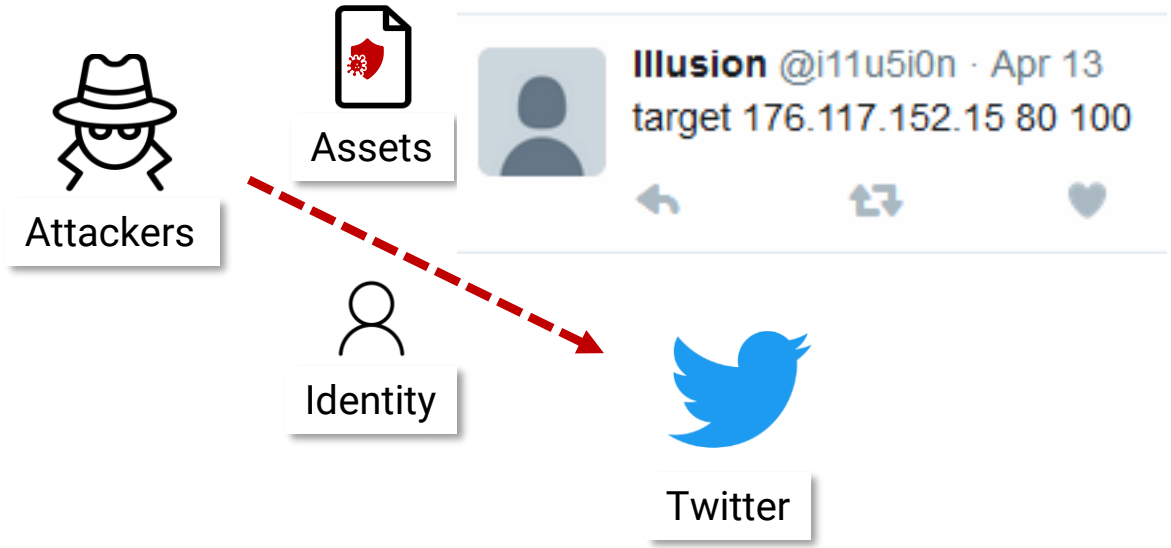
Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware

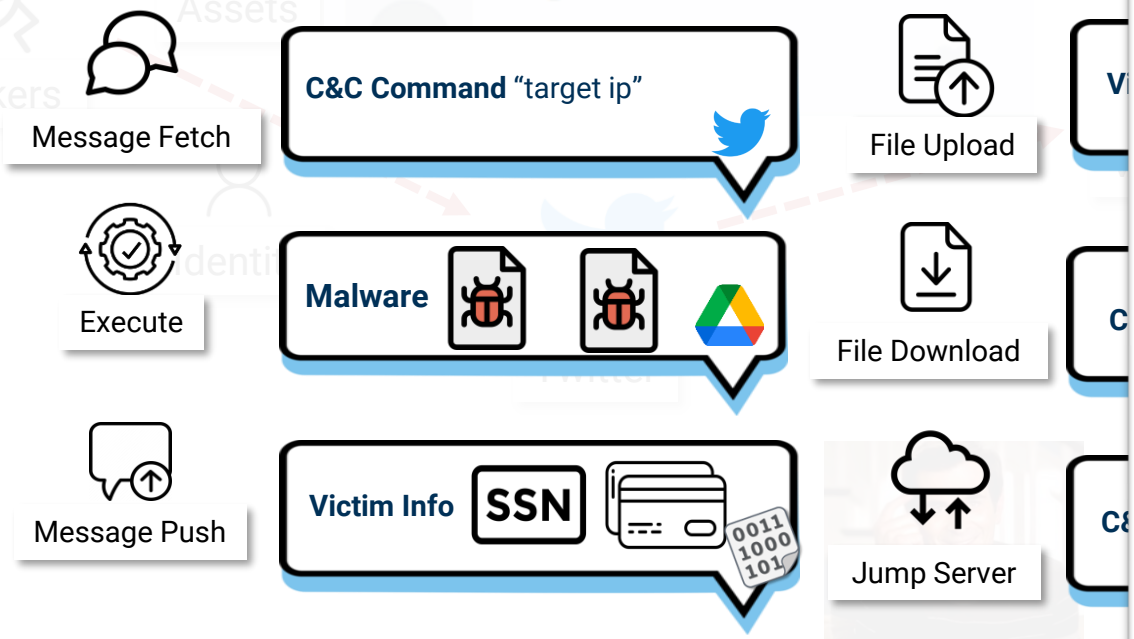
Mingxuan Yao, Jonathan Fuller, Ranjita Pai Sridhar,
Saumya Agarwal, Amit K. Sikder, Brendan Saltaformaggio

