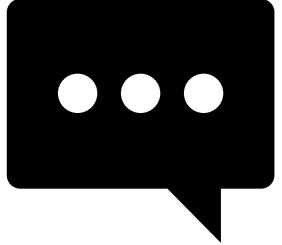
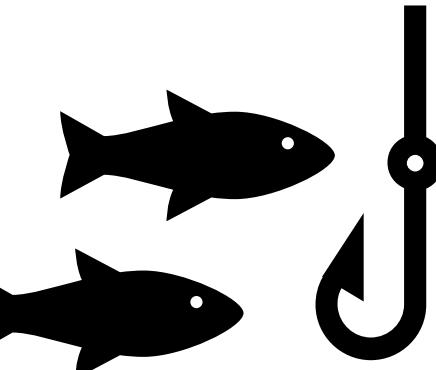


They Can't
Keep Getting
Away With It

Analysis of
Oktapus/ScatteredSpider
campaigns



C:\User\wthomas

Cyber Threat Intelligence Researcher (4 years)

Equinix – the world's digital infrastructure company 

Equinix Threat Analysis Center (ETAC)

Co-author of the SANS FOR589 Cybercrime Intelligence course

Co-founder of the Curated Intelligence trust group

- <https://blog.bushidotoken.net/>
- <https://twitter.com/BushidoToken>
- <https://github.com/BushidoUK>
- <https://www.sans.org/profiles/will-thomas/>
- <https://www.linkedin.com/in/william-t/>



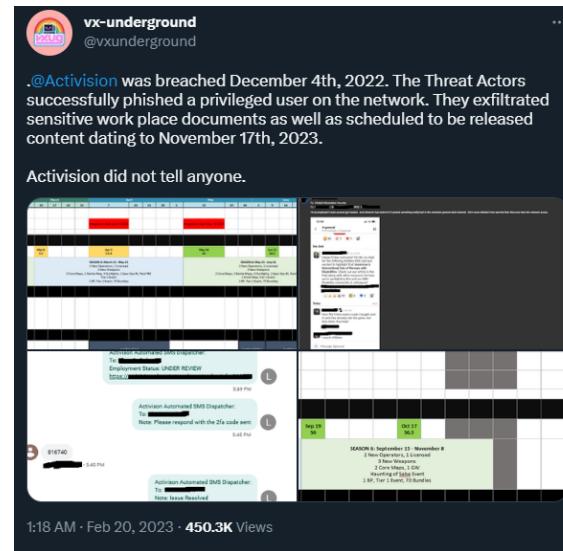
A Bunch of Big Breaches



Featured Article

DoorDash hit by data breach linked to Twilio hackers

Hackers accessed DoorDash customer information and some partial payment data



MOTHERBOARD TECH BY VICE

Hackers Demand \$10M From Riot Games to Stop Leak of 'League of Legends' Source Code

Motherboard obtained the ransom note that hackers sent Riot Games on Tuesday, which threatened to release 'League of Legends' source code.

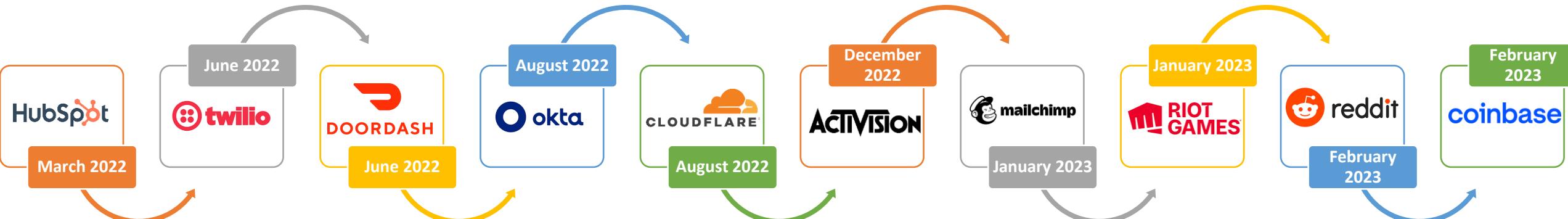
By Joseph Cox By Matthew Gault

Security

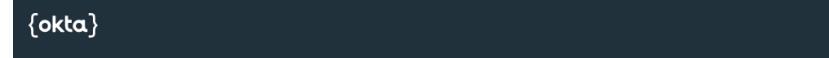
Mailchimp says it was hacked — again

Zack Whittaker @zackwhittaker / 5:45 PM GMT + January 18, 2023

Comment



Information About HubSpot's
March 18, 2022 Security
Incident



Detecting Scatter Swine: Insights into a Relentless Phishing Campaign

Defensive Cyber Operations

CLOUDFLARE The Cloudflare Blog

Product News Speed & Reliability Security Serverless Zero Trust Developers Deep Dive Life @Cloudflare

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

09/08/2022



Who?
What?
Why?
Where?
When?
How?

English-speaking cybercriminals

Successfully hacking the Fortune 500

Financially motivated

Mainly target North America

Active since early 2022 – Present

Launch persistent social engineering campaigns

They can trivially defeat enterprise-level security systems

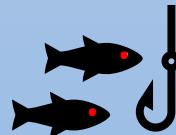
How do they do it?



The target receives an SMS text message with a malicious link



The user visits the malicious link and enters their credentials



The attackers enter the provided credentials and ask the user for the 2FA prompt



The user provides the 2FA prompt to the attacker and the attacker gains access



The attackers may also make a phone call and pose as the company IT team



Once inside, the attackers gain persistence, move laterally, and escalate privileges



Sensitive enterprise data or product source code is then stolen from the organization



The target organization is then likely to be extorted and the customer data is exploited

(Example on the next slide)

Activision Automated SMS Dispatcher:

To: [REDACTED]

Employment Status: UNDER REVIEW

[https://activision.\[REDACTED\]/employee/updateinfo/20032/](https://activision.[REDACTED]/employee/updateinfo/20032/)

5:39 PM

L

Activision Automated SMS Dispatcher:

To: [REDACTED]

Note: Please respond with the 2fa code sent

5:45 PM

L

816740

([REDACTED]) 6 • 5:45 PM

Activision Automated SMS Dispatcher:

To: [REDACTED]

Note: Issue Resolved

5:46 PM

L

Connecting to  Office 365

Sign-in with your Activision Blizzard Inc. - Prod account to access Blizzard Office 365

ACTIVISION.
BLIZZARD
ENTERTAINMENT



Sign In

Username

Password

Remember me

Sign In

Need help signing in?

Today, we received a ransom email. Needless to say, we won't pay.

While this attack disrupted our build environment and could cause issues in the future, most importantly we remain confident that no player data or player personal information was compromised.

2/7

3:00 PM · Jan 24, 2023 · 424.6K Views

"We do not wish to harm your reputation or cause public disturbance. Our sole motivation is financial gain."

"We will also provide insight into how the breach occurred and offer advice on preventing future breaches"

"It is alarming to know that you can be hacked within a matter of hours by an amateur-level hack"

"We have obtained your valuable data... your precious anti-cheat source code and the entire game code for League of Legends and its tools"

"...a small request for an exchange of \$10,000,000"

Dear Riot Games,

We have obtained your valuable data, including the precious anti-cheat source code and the entire game code for League of Legends and its tools, as well as Packman, your usermode anti-cheat. We understand the significance of these artifacts and the impact their release to the public would have on your major titles, Valorant and League of Legends. In light of this, we are making a small request for an exchange of \$10,000,000.

We uploaded a tree list pdf file, which you can view the tree of Packman and League of Legends source. If you require any files for proof, message us and we will provide you the raw file.

In return, we will immediately remove all source code from our servers and guarantee that the files will never be released to the public. We will also provide insight into how the breach occurred and offer advice on preventing future breaches. We suggest communicating through Telegram, you can join us here:

[[Telegram link](#)]

We do not wish to harm your reputation or cause public disturbance. Our sole motivation is financial gain.

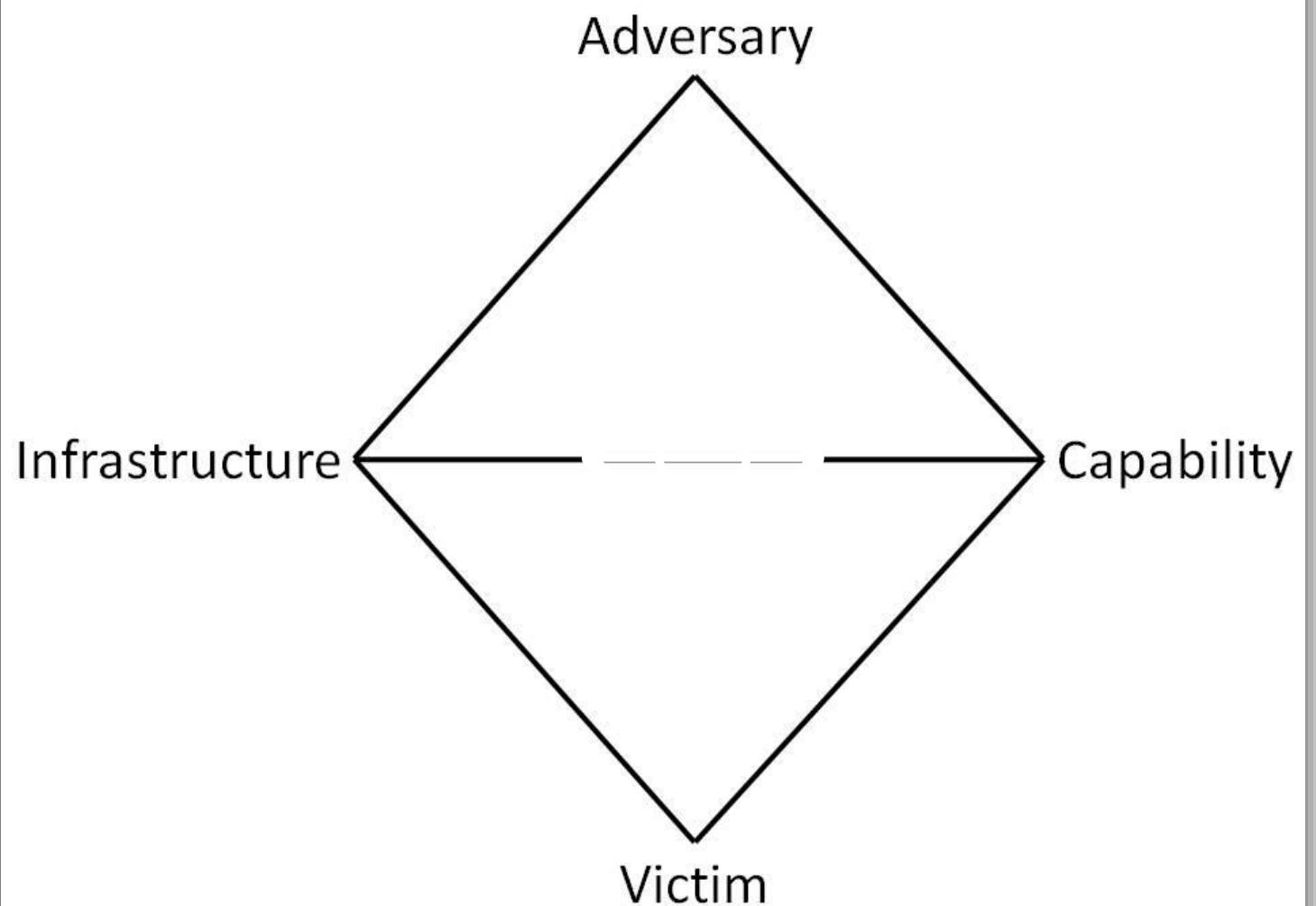
We have sent this message to the Directors only and have given you twelve hours to respond. Failure to do so will result in the hack being made public and the extent of the breach being known to more individuals.

