proofpoint.

Byte-sized Battles in Cyberspace

TLP Green

Threats against Small and Medium-Businesses (SMB) and Non-Profit Organizations (NPO)

Sarah Sabotka

Senior Threat Researcher, Proofpoint Threat Research

Central Illinois Cybersecurity Summit
June 22, 2023

For Customer Use

Contents

Proofpoint Threat Research Program

- *Unofficial* mission statement
- Threat Research Data Landscape
- Threat Intelligence Production

The Threat Landscape

- The Victims
- The Threat Actors
- The How: Tactics, Techniques, and Procedures (TTPs)

Looking Ahead

- Social Engineering
- Top Tactics to Look For
- Know The Enemy
- Protect Yourself

The Threat Landscape

For Customer Use

Email is still a threat actor’s #1 preferred attack vector.

https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

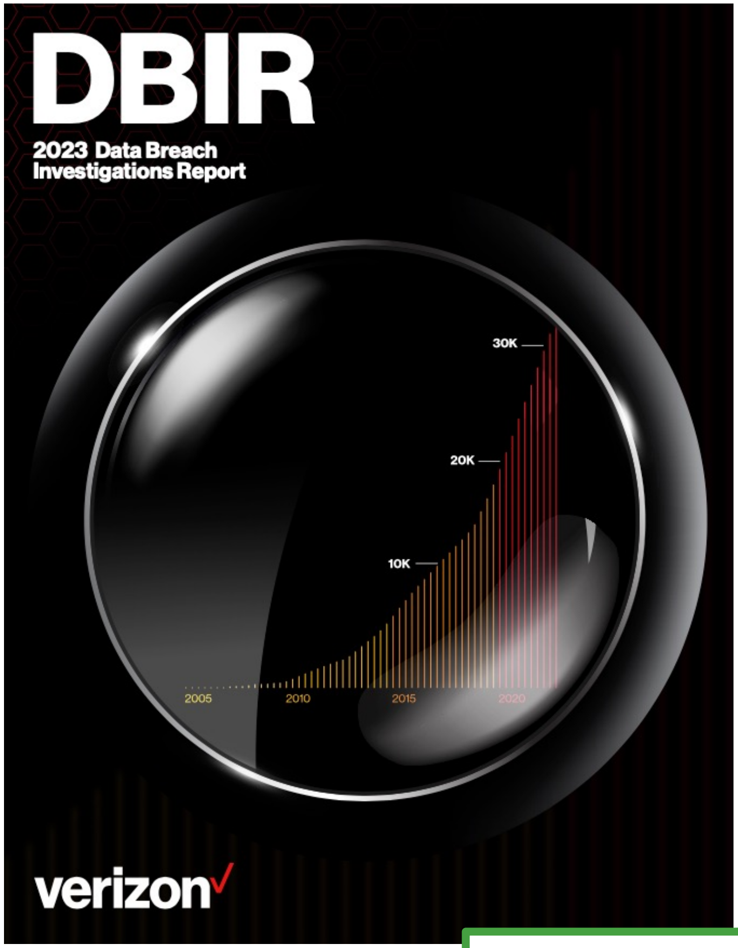
For Customer Use

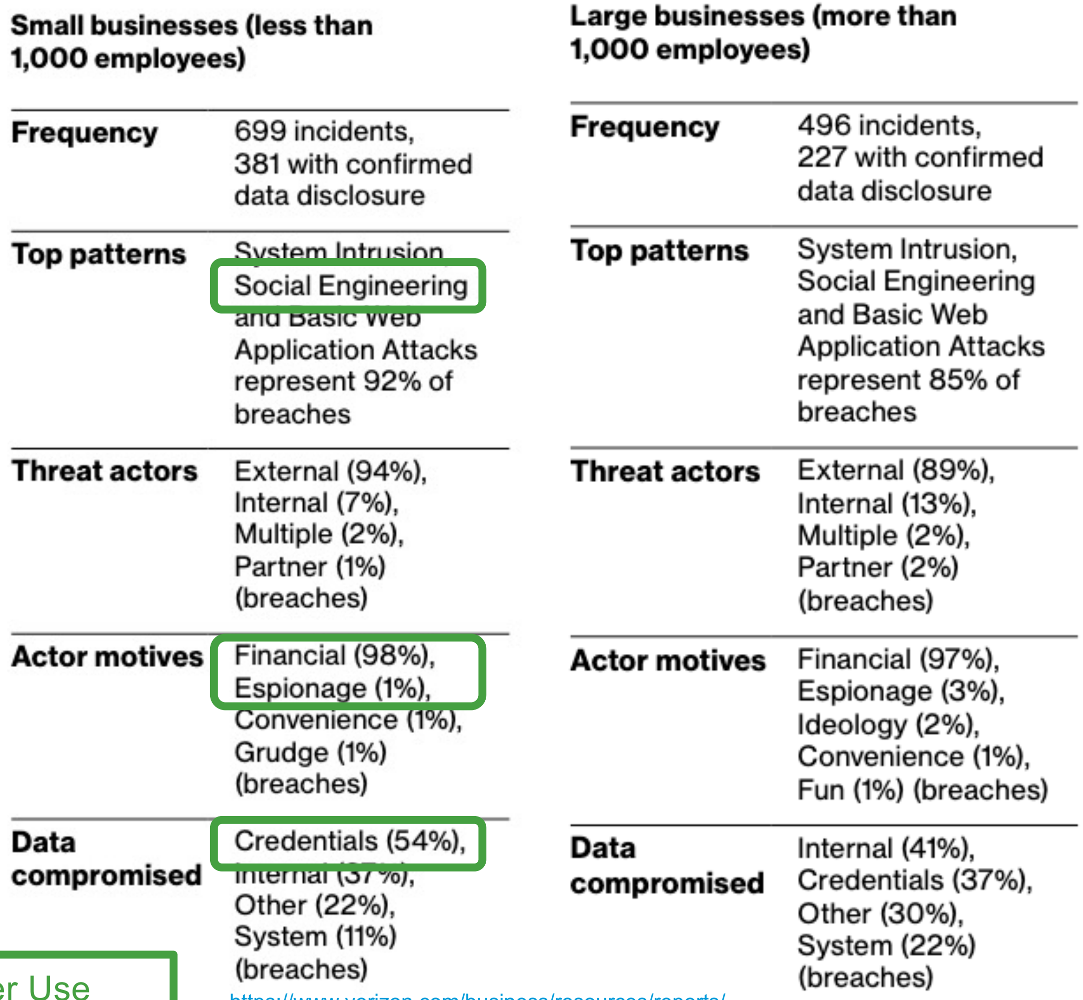
The Victims

Why SMBs and NPOs?

- Supply chain attacks – could your org be leveraged within a longer attack chain?
- Compromised infrastructure/accounts are always valuable.
- Likelihood of persistence, remain undetected for longer.
- Fewer resources
- “Soft target”
- Financially-driven objectives $

For Customer Use





Small businesses (less than 1,000 employees)	
Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

