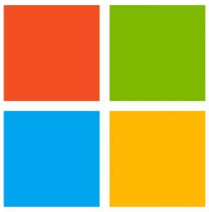
Cyber Security January Minor Project

Start Date: *Feb* 24th, 2022
End Date: *Feb* 28th, 2022

Table of Contents

Problem Statement

- Perform Footprinting on Microsoft Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots
- Test the System Security by using PRORAT / Darkcomet (Anyone Tool) Trojan by hacking virtual machines and try to take screenshots & Keystrokes along with change data in Desktop. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks
    - Hacker Machine : Windows 7 / Windows 10
    - Victim machine : Windows XP / Windows 7
- Use BVM Tool (Download from Internet) to create a virus and inject in to Virtual system and perform destruction program as per your wish and write a document along with screenshots and suggest the preventive measures to avoid this malware affect
    - Hacker Machine : Windows 7 / Windows 10
    - Victim machine : Windows XP / Windows 7
- Write a small batch program and save as .bat extension and execute in victim machine (Windows 7 /Windows 10 / Windows XP)
- Perform SQL injection on by using Havij Tool(Download it from Internet) on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections
- Use Wireshark Tool(Download it from Internet) to sniff the data and try to get the username and password of http://demo.testfire.net/
- Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing
- Try to Encrypt the Data in image file using quick stego tool (Download from Internet) and command prompt also and show them how to decrypt also. Write a report advantages of cryptography and steganography)



Microsoft

To empower every person and every organization on the planet to achieve more.

Footprinting

Passive Recon

Whois

Domain Information

Domain:	microsoft.com
Registrar:	MarkMonitor Inc.
Registered On:	1991-05-02
Expires On:	2022-05-02
Updated On:	2021-03-12
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1-205.azure-dns.com ns2-205.azure-dns.net ns3-205.azure-dns.org ns4-205.azure-dns.info

Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft

Administrative Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft

Technical Contact

Name:	MSN Hostmaster
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	msnhst@microsoft.com

Netcraft

Background

Site title	Microsoft – Cloud, Computers, Apps & Gaming	**Date first seen**	May 2004
Site rank	64	**Netcraft Risk Rating**	0/10
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	**Primary language**	English

Network

Site	https://www.microsoft.com	**Domain**	microsoft.com
Netblock Owner	Akamai Technologies, Inc.	**Nameserver**	ns1-205.azure-dns.com
Hosting company	Akamai Technologies	**Domain registrar**	markmonitor.com
Hosting country	US	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	104.95.181.163 (VirusTotal)	**Organisation**	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	**DNS admin**	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:9d00:193:0:0:0:356e	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS20940	**DNS Security Extensions**	unknown
Reverse DNS	a104-95-181-163.deploy.static.akamaitechnologies.com	**Latest Performance**	Performance Graph

IP delegation

IPv4 address (104.95.181.163)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.64.0.0-104.127.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 104.95.181.163	United States	AKAMAI	Akamai Technologies, Inc.

IPv6 address (2a02:26f0:9d00:193:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:9d00::/48	European Union	AKAMAI-PA	Akamai Technologies
↳ 2a02:26f0:9d00:193:0:0:0:356e	European Union	AKAMAI-PA	Akamai Technologies

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	www.microsoft.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Microsoft Corporation	**Application-Layer Protocol Negotiation**	h2
State	WA	**Next Protocol Negotiation**	Not Present
Country	US	**Issuing organisation**	Microsoft Corporation
Organisational unit	Microsoft Corporation	**Issuer common name**	Microsoft RSA TLS CA 01
Subject Alternative Name	privacy.microsoft.com, c.s-microsoft.com, microsoft.com, i.s-microsoft.com, staticview.microsoft.com, www.microsoft.com, wwwqa.microsoft.com	**Issuer unit**	Not Present
Validity period	From Jul 28 2021 to Jul 28 2022 (12 months)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US
Server	Not Present	**Issuer state**	Not Present

Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl
Protocol version	TLSv1.3	**Certificate Hash**	QyRrZTDEQusorQSXnornOyOPD0k
Public key length	2048	**Public Key Hash**	e7c6e239c1ada97166d0fdce166b3ac45239a3f69bce5480c384c97d15c38298
Certificate check	ok	**OCSP servers**	http://ocsp.msocsp.com - *100% uptime in the past 24 hours* **Performance Graph**
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	Certificate valid
Serial number	0x120014f1ec2395d56fdcc4dcb700000014f1ec	**OCSP data generated**	Feb 22 07:00:13 2022 GMT
Cipher	TLS_AES_256_GCM_SHA384	**OCSP data expires**	Feb 26 07:00:13 2022 GMT
Version number	0x02		

Certificate Transparency
Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2021-07-28 21:32:10	Success
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=	2021-07-28 21:32:10	Success
Certificate	Google Xenon 2022 RqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUc=	2021-07-28 21:32:10	Success

SSLv3/POODLE
This site does not support the SSL version 3 protocol.

SSL Certificate Chain

Common name	Baltimore CyberTrust Root
Organisational unit	CyberTrust
Organisation	Baltimore
Validity period	From 2000-05-12 to 2025-05-12
↓	
Common name	Microsoft RSA TLS CA 01
Organisational unit	Not Present
Organisation	Microsoft Corporation
Validity period	From 2020-07-21 to 2024-10-08

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	19-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	5-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	28-Jan-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	21-Jan-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	23.47.197.197	Linux	unknown	7-Jan-2022
Akamai Technologies	92.122.165.100	Linux	unknown	31-Dec-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	24-Dec-2021
Akamai Technologies	92.122.165.100	Linux	unknown	16-Dec-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	9-Dec-2021
Akamai Technologies	92.122.165.100	Linux	unknown	4-Nov-2021

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on microsoft.com: Check the **site report**.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any **mail-enabled subdomains**. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org**.

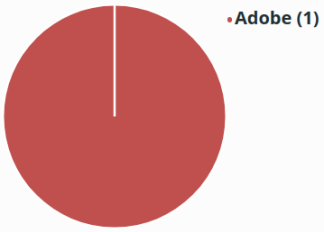
This host does not have a DMARC record. There may be a DMARC record on the site report for microsoft.com: Check the **site report**.

Web Trackers

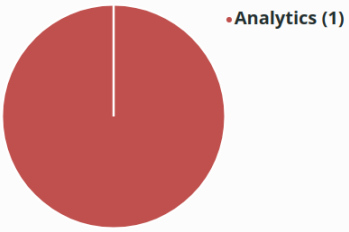
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known tracker was identified.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Adobe	Analytics	Omniture	www.verizon.com, www.vmware.com, www.dell.com

Site Technology (fetched 11 days ago)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	
Using ASP.NET	ASP.NET is running on the server	www.cnblogs.com, www.wordreference.com, fxpro.sharepoint.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Web Worker	*No description*	www.verajohn.com, www.epicgames.com, www.ig.com
Asynchronous Javascript	*No description*	www.ebay.co.uk, www.hulu.com, www.primevideo.com
Local Storage	*No description*	www.roblox.com, smile.amazon.com, portal.azure.com
Session Storage	*No description*	www.cisco.com, www.interia.pl, techcommunity.microsoft.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.xvideos.com, www.amazon.es, www.amazon.fr
AJAX	*No description*	www.amazon.in, yandex.ru, e.mail.ru

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Akamai	Web Content Delivery service provider	www.ibm.com, www.ikea.com, www.washingtonpost.com

E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

Technology	Description	Popular sites using this technology
General Domain Holding	Loading temporary content under a domain name	www.dell.com, www.taosamuebles.com, www.amazon.ca

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.sozcu.com.tr, www.seznam.cz, www.hp.com

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.linkedin.com, accounts.google.com, outlook.office.com
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	docs.microsoft.com, outlook.live.com, teams.microsoft.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	web.whatsapp.com, en.wikipedia.org, l.facebook.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.google.com, mail.google.com, mail-redir.mention.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	www.startpage.com, www.bbc.co.uk, discord.com

Privacy Management

Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.

Technology	Description	Popular sites using this technology
P3P	Platform for Privacy Preferences Project allows websites to express their privacy practices	login.microsoftonline.com, support.microsoft.com, photos.google.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	vk.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.instagram.com, www.msn.com, www.baidu.com
CSS Media Query	*No description*	www.canva.com, www.w3schools.com, www.paypal.com

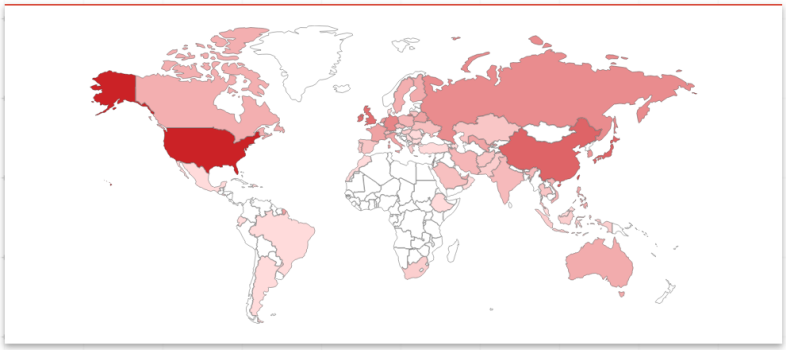
Shodan

Shodan Report

www.microsoft.com

Total: 1,486

// GENERAL



Countries

Hong Kong	440
United States	314
Taiwan	137
Japan	79
China	77

Ports

443	357
80	199
8081	94
1900	59
8083	27

MORE...

Organization

Hong Kong Telecommunications (HKT) Li...	312
Microsoft Corporation	168
Chunghwa Telecom Co.,Ltd.	95
IT7 Networks Inc	68
Amazon Technologies Inc.	31

MORE...

Vulnerabilities

CVE-2021-31206	1

Products

nginx	117
Apache httpd	74
Kerio Control	59
Microsoft IIS httpd	54
lighttpd	47

MORE...

Tags

cloud	423
cdn	7
self-signed	7

Operating Systems

No information available.

// HTTP INSIGHTS

Website Titles

Checking your credentials...	90
MediaTouch 2000 srl | Moodle Partner ...	47[48]
302 Found	
301 Moved Permanently	14
Veritas eDiscovery Platform log in	10

MORE...

Web Technologies

Cart Functionality	4
Microsoft ASP.NET	4
jQuery	4
Bootstrap	2
Google Font API	2

MORE...

Protocol Versions

http/1.1	51
h2	29
http/1.0	2

// SSL INSIGHTS

SSL/ TLS Versions

tlsv1.2	320
tlsv1.3	146
tlsv1	83
tlsv1.1	82
sslv3	4

MORE...

