



# No Cookies for You

Attacking and Defending Credentials in Chromium Browsers

**RSA**  
Conference™  
2023

**San Francisco**

April 24 – 27  
Moscone Center

# whoami - Andy Thompson



CYBERARK \ LABS

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



- LinkedIn: [in/andythompsoninfosec](https://www.linkedin.com/in/andythompsoninfosec)
- GitHub: [github.com/binarywasp](https://github.com/binarywasp)
- Twitter: [@Andy\\_Thompson](https://twitter.com/Andy_Thompson)
- Mastodon: [@Andy\\_Thompson@infosec.exchange](https://mastodon.social/@Andy_Thompson@infosec.exchange)
- Email: [Andy.Thompson@CyberArk.com](mailto:Andy.Thompson@CyberArk.com)







# CYBERARK \ LABS

- Vulnerability research
- Malware research
- Pentesting projects
- Publications
- Product enhancements
- Tools
- Sessions
- Patents
- Innovation projects



# What Are Secrets?

- Passwords (duh)
- Cookies
- Stored data
  - Credit card info
  - Stored addresses
  - Etc.

## New Emotet Variant Stealing Users' Credit Card Information from Google Chrome

📅 June 08, 2022 👤 Ravie Lakshmanan





---

# Where Are the Secrets?

- Keyed-in Data
- Intercepted Communications
- On Disk
- In Memory
- Information Delivered by the Browser  
(if you ask nicely)





# Keylogging



# Keylogging

## Recording secrets: one keystroke at a time.

### Hardware



### Software

- Real Free Keylogger ([link here](#))
- Basic-Windows-keylogger ([GitHub here](#), [blog here](#))
- EVERY C2 out there (Cobalt Strike, Metasploit, PowerShell Empire, Brute Ratel, etc.)

### TikTok's in-app browser could be keylogging, privacy analysis warns

Natasha Lomas @riptari / 5:36 AM CDT • August 19, 2022

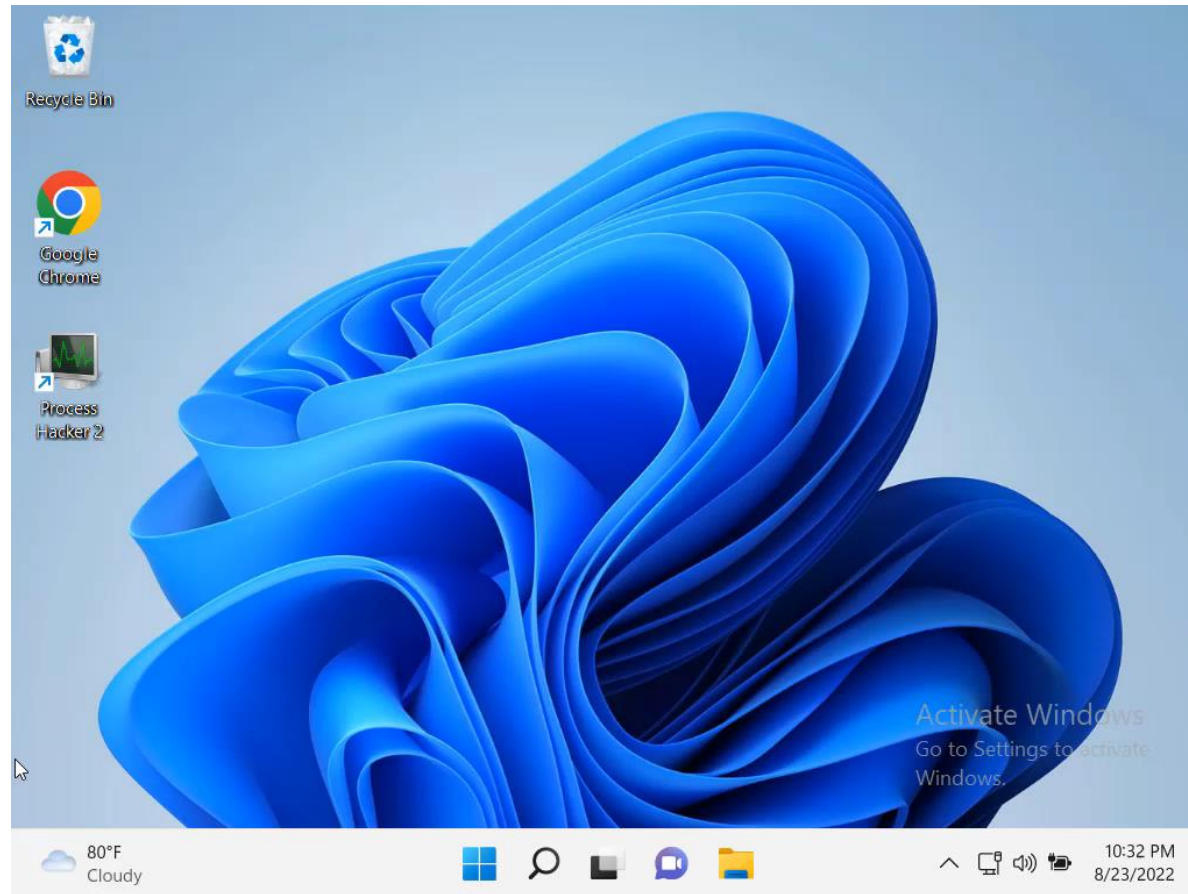
[Comment](#)





