CYBERARK \ LABS

Big Browser

Attacking & Defending the Process that Knows Everything.

whoami - Andy Thompson

CYBERARK \ LABS

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

Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr
- Email: rainmaker@MeteorMusic.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

https://thehackernews.com/2022/06/new-emotet-variant-stealing-users.html

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

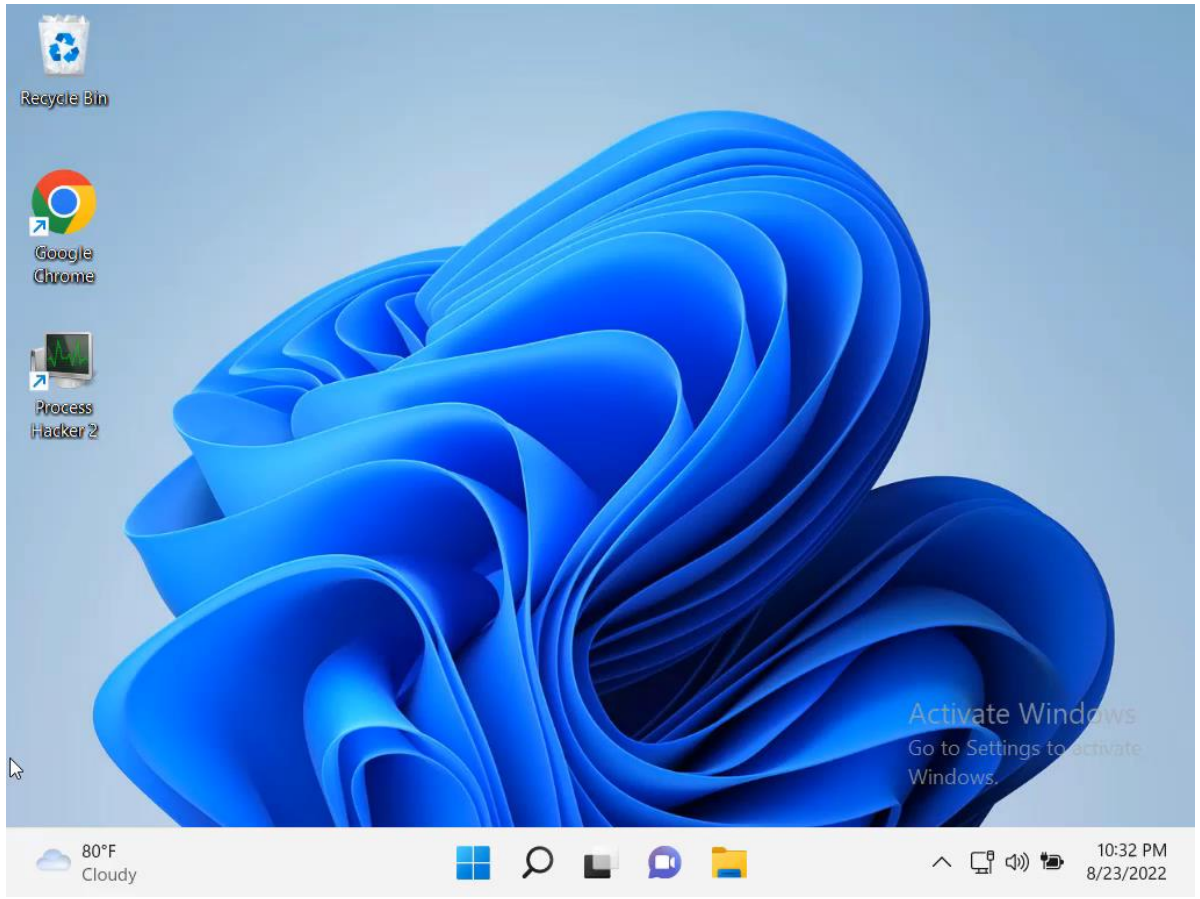
  (Cobalt Strike, Metasploit, PowerShell Empire, Brute Ratel, etc.)

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

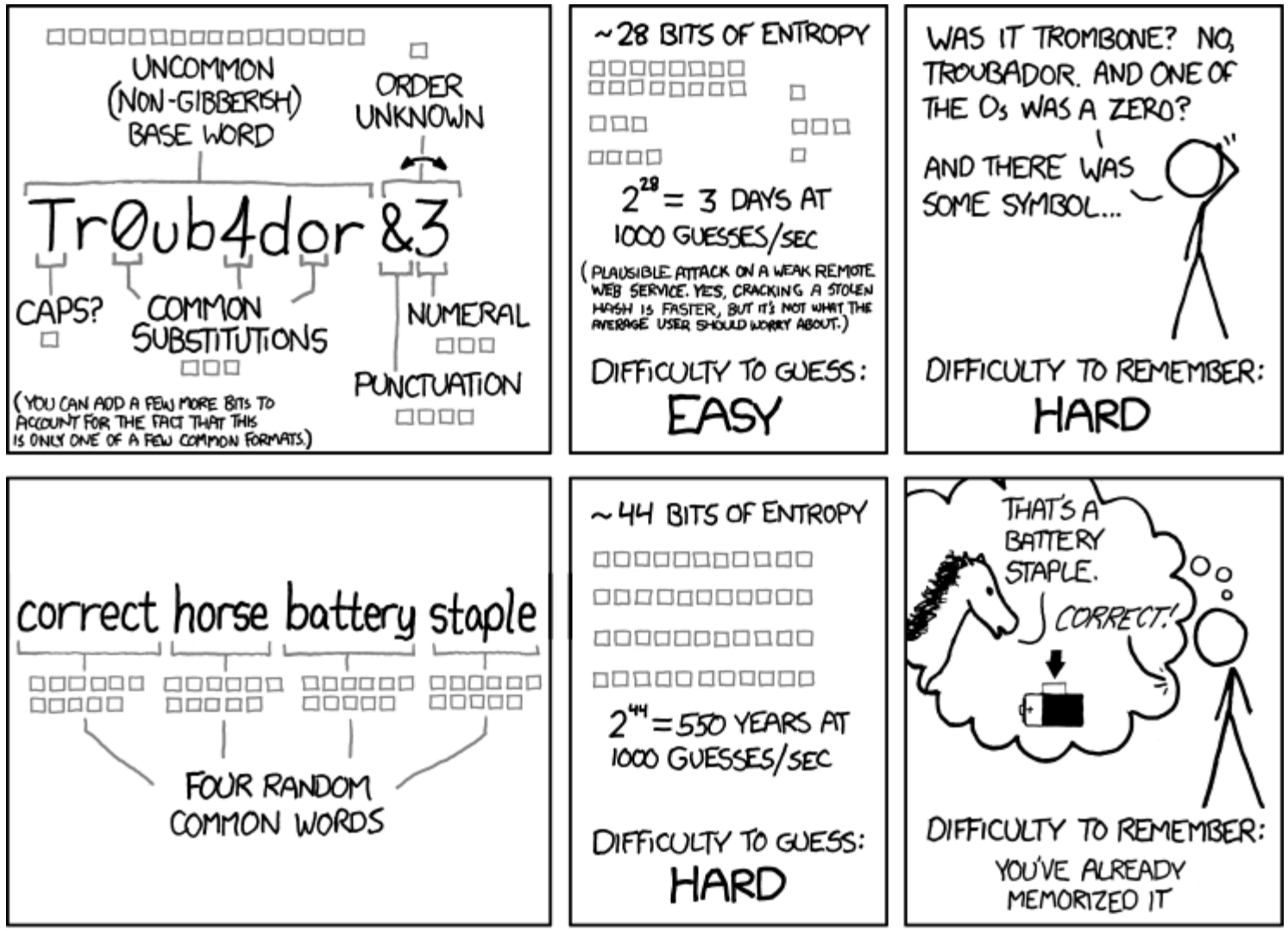
Natasha Lomas @riptari / 5:36 AM CDT • August 19, 2022 Comment

