# Automated Forensic Analysis-Driven Approach for the Remediation of Benign Service Abuse

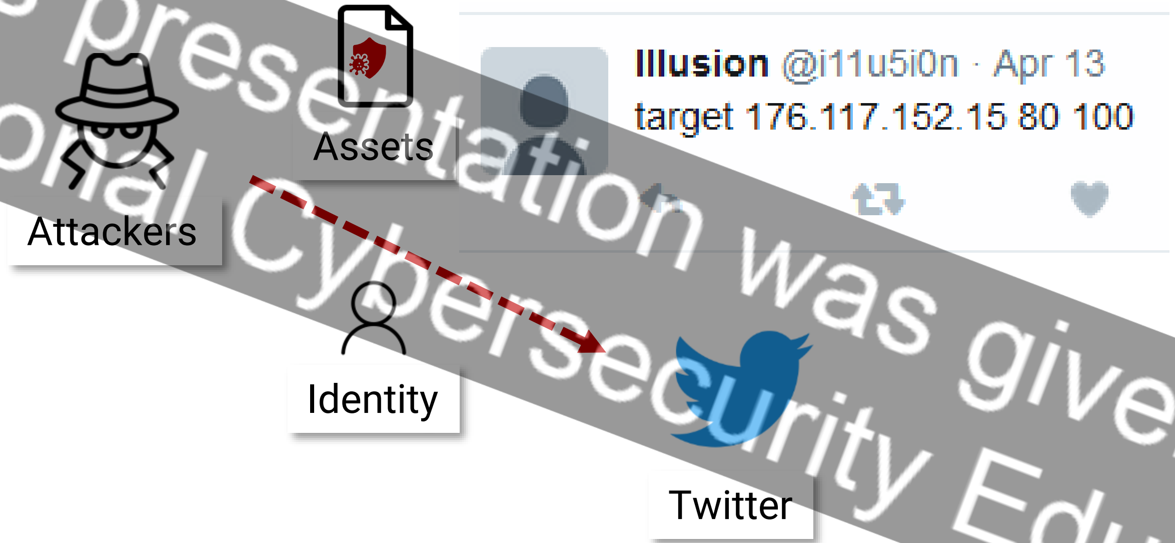
Mingxuan Yao

Advisor: Dr. Brendan Saltaformaggio

Georgia Tech

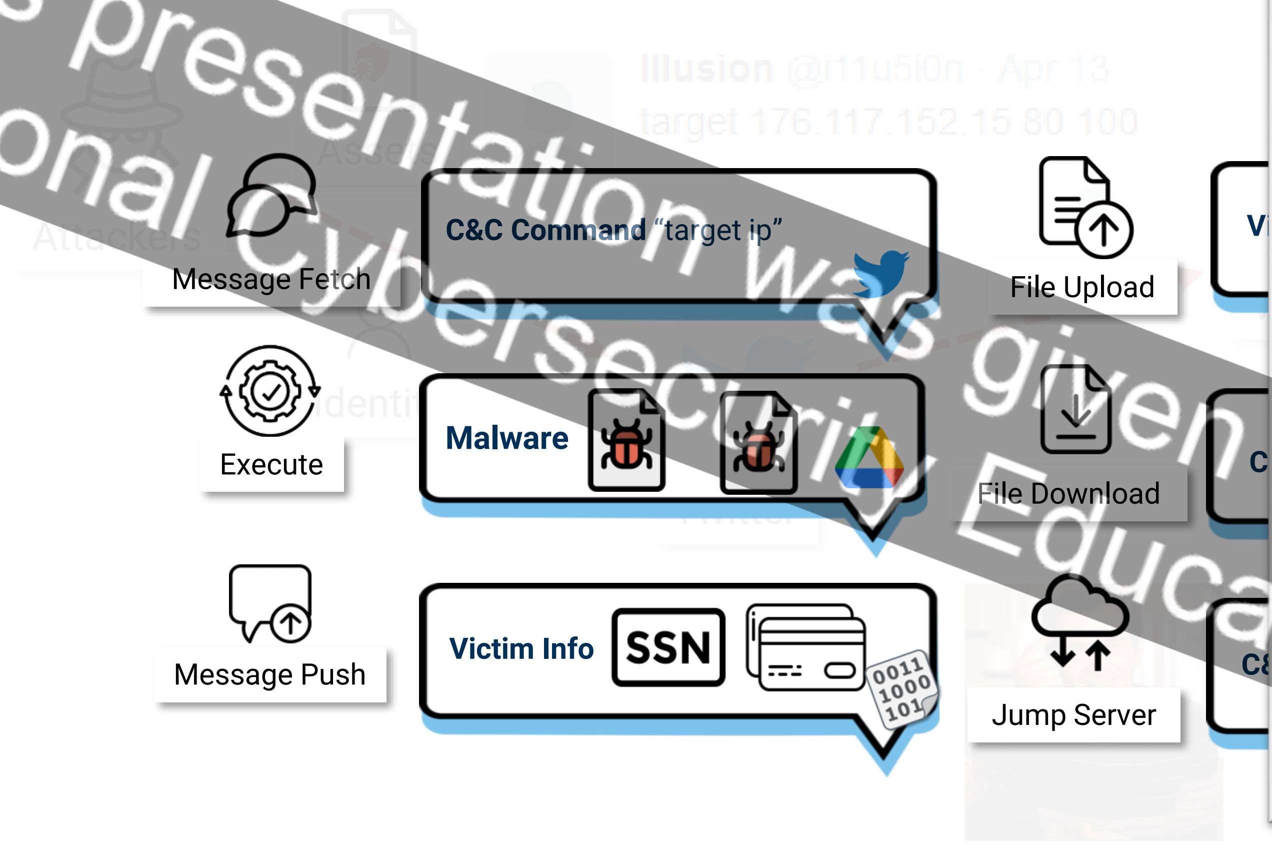
Georgia Tech | Cyber Forensics Innovation Lab

