Secureworks

Cyber Crime Is a Market Driven Underground Economy

Terry McGraw, *VP, Global Cyber Threat Analysis*
Secureworks
24 OCT 2023

Terrence “Terry” McGraw

Deputy Chief Threat Intelligence Officer, Executive Consultant

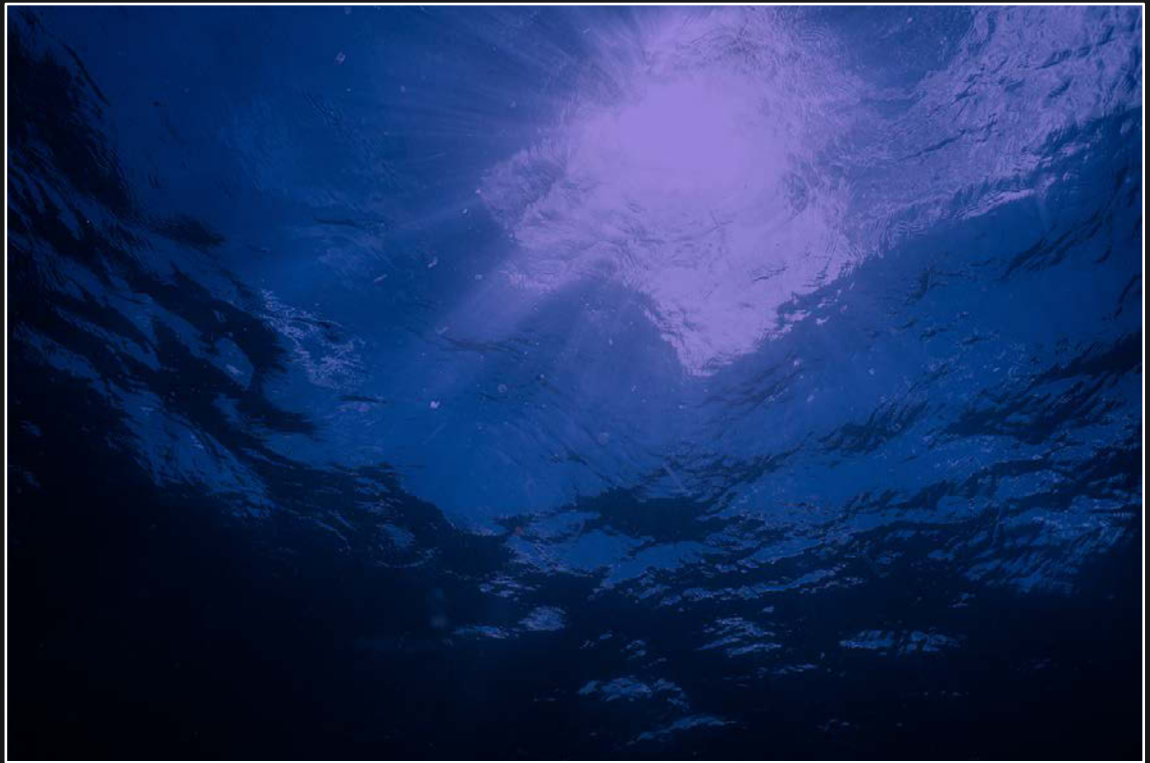
Terrence “Terry” McGraw is a retired Lieutenant Colonel from the United States Army and now serves as Vice President of Global Cyber Threat Analysis with over 20 years of providing expertise in cyber security architectural design and operations in both commercial and government sectors.

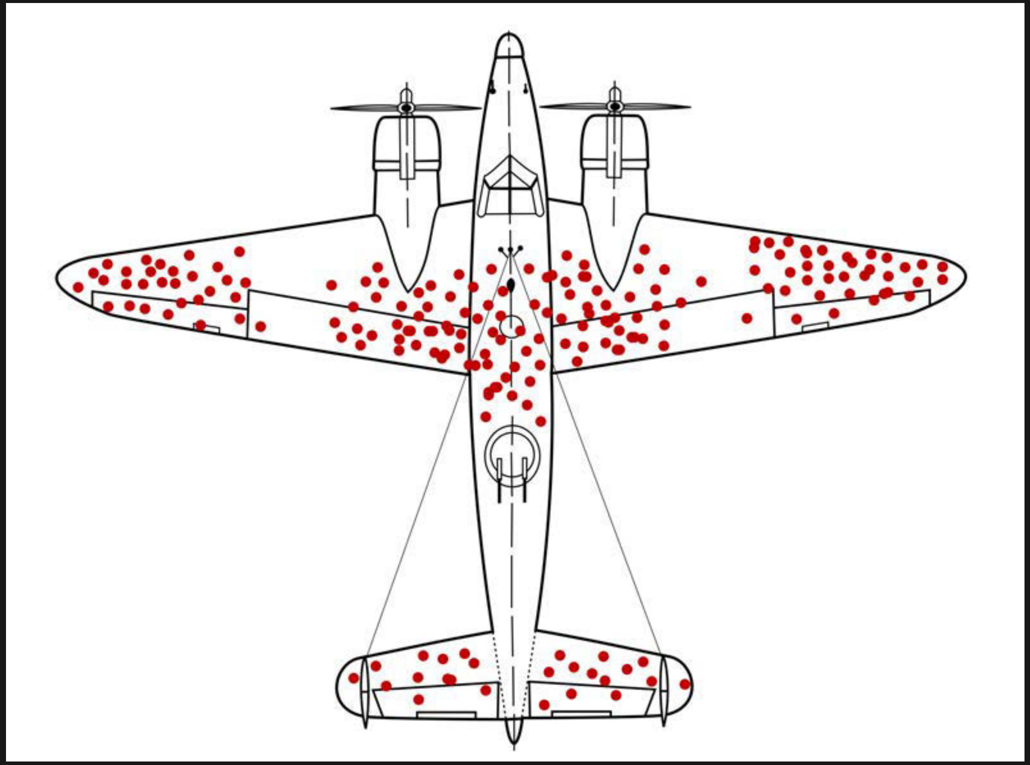
Terry previously served as president and principal consultant for Cape Endeavors, LLC, the Vice President of Global Cyber Threat Research and Analysis for Dell SecureWorks. He retired from the United States Army in 2014 completing 27 years of service; the last 10 years of his Army career were leading key Cyber initiatives for the Army’s Network Enterprise and Technology Command, Army Cyber Command and the National Security Agency (NSA). He has multiple combat tours with his culminating assignment, serving as the Director of Operations, Task Force Signal Afghanistan, 160th Signal Brigade (FWD), providing all strategic communications infrastructure in the theater of operations.

Classification: //Secureworks/Public Use

Why is Threat Intelligence so Important

Snell’s Window and Survivorship Bias





https://en.wikipedia.org/wiki/Survivorship_bias

https://epod.usra.edu/blog/2014/06/snells-window.html

Secureworks Today

$476M
LTM Revenue[1]

$222M
Taegis™ Platform ARR[2]

4,500+
Customers

20+ Years
Threat Actor Intelligence and Security Research

580B+
Daily Events Processed

1,800+
Teammates Across the Globe

~98%
MITRE ATT&CK® Framework Coverage

Industry Leader
Gartner, Forrester, IDC, Frost & Sullivan

200+
Threat Groups Monitored

~1,400
Incident Response and Adversarial Testing Engagements Annually

[1] Trailing revenue past 12 quarters reported in Q3 FY23 Earnings
[2] Reported revenue for Taegis in Q3 FY23 Earnings

Cybersecurity Threats

OPPORTUNISTIC

Organized Crime

Profit-motivated, looking to monetize access and/or stolen information

Financially-motivated: Targeting high-profile sectors and industries

TARGETED

Insider Threat

Involves theft of IP/trade secrets, competitive analysis, and/or prospect, customer, or market information

Various Motives: Personal benefit, disgruntled employee takes revenge, general recklessness

Nation-state

Traditional espionage that has moved into the cyber domain, disinformation campaigns, destructive attacks.

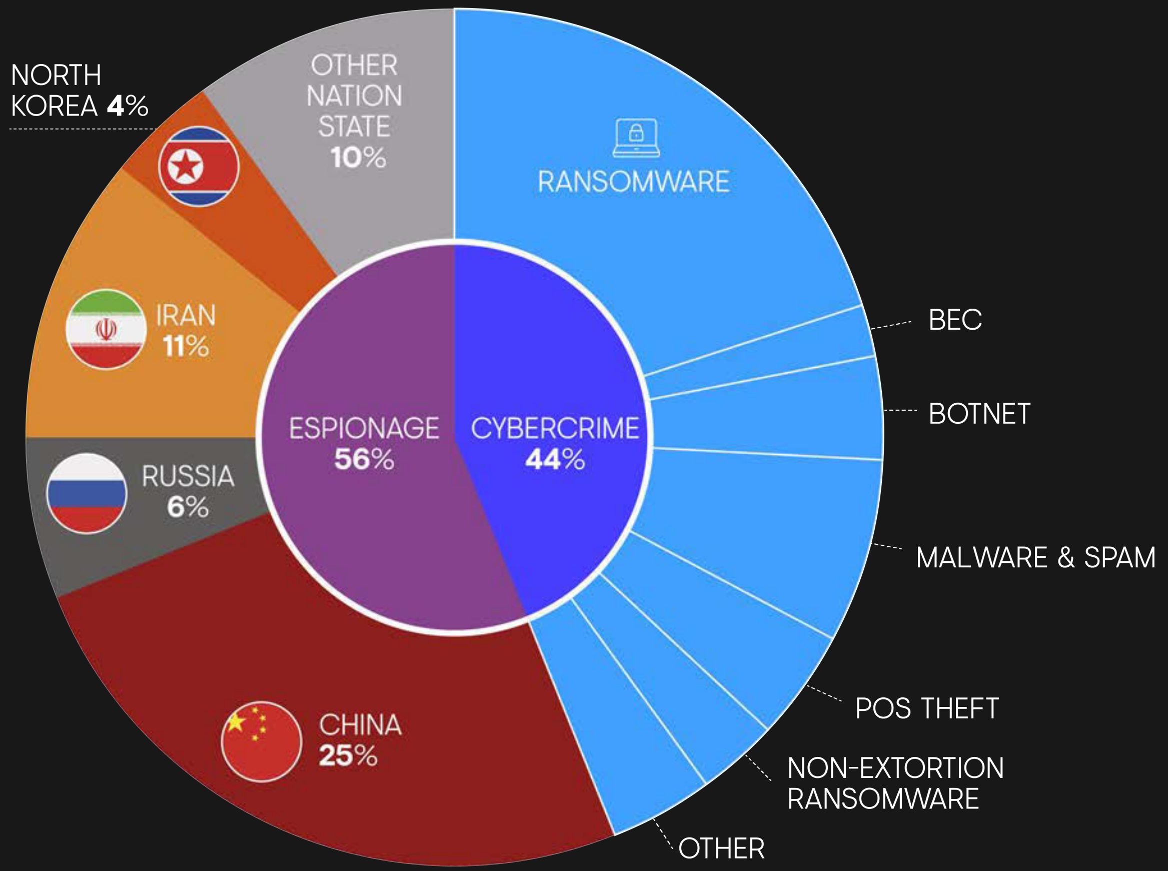
Two main types: National security-driven and commercial / economic espionage

