



**CYBERARK<sup>®</sup>**

# **BEYOND LEAST PRIVILEGE**

Credential Harvesting in  
Endpoint Privilege Manager

# ANDY THOMPSON

## Andy.Thompson@CyberArk.com

- LinkedIn: [in/andythompsoninfosec](https://www.linkedin.com/in/andythompsoninfosec)
- GitHub: [github.com/binarywasp](https://github.com/binarywasp)
- Twitter: @R41nMkr

- Global Research Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hacker
- Travel-Hacker



IT IS ALL ABOUT THE ENDPOINT

# Most attacks start on the endpoints

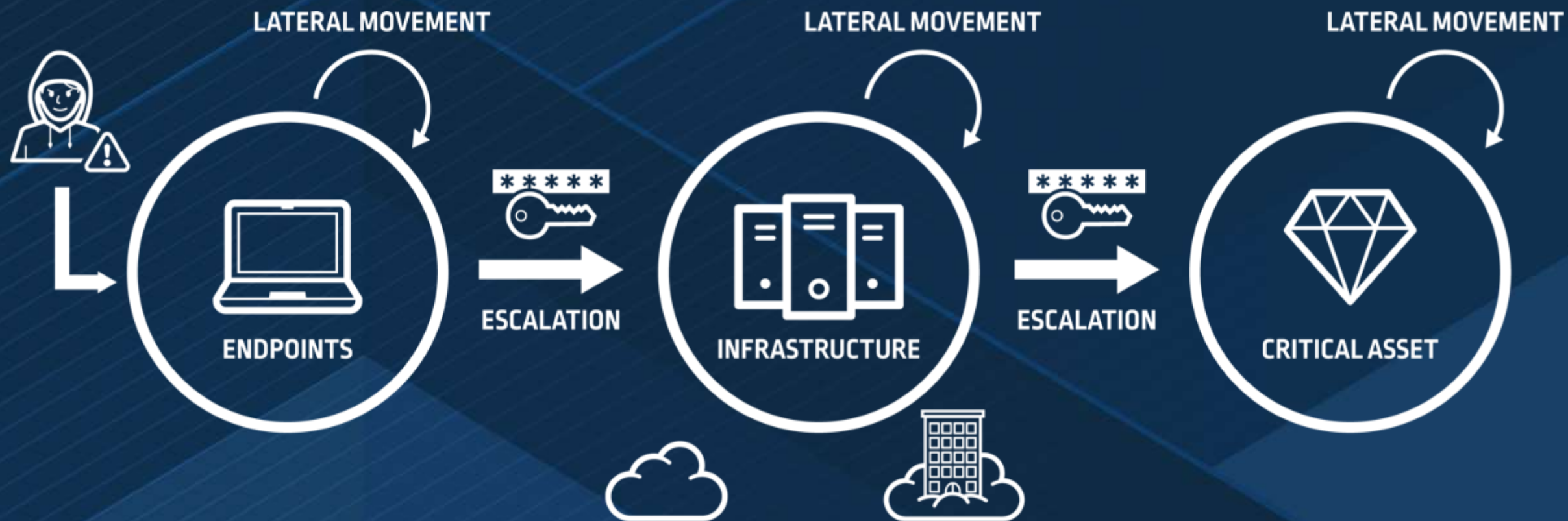


The endpoint is the best source for harvesting credentials.  
This facilitates lateral movement.



# AGENDA

# ATTACK PATTERN

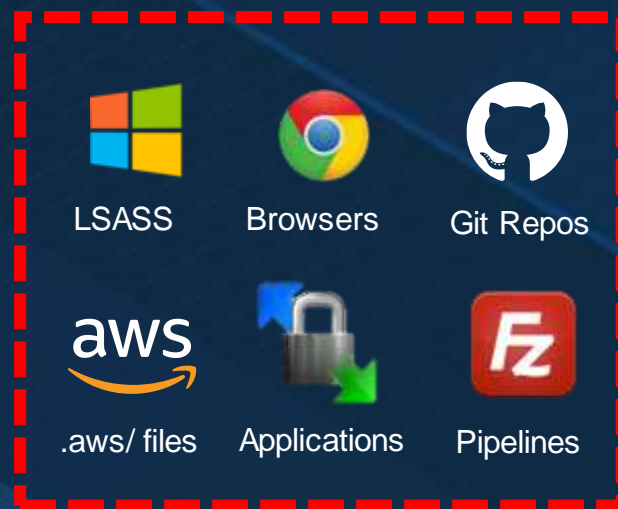




# CREDENTIAL THEFT

- ☐ System Processes
- ☐ Registry Locations
- ☐ Known File Paths
- ☐ Session Tokens

