Grrcon 2023

Advanced Persistent Teenagers

I’m Matt Muller.

THEN:

coinbase

Director, Security Operations

2018-2023

NOW:

Material Security

Product Lead, Phishing Protection

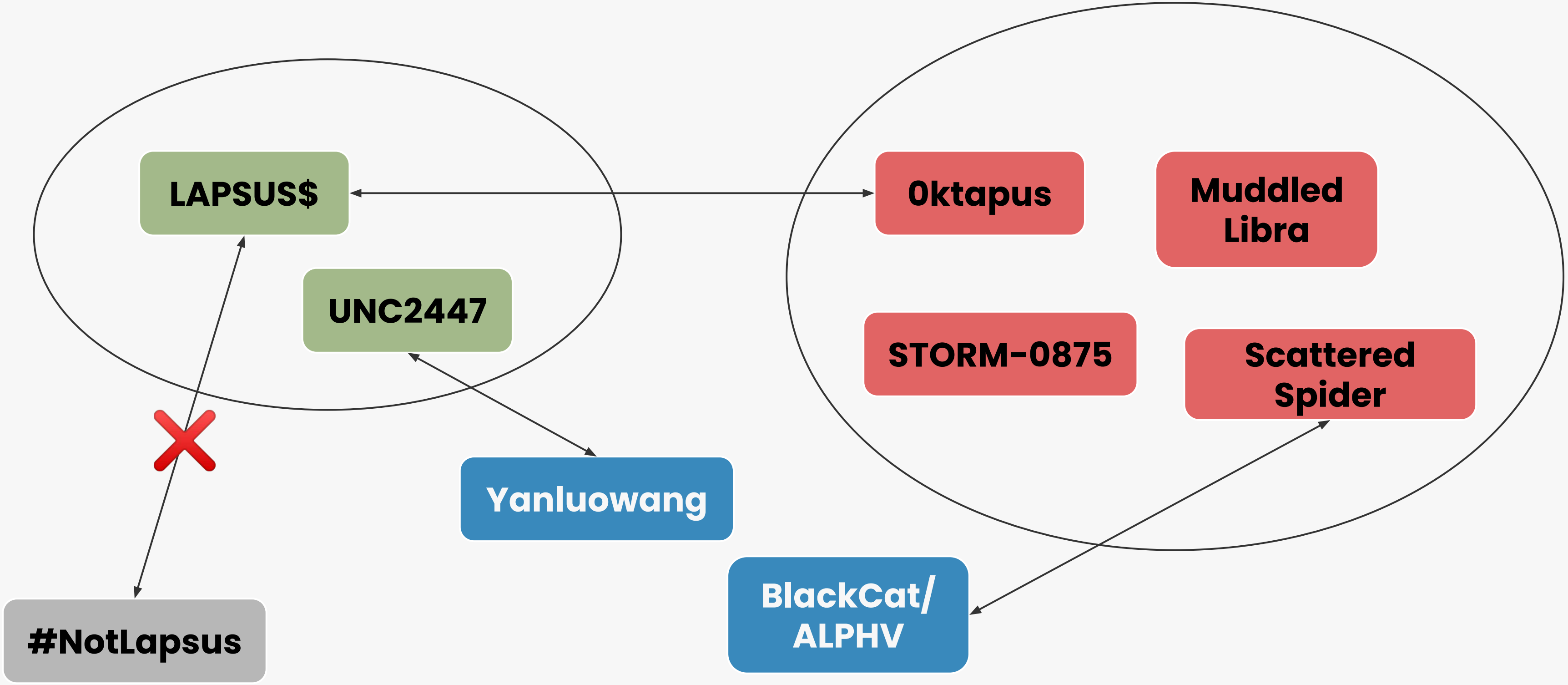
2023-Present

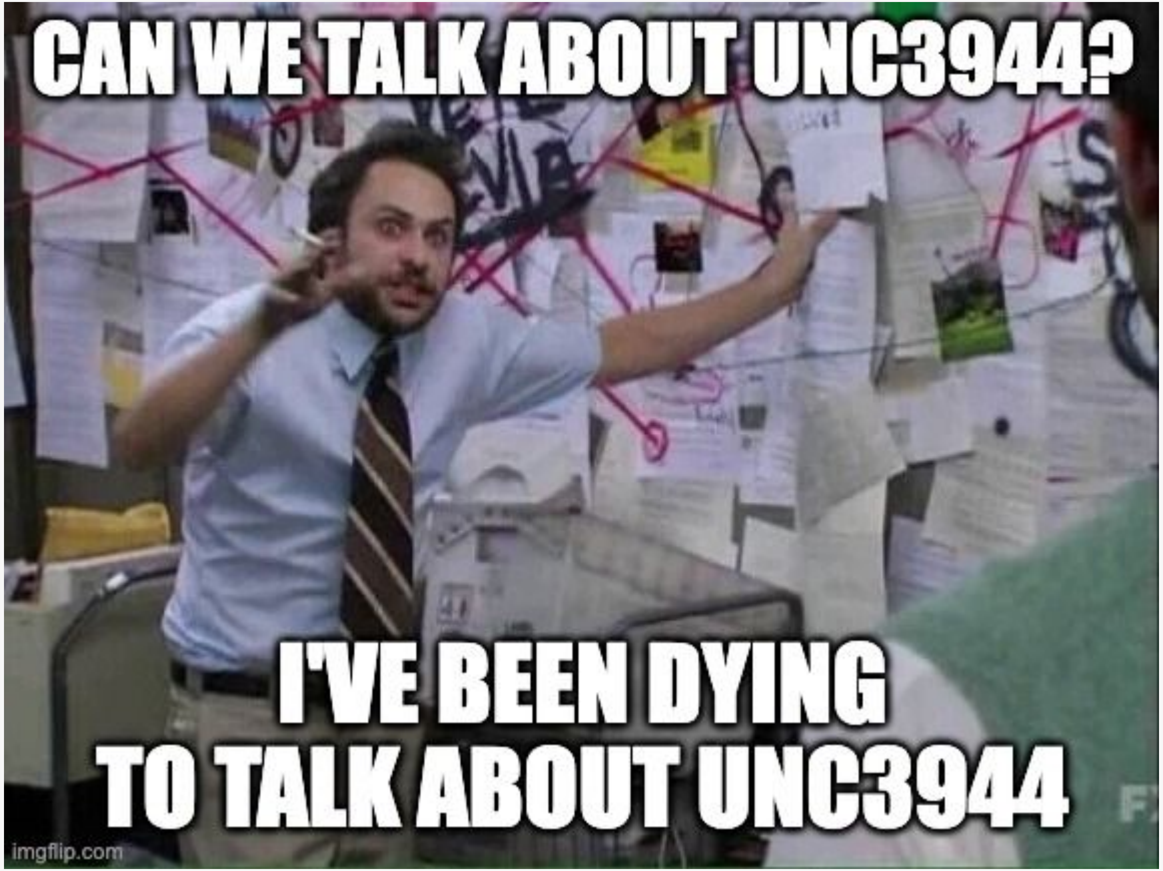
Housekeeping

Slides will be available on GitHub after the conference.

github.com/**themullinator**/talks

A quick note on attribution…




CAN WE TALK ABOUT UNC3944?
I'VE BEEN DYING
TO TALK ABOUT UNC3944
imgflip.com
FX

A quick note on attribution…

It doesn’t really matter*

*at least for this talk

Expectation:

Threat actors look a lot like these guys.

They have the resourcing and motivations of a nation state.

They probably won’t attack us, and if they do, there’s not much we can do about FSB hackers with 0-days.

WANTED BY THE FBI

RUSSIAN FSB CENTER 16 HACKERS

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Wire Fraud; Computer Fraud – Unauthorized Access to Obtain Information from Protected Computers; Aggravated Identity Theft; Aiding and Abetting

PAVEL ALEKSANDROVICH AKULOV
(Павел Александрович Акулов)

MIKHAIL MIKHAILOVICH GAVRILOV
(Михаил Михайлович Гаврилов)

MARAT VALERYEVICH TYUKOV
(Марат Валерьевич Тюков)

Reality:

Some of the most high-profile intrusions in the last few years have been performed by this teenager and his community.