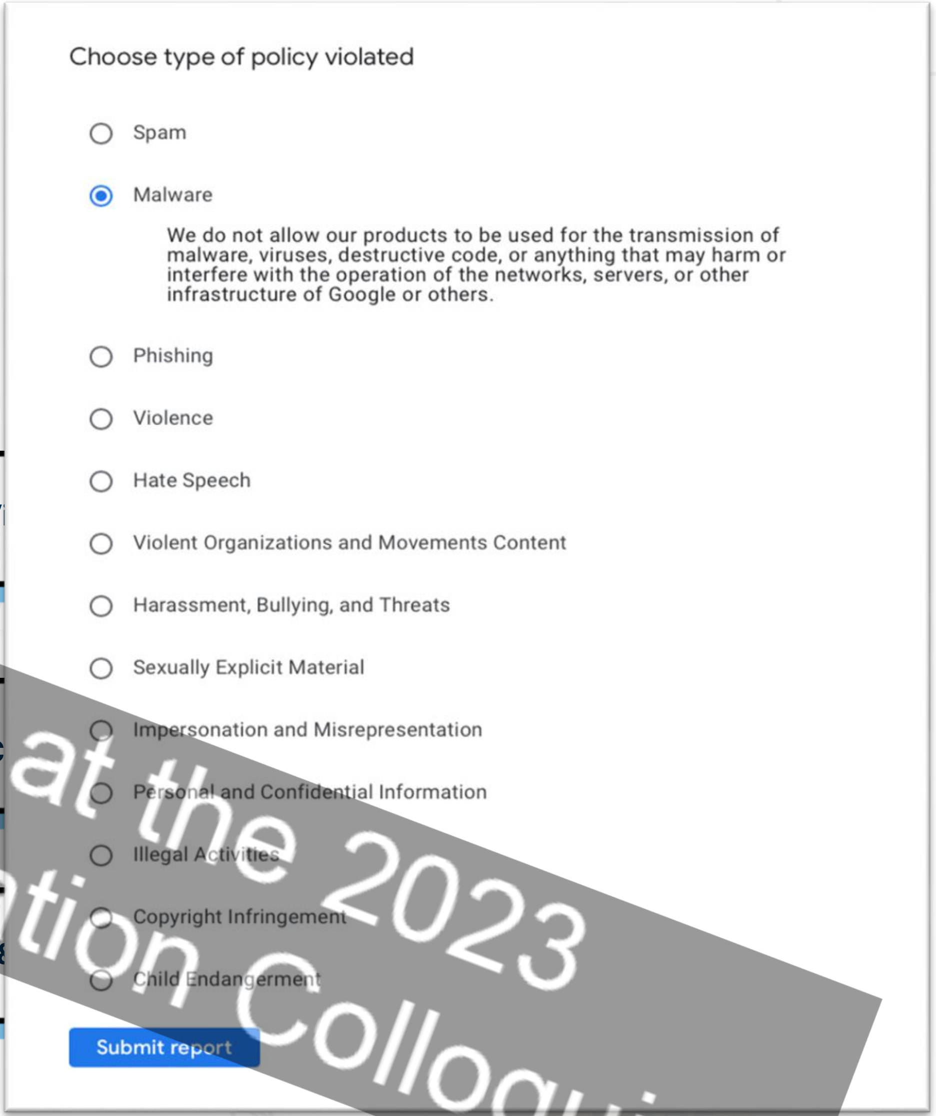
# Suspicious Message On Twitter



Illusion @i11u5i0n · Apr 13
target 176.117.152.15 80 100

# 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

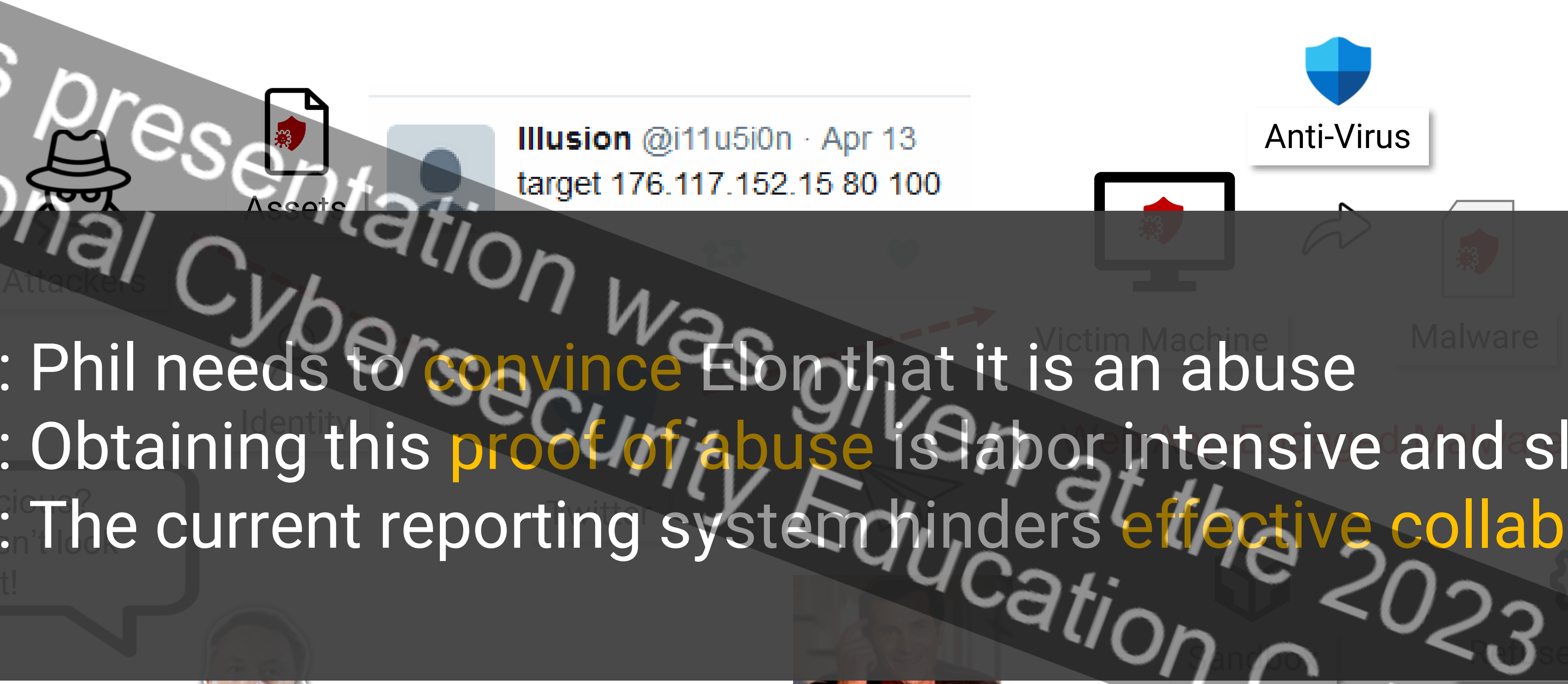