**First Action:**  
**Dump Credentials**



*Within Minutes  
or Seconds...*



**Cloud/On-Prem  
Network Takeover**



*Targeted Repositories*

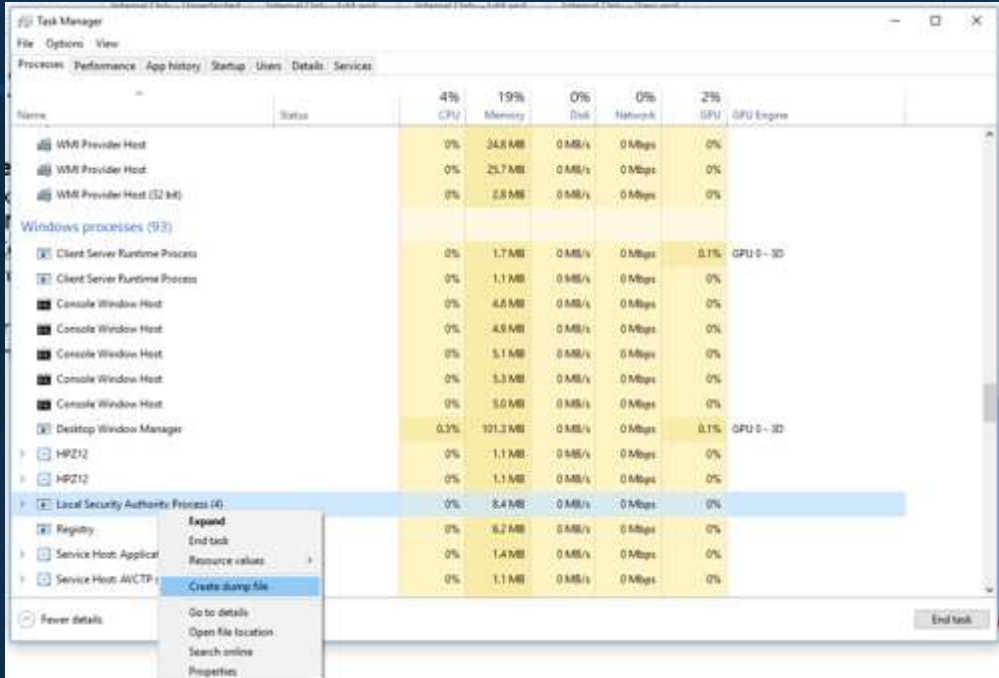


## CREDENTIAL THEFT

# RISK: SYSTEM PROCESSES

## LSASS memory:

Clear-text passwords of logged on users, Kerberos tickets, Kerberos encryption keys, SmartCard/Token PIN codes, LM/NTLM hashes, DPAPI Domain Backup Key, Domain Trust Auth Information, cached DPAPI MasterKeys, cached SysKey (need to decrypt SAM/LSA Secrets/Cached credentials/NTDS.dit), clear-text passwords of accounts, stored in Credential Manager.



The screenshot shows the Windows Task Manager Performance tab. The 'Processes' section is expanded, showing a list of running processes. The 'Local Security Authority Process (lsass.exe)' is highlighted, and a context menu is open over it, showing options like 'Expand', 'End task', 'Resource values', 'Create dump file', 'Go to details', 'Open file location', 'Search online', and 'Properties'. The 'Performance' section shows the following resource usage:

Resource	Usage
CPU	4%
Memory	19%
Disk	0%
Network	0%
GPU	2%
GPU Engine	0%

The 'Processes' section shows the following processes:

