



The rise and rise of ~~Advanced Persistence~~ Threat: Incident Response edition

Anurag Khanna



#whoami

- Senior Manager - Incident Response @CrowdStrike
- Advising organizations while they are responding to incidents
- SANS Certified Instructor, GSE #97
- Past speaker at Blackhat, RSA, BSides, SANS Summits, AISA Con etc

Find previous talks and this slide deck at
rudrasec.io/talks



Disclaimer

- The views expressed in this talk represent my own views and not those of my employer
- We are going to talk about known threat actor techniques, published by several organizations
- References are embedded across this presentation
- Icons attributed to Flaticon.com and respective organizations

Bottom Line Up Front - BLUF

- eCrime threat actors are getting faster, sophisticated and ruthless
 - Targeting identity, leveraging cloud and performing extortion
- Defenders need to investigate across domains and respond with certainty, and quicker



Level Up Faster

“Let your plans be dark and impenetrable as night, and when you move,
fall like a thunderbolt.”

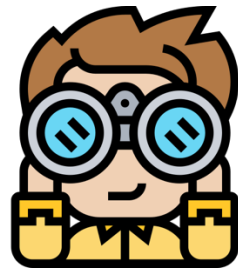


Sun Tzu, The Art of War

Defenders are Getting Better



Better Tooling



Better Visibility

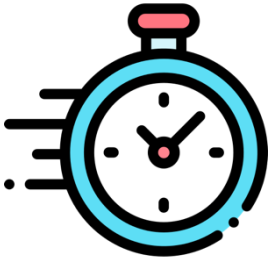


**Better Identity
management**

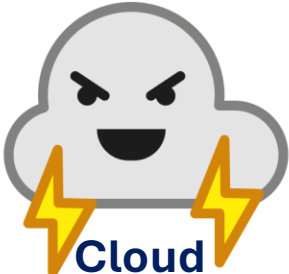


**Lower
Dwell Time**

Attackers are Responding



Faster



Cloud



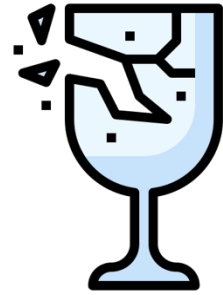
Targeting Identity



Living of the Land



When you move fast ⚡, time slows down.



When you move fast, you will break things.

**You can't hunt blind.
Visibility is a superpower.**



Visibility & Response Capabilities

- Defenders need visibility, across the three realms
 - Host based
 - Cloud based
 - Network based

Ability to respond in real time
puts us on same pedestal as the adversary



**Identity is the “key” to success
aka. \$\$\$\$.**



DEATH TO SFA



- Single Factor Authentication (SFA) is still the most common **initial access** mechanism for eCrime incidents

If you are using SFA – You will get Breached.

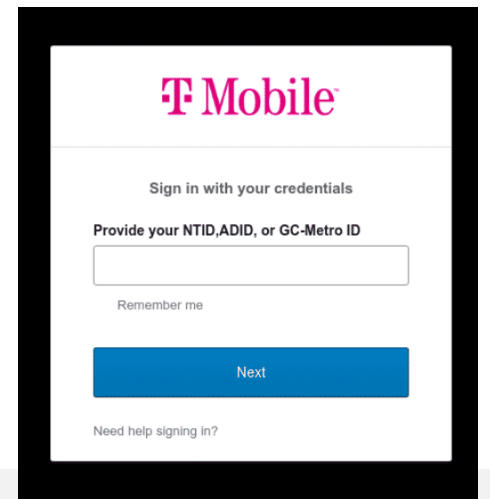
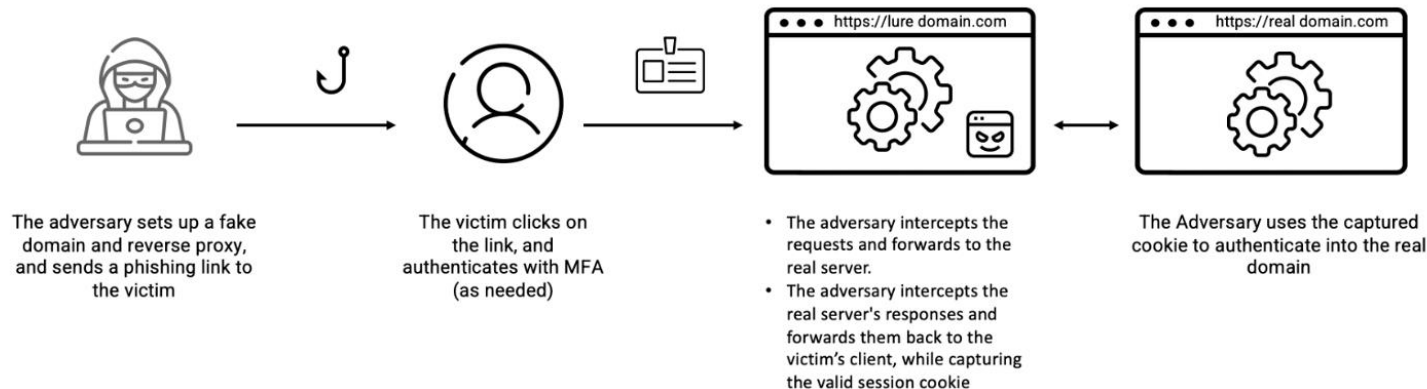
Call to Action:

ENFORCE MFA NOW!!!

- If this cannot be done while under attack, consider reducing the attack surface, by breaking the trust with central identity provider

Classic Social Engineering

- Old school phishing still works
 - Adversary-in-the-middle (AiTM) for bypassing MFA, EvilProxy, NakedPages
- Attackers are targeting privileged identities
 - Deploying phishing pages using **aged** domains over realistic fake single sign-on (SSO) portals using keywords such as 'okta', 'help', 'sso', and 'servicedesk'.
 - **More power = More risk**, Identity Admins, SSO Admins, AD Admins



Prepare

- Power credentials only on limited number of secured systems, Microsoft's Enterprise access model

Next Gen Social Engineering - Targeting Employees



- Calling/messaging Employees
 - Using personal information, such as home addresses and family names, along with physical threats to coerce victims into sharing credentials
 - Asking users to install RMM utilities, to control their systems, asking them to remove phishing resistant MFA like FIDO
 - SMS Phishing (Smishing) - target identity administrators in cloud infrastructures making them navigate to phishing website providing credentials
- Exploiting trust by using chat applications like Slack, Teams to perform social engineering

Prepare:

- Use awareness and a culture to not trust, report.

Next Gen Social Engineering - Targeting Helpdesk

- Attackers are becoming brazen, calling helpdesk, targeting privileged accounts, requesting password resets, including the MFA method
- Voice calls made by native English speakers, understanding the western culture, outside of business hours, showing urgency, and requesting password/MFA reset for privileged accounts, with prior information about target accounts

Prepare:

- No password resets without video and Manager/Peer verification

Respond:

- When under attack, stop all password resets through Helpdesk

MFA is not a silver bullet



- OTP Social Engineering
 - Perform social engineering, to get the One Time Password Over SMS, Emails, internal chat applications, phone calls, password bots
- Adding additional authentication factors by updating user account
 - Enrolling own MFA methods, mobile authenticator or email

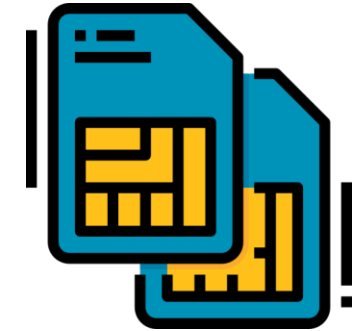
Prepare

- User awareness to communicate with Infosec if under such an attack
- Limit MFA attempts

Respond

- Disable registration/modification of MFA while responding to an incident
- Force strong verification for any change

Not All MFA is created equal



- SIM Swapping/Forwarding to bypass SMS/Call based MFA
 - Redirect the victim's phone to an attacker owned system
 - Setting call forwarding to bypass call-based MFA
 - Often using paid insiders, social engineering, or access to systems owned by partners or telecom companies
- MFA Fatigue/Spam Attack/Push Bombing to bypass Push Notification
 - Attackers can flood/spam victims with push notifications, and hope user accepts at least one notification

Prepare

- Do not use SMS/Call Forwarding or Push-Notifications as MFA second factor, use number matching or force users to enter code
- Disable registering of MFA device from a non-trusted location
- Implement SIM Locking and call Forwarding controls on organisation managed mobile devices