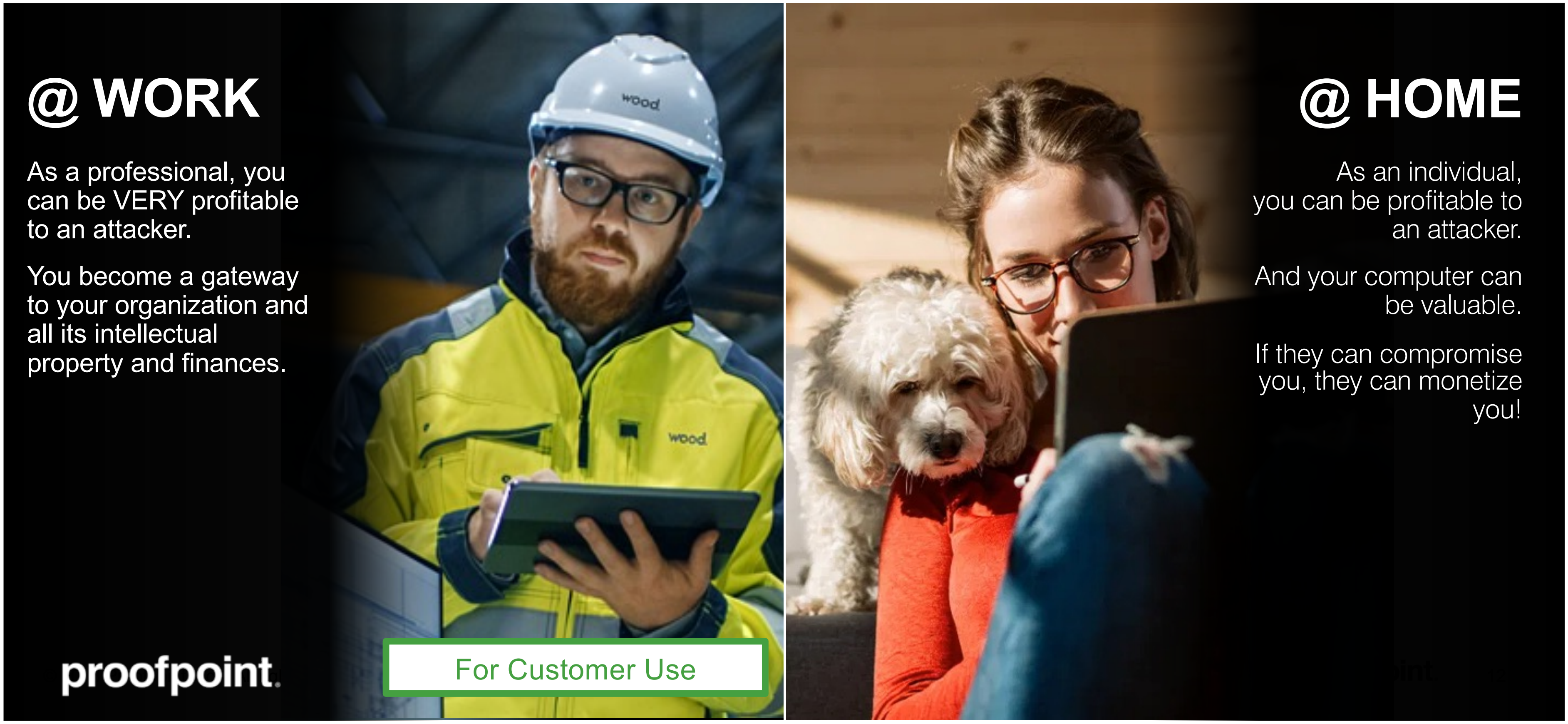
Large businesses (more than 1,000 employees)	
Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

For Customer Use

https://www.proofpoint.com/us/resources/threat-reports/2022-social-engineering-report

Are You a Target? We all are.



@ WORK

As a professional, you can be VERY profitable to an attacker.

You become a gateway to your organization and all its intellectual property and finances.

proofpoint.

For Customer Use

@ HOME

As an individual, you can be profitable to an attacker.

And your computer can be valuable.

If they can compromise you, they can monetize you!

The Threat Actors

Threat Types		Actor Types	
Malware	Malicious code that executes on end user systems	E-Crime	Financially-Motivated
Cred Harv	Theft of user credentials	APT	State-Aligned (espionage activities, etc.)
BEC	Pure Social Engineering perpetrating fraud	Hacktivism	Hacktivism, politically, and socially motivated

For Customer Use

Threat Actors Examples

E-Crime

Financially-Motivated

TA4903

Financially-motivated, BEC actor. Notable for spoofing various U.S. government entities in the pursuit of corporate credentials.

TA569

Injects malicious code into legitimate and high-traffic websites; profiles users before delivering malware to specific victims.

TA570

Initial Access Broker (IAB); objectives are to deliver and install various malware to attain and sell access to compromised machines to other threat actor groups (i.e. ransomware operators).

TA2536

Tracked for many years, financially-motivated threat actor most often observed using commodity keylogging malware to steal credentials.

For Customer Use

Threat Actor Examples

APT

APT/State-Aligned

TA473

(RU, aka Winter Vivern): phishing campaigns targeted US and European gov’t entities, Nov 2022-Feb 2023 – leveraged compromised SMB infrastructure.

TA444

(NK) phishing campaign targeting a medium-sized digital banking institution, impersonating ABF Capital, to deliver backdoor malware for the goal of financial theft.

TA450

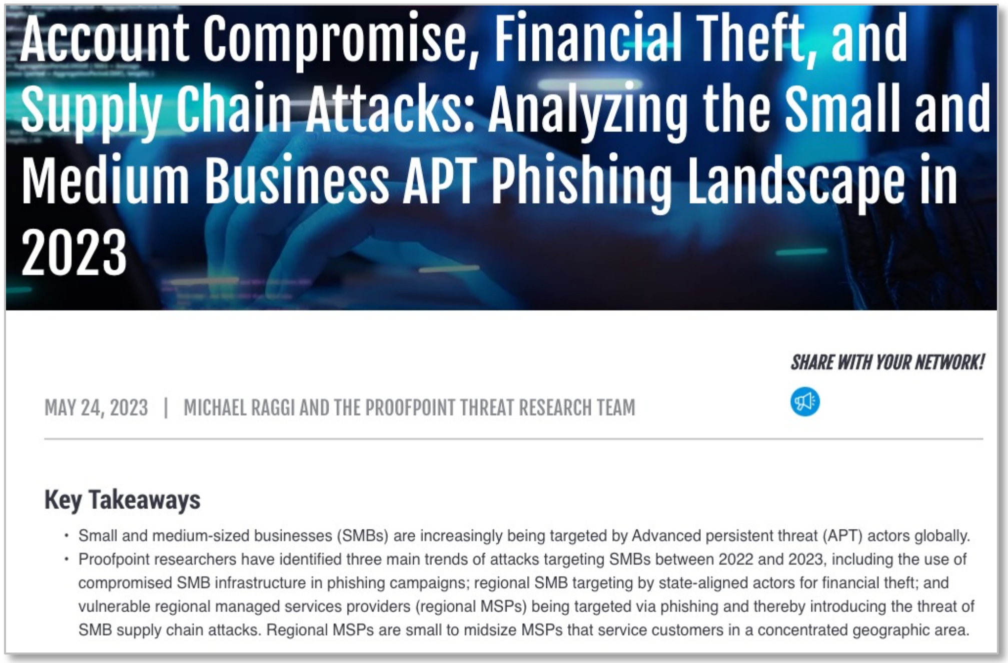
(IR) Phishing campaign targeting two Israeli regional MSPs and IT support businesses, with the goal of gaining access to downstream SMB users.

https://www.proofpoint.com/us/blog/threat-insight/small-and-medium-business-APT-phishing-landscape-in-2023

For Customer Use

Threat Insight: APT Trends in Targeting SMBs

This study looked at data from 200,000+ SMB organizations over the course of one year.



Account Compromise, Financial Theft, and Supply Chain Attacks: Analyzing the Small and Medium Business APT Phishing Landscape in 2023

MAY 24, 2023 | MICHAEL RAGGI AND THE PROOFPOINT THREAT RESEARCH TEAM

Key Takeaways

- Small and medium-sized businesses (SMBs) are increasingly being targeted by Advanced persistent threat (APT) actors globally.
- Proofpoint researchers have identified three main trends of attacks targeting SMBs between 2022 and 2023, including the use of compromised SMB infrastructure in phishing campaigns; regional SMB targeting by state-aligned actors for financial theft; and vulnerable regional managed services providers (regional MSPs) being targeted via phishing and thereby introducing the threat of SMB supply chain attacks. Regional MSPs are small to midsize MSPs that service customers in a concentrated geographic area.

https://www.proofpoint.com/us/blog/threat-insight/small-and-medium-business-APT-phishing-landscape-in-2023

For Customer Use

SMB Study Key Observations

1. APT actors used compromised SMB infrastructure in phishing campaigns;

2. APT actors engaged in targeted state-aligned, financially-motivated attacks against SMB financial services;

3. APT actors targeted SMBs to initiate supply chain attacks.

https://www.proofpoint.com/us/blog/threat-insight/small-and-medium-business-APT-phishing-landscape-in-2023

For Customer Use

The Tools: Tactics, Techniques, and Procedures (TTPs)

