Modern Kill Chains

Real World SaaS Attacks and Mitigation Strategies

Cory Michal
VP of Security

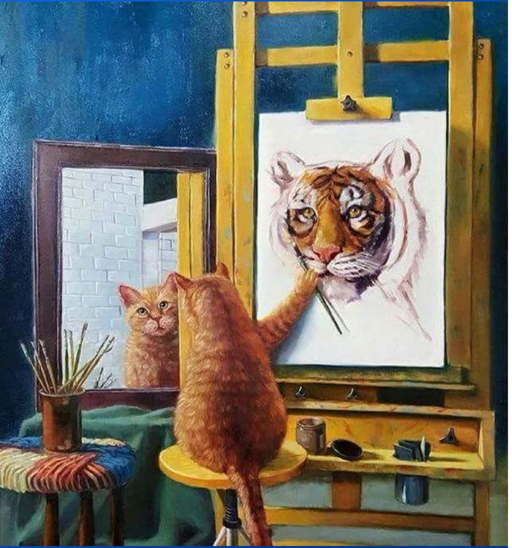
Brandon Levene
Principal Product Manager, Threat Detection

Ben Pruce
Lead Threat Detection Engineer

August 7, 2024

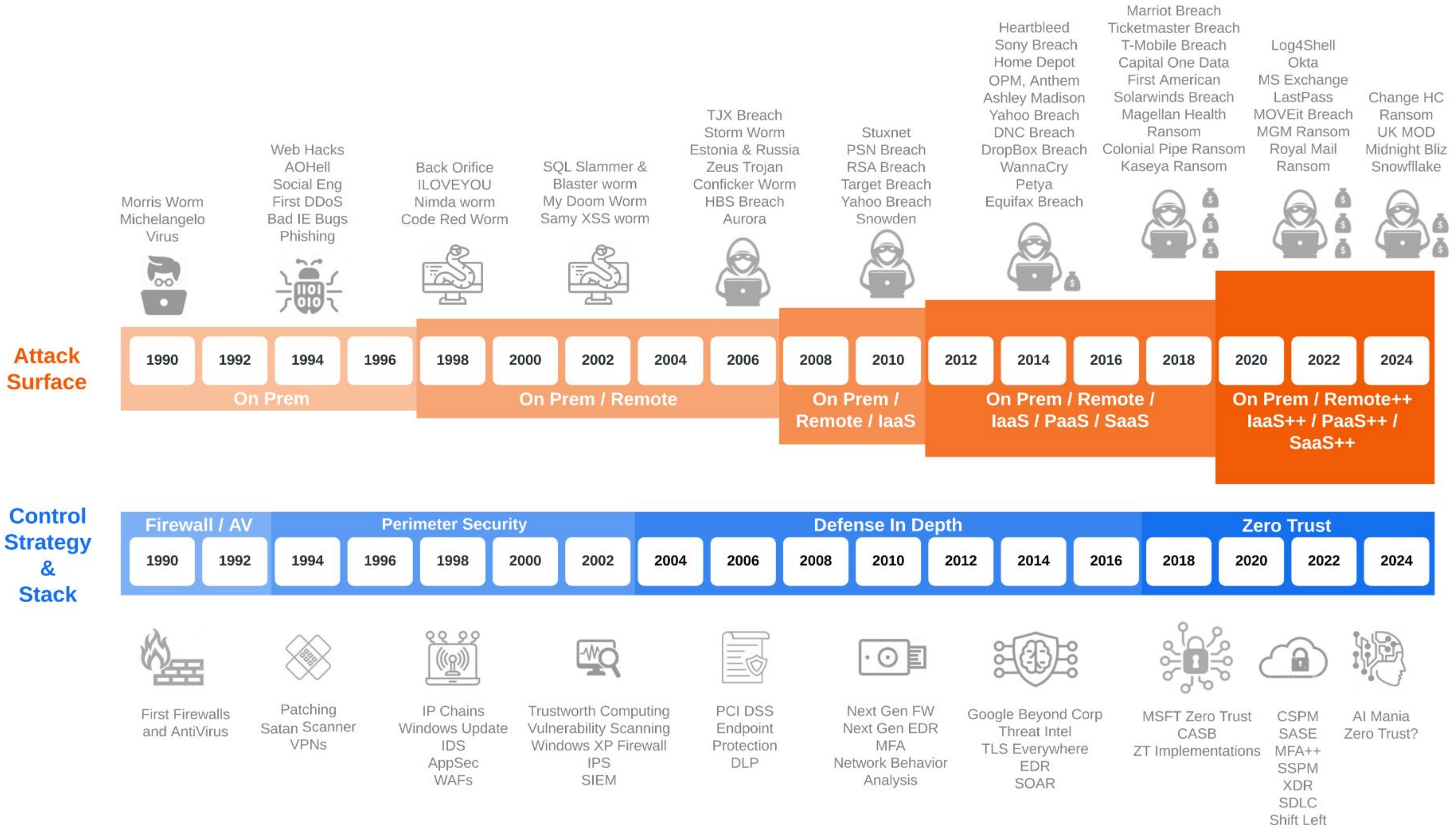
black hat

Agenda



- Reflect on where we are currently
- Hypothesize why we are here
- Examine what it is like to be here
- Determine if something better is possible
- Outline how we could move to better state

Historical Attack Surface Change



Morris Worm
Michelangelo
Virus

Web Hacks
AOHell
Social Eng
First DDoS
Bad IE Bugs
Phishing

Back Orifice
ILOVEYOU
Nimda worm
Code Red Worm

SQL Slammer &
Blaster worm
My Doom Worm
Samy XSS worm

TJX Breach
Storm Worm
Estonia & Russia
Zeus Trojan
Conficker Worm
HBS Breach
Aurora

Stuxnet
PSN Breach
RSA Breach
Target Breach
Yahoo Breach
Snowden

Heartbleed
Sony Breach
Home Depot
OPM, Anthem
Ashley Madison
Yahoo Breach
DNC Breach
DropBox Breach
WannaCry
Petya
Equifax Breach

Marriot Breach
Ticketmaster Breach
T-Mobile Breach
Capital One Data
First American
Solarwinds Breach
Magellan Health
Ransom
Colonial Pipe Ransom
Kaseya Ransom

Log4Shell
Okta
MS Exchange
LastPass
MOVEit Breach
MGM Ransom
Royal Mail
Ransom

Change HC
Ransom
UK MOD
Midnight Bliz
Snowfllake

Attack Surface

1990 1992 1994 1996 1998 2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020 2022 2024

On Prem

On Prem / Remote

On Prem / Remote / IaaS

On Prem / Remote / IaaS / PaaS / SaaS

On Prem / Remote++ IaaS++ / PaaS++ / SaaS++

Control Strategy & Stack

Firewall / AV

Perimeter Security

Defense In Depth

Zero Trust

1990 1992 1994 1996 1998 2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020 2022 2024

First Firewalls
and AntiVirus

Patching
Satan Scanner
VPNs

IP Chains
Windows Update
IDS
AppSec
WAFs

Trustworth Computing
Vulnerability Scanning
Windows XP Firewall
IPS
SIEM

PCI DSS
Endpoint
Protection
DLP

Next Gen FW
Next Gen EDR
MFA
Network Behavior
Analysis

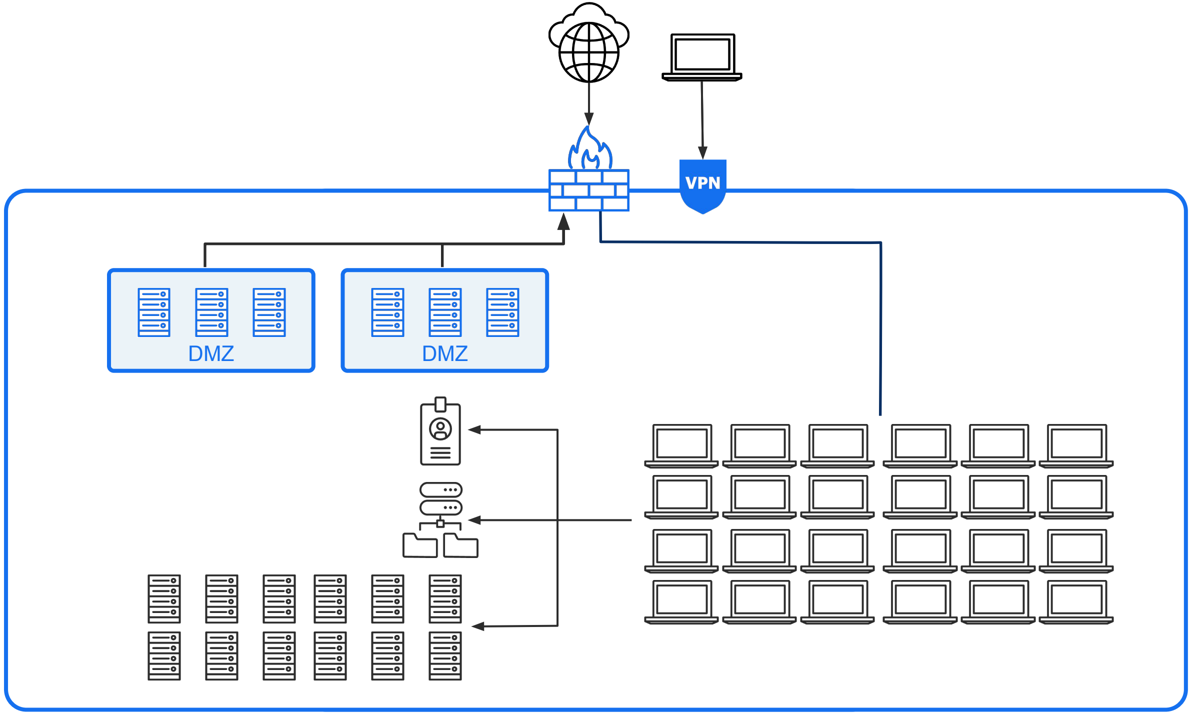
Google Beyond Corp
Threat Intel
TLS Everywhere
EDR
SOAR