Hacktivist

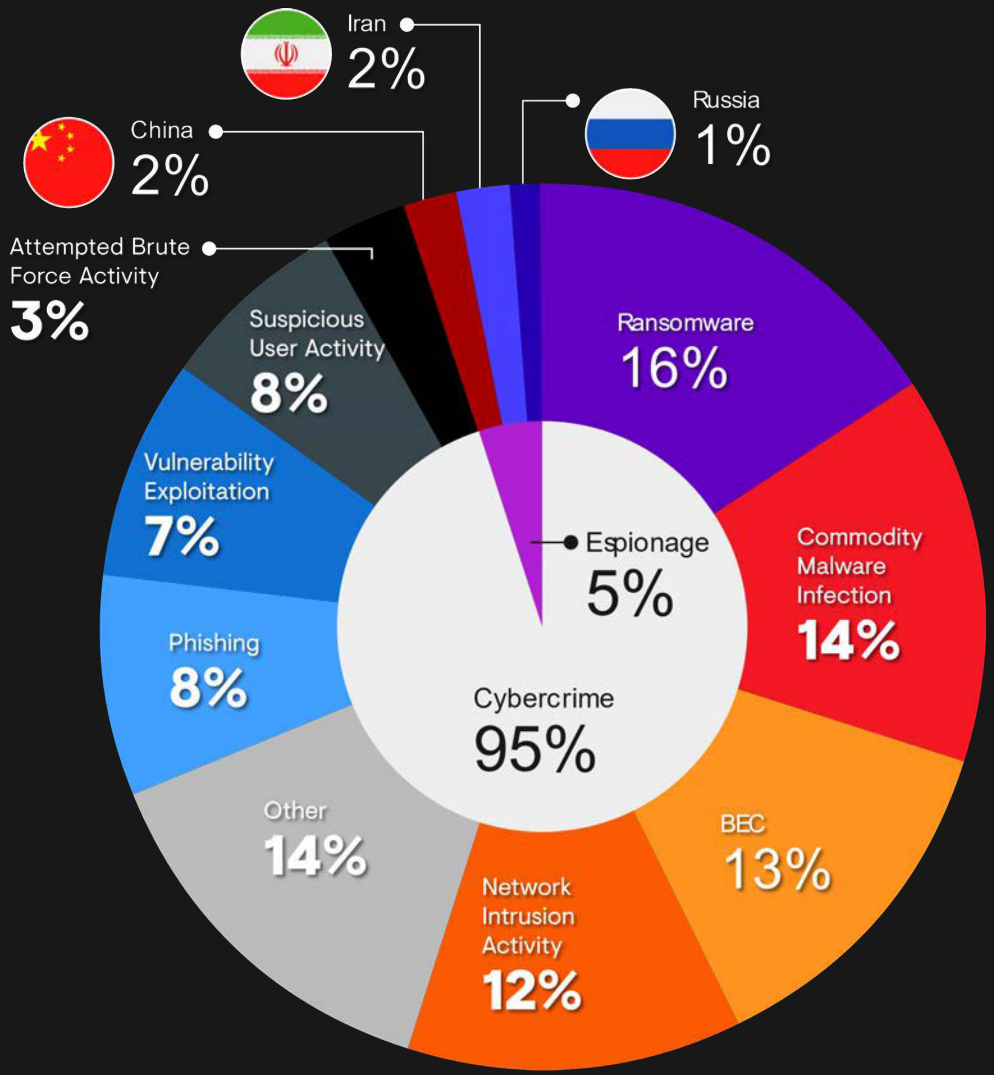
Issue-motivated, aiming to distract, expose, embarrass or inflict public harm

Disruption/ Embarrassment: to make a point and raise awareness

The Threat Landscape



Active Threat Groups

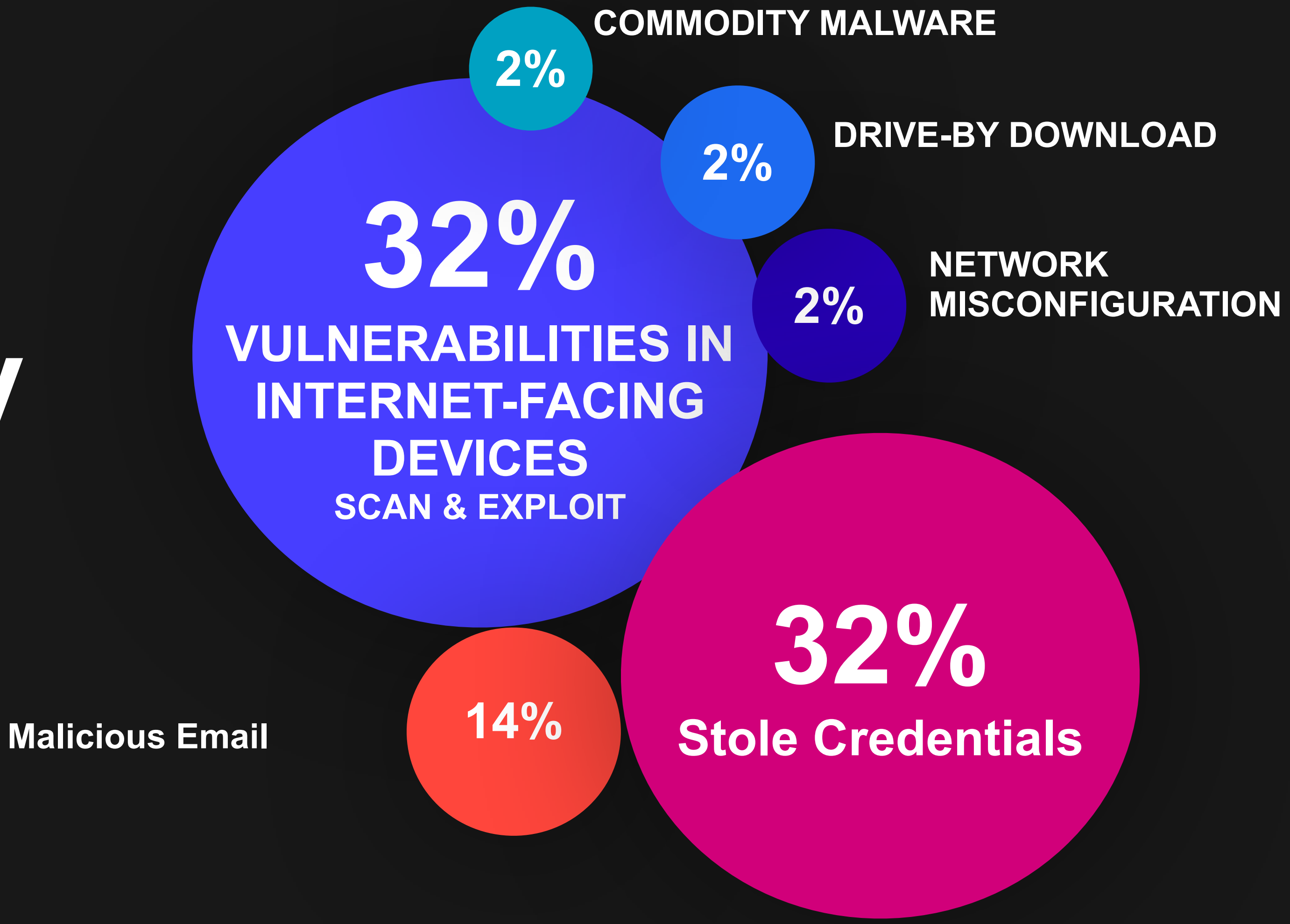


Incidents

Classification: //Secureworks/Public Use

Q2 2022/23 - Initial Access Vectors (IAV)

How are they getting in?



Classification: //Secureworks/Public Use

The Ransomware Ecosystem

Operators & Developers

- Operators handle the business side.
- Developers write the ransomware and decryption software.
- Supply privately or offer on Ransomware-as-a-service (RaaS) basis.

Affiliates

- Partners of the ransomware Operators. Selected based on Operator requirements.
- Top tier RaaS Operators seek the best Affiliates.
- Affiliates access targets and deploy the ransomware. May also steal data in bulk.