JARM Fingerprints

2ad2ad0000000000002ad2ad2ad2ad0f0dcb2...	83
3fd3fd20d00000000043d3fd3fd43dd812443...	54
15d3fd16d29d29d00042d43d000000f6a7635...	25
29d29d00029d29d00029d29d29d29d4d0c5ee...	20
20d08b20d21d20d20c42d08b20b41d4e14647...	13

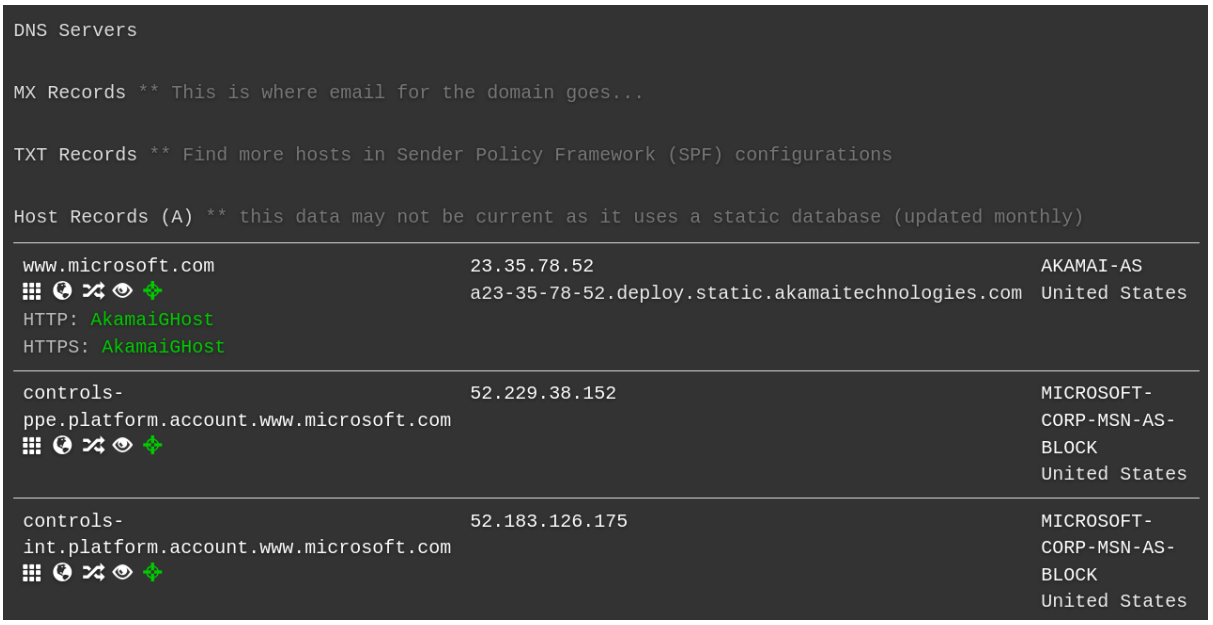
MORE...

JA3S Fingerprints

1d9c3e8c45ab7a2112263449a3ad9ece	88
303951d4c50efb2e991652225a6f02b1	72
0debd3853f330c574b05e0b6d882dc27	41
e35df3e00ca4ef31d42b34bebaa2f86e	39
ccc514751b175866924439bdbb5bba34	29

MORE...

DNSdumpster



Crunchbase

About

Microsoft is a software corporation that develops, manufactures, licenses, supports, and sells a range of software products and services.

- Redmond, Washington, United States
- 10001+
- Venture - Series Unknown
- Public
- www.microsoft.com
- 1,636

Highlights

Stock Symbol NASDAQ:MSFT	Acquisitions 250
Investments 162	Exits 48
Total Funding Amount $1M	Contacts 9,038

Industries
Developer Tools, Enterprise Software, Operating Systems, Software

Headquarters Regions
Greater Seattle Area, West Coast, Western US

Founded Date
Apr 4, 1975

Founders
Bill Gates, Paul Allen

Operating Status
Active

Last Funding Type
Venture - Series Unknown

Also Known As
msn

Legal Name
Microsoft Corporation

Related Hubs
Microsoft Alumni Founded Companies, Microsoft Portfolio Companies

Stock Symbol
NASDAQ:MSFT

Company Type
For Profit

Investment Stage
Late Stage Venture, Private Equity

Number of Exits
48

Contact Email
mdcc@microsoft.com

Phone Number
1800 1 441 0158

Sub-Organizations

Number of Sub-Orgs: 38

Xbox Game Studios
Division

Xamarin
Subsidiary

Wunderlist
Subsidiary

Visual Studio
Division

Vexcel
Subsidiary

Turn 10 Studios
Subsidiary

SoftArtisans
Subsidiary

Skype
Subsidiary

Razorfish
Subsidiary

Opalis Software
Subsidiary

$ Funding

Microsoft has raised a total of **$1M** in funding over **1** round. This was a **Venture - Series Unknown** round raised on **Sep 1, 1981**.

Microsoft is registered under the ticker **NASDAQ:MSFT**.

Microsoft is funded by **Technology Venture Investors**.

Microsoft has made **162** investments. Their most recent investment was on Feb 11, 2022, when **The Awareness Company** raised

Microsoft has made **2** diversity investments. Their most recent diversity investment was on Mar 7, 2018, when **Voicea** raised $14.5M.

Microsoft has had **48** exits. **Microsoft**'s most notable exits include **Cruise**, **Meta**, and **Apple**.

Microsoft has acquired **250** organizations. Their most recent acquisition was **Activision Blizzard** on Jan 18, 2022. They acquired **Activision Blizzard** for $68.7B.

Investments

Number of Investments
162

Number of Lead Investments
64

Microsoft has made **162** investments. Their most recent investment was on Feb 11, 2022, when **The Awareness Company** raised

How many investments has this organization made over time? SHOW

Which industries has this organization most actively invested in? SHOW

ed Date	Organization Name	Lead Investor	Funding Round
Feb 11, 2022	The Awareness Company	Yes	Venture Round - The Awareness Company
Jan 17, 2022	Wayve	–	Series B - Wayve
Nov 19, 2021	Wejo	–	Post-IPO Equity - Wejo
Sep 29, 2021	Truveta	Yes	Corporate Round - Truveta

Exits

Number of Exits
48

Microsoft has had **48** exits. **Microsoft**'s most notable exits include **Cruise**, **Meta**, and **Apple**.

Which industries has this organization had the most exits in? SHOW

Cruise
Cruise builds self-driving vehicles that safely connect people to places, things, and experiences they care about.

Meta
Meta is a social technology company that enables people to connect, find communities, and grow businesses.

Apple
Apple is a multinational corporation that designs, manufactures, and markets consumer electronics, personal computers, and software.

DocuSign
DocuSign helps small- and medium-sized businesses collect information, automate data workflows, and sign on various devices.

Uber
Uber develops, markets, and operates a ride-sharing mobile application that allows consumers to submit a trip request.

Equinix
Equinix is an internet company that provides data center services for companies, businesses, and organizations.

Acquisitions

Number of Acquisitions

250

Microsoft has acquired **250** organizations. Their most recent acquisition was **Activision Blizzard** on Jan 18, 2022. They acquired **Activision Blizzard** for $68.7B.

Which types of acquisition does this organization make most frequently? SHOW

Acquiree Name	Announced Date	Price	Transaction Name
Activision Blizzard	Jan 18, 2022	$68.7B	Activision Blizzard acquired by Microsc
Xandr	Dec 21, 2021	–	Xandr acquired by Microsoft
Two Hat Security	Oct 29, 2021	–	Two Hat Security acquired by Microsc
Clear Software	Oct 22, 2021	–	Clear Software acqu by Microsoft
Ally.io	Oct 7, 2021	$76M	Ally.io acquired by Microsoft
TakeLessons	Sep 10, 2021	–	TakeLessons acquir by Microsoft
Clipchamp	Sep 7, 2021	–	Clipchamp acquired Microsoft
Peer5	Aug 10, 2021	–	Peer5 acquired by Microsoft
Suplari	Jul 28, 2021	–	Suplari acquired by Microsoft
CloudKnox Security	Jul 21, 2021	–	CloudKnox Security acquired by Microsc

Name	Profession
Aamer Hydrie	CTO - Microsoft Dynamics 365 for Sales Executive Sales
Aaron Getz	Chief Executive Executive Operations
Abdulkhamid Godina	Co-Chief Executive Officerm Executive Management
Abel Wang	Chief Architect Executive Engineering, Operations
Ackhadet Viradet	Chief of Staff Executive Operations
Adam Ruderman	Chief Architect, Customer Success Executive Management, Operations
Aj Bhandari	CEO Executive Operations
Aja West	CEO Executive Management, Operations
Al Smith	Chief Business Applications Architect Executive Operations
Alaks Sevugan	Chief Operations Officer Executive Operations

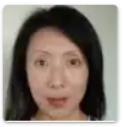
Employee Profiles

Number of Employee Profiles

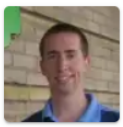
2,571

Microsoft has **2,571** current employee profiles, including Principal PM Manager **Hani Loza**.

Hani Loza
Principal PM Manager



Paige Liu
Principle Software Design Engineer



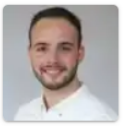
Seth Goings
Principal Software Engineer

Claude Lorenson
Sr Product Marketing Manager, Cloud&Enterprise Platform

Dan Taylor
Principal PM Manager

Cody Beyer
Program Manager - Visual Studio for Mac

Caitlin Hart
Principal Program Manager



Ross Gibson
Account Executive for Police

Board Member and Advisor Profiles

Number of Board Member and Advisor Profiles

54

Microsoft has **54** board members and advisors, including **Maria Klawe**.

Maria Klawe
Board Member
Mar 2009

Helmut Panke
Board Member
Nov 11, 2003

Yoshua Bengio
Advisor
Jan 2017

Reid Hoffman
Board Member
Mar 14, 2017

Reza Zadeh
Advisor
Nov 29, 2015

Brad Smith
Board Member

Renjith Varma
Advisor
Jul 2007

John Tucker
Board Member
Mar 2021

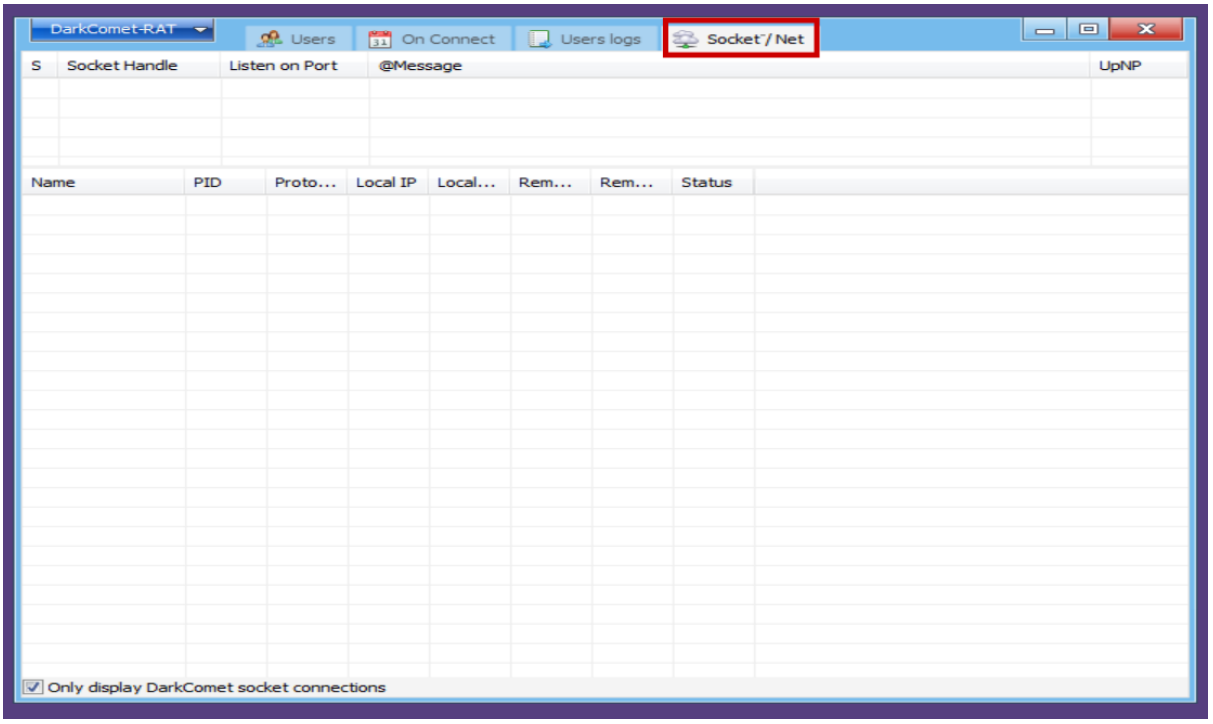
Overview

- Microsoft has made **162** investments and has **250** acquisitions
- Microsoft has **1486** servers around the global as per shodan report
- Microsoft uses **nginx** servers more than **Microsoft IIS httpd**
- **ASP.NET** and **jQuery** are the two most used web technologies on microsoft website
- Microsoft.com is registered on **MarkMonitor Inc.**
- www.microsoft.com uses **Akamai Technologies** for hosting
- **IP Addresses**
    - 23.203.17.160
    - 23.34.25.163
    - 104.95.181.163
    - 2a02:26f0:9b00:291:0:0:0:356e
    - 2600:140f:6:7a9::356e
    - 2600:140f:6:789::356e
    - 2600:1404:d400:194::356e
    - 2600:1404:d400:18c::356e

