S11L5

-Quali sono gli output del comando `dir`?

Elenca i file e le directory presenti nella cartella corrente.

-Quali sono i risultati?

`ping`: verifica la connettività con un altro host inviando pacchetti ICMP.

`cd`: cambia la directory di lavoro corrente.

`ipconfig`: mostra la configurazione IP corrente.

-Qual è il comando PowerShell per `dir`?

Get-ChildItem.

-Qual è il gateway IPv4?

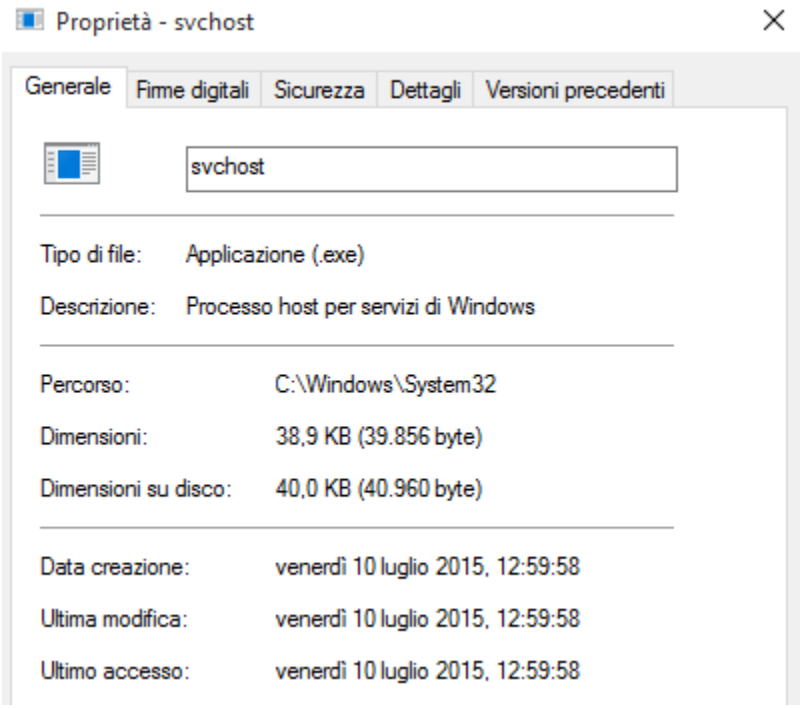
192.168.50.1

```
C:\Users\user>netstat -r
===========================================================================
Elenco interfacce
  4...08 00 27 68 01 a1 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  5...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0     192.168.50.1     192.168.50.4     10
```

-Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Puoi vedere il nome esatto dell'eseguibile, il percorso su disco, l'utilizzo di memoria/CPU, l'utente che ha lanciato il processo e la descrizione del servizio.



-Cosa è successo ai file nel Cestino?

Sono stati eliminati definitivamente dal sistema.

Report

File analizzato: `Jvczfhe.exe`

Fonte: Scaricato da repository GitHub.

Verdetto Sandbox: **MALICIOUS ACTIVITY**

Data analisi: 25 Agosto 2024

Tags rilevati: `github`, `netreactor`.

Catena di infezione:

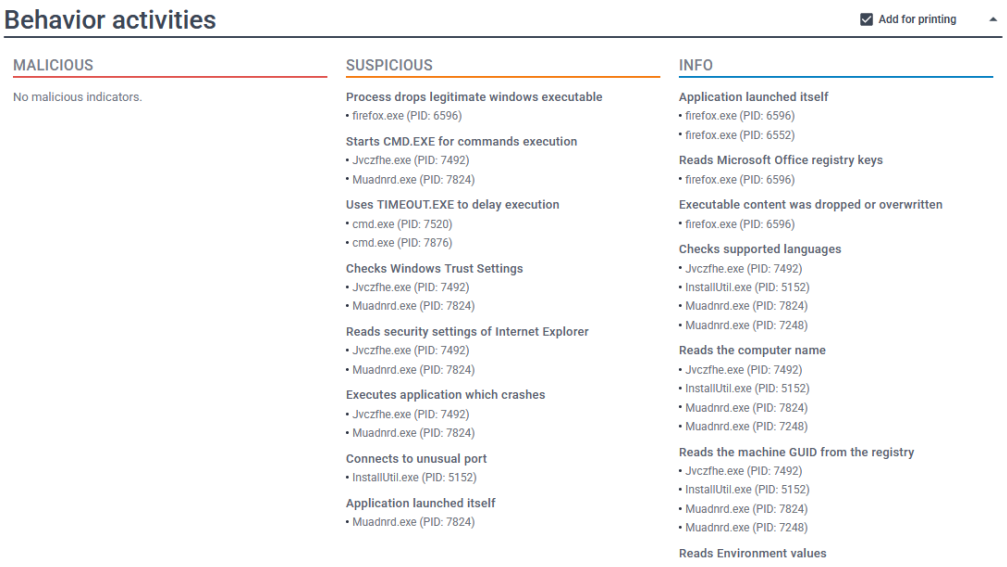
L'attacco segue una catena di esecuzione a più stadi:

- L'utente scarica ed esegue il file malevolo **Jvczfhe.exe** tramite il browser **Firefox**.
- Il processo malevolo avvia diverse istanze di **CMD.EXE** per eseguire comandi di sistema.
- Viene lanciato un secondo eseguibile, **`Muadnrd.exe`**, che sembra essere una copia o un secondo stadio del malware, il quale tenta di rendersi persistente o eseguire il payload finale.
- Viene utilizzato il processo legittimo **InstallUtil.exe** per mascherare l'attività di rete.

Analisi dei comportamenti sospetti (Threat Indicators):

Dall'analisi comportamentale emergono le seguenti tecniche tipiche dei malware (Trojan/Stealer):

- **Evasione della Sandbox:** il malware utilizza il comando `TIMEOUT.EXE` per ritardare l'esecuzione, questa è una tecnica classica per ingannare gli antivirus e le sandbox, che spesso analizzano i file solo per pochi secondi, se il malware "dorme" all'inizio, l'analisi termina prima che il virus si attivi.
- **Ricognizione:** il malware raccoglie informazioni sulla vittima prima di attaccare, leggendo:
    - Il nome del computer e il **GUID** della macchina dal registro.
    - Le impostazioni di sicurezza di Internet Explorer e i certificati di attendibilità, questo serve al virus per capire se si trova su un PC reale (da attaccare) o su una macchina di ricerca (da evitare).
- **Comunicazione C2 (Command & Control):** il processo `InstallUtil.exe`, normalmente innocuo, viene sfruttato per connettersi a **porte insolite**, questo indica che il malware sta cercando di comunicare con il server dell'attaccante per esfiltrare dati o ricevere nuovi comandi, nascondendosi dietro un processo di sistema fidato.



Conclusioni:

Il campione analizzato è un **Trojan/Loader** offuscato con .NET Reactor, la sua natura è quella di infiltrarsi nel sistema, raccogliere dati identificativi della vittima ed eludere i controlli di sicurezza ritardando la propria esecuzione e nascondendo il traffico di rete all'interno di processi legittimi come `InstallUtil.exe`.

Bonus 1

-Cos'è Nmap?

Network Mapper è uno strumento open source per l'esplorazione della rete e l'audit di sicurezza.

-Per cosa viene usato nmap?

Per determinare quali host sono disponibili, quali servizi offrono, i sistemi operativi in esecuzione e i firewall in uso .

-Qual è il comando nmap usato?

nmap -A -T4 scanme.nmap.org

-Cosa fa l'opzione `-A`?

Abilita il rilevamento del sistema operativo (OS detection), il rilevamento della versione dei servizi, lo script scanning e il traceroute.

-Cosa fa l'opzione `-T4`?

Imposta il template di temporizzazione per un'esecuzione più veloce.

-Quali porte e servizi sono aperti?

Porta 21: servizio **FTP**

Porta 22: servizio **SSH**

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-05 10:11 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000064s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```

-A quale rete appartiene la tua VM?

192.168.50.0/24

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 4a:86:7d:80:5d:76 brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f6:bc:b1:cb:94:4e brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2f:87:a7 brd ff:ff:ff:ff:ff:ff
    altname enx0800272f87a7
    inet 192.168.50.9/24 metric 1024 brd 192.168.50.255 scope global dynamic enp0s3
       valid_lft 578sec preferred_lft 578sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

-Quanti host sono attivi?