Georgia Tech

Suspicious Message On Twitter



Suspicious Message On Twitter



Choose type of policy violated

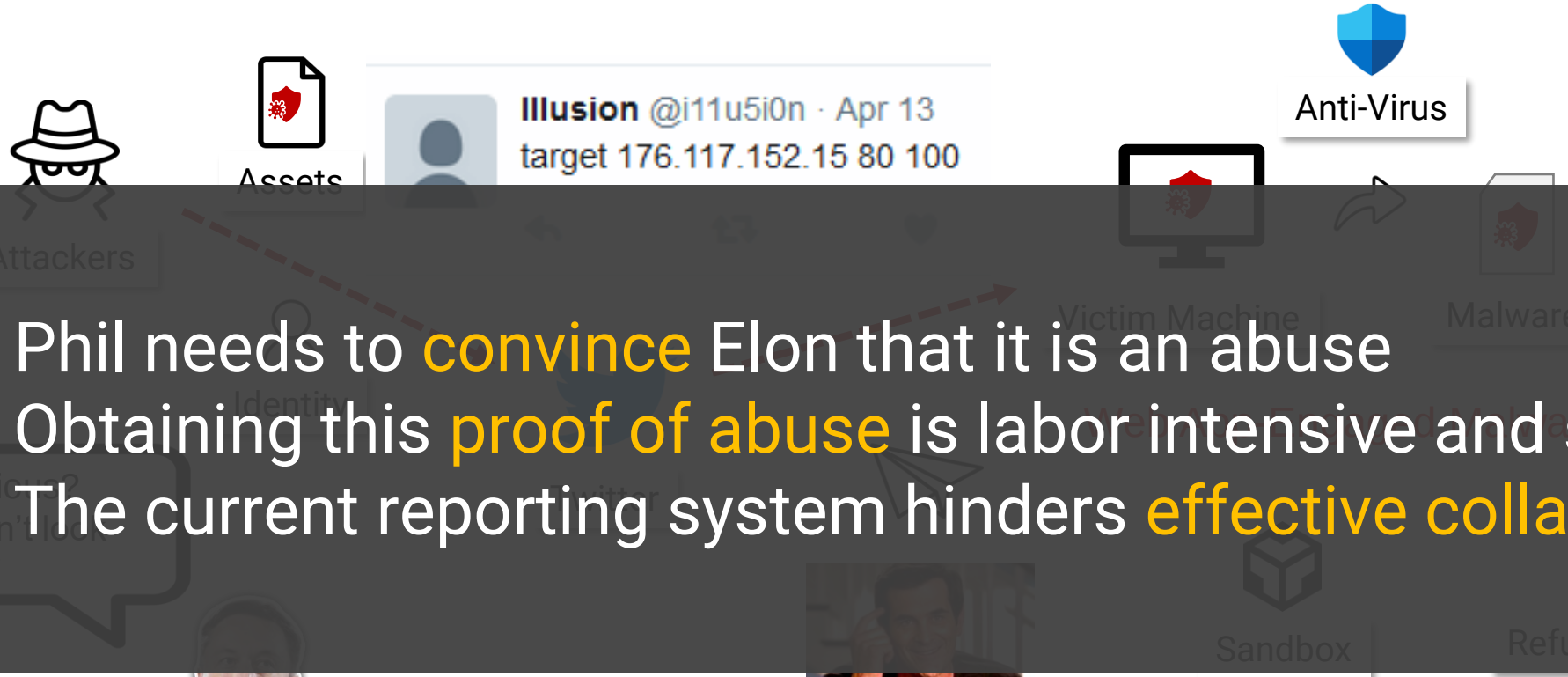
- ○ Spam
- ◉ Malware

  We do not allow our products to be used for the transmission of malware, viruses, destructive code, or anything that may harm or interfere with the operation of the networks, servers, or other infrastructure of Google or others.