Email threats start with social engineering…

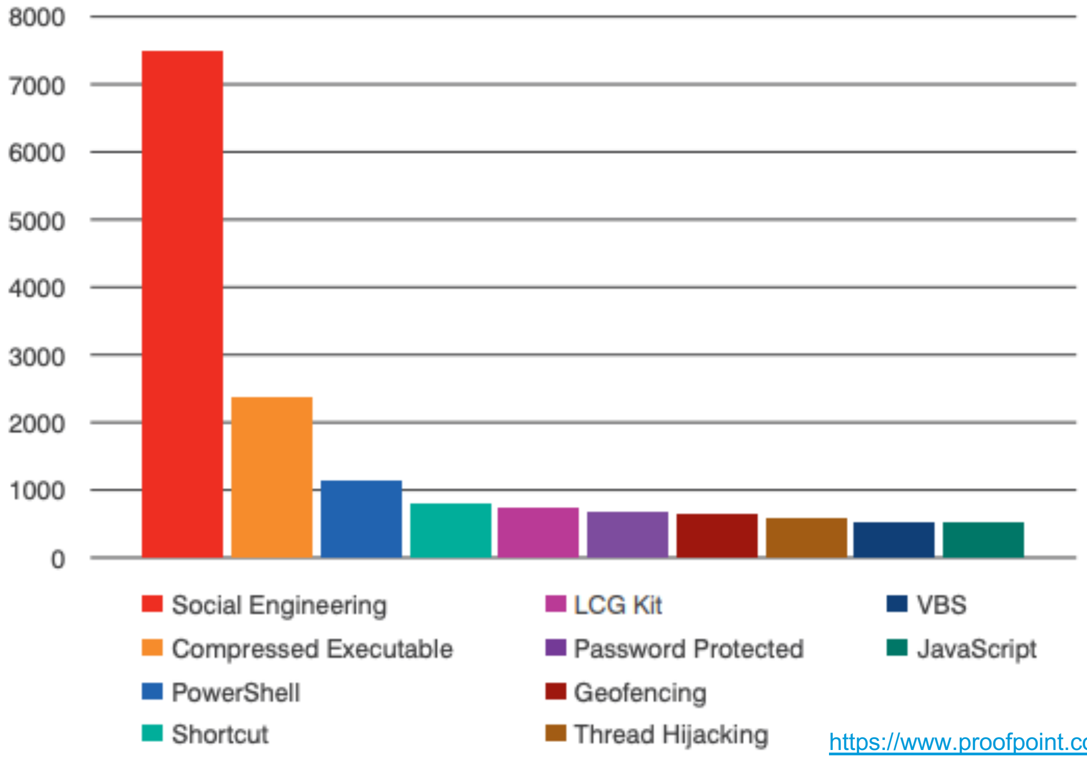
TTP: Social Engineering Defined

The set of tactics that relies on human interaction, using manipulation, persuasion, and exploitation to deceive users into taking an action that could lead to the compromise of information and/or systems.

https://www.proofpoint.com/us/threat-reference/social-engineering

For Customer Use

Top TTP: Social Engineering



https://www.proofpoint.com/us/blog/threat-insight/2023-human-factor-analyzes-evolving-threats-attack-chain

For Customer Use

Social Engineering: How Threat Actors Exploit Victims

Fatigue/
Timing

Trust

Emotions

https://www.proofpoint.com/us/resources/threat-reports/2022-social-engineering-report

TTP: What is Phishing?

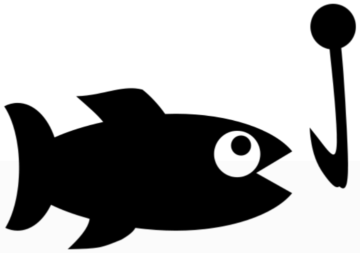
Fishing > Phishing

Emails that fish for information and access

Worms > Lures

Messages that lure you in to take the bait

Hooked > Breached



Once you're hooked…it's not good

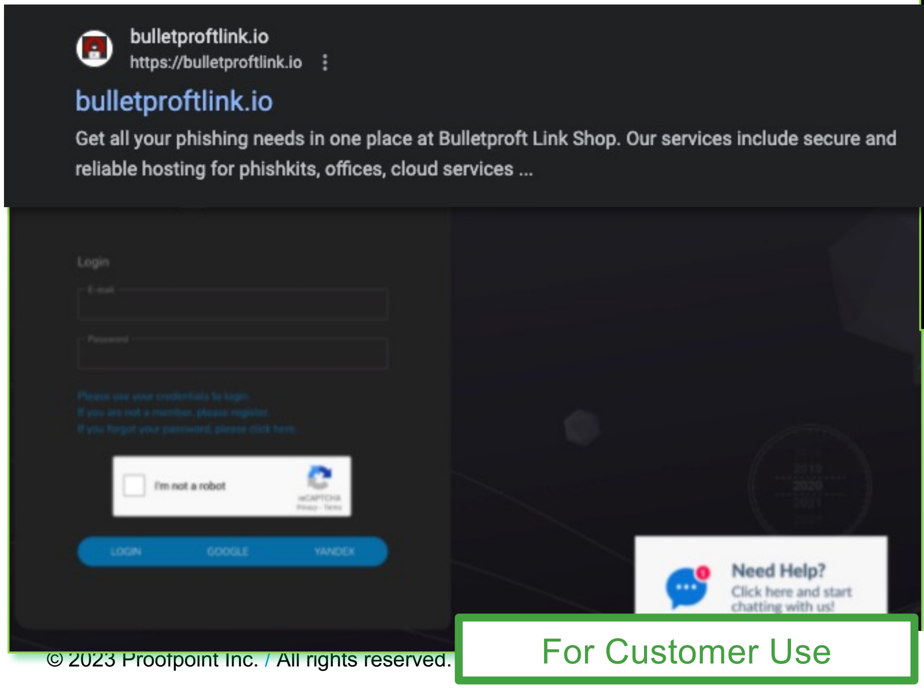
For Customer Use

TTP:

Phishing-as-a-Service & Phish Kits

https://www.proofpoint.com/us/blog/threat-insight/have-money-latte-then-you-too-can-buy-phish-kit

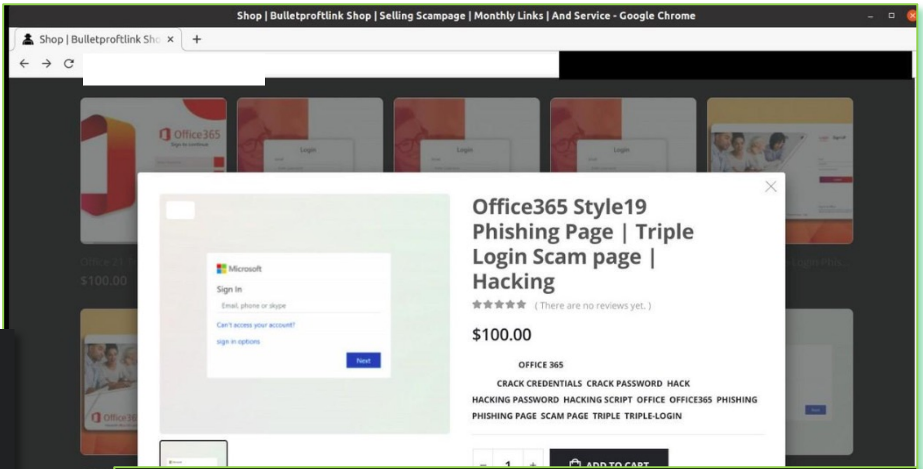
https://www.proofpoint.com/us/blog/threat-insight/mfa-psa-oh-my



bulletproftlink.io
https://bulletproftlink.io

bulletproftlink.io

Get all your phishing needs in one place at Bulletproft Link Shop. Our services include secure and reliable hosting for phishkits, offices, cloud services ...



Shop | Bulletproftlink Shop | Selling Scampage | Monthly Links | And Service - Google Chrome

Shop | Bulletproftlink Sh

[redacted]

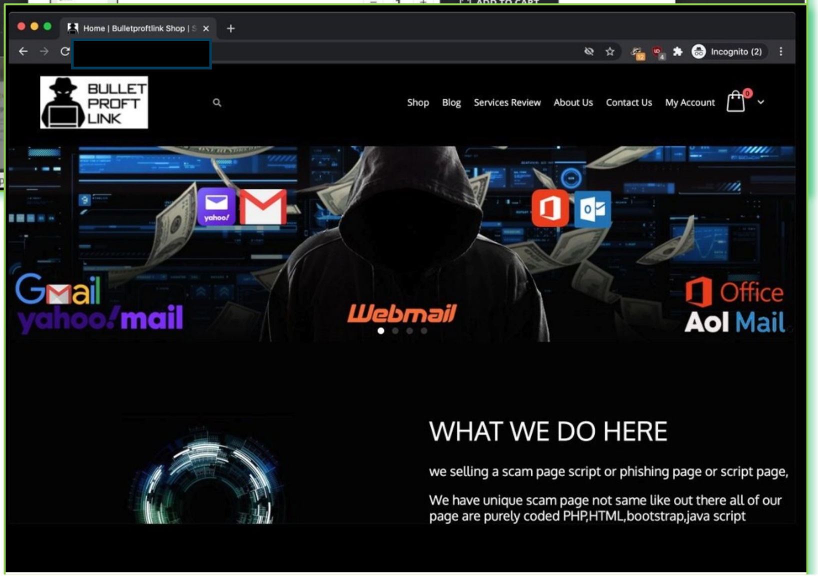
Office365 Style19 Phishing Page | Triple Login Scam page | Hacking

(There are no reviews yet.)