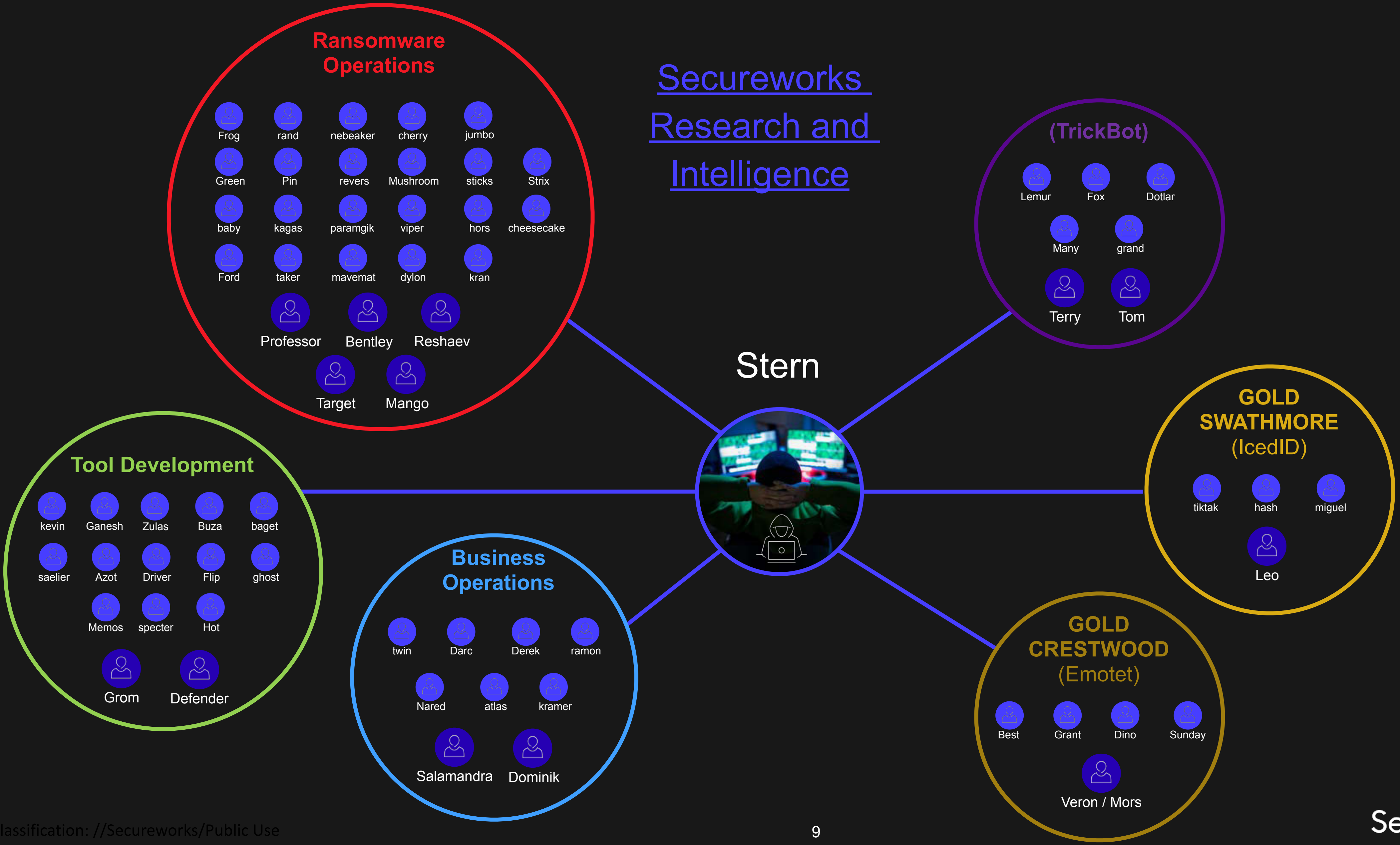
Initial Access Brokers

- Specializes in supplying access to Affiliates.
- Exploits 0-day, N-day and poor security practices to gain access to victims.
- Access is sold to Affiliates for further exploitation.

Classification: //Secureworks/Public Use

The Cybercrime Ecosystem

[Secureworks Research and Intelligence]



Ransomware Operations

Frog, rand, nebeaker, cherry, jumbo, Green, Pin, revers, Mushroom, sticks, Strix, baby, kagas, paramgik, viper, hors, cheesecake, Ford, taker, mavemat, dylon, kran, Professor, Bentley, Reshaev, Target, Mango

(TrickBot)

Lemur, Fox, Dotlar, Many, grand, Terry, Tom

Stern

GOLD SWATHMORE (IcedID)

tiktak, hash, miguel, Leo

Tool Development

kevin, Ganesh, Zulas, Buza, baget, saelier, Azot, Driver, Flip, ghost, Memos, specter, Hot, Grom, Defender

Business Operations

twin, Darc, Derek, ramon, Nared, atlas, kramer, Salamandra, Dominik

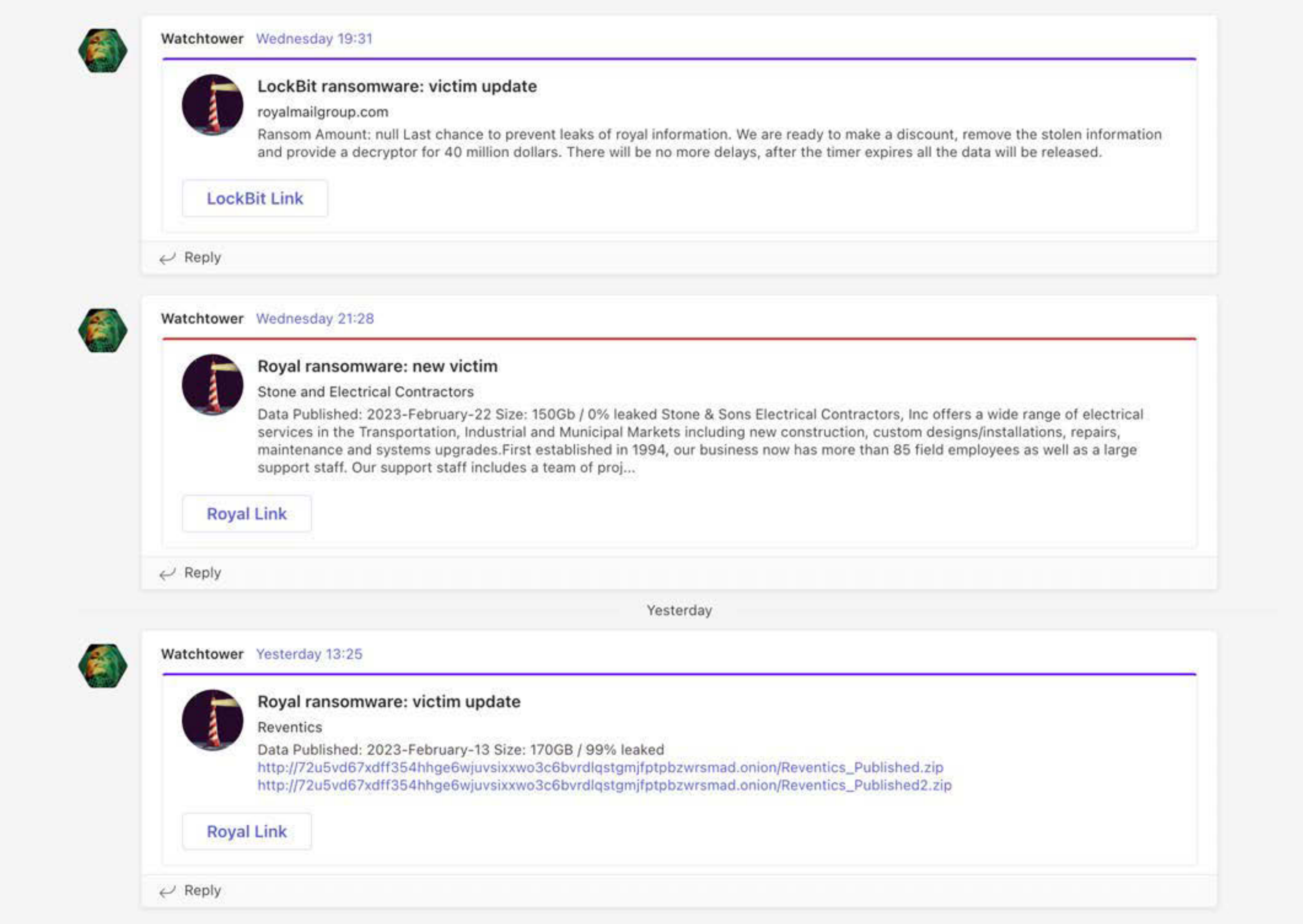
GOLD CRESTWOOD (Emotet)

Best, Grant, Dino, Sunday, Veron / Mors

Classification: //Secureworks/Public Use

Classification: //Secureworks/Public Use

Ransomware in numbers – 2022 Leak Site Data



Watchtower Wednesday 19:31

LockBit ransomware: victim update

royalmailgroup.com

Ransom Amount: null Last chance to prevent leaks of royal information. We are ready to make a discount, remove the stolen information and provide a decryptor for 40 million dollars. There will be no more delays, after the timer expires all the data will be released.

Watchtower Wednesday 21:28

Royal ransomware: new victim

Stone and Electrical Contractors

Data Published: 2023-February-22 Size: 150Gb / 0% leaked Stone & Sons Electrical Contractors, Inc offers a wide range of electrical services in the Transportation, Industrial and Municipal Markets including new construction, custom designs/installations, repairs, maintenance and systems upgrades.First established in 1994, our business now has more than 85 field employees as well as a large support staff. Our support staff includes a team of proj...

Yesterday

Watchtower Yesterday 13:25

Royal ransomware: victim update

Reventics

Data Published: 2023-February-13 Size: 170GB / 99% leaked
http://72u5vd67xdff354hhge6wjuvsixxwo3c6bvrdlqstgmjfptpbzwrsmad.onion/Reventics_Published.zip
http://72u5vd67xdff354hhge6wjuvsixxwo3c6bvrdlqstgmjfptpbzwrsmad.onion/Reventics_Published2.zip