We also want to remind you that it would be a shame to see your company publicly exposed, especially when you take great pride in your security measures. It is alarming to know that you can be hacked within a matter of hours by an amateur-level hack.

We urge you to take this matter seriously and consider our proposal.

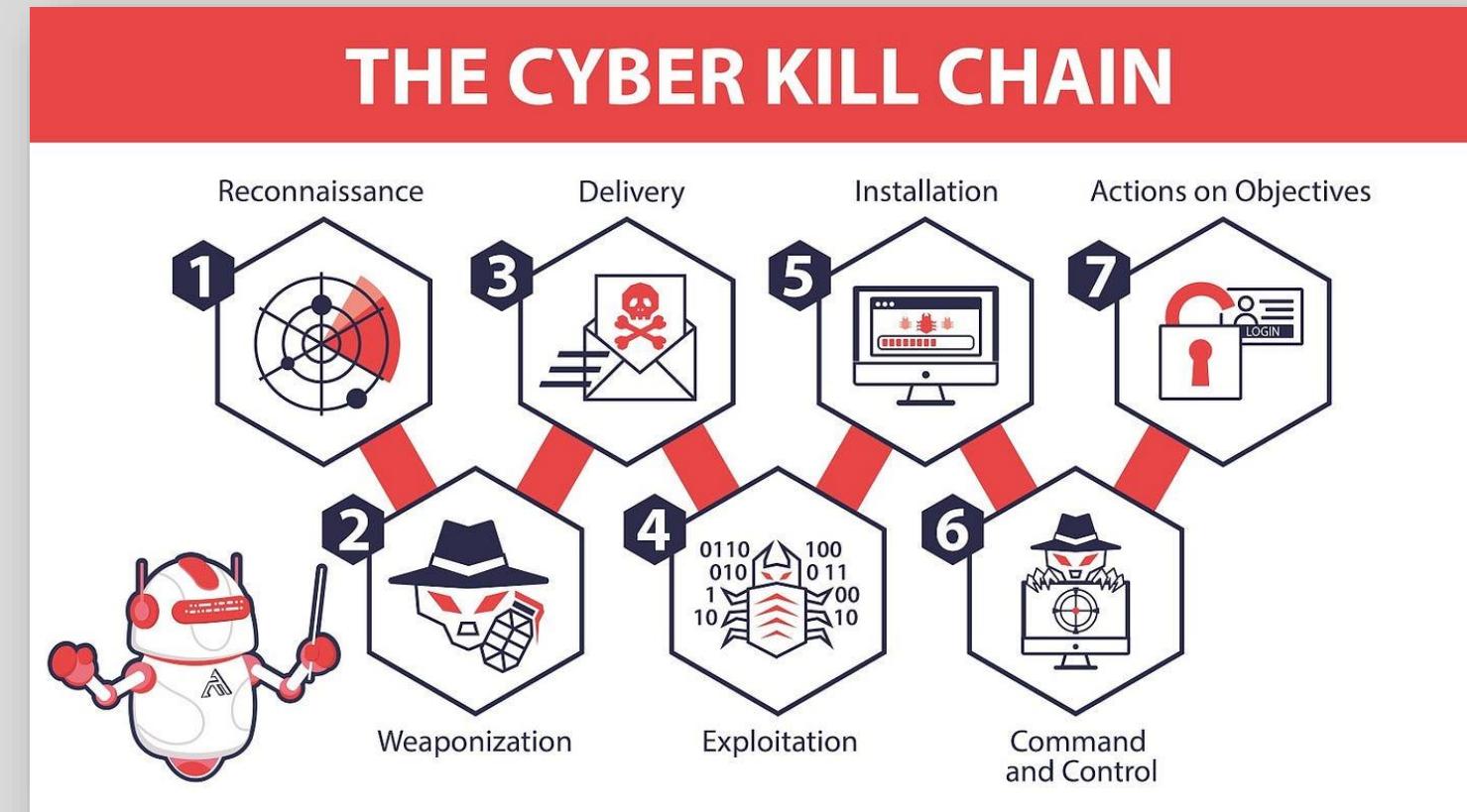
A Threat Analysis Framework

The Diamond Model



The Lockheed Martin Cyber Kill Chain®

An Intrusion Analysis Framework



The MITRE ATT&CK® framework

Adversary Tactics,
Techniques & Common
Knowledge

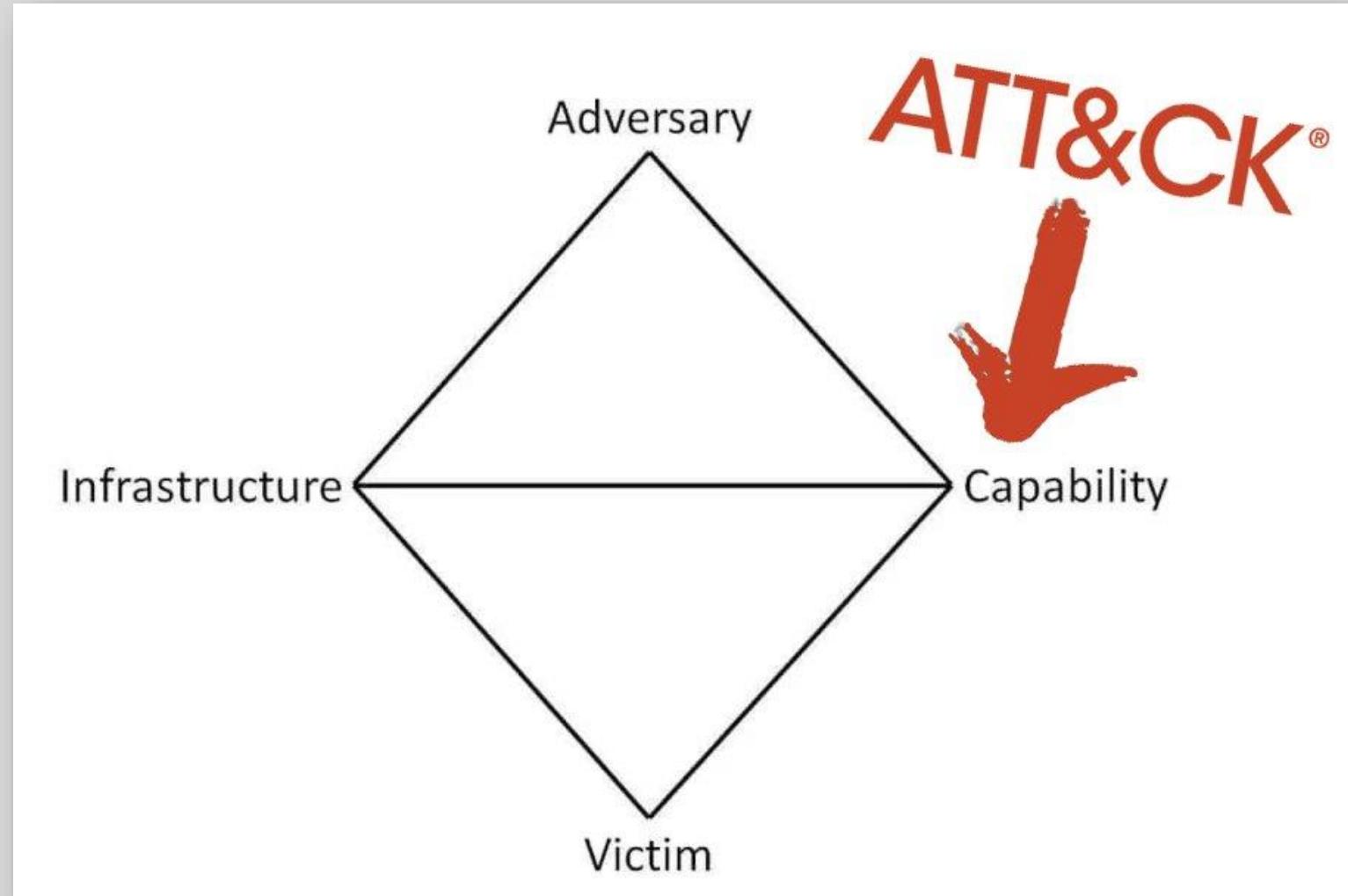
A Capability Analysis Framework

MITRE ATT&CK®											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control		
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques		
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)		
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Credentials from Password Stores (3)		Application Window Discovery	Internal Spearphishing		Audio Capture		
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)			Exploitation for Credential Access	Browser Bookmark Discovery	Automated Collection		Communication Through Removable Media		
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)		Forced Authentication	Cloud Service Dashboard	Cloud Service Discovery	Clipboard Data		Data Encoding (2)		
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Direct Volume Access	Input Capture (4)	Domain Trust Discovery	File and Directory Discovery	Remote Service Session Hijacking (2)		Data Obfuscation (3)		
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Execution Guardrails (1)	Man-in-the-Middle (1)	File and Directory Permissions Modification (2)	Network Service Scanning	Data from Cloud Storage Object		Dynamic Resolution (3)		
Supply Chain Compromise (3)	Software Deployment Tools	Create or Modify System Process (4)	Exploitation for Defense Evasion	Modify Authentication Process (3)	Network Share Discovery	Network Sniffing	Remote Services (6)		Encrypted Channel (2)		
Trusted Relationship	Create Account (3)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	Network Sniffing	Password Policy Discovery			Fallback Channels		
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	OS Credential Dumping (8)	Peripheral Device Discovery	Peripheral Device Discovery	Taint Shared Content		Ingress Tool Transfer		
	Windows Management Instrumentation	Group Policy Modification	Hide Artifacts (6)	Steal Application Access Token	Permission Groups Discovery (3)	Permission Groups Discovery (3)	Use Alternate Authentication Material (4)		Multi-Stage Channels		
			Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Process Discovery	Process Discovery	Data Staged (2)	Non-Application Layer Protocol			
			Hijack Execution Flow (11)	Indirect Command Execution	Query Registry	Query Registry	Email Collection (3)	Non-Standard Port			
			Impair Defenses (6)	Steal Web Session Cookie	Remote System Discovery	Remote System Discovery	Input Capture (4)	Protocol Tunneling			
			Indicator Removal on Host (6)	Two-Factor Authentication Interception	Software Discovery (1)	Software Discovery (1)	Man in the Browser	Proxy (4)			
			Scheduled Task/Job (5)	Unsecured Credentials (4)	System Information Discovery	System Information Discovery	Man-in-the-Middle (1)	Remote Access Software			
			Valid Accounts (4)				Screen Capture		Traffic Signaling (1)		
							Video Capture		Web Service (3)		