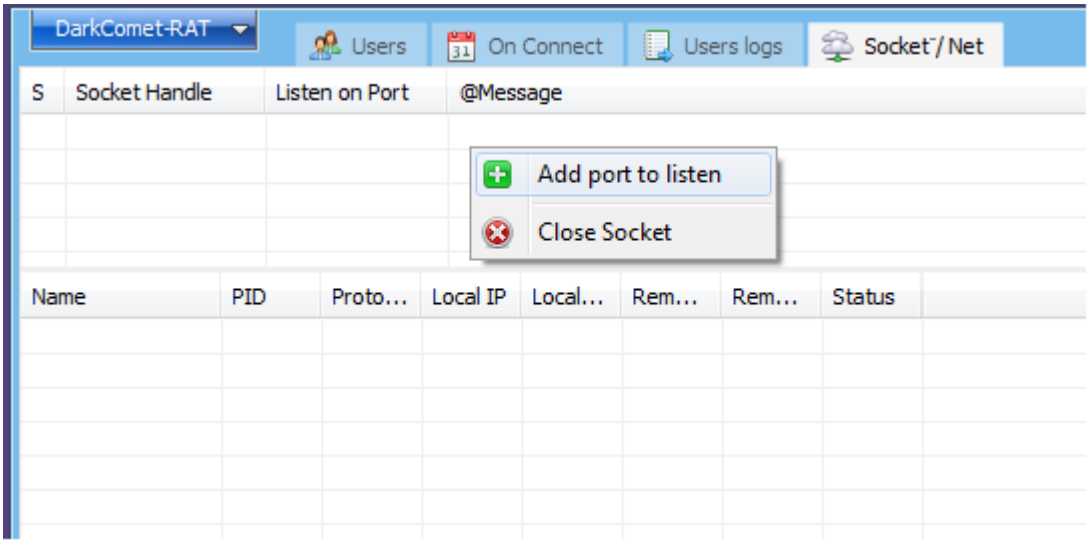
Remote Access Trojan

Proof Of Concept (PoC)

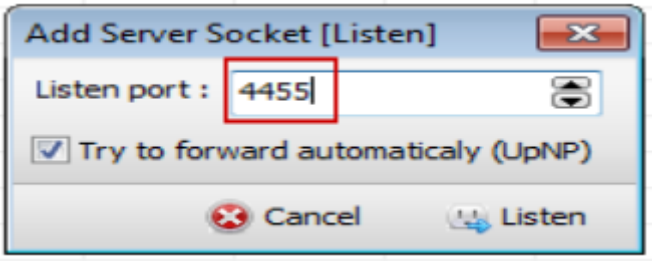
- Download Darkcomet from the internet. Then install it on the attacker machine.
- Open the DarkComet and select Socket/Net tab



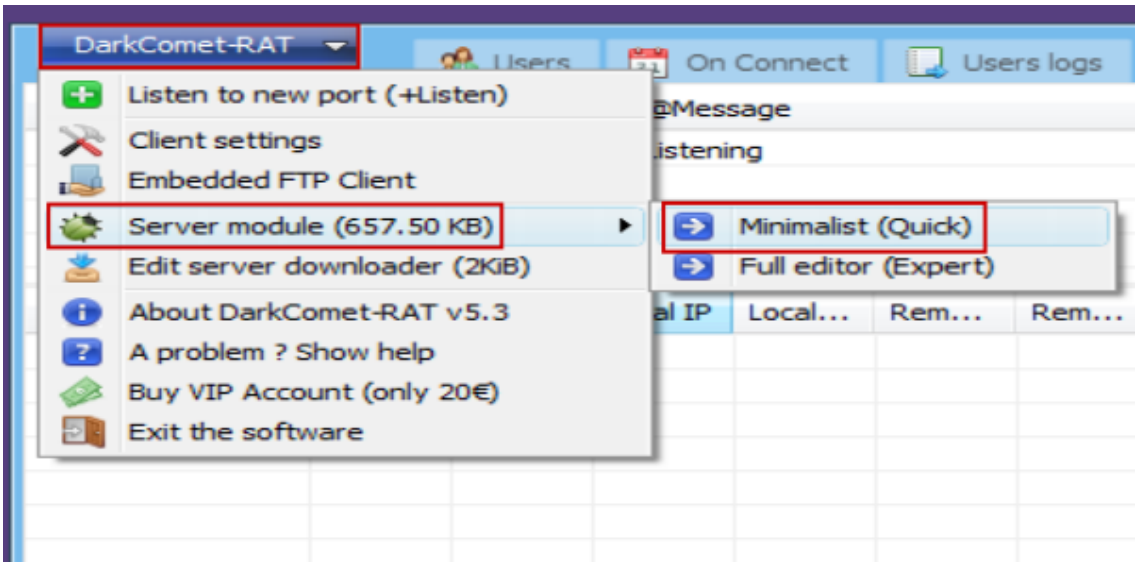
- Right click below Socket Handle title bar as shown below and select **Add port to listen**



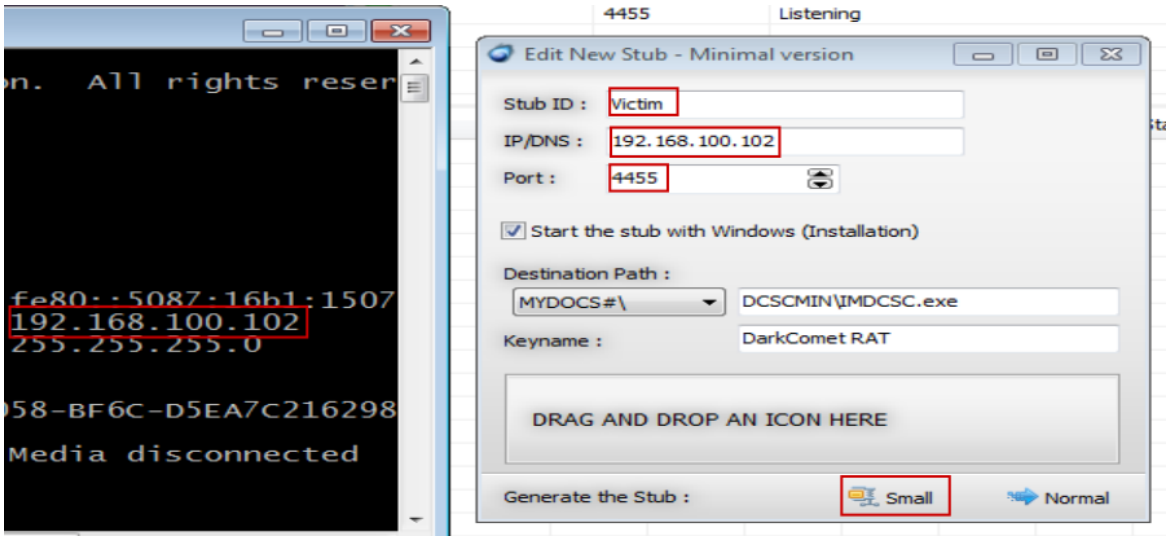
- And give a port number to listen and click on **Listen**



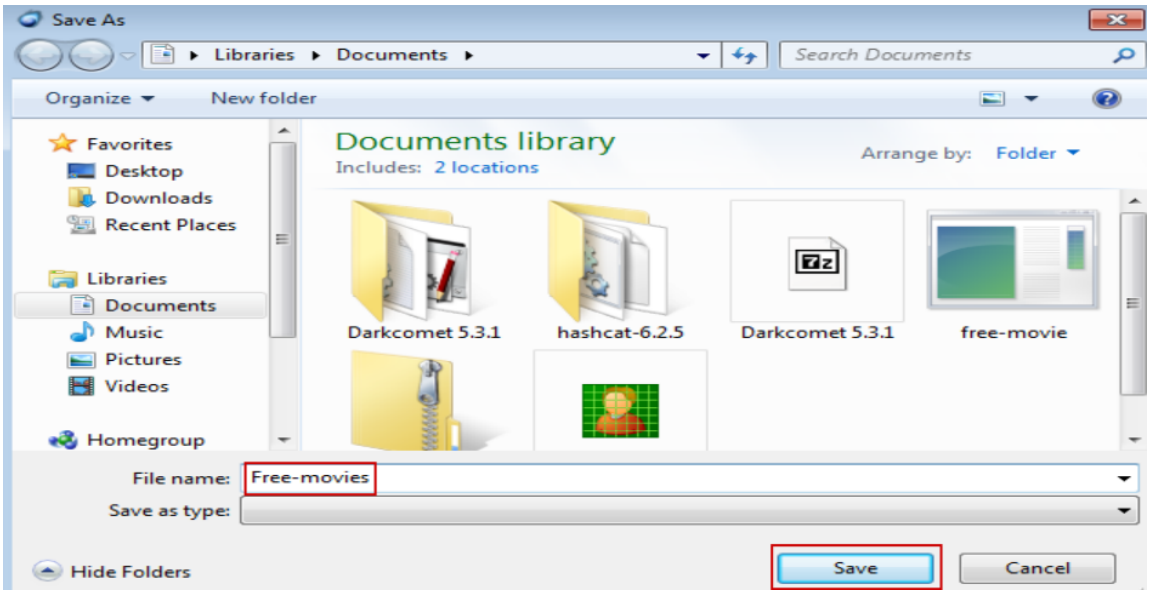
- Click on **DarkComet-RAT** then **Server module** and finally **Minimalist**



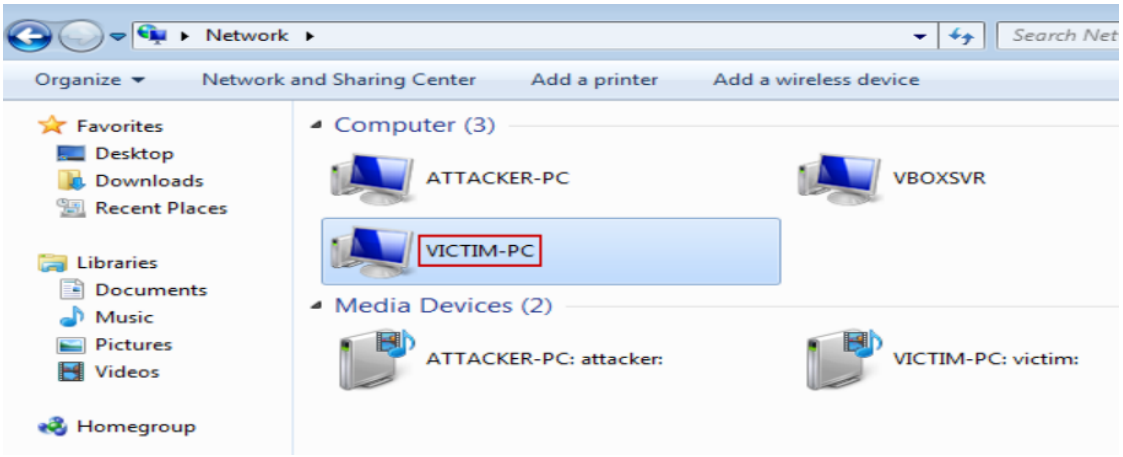
- For **Stub ID** give any name, here it is victim , for **IP/DNS** give your local IP as this virtual environment and for **Port** give the same port we used for listening before. And, finally click on either **Small** or **Normal**