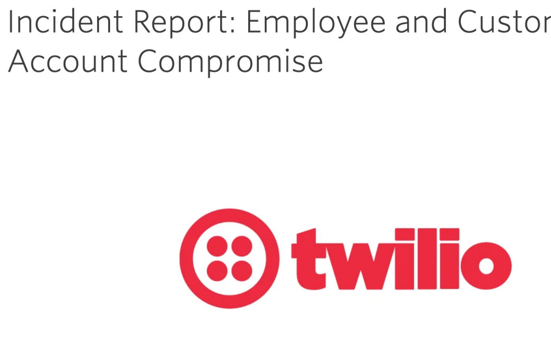
They did it without advanced tools or 0-days.

As an industry, we should have seen it coming.

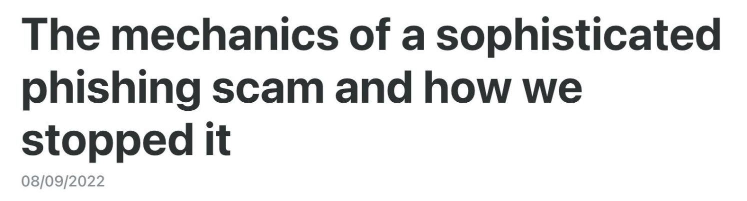
Teenagers are the perfect adversaries.

Way too much time on their hands	➔	Pentests are boredom-bound, not time-bound
False sense of invincibility	➔	Behavior isn’t shaped by potential consequences
Always playing video games	➔	Exposure to game mods and cheats
Will jump off a bridge because their friends did	➔	Unpredictable objectives and motivations

This is the result.



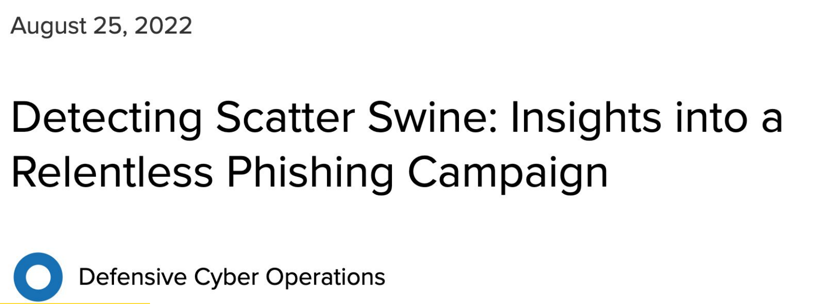
Incident Report: Employee and Customer Account Compromise



The mechanics of a sophisticated phishing scam and how we stopped it

08/09/2022

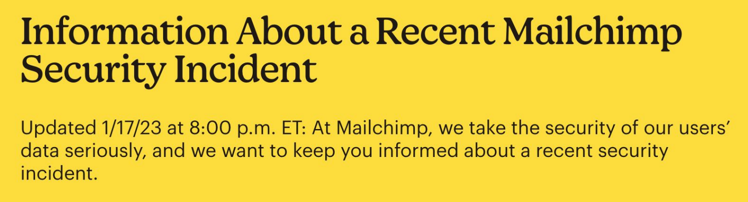
iel Stinson-Diess Sourov Zaman



August 25, 2022

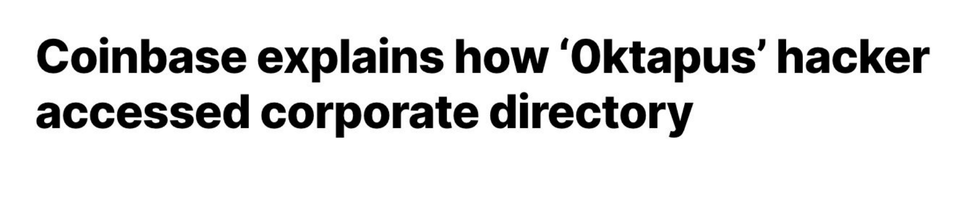
Detecting Scatter Swine: Insights into a Relentless Phishing Campaign