Targeting SSPR - Self Service Password Reset

- Capability to allow users to change password without intervention of the end users in EntraID
 - By default, Admins are enrolled for SSPR and require only one method to perform password reset
 - Attackers may **abuse** this by performing SIM Swap/Call forwarding and bypass the authorization check, question based SSPR is easy to bypass
- Attackers can add a persistence mechanism by adding their own MFA methods for SSPR for accounts they want to maintain access through

Prepare:

- Consider disabling, Self Service Password Reset (SSPR) functionality, at-least for privileged accounts
- Ensure multiple factors (more the better) are required for password reset. Not email/SMS

Respond:

- Disable SSPR (at least for privileged accounts)

Targeting Password Managers

- Password managers are a goldmine, organizations love them and so do attackers
 - Cloud based password managers are often targeted to gain access to credentials
- Password Vaults
 - Privileged Access Managers (PAMs) targeted to gain access to multiple credentials
- Target identity admin/managers to synchronize credentials to attacker-controlled system



Prepare:

- Restrict privileges to access password managers, to limited personnel
- Enforce MFA when accessing credential vaults

Targeting Identity Providers

- Continue targeting Active Directory, copying NTDS.DIT
 - Shutting and mounting domain controllers using other unmanaged VMs/Cloud systems
- Add Attacker managed Identity Provider as federated identity
 - Allows Attacker to authenticate as any Entra ID user, without valid credentials
 - Attacker needs to have a privileged identity
- Adding additional Identity Provider, also controlled by the attacker, as a “source” IdP in an inbound federation relationship with the target
- Targeting organisations that provide identity services like [Okta](#), PingIdentity, JumpCloud

Prepare:

- Implement token binding based on network location

Targeting Identity Providers - Respond

- Several systems authenticate with Identity Platforms like Active Directory, Okta, EntraID in enterprises,

Prepare:

- Limit Identity management privileges
- Review identity configuration

Respond

- **Consider breaking centralized authentication** when under an active attack and instead use local credentials
 - VCenter integration with Active Directory
 - Backup Solution integration
 - Hybrid Identity solutions, Integration of Cloud Identity and Access management
- Hunt for any changes to Identity Provider configuration

Targeting Credentials



- Password Guessing/Password Spraying still works
- Long term keys and credentials being used extensively to access cloud orchestration planes
 - Often keys are stored in plain text on disks, akin to storing passwords on disk
 - Accidentally leaked cloud credentials from publicly exposed code repositories like GitHub
 - Likely use of automated tools looking for credential material in public repositories, and use them like Jecretz, TruffleHog
- Leveraging credentials from Initial Access Brokers
 - Credentials from stealers like Stealc, Raccoon Stealer, Vidar Stealer, and RedLine Stealer

Prepare:

- Implement rate limits to mitigate password guessing and password spraying
- Disable accounts if multiple password guessing attacks identified

Adding new Accounts

- Adding new accounts in Cloud orchestration layer
 - CreateLoginProfile
 - PutUserPolicy with full rights
 - Effect Allow, Action * Resource *
- Adding additional long-term credentials to IAM accounts
- Adding SSH keys to Linux systems using orchestration layer features
- Create new local, domain or cloud accounts
- Create and use local VPN accounts on VPN devices



Respond:

- Hunt and remove any new accounts added in the environment

Secure your identity



Prepare

- [Use phishing resistant Multi Factor Authentication](#)
- Transition to hardware-based tokens like YubiKey or Hello for Business
- Remove Push notification/SMS as an option, use number matching
- Only allow user accounts to connect over VPN – Service accounts do not need to connect over VPN
- Consider Host Integrity checks for VPN, checking if the host
 - Has a Certificate?
 - Is part of the domain?
 - Has the Enterprise security tooling present?

Respond

- Consider blocking all egress traffic while incident is being contained?
- Consider disabling VPN or limit it to limited personnel



Advanced in APT often stands for effectiveness of adversary's information gathering capability.