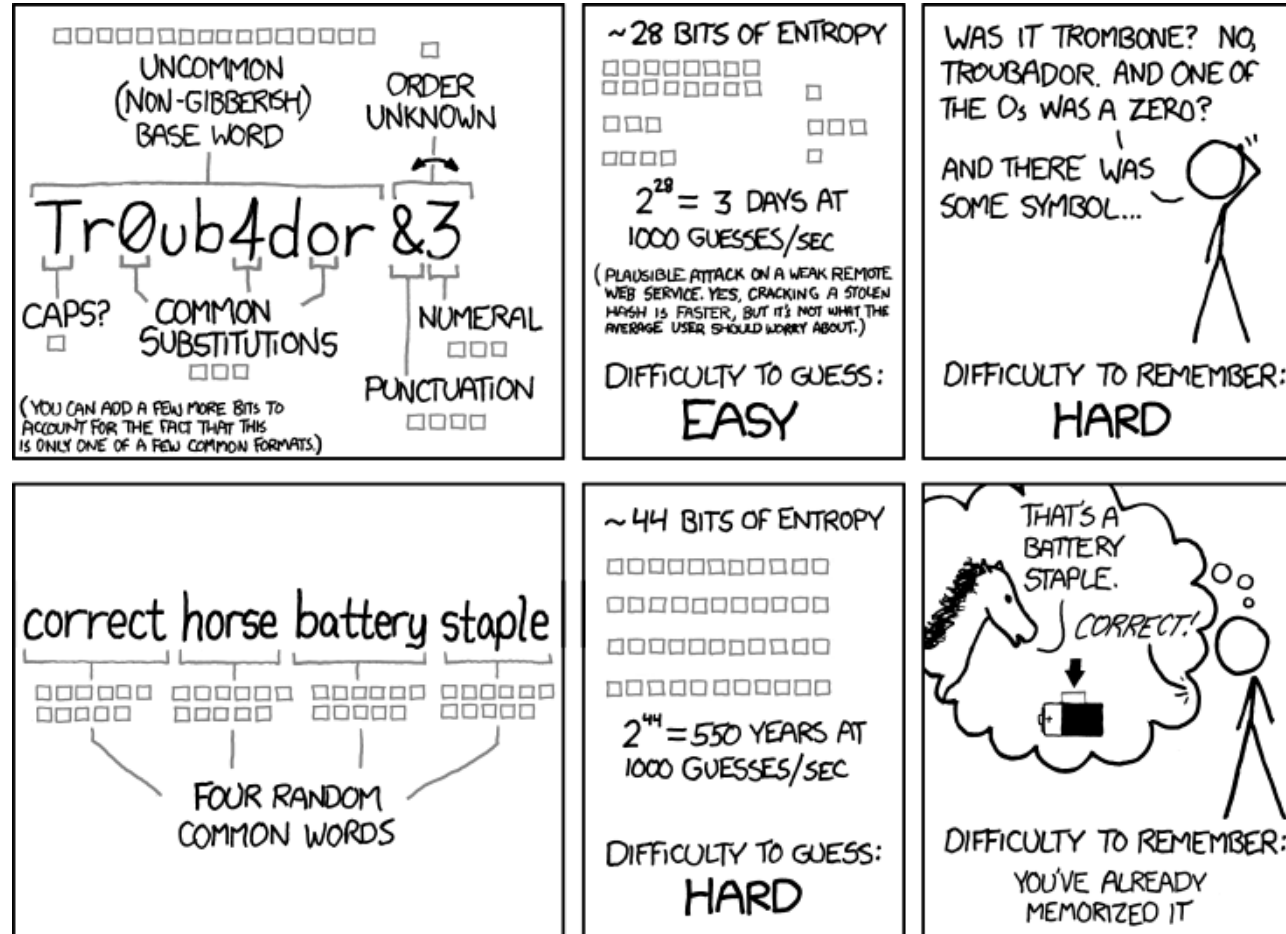
# Demo

Basic-Windows-keylogger (GitHub [here](#), blog [here](#))





# XKCD — Password Strength



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



---

# Mitigation

- Keylogging is a broad general issue that is not specific to browsers, and there are various commercial anti-keylogging products available.
  - Ghostpress [[Link here](#)]
  - KL-Detector [[Link here](#)]
- Password managers



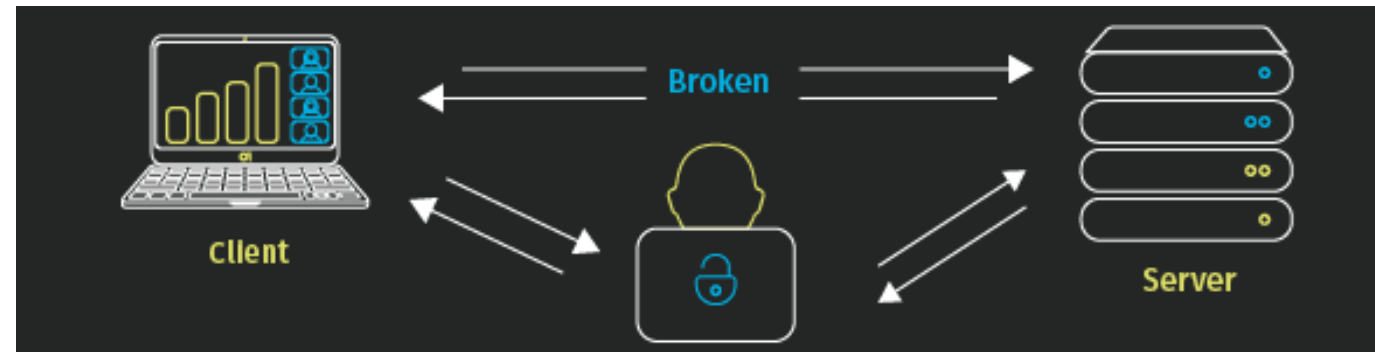
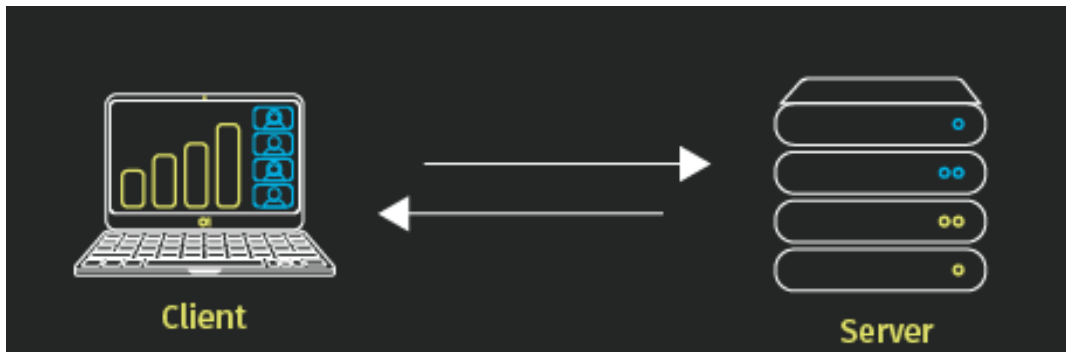


# ○ In-line Attacks



# In-line Attack (MITRE T1539, MITRE T1557)


- “This issue is out of the scope of this presentation and is included in this list of attack vectors on browsers for the sake of completeness.”
- An in-line attack on the connection between the browser and the server of a web application can capture clear-text passwords and cookies (with “tokens”) if the communication is not secured (HTTP and not HTTPS).