Demo

Basic-Windows-keylogger (GitHub here, blog here)



XKCD – Password Strength



Mitigation

Keylogging is a broad general issue that is not specific to browsers, and there are various commercial anti-keylogging products available.

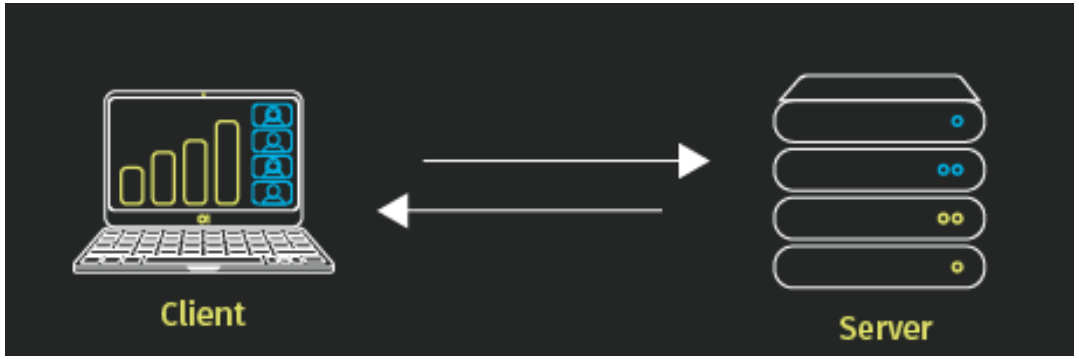
- Ghostpress [Link here]
- KL-Detector [Link here]

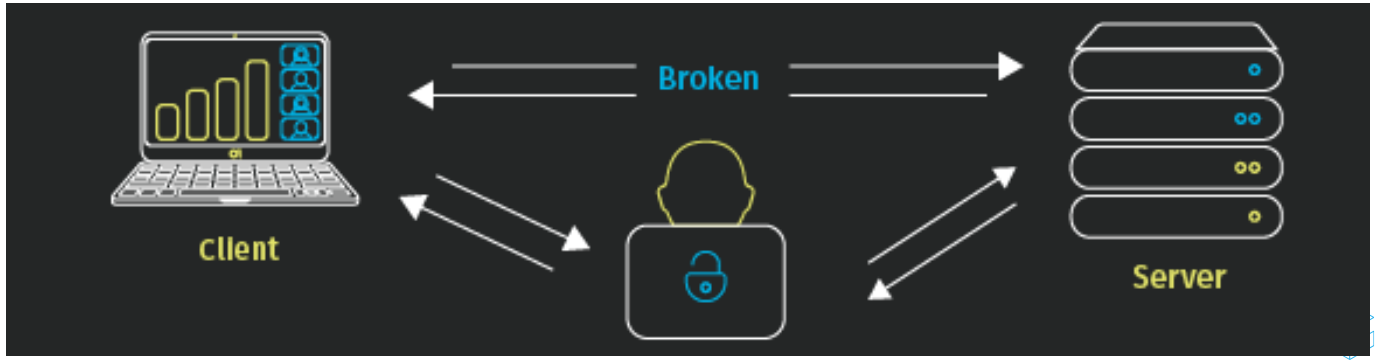
Password Managers

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).