$100.00

OFFICE 365

CRACK CREDENTIALS CRACK PASSWORD HACK HACKING PASSWORD HACKING SCRIPT OFFICE OFFICE365 PHISHING PHISHING PAGE SCAM PAGE TRIPLE TRIPLE-LOGIN



Home | Bulletproftlink Shop | S

[redacted]

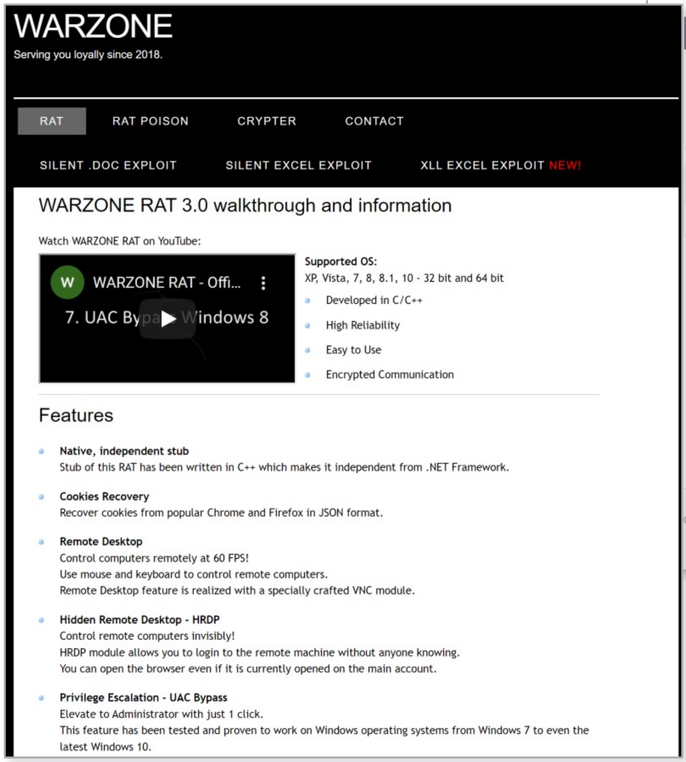
WHAT WE DO HERE

we selling a scam page script or phishing page or script page,

We have unique scam page not same like out there all of our page are purely coded PHP,HTML,bootstrap,java script

For Customer Use

TTP: Malware-as-a-Service



WARZONE

Serving you loyally since 2018.

WARZONE RAT 3.0 walkthrough and information

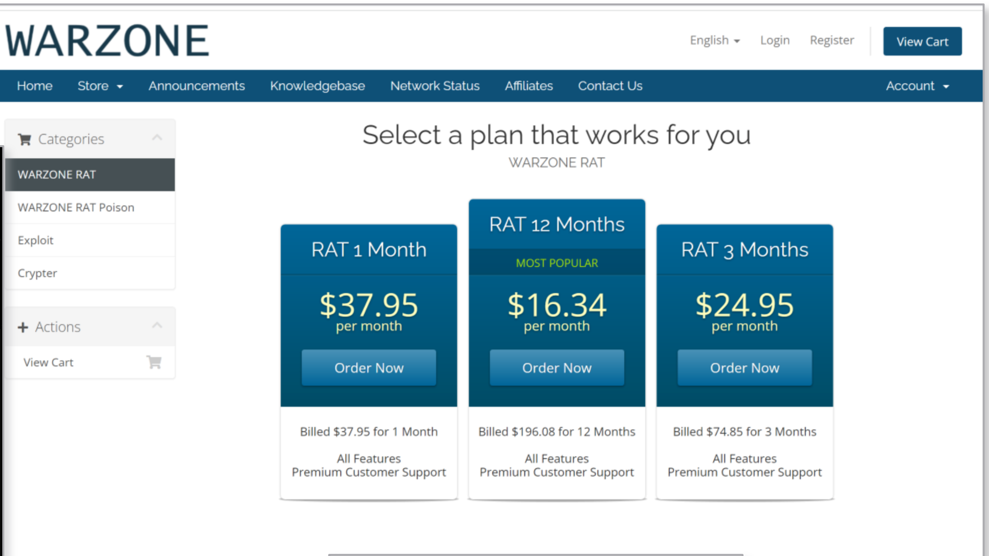
Watch WARZONE RAT on YouTube:

Supported OS:
XP, Vista, 7, 8, 8.1, 10 - 32 bit and 64 bit

- Developed in C/C++
- High Reliability
- Easy to Use
- Encrypted Communication

Features

- **Native, independent stub**
  Stub of this RAT has been written in C++ which makes it independent from .NET Framework.
- **Cookies Recovery**
  Recover cookies from popular Chrome and Firefox in JSON format.
- **Remote Desktop**
  Control computers remotely at 60 FPS!
  Use mouse and keyboard to control remote computers.
  Remote Desktop feature is realized with a specially crafted VNC module.
- **Hidden Remote Desktop - HRDP**
  Control remote computers invisibly!
  HRDP module allows you to login to the remote machine without anyone knowing.
  You can open the browser even if it is currently opened on the main account.
- **Privilege Escalation - UAC Bypass**
  Elevate to Administrator with just 1 click.
  This feature has been tested and proven to work on Windows operating systems from Windows 7 to even the latest Windows 10.



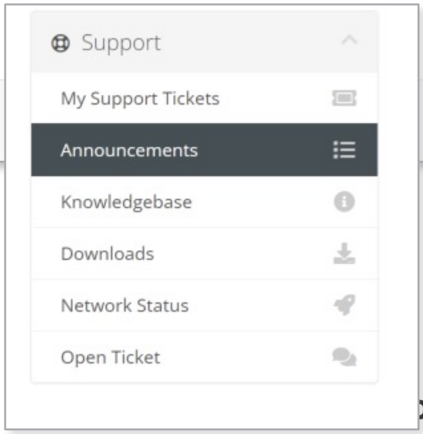
WARZONE

Select a plan that works for you

WARZONE RAT

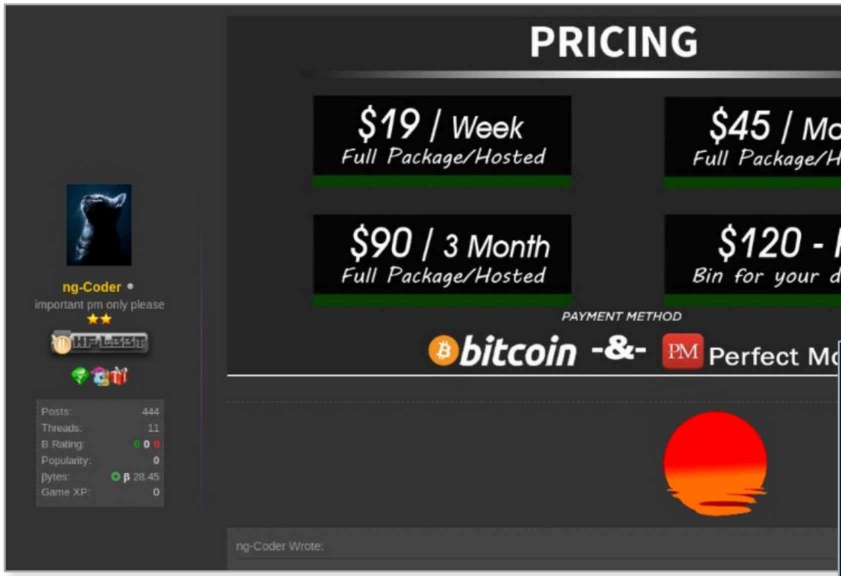
RAT 1 Month	RAT 12 Months	RAT 3 Months
	MOST POPULAR	
$37.95 per month	$16.34 per month	$24.95 per month
Order Now	Order Now	Order Now
Billed $37.95 for 1 Month	Billed $196.08 for 12 Months	Billed $74.85 for 3 Months
All Features Premium Customer Support	All Features Premium Customer Support	All Features Premium Customer Support

Copyright © 2022 WARZONE. All Rights Reserved.