# Examples


- Evilginx 2 [GitHub [here](#)] [Blog [here](#)]
- EvilProxy
- MITMF [Link [here](#)]
- Social Engineering Toolkit (SET) [Link [here](#)]


 **Jeremy Kirk**  
@Jeremy\_Kirk

Bypassing MFA at a big scale may be possible with "EvilProxy" a cybercriminal service discovered by @RESecurity. It uses a reverse proxy to nab session cookies, a technique that's been used before but now is wrapped in a slick phishing kit. Yikes. #infosec [databreachtoday.com/cybercriminal-...](https://databreachtoday.com/cybercriminal-...)

[EvilProxy] Phishing as a Service / Фишинг как услуга  
by evilproxy · Monday July 4, 2022 at 09:48 AM

July 4, 2022, 09:48 AM (This post was last modified: July 12, 2022, 07:03 AM by evilproxy.)

 **evilproxy**



GOD User

Reverse proxy  
Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

Мы можем помочь вам повысить устойчивость к фишинговым атакам. Мы поддерживаем безопасность для всех сотрудников организации. Наши симуляции фишинга поддерживаются программной платформой, полным набором функций, необходимых для проведения фишинговых кампаний. Получите демоверсию совершенно бесплатно на 1 день!

We can help you improve your resilience against phishing attacks. Phish! Our phishing simulations are supported by an in-house developed software to conduct phishing campaigns: [Get a demo completely free 1 day!](#)

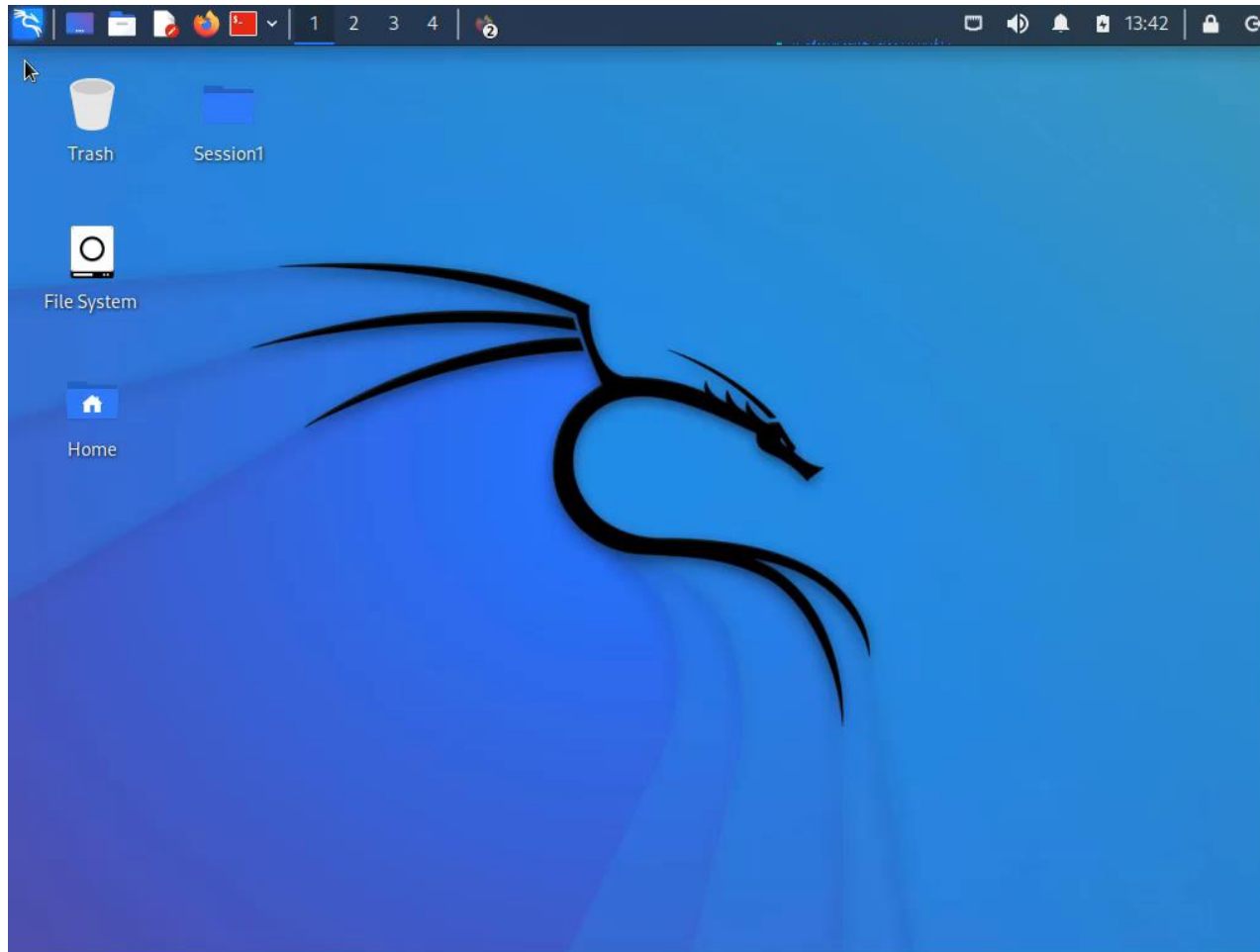
+ Services:

- google.com 10/20/31 days = 250/450/600\$ (Click!)
- microsoft 10/20/31 days = 150/250/400\$ (Hotmail, CORP, Remote)
- icloud.com 10/20/31 days = 150/250/400\$ (auto token/cookies ref)
- dropbox.com 10/20/31 days = 150/250/400\$ (also sign in with goo)
- github.com 10/20/31 days = 150/250/400\$
- linkedin 10/20/31 days = 150/250/400\$

5:34 AM · Sep 5, 2022 · Twitter Web App



# Demo: Social Engineering Toolkit





# Mitigation

- Encryption
  - TLS/SSL
  - VPN
- End User Awareness



# ○ Secrets on Disk







# Secrets Stored on Disk

- Stored by Chromium in disk files using DPAPI encryption
  - Cached logon credentials used as decryption key

AppData\Local\Google\Chrome\User Data\Default>Login Data

MITRE T1555/003

<https://attack.mitre.org/techniques/T1555/003/>



# Examples

- ChromePass [Link [here](#)]
- LaZagne [Link [here](#)]
- HackChrome [Link [here](#)]