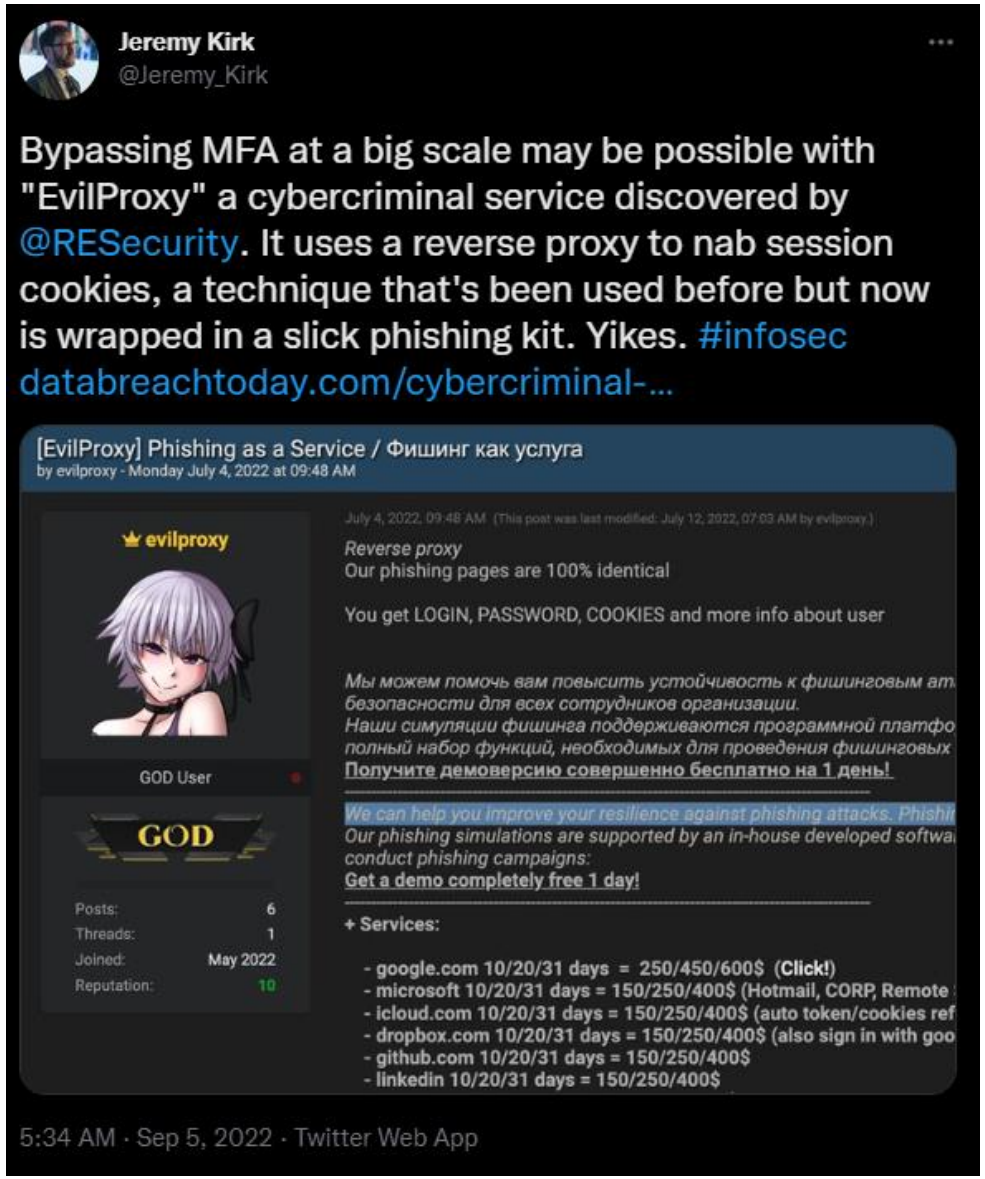




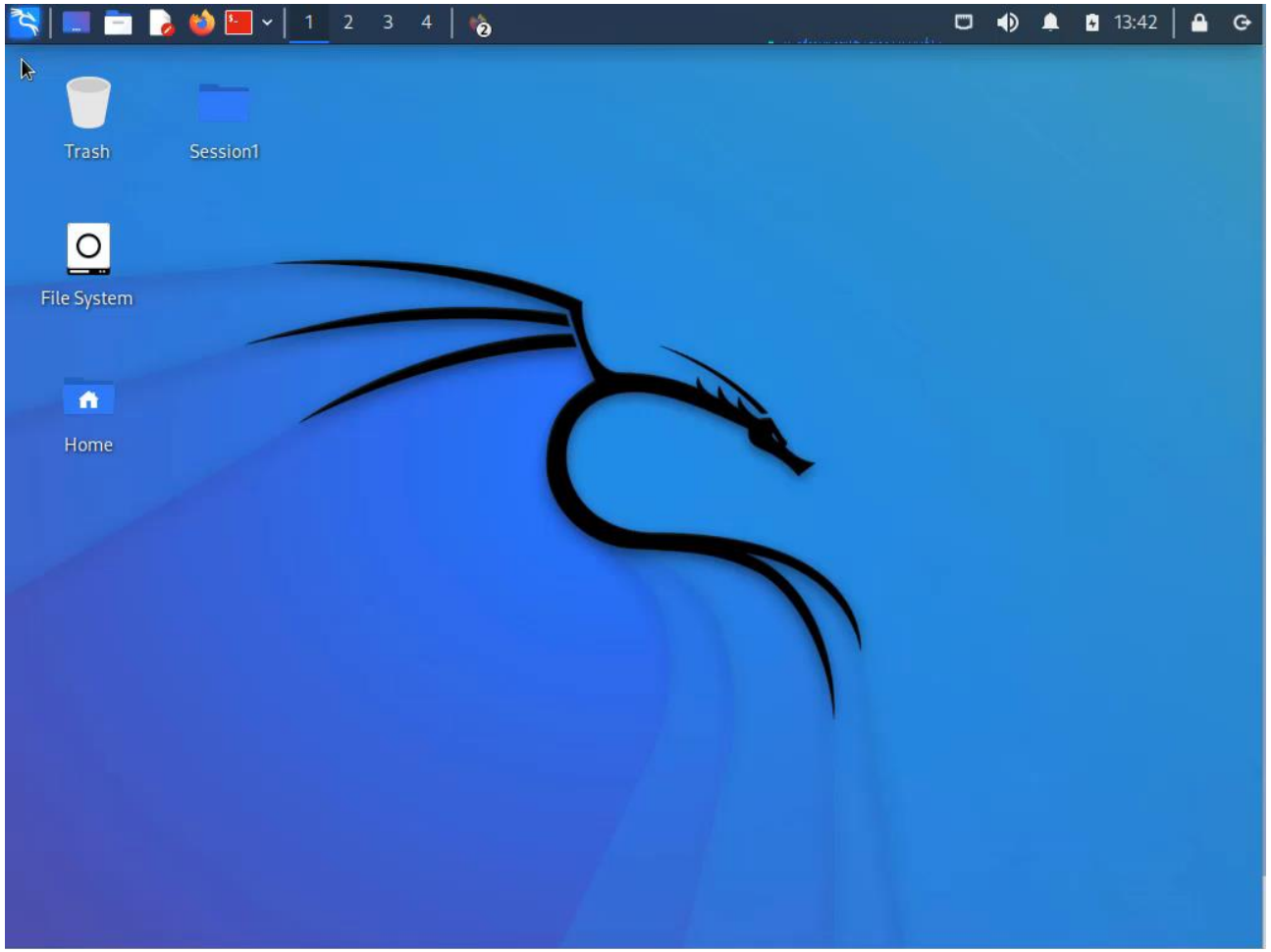
Examples:

- **Evilginx 2** [GitHub here] [Blog here]
- **EvilProxy**

- **MITMF** [Link here]
- **Social Engineering Toolkit** (SET) [Link here]



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!

Command Prompt

```
C:\temp>
```

Mitigation

Block unauthorized processes from accessing sensitive browser files.

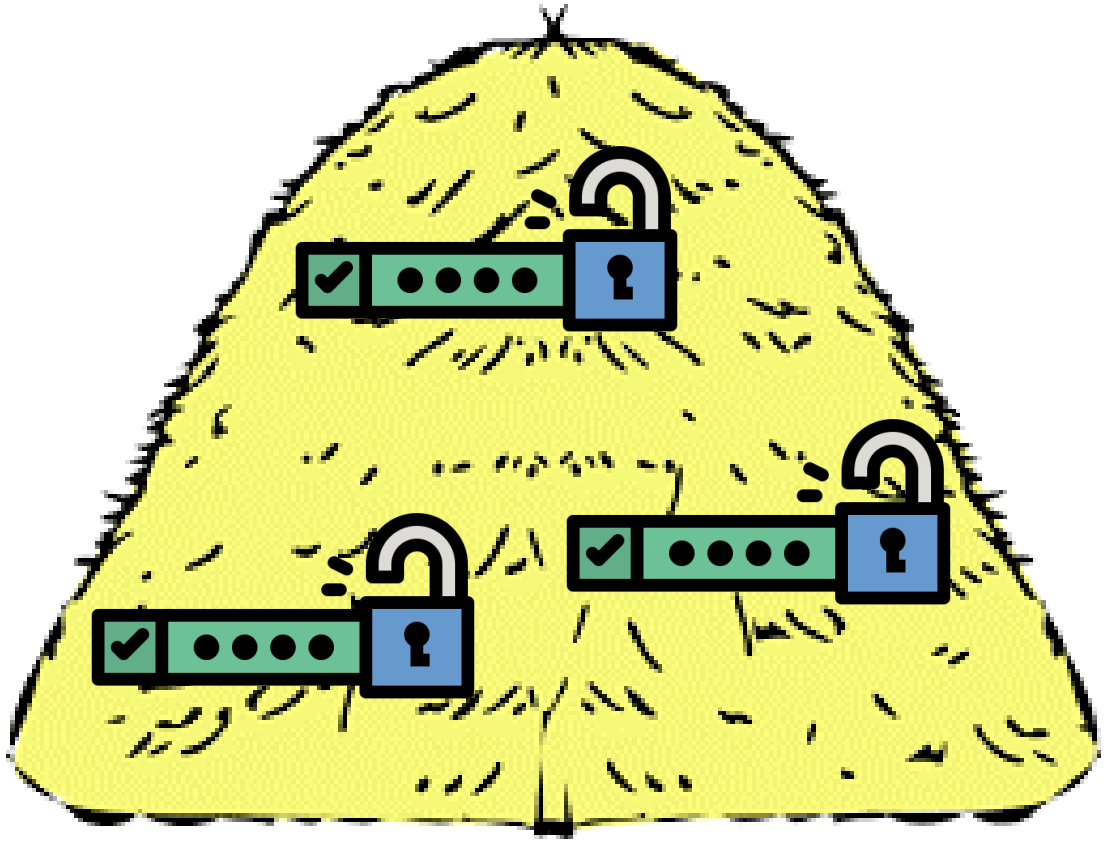
AppData\Local\Google\Chrome\User Data\Default\Login Data