For Customer Use

TTP: Malware-as-a-Service



ng-Coder

important pm only please

HF L33T

Posts:	444
Threads:	11
B Rating:	0 0 0
Popularity:	0
βytes:	β 28.45
Game XP:	0

PRICING

$19 / Week
Full Package/Hosted

$45 / Month
Full Package/Hosted

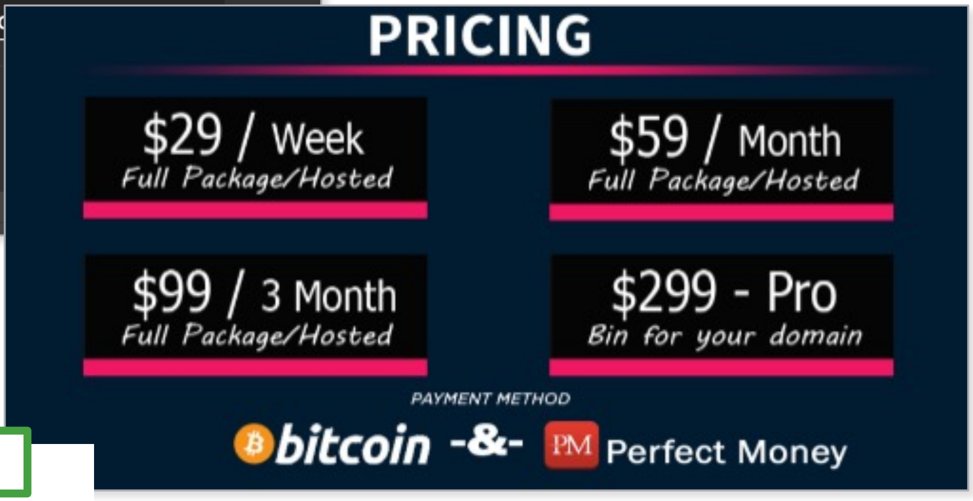
$90 / 3 Month
Full Package/Hosted

$120 - Pro
Bin for your domain

PAYMENT METHOD

bitcoin -&- PM Perfect Mo

ng-Coder Wrote:



PRICING

$29 / Week
Full Package/Hosted

$59 / Month
Full Package/Hosted

$99 / 3 Month
Full Package/Hosted

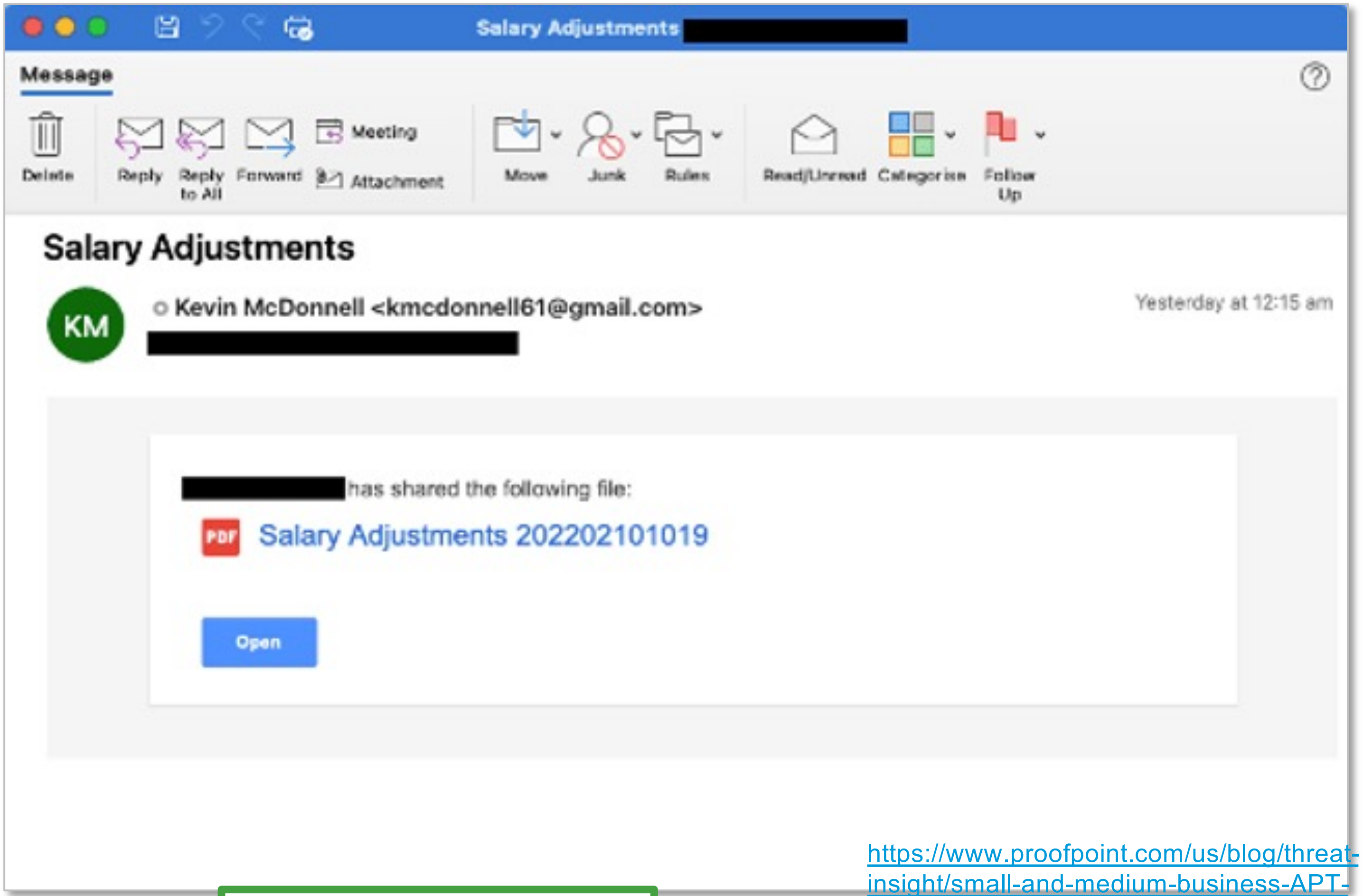
$299 - Pro
Bin for your domain

PAYMENT METHOD

bitcoin -&- PM Perfect Money

For Customer Use

What does this look like as an email end user?



Salary Adjustments [redacted]

Salary Adjustments

Kevin McDonnell <kmcdonnell61@gmail.com>

[redacted]