# DEMO TIME

C:\> Command Prompt

```
C:\temp>
```





# Mitigation

Block unauthorized processes from accessing sensitive browser files.

```
AppData\Local\Google\Chrome\User Data\Default>Login Data  
“?:\Users\*\AppData\Local\Google\Chrome\User Data\*\Login  
Data”
```

- Direct READ access (i.e., copy operation)
- File or path rename operation  
(which might take the file out of the scope defined above)
- Zipping or archiving by any standard program  
(i.e., tar.exe should not be authorized to access this file)

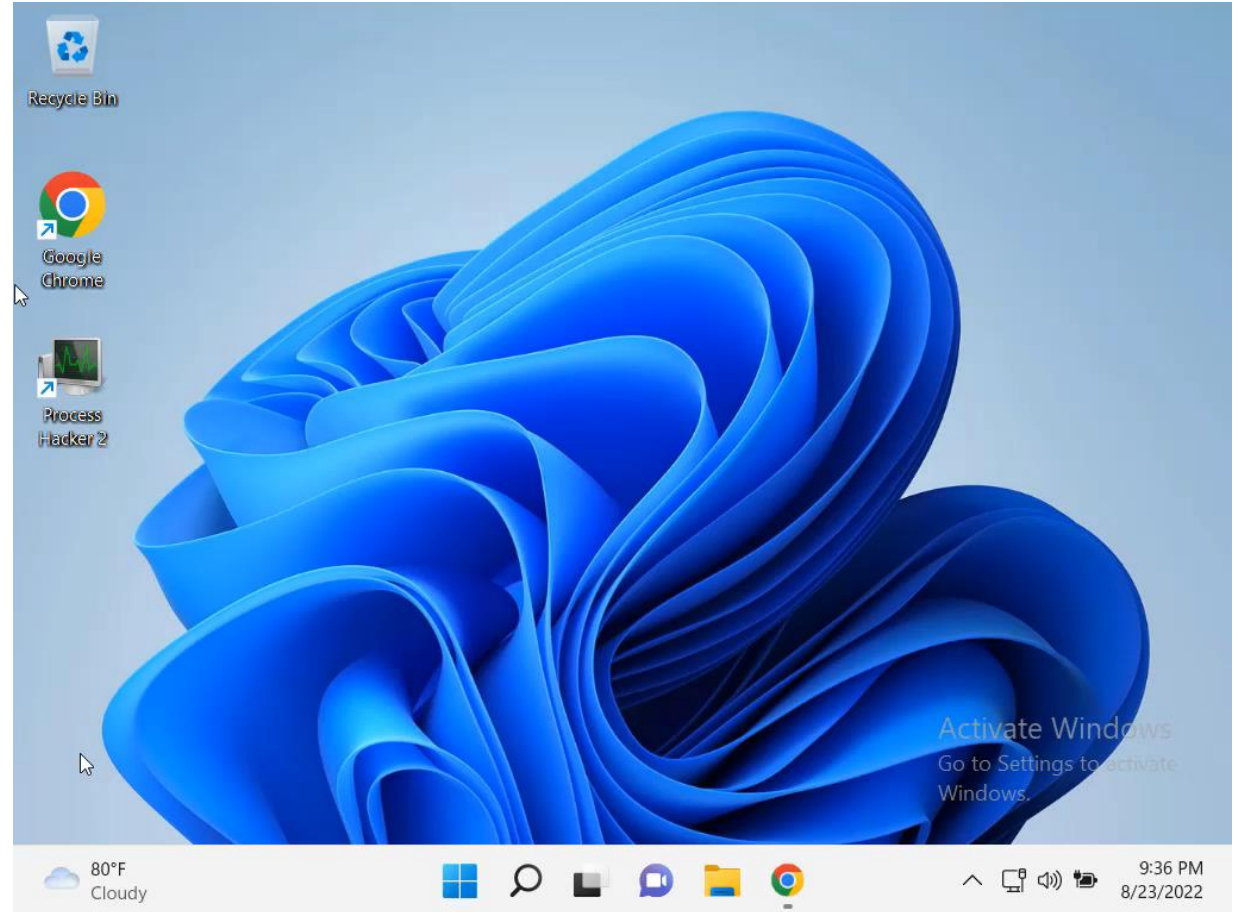


# ○ Secrets in Memory





# Cleartext Secrets in Unprotected Memory





---

# Secrets in Memory

- Access browser from an external process.
- Create a browser process.
- Dump the memory of the browser process.

MITRE T1555/003

<https://attack.mitre.org/techniques/T1555/003/>



# Example

mimikittenz [GitHub [here](#)]