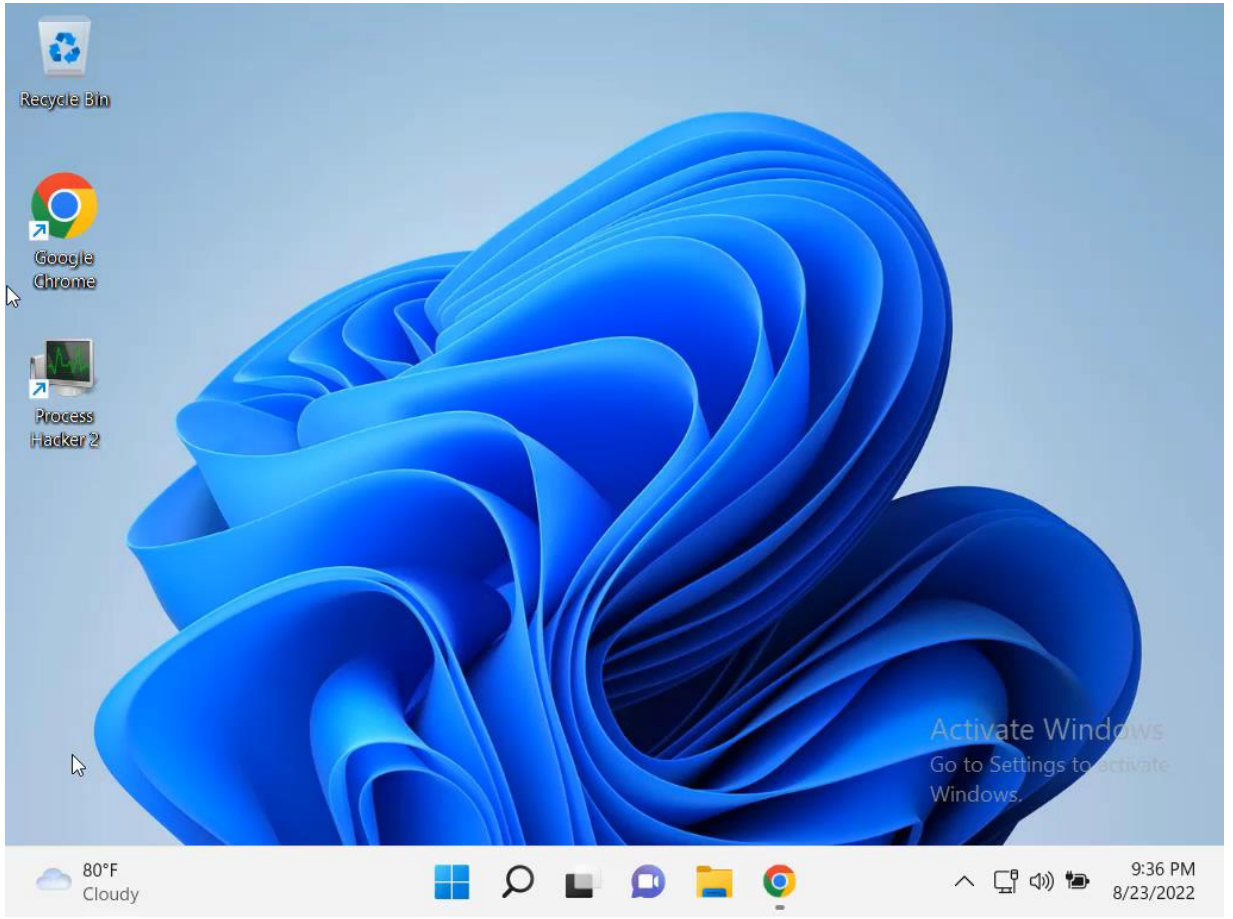
“?:\Users*\AppData\Local\Google\Chrome\User Data*\Login Data”

- 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

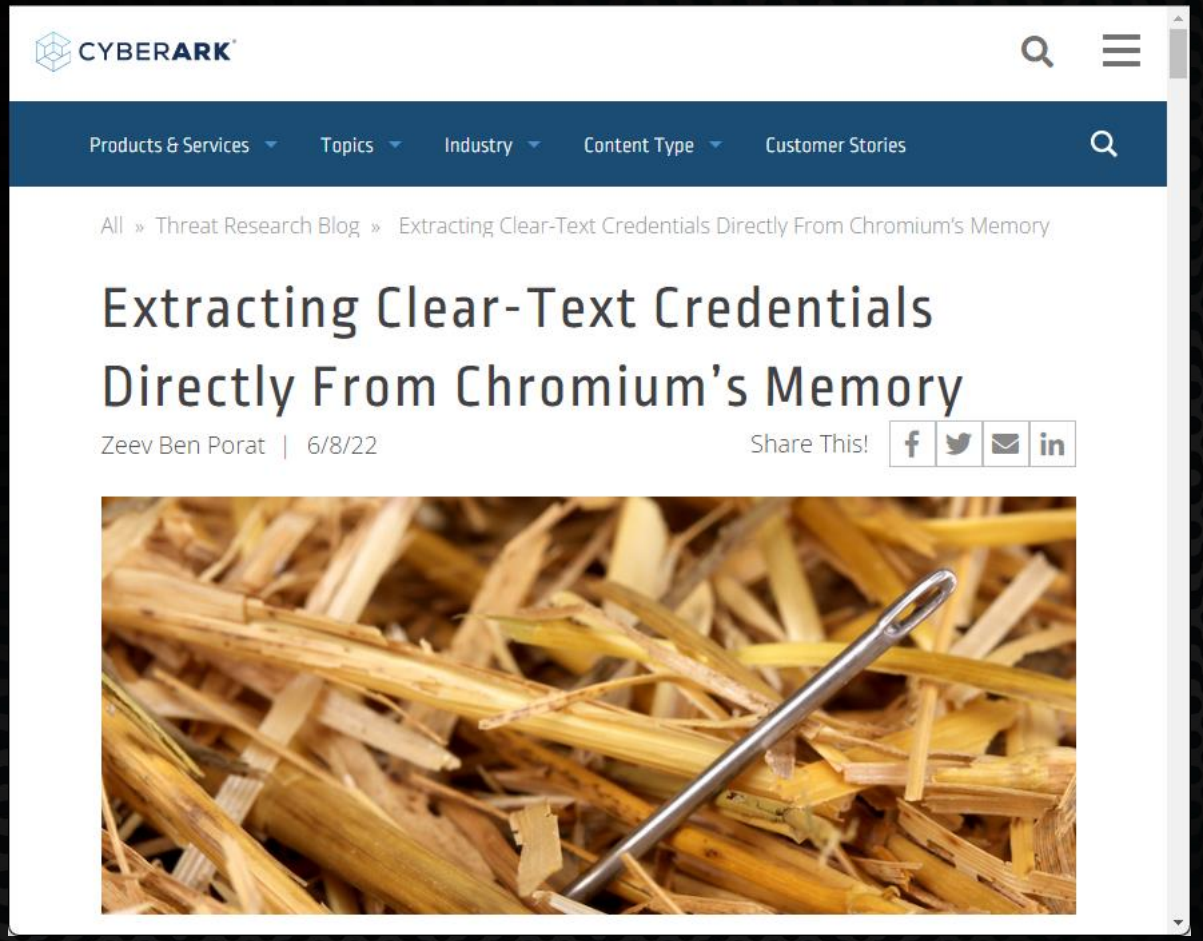
- Access browser from an external process
- Create a browser process
- Dump the memory of the browser process