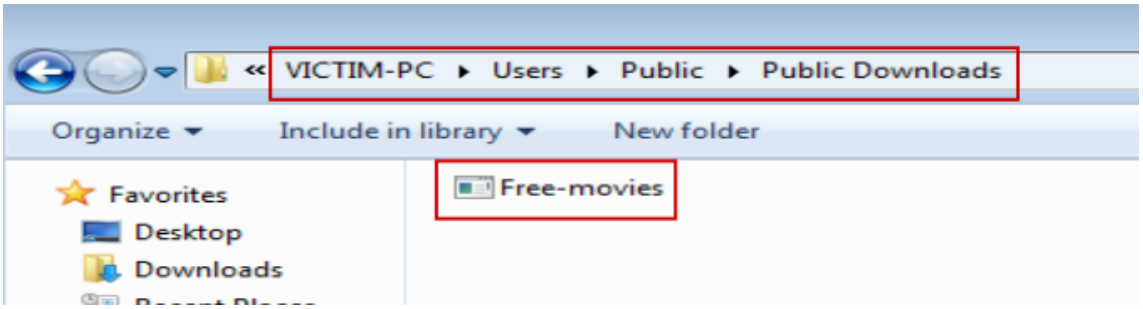


- Here I clicked on **Small**, give a name and click on **Save**

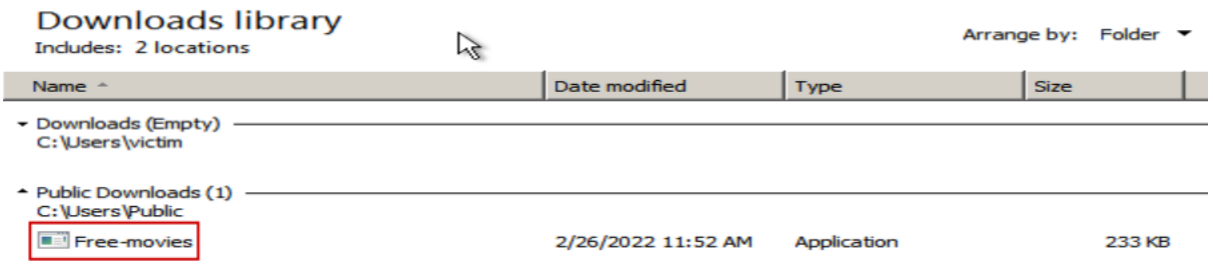


- Now deliver this RAT to the victim through any means like social engineering etc. Here I'll copy and paste the RAT in victim's **public downloads** folder through share

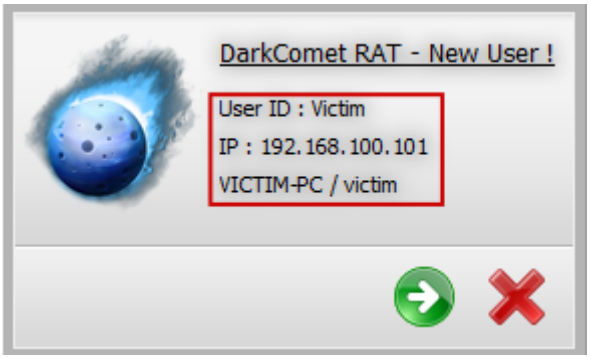




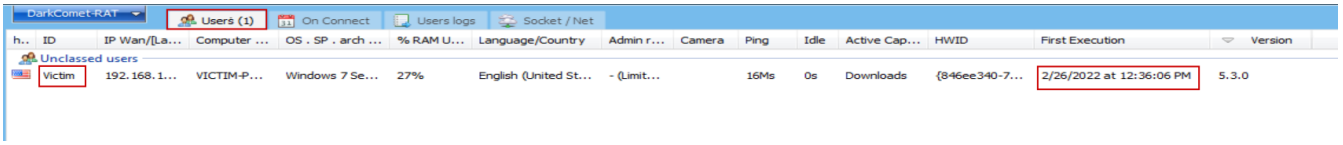
- On victim's PC:



- Once our victim executes the program, we get victim's PC connection to Darkcomet



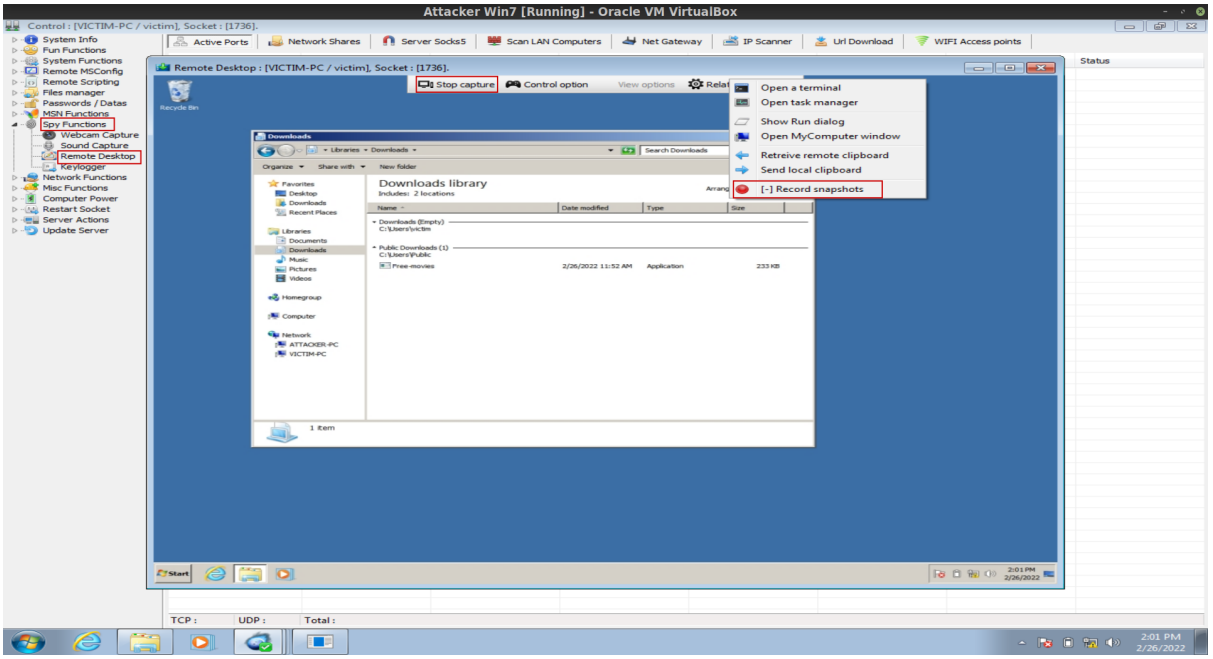
- Navigate to Users tab in Darkcomet, we get all info about our victim including time of execution of our RAT



- Double click on it, we will get as many controls over our victim's PC as possible

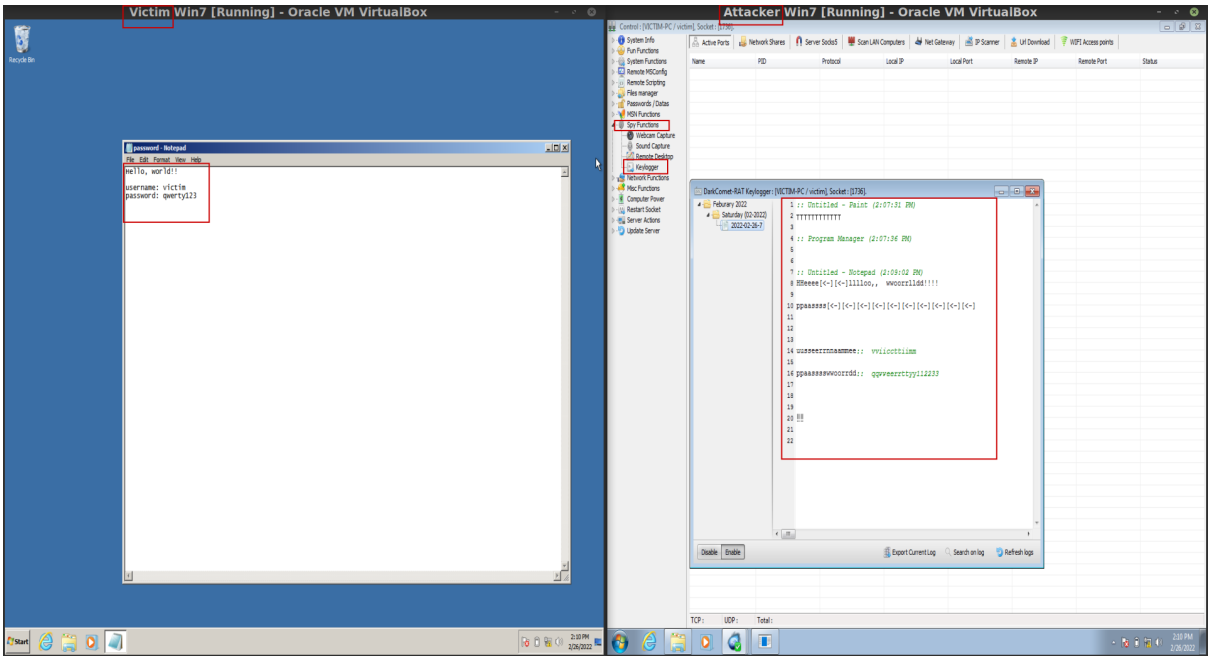
PoC to take screenshots:

- Click on **Spy Functions** > **Remote Desktop** > **Start Capture** and click on **Related Commands** > **Record snapshots**



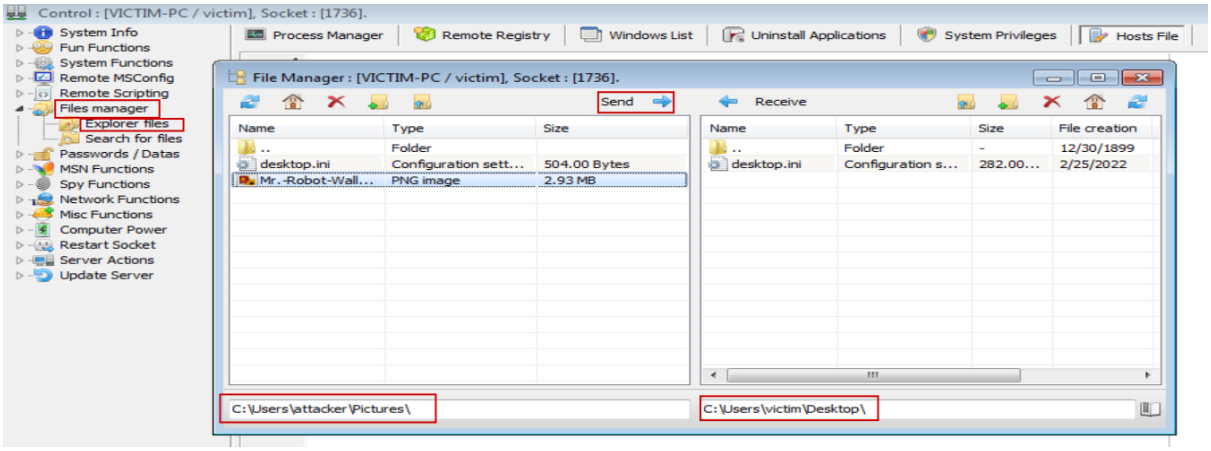
PoC to take Keystrokes:

- Click on **Spy Functions** > **Keylogger** >

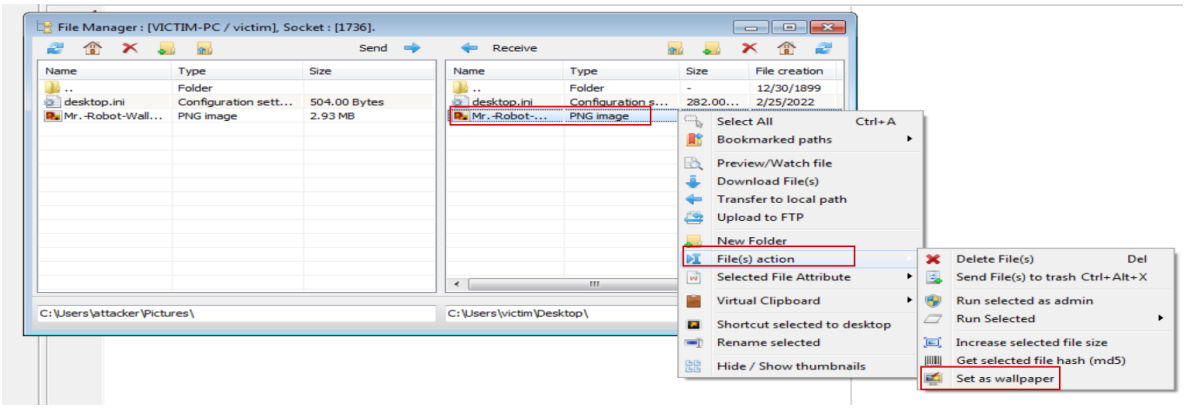


PoC to change Desktop data:

- Click on **File manager** > **Explorer Files** and select file which you want to send on left side and chose the location for receiving on victim's machine on right side and click **Send**



- After sending the image file, we can set it as desktop background - the same can be achieved using **Remote Desktop**



Recommendations

- Never download or install software from a source you don't trust completely
- Never open an attachment or run a program sent to you in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on your computer
- Don't execute any program that you don't know
- Use firewalls

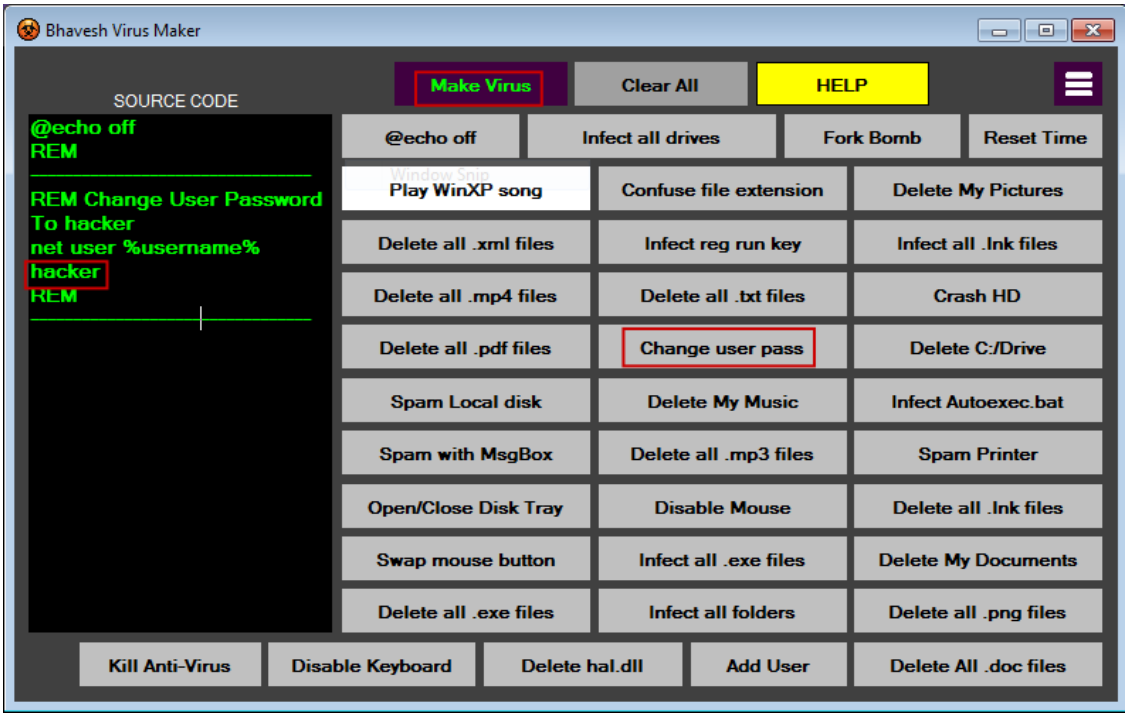
References

- What is a Trojan Virus & How to Protect Against It | Webroot
- Remote Access Trojan (RAT) | RAT Malware | RAT Trojans | Malwarebytes Labs | Threats
- Remote desktop software - Wikipedia
- DarkComet - Wikipedia

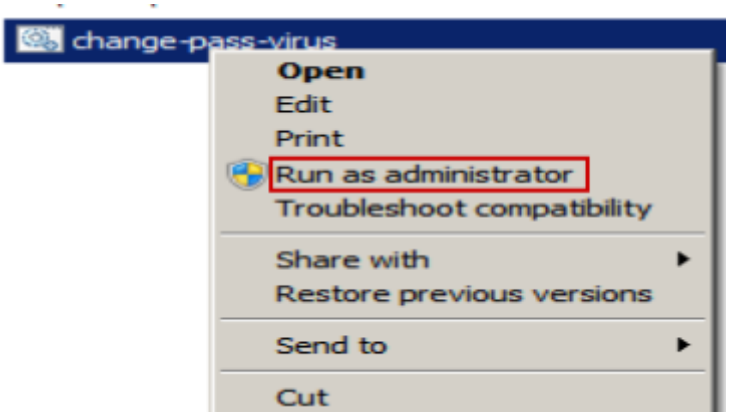
Batch Virus Maker by Bhavesh Kaul

Proof Of Concept (PoC)

- Download the tool from here: [Bhavesh Virus Maker download | SourceForge.net](#) and install it
- Choose any payload provided in the tool as shown below



- Here, I'm changing the password of the user
- After you're done crafting your virus with payloads you can generate virus with **Make Virus** button and give it a name when saving it
- Deliver the virus to victim through any means and victim needs to execute it with **Administrator** permissions to work

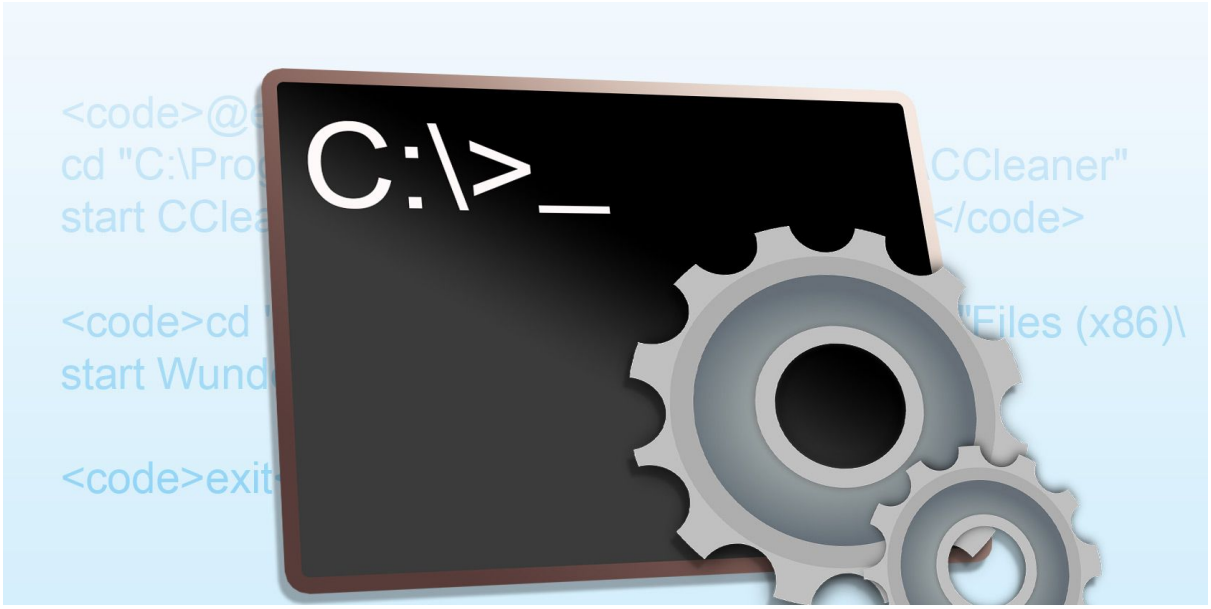


Recommendations

- Never download or install software from a source you don't trust completely
- Never open an attachment or run a program sent to you in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a antivirus is installed and running on your computer
- Don't execute any program that you don't know
- Use firewalls

References

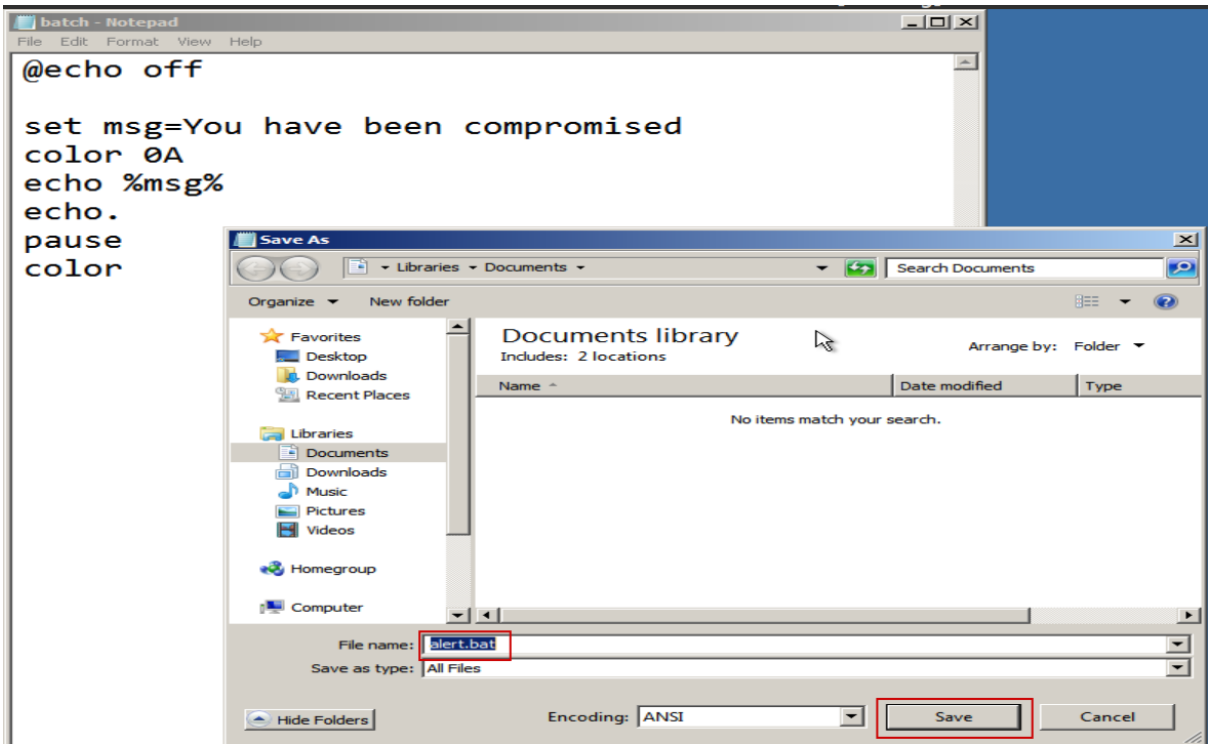
- Computer_virus | Wiki
- Ransomware | Wiki
- Mitigating malware and ransomware attacks - NCSC.GOV.UK