2914

Hive : 1500 victims, 209 on leak site implies that 87% of victims paid

Avaddon: 3000 victims, 182 on leak site implies that 94% of victims paid

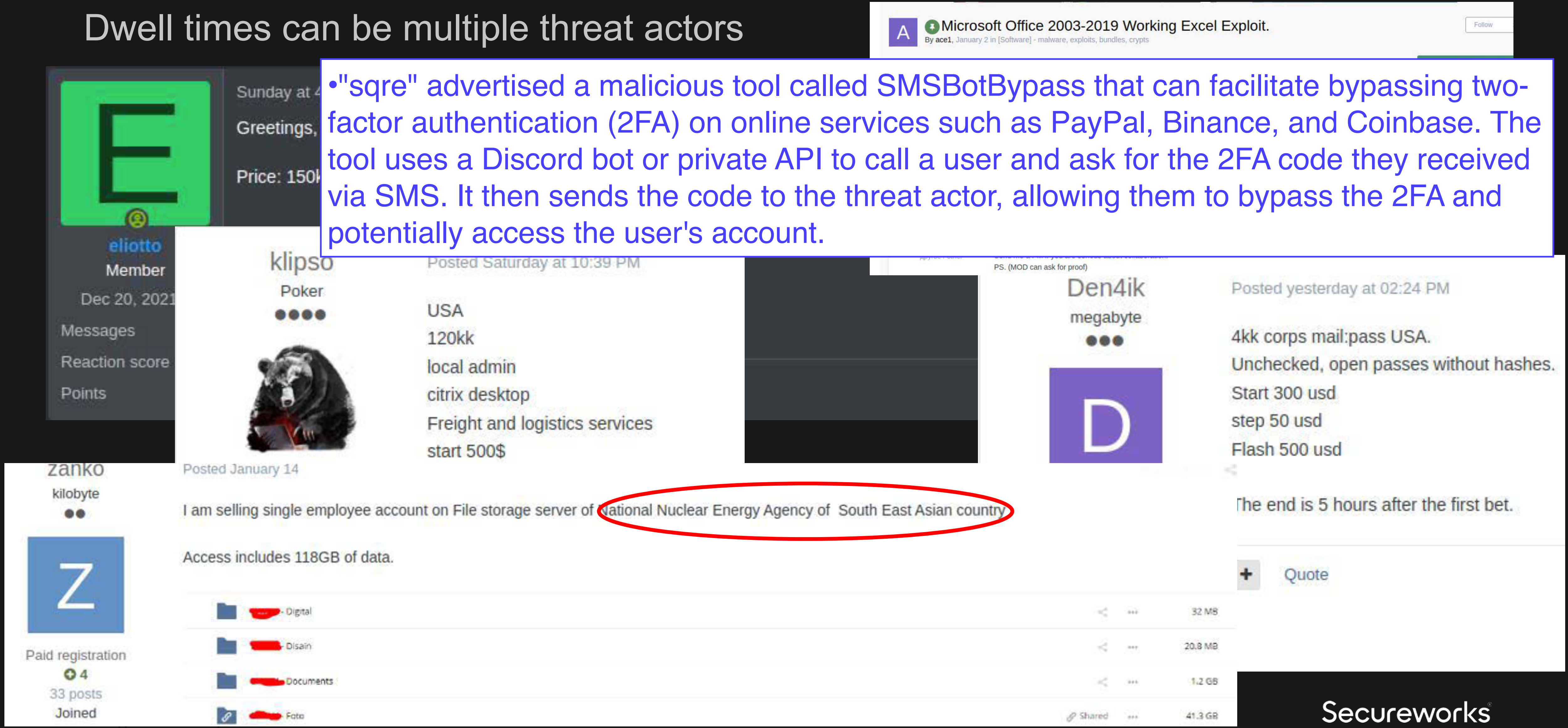
Potentially 30,000 victims of ransomware in 2022

Classification: //Secureworks/Public Use

[Threat Intelligence Publication - XDR (secureworks.com)](https://www.secureworks.com)

Initial Access Brokers

Dwell times can be multiple threat actors



•"sqre" advertised a malicious tool called SMSBotBypass that can facilitate bypassing two-factor authentication (2FA) on online services such as PayPal, Binance, and Coinbase. The tool uses a Discord bot or private API to call a user and ask for the 2FA code they received via SMS. It then sends the code to the threat actor, allowing them to bypass the 2FA and potentially access the user's account.

A Microsoft Office 2003-2019 Working Excel Exploit.
By ace1, January 2 in [Software] - malware, exploits, bundles, crypts

PS. (MOD can ask for proof)

eliotto
Member
Dec 20, 2021
Messages
Reaction score
Points

Sunday at 4

Greetings,

Price: 150k

klipso
Poker

Posted Saturday at 10:39 PM

USA
120kk
local admin
citrix desktop
Freight and logistics services
start 500$

Den4ik
megabyte

Posted yesterday at 02:24 PM

4kk corps mail:pass USA.
Unchecked, open passes without hashes.
Start 300 usd
step 50 usd
Flash 500 usd

The end is 5 hours after the first bet.

Quote

zanko
kilobyte
Paid registration
4
33 posts
Joined

Posted January 14

I am selling single employee account on File storage server of National Nuclear Energy Agency of South East Asian country

Access includes 118GB of data.

[redacted] Digital		32 MB
[redacted] Disain		20.8 MB
[redacted] Documents		1.2 GB
[redacted] Foto	Shared	41.3 GB

Secureworks

Loaders and Info Stealers

Lighter Weight, easier to obtain and use

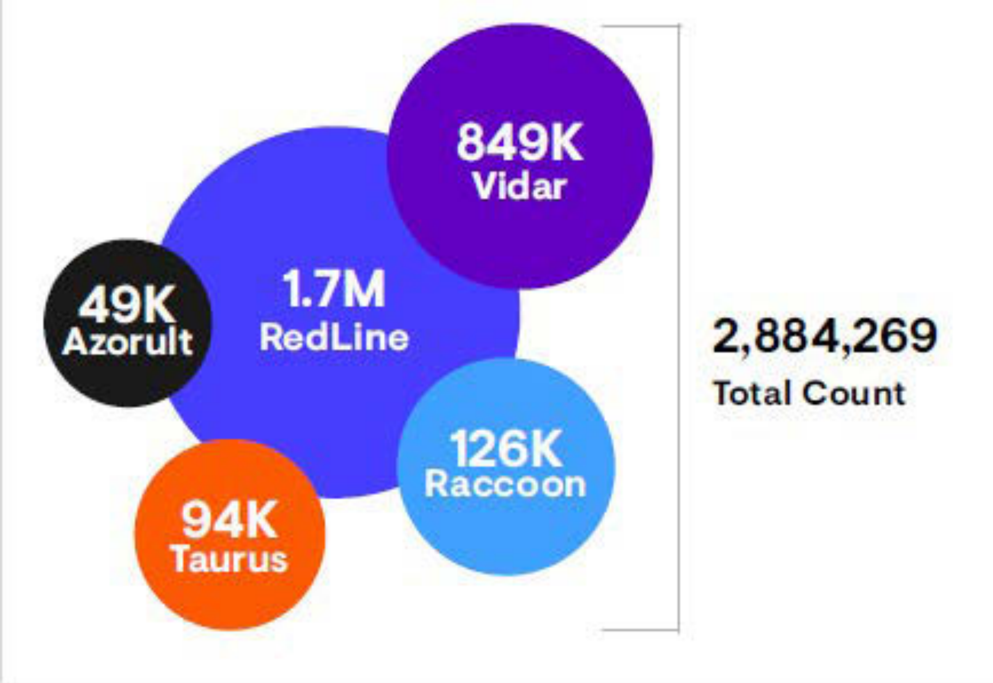
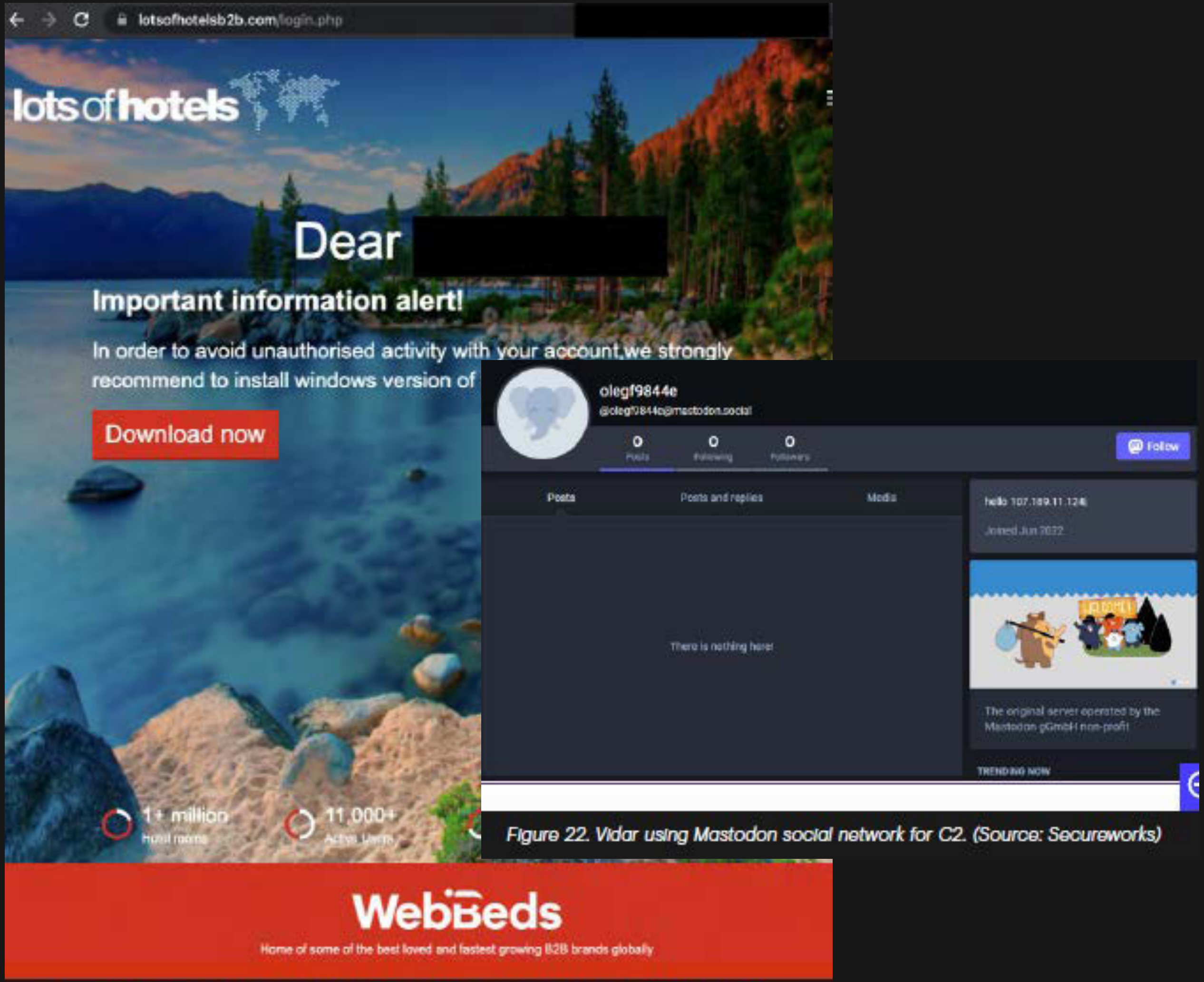


Figure 17. Logs from popular stealers for sale on Russian Market underground forum on June 2, 2022. (Source: Secureworks)



lotsofhotelsb2b.com/login.php [redacted]

Dear [redacted]

Important information alert!