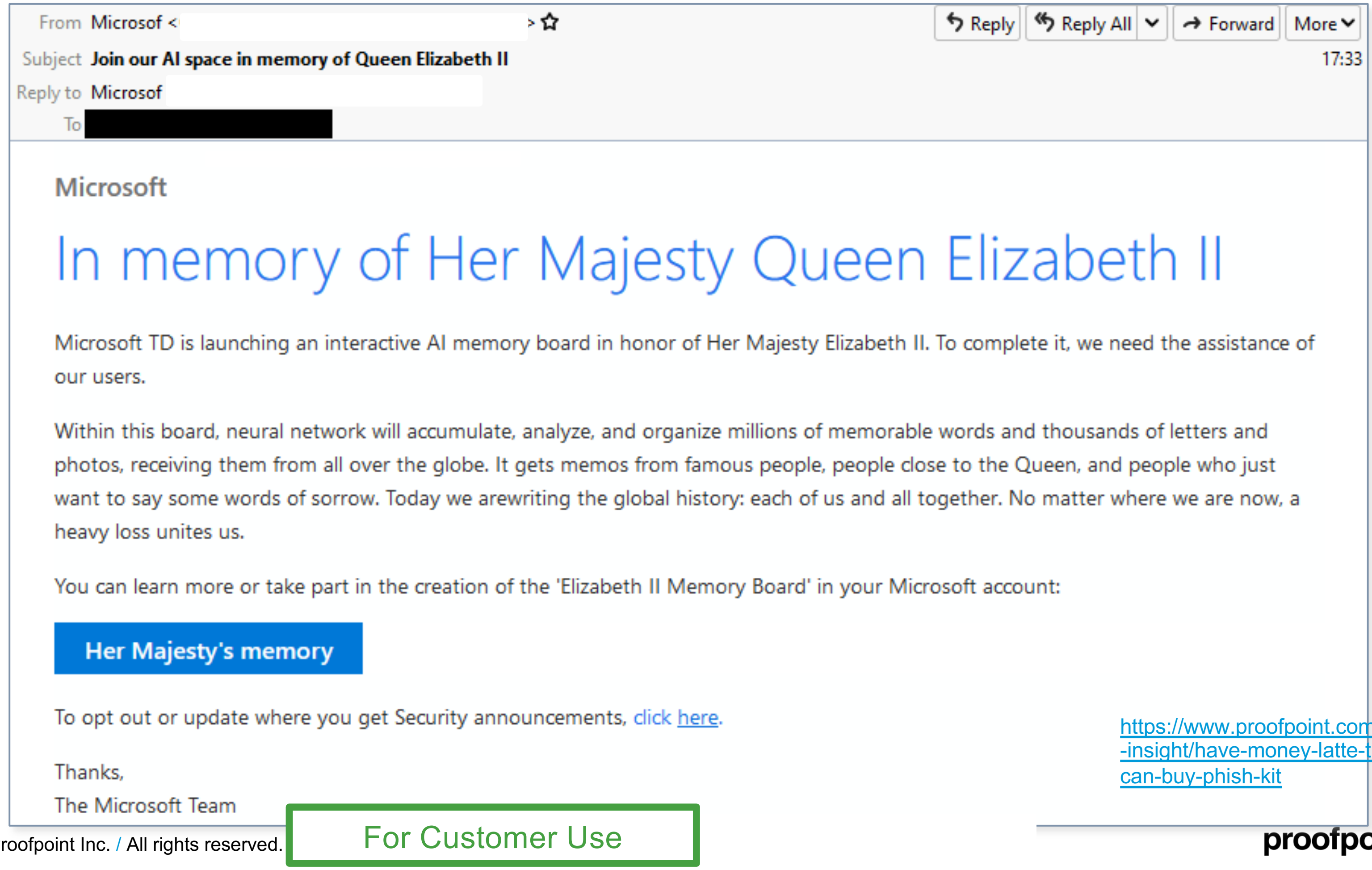
Yesterday at 12:15 am

[redacted] has shared the following file:

Salary Adjustments 202202101019

For Customer Use

https://www.proofpoint.com/us/blog/threat-insight/small-and-medium-business-APT-phishing-landscape-in-2023



From Microsof < > ☆

Subject **Join our AI space in memory of Queen Elizabeth II**

17:33

Reply to Microsof

To [redacted]

Microsoft

In memory of Her Majesty Queen Elizabeth II

Microsoft TD is launching an interactive AI memory board in honor of Her Majesty Elizabeth II. To complete it, we need the assistance of our users.

Within this board, neural network will accumulate, analyze, and organize millions of memorable words and thousands of letters and photos, receiving them from all over the globe. It gets memos from famous people, people close to the Queen, and people who just want to say some words of sorrow. Today we arewriting the global history: each of us and all together. No matter where we are now, a heavy loss unites us.

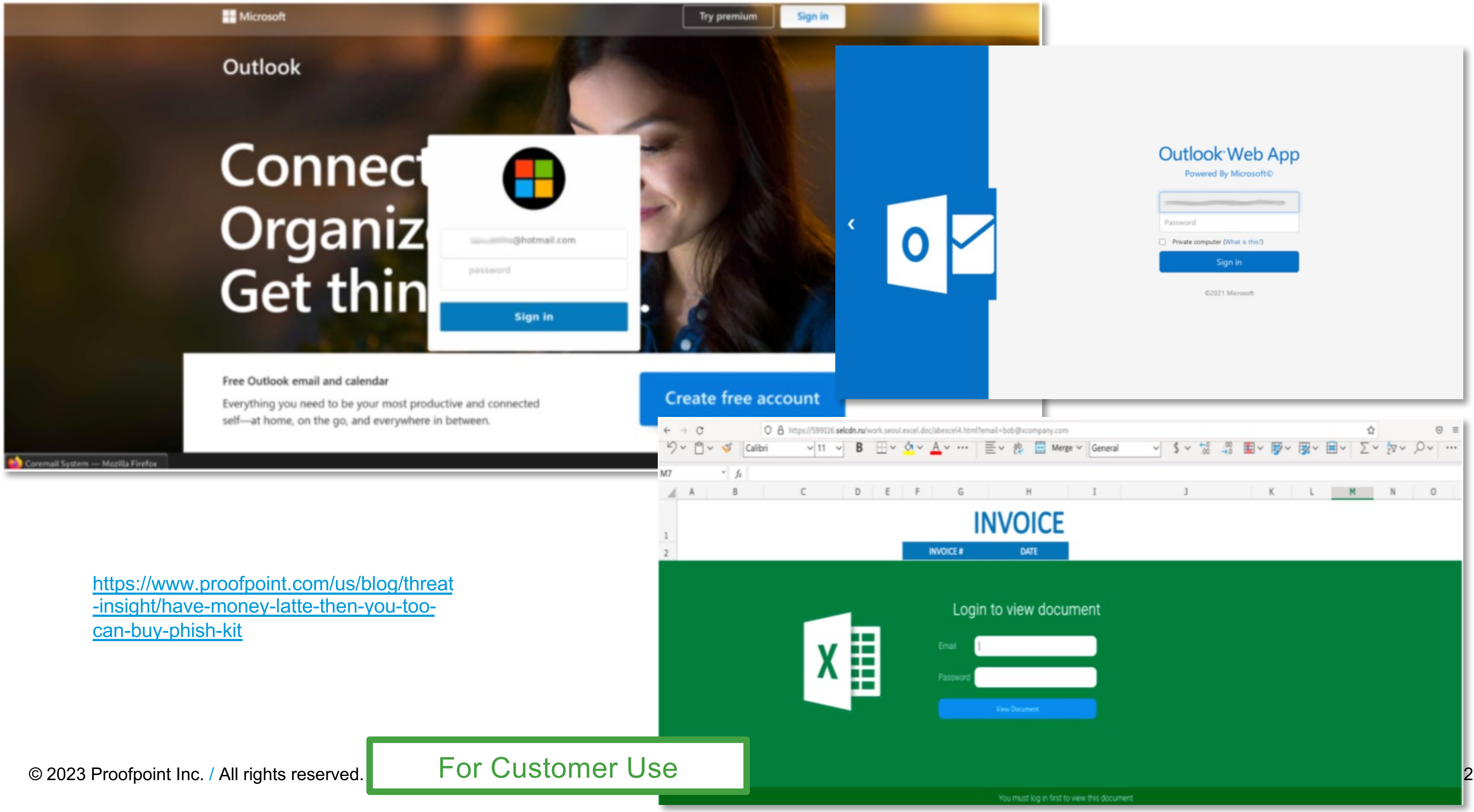
You can learn more or take part in the creation of the 'Elizabeth II Memory Board' in your Microsoft account:

Her Majesty's memory

To opt out or update where you get Security announcements, click here.

Thanks,
The Microsoft Team

https://www.proofpoint.com/us/blog/threat-insight/have-money-latte-then-you-too-can-buy-phish-kit



Microsoft

Try premium

Sign in

Outlook

Connect

Organiz

Get thin

[redacted]@hotmail.com

password

Sign in

Free Outlook email and calendar

Everything you need to be your most productive and connected self—at home, on the go, and everywhere in between.

Create free account

Coremail System — Mozilla Firefox

Outlook Web App

Powered By Microsoft©

[redacted]

Password

□ Private computer (What is this?)

Sign in

©2021 Microsoft

https://599116.selcdn.ru/work.seoul.excel.doc/abexcel4.html?email=bob@xcompany.com