Sono attivi due host:

192.168.50.9 (Cyberops Workstation)

192.168.50.10 (Kali Linux)

```
[analyst@secOps ~]$ nmap -A -T4 192.168.50.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-05 09:03 -0500
Nmap scan report for 192.168.50.2
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.50.2 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.9
Host is up (0.00085s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Nmap scan report for 192.168.50.10
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.2p1 Debian 2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (3 hosts up) scanned in 60.67 seconds
```

-Quali porte e servizi sono aperti?

Porta 22: servizio **SSH** (versione: OpenSSH 6.6.1p1 Ubuntu)

Porta 80: servizio **HTTP** (versione: Apache httpd 2.4.7)

Porta 9929: servizio **nping-echo**

Porta 31337: servizio **tcpwrapped**

-Quali porte e servizi sono filtrati?

Nmap indica che ci sono **996 porte TCP filtrate** ("*Not shown: 996 filtered tcp ports*").

-Qual è l'indirizzo IP del server?

45.33.32.156 (*"Nmap scan report for scanme.nmap.org"*).

-Qual è il sistema operativo?

Linux (*"Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel").*

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-05 09:09 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.00 seconds
```

Domanda di riflessione

Nmap è uno strumento potente per l'esplorazione e la gestione della rete.

-Come può Nmap aiutare con la sicurezza della rete?

Può aiutare con la sicurezza della rete trovando porte aperte dimenticate o servizi non aggiornati per chiuderli.

-Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Può essere utilizzato da attori malevoli per mappare la rete vittima e trovare punti di ingresso vulnerabili.

Bonus 2

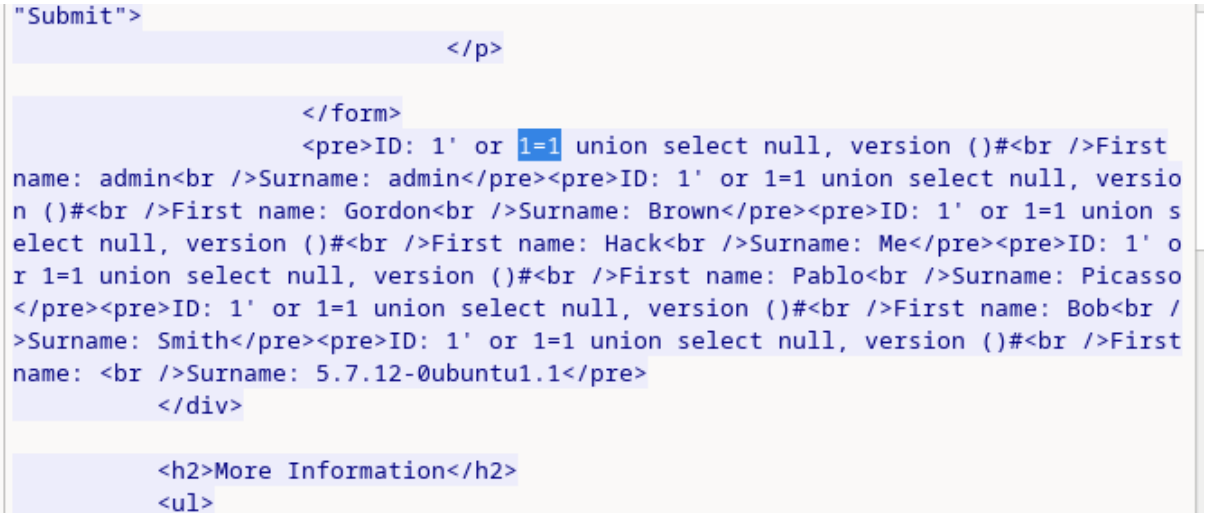
-Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?

Sorgente: **`10.0.2.4`**

Destinazione: **`10.0.2.15`**

-Qual è la versione?

`5.7.12-0ubuntu1.1`



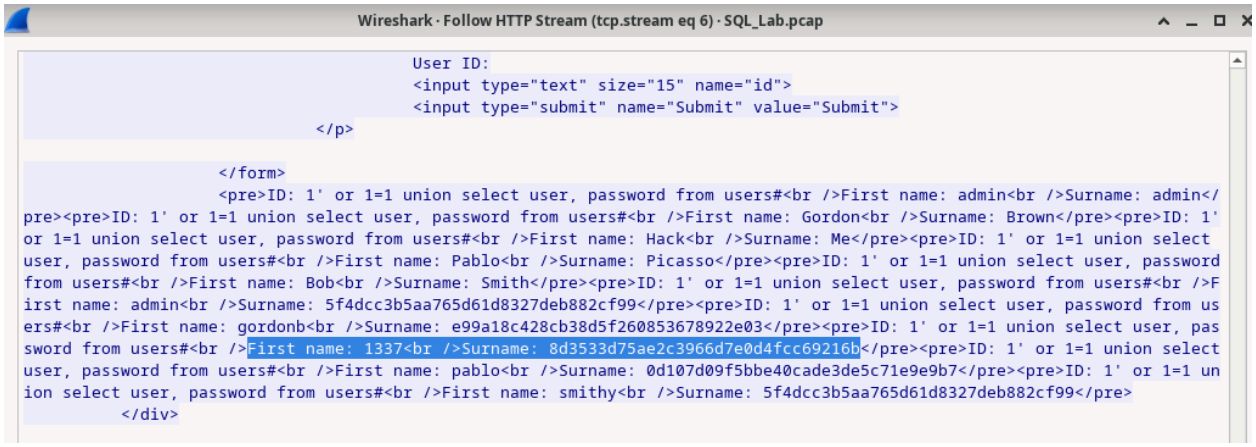
```
"Submit">
                                </p>