In order to avoid unauthorised activity with your account,we strongly recommend to install windows version of

olegf9844e

@olegf9844e@mastodon.social

There is nothing here!

hello 107.189.11.124

Joined Jun 2022

The original server operated by the Mastodon gGmbH non-profit

Figure 22. Vidar using Mastodon social network for C2. (Source: Secureworks)

WebBeds
Home of some of the best loved and fastest growing B2B brands globally

Figure 21. Cloned website containing a security warning and download prompt for Redline payload. (Source: Secureworks)

Dwell Times

Better Tools and Market Maturation

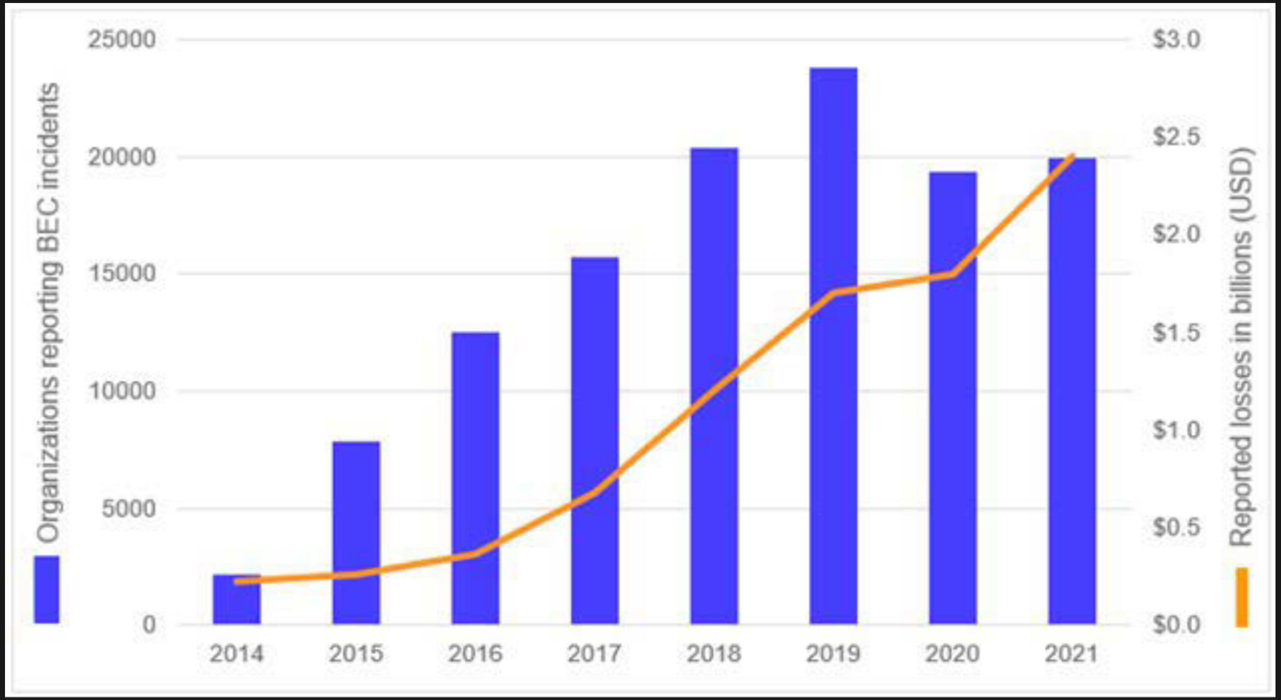
- 2015: Mean 270 days
- 2021: Mean 22 days
- 2022: Mean 11 days; Median was 4.5
- 2023: Mean 1 days; low was **5 hours**

Classification: //Secureworks/Public Use

Business Email Compromise (BEC)

Impacts and Losses

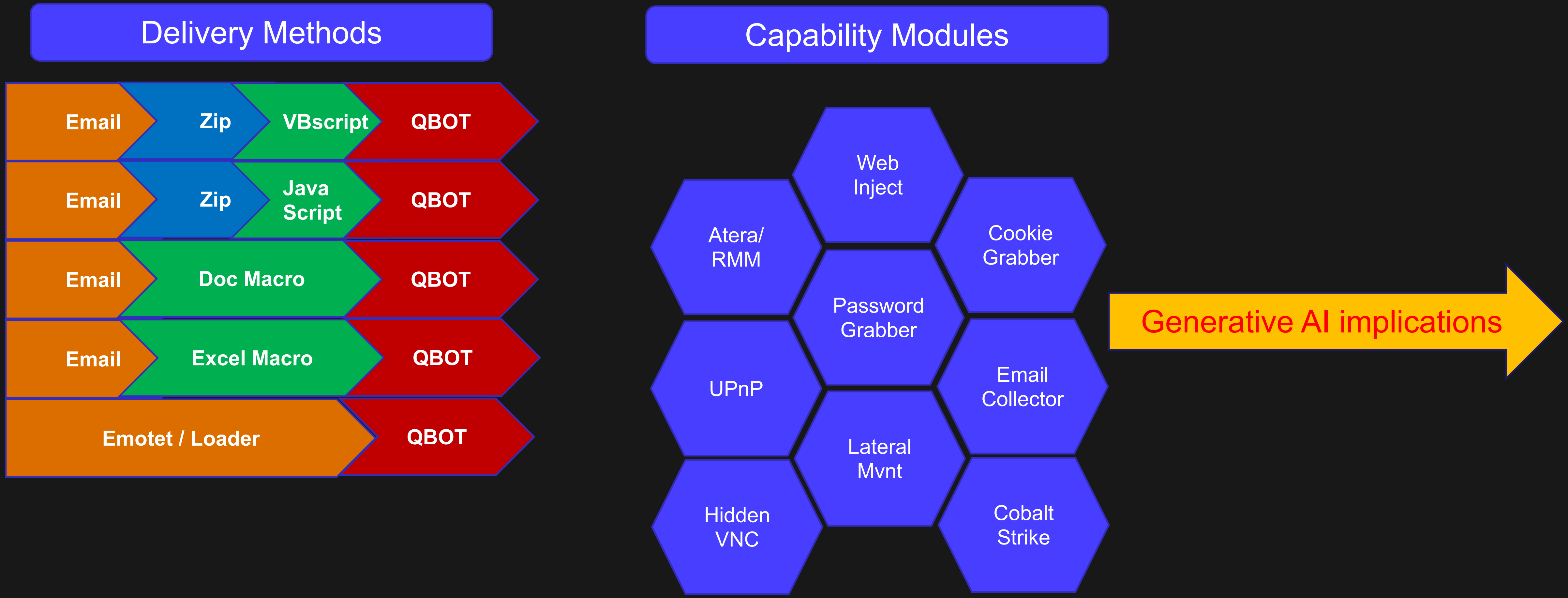
- Doubled in frequency last year
- Steady increase since 2014
- Global growth
- Drop off in 2020
- Global losses amounting to $43 billion since 2016



Organizations reporting BEC incidents and reported losses between 2014 and 2020. (Source: Secureworks, based on data from the Internet Crime Complaint Center (IC3))