Name	Status	CPU	Memory	Disk	Network	GPU	GPU Engine
WMI Provider Host	Running	0%	34.8 MB	0 MB/s	0 Mbps	0%	
WMI Provider Host	Running	0%	25.7 MB	0 MB/s	0 Mbps	0%	
WMI Provider Host (32 bit)	Running	0%	2.8 MB	0 MB/s	0 Mbps	0%	
Windows processes (93)							
Client Server Runtime Process	Running	0%	1.7 MB	0 MB/s	0 Mbps	0.1%	GPU 0 - 3D
Client Server Runtime Process	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%	
Console Window Host	Running	0%	4.8 MB	0 MB/s	0 Mbps	0%	
Console Window Host	Running	0%	4.8 MB	0 MB/s	0 Mbps	0%	
Console Window Host	Running	0%	5.1 MB	0 MB/s	0 Mbps	0%	
Console Window Host	Running	0%	5.3 MB	0 MB/s	0 Mbps	0%	
Console Window Host	Running	0%	5.0 MB	0 MB/s	0 Mbps	0%	
Desktop Window Manager	Running	0.3%	101.3 MB	0 MB/s	0 Mbps	0.1%	GPU 0 - 3D
HPZ12	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%	
HPZ12	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%	
Local Security Authority Process (lsass.exe)	Running	0%	8.4 MB	0 MB/s	0 Mbps	0%	
Registry	Running	0%	8.2 MB	0 MB/s	0 Mbps	0%	
Service Host: Application	Running	0%	1.4 MB	0 MB/s	0 Mbps	0%	
Service Host: AVCTP	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%	



# DEMO VID OF ATTACK & BLOCK





CREDENTIAL  
THEFT

# RISK: SYSTEM REGISTRY

**SAM registry hive/file: LM/NTLM hashes of local users;**

## What is the SAM File?

The Security Account Manager (SAM) is a database file in Microsoft Windows OS's that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory is used to authenticate remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.

During normal operation of a Windows system, the SAM database cannot be copied due to restrictions enforced by the operating system kernel. The SAM database is stored in two places within

Windows: `%systemroot%\system32\config\sam` is the location of the main storage for passwords and `%systemroot%\repair\sam._` is a backup of the main file in the event that recovery is required for a repair process.

# DEMO VID OF ATTACK & BLOCK



CREDENTIAL  
THEFT

## RISK: KNOWN FILE PATHS

### NTDS.dit file:

**Hashes of domain accounts, Domain Backup Key;**

**Offline** – grab SAM/SYSTEM/SECURITY/NTDS.dit from compromised host and process it using special tools.

**Online** – run special tool directly on compromised host (this tool will do all necessary work itself)

Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.