Defensive Cyber Operations



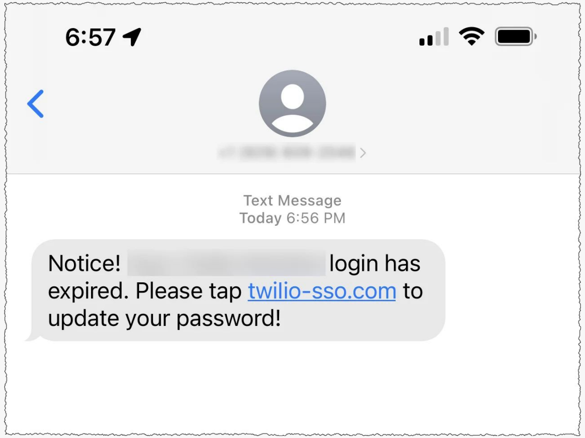
Information About a Recent Mailchimp Security Incident

Updated 1/17/23 at 8:00 p.m. ET: At Mailchimp, we take the security of our users' data seriously, and we want to keep you informed about a recent security incident.



Coinbase explains how 'Oktapus' hacker accessed corporate directory

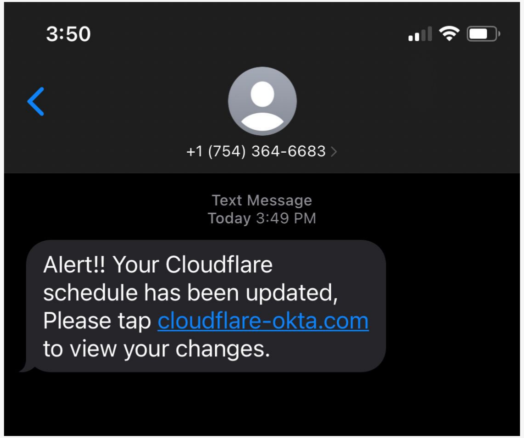
Headlines and IOCs only tell half the story.



[redacted]

Text Message
Today 6:56 PM

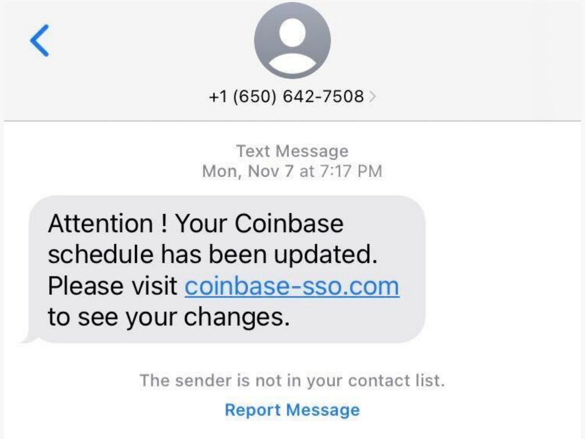
Notice! [redacted] login has expired. Please tap twilio-sso.com to update your password!



+1 (754) 364-6683

Text Message
Today 3:49 PM

Alert!! Your Cloudflare schedule has been updated, Please tap cloudflare-okta.com to view your changes.


+1 (650) 642-7508

Text Message
Mon, Nov 7 at 7:17 PM

Attention ! Your Coinbase schedule has been updated. Please visit coinbase-sso.com to see your changes.

The sender is not in your contact list.