INVOICE

INVOICE # DATE

Login to view document

Email

Password

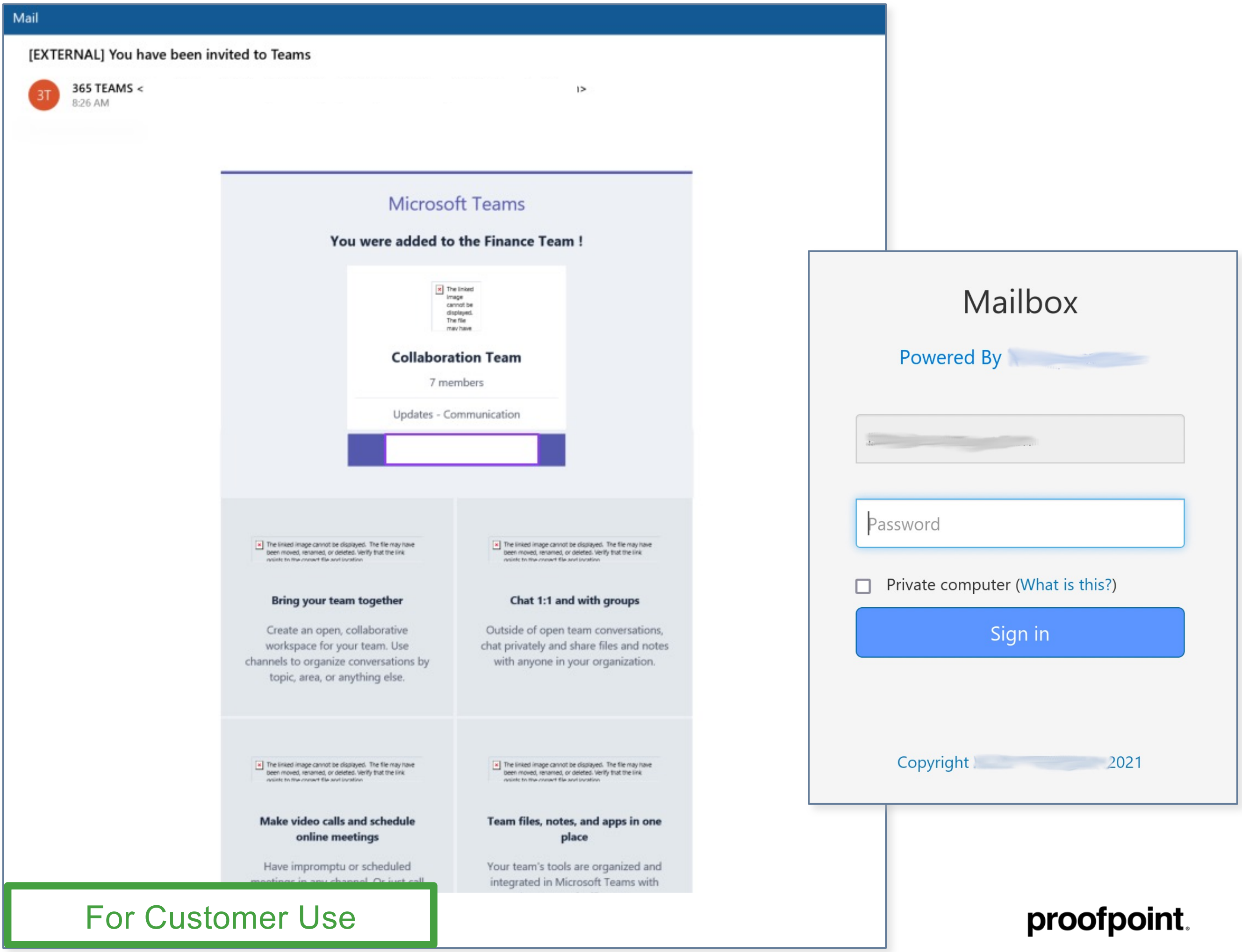
View Document

You must log in first to view this document

https://www.proofpoint.com/us/blog/threat-insight/have-money-latte-then-you-too-can-buy-phish-kit

For Customer Use

https://www.proofpoint.com/us/blog/threat-insight/have-money-latte-then-you-too-can-buy-phish-kit



Mail

[EXTERNAL] You have been invited to Teams

3T 365 TEAMS < [redacted] >
8:26 AM

Microsoft Teams

You were added to the Finance Team !

The linked image cannot be displayed. The file may have

Collaboration Team

7 members

Updates - Communication

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Bring your team together

Create an open, collaborative workspace for your team. Use channels to organize conversations by topic, area, or anything else.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Chat 1:1 and with groups

Outside of open team conversations, chat privately and share files and notes with anyone in your organization.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Make video calls and schedule online meetings

Have impromptu or scheduled meetings in any channel. Or just call

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Team files, notes, and apps in one place

Your team's tools are organized and integrated in Microsoft Teams with

Mailbox

Powered By [redacted]

[redacted]

Password

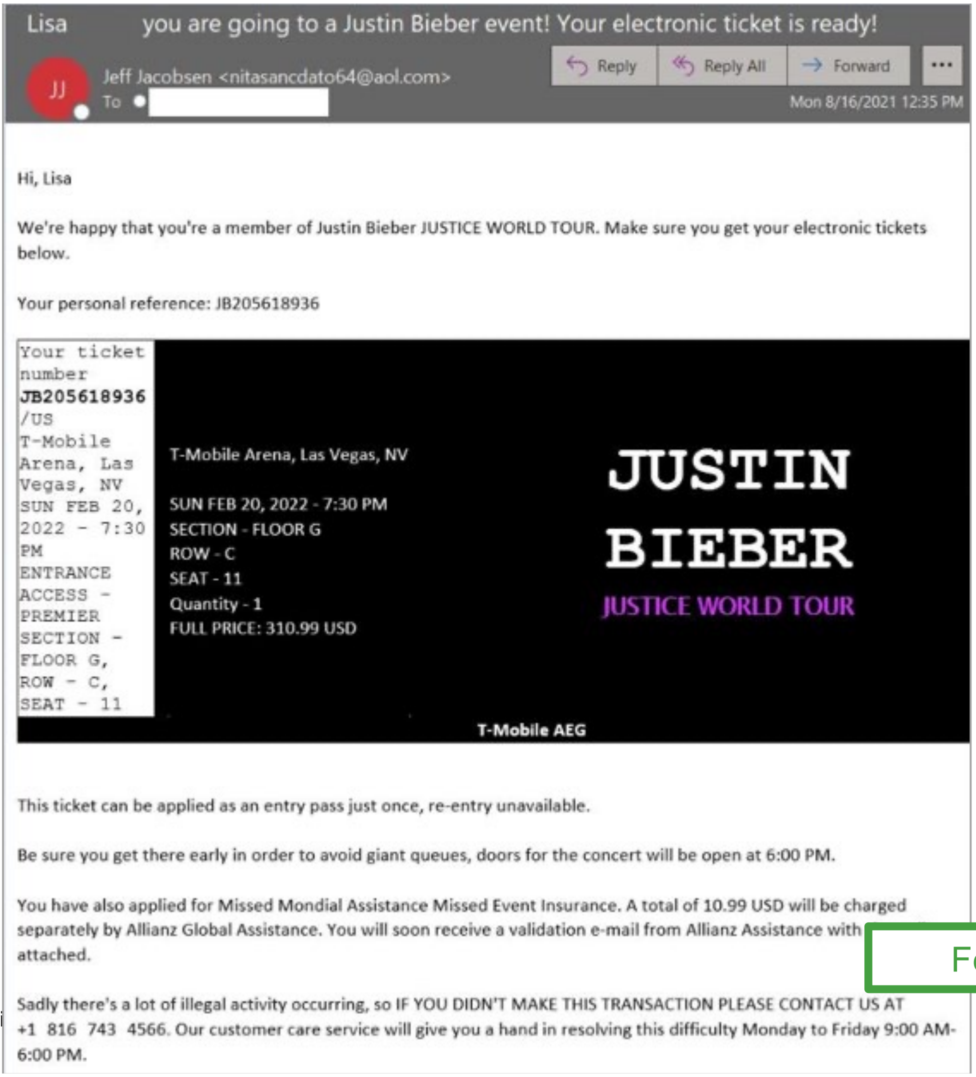
□ Private computer (What is this?)

Sign in

Copyright [redacted] 2021

For Customer Use

https://www.proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery



Lisa you are going to a Justin Bieber event! Your electronic ticket is ready!

Jeff Jacobsen <nitasancdato64@aol.com>
To [redacted]

Mon 8/16/2021 12:35 PM

Hi, Lisa

We're happy that you're a member of Justin Bieber JUSTICE WORLD TOUR. Make sure you get your electronic tickets below.

Your personal reference: JB205618936

Your ticket number **JB205618936** /US T-Mobile Arena, Las Vegas, NV SUN FEB 20, 2022 - 7:30 PM ENTRANCE ACCESS - PREMIER SECTION - FLOOR G, ROW - C, SEAT - 11

T-Mobile Arena, Las Vegas, NV

SUN FEB 20, 2022 - 7:30 PM
SECTION - FLOOR G
ROW - C
SEAT - 11
Quantity - 1
FULL PRICE: 310.99 USD

JUSTIN BIEBER
JUSTICE WORLD TOUR

T-Mobile AEG

This ticket can be applied as an entry pass just once, re-entry unavailable.

Be sure you get there early in order to avoid giant queues, doors for the concert will be open at 6:00 PM.

You have also applied for Missed Mondial Assistance Missed Event Insurance. A total of 10.99 USD will be charged separately by Allianz Global Assistance. You will soon receive a validation e-mail from Allianz Assistance with attached.

Sadly there's a lot of illegal activity occurring, so IF YOU DIDN'T MAKE THIS TRANSACTION PLEASE CONTACT US AT +1 816 743 4566. Our customer care service will give you a hand in resolving this difficulty Monday to Friday 9:00 AM-6:00 PM.

For Customer Use

Looking Ahead

It’s not all doom and gloom!