› This PC › Windows (C:) › Program Files (x86) › Common Files ›



# DEMO VID OF ATTACK & BLOCK



CREDENTIAL  
THEFT

# RISK:SESSION TOKENS



## Application

- End User Layer
- HTTP, FTP, IRC, SSH, DNS

## Presentation

- Syntax Layer
- SSL, SSH, IMAP, TFP, MPEG, JPEG

## Session

- Synch & send to port
- API's, Sockets, Winsock

## Transport

- End-to-end connections
- TCP, UDP

## Network

- Packets
- IP, ICMP, IPSec, IGMP

## Data Link

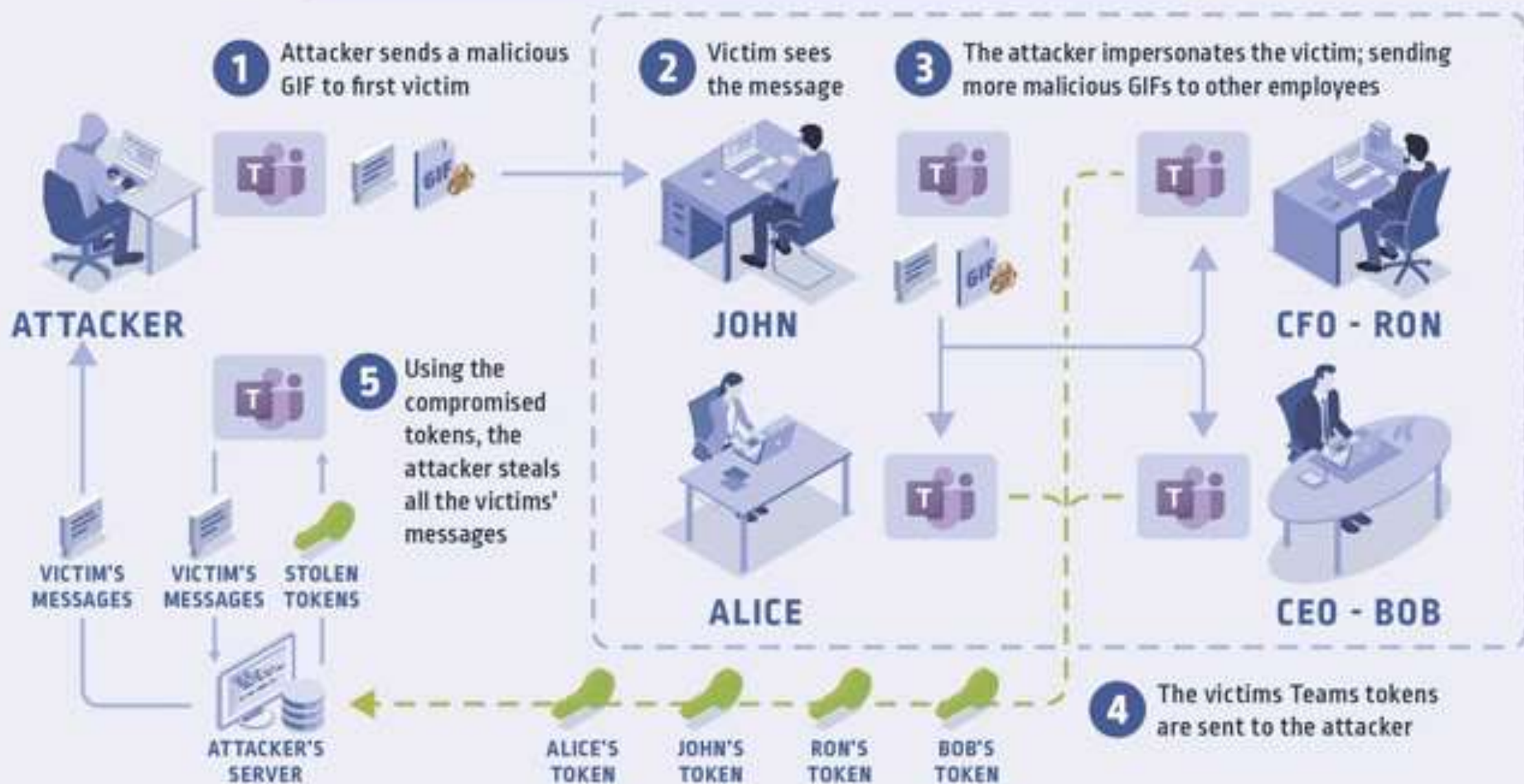
- Frames
- Ethernet, PPP, Switch, Bridge