Oktapus/ ScatteredSpider Capabilities

- Preparation
- Social Engineering
- Evading Security
- Cloud Exploits
- Exfiltrating Data

MITRE ATT&CK



Capabilities: Preparation

Research the target's Single Sign-On (SSO) provider

- <https://duo.com/solutions/customer-stories>
- <https://www.okta.com/customers/>
- <https://customers.twilio.com/>

Using OSINT for
“Customer success stories”
reveal which organizations
use which SSO services

Use Data Brokers for Targets of Interest

- Employer
- Name
- Phone Number
- Email Addresses
- Passwords



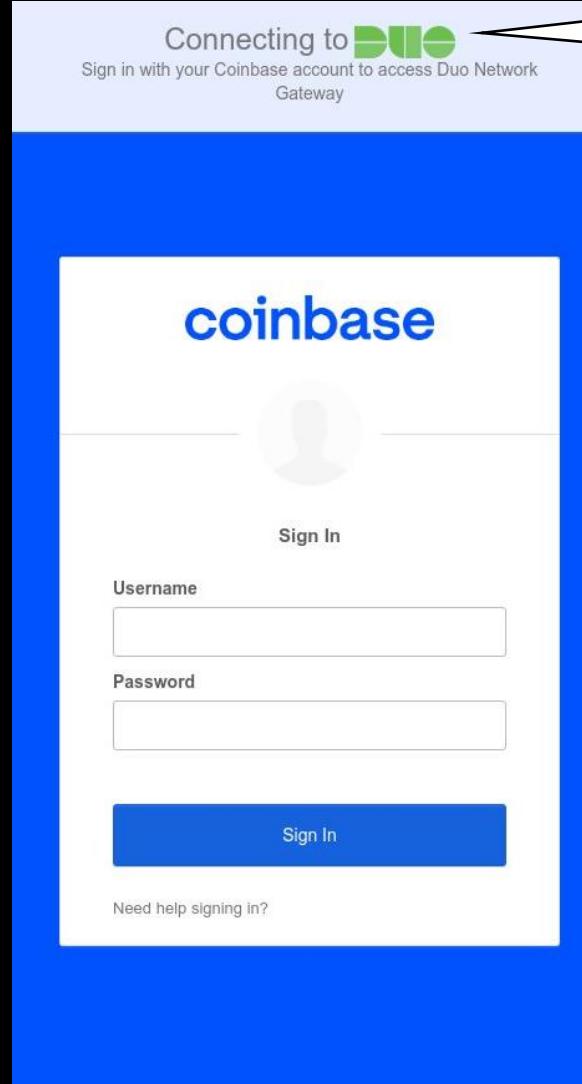
DEHASHED™



RocketReach

Capabilities: Social Engineering

- SMS phishing
 - “Schedule changed”
 - “Employment Terminated”
- Voice Calls
 - Threatening Individuals
 - Bribing Individuals
- SIM Swapping
 - Hijacking phone numbers



The adversary knew which SSO provider Coinbase used

“The attacker claimed to be from Coinbase corporate Information Technology (IT) and they needed the employee’s help”
– Coinbase (Feb. 2023)





What is SIM swapping?



SIM swapping involves tricking employees of a mobile provider into transferring someone else's number to a SIM card controlled by a threat actor



They can accomplish that by social engineering. Also, fraudsters have bribed or otherwise compromised telecommunications employees to help them



With control of a number, fraudsters can intercept one-time passcodes (OTPs) used to log into online accounts.



Successful SIM swaps have resulted in raided cryptocurrency accounts and staggering losses



Possession of a phone number can be enough to reset passwords for other online accounts as well



The victim is compromised because the mobile provider failed to securely vet the number transfer

Evading Enterprise Security

Remote Monitoring and Management (RMM) tools

- AnyDesk, TeamViewer... and 20 others

Session Hijacking

- EditThisCookie browser extension

Bring-Your-Own-Vulnerable-Driver (BYOVD)

- Intel Ethernet diagnostics driver

Code-signing Certificates

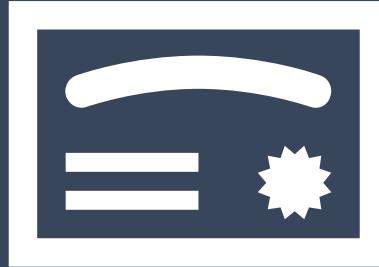
- NVIDIA stolen certificate

UEFI bootkit

- BlackLotus

Tunneling tools

- Rsocx, Ngrok, Plink



Remote Monitoring and Management (RMM) Tools

AnyDesk	BeAnywhere	Domotz	DWservice
Fixme.it	Fleetdeck.io	Itarian Endpoint Manager	Level.io
Logmein	ManageEngine	N-Able	Pulseway
Rport	Rsocx	ScreenConnect	ISL Online
Teamviewer	TrendMicro Basecamp	Sorillus	ZeroTier

(Up to 20 different RMM tools!)



A screenshot of the Google Chrome browser. The main window displays the "Welcome to Chrome" screen, which includes a "Still need help?" button and a "Learn More" link. Overlaid on the bottom-left of the screen is the "EditThisCookie" extension's cookie editor interface. This interface has a dark background with white text and several input fields. One visible field shows a cookie entry for "utma" with the value "21104190.1330160049.1.1.utma= [obscured]". Other fields include "domain" (set to "tools.google.com"), "hostOnly" (unchecked), "path" (set to "/chrome/intro/nav"), "secure" (unchecked), "httpOnly" (unchecked), and "session" (unchecked). A "expiration" section shows "2 month 5 year 2012". At the bottom of the editor is a "Submit Cookie Changes" button.

Edit all your cookies

EditThisCookie

Intended for Website Testing

Used for stealing Web Session Cookies

Enables Browser Session Hijacking attacks

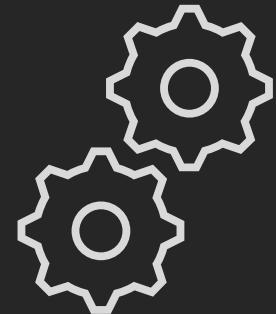
Provides access to Web Apps and SaaS platforms

Bypasses Multi-factor Authentication (MFA) protocols

Can pivot into an Authenticated Intranet

Bring-Your-Own-Vulnerable-Driver (BYOVD)

Windows does not allow unsigned kernel-mode drivers to run by default.

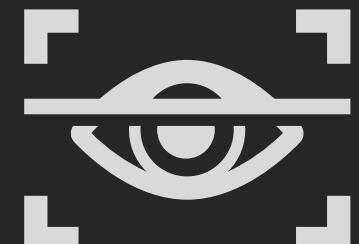


BYOVD makes it possible bypass Windows kernel protections



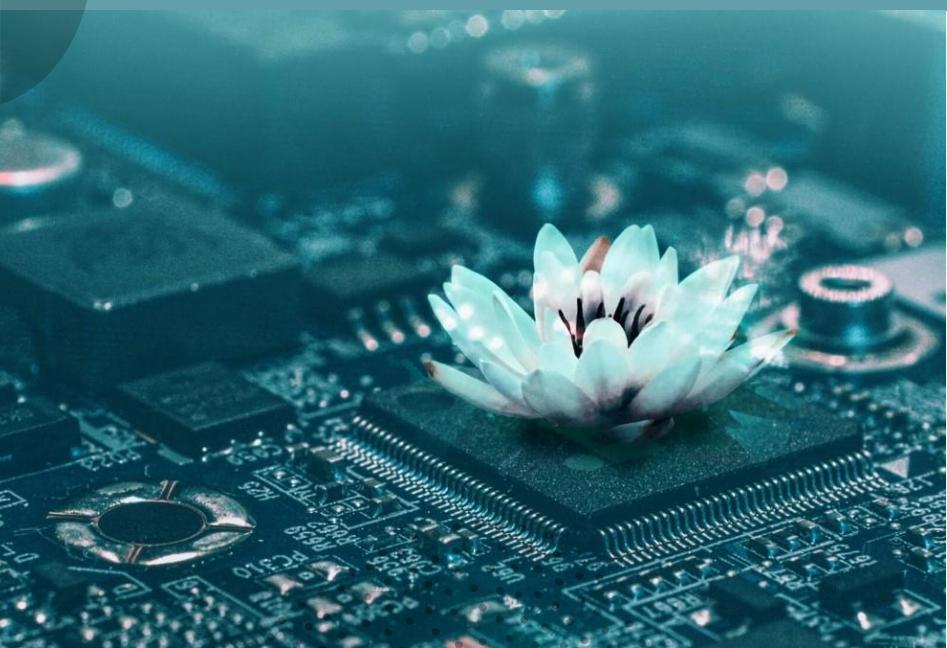
The adversary deployed an Intel Diagnostics Driver vulnerable to CVE-2015-2291

CrowdStrike saw it bypass MS Defender, Palo Alto Networks Cortex XDR, and SentinelOne EDR



By disabling the endpoint security the actor can further their actions on objectives

BlackLotus Unified Extensible Firmware Interface (UEFI) Bootkit



maxwell187 Posted October 6 Report post

kilobyte

••



Paid registration + 3 posts

35 posts Joined 08/29/22 (ID: 135469)

Activity

Dear members,

BlackLotus is a new UEFI Bootkit for Windows with integrated Secure Boot bypass and Ring0/Kernel protection against removal. The purpose of this software is to act as a HTTP Loader.