MSFT Zero Trust
CASB
ZT Implementations

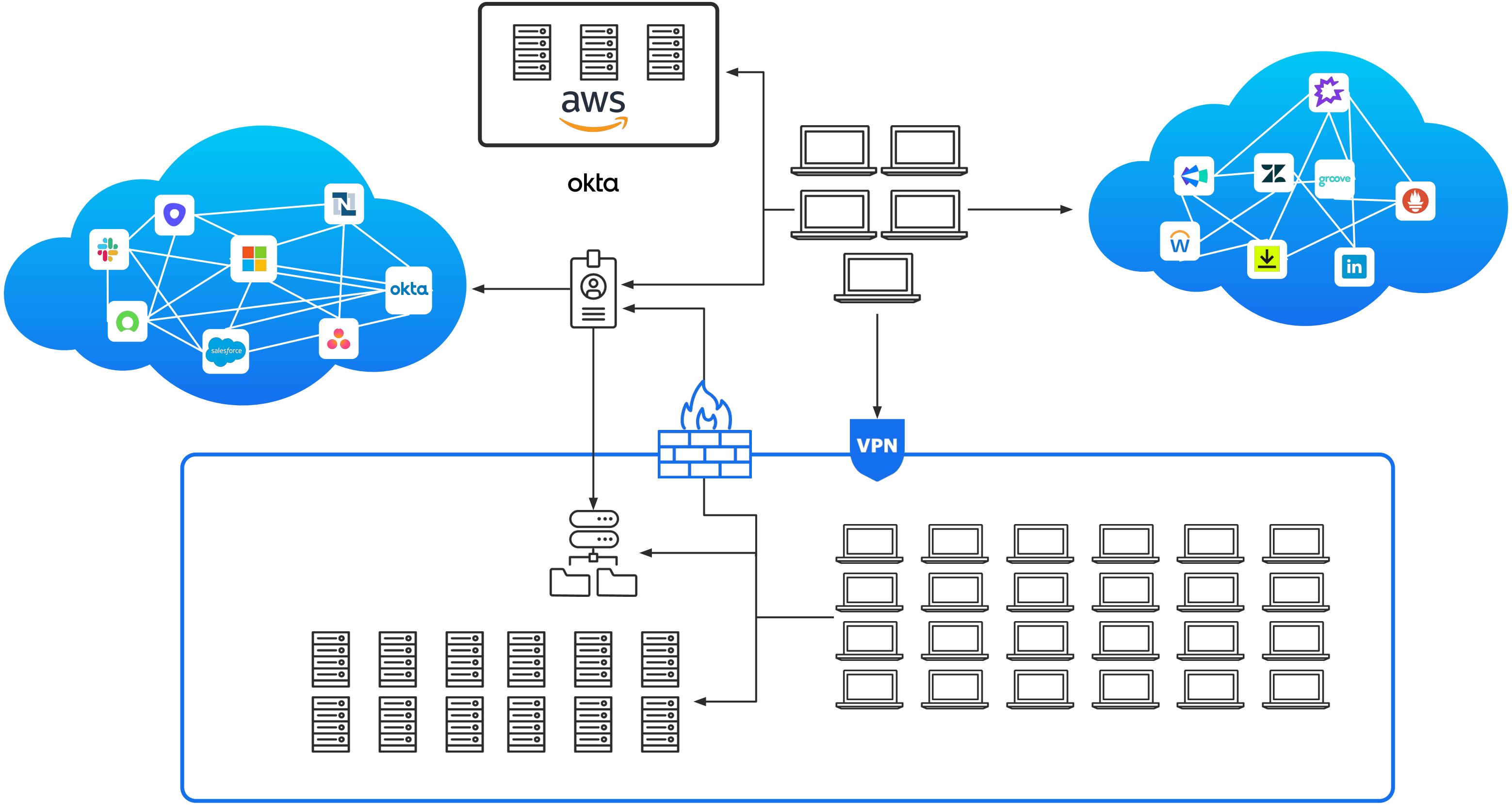
CSPM
SASE
MFA++
SSPM
XDR
SDLC
Shift Left

AI Mania
Zero Trust?

Pre Cloud & SaaS Attack Surface ~ 2009



Modern Attack Surface ~ 2020



Attack Surface Observations

Legacy Attack Surface

- Hardened network perimeters
- VPN access
- Physical access controls
- Network Access Control / Wifi
- Endpoint protection
- Internal IdP
- Internal IT Systems
- Internal Business Systems
- Logging / Monitoring / SIEM / Flow

Modern Attack Surface

⬇ Rapidly dissolving perimeters

⬇ Access from work or BYOD

⬇ Remote access from anywhere

⬇ Uncontrolled network upstream

⬆ Endpoint protection

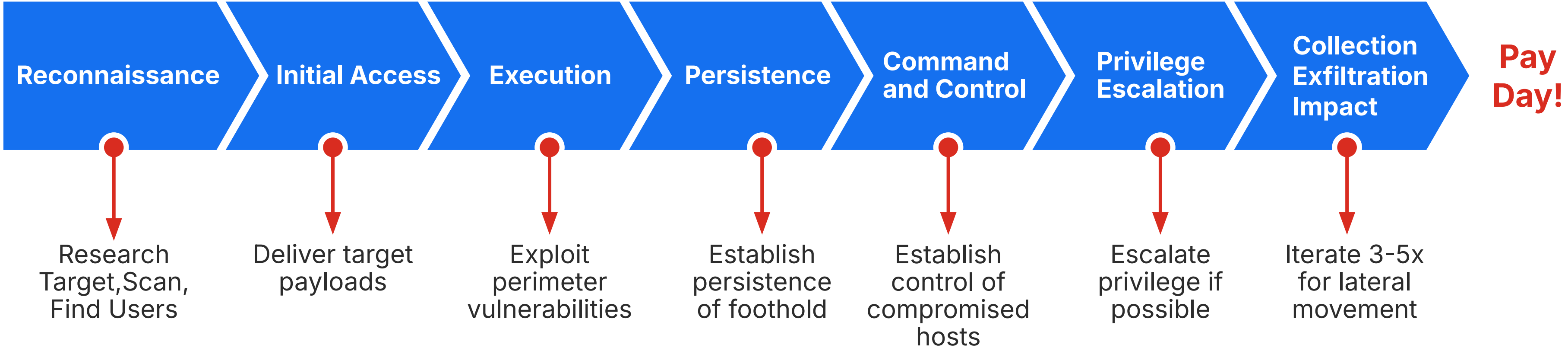
⬇ External IdP

⬇ External SaaS Systems

➡ External IaaS/PaaS

⬇ Substantially reduced visibility

Pre-Cloud and SaaS Mapped to ATT&CK



Reconnaissance

Research Target,Scan, Find Users

Initial Access

Deliver target payloads

Execution

Exploit perimeter vulnerabilities

Persistence

Establish persistence of foothold

Command and Control

Establish control of compromised hosts

Privilege Escalation

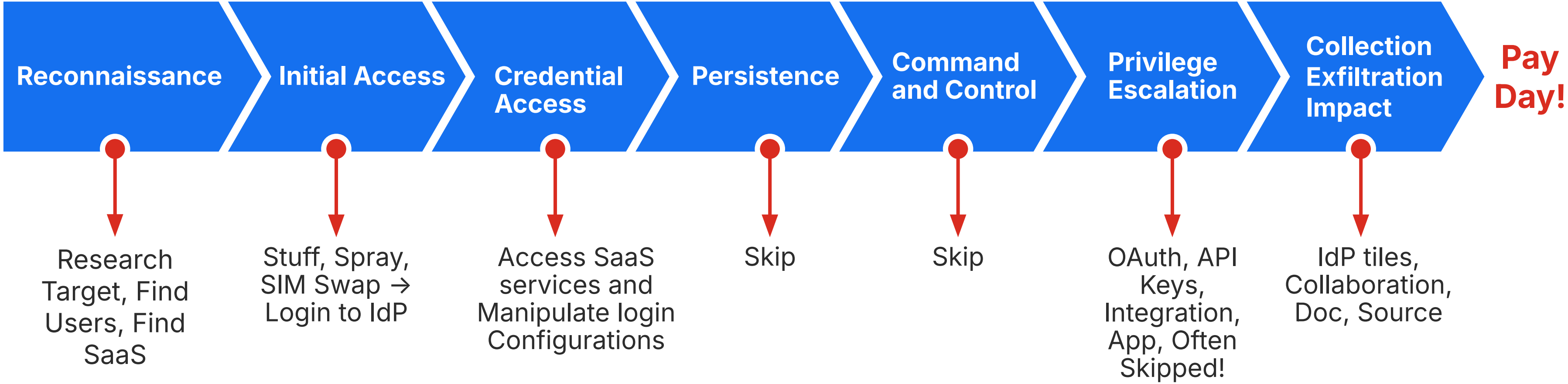
Escalate privilege if possible

Collection Exfiltration Impact

Iterate 3-5x for lateral movement

Pay Day!