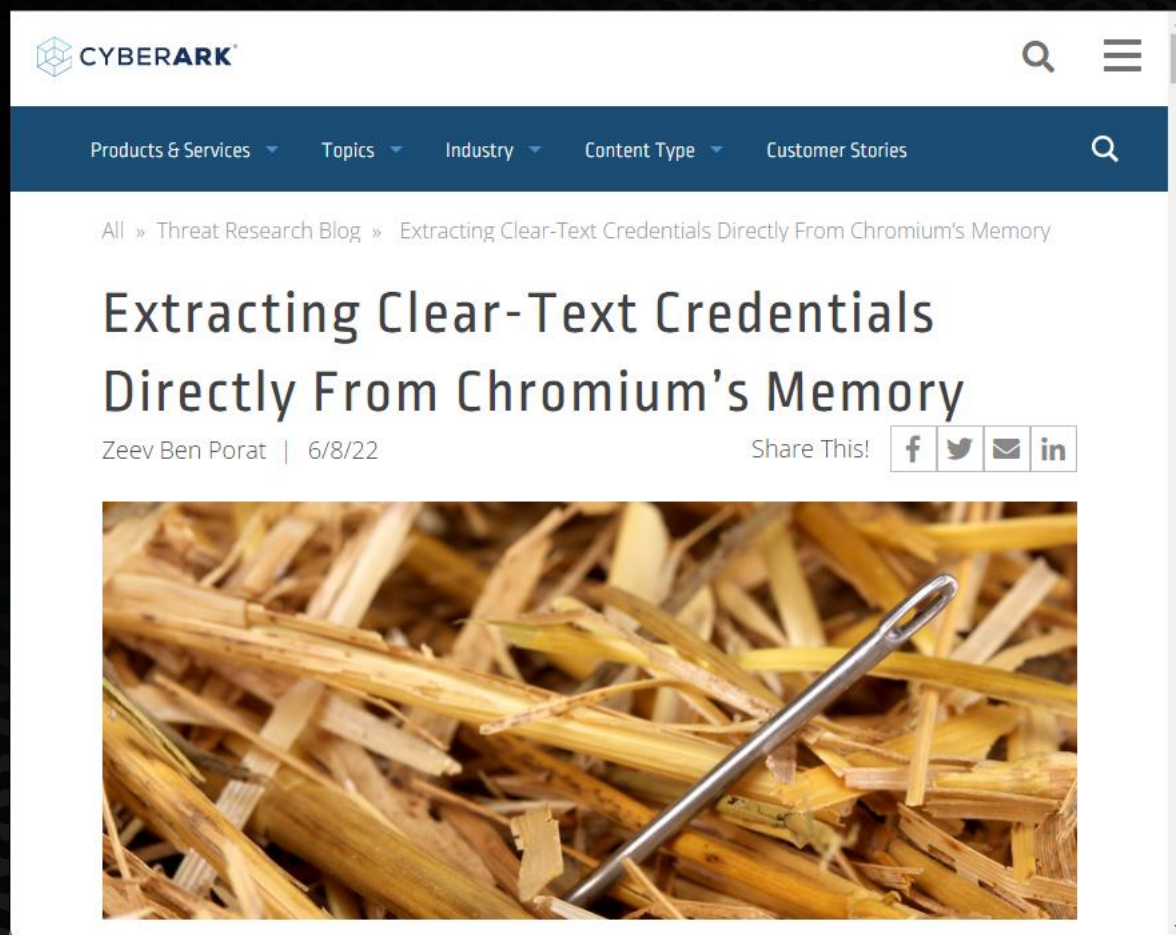
```
Windows PowerShell
PS C:\Users\Thomass> Invoke-mimikittenz

mimikittenz-1.0-alpha
CAN I HAZ WAM?
jamieson@dringensec.com

PatternName      PatternMatch
-----
Dropbox          login_email=papalupal%40paypal.com&login_password=cro0ducile%40&
Slack            &crumb=-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=on ...
Slack            &crumb=-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=onon ...
Slack            &crumb=-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=on7...
Slack            &crumb=-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=on7...
Xero             fragment=&userName=tfntrader%40ato.com&password=wherethetfns%40&__RequestVerificationToken=
Xero             fragment=&userName=tfntrader%40ato.com&password=wherethetfns%40&__RequestVerificationToken=
awsWebServices  &email=awsadmin%40test.com&create=0&password=gizmedeseawskeysbr0&metadata1=
Jira             username=jira%40test.com&password=testjira028%40&rememberMe=
Gmail            &Email=putterpanda%40gmail.com&Passwd=putterpandaAPTchall&PersistentCookie=
Dropbox          login_email=droppingboxes%40trustyemail.com&login_password=testerouspasserous2&
Gmail            &Email=putterpanda@gmail.com&Passwd=putterpandaAPTchall&PersistentCookie=
Jira             username=jira@test.com&password=testjira028&rememberMe=
Jira             username=jira@test.com&password=testjira28&rememberMe=

PS C:\Users\Thomass>
```



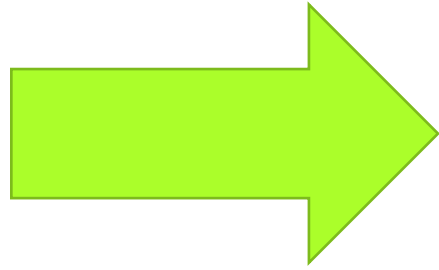


**Labs.CyberArk.com**





# DEMO TIME



# Chrome Password Manager Dump

- Forces the password manager to load all passwords into the memory.
- Extracts passwords (and associated usernames and URLs) from the memory.

```
Command Prompt - Local Administrator Authentication... Windows 10 20H2 OS 4
C:\Users\VC2>whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeShutdownPrivilege Shut down the system       Disabled
SeChangeNotifyPrivilege Bypass traverse checking    Enabled
SeUndockPrivilege    Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege  Change the time zone       Disabled

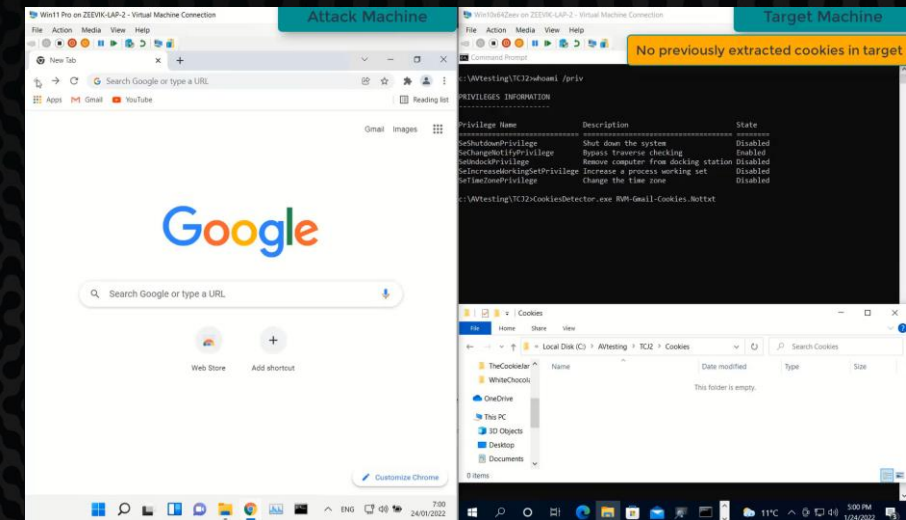
C:\Users\VC2>
C:\Users\VC2>
C:\Users\VC2>
C:\Users\VC2>LoginDataExtractor.exe AutoRunChrome+
```