Due to the strong persistence there is no need to regularly update the Agent with new crypts. Once installed, AVs will be unable to scan and remove it.

The software consists of two main components: Agent (installed on the target device) and Web Interface (used by administrators to control bots). Bot = Device with Agent installed.

BlackLotus was first advertised on a cybercriminal underground forum in October 2022 for \$5,000

BlackLotus Features

An common unwritten rule
for malware developers
from Russian or the
Commonwealth of
Independent States (CIS)

It can run on Windows 10 and 11 systems with UEFI Secure Boot enabled

It is the first malware to exploit CVE-2022-21894 to bypass UEFI Secure Boot in Windows

It can be used to disable BitLocker, hypervisor-protected code integrity (HVCI), and Windows Defender

Some BlackLotus installers do not proceed if the host uses is in Armenia, Belarus, Kazakhstan, Moldova, Russia, or Ukraine

Also... they attack Cloud and Virtualized Infra

Azure

- Used compromised credentials to access Azure Tenants
- Launched **Azure VMs** for lateral movement to on-premises systems
- Exported the configuration of Azure AD tenants and its users

AWS

- Compromised **ForgeRock OpenAM** servers to assume **AWS Instance Roles**
- Used **aws_console** to create accounts for non-existent users issued by identity and access management (IAM) users
- Pivot from the **AWS CLI** to console sessions without the need for MFA

VMware ESXi

- Installed the **rsocx reverse proxy tool** and **Level.io RMM** tool on an ESXi hypervisor appliance
- Launched the **RustScan** port scanner from a Docker container running on an ESXi appliance

The VMware logo, featuring the word "vmware" in a lowercase sans-serif font with a registered trademark symbol.

Oktapus/ ScatteredSpider

A blueprint of
their attacks

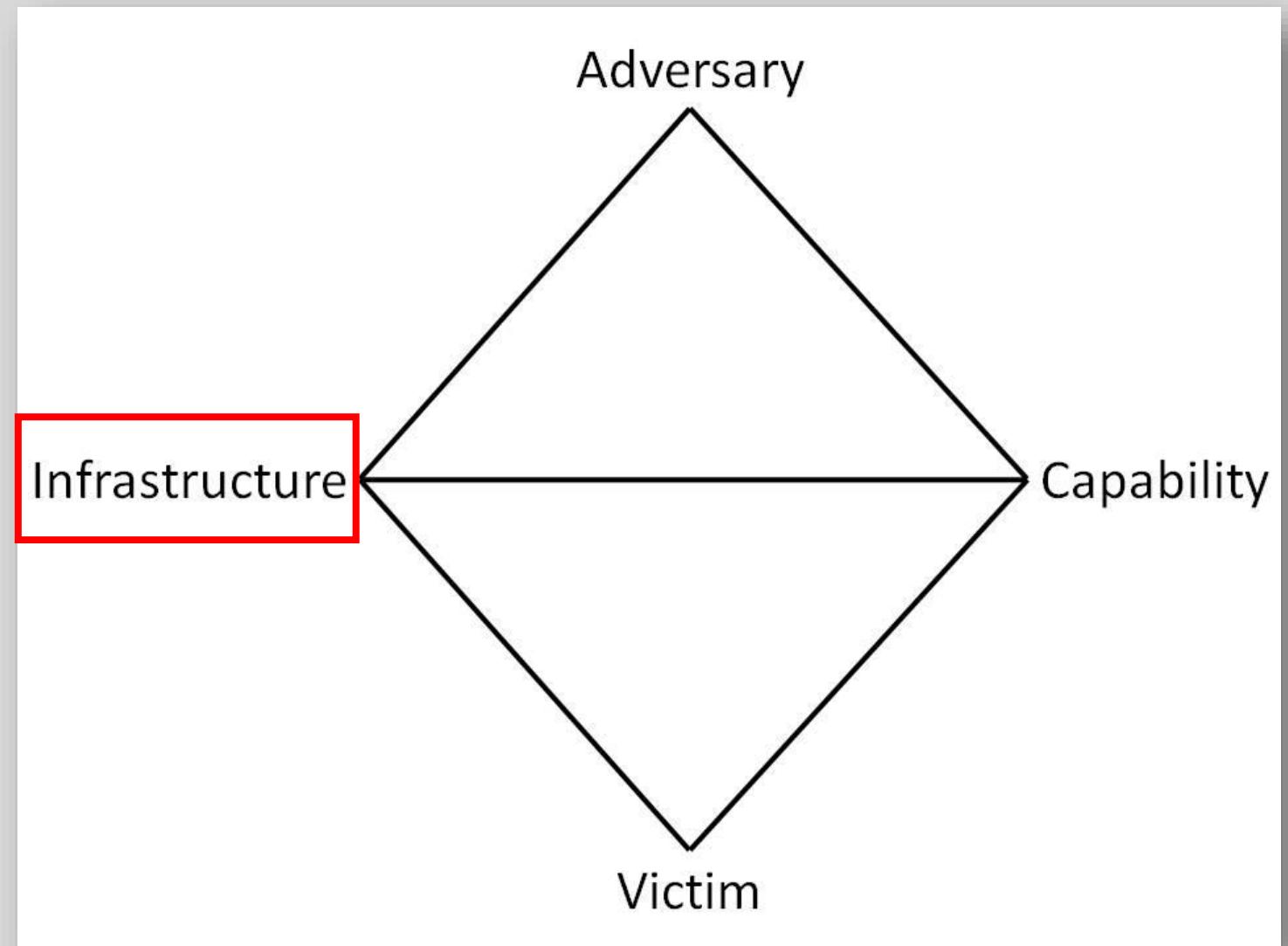
MITRE ATT&CK TTPs

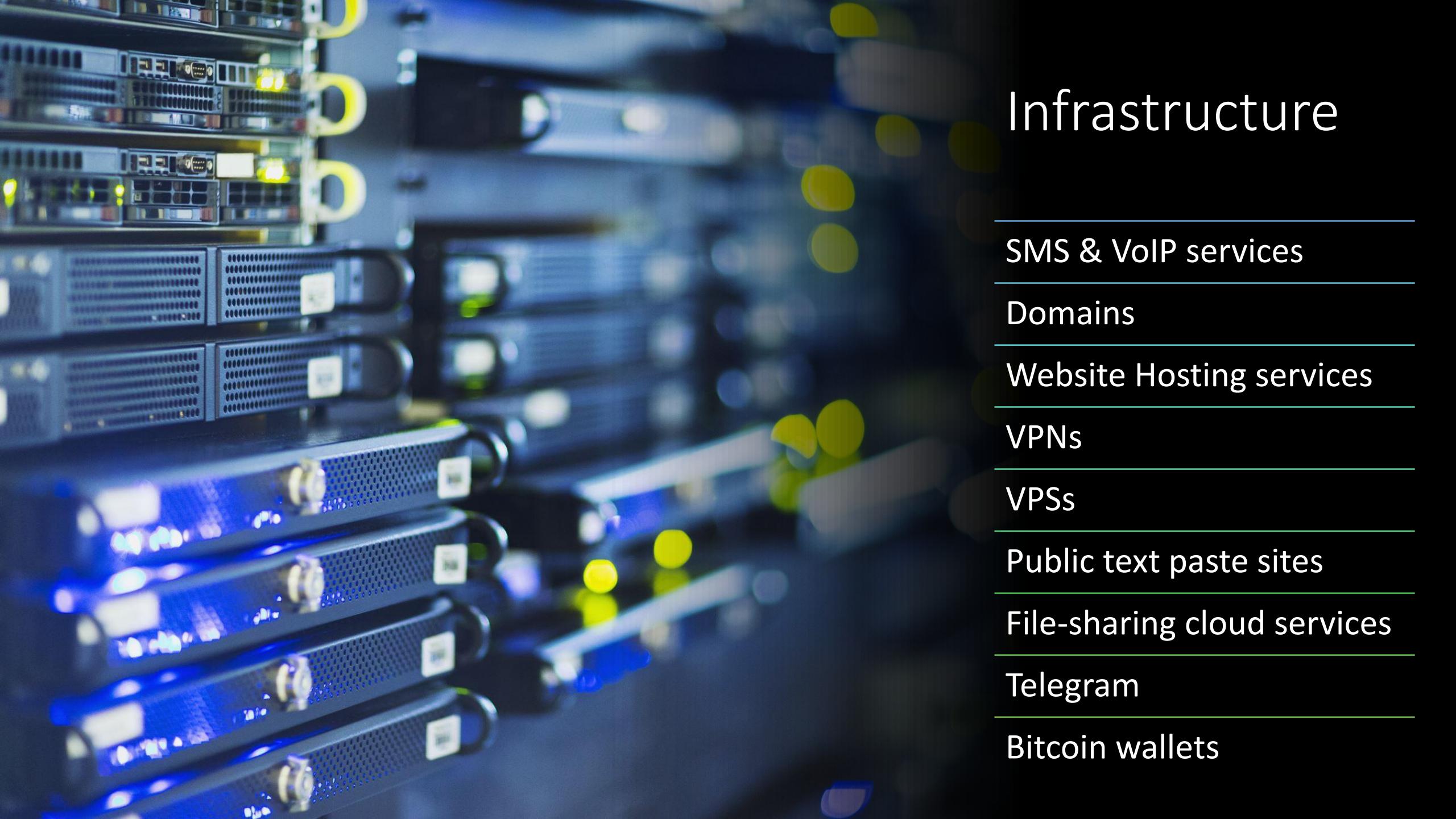
Tactic	Technique	Procedure
Reconnaissance	Gather Victim Org Information	Identify SSO provider, Clone Login Page
	Gather Victim Identity Information	Phone Numbers, Employment
Resource Development	Acquire Infrastructure	Register Domains and Host phishing pages
Initial Access	Phishing	SMS texts with malicious links
	Vishing	Calling victims and social engineering them
Execution	User Execution	Clicking malicious links, providing credentials
Persistence	Valid Accounts	Credentials provided by user via phishing
	Browser Extensions	Install Cookie stealing browser extension
Credential Access	Steal Web Session Cookie	Using the browser extension
	Code-signing	Delivers tools signed with valid certificates
Defense Evasion	Rootkit	Leverages a Windows Driver to terminate EDR
	Bootkit	Leverages BlackLotus UEFI Bootkit to disable tooling
Command and Control	Remote Access Software	Use a legitimate tool to control victim's system
	Proxy	Tunnelling tools and VPN to conceal connections
Exfiltration	Exfiltration via Cloud Service	File-sharing Cloud services to upload files to