SaaS ATT&CK Tactics



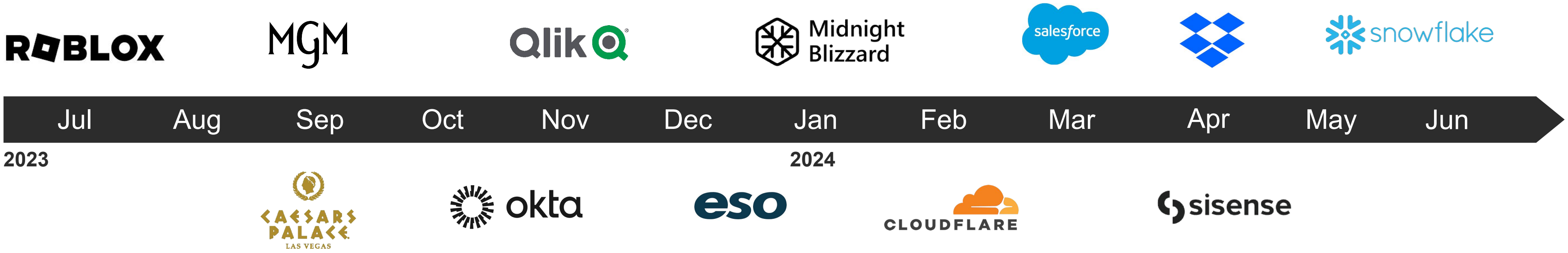
Reconnaissance
Initial Access
Credential Access
Persistence
Command and Control
Privilege Escalation
Collection Exfiltration Impact
Pay Day!
Research Target, Find Users, Find SaaS
Stuff, Spray, SIM Swap → Login to IdP
Access SaaS services and Manipulate login Configurations
Skip
Skip
OAuth, API Keys, Integration, App, Often Skipped!
IdP tiles, Collaboration, Doc, Source

This is Why We Can’t Have Nice Things

- Substantially expanded our attack surface
- Attack surface is now on other people’s stacks
- IaaS and SaaS companies have similar problems
- Substantially reduced effective security controls
- Shortened and compressed the Kill Chains
- Internet remains a relatively lawless free for all

2010
Lets put IdP
on Internet
2020
Lets put IdP
on Internet
imgflip.com

Current State of Affairs



ROBLOX

MGM

Qlik

Midnight Blizzard

salesforce

snowflake

Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun

2023

2024

CAESARS PALACE LAS VEGAS

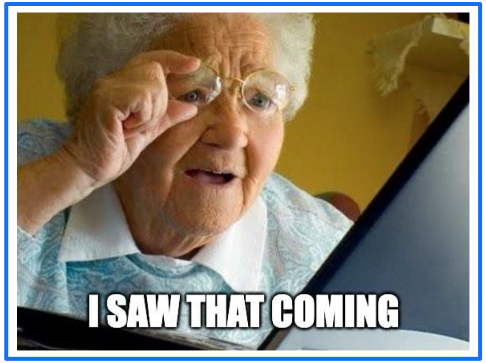
okta

eso

CLOUDFLARE

sisense

- Phishing, Social Eng, SIM Swap groups - Winning
- Ransomware Affiliates and RaaS Platforms - Winning
- Credential Spraying Actors - Winning
- Infostealer Actors – Winning
- APTs Hacking Supply Chain - Winning
- Sophisticated attackers we don’t see – Probably Winning
- Organizations and Regular folks on the Internet - Losing



Telemetry Information

Raw Processed Data:

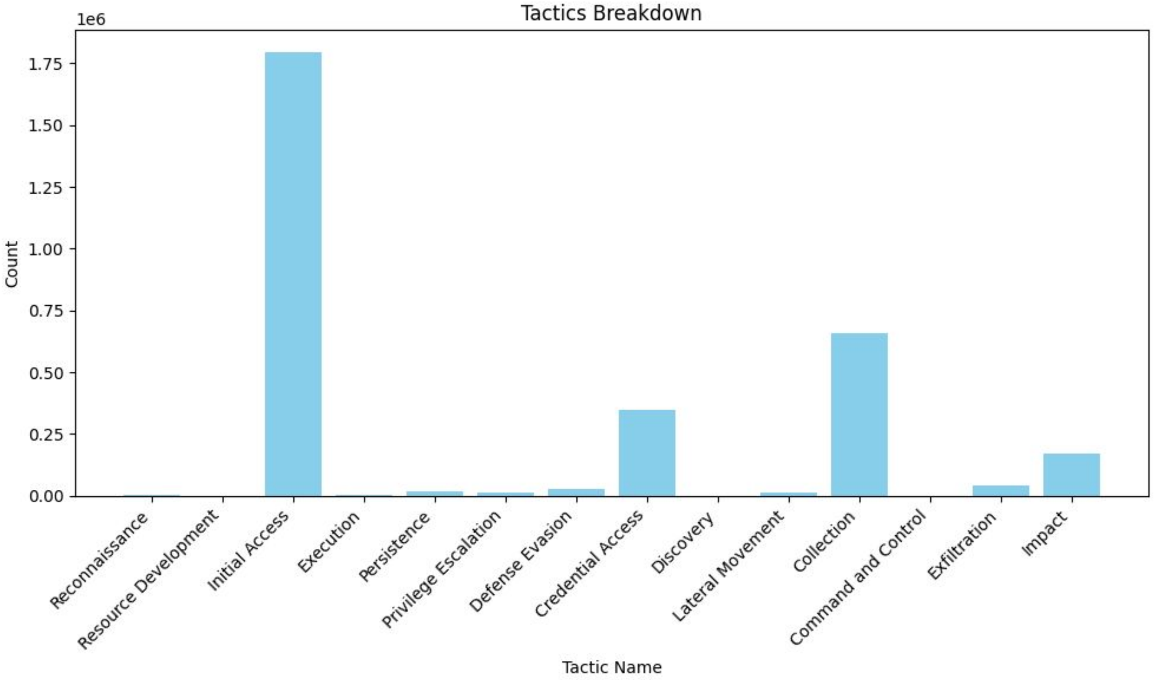
- 230 **Billion** SaaS Audit Log Events YTD
- 950 **TB** of events collected
- Average 1.2 **Billion** events per day
- 24 distinct SaaS Services

Signals/Alerts Analyzed:

- 1.9 Million over last 180 days
- 300K Unique IPs

1 HPU - Hamster Processing Unit

SaaS Attacks Don't Require Most Killchain Activities

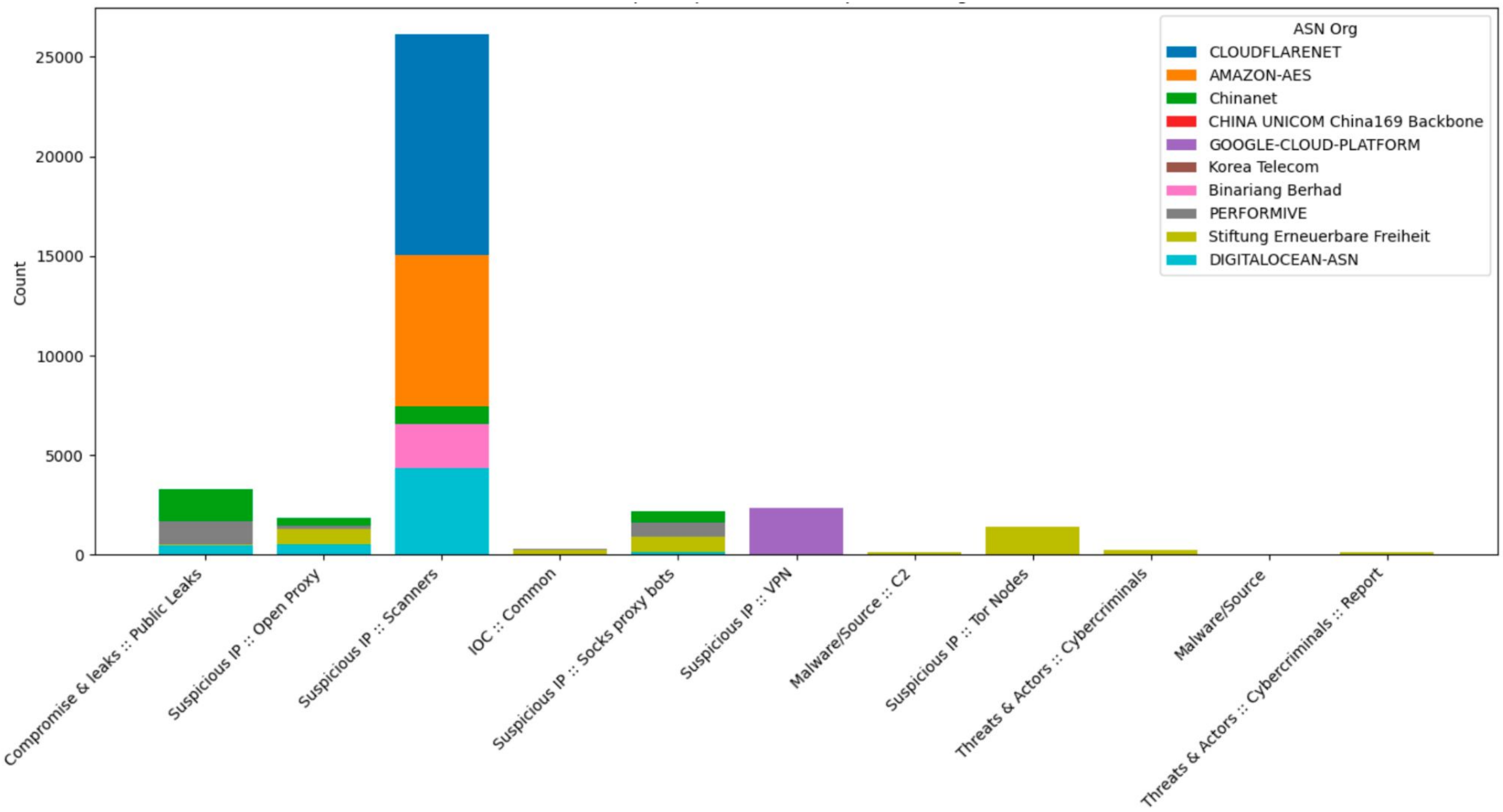


- Reconnaissance activities not logged in most SaaS

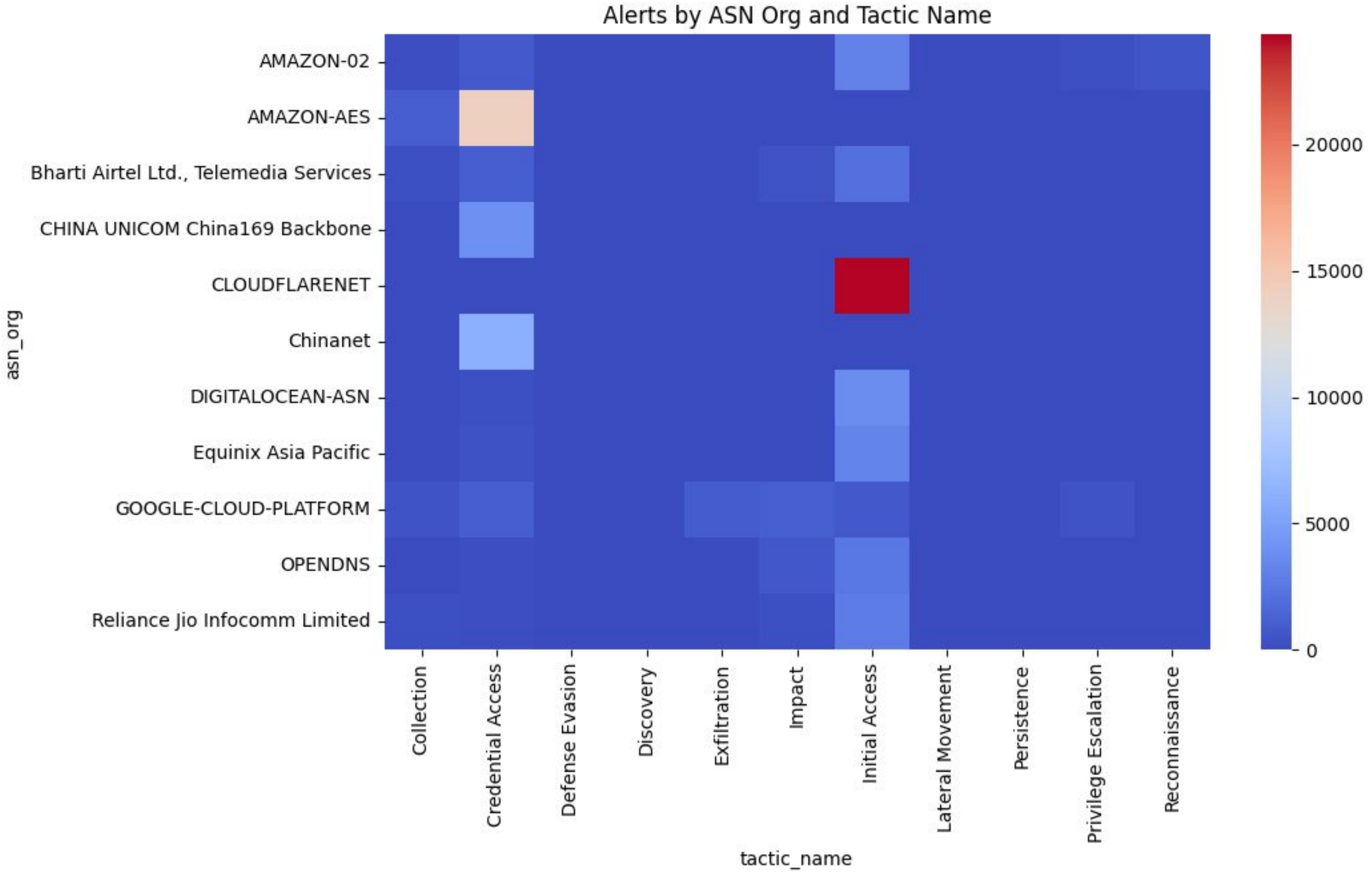
- Valid credential activity and data movement are highest observed activities **~70%**

- Maintaining foothold - while somewhat present is in many cases not required to achieve objectives **<2%**

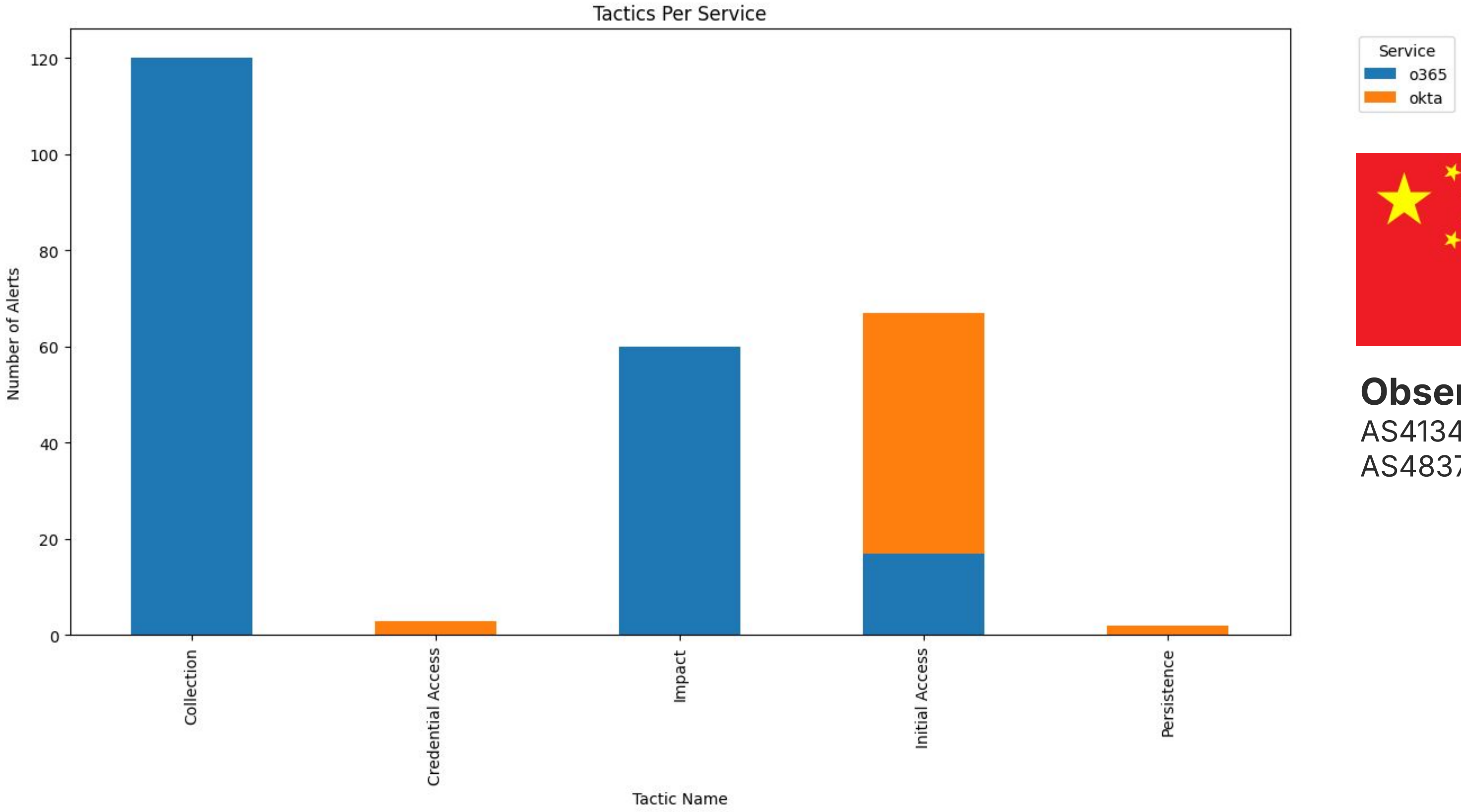
SaaS Attacks Heavily Leverage Cloud Providers