Targeting Privileged Identities

- Attackers target high privileged accounts, Identity Admins, Domain Admins, Global Admins, Users with access to password vaults
- If you have identity details in a single solution, that solution will be targeted
 - Identity administrators have access to view/reset credentials

Prepare:

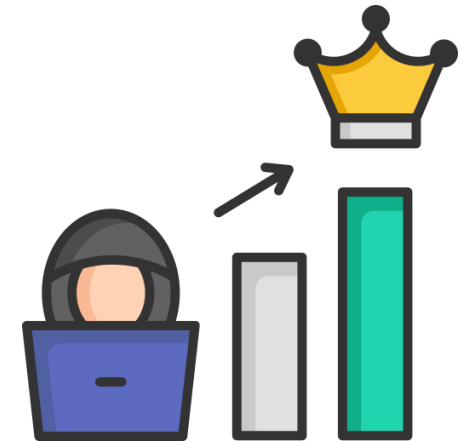
- Identify and reduce the Privileged accounts in the environment, Enforce long passwords

Respond:

- Rotate credentials, disable accounts, while incident is ongoing
- Do not store new passwords in Privileged Access Management solutions

Information gathering for profit

- Looking for legitimate credentials
 - Password in spreadsheets, text files
 - Access keys, Code, privileged credentials in scripts etc.
- Looking for Ransomware specific details
 - Ransomware protection mechanisms
 - Cyber insurance/Company policies regarding payment protocols in the event of a ransomware incident
- Understanding the target IT environment
 - Remote connection requirements



Information gathering for profit

- Bulk exporting users, groups, and device information
- Targeting internal information platforms
 - Ticketing systems to gather help desk tickets and understanding their working
 - Internal Wiki platforms like Confluence to understand policies in the organisation, network architecture, employee on-boarding, password reset procedure, VDI access, VPN access documentation etc.
 - Internal chat applications like Teams and Slack
 - Code repositories, File Shares
 - Data sharing platforms
 - OneDrive, SharePoint, Box, DropBox etc.

Targeting Software as a Service

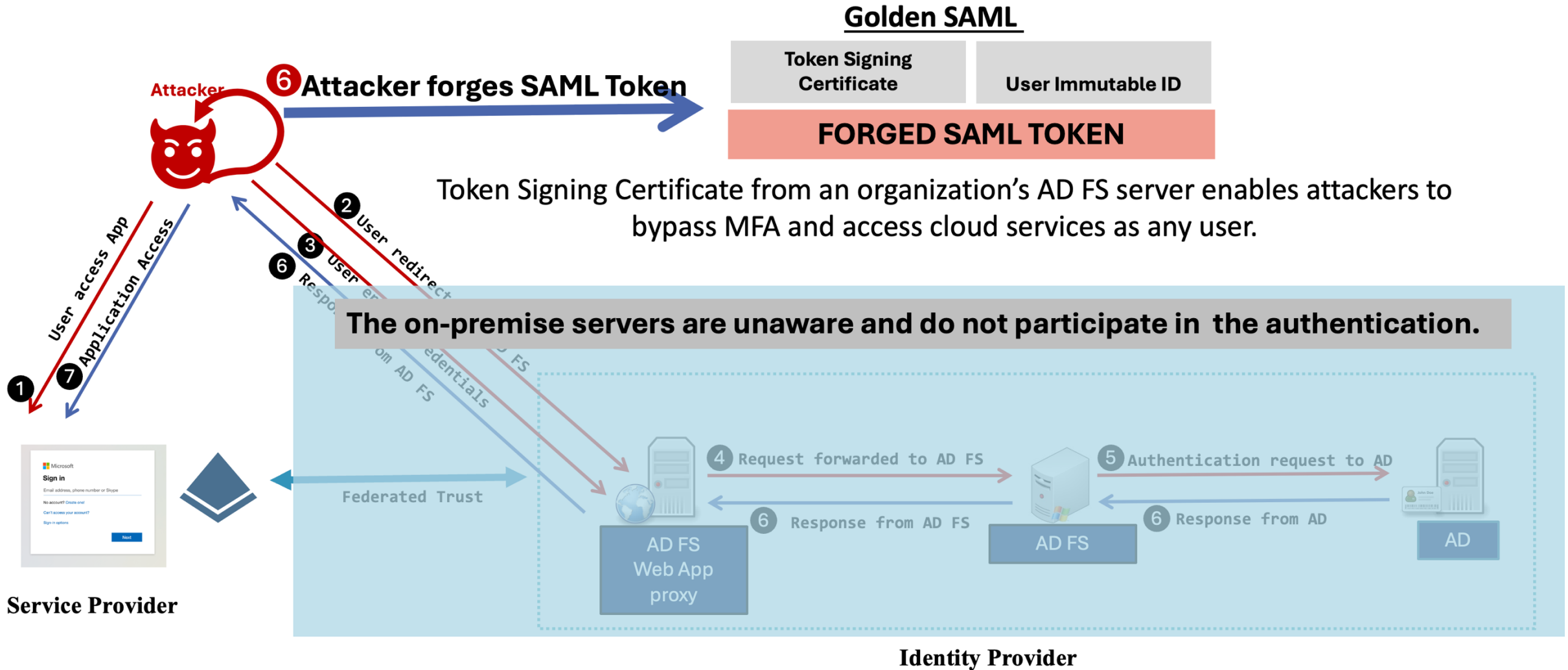
- Targeting Identity SSO platforms to self-assign access to all SAAS tiles
- SAAS applications often have limited logging and have critical data
- Targeting Active Directory Federation Service (AD FS) to steal the SAML signing certificate to get access to SAAS applications - Golden SAML attack