Phishing Malware

Pressure testing your entire security architecture



Delivery Methods

Email Zip VBscript QBOT

Email Zip Java Script QBOT

Email Doc Macro QBOT

Email Excel Macro QBOT

Emotet / Loader QBOT

Capability Modules

Web Inject

Atera/ RMM

Cookie Grabber

Password Grabber

UPnP

Email Collector

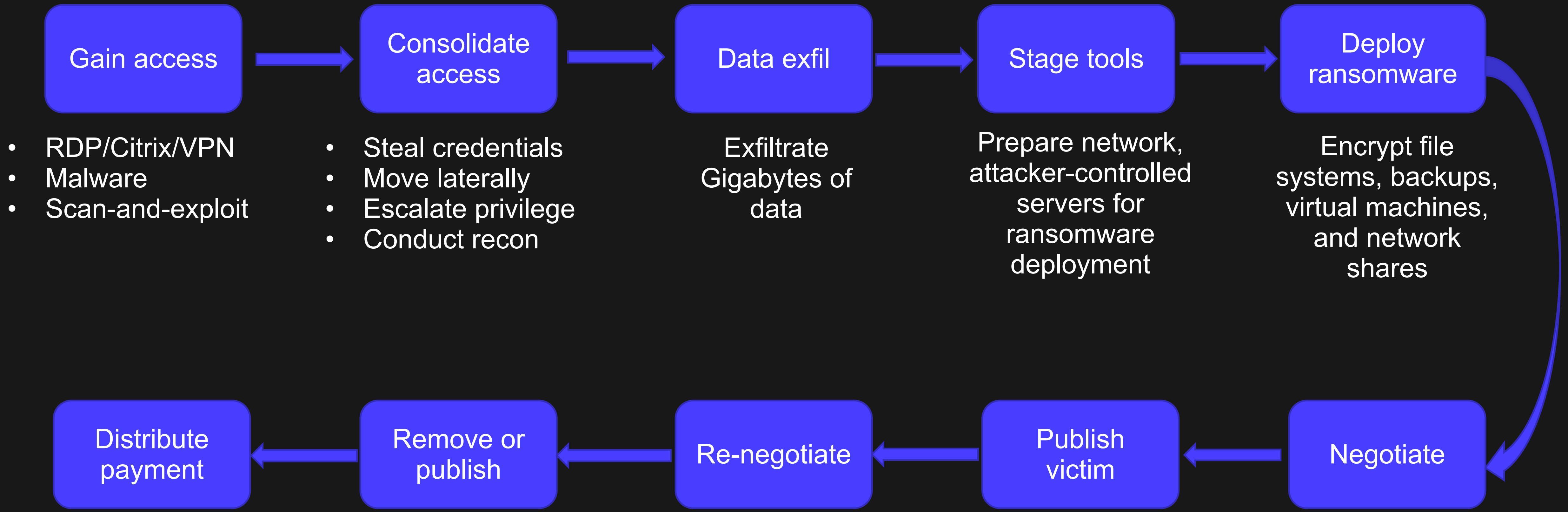
Lateral Mvnt

Hidden VNC

Cobalt Strike

Generative AI implications

Ransomware 'Name-and-Shame' Playbook



Gain access

- RDP/Citrix/VPN
- Malware
- Scan-and-exploit

Consolidate access

- Steal credentials
- Move laterally
- Escalate privilege
- Conduct recon

Data exfil

Exfiltrate Gigabytes of data

Stage tools

Prepare network, attacker-controlled servers for ransomware deployment

Deploy ransomware

Encrypt file systems, backups, virtual machines, and network shares

Negotiate

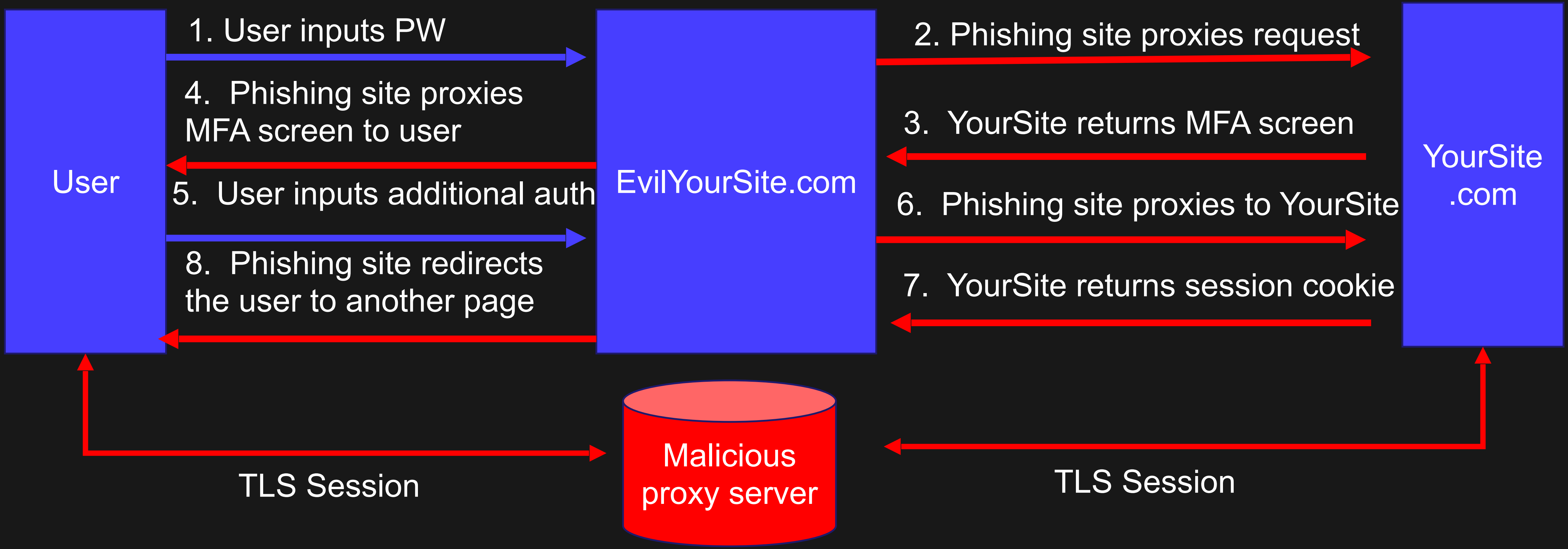
Publish victim

Re-negotiate

Remove or publish

Distribute payment

Attacker in the Middle- MFA Bypass



User
1. User inputs PW
4. Phishing site proxies MFA screen to user
5. User inputs additional auth
8. Phishing site redirects the user to another page
EvilYourSite.com
2. Phishing site proxies request
3. YourSite returns MFA screen
6. Phishing site proxies to YourSite
7. YourSite returns session cookie
YourSite .com
Malicious proxy server

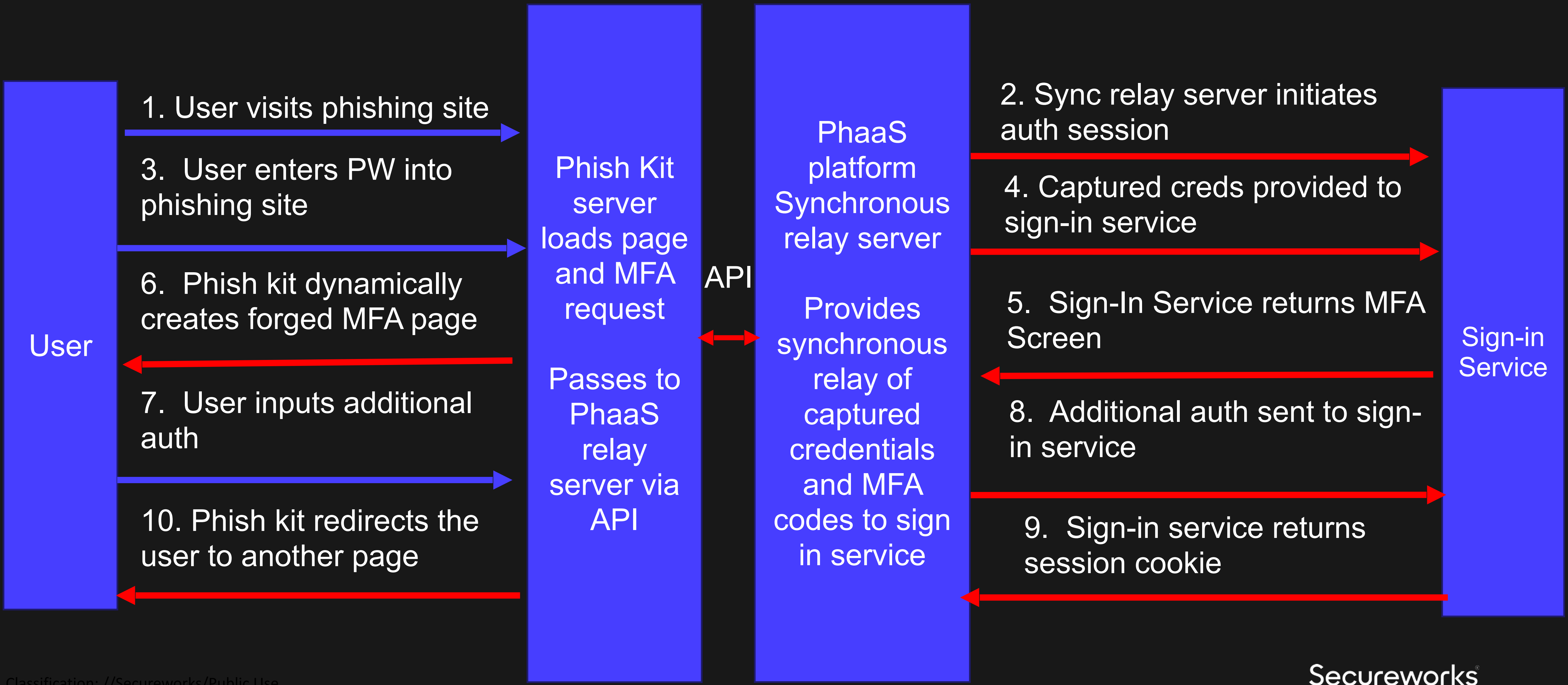
TLS Session

TLS Session

Classification: //Secureworks/Public Use

Attacker in the Middle- MFA Bypass

No Network traffic proxied



User

1. User visits phishing site

3. User enters PW into phishing site

6. Phish kit dynamically creates forged MFA page

7. User inputs additional auth

10. Phish kit redirects the user to another page

Phish Kit server loads page and MFA request

Passes to PhaaS relay server via API

API

PhaaS platform Synchronous relay server

Provides synchronous relay of captured credentials and MFA codes to sign in service

2. Sync relay server initiates auth session

4. Captured creds provided to sign-in service

5. Sign-In Service returns MFA Screen

8. Additional auth sent to sign-in service

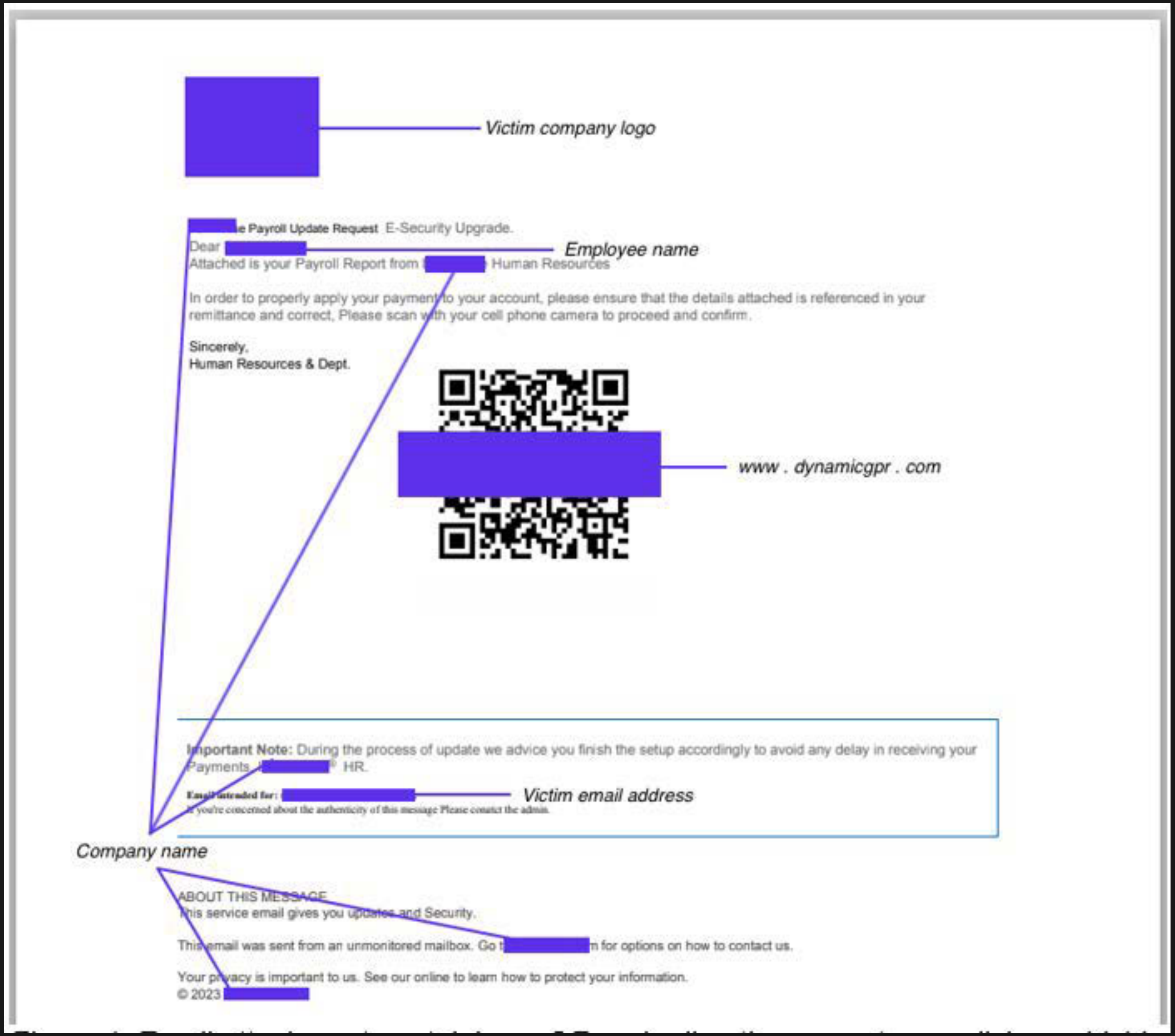
9. Sign-in service returns session cookie