Oktapus/ ScatteredSpider

Infrastructure

Attack and Campaign Infrastructure





Infrastructure

SMS & VoIP services

Domains

Website Hosting services

VPNs

VPSs

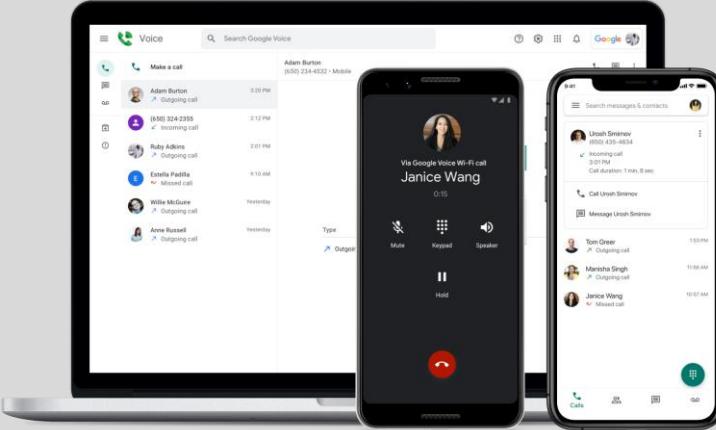
Public text paste sites

File-sharing cloud services

Telegram

Bitcoin wallets

Infrastructure: SMS for phishing and VoIP for vishing



- Communications Platform-as-a-Service
- Google Voice
- Skype
- Vonage (formerly Nexmo)
- Bandwidth



Connecting to

Sign-in with your HubSpot - Corp account to access Okta Dashboard



Sign in

Username

Password

Remember me

Sign in

Need help signing in?

twilio

Sign in

Username

Next

Need help signing in?

mailchimp

Sign In

Username

Password

Remember me

Sign In

Need help signing in?

Connecting to

Sign-in with your Activision Blizzard Inc. - Prod account to access Blizzard Office 365

ACTIVISION.





Sign In

Username

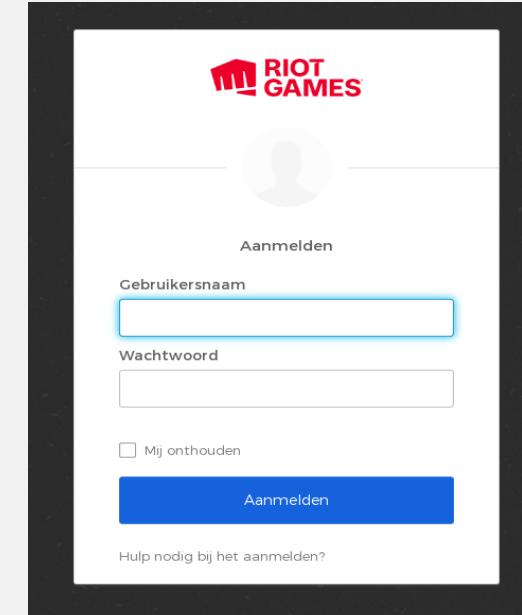
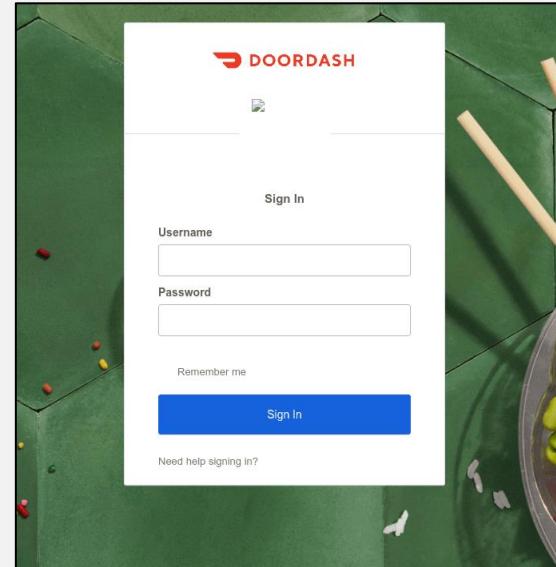
Password

Remember me

Sign In

Need help signing in?

Noticed that the same phishing kit is used for each fake login page



Infrastructure:
SMS phishing pages
posing as Single Sign-On
(SSO) authentication
logins

Infrastructure: Domains linked to SSO and Okta themed phishing pages

stargate-sso.co	okta-teams.com	grubhub-care.com	tmo-corp.com
stargate-sso.net	okta-access.com	grubhub.carebear-sso.com	t-ticket.tk
mcointernal-sso.com	oktaservice.com	grubhub-sso.com	t-helpdesk.tk
opensea-sso.com	oktasignin.com	grubhub.desk-prod.com	t-tickets.tk
luno-sso.com	riotgames-inc.com	segment-sso.com	t-tickets.com
okcoin-sso.com	riotgames-sso.com	segment.corplogon.com	tsp-tmo.com
reddit-sso.com	riot-sso.net	arise-sso.com	rss-tmo.com
sso-rbx.com	riotgames.team	arise.employee-cloud.com	rtt-tmo.com
sso-serverplan.com	corp-mailgun.com	bandwidth-sso.com	tmohelp.me
riot-sso.net	sso-mailgun.com	bandwidth.employees-cloud.com	tmoconnect.vip
sso-osp.live	service-mailgun.com	approve-sparkpost.com	t-rsa.com
sso-activecampaign.com	service-sendgrid.com	timetable-sparkpost.com	tmopanel.online
activecampaign-sso.com	sso-cbhq.com	calendar-sparkpost.com	tmo-panel.live
sso-cloud.com	sso-cb.com	schedule-sparkpost.com	t-nsa.com
networksolutions-sso.com	sso-sforce.com	workday-sparkpost.com	t-eit.info
riot-sso.com	lesschwab.cloud-auth.org	discord-okta.com	tmoeit.com
digicert-sso.com	drop-boxhr.com	discord.sso.okta.vip	calendar-tmo.com
segment-sso.com	sso-mcvpn.com	identity.mgmresurts.com	tmo-tickets.com
bandwidth-sso.com	sso-mchimp.com	benefits.mgm-resorts.health	t-rss.us
grubhub-sso.com	mailchimp.mcadmln.com	mgrmresorts.co	t-rss.com
gemini-stargate.com	mailgun-sso.com	mgmresortsapp.com	tmobile-eit.com
cloudsso-prod.com	digicert-sso.com	mgmresorts-okta.com	tmobile.vip
riotgames-sso.com	digicert.cloudsso-prod.com	schedule.mgmresorthotels.com	tmobiledesk.support

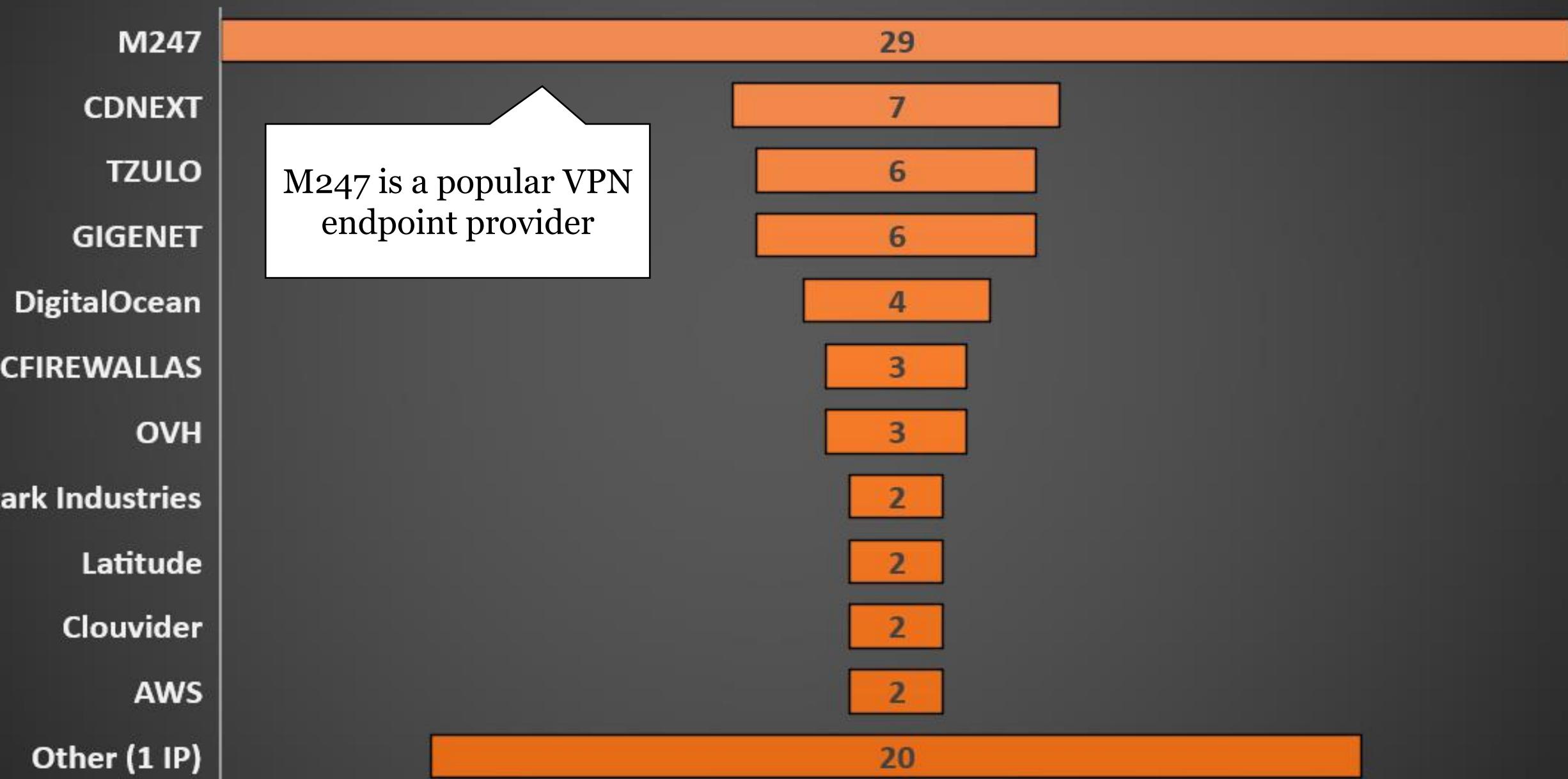
Patterns: "sso", "okta", "cloud"