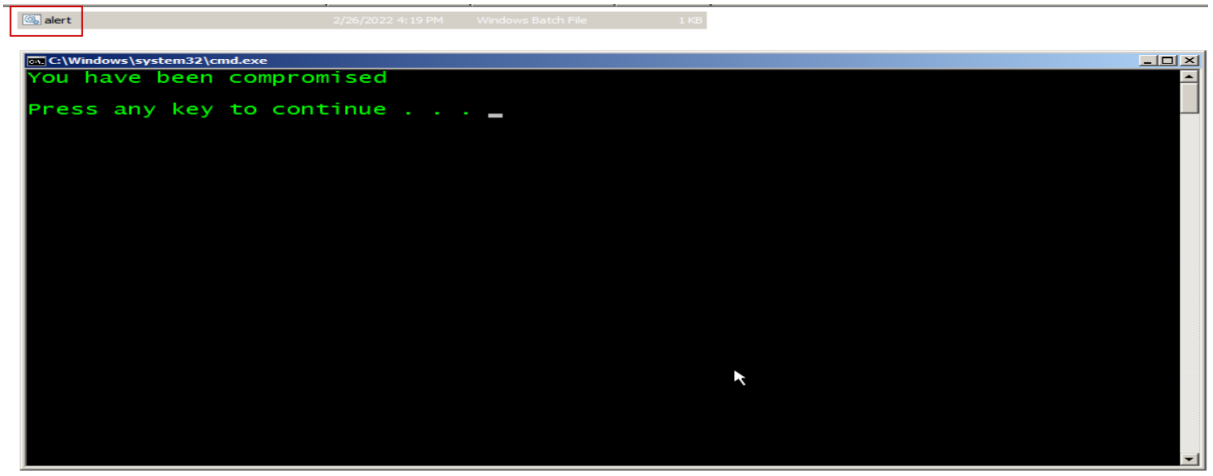
Simple Batch Program

Proof Of Concept (PoC)

- A simple minimum prank script:



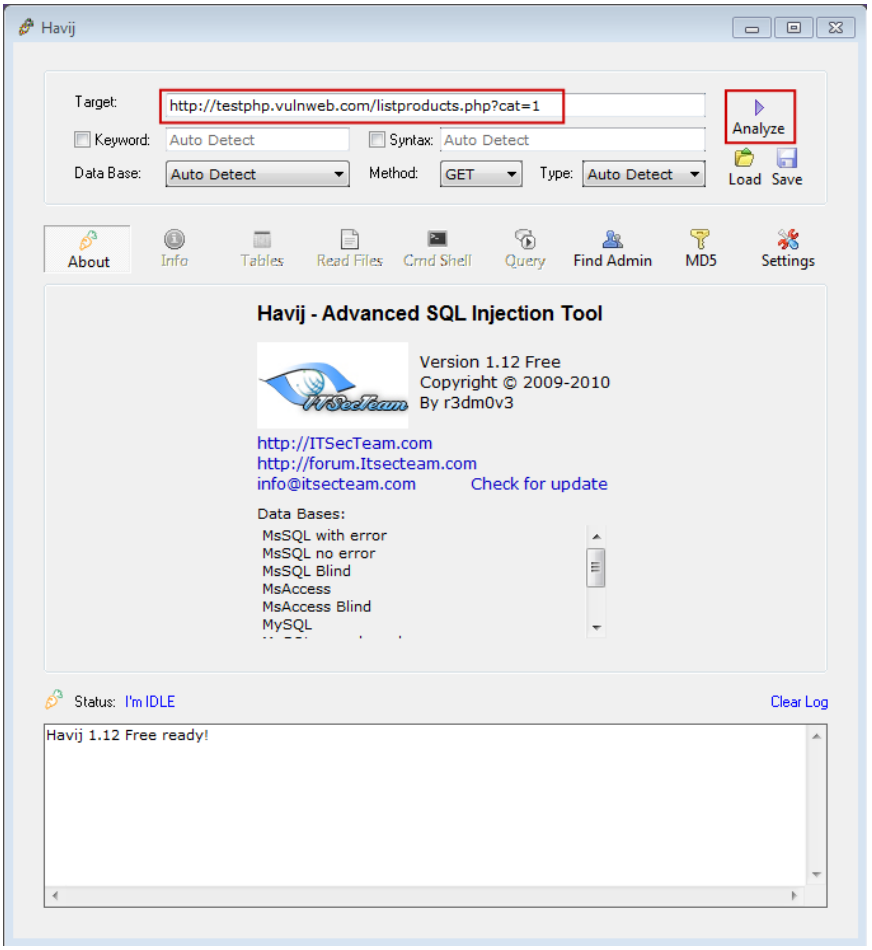
- Save it with **.bat** extension and select **Save as type:** as **All Files**
- Double click it and it will execute:



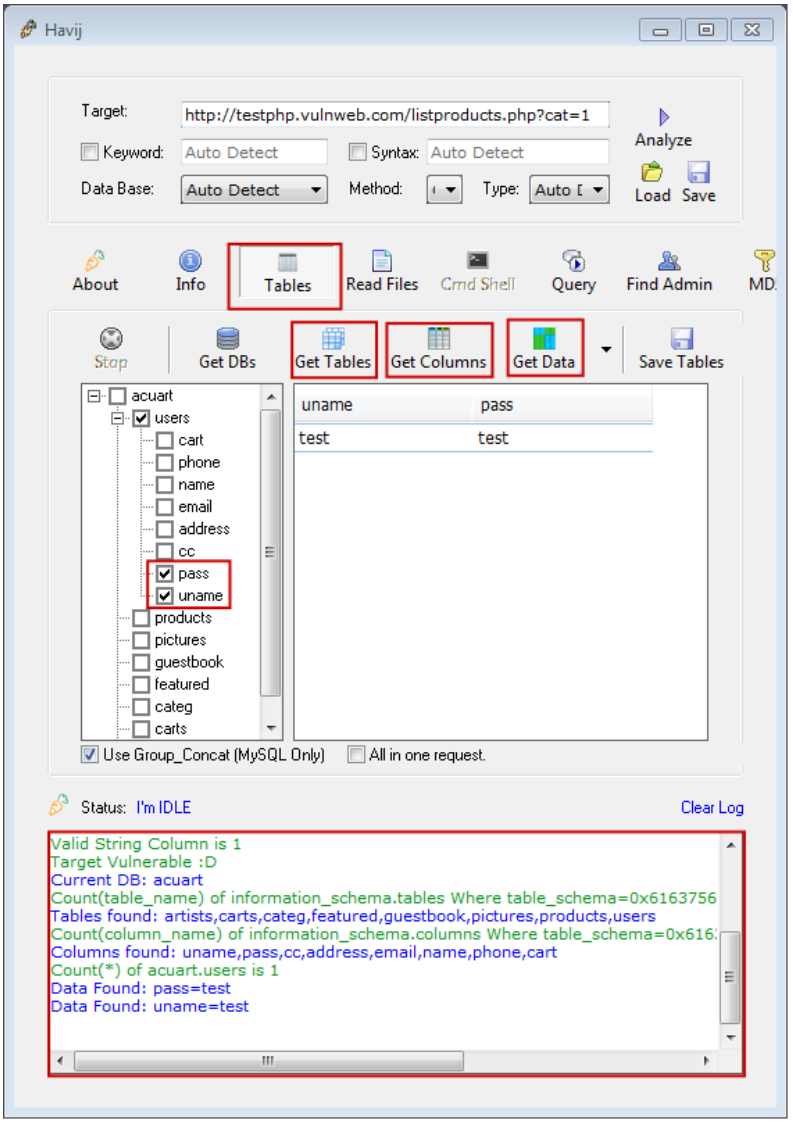
Automated SQL Injection Tool

Proof Of Concept (PoC)

- Download the Havij tool and install it and run it
- Insert you target in **Target:** field as shown below and click on **Analyze**



- After Havij successfully find SQL injection in the target, we can enumerate data like below
- Click on **Tables** > **Get Tables** > **Get Columns** and select columns then click **Get Data**



- Here we can see one user with test as username and password

Recommendations

Take the following precautions to avoid exploitation of SQL injections:

- Whitelist User Input: Whitelist all user input for expected data only. For example if you are expecting a flower name, limit it to alphabets only upto 20 characters in length. If you are expecting some ID, restrict it to numbers only
- Prepared Statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query
- Character encoding: If you are taking input that requires you to accept special characters, encode it. Example. Convert all ‘ to \’ , “ to \”, \ to \\. It is also suggested to follow a standard encoding for all special characters such has HTML encoding, URL encoding etc
- Do not store passwords in plain text. Convert them to hashes using SHA1 SHA256 Blowfish etc
- Do not run Database Service as admin/root user
- Disable/remove default accounts, passwords and databases
- Assign each Database user only the required permissions and not all permissions

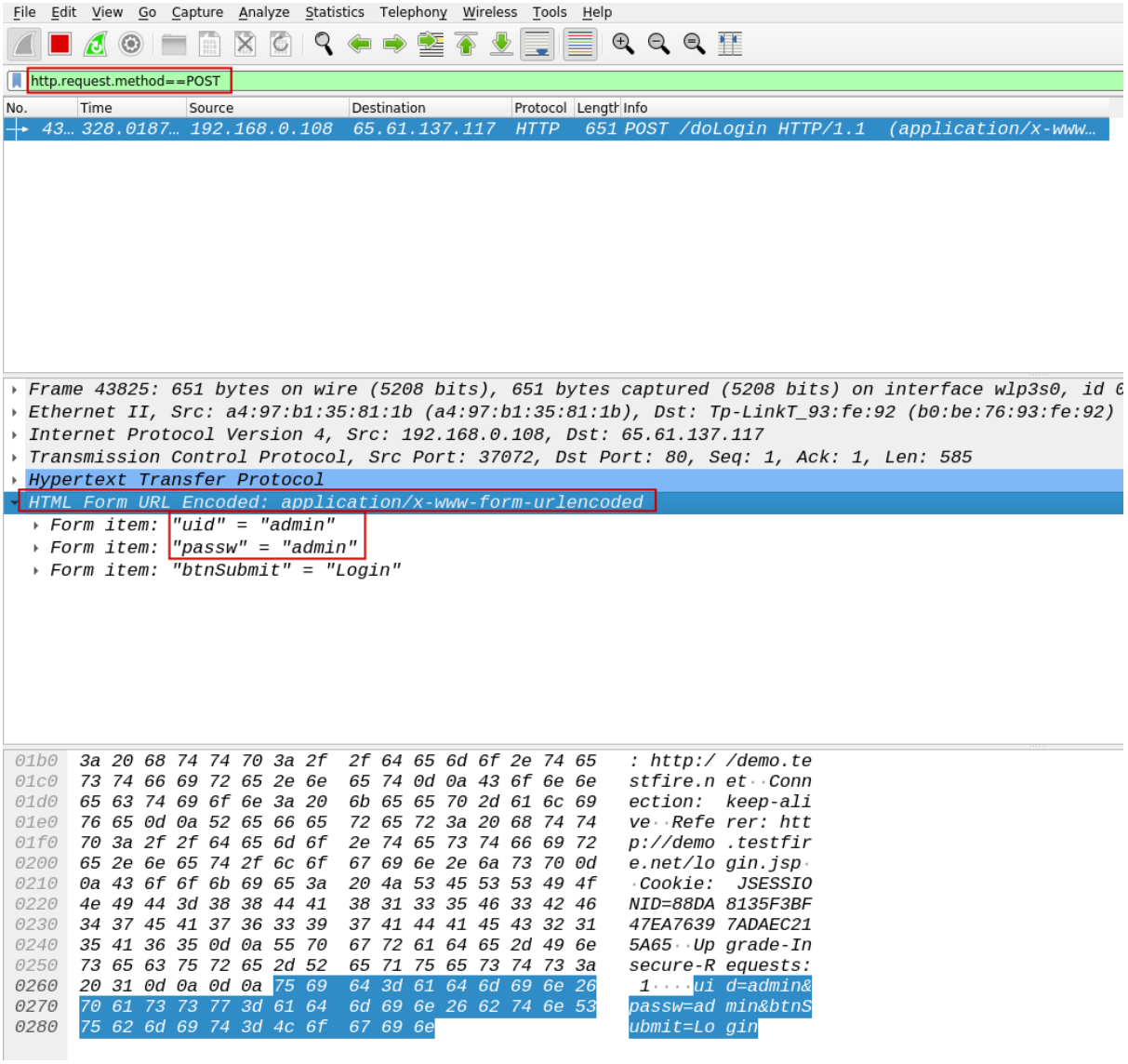
References

- SQL Injection | OWASP
- SQL injection

Wireshark Sniffing

Proof Of Concept (PoC)

