NASACT 2023
ANNUAL CONFERENCE
August 13-16 | Portland, Oregon

THUNDERHEADS AHEAD: ADOPTION HAZARDS

TALES FROM THE CLOUD FRONT LINE

Russ McRee, PhD grmc at google dot com
@holisticinfosec

The mastermind of 2022's most prolific and successful hacker group, known for compromising numerous companies and government agencies, was…

a 16 year old in the UK, living in his mom's basement

I was…

Partner Director, Operations for the Microsoft Security Response Center

I am…

Director, GCP Enterprise Protection for Google Trust & Safety

I have…

directly experienced, and responded to, many of the worst attacks and abuses in internet and cloud history

Pick your poison: the SVR or LAPSUS$

Russia's foreign intelligence service, known as the SVR (Nobelium), was responsible for the SolarWinds hack

According to Microsoft, one of the victims of the SolarWinds hack, the group targeted technology companies that **resell and provide cloud services for customers**

LAPSUS$ (DEV-0537) was known for using a pure extortion and destruction model without deploying ransomware payloads. DEV-0537 targeted globally, including organizations in government, technology, telecom, media, retail, and healthcare sectors

DEV-0537 was also known to take over individual user accounts at **cryptocurrency** exchanges to drain **cryptocurrency** holdings

The aforementioned 16 year old master mind had $14m in bitcoin at his peak of criminal activity

Attacktics: SVR and LAPSUS$ commonalities

Nobelium: supply chain attack to insert malicious code in Solarwinds Orion

SVR **targeted privileged accounts of service providers** to move laterally in cloud environments, using trusted relationships to gain access to downstream customers & enable further attacks or access targeted systems

In one case, SVR chained together access across four distinct service providers to reach their end target

Lapsus$: used a variety of attacks, including social engineering, **MFA fatigue** , SIM swapping, and **targeting suppliers**

Focused social engineering efforts to gather knowledge about target's business operations, including intimate knowledge about employees, team structures, help desks, crisis response workflows, and **supply chain relationships**

Paid employees at targeted organizations or suppliers/business partners for access to credentials and MFA approval

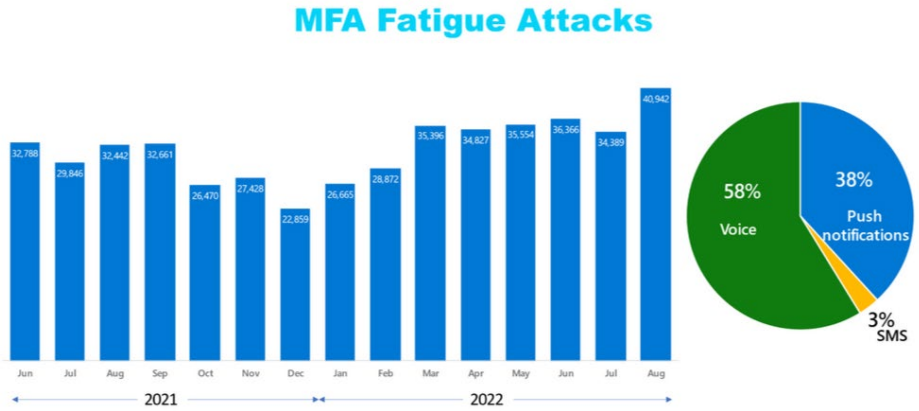
What the @#&^ is MFA Fatigue?

MFA fatigue , or MFA push spam: technique to bypass multi-factor authentication checks

MFA fatigue occurs when threat actors run scripts that attempts to log in repeatedly with stolen credentials, resulting in an endless stream of MFA push requests sent to the account holder's mobile device

Threat actor pushes repeated MFA notifications, then contacts targets via email, messaging, or phone, pretending to be IT support to convince targets to accept the MFA request

Targets are so overwhelmed that they accidentally click the "Approve" button or simply accept the MFA request to end the flood of notifications sent to their phone



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

The cumulative illicit use of public clouds for crypto-mining was valued at $100 million or more in 2022

Crypto-mining is only one of 13+ cloud abuse type classifications

Cloud Abuse Landscape

Network Abuse

Intrusion Attempt
Port-scanning Attacks
DDoS attacks
Compromised VMs

Resource Abuse

Cryptocurrency Mining
Sharding
Illegal Video Streaming

Content Abuse

Malware
Phishing
Unwanted Software

Payment Fraud

Stolen Instruments
Delinquency
Payments Risk

Is all hope lost?

Observations and Lessons

Cloud Providers

- Cloud providers fight the war on two fronts: defend customers, defend themselves
  - Cloud providers often espouse “shared responsibility”

Resellers and Cloud Service Providers

- Cloud providers love resellers but may not hold them to an acceptable level of security accountability
  - You’re on as strong as your weakest link

Cloud adoption is NOT a lift and shift operation

- Architecture and implementation for cloud are not the same as on premises
  - Replication of on-premises practices in the cloud often results in failure

Action and Mitigation

IAM

- Identities, credentials, service accounts, etc are the primary target
- Protect them at all costs: avoid leaks in source code, loss via social engineering
- Utilize **strong** Multi Factor Authentication (MFA) everywhere possible

Configuration

- Misconfiguration is a significant contributor to fraud, loss, and abuse
- Be mindful of weak and/or overly permissive settings
- Simply business logic flaws can be exploited

Action and Mitigation

Logging

- Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack (CIS Control 08 Audit Log Management)
  - 8.12 Collect Service Provider Logs where supported: example implementations include **collecting authentication and authorization events** ; data creation and disposal events; and **user management events**

Detection

- Operate processes and tooling to establish and maintain comprehensive network monitoring &defense against security threats across the enterprise's network infrastructure and user base (CIS Control 13 Network Monitoring &Defense)
  - 13.1 Centralize security event alerting across enterprise assets for log correlation and analysis

Action and Mitigation

Threat Model

- Determines what threats exist that could lead to attacks on, and abuse of, cloud services and infrastructure
- Identify threat mitigation to protect those services and infrastructure
- Identified threats can be prioritized to manage engineering & preventative measures in a proactive manner

Purple Team

- Test every assumption
- Adversary emulation, hand in hand with defensive techniques, to quickly and comprehensively close gaps

CIS Controls Cloud Companion Guide v8

- 01 Inventory and Control of Enterprise Assets
- 02 Inventory and Control of Software Assets
- 03 Data Protection
- 04 Secure Configuration of Enterprise Assets and Software
- 05 Account Management
- 06 Access Management Control
- 07 Continuous Vulnerability Management
- 08 Audit Log Management
- 09 Email and Web Browser Protections
- 10 Malware Defenses
- 11 Data Recovery
- 12 Network Infrastructure Management
- 13 Network Monitoring and Defense
- 14 Security Awareness and Skills Training
- 15 Service Provider Management
- 16 Application Software Security
- 17 Incident Response Management
- 18 Penetration Testing

NASACT 2023
ANNUAL CONFERENCE
August 13-16 | Portland, Oregon

Q & A

THANK YOU

Russ McRee, PhD grmc at google dot com
@holisticinfosec