Registrars: NameSilo, Tucows, Njalla

ScatteredSpider Infrastructure Analysis

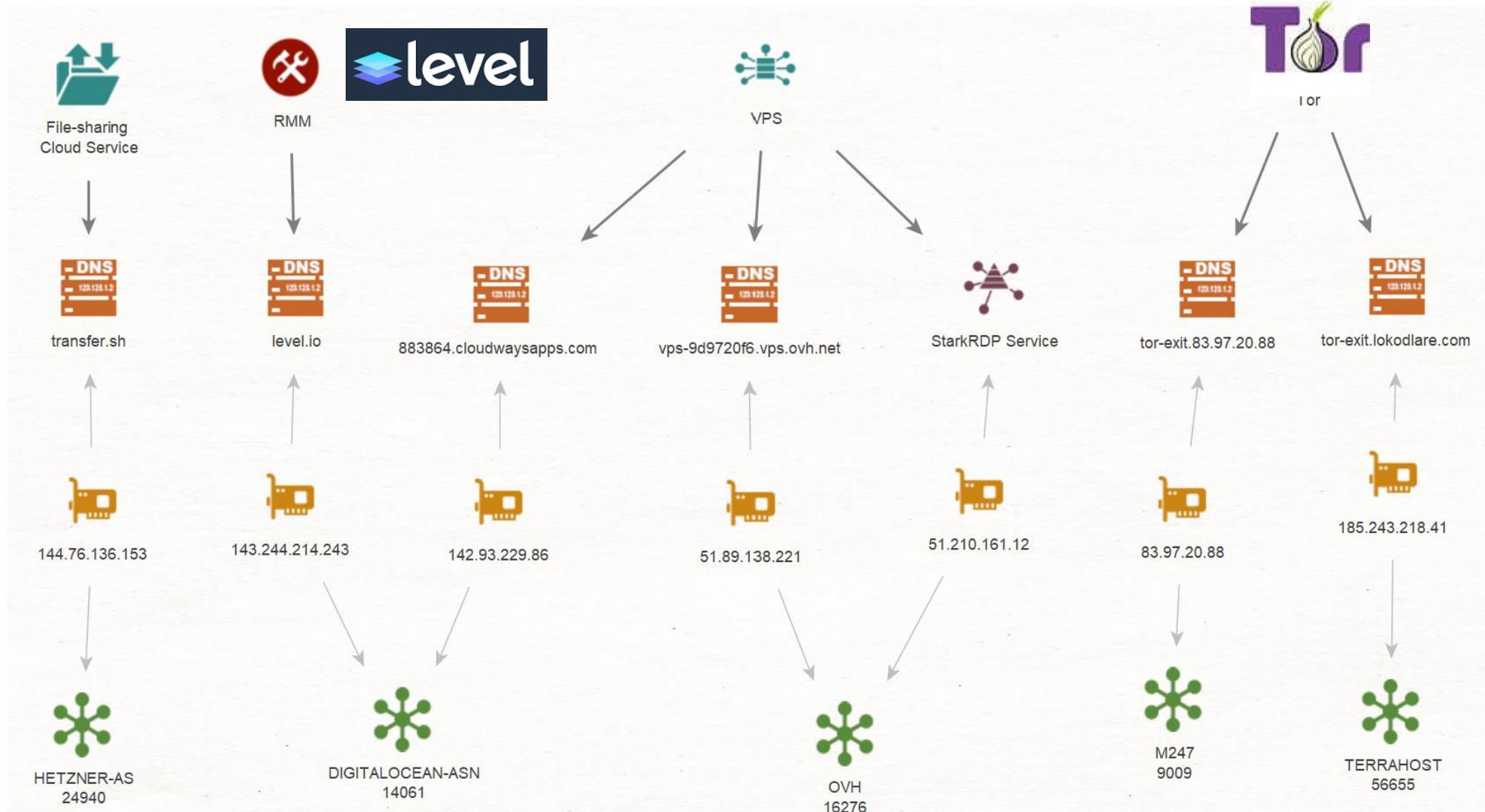
(Source: IPs shared by CrowdStrike)

IPs



(Source: IPs shared by CrowdStrike)

Infrastructure: Services



Infrastructure: VPNs

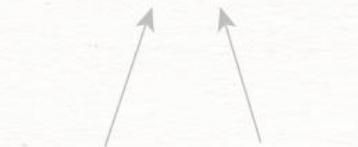
All the VPNs accept
Bitcoin as payment for
accounts



(Source: IPs shared
by CrowdStrike)



VPN Service: EXPRESS_VPN



45.91.21.61

93.115.7.238



SE



RO



NO



CA



VPN Service: SURFSHARK_VPN



146.70.103.228

146.70.112.126

146.70.127.42

146.70.45.182

146.70.45.166

193.27.13.184

217.138.222.94

68.235.43.38

68.235.43.21

185.156.46.141



US



VPN Service: MULLVAD_VPN



193.27.13.184

217.138.222.94

68.235.43.38

68.235.43.21

185.156.46.141



TZULO
11878



CDNEXT
212238



M247
9009

File-sharing Sites

Public text paste sites

- Paste[.]ee,
Riseup[.]com

File-sharing cloud services

- Transfer[.]sh,
File[.]io,
Github[.]com

The image shows two screenshots of file-sharing websites. The top screenshot is from Paste.ee, a public text paste site. It features a form with fields for 'Expiration' (set to '1 month'), 'Description' (empty), and 'Paste'. The 'Paste' section includes a 'NEW PASTE 1' button and a text input field with placeholder text 'Give this section a title'. The bottom screenshot is from share.riseup.net, a file-sharing service. It shows a browser window with the URL https://share.riseup.net. The page has a green background with a large white arrow pointing right containing the text 'Free way to store payloads in the public cloud or exfiltrate data from inside the network'. To the right of the arrow is a green button labeled 'Upload'. At the bottom of the page, there is a black footer bar with the text 'CLI - Contact - Up1' and 'Upload is currently limited to 50mb and files are stored no longer than 12 hours!'

Paste.ee

HOME ABOUT WIKI CONTACT

NOT LOGGED IN ▾

Expiration

1 month

Description

Paste

NEW PASTE 1 +

Give this section a title

Text

InPrivate

New Paste

share.riseup.net

https://share.riseup.net

Free way to store payloads in the public cloud or exfiltrate data from inside the network

Upload

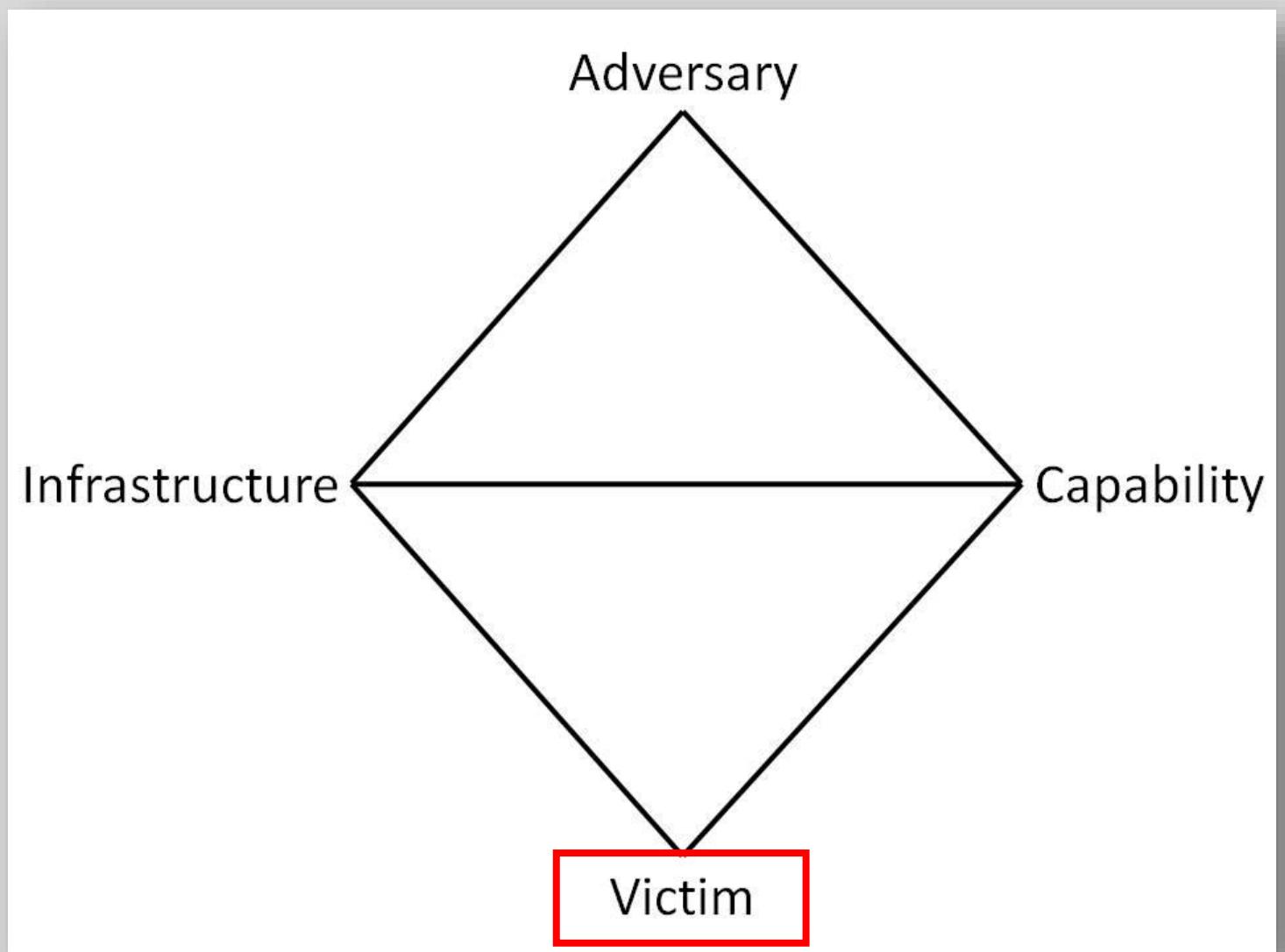
CLI - Contact - Up1

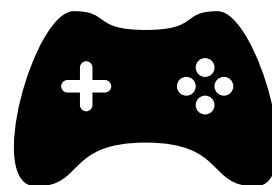
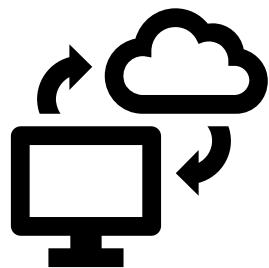
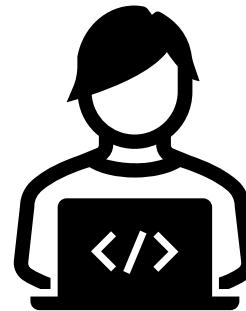
Upload is currently limited to 50mb and files are stored no longer than 12 hours!