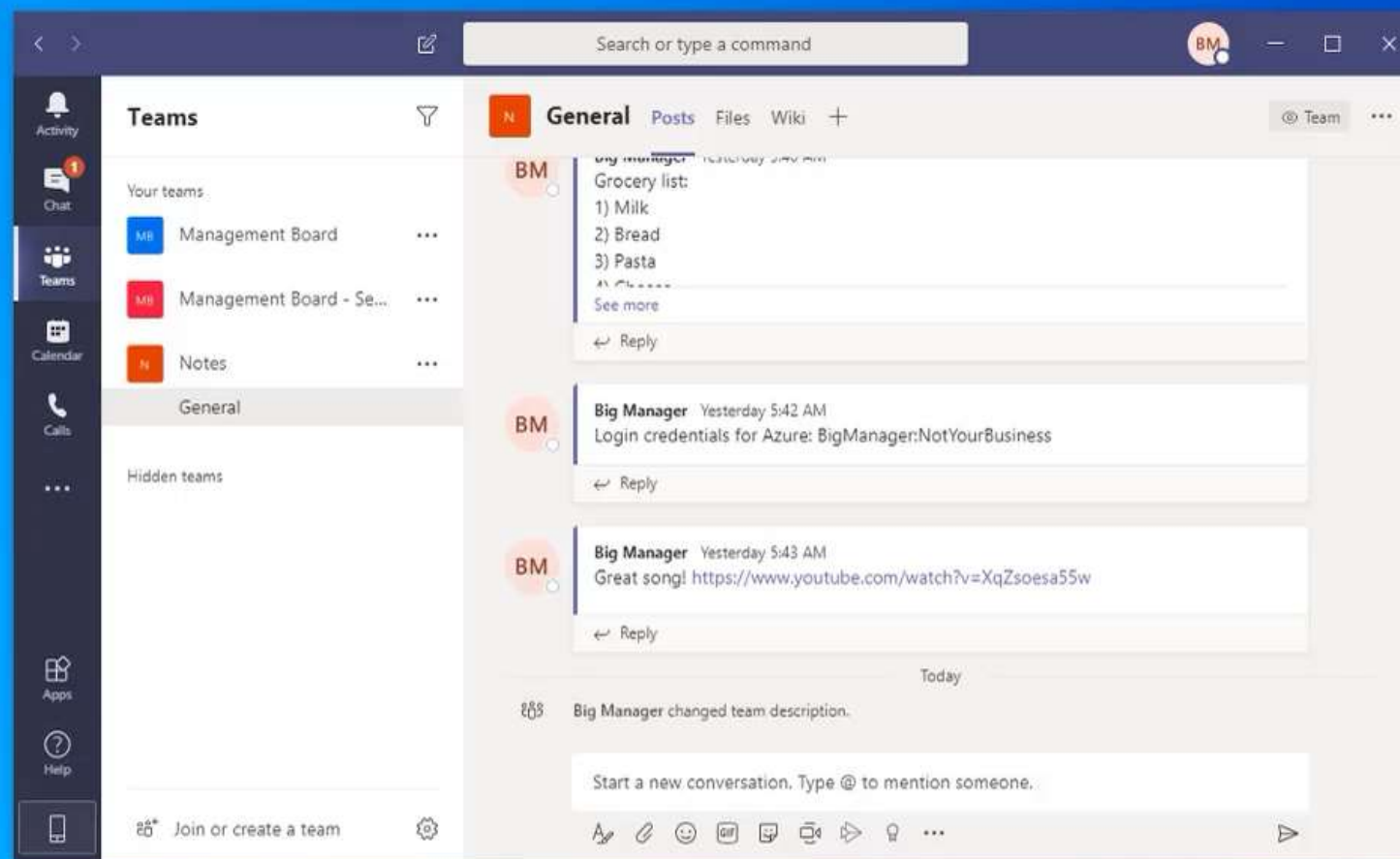
## Physical

- Physical Structure
- Coax, Fibre, Wireless, Hubs, Repeaters



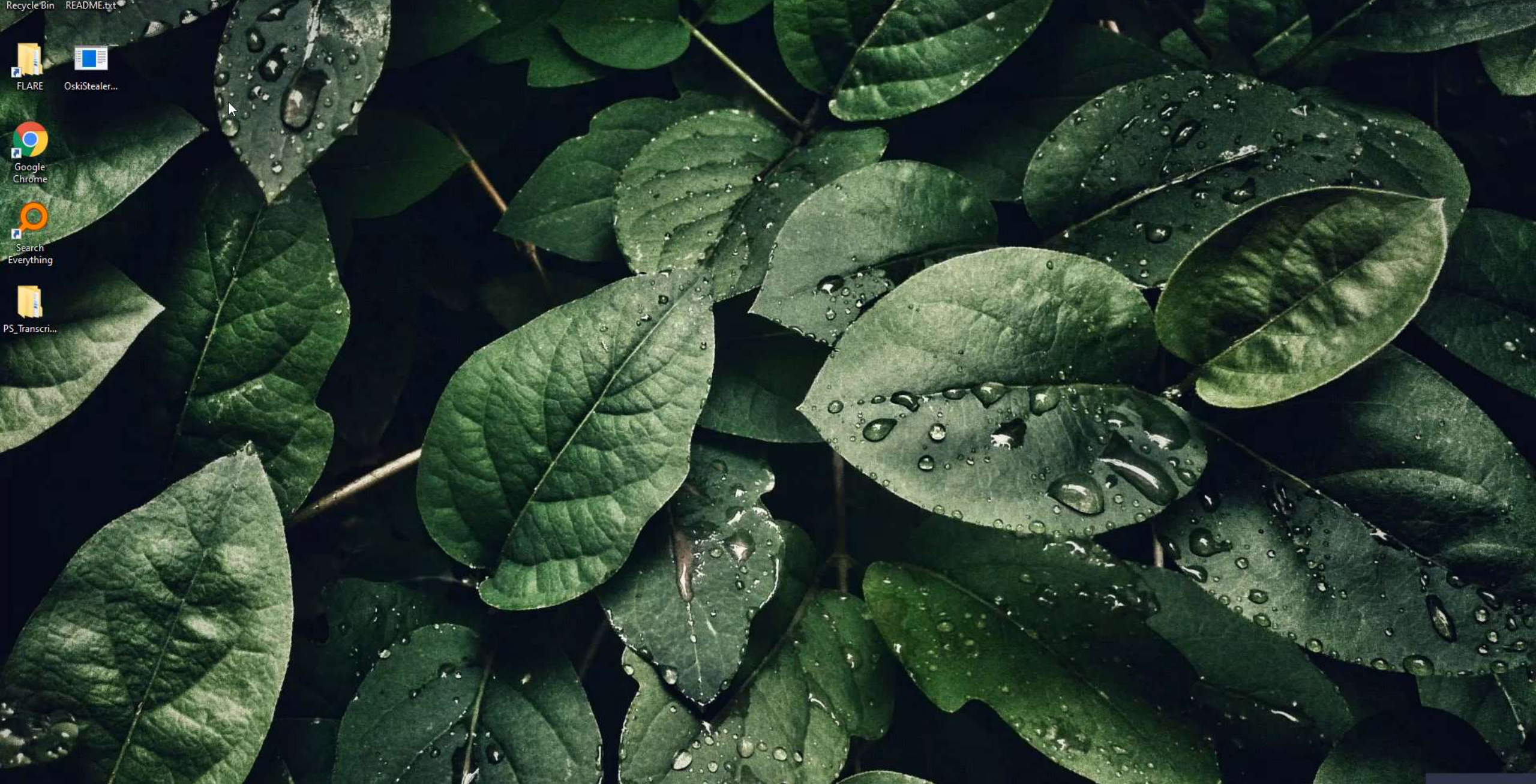
# MICROSOFT TEAMS ATTACK WORKFLOW





Victim's Screen





Recycle Bin

README.txt



FLARE



OskiStealer...



Google  
Chrome



Search  
Everything



PS\_Transcri...



Type here to search



30°C שמש



Victim



# PURCHASING STOLEN COOKIES

# WHY?

- Identity Theft
- Account Take-over
- Targeted Phishing
- Data Breaches
- Profit

# CASE STUDY: ELECTRONIC ARTS (EA)

- Began attack by purchasing Slack access for \$10.
- Tricked employee to reset MFA
- Exfil Data
  - 780GB stolen Source Code, SDK's and other proprietary tools.
    - FIFA 21 Source Code
    - Frostbyte Engine



## Genesis Wiki

**Genesis Store** - professional place that helps you to increase anonymity in World Wide Web.

Genesis Store specializing in selling:

- FingerPrints (FP),
- Cookies,
- Inject Scripts info,
- Form Grabbers (Logs),
- Saved Logins,
- Other personal data obtained from different devices in the WEB.

Each bot in the store may include all mentioned above info of partial.

To help you work with this information we have developed professional software:

**Genesis Security** - the proprietary plugin which can simplify your work with FingerPrints and Cookies of the bots (holders).

You may purchase all the necessary data on any bot (holder).