                    </form>
                    <pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null, versio
n ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union s
elect null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' o
r 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso
</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br />
>Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
          </div>

          <h2>More Information</h2>
          <ul>
```

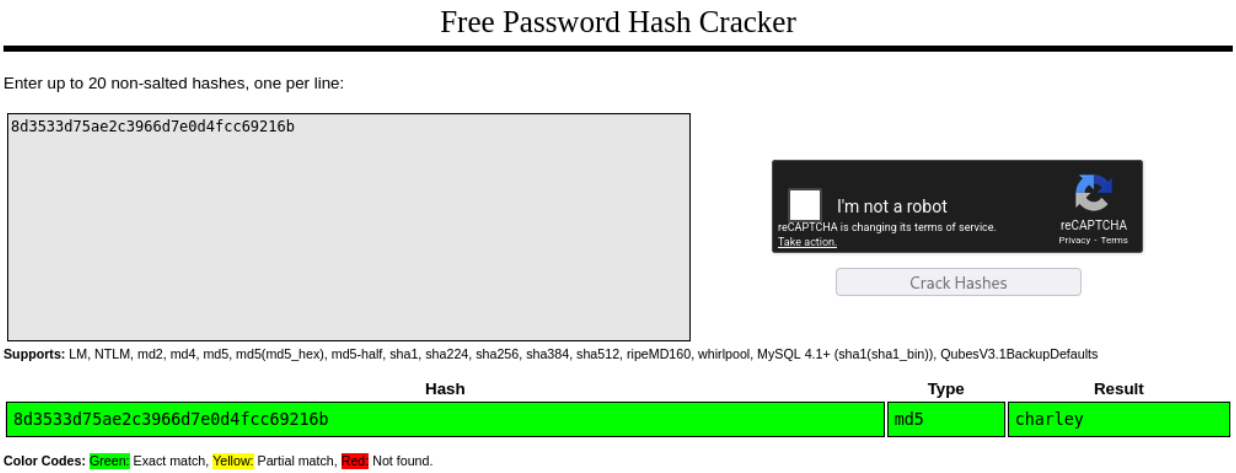
-Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

L'utente **1337**.



-Qual è la password in chiaro?

La password in chiaro è **charley**.



Domanda di riflessione

-Qual è il rischio che le piattaforme utilizzino SQL?

Se l'input utente non è sanitizzato, gli attaccanti possono manipolare le query del database (SQL Injection) per leggere, modificare o cancellare dati sensibili.

-Naviga in internet ed esegui una ricerca per "prevenire attacchi di SQL injection". Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

Sanitizzazione dell'input utente.

Uso di query parametrizzate.

Implementazione di web application firewall.