Oktapus/ ScatteredSpider Victims

- Region
- Sector
- Systems
- People
- Information

Victims of Attacks





Victims

Targeted Regions

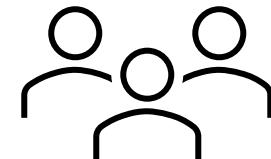
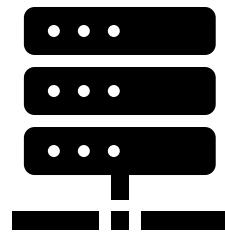
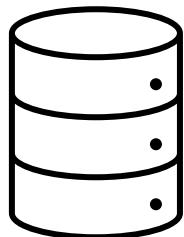
- Mainly North America
- Few in EMEA and APAC

Targeted sectors

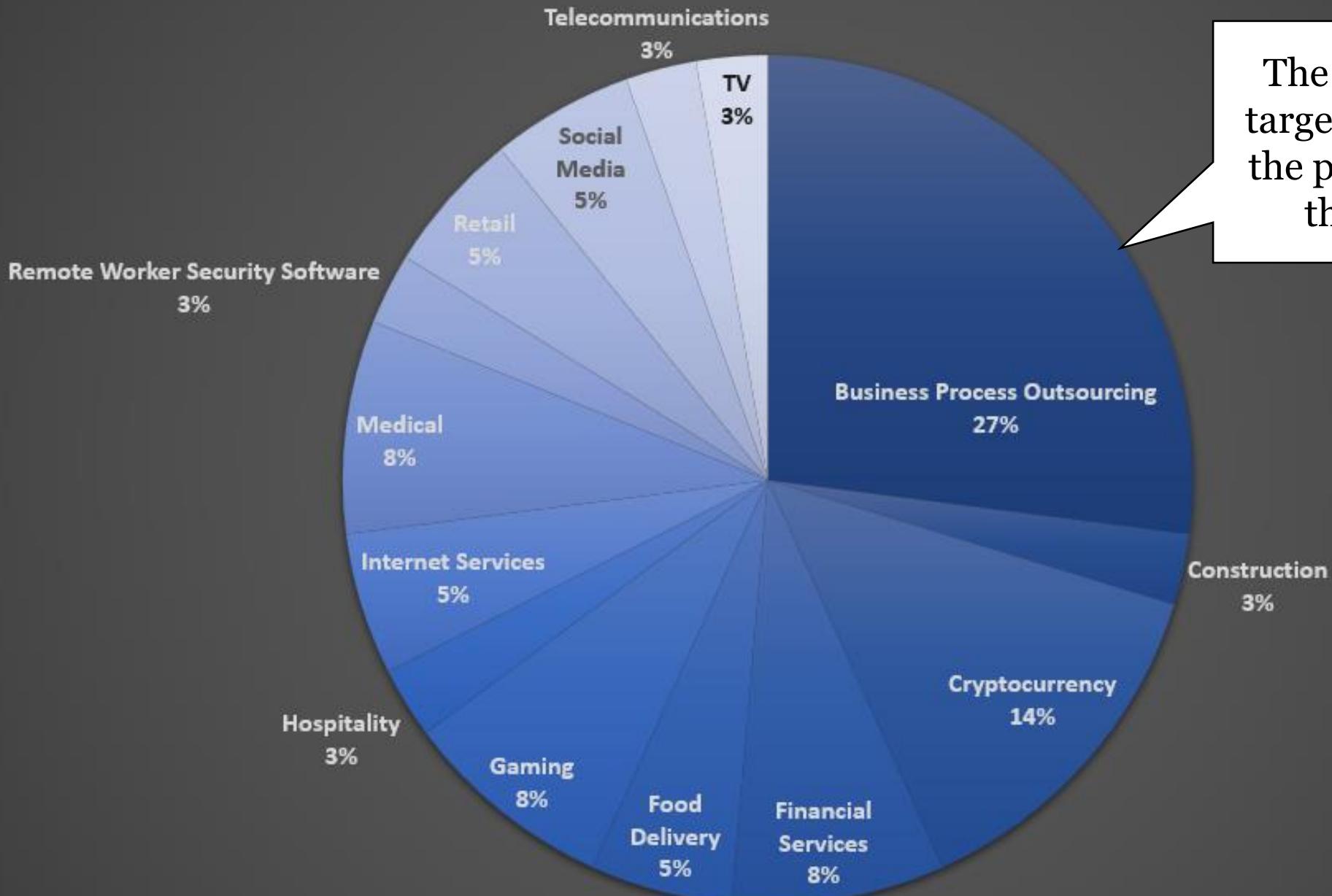
- Business Process Outsourcing (BPO)
- Software-as-a-Service
- Customer Data Platform (CDP), Customer Relationship Management (CRM), Email Marketing
- Telecommunications
- Communications Platform-as-a-Service (PaaS) that offer SMS and VoIP
- Cryptocurrency Exchanges
- Gaming Developers or Publishers
- Social Media Platforms
- Food Delivery

Victim Demographics

People targeted	Systems targeted	Information targeted
<ul style="list-style-type: none">• Employees at large organizations• IT Staff• Software Developers	<ul style="list-style-type: none">• Software-as-a-Service• Collaboration Applications• Code Repositories	<ul style="list-style-type: none">• Source Code• File Shares• Cryptocurrency Private Keys



Organizations Targeted by ScatteredSpider



The preference of targeting highlights the priorities of the threat actors

(Source: URLscan data and data breach reports)

Impact to Victims

Twilio	DoorDash	Okta	HubSpot
<ul style="list-style-type: none">Employee account was compromised163 Twilio customersCustomer contact information from user account details was stolenSMS OTP information related to a limited number of customer accounts was also accessed	<ul style="list-style-type: none">Gained access to internal tools via TwilioAccessed a small number of users' name, email address, delivery address and phone numberAccessed a smaller set of consumers' basic order information and partial payment card information	<ul style="list-style-type: none">A small number of mobile phone numbers and associated SMS messages containing the one-time passcodes were accessible to the threat actorThe threat actor gained access via the Twilio console	<ul style="list-style-type: none">An employee account was compromisedCompany HubSpot portals were accessedAffected firms: Swan and BlockFiFinancial data and funds of their customers weren't affected, but personal information was likely exposed

Impact to Victims (continued)

Cloudflare

- 76 employees were targeted in 1 minute
- Three employees entered their credentials
- FIDO2-compliant YubiKeys are required for authentication **stopped the attack**

Coinbase

- One employee entered their credentials
- The SSO MFA requirement **locked the attacker out**
- The employee was called by the attacker and **socially engineered** into giving them access
- Other **Coinbase employee details** were accessed

Activision

- One employee's account was compromised
- **Employee personal information** was stolen by the attackers
- Data related to Activision's Call of Duty franchise **was accessed** and screenshots were shared online

RiotGames

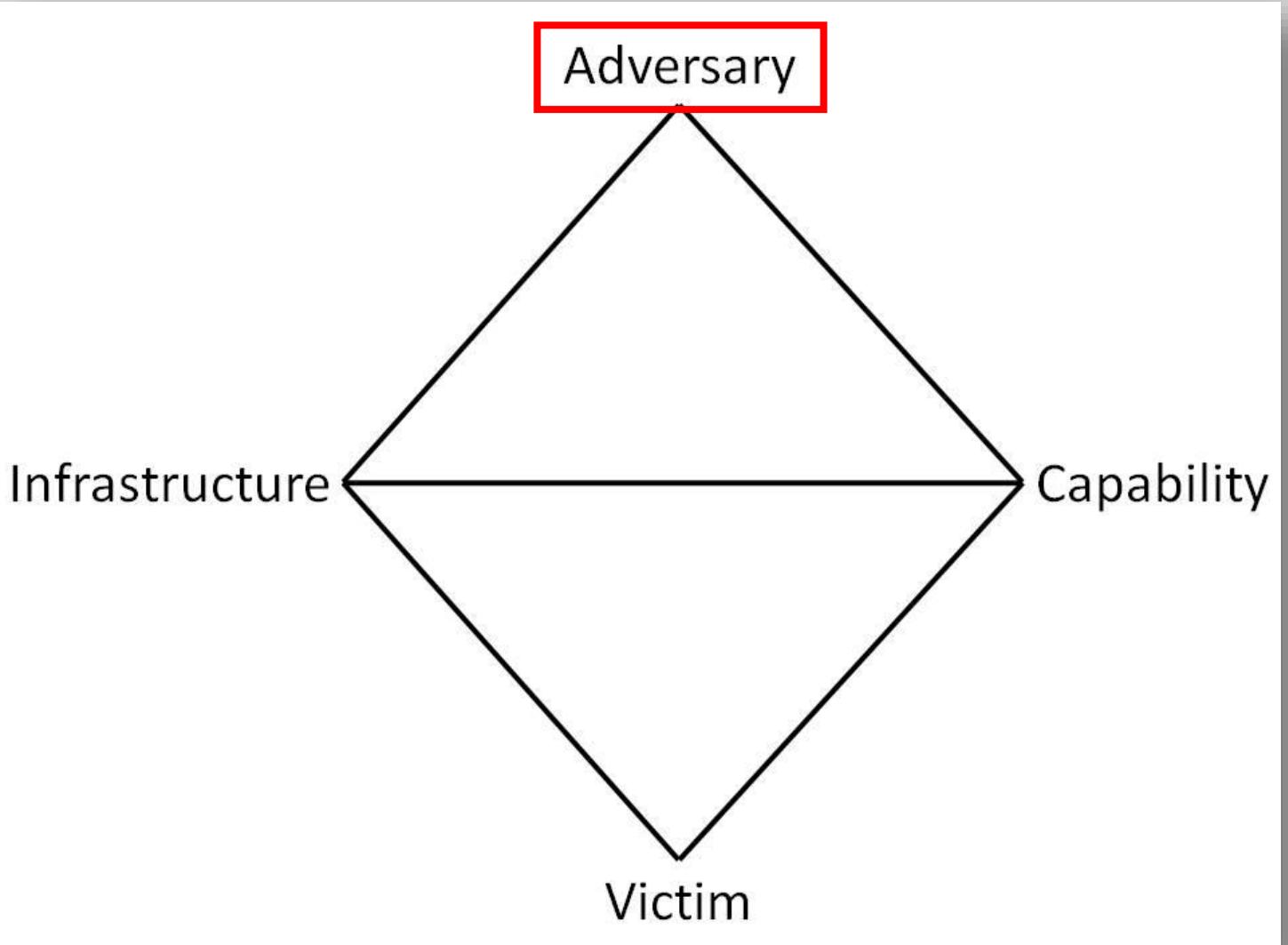
- An employee was granted access to the **development environment** was phished
- **Source code** for League of Legends and Teamfight Tactics, as well as the company's legacy anti-cheat system was stolen
- **\$10 million USD ransom** was demanded

Oktapus/ ScatteredSpider

The Adversaries

- Attributes
- Objectives
- Who?