- ○ Phishing
- ○ Violence
- ○ Hate Speech
- ○ Violent Organizations and Movements Content
- ○ Harassment, Bullying, and Threats
- ○ Sexually Explicit Material
- ○ Impersonation and Misrepresentation
- ○ Personal and Confidential Information
- ○ Illegal Activities
- ○ Copyright Infringement
- ○ Child Endangerment

Submit report

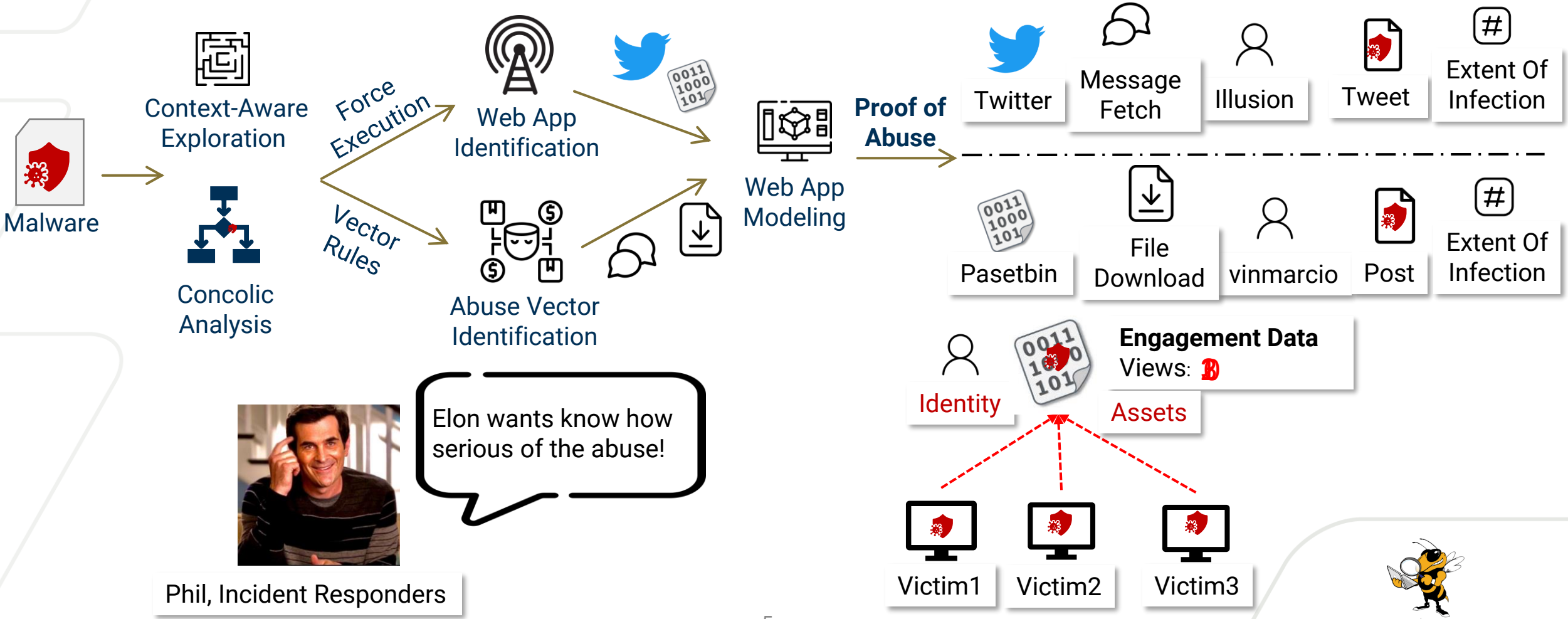
Suspicious Message On Twitter - Hide In Plainsight



Problem 1: Phil needs to convince Elon that it is an abuse
Problem 2: Obtaining this proof of abuse is labor intensive and slow
Problem 3: The current reporting system hinders effective collaboration