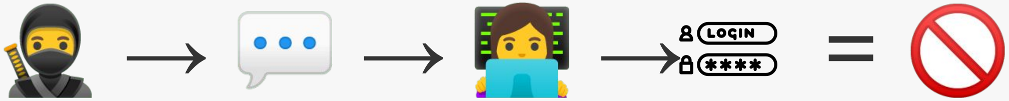
A day in the life of an 0ktapus intrusion

2020: Experimentation

🥷 → 📱 → 👩‍💻 = 🚫

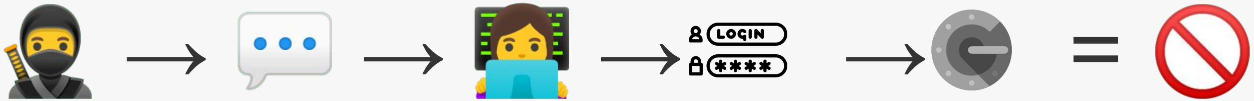
Call the target as “Coinbase IT”, gather intel until the person gets suspicious and hangs up on you. Maybe try to get them to install AnyDesk.

2021: Iteration



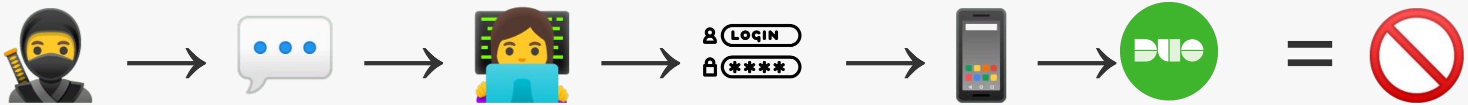
Send SMS lures to a small number of targets. Collect their Okta email and password. Test that the credentials are valid.

2021: Iteration



Add TOTP interception to the mix. See if it works. (It doesn’t)

2021: Iteration



Time to hop back on the phone as “Brian” from Coinbase IT and get your target to accept a Duo Push! (Too bad you’re using an unmanaged Windows VM)

2022: Refinement

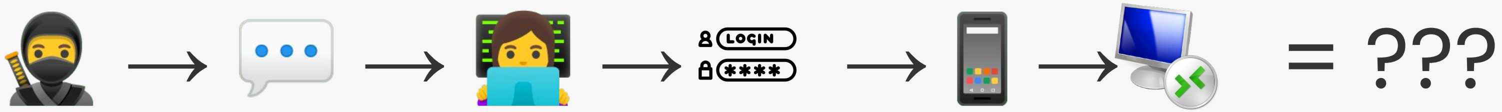
DUO
+
CROWDSTRIKE
=

With a working technique for reliably collecting credentials, focus on fooling device posture checks (spoiler alert: even tampering with Duo Device Health payloads won’t help)

2022: Refinement

Maybe it’s time to go back to basics…

2023: Persistence Pays Off

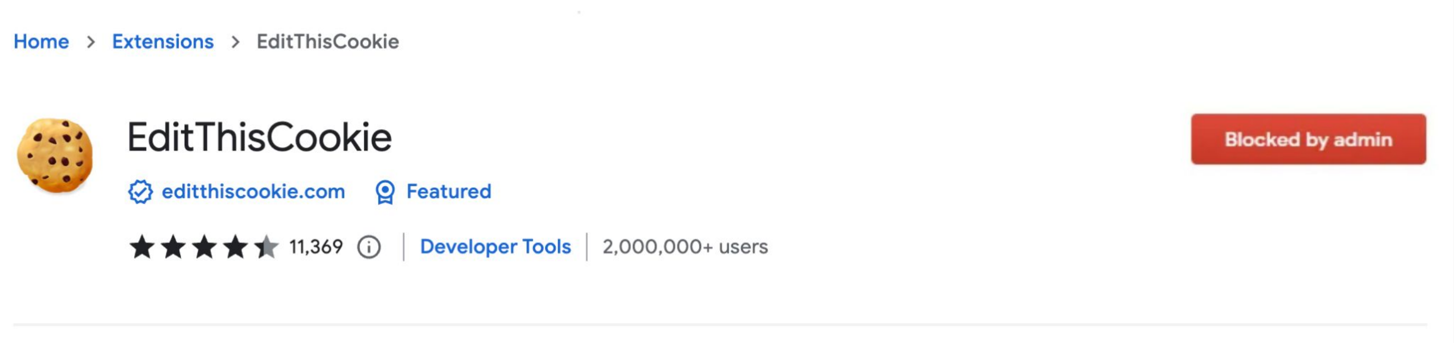


No need to impersonate a managed device if you can just get remote access to one, right?