NB: we do not check the sources or the accounts, we provide the info «as it is».

Fingerprints may be obtained in 2 different ways:

- real FP scratched by bot from the user's Device,
- generated FP based on the data grabbed by bot on the user's Device.

To find usefull information how to use this service, you can look at following sections:

## Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
 221	+819	+6732	+28108	<a href="#">424654</a>
Grouped by 				
 US	+52	+641	+3061	<a href="#">13390</a>
 ES	+70	+559	+2265	<a href="#">34857</a>
 FR	+73	+536	+2227	<a href="#">40666</a>
 IT	+89	+585	+2202	<a href="#">57045</a>
 RO	+88	+564	+2086	<a href="#">22700</a>
 AR	+53	+482	+1901	<a href="#">17252</a>
 PL	+47	+464	+1684	<a href="#">19126</a>
 HU	+45	+426	+1559	<a href="#">13062</a>
 CL	+35	+372	+1429	10335

## Bots

Extended Search

☐ Enabled☒ Resource name / URL ☐ Without Resources

Resources total

paypal,ebay,hotmail.com...

min

max

\$ Price

mix

max

☒ FormParser☒ SavedLogins☒ InjectScript☐ Only Sale

Bot Name

Bot name

Bot OS

Win

Fingerprints (browsers)

min

max

Date Install

from yyyy-mm-dd

Last Update

from yyyy-mm-dd

Bot Country

Any country

IP

95.123

to yyyy-mm-dd

to yyyy-mm-dd

Reset all

Reset

Search

BOT NAME/

RESOURCES KNOWN / OTHER

COUNTRY / HOST

PRICE

Filter bot name

Any

Filter resource name/domain: paypal,ebay.com,hotmail.com...