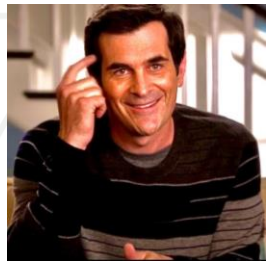
To Help Phil: Design Of Marsea

Key Idea Automated malware analysis + web app platforms information = proof of abuse



Our Proof of Abuse Enables Novel Collaborations

Phil provides in-depth Proof of Abuse

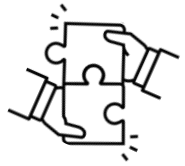


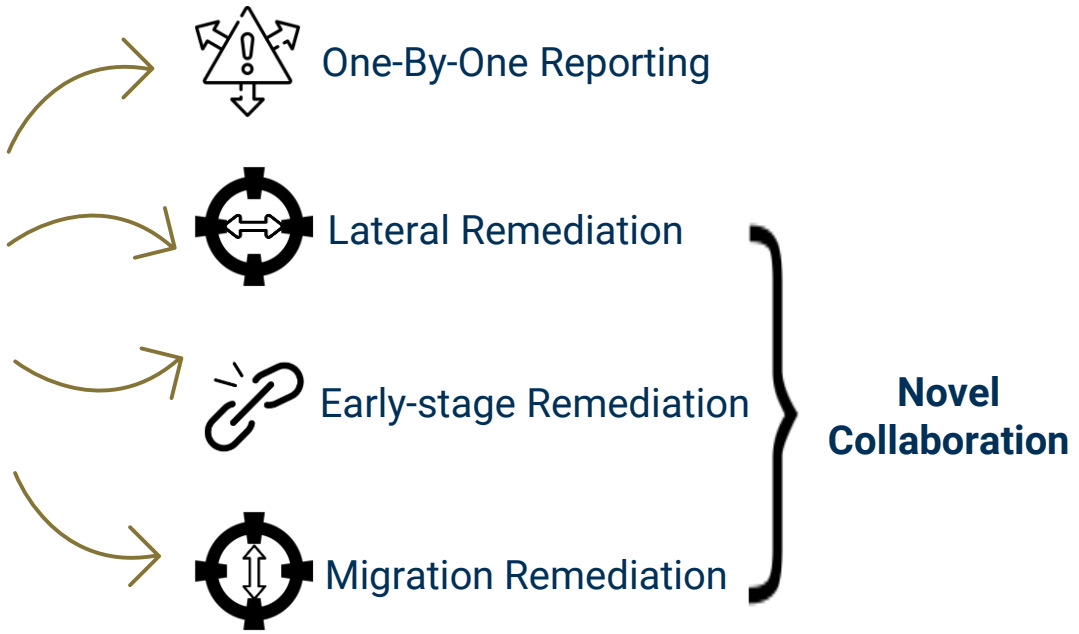
Phil: Incident Responders

Proof of Abuse

Elon: Service Providers

Elon can use Proof of Abuse to remediate





Phil should give Proof of Abuse to Elon!

Let’s Collaborate

Leading Secure Access Service Edge Provider, providing service to more than 25% of the Fortune 100

Dataset: 10K Malware

3K randomly pulled from VT
1K per year 2020-2022
7K Netskope-observed malware

Web Apps	Malware	Live Malware	Response Delay
Google Drive	322	36% found malware abusing Google	59
Github	46	34	583
Pastebin	56	33	118
Telegram	4	2	327
Twitter	54	26	-51
Wordpress	9	3	29
Discord	86	21	51
Blogspot	6	4	-13
Dropbox	13	10	813
…	…	…	…
Total	893	430	253

Let’s Collaborate

Leading Secure Access Service Edge Provider, providing service to more than 25% of the Fortune 100

Dataset: 10K Malware

3K randomly pulled from VT
1K per year 2020-2022
7K Netskope-observed malware

Web Apps	Malware	Live Malware	Response Delay
Google Drive	322	214	59
Github	46	34	583
Pastebin	56	33	118
Telegram	4	2	327
Twitter	54	26	-51
Wordpress	9	3	29
Discord	86	21	51
Blogspot	6	4	-13
Dropbox	13	10	813
…	…	…	…
Total	893	430	253

8.9% Web App-Engaged Malware

Let’s Collaborate

Leading Secure Access Service Edge Provider, providing service to more than 25% of the Fortune 100