○ Personal and Confidential Information

○ Illegal Activities

○ Copyright Infringement

○ Child Endangerment

# Suspicious Message On Twitter - Hide In Plainsight



Illusion @i11u5i0n · Apr 13
target 176.117.152.15 80 100

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

Elon: Service Providers

Phil: Incident Responders

Manual Analysis

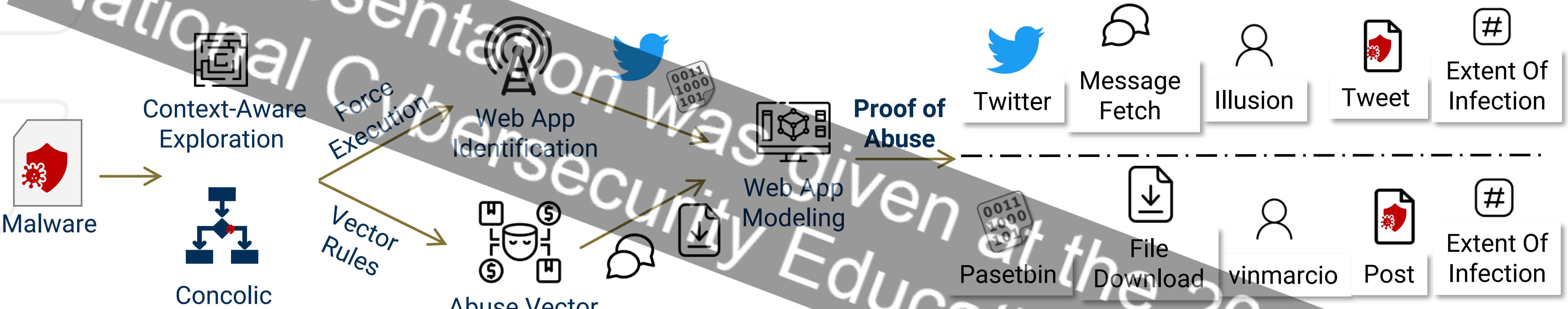
Time Consuming

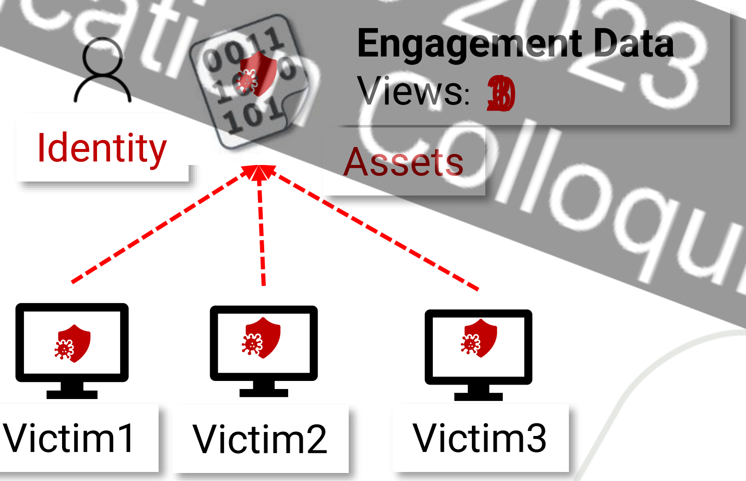
# Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware

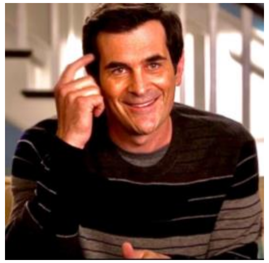
Mingxuan Yao, Jonathan Fuller, Ranjita Pai Sridhar, Saumya Agarwal, Amit K. Sikder, Brendan Saltaformaggio

[Usenix Security '23]

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







Elon wants know how serious of the abuse!

Phil, Incident Responders

# Let’s Collaborate

netskope

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 | [illegible] | 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 |

36% found malware abusing Google

# 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

netskope

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 |

Need 253 days to detect malware

# Let’s Collaborate

netskope

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

**Dataset: 10K Malware**

3K randomly pulled from VT

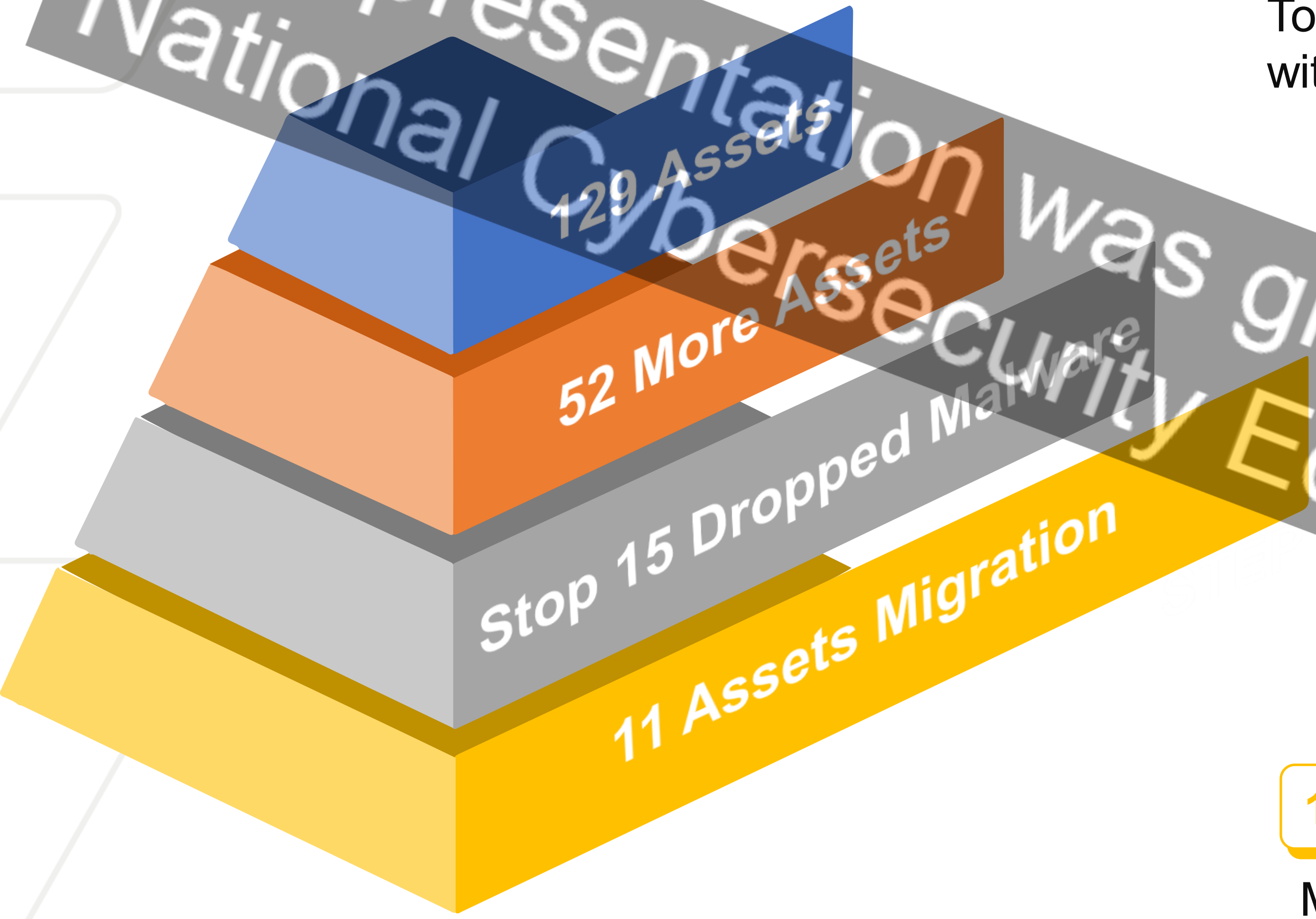
1K per year 2020-2022

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

# Let’s Collaborate: Real-World Impact



**129 unique active Assets**

Took down 80% by collaborating with service providers

**52 More Assets**

Identified 52 more assets from the same identity. Took down 100% of them

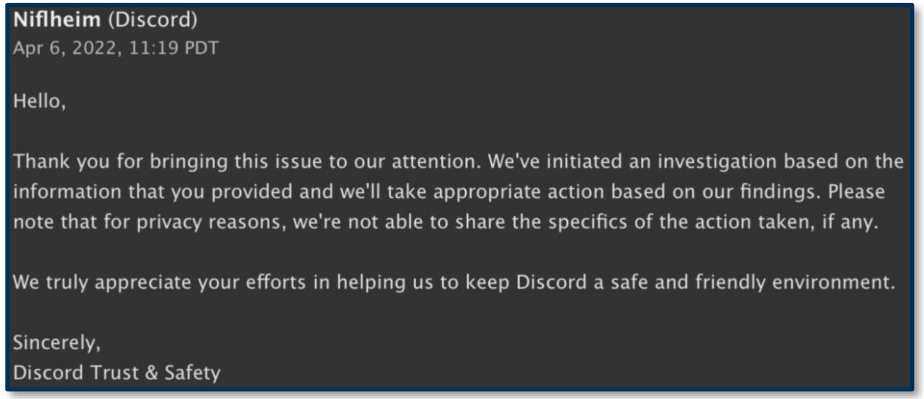
**15 Dropped Malware**

By took down active assets, my research prevents 15 additional malware from being dropped

**11 Migrated Assets**

My research prevents 11 assets migration

# Positive Feedbacks



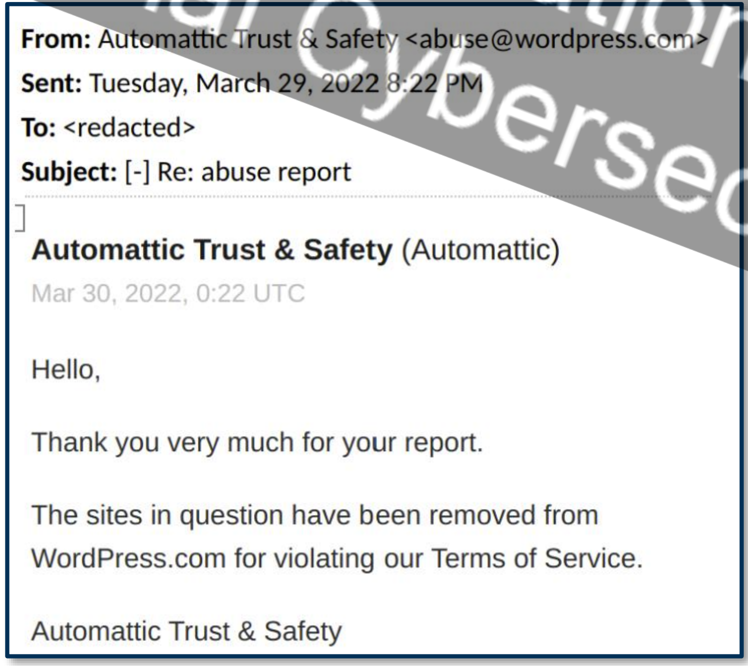
**Niflheim** (Discord)
Apr 6, 2022, 11:19 PDT