For Customer Use

Despite the availability of MaaS and PhaaS, and other tools – threat actors are still needing to be creative with social engineering, and continuously evolve tools – why?

User education – we are watching them and staying ahead!

https://www.proofpoint.com/us/resources/threat-reports/2022-social-engineering-report

Common Social Engineering Tactics

Masquerading as someone you know or trust

Your emotions are heightened

The request is urgent

The offer feels too good to be true

Receiving help you didn't ask for

The sender can't prove their identity

For Customer Use

Common Misconceptions Clarified:

- Threat actors will take the time to build trust by engaging in extended conversations with victims. Build rapport.

- Threat actors will abuse trusted companies' services, recognizable brands.
  - E.g.: Google and Microsoft

- Threat actors will leverage orthogonal tech in their attack chain to adopt new techniques as security controls evolve and are more effective.
  - E.g.: Telephone as seen in TOAD

- Threat actors are aware of and will use email conversations and existing threads with colleagues.
  - E.g.: Thread Hijacking

- Threat actors will leverage topical, timely, and socially relevant themes.
  - E.g.: Covid-19, UA/RU conflict, Tax season, holiday travel

https://www.proofpoint.com/us/resources/threat-reports/2022-social-engineering-report

Infection chains (malware) are getting longer and more complex because advancing security controls and solutions are crushing threat actor efforts (yes!!).

Community Resource: *ET Open*

ET Open

SNORT/Suricata ruleset/feed for detecting and blocking network threats.

- Malware Delivery
- C2
- In-the-wild Exploits and Vulnerabilities
- DDoS
- Exploit Kits, and more!

Rules published daily = ~5

Subscription based, FREE

Platform agnostic (IDS/IPS)

ET Pro

Paid Subscription
~50 rules published/day

ET Intel

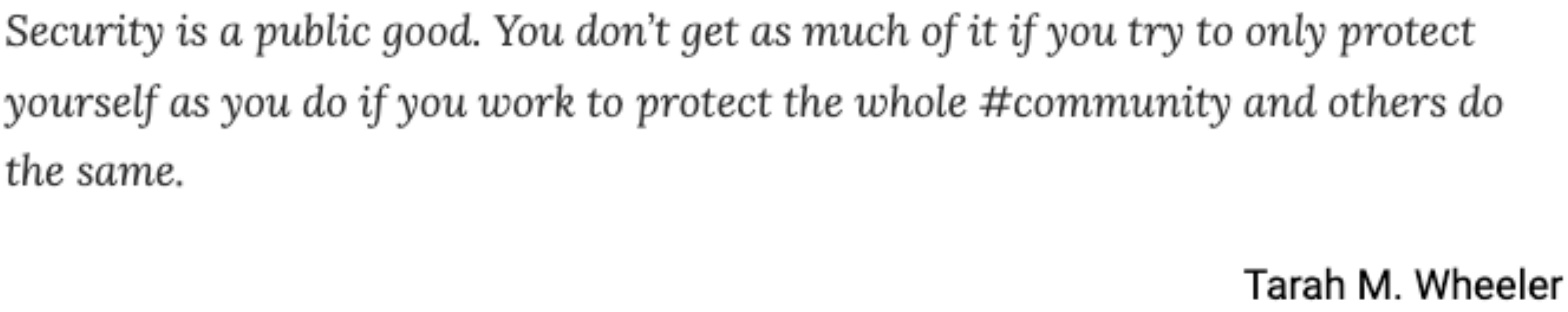
Context for IOCs that triggered detection.
IPs, Domains, etc.
Paid Subscription

https://www.proofpoint.com/sites/default/files/pfpt-us-ds-et-intelligence.pdf
https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
https://rules.emergingthreatspro.com/
https://docs.opnsense.org/manual/etpro_telemetry.html

https://www.proofpoint.com/sites/default/files/data-sheets/pfpt-us-ds-etpro-vs-etopen-ruleset.pdf

For Customer Use

Thoughts on Community Resources



Security is a public good. You don't get as much of it if you try to only protect yourself as you do if you work to protect the whole #community and others do the same.

Tarah M. Wheeler

People-Centric

*“Information Security is a never-ending chess match between threat actors and network defenders.”**

*We are all network defenders.

For Customer Use

User education and awareness is an incredibly powerful tool in a security stack– if you know what your enemy is doing, then you know what to look for and avoid.

DON’T CLICK!

Protect Yourself

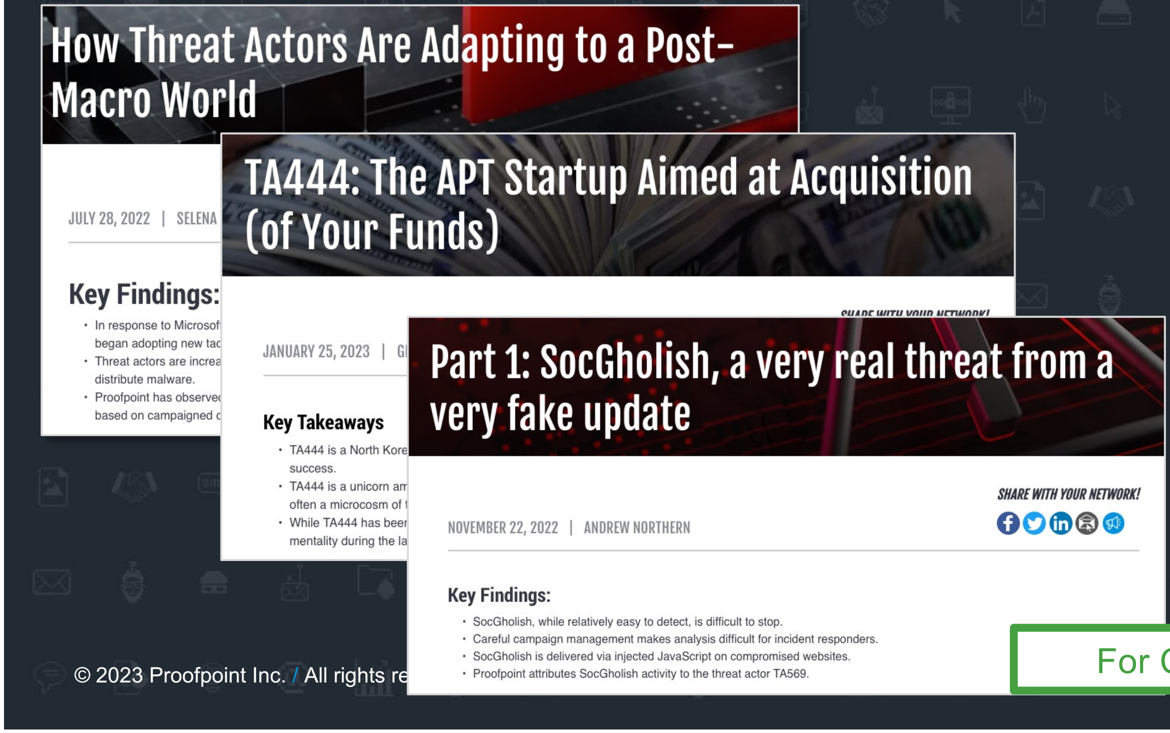
- Be careful what you click
- Remember that you, your computer, your data and your services are valuable to attackers
- Don’t be shy to report your suspicions to the help desk
- Get suspicious if an email tries to elicit an emotional response
- When in doubt – ask the security team

For Customer Use

Want More Threat Research?

Threat Insight Blog

https://www.proofpoint.com/us/blog/threat-insight



How Threat Actors Are Adapting to a Post-Macro World

JULY 28, 2022 | SELENA

Key Findings:

- In response to Microsof began adopting new tac
- Threat actors are increa distribute malware.
- Proofpoint has observed based on campaigned c

TA444: The APT Startup Aimed at Acquisition (of Your Funds)

JANUARY 25, 2023 | GI

SHARE WITH YOUR NETWORK!

Key Takeaways

- TA444 is a North Kore success.
- TA444 is a unicorn am often a microcosm of t
- While TA444 has been mentality during the la

Part 1: SocGholish, a very real threat from a very fake update

NOVEMBER 22, 2022 | ANDREW NORTHERN

SHARE WITH YOUR NETWORK!

Key Findings:

- SocGholish, while relatively easy to detect, is difficult to stop.
- Careful campaign management makes analysis difficult for incident responders.
- SocGholish is delivered via injected JavaScript on compromised websites.
- Proofpoint attributes SocGholish activity to the threat actor TA569.

Proofpoint Threat Research Podcasts

https://www.proofpoint.com/us/podcasts

For Customer Use

proofpoint®