Completing the Diamond



Adversary

Aliases

- Oktapus (Group-IB)
- SCATTERED SPIDER (CrowdStrike)
- UNC3944 (Mandiant)

Attributes

- English-speaking
- Likely young adolescents
- Financially motivated

Objectives

- Data Exfiltration
- Source Code Theft and Extortion
- Cryptocurrency Theft



Adversary Summary



- Not too technologically advanced but rehearsed in enterprise-level security protection systems
 - Has a focus on social engineering and targeting the human factor of security
 - They do not develop their own malware or tools, they either use free or trial software or purchase it from the cybercrime underground
- **Important Final Assessment:**
- This adversary should be treated more like a community of threat actors – rather than tracked as a monolithic entity – due to the wide range of TTPs, targets, and actions on objectives

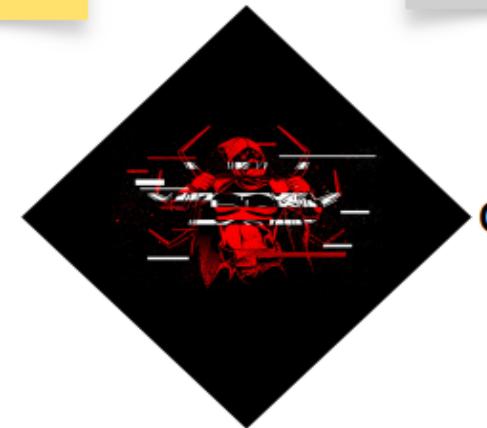
Oktapus
ScatteredSpider
UNC3944

Adversary

English-speaking
Financially motivated

Infrastructure

SMS and VoIP services
SSO-themed domains
Paste Sites
VPNs
Bitcoin Wallets



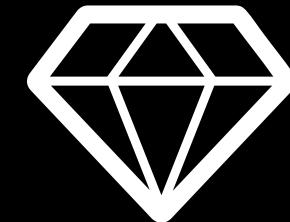
Victim

Business Process Outsourcing (BPO)
Telecommunications
Gaming and Social Media
Cryptocurrency
Software Source Code

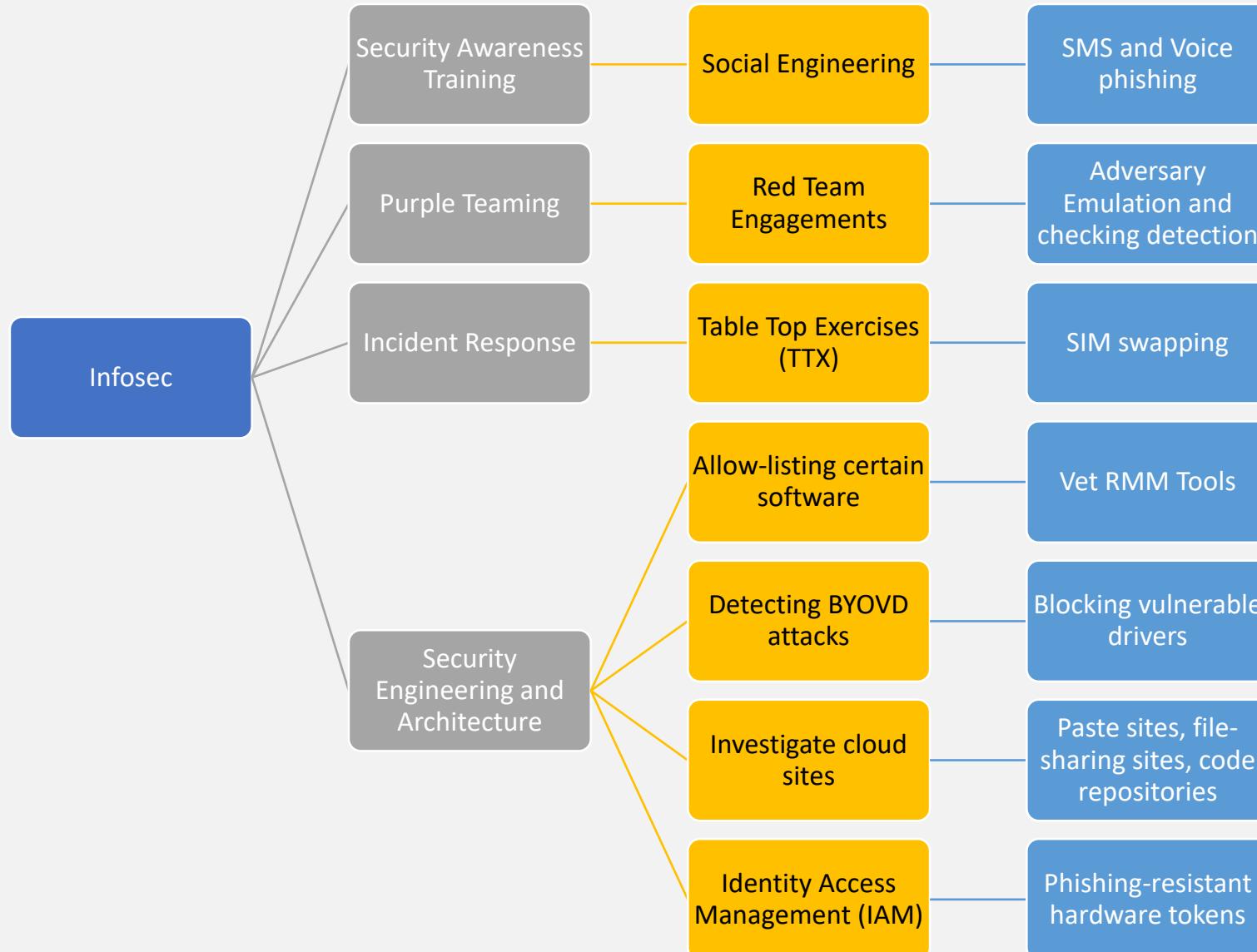
Capabilities

Social Engineering
SMS phishing
Vishing
Site Cloning
RMM Tools
Proxies
BYOVD
UEFI Bootkit
OSINT
Breach Data

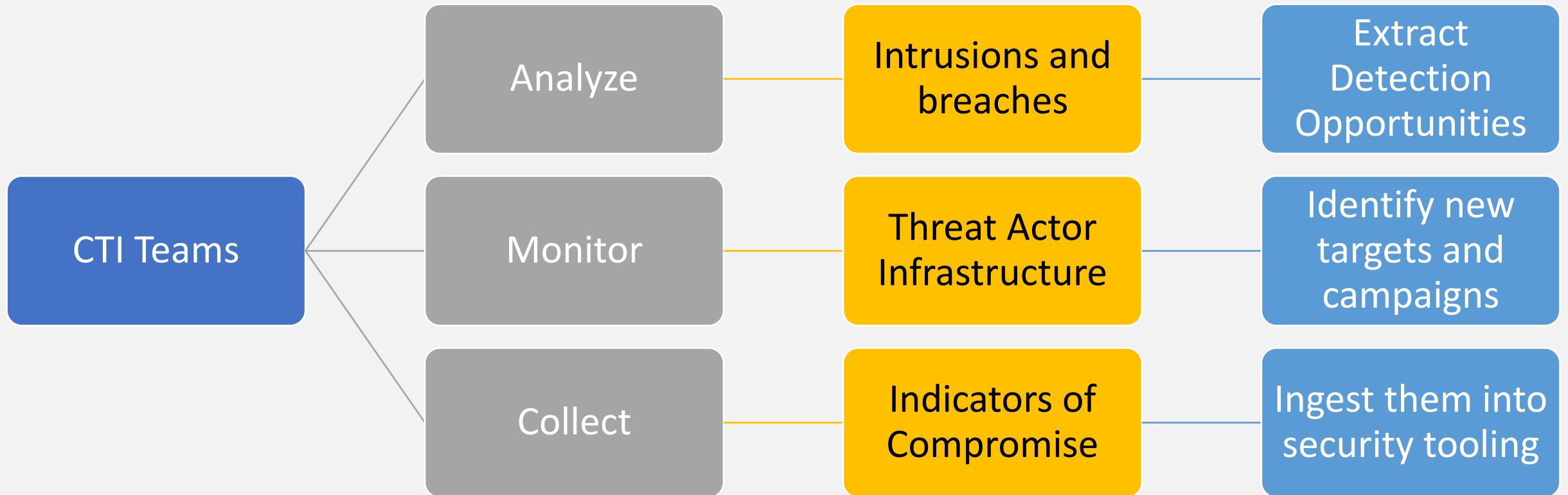
Completing the Diamond



Mitigating these attacks before they happen:



How Cyber Threat Intelligence can help:



Thanks for Listening!

- blog.bushidotoken.net
- twitter.com/BushidoToken
- github.com/BushidoUK
- sans.org/profiles/will-thomas
- linkedin.com/in/william-t



References

- [https://www.reddit.com/r/reddit/comments/10y427y/we had a security incident heres what we know/](https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/)
- <https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/>
- <https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/>
- <https://www.twilio.com/blog/august-2022-social-engineering-attack>
- <https://techcrunch.com/2022/08/08/twilio-breach-customer-data/>
- <https://www.bleepingcomputer.com/news/security/twilio-breach-let-hackers-gain-access-to-authy-2fa-accounts/>
- <https://twitter.com/signalapp/status/1559221383107854336>
- <https://doordash.news/get-the-facts/how-were-responding-to-a-third-party-vendor-phishing-incident/>
- <https://www.digitalocean.com/blog/digitalocean-response-to-mailchimp-security-incident>
- <https://mailchimp.com/en-gb/august-2022-security-incident/>
- <https://blog.group-ib.com/0ktapus>
- <https://blog.cloudflare.com/2022-07-sms-phishing-attacks/>
- <https://sec.okta.com/scatterswine>
- <https://www.hubspot.com/en-us/march-2022-security-incident>
- <https://techcrunch.com/2023/01/18/mailchimp-hacked/>
- <https://techcrunch.com/2023/01/24/riot-games-hack-cheaters/>
- <https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study>