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



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

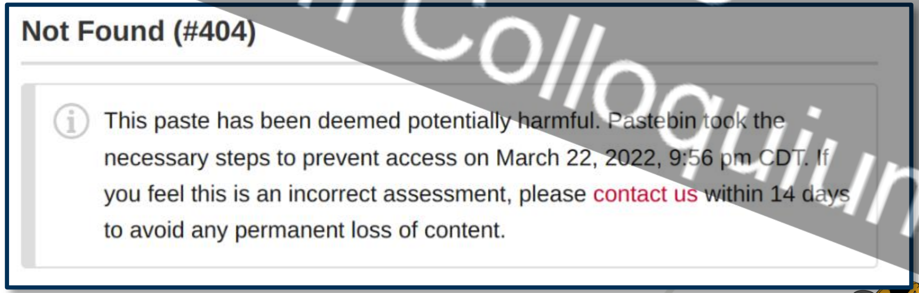
**Automattic Trust & Safety** (Automattic)
Mar 30, 2022, 0:22 UTC

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

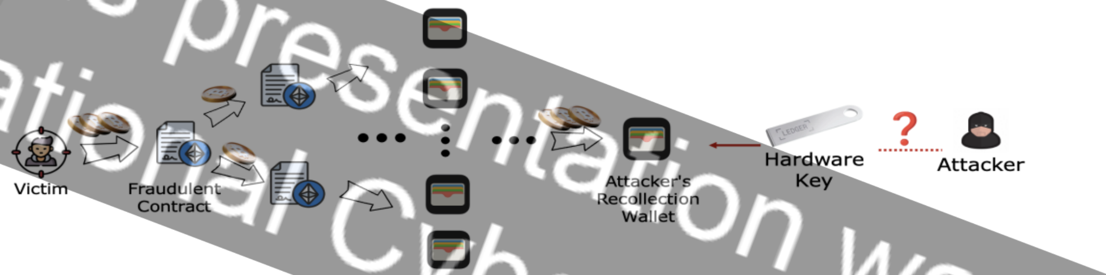


**Not Found (#404)**

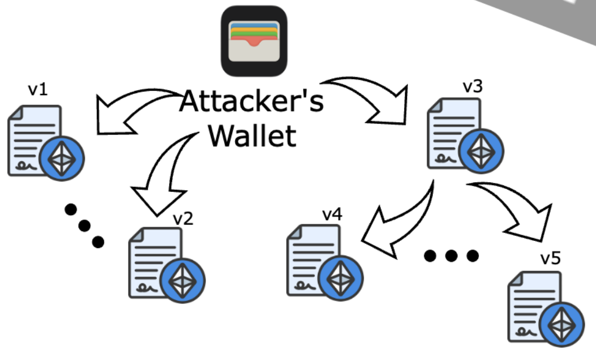
ⓘ This paste has been deemed potentially harmful. Pastebin took the necessary steps to prevent access on March 22, 2022, 9:56 pm CDT. If you feel this is an incorrect assessment, please contact us within 14 days to avoid any permanent loss of content.

# Ongoing And Future Work

## Remediate financial fraud on blockchain



## Forensics analysis on blockchain supply chain



## Vision and Long Term Research Direction

Attackers invariably make sacrifices when exploiting benign services for malicious purposes.

Automated Forensic Analysis-Driven Approach for the Remediation of Benign Service Abuse

Many thanks!

Cyber Forensics Innovation Lab

Mingxuan Yao
mingxuanyao@gatech.edu

Georgia Tech | Cyber Forensics Innovation Lab

Georgia Tech