# Gmail Session Hijack

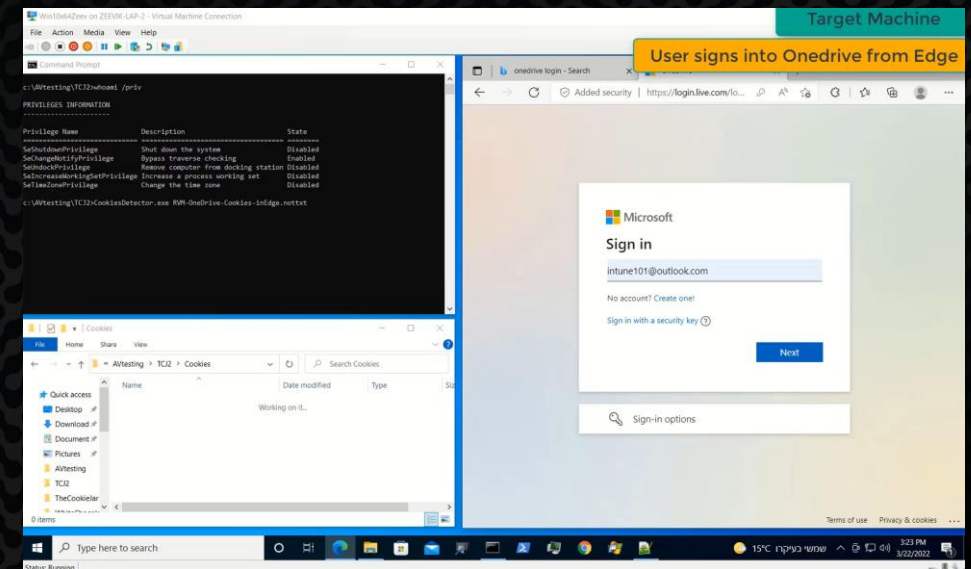
- Wait for user to start a Gmail session.
- Extract session cookies from memory.
- Activate “same” session on a remote computer.





# OneDrive Session Hijack (from Edge)

- Wait for user to start a OneDrive session.
- Extract session cookies from memory.
- Encode cookies for Cookie Manager.
- Activate “same” session on remote computer.



## 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	<a href="#">10335</a>
 NP	+28	+265	+1245	9950





## Bots

Extended Search

☐ Enabled ☒ Resource name / URL ☐ Without Resources **Resources total** min max **\$ Price** mix max

paypal,ebay,hotmail.com...

☒ FormParser ☒ SavedLogins ☒ InjectScript ☐ Only Sale

**Bot Name** Bot name **Bot OS** Win **Fingerprints (browsers)** min max

**Date Install** from yyyy-mm-dd to yyyy-mm-dd **Last Update** from yyyy-mm-dd to yyyy-mm-dd **Bot Country** Any country **IP** 95.123

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
<a href="#">258498755844CAF0CD64FA768CE149A5</a>	<div><div> Instagram</div><div> Tumblr</div><div> Office365</div><div> EtsyStore</div><div> wifiguest.ecsd.net</div></div> <div><div> Netflix</div><div> ShutterflyStore</div><div> Live</div><div> Amazon</div><div> EANetwork</div></div> <div><div> Google</div><div> Twitter</div><div> Steam</div><div> WishStore</div><div> Indig...</div></div>	US	59.00
<a href="#">B3371B2079C2DF4819CDE7D3FD432CF6</a>	<div><div> Alibaba</div><div> 126com</div><div> AppleStore</div><div> Netflix</div></div> <div><div> Facebook</div><div> LinkedIn</div><div> iCloud</div></div> <div><div> GCKeyCanada</div><div> Twitter</div><div> PayPal</div></div>	US	57.00

- News21
- Bots400k+
- Generate FP
- Orders
- Purchases
- Payments
- Tickets
- Software6.3|19.0
- Profile
- Invites
- Logout

937F534FCFE2384B8E251C7A6F5ACA40

Country	US
Resources	77
Browsers	2
Installed	2021-09-02 16:24:44
Updated	2021-09-02 17:45:11
Ip	76.189...
Os	Windows 10 Home
Price Usd	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
MEGAnz	1	WishStore	1	Office365	1	Dropbox	1	Points2shop	1
Vimeo	1							Live	1
								Bankmobil...	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

1 Live

4

1 Amazon

2

1 Google

2

1 Netflix

1

1 Alibaba

1

1 Facebook

1

Other resources: 8

1 evoload.io

1

1 www.encuentra24.com

1

1 mls.foreclosure.com

1

1 learn.canvas.net

1

1 www.puntosreales.com

1

1 puntosreales.com

1

1 id.tigo.com

1

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





# THIS WEBSITE HAS BEEN SEIZED



## OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

Been active on Genesis Market? In contact with Genesis Market administrators?  
Email us, we're interested: [FBIMW-Genesis@fbi.gov](mailto:FBIMW-Genesis@fbi.gov)



AFP



GUARDIA CIVIL



**NCA**  
National Crime Agency



**EUROPOL**

**EUROJUST**

**POLIISI**  
KESKUSRIKOSPOLIISI  
Centralkriminalpolisen  
National Bureau of Investigation  
**POLITIE**



**Polisen**  
Swedish Police





---

# Mitigation

Block unauthorized processes from accessing browser's memory.

- Only binaries signed by the developer (i.e., Google)
- Only binaries where OriginalFileName = "chrome.exe"





# Ask the Browser Nicely

(Command Line Arguments)





# Command Line Arguments

In 2018, “Alex” (@mangopdf) published a method to activate the browser with a command line parameter (`--remote-debugging-port`) that lets you ask the browser “nicely” to give you all its cookies.