SaaS Attacks Heavily Leverage Cloud Providers



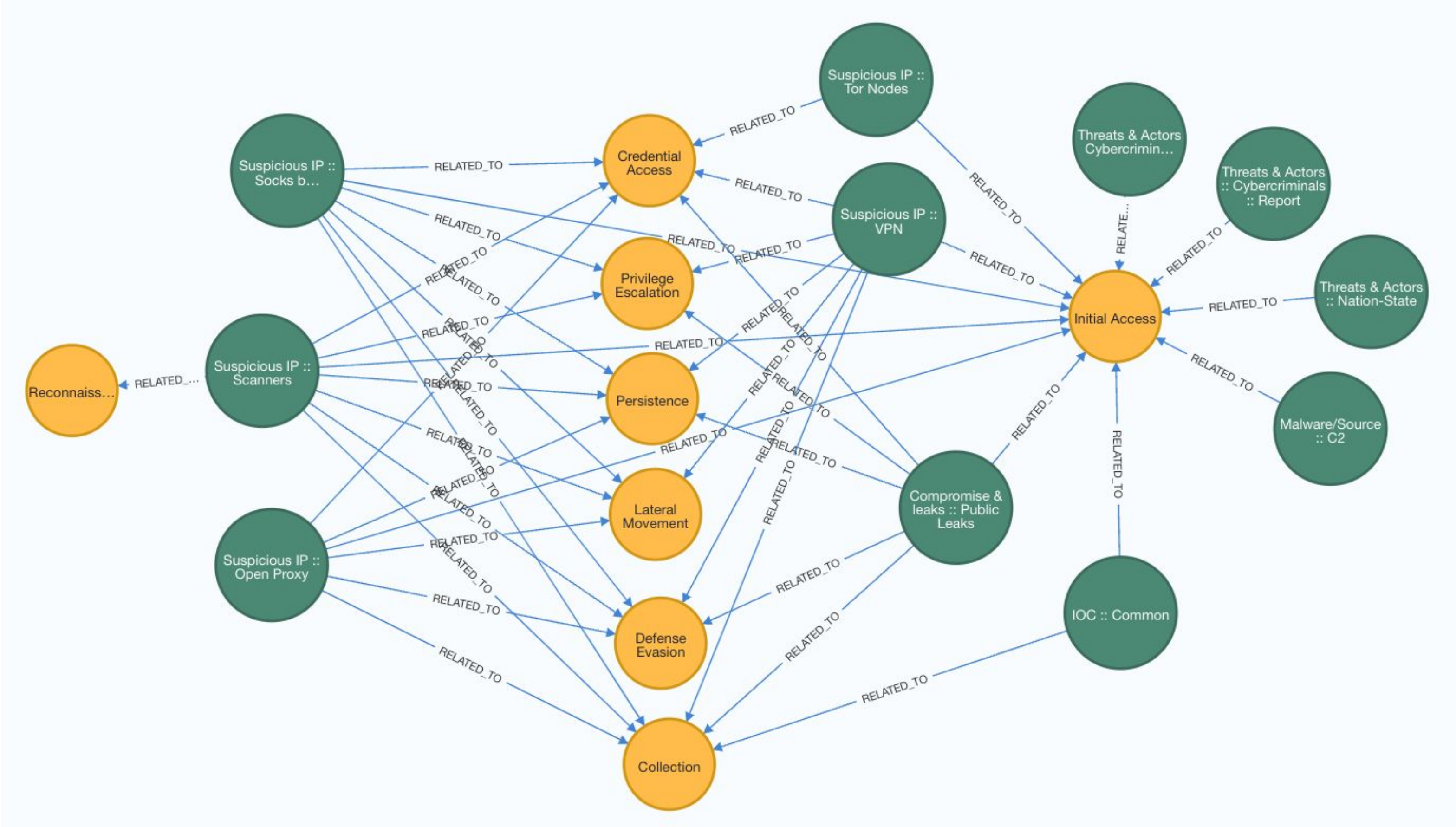
Chinese-Affiliated Attacks Focused on Microsoft 365



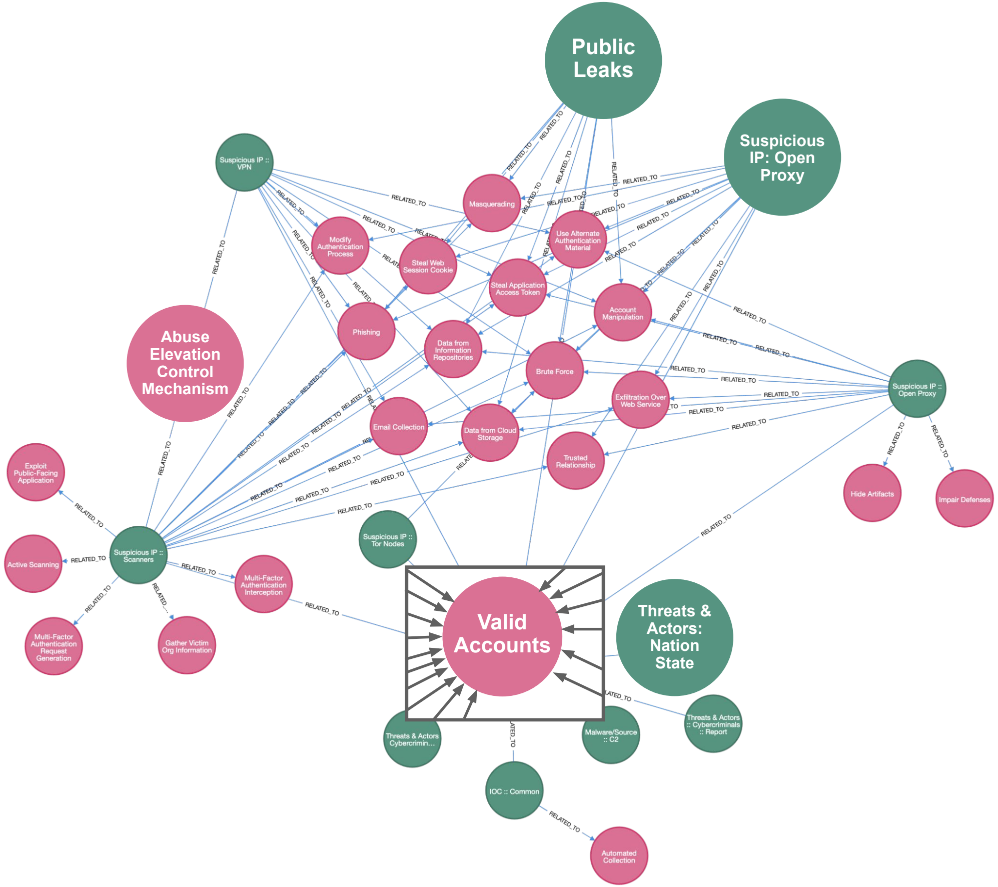
Observed ASN:

AS4134
AS4837

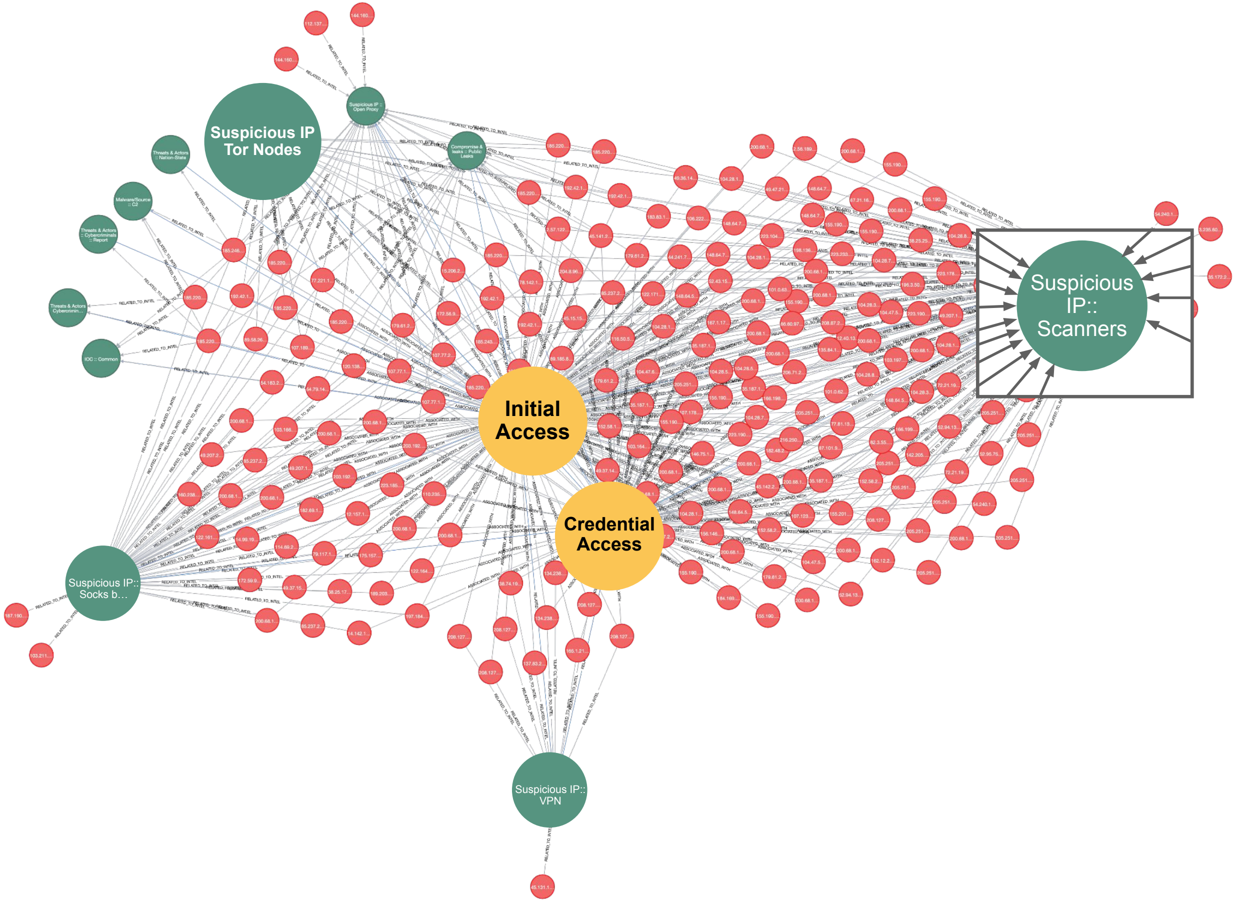
Enriched Alerts Organized by Tactic


Suspicious IP :: Tor Nodes
Threats & Actors Cybercrimin…
Threats & Actors :: Cybercriminals :: Report
Threats & Actors :: Nation-State
Malware/Source :: C2
Suspicious IP :: Socks b…
Suspicious IP :: VPN
Suspicious IP :: Scanners
Suspicious IP :: Open Proxy
Compromise & leaks :: Public Leaks
IOC :: Common
Credential Access
Privilege Escalation
Persistence
Lateral Movement
Defense Evasion
Collection
Initial Access
Reconnaiss…
RELATED_TO
RELATED_…
RELATE…

Threat Actors Target Valid Account and MFA Techniques

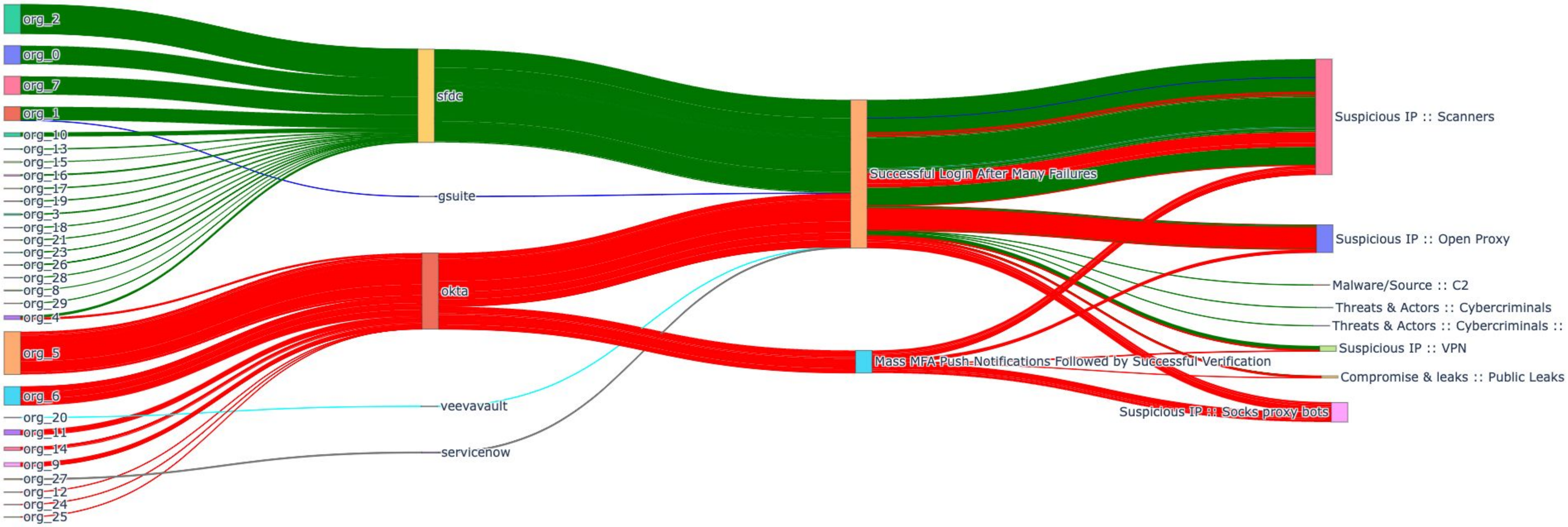

Public Leaks
Suspicious IP: Open Proxy
Suspicious IP :: VPN
Masquerading
Modify Authentication Process
Steal Web Session Cookie
Use Alternate Authentication Material
Steal Application Access Token
Account Manipulation
Phishing
Data from Information Repositories
Brute Force
Abuse Elevation Control Mechanism
Exfiltration Over Web Service
Suspicious IP :: Open Proxy
Email Collection
Data from Cloud Storage
Trusted Relationship
Exploit Public-Facing Application
Hide Artifacts
Impair Defenses
Active Scanning
Suspicious IP :: Scanners
Multi-Factor Authentication Interception
Suspicious IP :: Tor Nodes
Multi-Factor Authentication Request Generation
Gather Victim Org Information
Valid Accounts
Threats & Actors: Nation State
Threats & Actors :: Cybercriminals :: Report
Threats & Actors Cybercrimin...
Malware/Source :: C2
IOC :: Common
Automated Collection
RELATED_TO