2023: Persistence Pays Off

ANYDESK
ISL ONLINE
imgflip.com

2023: Persistence Pays Off



Home > Extensions > EditThisCookie

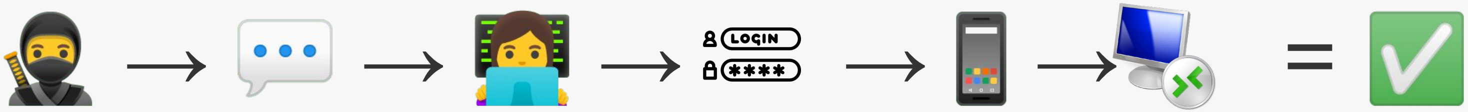
EditThisCookie

editthiscookie.com Featured

11,369 | Developer Tools | 2,000,000+ users

If you can’t steal cookies with your favorite Chrome extension, maybe just ask your victim politely to run some console commands.

2023: Persistence Pays Off



Time for a well-deserved vacation!

No, seriously. Please take a break. Ideally forever.

Lessons Learned

Multi-Factor Authentication

Easy to defeat

- SMS (duh)
- TOTP
- Push

Good with caveats

- Push + Number Matching
- Passkeys

Highly recommended

- Hardware Security Keys

Device Trust

Easy to defeat

- Impossible travel alerts
- Session change alerts

Good with caveats

- Device posture checks
- BYOD restrictions

Highly recommended

- Device-bound certificates
- BYOD ban

Browser Extensions

Easy to defeat

- Extension install monitoring

Good with caveats

- Managed profiles
- Extension blocklist

Highly recommended

- Managed browsers
- Extension allowlist

Binary Allowlisting

Easy to defeat

- Binary blocklists

Good with caveats

- Chromebooks

Highly recommended

- Binary allowlists
- No local admin

What’s (probably) next?

- Increased targeting of employee personal accounts and devices
- Insider recruitment (whether voluntary or extorted)
- Supply-chain focus for hard targets (marketing vendors, BPOs)
- Professionalized operations (more ransomware partnerships)

Thank You

References

- https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
- https://www.group-ib.com/blog/0ktapus/
- https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
- https://blog.bushidotoken.net/2023/08/tracking-adversaries-scattered-spider.html
- https://www.bbc.com/news/technology-66549159
- https://www.grip.security/blog/what-is-0ktapus-the-ongoing-campaign-targeting-customers-of-iam-giant-okta
- https://therecord.media/lapsus-the-script-kiddies-are-alright
- https://flashpoint.io/blog/lapsus/
- https://blog.talosintelligence.com/recent-cyber-attack/
- https://sec.cloudapps.cisco.com/security/center/resources/corp_network_security_incident
- https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial
- https://www.trellix.com/en-us/about/newsroom/stories/research/yanluowang-ransomware-leaks-analysis.html
- https://mailchimp.com/january-2023-security-incident/
- https://www.bleepingcomputer.com/news/security/hackers-auction-alleged-source-code-for-league-of-legends/
- https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html
- https://explore.avertium.com/resource/unraveling-scattered-spider-a-stealthy-and-persistent-threat-actor
- https://therecord.media/coinbase-explains-how-0ktapus-hacker-accessed-corporate-directory
- https://blog.cloudflare.com/2022-07-sms-phishing-attacks/
- https://www.twilio.com/blog/august-2022-social-engineering-attack
- https://www.cshub.com/attacks/news/oktapus-attack-on-twilio-exposes-data-of-163-companies
- https://unit42.paloaltonetworks.com/muddled-libra/
- https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/
- https://sec.okta.com/scatterswine
- https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study
- https://www.bleepingcomputer.com/news/security/riot-games-hacked-delays-game-patches-after-security-breach/