Dataset: 10K Malware

3K randomly pulled from VT
1K per year 2020-2022
7K Netskope-observed malware

Web Apps	Malware	Live Malware	Response Delay
Google Drive	322	214	59
Github	46	34	583
Pastebin	56	33	118
Telegram	4	2	327
Twitter	54	26	-51
Wordpress	9	3	29
Discord	86	21	51
Blogspot	6	4	-13
Dropbox	13	[illegible]	813
…	…	…	…
Total	893	430	253

Need 253 days to detect malware

Let’s Collaborate

Leading Secure Access Service Edge Provider, providing service to more than 25% of the Fortune 100

Dataset: 10K Malware

3K randomly pulled from VT
1K per year 2020-2022
7K Netskope-observed malware

Web Apps	Malware	Live Malware	Response Delay
Google Drive	322	214	59
Github	46	34	583
Pastebin	56	33	118
Telegram	4	2	327
Twitter	54	26	-51
Wordpress	9	3	29
Discord	86	21	51
Blogspot	6	4	-13
Dropbox	13	10	813
…	…	…	…
Total	893	430	253

48% Malware With Active Assets

One-By-One Reporting

Web App-Engaged Malware

430 Web App-Engaged Malware
129 unique assets with proof of abuse

Reporting

Visited abused web apps

Navigated to the assets on the platform

Located the reporting systems
- Email
- One click flag
- Radio button web form
- Free response web form

Reported them all one by one

Web Apps	Response Time (days)	Reported	Take Down
Discord	2	21	19
Github	103	27	16
DuckDNS	2	1	1
Afraid	2	1	1
MediaFire	1	1	1
Twitter	3	1	0
Facebook	12	1	0
Pastebin	1	13	13
Google	138	42	
…	…	…	
Total	24	129	103

Took down 80% assets

One-By-One Reporting

Web App-Engaged Malware

430 Web App-Engaged Malware
129 unique assets with proof of abuse

Reporting

Visited abused web apps

Navigated to the assets on the platform

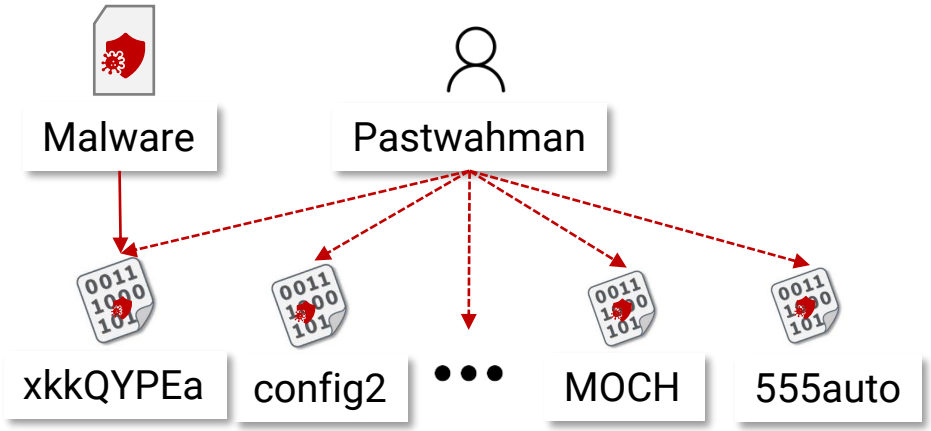
Located the reporting systems
- Email
- One click flag
- Radio button web form
- Free response web form

Reported them all one by one

Web Apps	Response Time (days)	Reported	Take Down
Discord	2	21	19
Github	103	27	16
DuckDNS	2	1	1
Afraid	2	1	1
MediaFire	1	1	1
Twitter	3	1	0
Facebook	12	1	0
Pastebin	1	13	13
Google	138	42	31
…	…	…	…
Total	24	129	103

Long response time

Lateral Remediation



Family	Identity	Assets	Other Assets
Neshta	vinmarcio	g3w5Zkzi	3
Bymeria	Huynhnhi92	Y8VWhxtG	5
Urse	pastwahman	xkkQYFEa	47