Prepare

- Improve monitoring of SAAS application logs
- Secure ADFS systems as you do for your AD Domain Controllers.

Golden SAML Attack



Cloud Aware Adversary



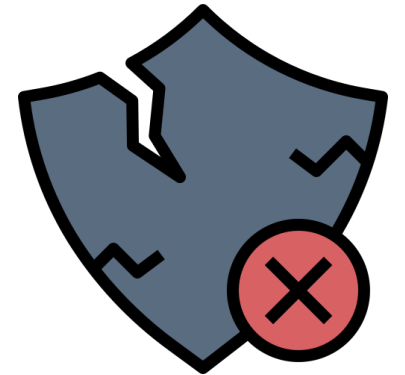
Defenders have a home ground advantage when responding to on-premises incidents.

This ceases in the Cloud.



Security Degradation

- Degrade logging capabilities, to hinder logging
- Enable incoming connections by editing Network Security Groups
 - Delete Firewall rules, add rules allowing incoming and outgoing traffic
- AWS Security rule to allow incoming access
 - RDP, RDS Service, SSH, Remote management access
- Create RDS Proxy, connect to the RDS instance using SQL Client
- Add trusted locations in Conditional Access Policies in Azure



Prepare

- Monitor for changes in the Cloud environment

Targeting Storage as a Service

- Data exfiltration and destruction in Storage as a Service
 - Direct data deletion
 - Object replacement
 - Encrypt/Re-encrypt files
 - Use Lifecycle policies to delete data
 - Delete/Remove encryption key

Prepare

- Enable bucket versioning
- Enforce MFA for deletion
- S3 Delete lock
- Remove S3 and KMS permissions that are not required
- Monitor for changes to versioning, MFA, delete lock, permissions etc.

New Unmanaged Cloud VMs

- Once attacker has access to cloud, they can create virtual machines and leverage them to target the victim, the VMs are often named according to the organisations naming conventions

Respond

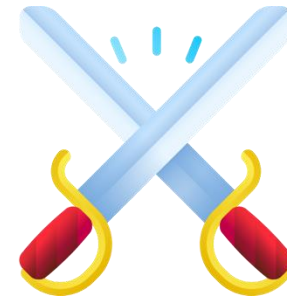
- Identify and stop any recently created virtual machines

```
PS C:> aws ec2 describe-instances --query 'Reservations[].Instances[?LaunchTime>=`2024-08-20`][].{id: InstanceId, type: InstanceType, launched: LaunchTime}'  
[  
  {  
    "id": "i-03ce8456bd86495af",  
    "type": "t2.micro",  
    "launched": "2024-08-26T01:38:59+00:00"  
  }  
]
```

```
PS C:> stop-instances --instance-ids i-03ce8456bd86495af
```

Containment/Knife fight - Cloud

- Often attackers gain access to Cloud orchestration layer
 - When a Conditional Access policy targets the **Microsoft Admin Portals cloud app**, the policy is enforced for tokens issued to application IDs of:
 - Azure portal
 - Exchange Admin center
 - Microsoft 365 Admin center
 - Microsoft 365 Defender portal
 - Microsoft Entra Admin center
 - Microsoft Intune Admin center
 - Microsoft Purview compliance portal
 - Microsoft Teams Admin center