US

Filter \$

[258498755B44CAF0CD64FA768CE149A5](#)

2021-06-27 02:59:07

2021-06-27 19:08:44

Instagram  
Servus  
Tumblr  
Office365  
EtsyStoreNetflix  
ShutterflyStore  
Live  
Amazon  
EANetworkGoogle  
Twitter  
Steam  
WishStore  
Indig...

64 64 = 64

US  
46.244...  
Windows 10 Home

59.00



wifiguest.ecsd.net

account.mycommerc...

...known 28  
...other 36[B3371B2079C2DF4819CDE7D3FD432CF6](#)

2021-02-26 08:35:28

2021-02-28 08:29:15

Alibaba  
126com  
AppleStore  
NetflixFacebook  
LinkedIn  
iCloudGCKeyCanada  
Twitter  
PayPal

57 57 = 57

US  
104.233...  
Windows 10  
Codename 19H2  
Insider Preview

57.00



## 937F534FCFE2384B8E251C7A6F5ACA40

Country  
Resources  
Browsers  
Installed  
Updated  
Ip  
Os  
Price Usd




US  
77  
2  
2021-09-02 16:24:44  
2021-09-02 17:45:11  
76.189...  
Windows 10 Home  
24.00

Browsers for Genesis Security:  

Last update info: 2021-09-02 17:45:11

937F534FCFE2384B8E251C7A6F5ACA40

 edge  
Cookies 31 (2021-09-02 17:43:13)  
 chrome  
Cookies 1556 (2021-09-02 17:43:13)

Resources: 77 =  0  77  0

Know resources: 18

 Google	3	 Steam	3	 Airdroid	2	 Box	1	 Facebook	1	 Live	1
 MEGAnz	1	 WishStore	1	 Office365	1	 Dropbox	1	 Points2shop	1	 Bankmobil...	1
 Vimeo	1										

Other resources: 59

 www.asecampus.com	2	 www.wizard101.com	2	 stark.mywconline.com	2	 plarium.com	1
 watchseries.cr	1	 forums.nexusmods.com	1	 popplet.com	1	 poster.gamesprite.me	1
 www.explorelearning.com	1	 accounts.nintendo.com	1	 www.sidereel.com	1	 manage.airpush.com	1
 www.coolflashcards.com	1	 www.nexusmods.com	1	 login.cengagebrain.com	1	 starkstate.emsicc.com	1
 www.pandora.com	1	 sep.snapon.com	1	 login3.id.hp.com	1	 my.scloud.live	1
 bankmobilevibe.com	1	 www.darkness-realm.com	1	 www.filmlush.com	1	 accounts.fitbit.com	1
 tubitv.com	1	 www.getrave.com	1	 bethesda.net	1	 www.supertracker.usda.gov	1
 ssc-cas2.starkstate.edu	1	 ssc-cas1.starkstate.edu	1	 sso.pokemon.com	1	 www.romulation.net	1...

Last update Saved Logins: 2021-09-02 16:48:52

Last update Form Parser: 1970-01-01 00:00:00

Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL

[SOURCE](#)

[DATASETS](#)

[BROWSER](#)

[KNOWN](#)

[GRABBED / UPDATED](#)



## C401B4177825109E5F8150FF882AEEEE

Add to Cart

Reserve

Buy

Country	US
Resources	19
Browsers	2
Installed	2021-08-27 18:25:54
Updated	2021-09-02 16:08:51
Ip	71.191...
Os	Windows 10 Home
Price Usd	17.00

1 fingerprints

Browsers for Genesis Security:

Last update info: 2021-09-02 16:08:51

## C401B4177825109E5F8150FF882AEEEE

edge

Cookies 408 (2021-08-27 18:56:18)

chrome

Cookies 47 (2021-08-27 18:56:18)

Configs 1:

Version **Chrome 92** (Chrome 92.0.4515.159)

Config Update 2021-09-02 14:58:16

User Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36

IP 66.176...

Resources: 19 = 1 18 0

Know resources: 11

Live

4

Amazon

2

Google

2

Netflix

1

Alibaba

1

Facebook

1

Other resources: 8

evoload.io

1

www.encuentra24.com

1

mls.foreclosure.com

1

learn.canvas.net

1

www.puntosreales.com

1

puntosreales.com

1

id.tigo.com

1

micuenta.tigo.com.ni

1

Last update Saved Logins: 2021-08-27 19:06:55

Last update Form Parser: 2021-08-30 07:34:10

Last update Inject Script: 1970-01-01 00:00:00