MITRE T1555/003
https://attack.mitre.org/techniques/T1555/003/

Example

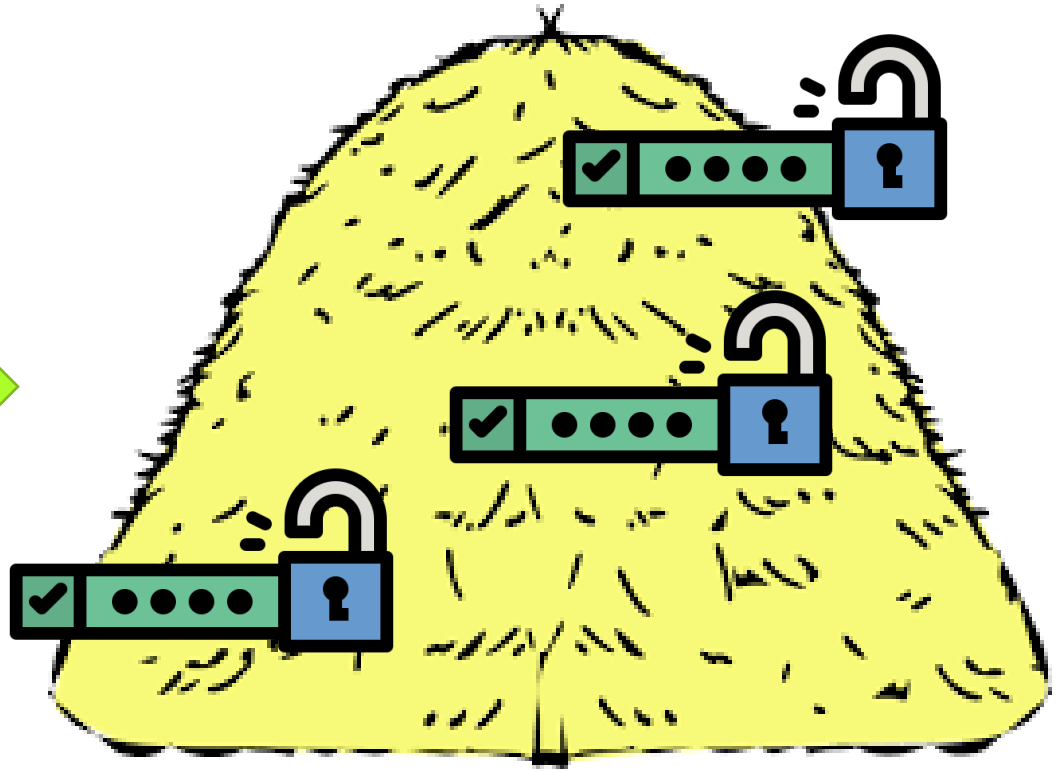
mimikittenz [GitHub here]