Attacker Observations - Credential Access

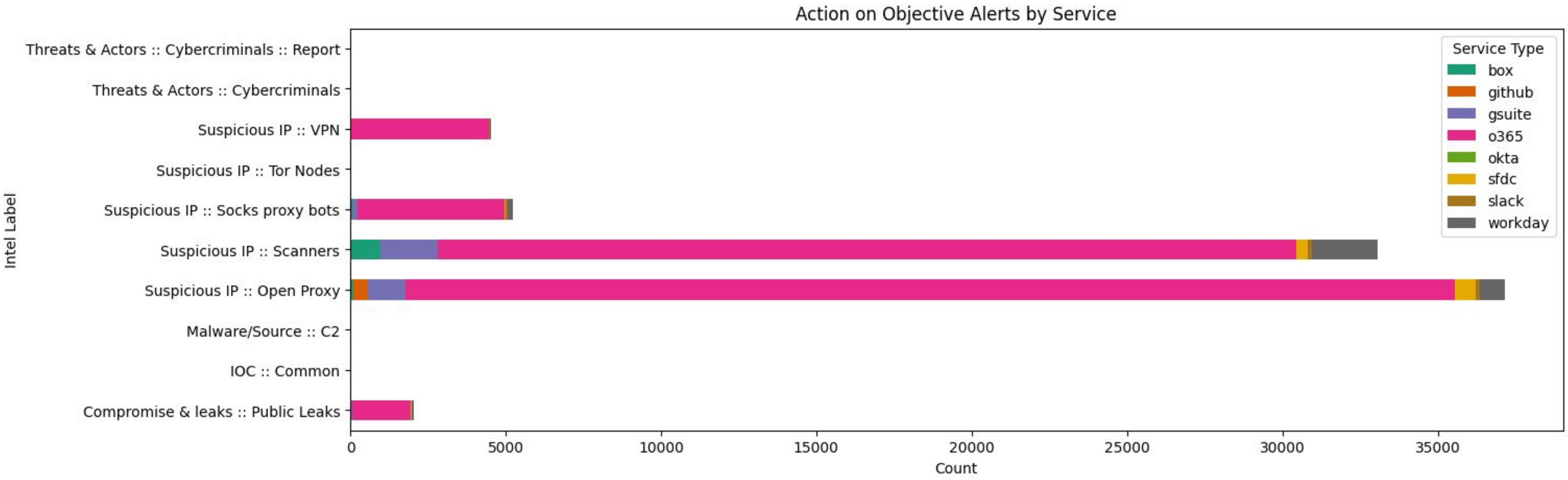


Attacker Observations - Credential Access

Brute Force & MFA Exhaustion

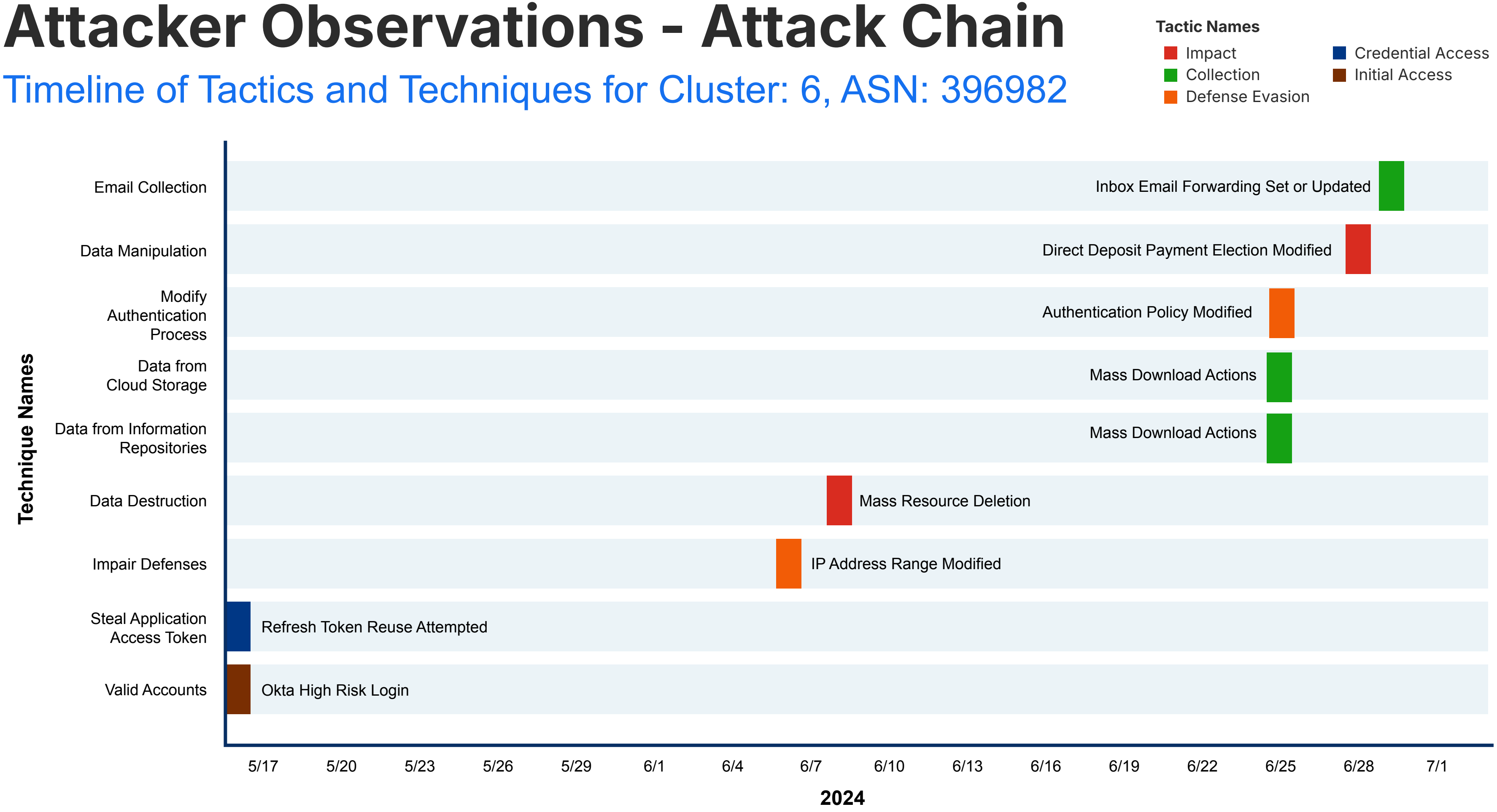


Attacker Observations - Actions on Objectives



Attacker Observations - Attack Chain

Timeline of Tactics and Techniques for Cluster: 6, ASN: 396982

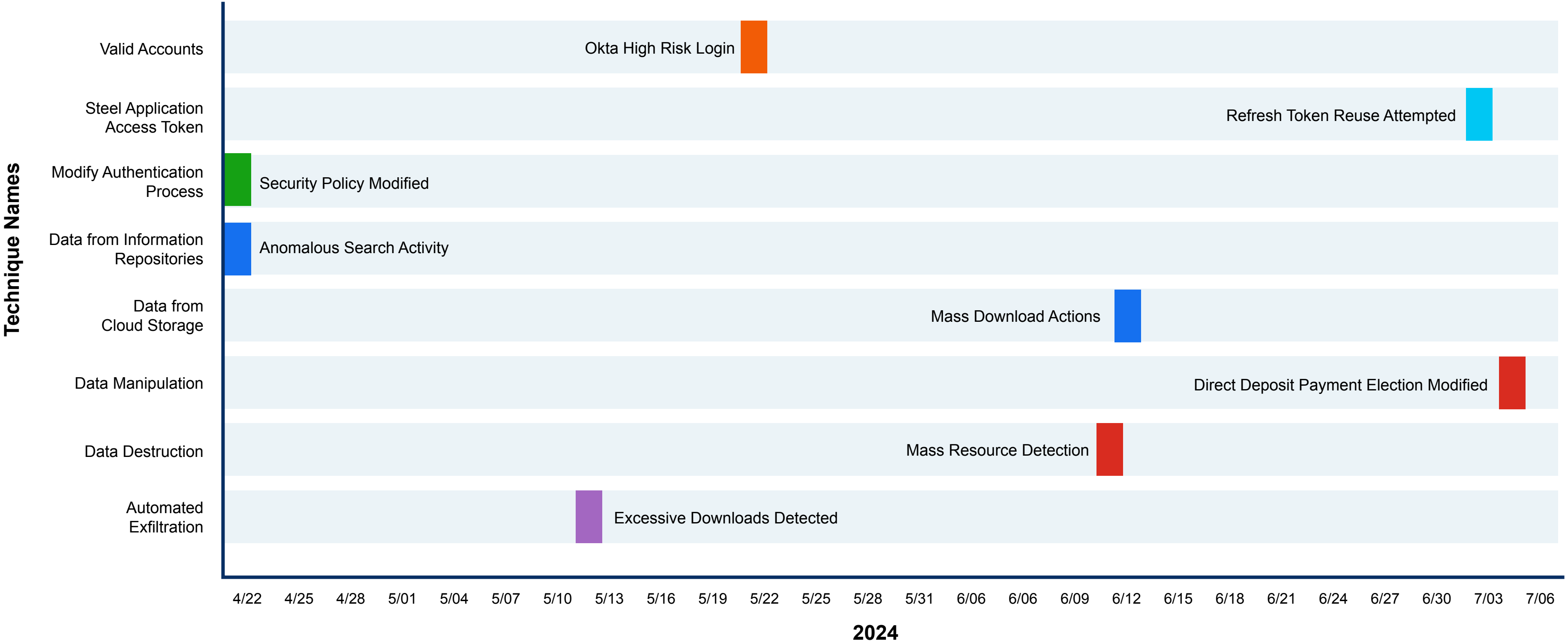


Attacker Observations - Attack Chain

Timeline of Tactics and Techniques for Cluster: 11, ASN:396982

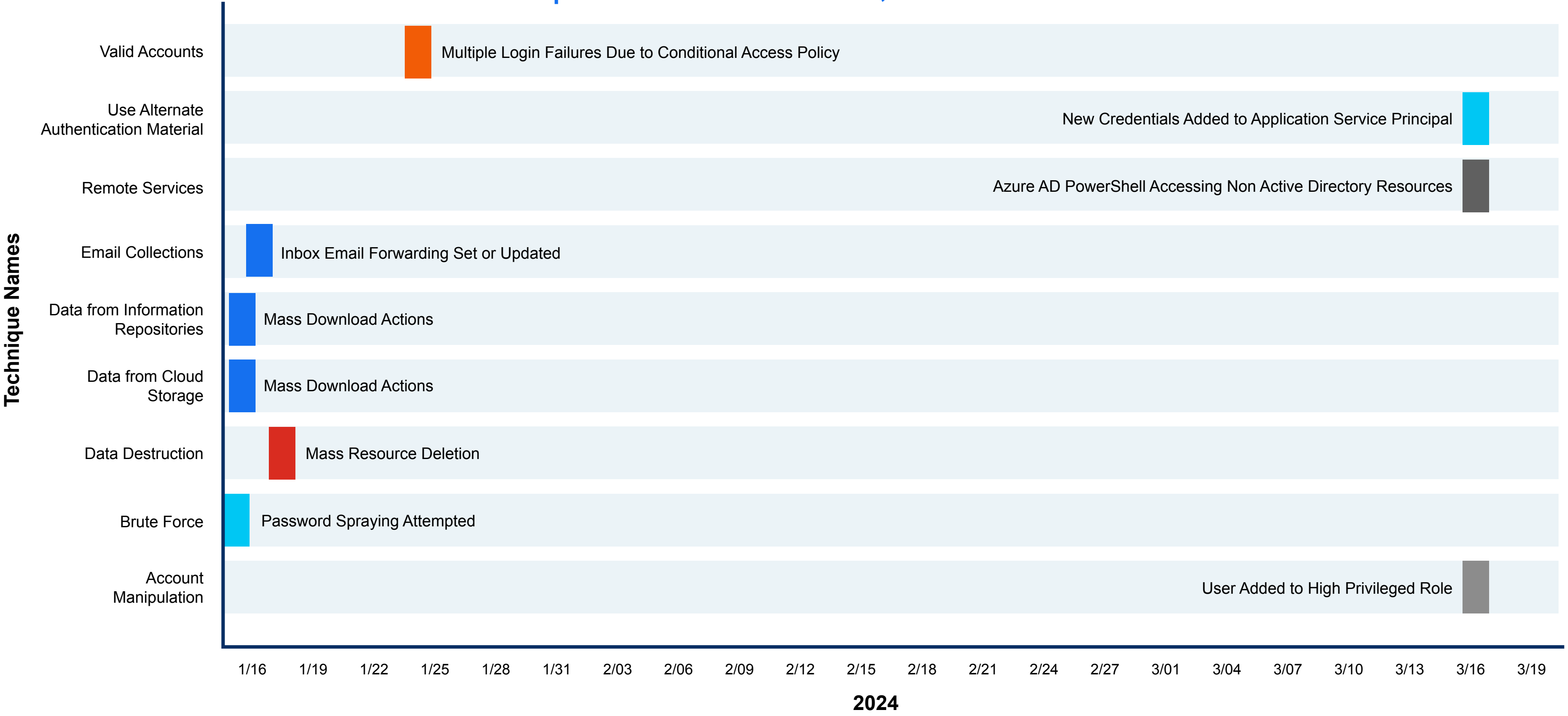
Tactic Names

- 🟪 Exfiltration
- 🟥 Impact
- 🟦 Collection
- 🟩 Defense Evasion
- 🟦 Credential Access
- 🟧 Initial Access



Attacker Observations - Attack Chain

Timeline of Tactics and Techniques for Cluster: 12, ASN:15830



System Identity controls are lacking in most SaaS products

- Network Level
  - IP allowlist? **Maybe, likely can't be utilized**
  - Block TOR Access? **Doubtful**

- Device Level
  - Corp Device Check? **Doubtful**
  - Device Attribute Profile Monitoring? **Maybe**

- Authentication Flow
  - SSO Available? **Sure - pay the SSO Tax**
  - Restrict Alternative Auth Methods? **Doubtful**
  - MFA Available? **Yes - likely not for service accounts**

Observed TTPs Summary

Credential Access

- Buy
- Phish
- Cred Spray
- Cred Stuff
- Enter front door

Persistence

- Modify Authentication
- Create/Use Alternative Credentials

Impact

- Stage data and push to cloud resources
- Download directly
- Email Forwarding Rules