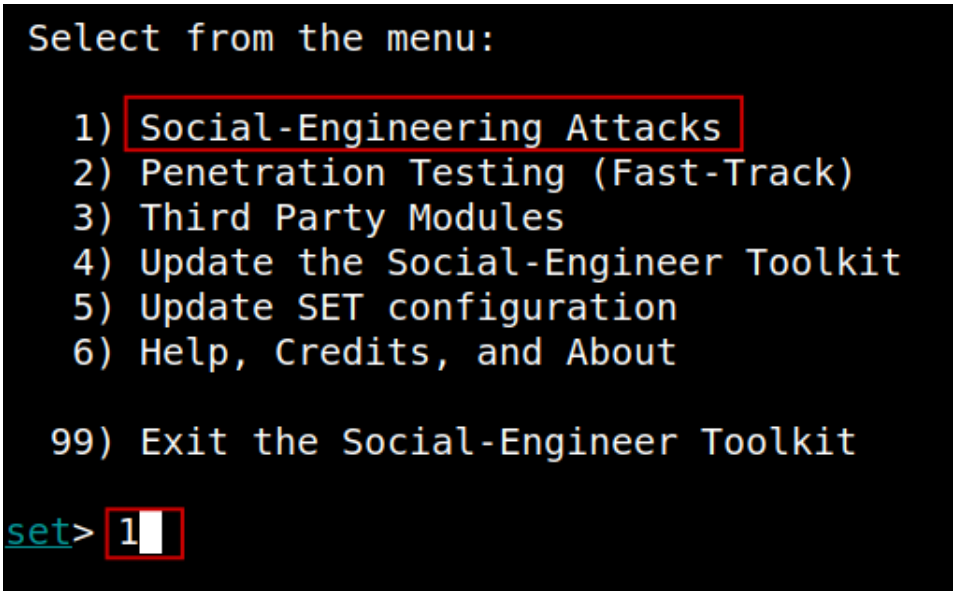
- Download and install wireshark. Launch the wireshark and select your internet interface and double click on it or press **crtl + E**
- Go to http://demo.testfire.net/login.jsp use **admin** as username & password
- In the wireshark, type **http.request.method==POST** as filter and select the packet and dropdown **HTML Form URL Encoded: application/x-www-form-urlencoded**
- Username and password will be visible as udi and passw respectively.



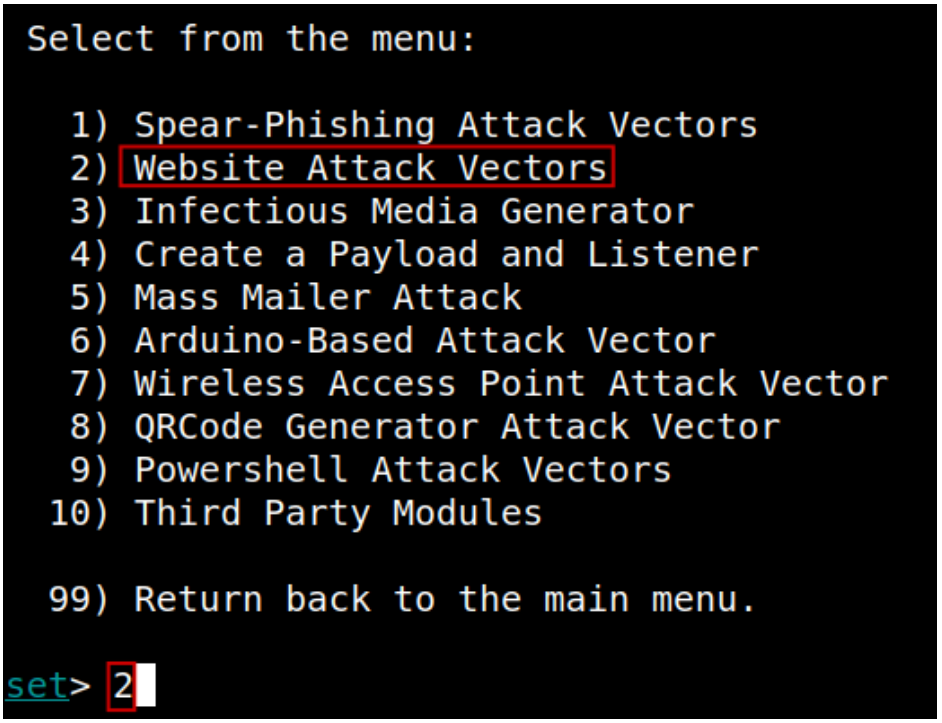
Phishing Attacks

Proof Of Concept (PoC)

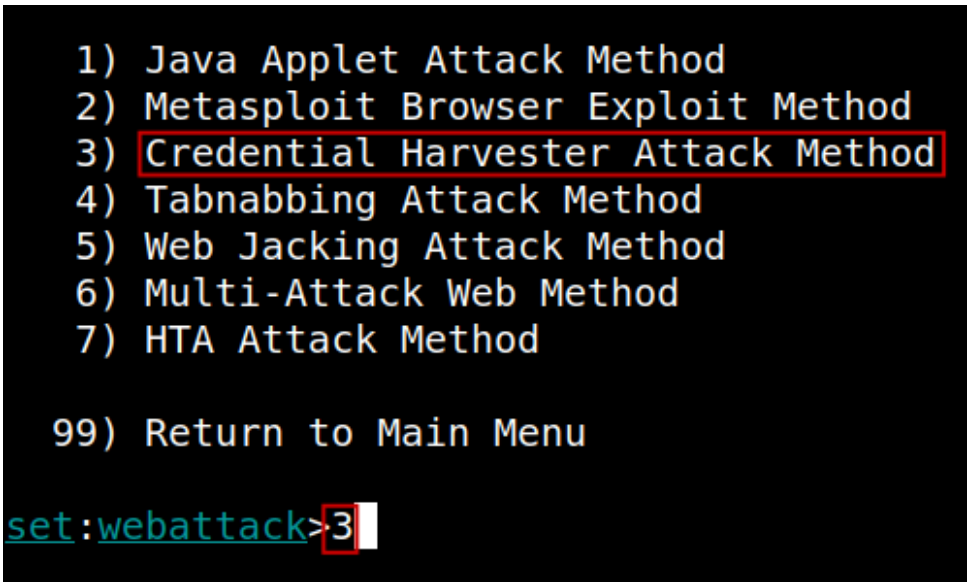
- Download Social Engineering Toolkit, install and run
- It'll give a fair disclaimer and accept it by typing **y** and press enter
- Then select **Social-Engineering Attacks** by typing **1** and press enter



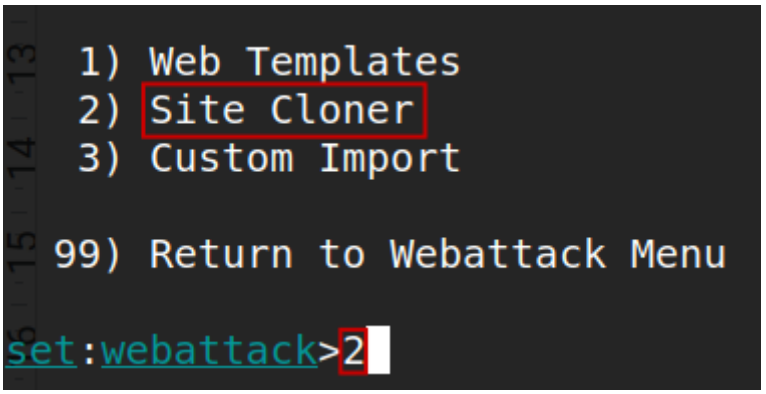
- Then select **Website Attack Vectors** by typing **2** and press enter



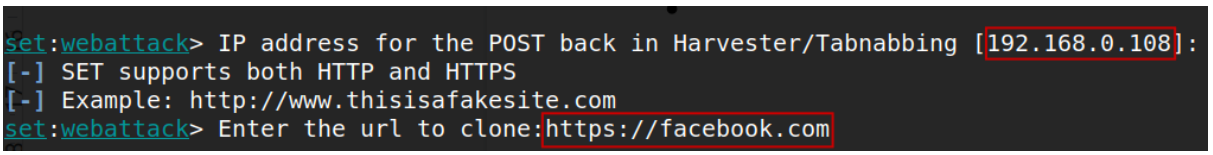
- Select **Credential Harvester Attack Method** by typing **3** and press enter



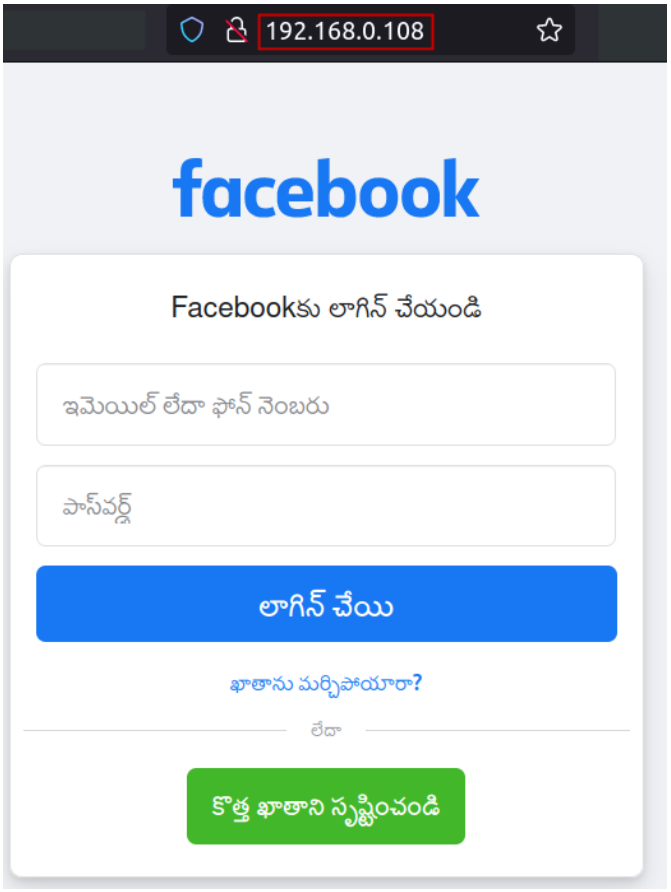
- Select **Site Cloner** by typing **2** and press enter



- Press enter for IP address if it is correct interface and enter the site you want to clone next as shown below



- Visit the IP address you gave, the site should be running on port 80
- Enter any username & password and click login



- Goto terminal and press **crtl+C**
- Data will be stored in this directory: **/root/.set/reports**

```
root@kickass-PC:~/.set/reports# grep email= 2022-02-28\ 17\:46\:13.487204.xml
      <param>email=test_username</param>
root@kickass-PC:~/.set/reports# grep pass= 2022-02-28\ 17\:46\:13.487204.xml
      <param>pass=test_password</param>
root@kickass-PC:~/.set/reports#
```

Recommendations

- **Think Before You Click!** – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them.
- **Install an Anti-Phishing Toolbar** – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites.
- **Verify a Site's Security –** It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar.
- **Check Your Online Accounts Regularly** – If you don't visit an online account for a while, someone could be having a field day with it.
- **Keep Your Browser Up to Date** – Security patches are released for popular browsers all the time.
- **Be Wary of Pop-Ups** – Pop-up windows often masquerade as legitimate components of a website.
- **Never Give Out Personal Information** – As a general rule, you should never share personal or financially sensitive information over the Internet.