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

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

PatternName     PatternMatch
-----------     ------------
Dropbox         login_email=papaluspal%40paypil.com&login_password=cro0ducile%40&
Slack           &crumb=s-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=on ...
Slack           &crumb=s-1467644415-719b8f8a1-&email=slacker@slacker.com&password=slackmeup2&remember=onon  □□    I□...
Slack           &crumb=s-1467644415-719b8f08a1-%E2%98%83&email=slacker%40slacker.com&password=slackmeup2&remember=on7...
Slack           &crumb=s-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@ato.com&password=wherethetfns@&__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>
```



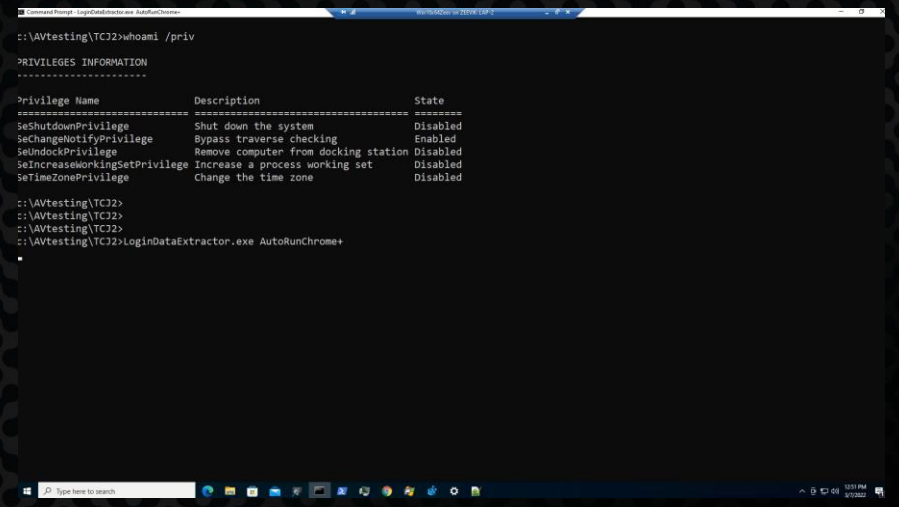
Labs.CyberArk.com

DEMO TIME!



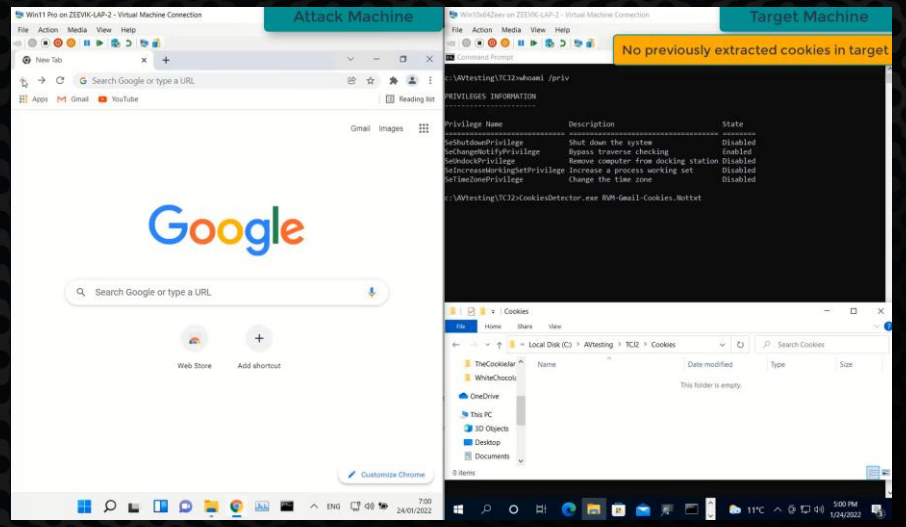
Chrome Password Manager Dump

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



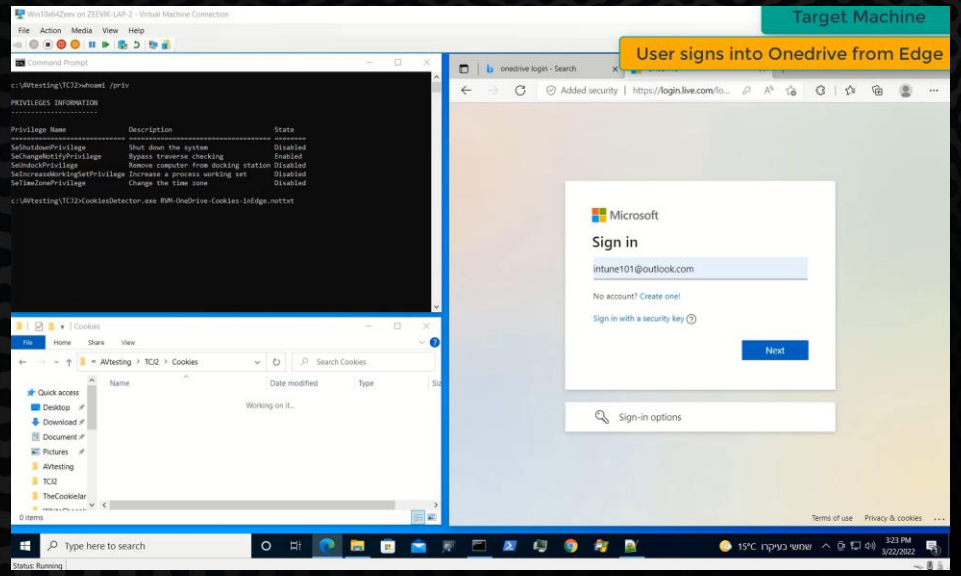
Gmail Session Hijack

- Waiting for user to start a Gmail session.
- Extracting session cookies from memory.
- Activating “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:

genesis

- Dashboard (new)
- Genesis Wiki
- News (21)
- Bots (400k+)
- Generate FP
- Orders
- Purchases
- Payments
- Tickets
- Software (6.3 | 19.0)
- Profile
- Invites
- Logout

Home

Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
221	+819	+6732	+28108	424654
Groupped by				
US	+52	+641	+3061	13390
ES	+70	+559	+2265	34857
FR	+73	+536	+2227	40666
IT	+89	+585	+2202	57045
RO	+88	+564	+2086	22700
AR	+53	+482	+1901	17252
PL	+47	+464	+1684	19126