Sign-in Service

Secureworks

QR code phishing

- Seeing increased volumes
- Bypasses mail filtering
- Phishing happens on user device, outside of corporate controls
- Can capture MFA tokens
- Can lead to Azure account access and BEC style fraud



[redacted]

[redacted]e Payroll Update Request E-Security Upgrade.
Dear [redacted]
Attached is your Payroll Report from [redacted] Human Resources

In order to properly apply your payment to your account, please ensure that the details attached is referenced in your remittance and correct, Please scan with your cell phone camera to proceed and confirm.

Sincerely,
Human Resources & Dept.

[redacted]

Important Note: During the process of update we advice you finish the setup accordingly to avoid any delay in receiving your Payments [redacted] HR.

Email intended for: [redacted]
If you're concerned about the authenticity of this message Please contact the admin.

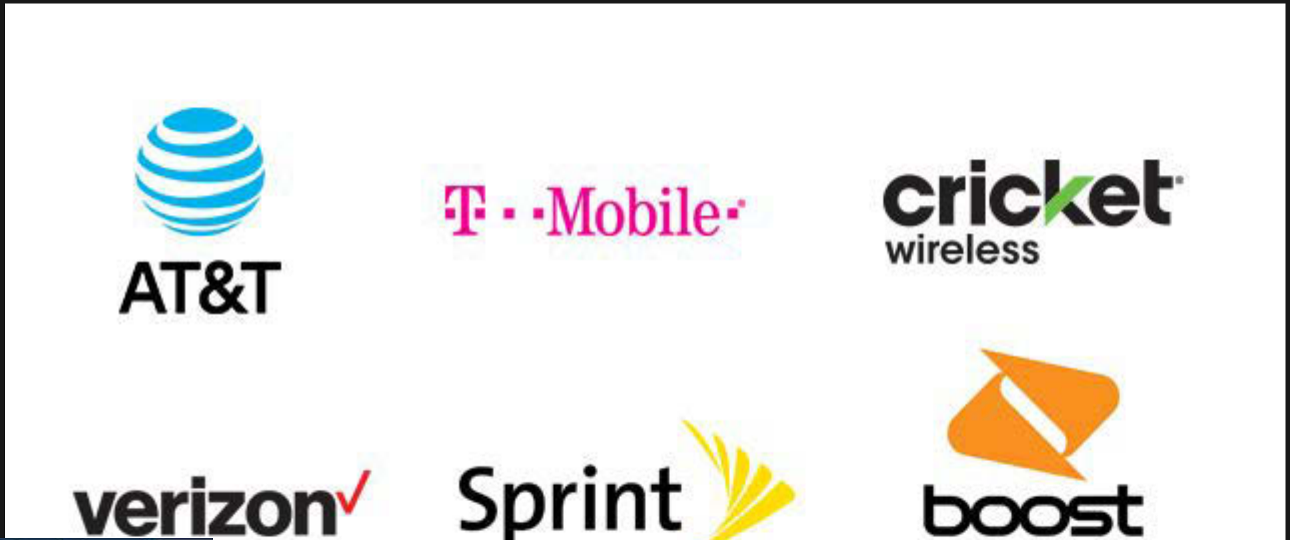
ABOUT THIS MESSAGE
This service email gives you updates and Security.

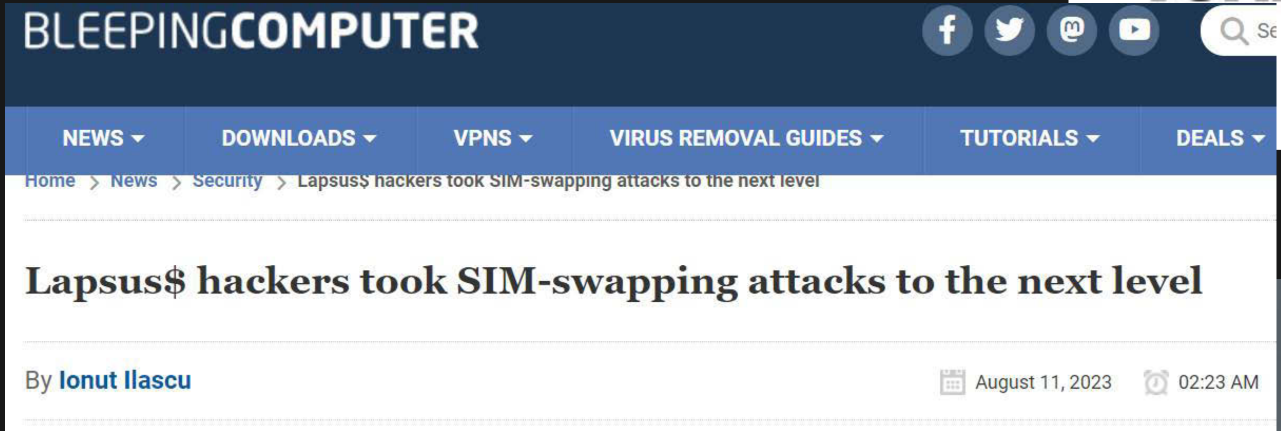
This email was sent from an unmonitored mailbox. Go t[redacted]m for options on how to contact us.

Your privacy is important to us. See our online to learn how to protect your information.
© 2023 [redacted]

Classification: //Secureworks/Public Use

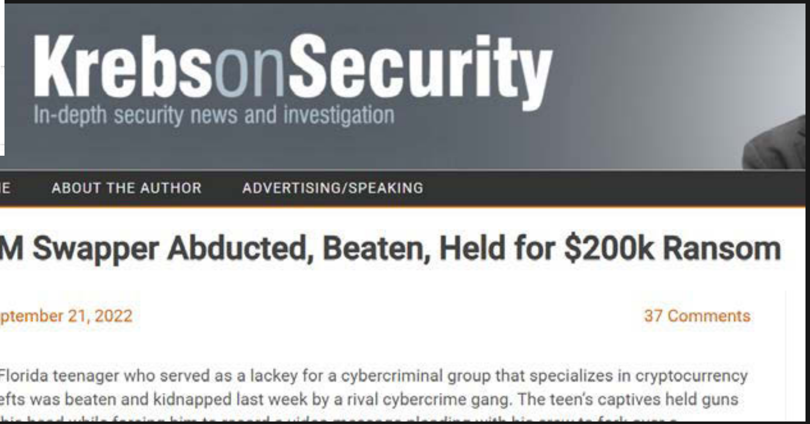
SIM Swapping




BLEEPINGCOMPUTER
NEWS
DOWNLOADS
VPNS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
Home > News > Security > Lapsus$ hackers took SIM-swapping attacks to the next level

