Feature or Program (MITRE ATT&CK® ID:M1042), in questo caso per disabilitare o rimuovere gli interpreter
- Code Signing (MITRE ATT&CK® ID:M1045), per limitare l'uso di script ed avere la possibilità di usarne solo alcuni segnati.
- Execution Prevention (MITRE ATT&CK® ID: M1038), per bloccare completamente l'esecuzione di codice tramite interpreter o tramite script.

ACTION

Red Team

In questa ultima fase l'attaccante ha la possibilità di muoversi liberamente tra le directory della macchina della vittima, con la tecnica **File and Directory Discovery** (MITRE ATT&CK® ID: T1083), fino ad arrivare alla directory in cui è stato scaricato il file InfinityCrypt.exe ed eseguirlo con powershell, tecnica **User Execution**(MITRE ATT&CK® ID: T1204). In quell'esatto momento, tutti i file sulla macchina della vittima saranno criptati, **Data Encrypted for Impact** (MITRE ATT&CK® ID: T1486).



Blue Team

Le possibili mitigazioni per questa fase sono le seguenti:

- **Behavior Prevention on Endpoint** (MITRE ATT&CK® ID: M1040), in modo da bloccare l'esecuzione di file simili a Ransomware.
- **Data Backup** (MITRE ATT&CK® ID: M1053).

CONCLUSIONI

Attraverso la simulazione di questo attacco, si è messo in evidenza quanto sia importante (e non solo per le piccole aziende) non sottovalutare la sicurezza informatica. Spenderci denaro, tempo e impegno non si rivelerà mai una scelta sbagliata.
Vorrei concludere con una citazione:

History has taught us: never underestimate the amount of money, time and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did".

Bruce Schneier