HU	+45	+426	+1559	13062
CL	+35	+372	+1429	10335
NP	+28	+265	+1245	9950

Bots

Extended Search

Enabled | Resource name / URL | Without Resources

paypal,ebay,hotmail.com...

Resources total: 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 / 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	Filter $
258498755B44CAF0CD64FA768CE149A5 2021-06-27 02:59:07 2021-06-27 19:08:44	0 64 0 = 64 Instagram, Servus, Tumblr, Office365, EtsyStore Netflix, ShutterflyStore, Live, Amazon, EANetwork Google, Twitter, Steam, WishStore, Indig... ...known 28 wifiguest.ecsd.net account.mycommerc... ...other 36	US 46.244... Windows 10 Home	59.00
B3371B2079C2DF4819CDE7D3FD432CF6 2021-02-26 08:35:28 2021-02-28 08:29:15	0 57 0 = 57 Alibaba, 126com, AppleStore, Netflix Facebook, LinkedIn, iCloud GCKeyCanada, Twitter, PayPal ...known 11	US 104.233... Windows 10 Codename 19H2 Insider Preview	57.00

937F534FCFE2384B8E251C7A6F5ACA40

Add to Cart | Reserve | Buy

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	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 fingeprints

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

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)

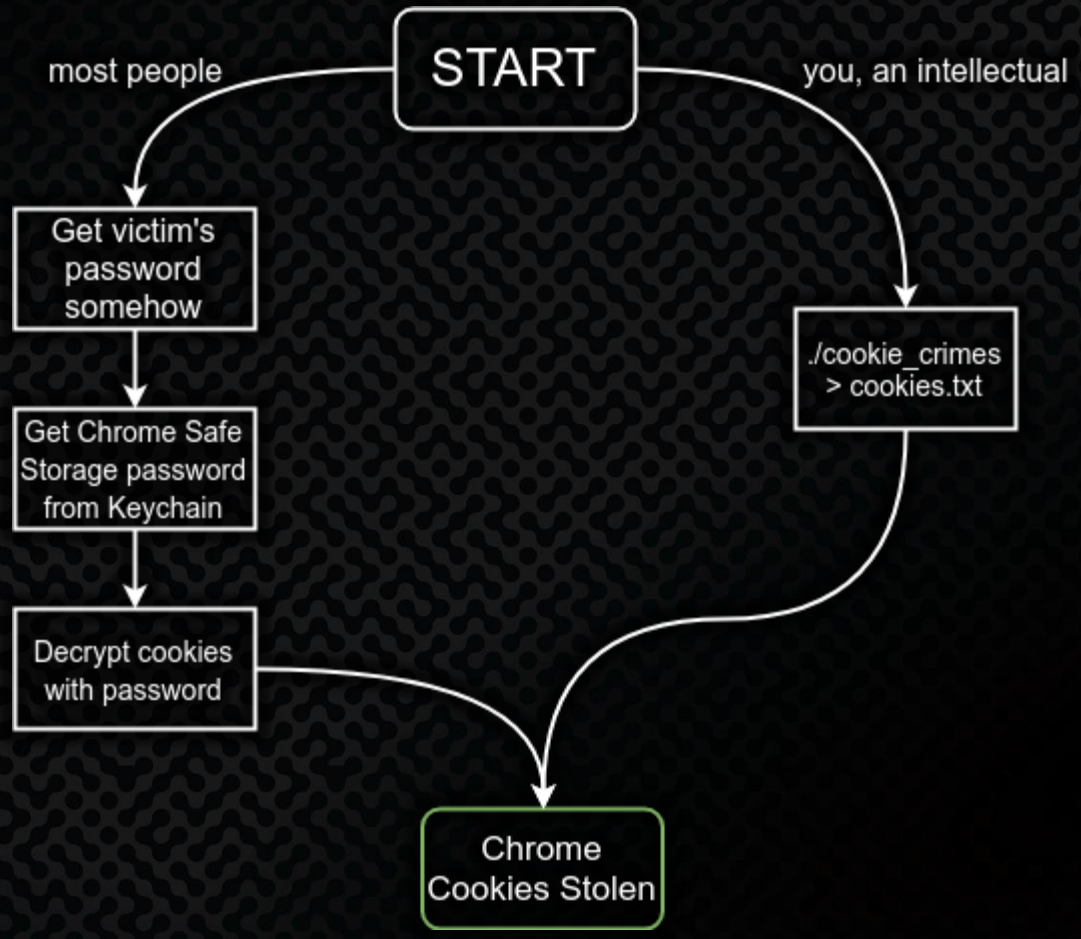
Command line arguments

“Alex” (@mangopdf) published in 2018 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.

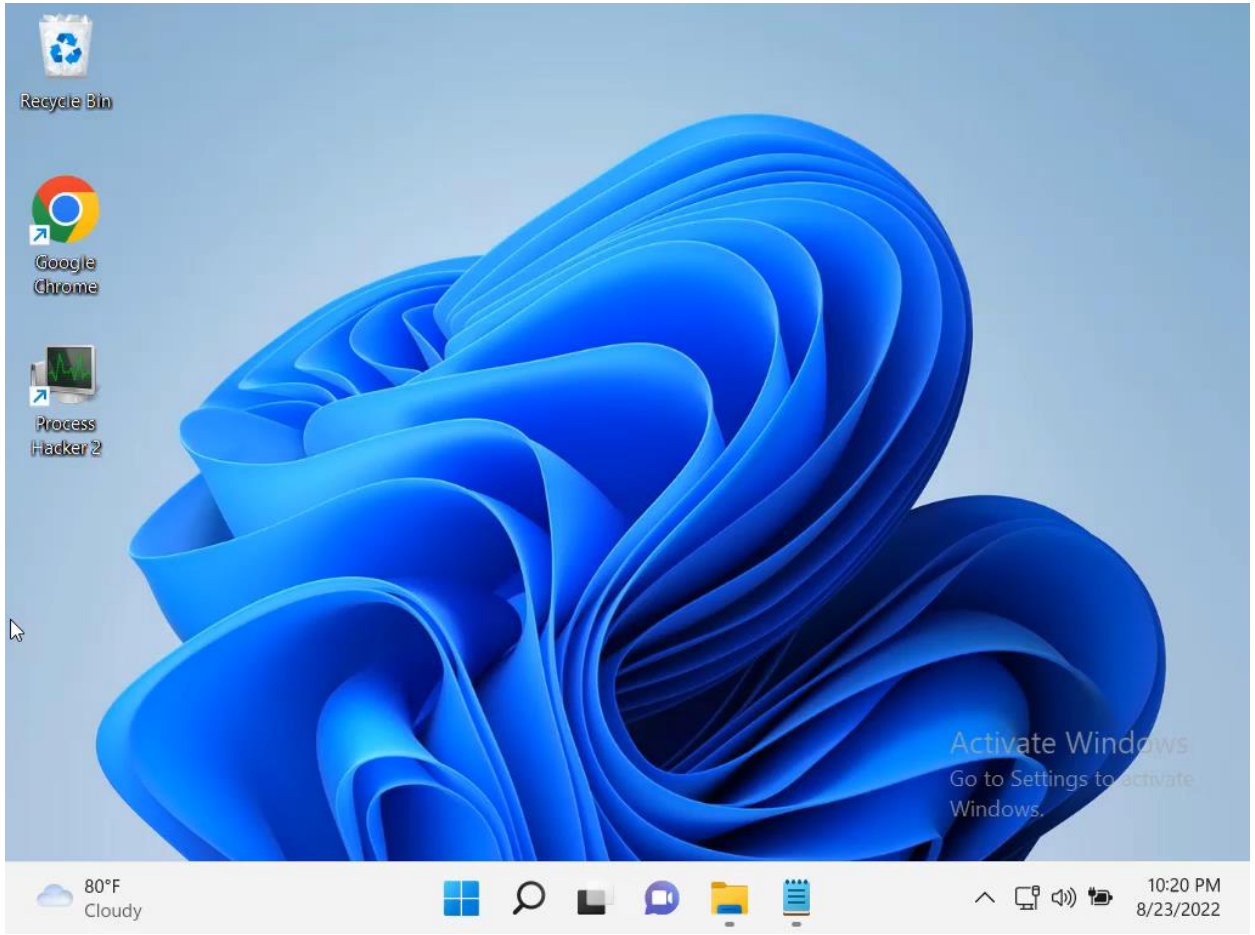
https://www.youtube.com/watch?v=BWAetsJqey0

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 VM
- Prevent unauthorized processes from creating the browser process
- Block suspicious command line options when browser is created

Thank you!

Terima kasih!