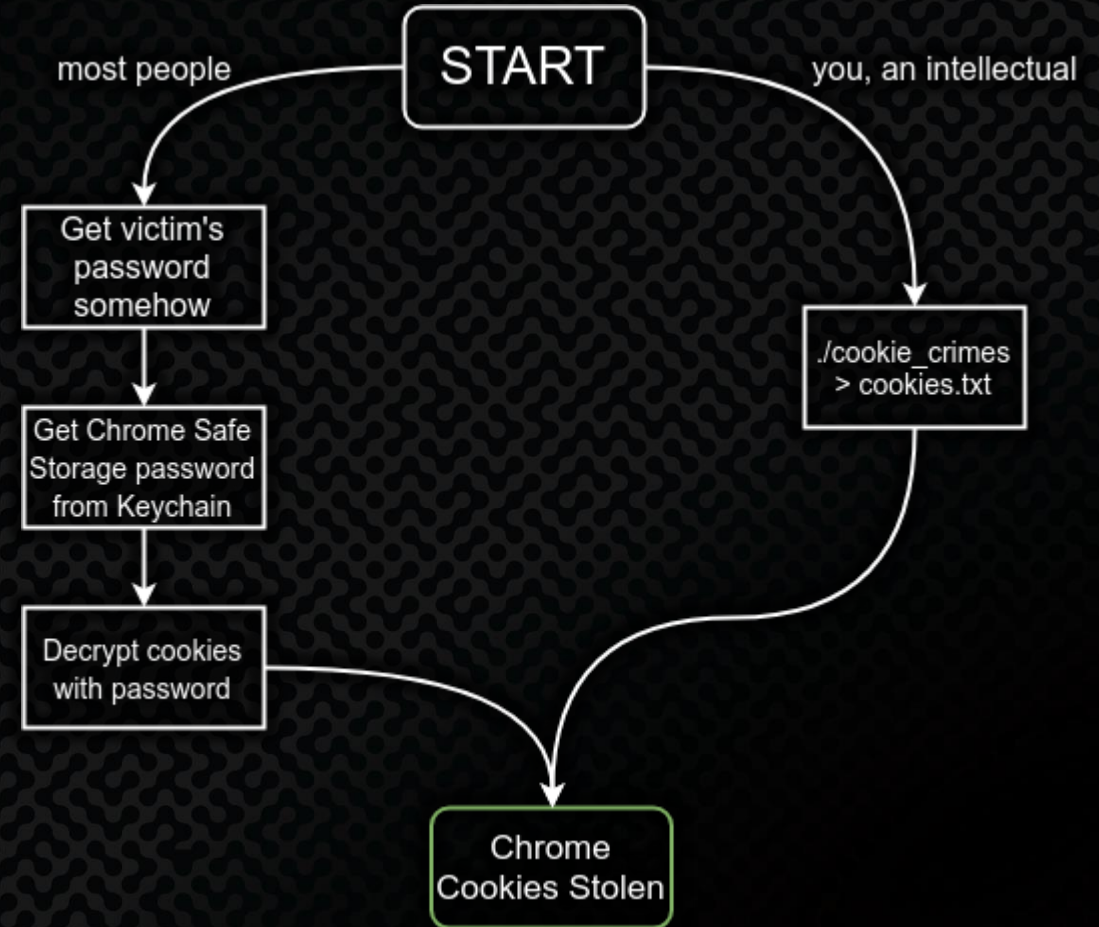


<https://www.youtube.com/watch?v=BWAetsJqey0>



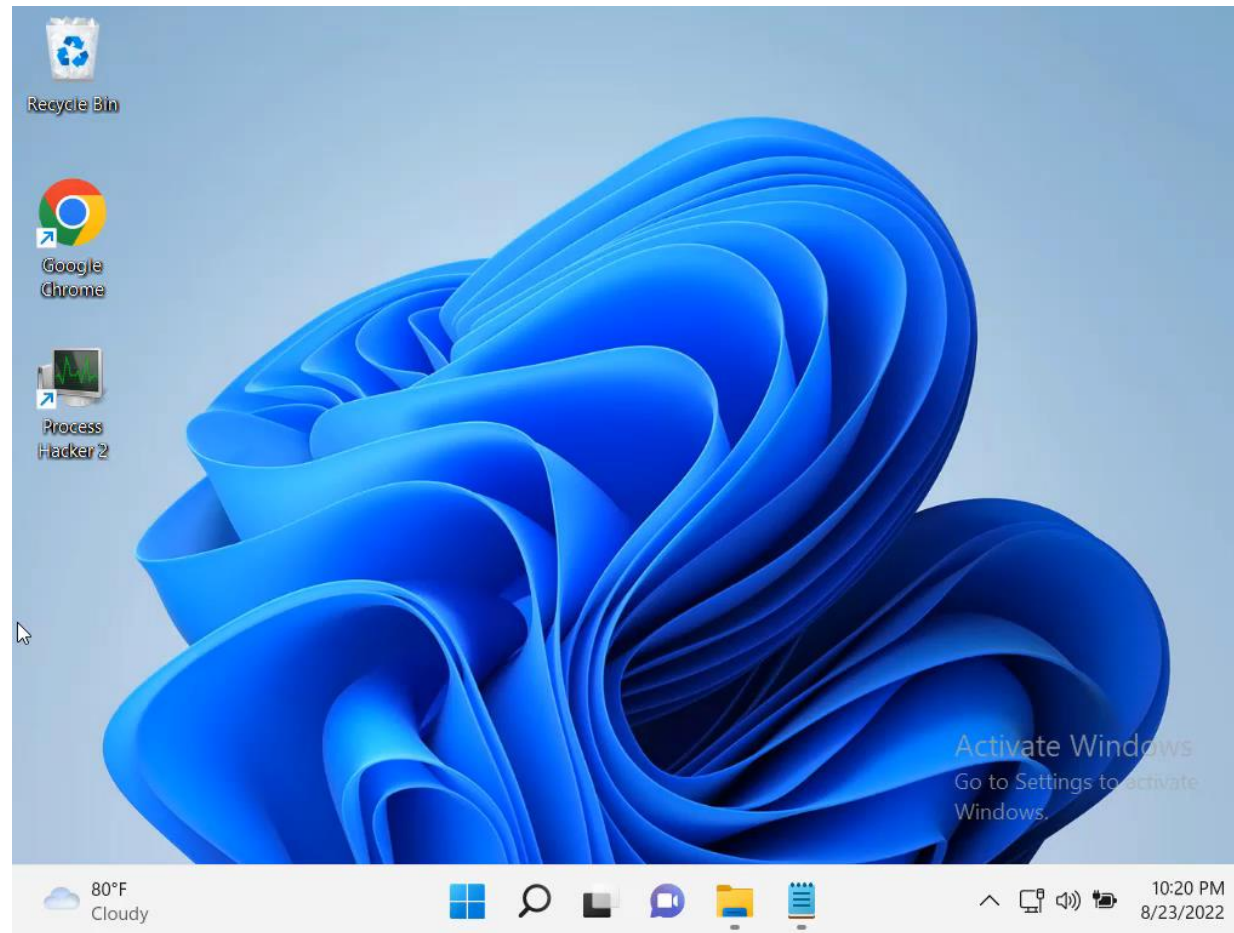
# Example: Cookie Crimes

[GitHub [here](#)] ["Alex"'s blog [here](#)]





# Demo: Cookie Crimes





# Mitigation

Block unauthorized processes from creating a browser with “dangerous” command line arguments.