Key observation

Malware authors use same identity to host many Web App-Engaged assets

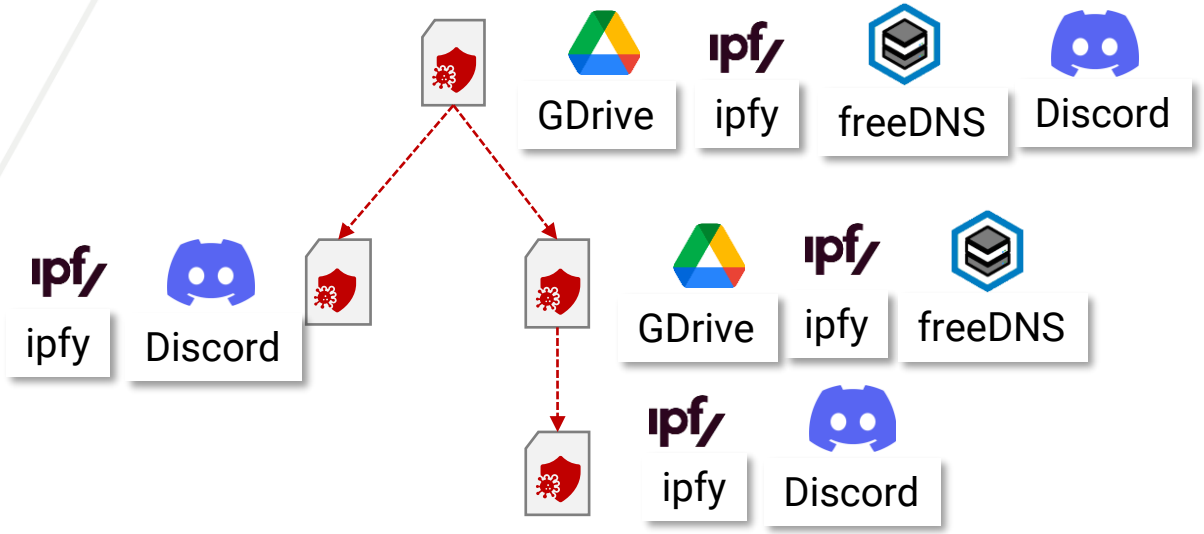
How is it done

Marsea → identity → other assets → lateral remediation

Benefits unlocked

From **3** abused assets, Lateral Remediation took down **52** additional assets

Early-Stage Remediation



Family	Malware	Web Apps	Web Apps In Chain	Total Dropped
Dkomet	11	2	4	9
Binder	2	4	4	5
Wapomi	1	2	0	1

Key observation

Web App-Engaged malware drop additional Web App-Engaged malware, forming an infection chain