Obfuscation Methods

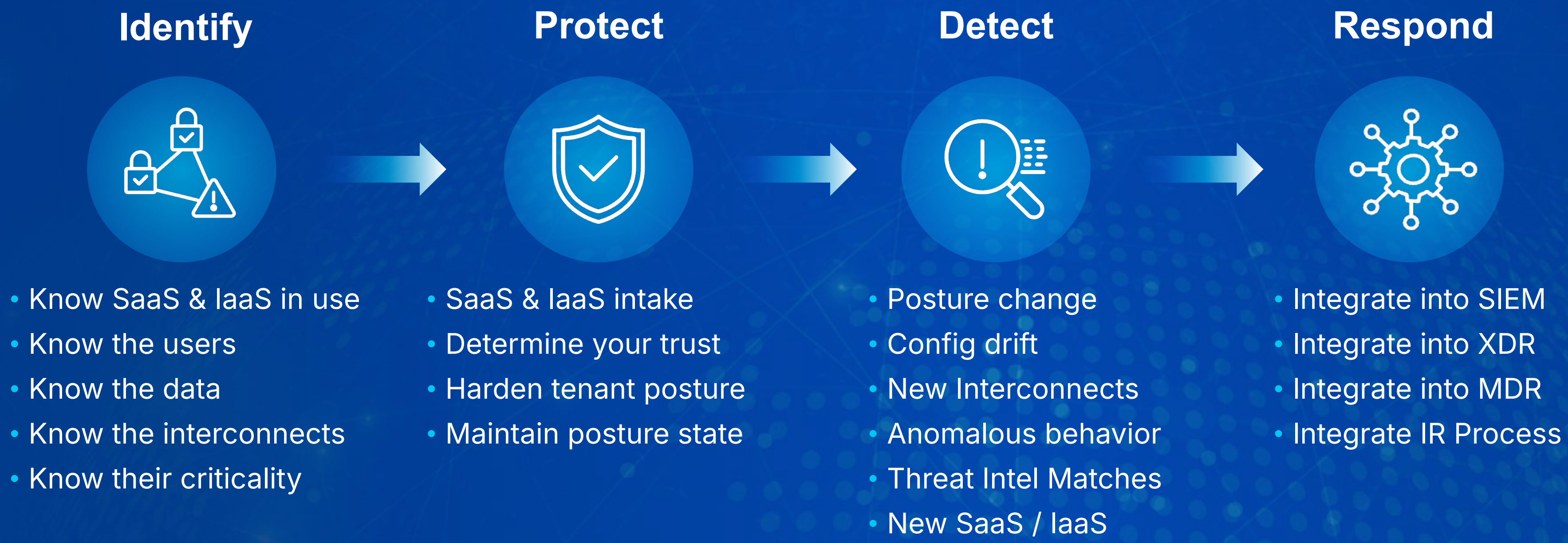
- VPNs
- Proxies
- Cloud Providers
- TOR

Well… How Did We Get Here?

- Bought ~150 SaaS products and 3 IaaS/PaaS
- Moved most business processes to SaaS
- Moved most data processing to IaaS/PaaS
- Moved our IdP to the Cloud
- Considered security ramifications too late
- Covid accelerated remote work and SaaS
- Diluted the “Zero Trust” protection strategy

Embrace Your New Attack Surface

Key Takeaways: Strategic



Identify

- Know SaaS & IaaS in use
- Know the users
- Know the data
- Know the interconnects
- Know their criticality

Protect

- SaaS & IaaS intake
- Determine your trust
- Harden tenant posture
- Maintain posture state

Detect

- Posture change
- Config drift
- New Interconnects
- Anomalous behavior
- Threat Intel Matches
- New SaaS / IaaS

Respond

- Integrate into SIEM
- Integrate into XDR
- Integrate into MDR
- Integrate IR Process

What Should We Do?

Key Takeaways: Tactical

- Use Phishing resistant hardware MFA devices
- Move important SaaS behind an IdP you can trust
- Enforce Hardware Key + Device Trust with IdP
- Avoid the use of “Service Accounts” when possible
- Ingest your SaaS logs and monitor them
- Enrich your logs with proxy, VPN, tor, and ASN tagging
- Utilize UEBA capability at the SIEM
- Implement Zero Trust, for real

Thank You

AppOmni

black hat

Booth #1660

ASK US HOW TO

Assess SaaS Threats in Your Environments

https://appomni.com/risk-assessment/