- `--remote-debugging-port`
  - Track all browser debugging ports that are currently open.
  - Allow only specific applications (e.g., ChromeDriver.exe) to connect to these ports.
- `--remote-debugging-pipe`
- `-- headless`



---

# Summary of Secrets

- Keyed-in Data
- Intercepted Communications
- On Disk
- In Memory
- Information Delivered by the Browser  
(if you ask nicely)







# Mitigation Summary

- Deny any access to sensitive files.
- Deny any access to browser's virtual machine (VM).
- Prevent unauthorized processes from creating the browser process.
- Block suspicious command line options when browser is created.





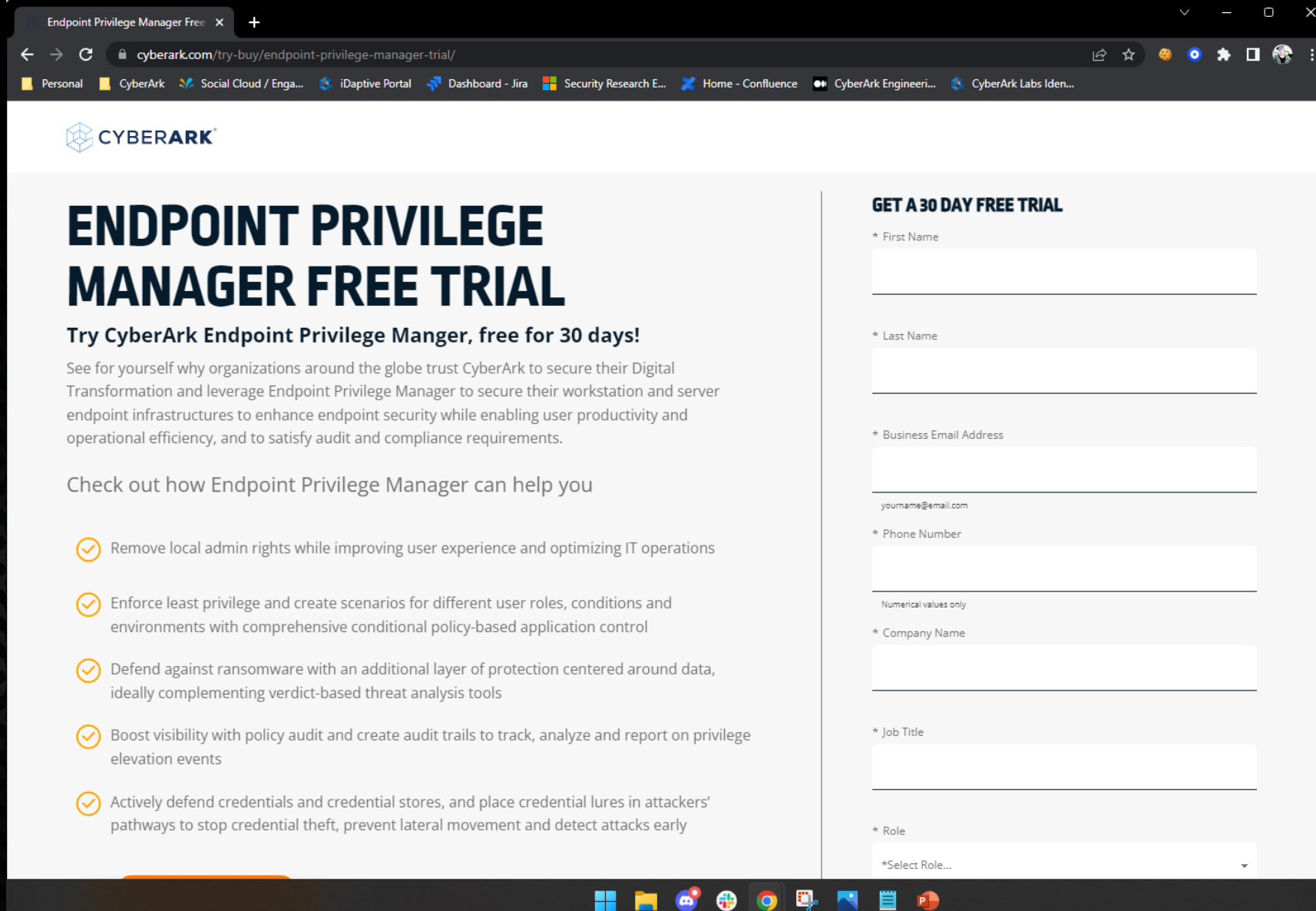
# The Tip of the Iceberg...



- System processes
- Registry keys
- Memory
- File locations
- And more!



# o CyberArk EPM Free Trial



The screenshot shows a web browser window with the URL `cyberark.com/try-buy/endpoint-privilege-manager-trial/`. The page features the CyberArk logo at the top left. The main heading is "ENDPOINT PRIVILEGE MANAGER FREE TRIAL". Below this, a subheading reads "Try CyberArk Endpoint Privilege Manger, free for 30 days!". A paragraph of text explains the benefits of the trial. To the right, a section titled "GET A 30 DAY FREE TRIAL" contains a registration form with fields for First Name, Last Name, Business Email Address, Phone Number, Company Name, Job Title, and Role. A list of five benefits is provided on the left side of the form.

**ENDPOINT PRIVILEGE MANAGER FREE TRIAL**

**Try CyberArk Endpoint Privilege Manger, free for 30 days!**

See for yourself why organizations around the globe trust CyberArk to secure their Digital Transformation and leverage Endpoint Privilege Manager to secure their workstation and server endpoint infrastructures to enhance endpoint security while enabling user productivity and operational efficiency, and to satisfy audit and compliance requirements.

Check out how Endpoint Privilege Manager can help you

- ✓ Remove local admin rights while improving user experience and optimizing IT operations
- ✓ Enforce least privilege and create scenarios for different user roles, conditions and environments with comprehensive conditional policy-based application control
- ✓ Defend against ransomware with an additional layer of protection centered around data, ideally complementing verdict-based threat analysis tools
- ✓ Boost visibility with policy audit and create audit trails to track, analyze and report on privilege elevation events
- ✓ Actively defend credentials and credential stores, and place credential lures in attackers' pathways to stop credential theft, prevent lateral movement and detect attacks early

**GET A 30 DAY FREE TRIAL**

\* First Name

\* Last Name

\* Business Email Address   
yourname@email.com

\* Phone Number   
Numerical values only

\* Company Name

\* Job Title

\* Role   
\*Select Role...





Thank you!