Lapsus$ hackers took SIM-swapping attacks to the next level

By Ionut Ilascu August 11, 2023 02:23 AM



SIM Swapper Abducted, Beaten, Held for $200k Ransom

September 21, 2022 37 Comments

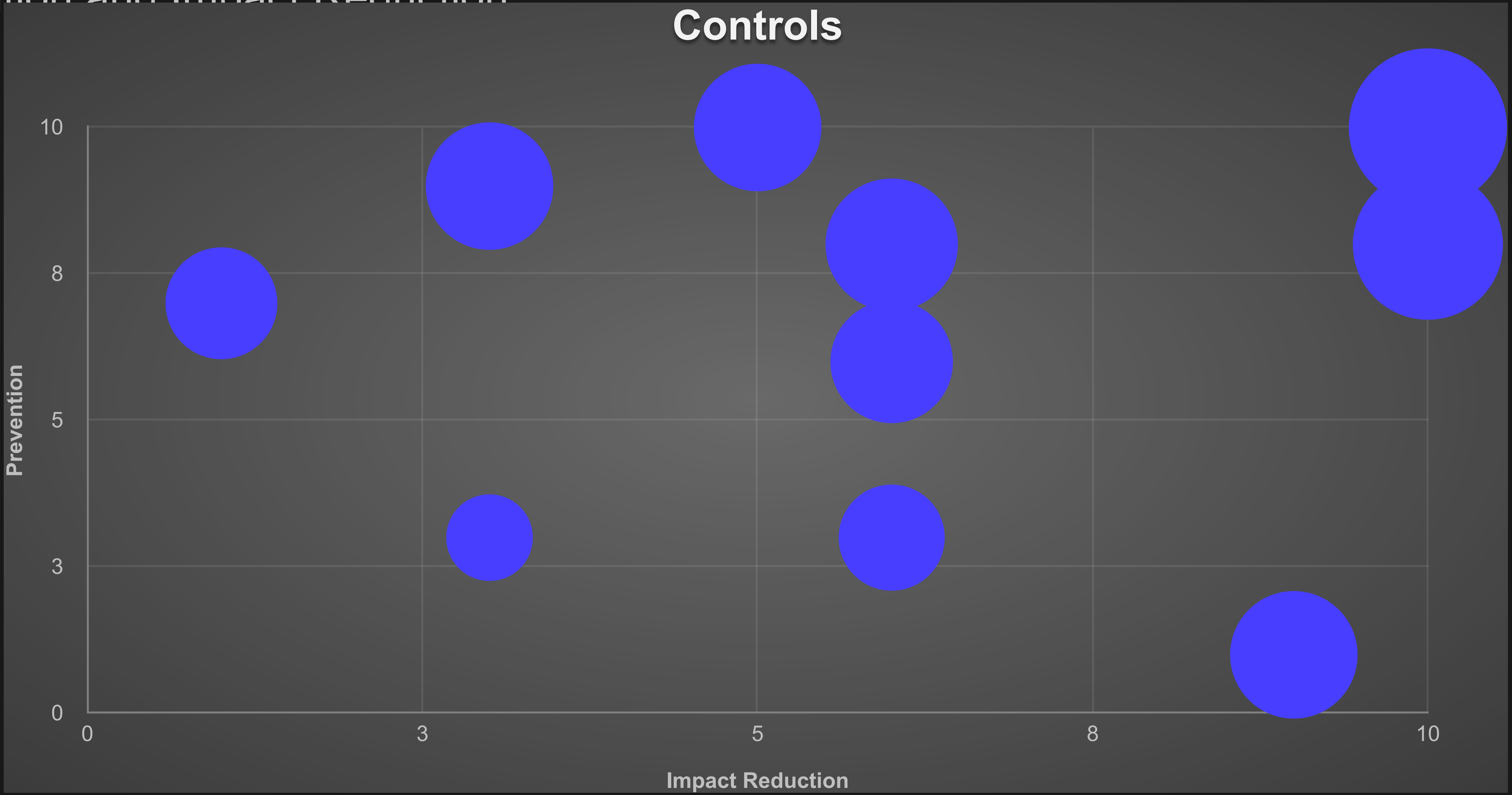
A Florida teenager who served as a lackey for a cybercriminal group that specializes in cryptocurrency thefts was beaten and kidnapped last week by a rival cybercrime gang. The teen's captives held guns

[FBI Tech Tuesday: SIM Swapping — FBI]()

Classification: //Secureworks/Public Use

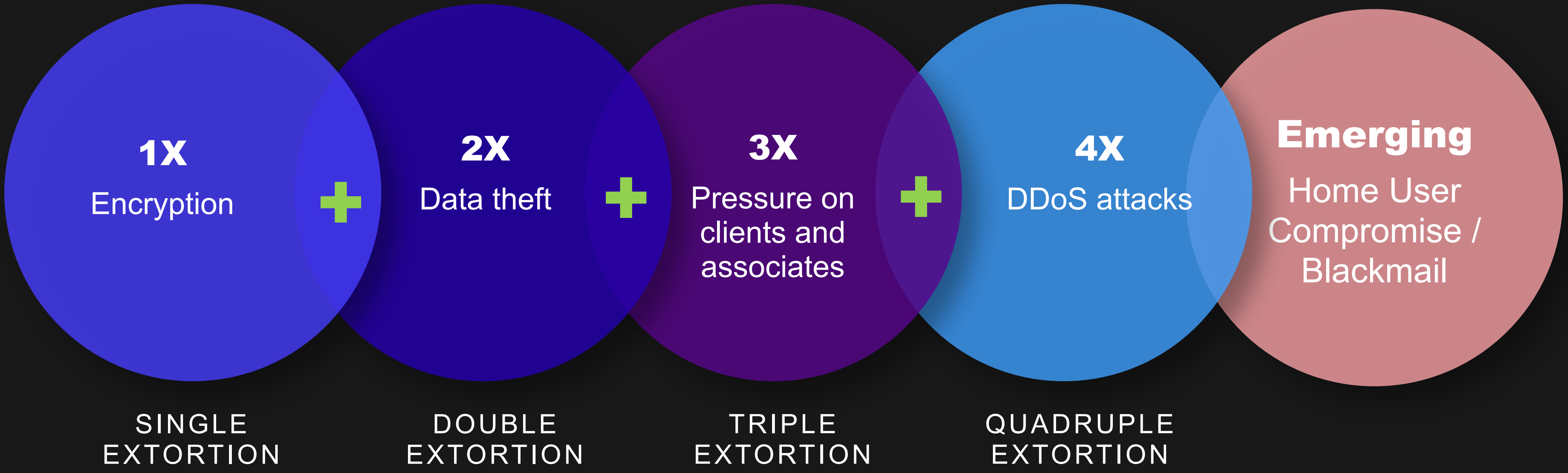
Top Security Controls

Prevention and Impact Reduction



Classification: //Secureworks/Public Use

The Truth about Ransomware Attacks



1X
Encryption

SINGLE EXTORTION

+

2X
Data theft

DOUBLE EXTORTION

+

3X
Pressure on clients and associates

TRIPLE EXTORTION

+

4X
DDoS attacks

QUADRUPLE EXTORTION

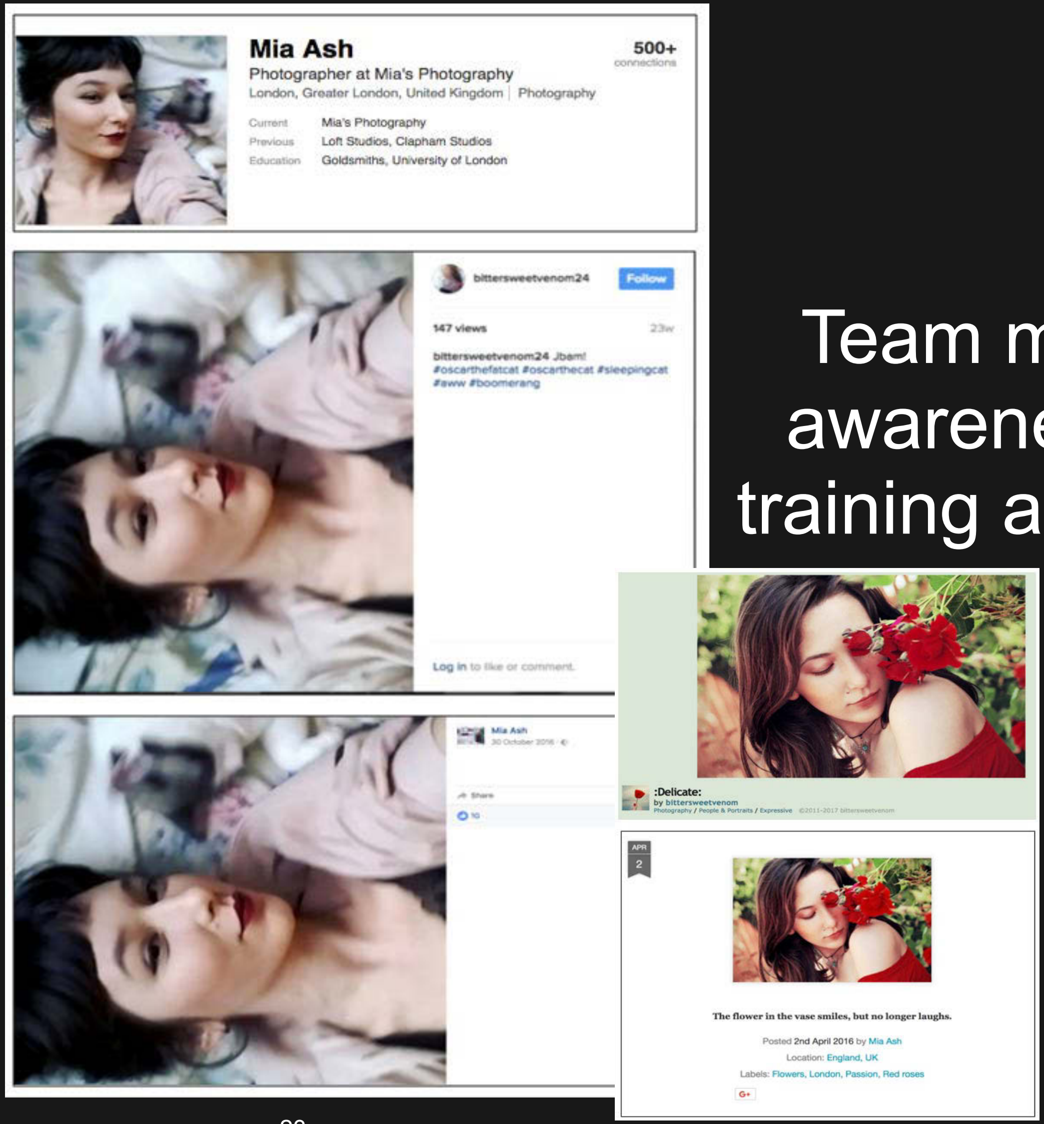
Emerging
Home User Compromise / Blackmail

Classification: //Secureworks/Public Use

The Curious Case of Mia Ash

Social Engineering works

- Phishing
- Smishing
- Catfishing
- MFA Fatigue
- Blackmail



Mia Ash

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

500+ connections

Current Mia's Photography

Previous Loft Studios, Clapham Studios

Education Goldsmiths, University of London

bittersweetvenom24 Follow

147 views 23w

bittersweetvenom24 Jbam! #oscarthefatcat #oscarthecat #sleepingcat #aww #boomerang

Log in to like or comment.

Mia Ash
30 October 2016

Share

10

:Delicate:
by bittersweetvenom
Photography / People & Portraits / Expressive ©2011-2017 bittersweetvenom

APR 2

The flower in the vase smiles, but no longer laughs.

Posted 2nd April 2016 by Mia Ash

Location: England, UK

Labels: Flowers, London, Passion, Red roses

G+

Team member awareness and training are critical

[The Curious Case of Mia Ash - COBALT GYPSY Threat Intelligence | Secureworks]

Thank You