References

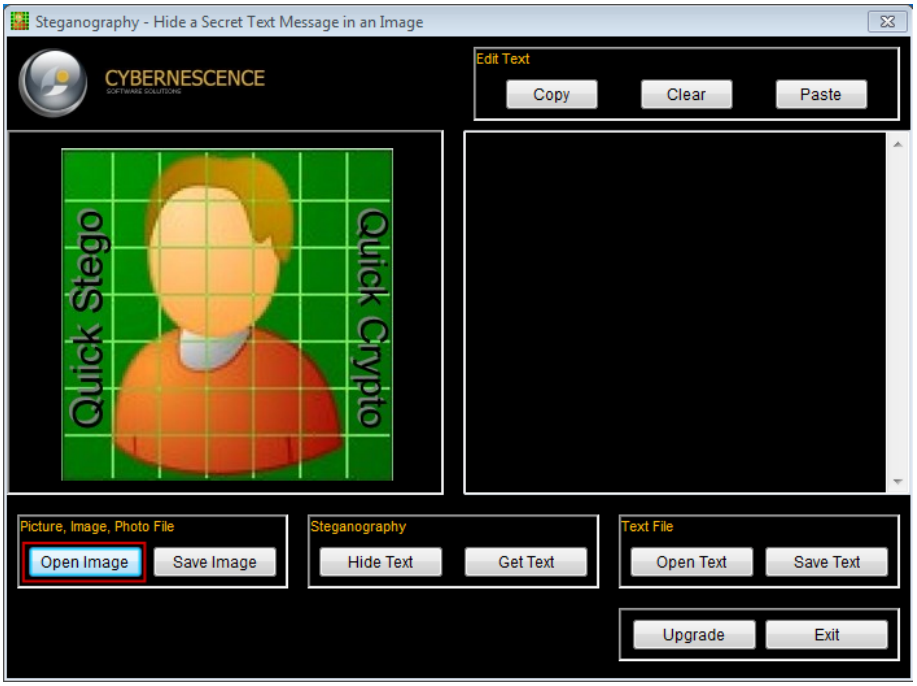
- 10 Ways to Avoid Phishing Scams
- Phishing | Wiki

Steganography

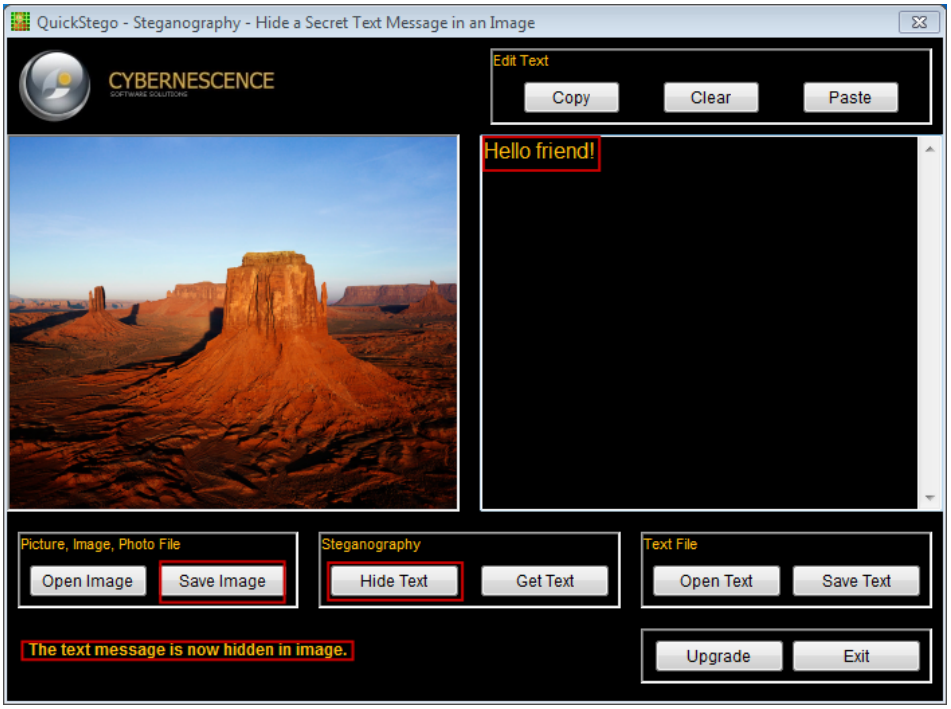
with Quick Stego tool and copy command

Proof Of Concept (PoC)

- Download Quick Stego tool, install and run
- Click on **Open Image** and select image



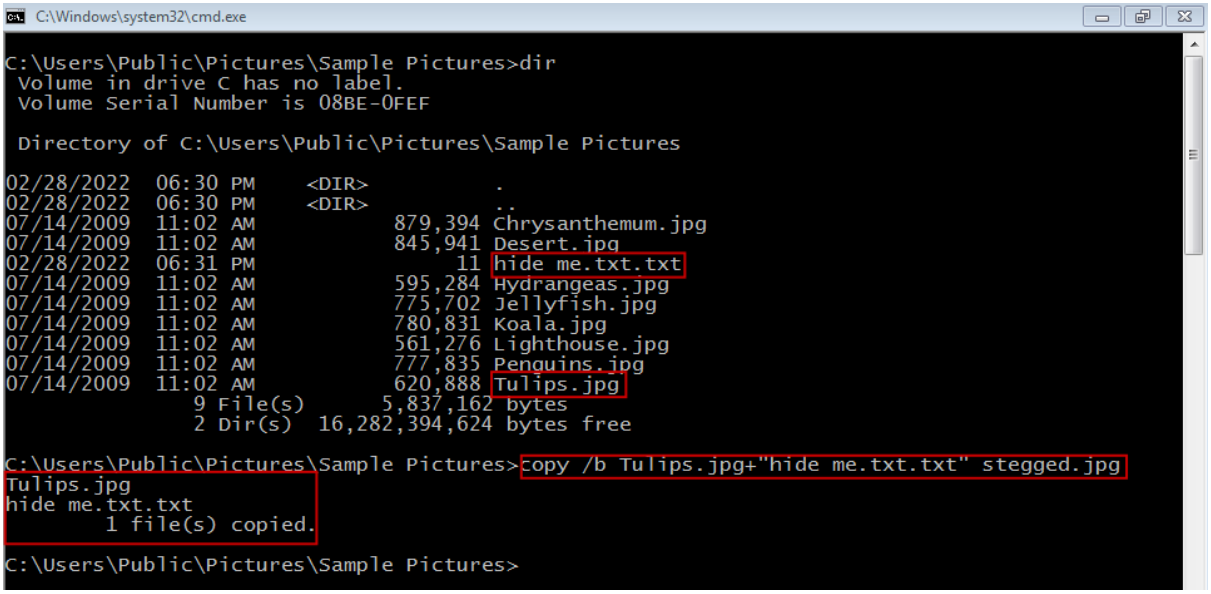
- Type text you want to hide on right empty space & click on **Hide Text**
- Then Click on **Save Image** and give it a name



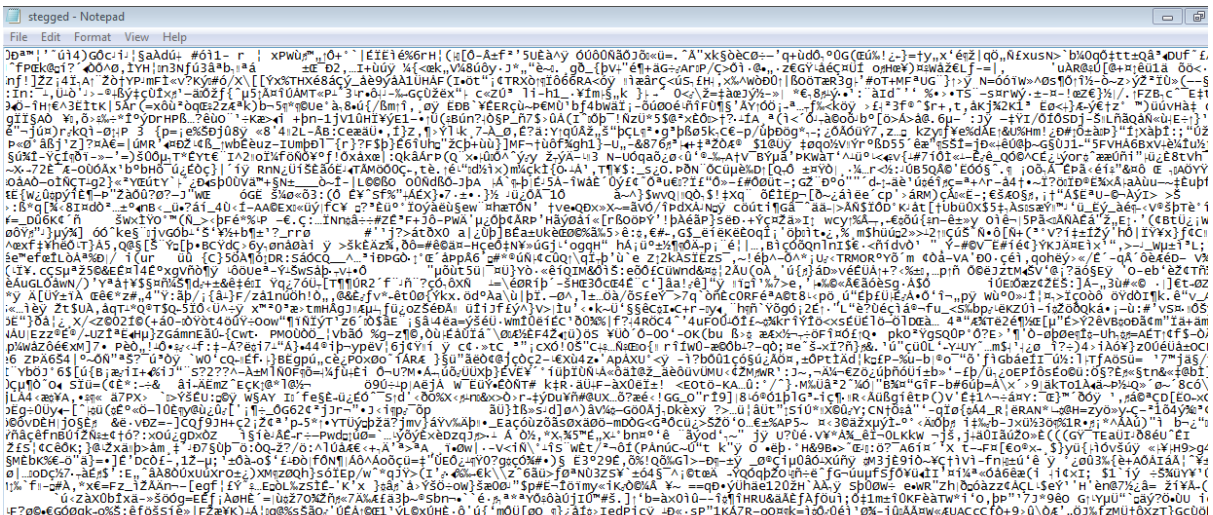
- To decode a image launch the Quick Stego tool and click on **Open Image** select the image you want to decode and quick stego tool will decode it; secret text will be shown on right column

PoC - copy command

- Create a text document in the images directory and use the below command
- Command: `copy /b original.jpg+"hide me.txt" bindedSteg.jpg`
- `/b` - this flag means bind
- Replace **original.jpg** and **hide me.txt** with filenames of image and file you want to hide respectively.
- Last part of the command is the filename you want to assign for the resulting file



- To extract the text from the image, open the image with notepad and scroll down to last because the text is appended to file at the last



Advantages of Steganography

- Hard to detect. Original image is very similar to the altered image. Embedded data resembles Gaussian noise.
- Hard to detect as message and fundamental image data share the same range.
- The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may therefore be incriminating in countries in which encryption is illegal.

Advantages of Cryptography

Cryptography is an essential information security tool. It provides the four most basic services of information security −

- **Confidentiality** − Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** − The cryptographic hash functions are playing a vital role in assuring the users about the data integrity.
- **Non-repudiation** − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of a passing message by the sender.

All these fundamental services offered by cryptography have enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

Thank You!

Contact:

+91 8074346267

jaswanthsunkara@protonmail.com

https://kickass101.github.io