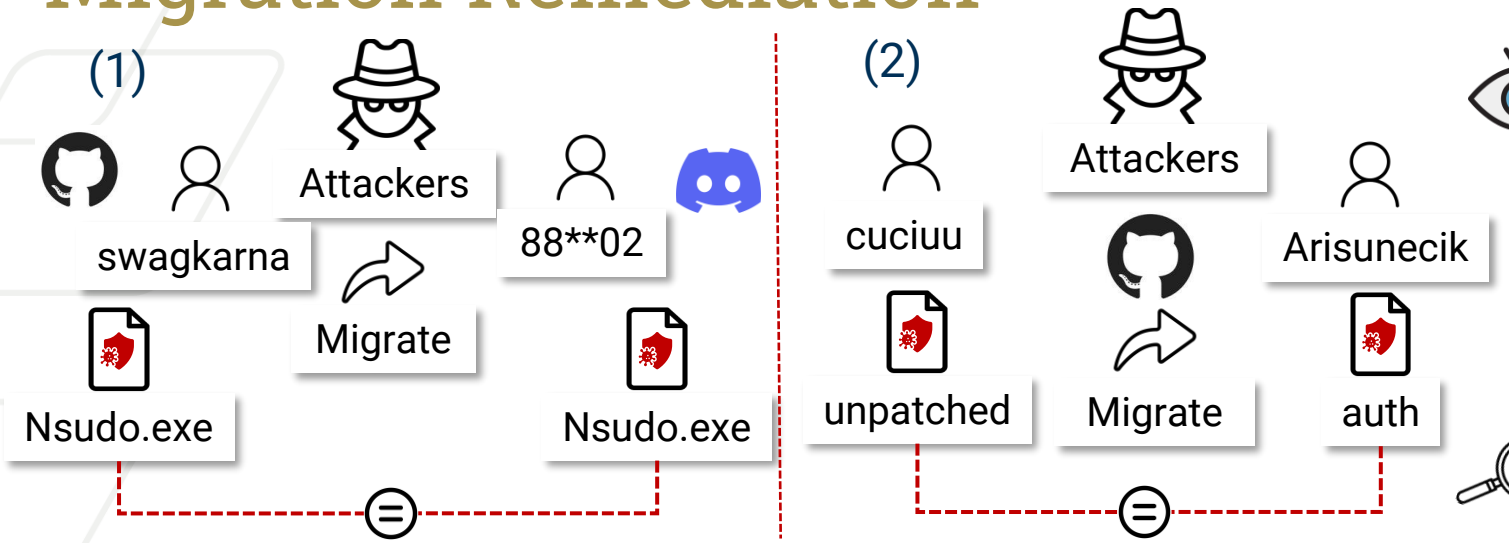
How is it done

Marsea → Infection chain → Take down chain through early-stage remediation

Benefits unlocked

Given **14** malware from **3** families, early-stage remediation could prevent **15 additional** malware from being dropped

Migration Remediation



Family	Web Apps	Identity	Assets	Malware
Sohanad	Webs	se***3	setting.xls	2
		ad***9	setting.doc	1
Sabsik	Github	cu***u	unpatched	1
		Ar***k	auth	8
Hynamer	Github	sw***a	Nsudo.exe	2
	Discord	88***2	Nsudo.exe	1
Msil	Dropbox	4g***a	hwid.txt	1
	GDrive	sa***a	hwid.txt	1

Key observation

Attackers migrate between
(1) different web apps
(2) different identities on the same web app

How is it done

Marsea → Web App-Engaged asset
→ service provider performs assets matching across identities
→ information sharing between service providers
→ across web apps sanitizing

Benefits unlocked

Given **6** assets, the migration remediation remediates **11** more Web App-Engaged assets

Positive Feedbacks

From: Automattic Trust & Safety <abuse@wordpress.com>
Sent: Tuesday, March 29, 2022 8:22 PM
To: <redacted>
Subject: [-] Re: abuse report

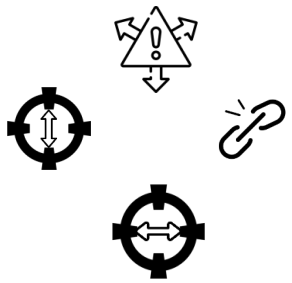
Automattic Trust & Safety (Automattic)
Mar 30, 2022, 0:22 UTC

Hello,

Thank you very much for your report.

The sites in question have been removed from WordPress.com for violating our Terms of Service.

Automattic Trust & Safety



Niflheim (Discord)
Apr 6, 2022, 11:19 PDT

Hello,

Thank you for bringing this issue to our attention. We've initiated an investigation based on the information that you provided and we'll take appropriate action based on our findings. Please note that for privacy reasons, we're not able to share the specifics of the action taken, if any.

We truly appreciate your efforts in helping us to keep Discord a safe and friendly environment.

Sincerely,
Discord Trust & Safety

Not Found (#404)

This paste has been deemed potentially harmful. Pastebin took the necessary steps to prevent access on March 22, 2022, 9:56 pm CDT. If you feel this is an incorrect assessment, please contact us within 14 days to avoid any permanent loss of content.

Much More in the Paper!

One abused identity with 5M views!

Crytocurrency stealing Web App-Engaged malware

Evaluation of packed malware

Ethical considerations

More highlights!

Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware

M. Yao, J. Fuller, R. Kasturi, S. Agarwal, A. Sikder, B. Saltaformaggio

USENIX, 2023

Mingxuan Yao
mingxuanyao@gatech.edu

Many thanks!

netskope

Cyber Forensics Innovation Lab

Georgia Tech Cyber Forensics Innovation Lab

Georgia Tech