Containment/Knife fight - Cloud

Respond

- Revoke all User session tokens
- Isolate Virtual infrastructure using Firewalls
- Remove identity integration with Active Directory and proactively rotate credentials for local accounts
- Deploy Conditional access policy to enforce [MFA for access](#) to **Microsoft Admin Portals cloud app**
- Deploy Conditional access policy targeting [Microsoft Admin Portals cloud app](#) only allowing certain accounts to access Cloud

```
Revoke-AzureADUserAllRefreshToken -ObjectId "a1d91a49-70c6-4d1d-a80a-b74c820a9a33"
```

Access Cloud systems

- Cloud Service providers have capability to access virtual machines from the orchestration platform
 - Access via Serial Connection
 - Access via SSM
- Enable serial ports and using them to evade firewall rules

Prepare

- Don't let the attacker hack your Cloud
- This activity can be detected if you have visibility

You can't see me.

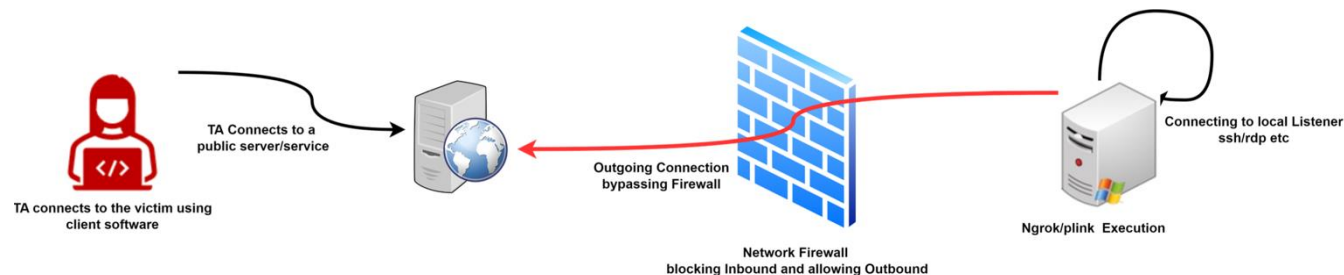
You cannot protect from what you can't see.



I am you - Pivoting

```
ssh -R 0.0.0.0:8888:localhost:3389
```

- As a community we have done a good decent job of gaining visibility on endpoint
- Threat Actors find ways of evading that detection
 - Deploy SOCKS Proxy on unmonitored systems Hypervisors, IOT devices, NAS boxes..
 - Tools like, Chisel, [Ngrok](#), rsox, socat, pivotnacci, SharpChisel, Ligolo, Ligolo-ng, Gost, Rpivot, plink, revsocks, cloudflared, mobaxterm and more
- Use Living of the Land tools like SSH to create reverse proxy tunnels



Prepare

- Don't let the attacker in the environment
- Secure, monitor and isolate unmonitored systems

Detect

- Source IP address of the RDP connection would be the same system/pivot machine

I come from nowhere



- Use Anonymization services like Tor Network
- Commercial VPN services using crypto, to connect from same geography as the victim
- [Residential Proxies \(RESIP\)](#) - Virtual private network (VPN) sessions through residential IP addresses to appear less suspicious
- Connect from Data centers and hosting providers, AWS, Azure, whatever the victim



Prepare

- Block access from suspicious sources at the perimeter, cloud, [Identity Providers](#)

When fence eats the garden

Living of the Security Tooling - (LOST)

- Attackers can **leverage Security software to perform malicious activity**
- Security tooling often has remote management capabilities to manage endpoints from the Cloud
- Create exceptions in the detection mechanisms of the security software, suppress alerts, tag detections as false
- Use cloud features to search for data of interest like O-365 compliance search

Prepare

- Phishing resistant Multi Factor Authentication for Security Tooling portal
- Limited access to users who do not need Remote endpoint management access

Respond

- Remove SSO from Security tooling
- Work with your security vendor to limit access to the portal

I drive(r) you crazy- disable visibility



- Drivers run in the Kernel space, giving them capability to bypass tamper protection mechanisms used by Endpoint Security mechanisms
 - Windows does not allow unsigned kernel-mode drivers to run by default
- Leverage Microsoft signed drivers
 - Microsoft has an [attestation signing process](#) for drivers, [Attestation Signed Malware](#), attackers are known to run Driver Signing as a Service (DSAAS)
 - Get a malicious driver signed by Microsoft, to disable EDR to then deploy Ransomware e.g. (PoorTry + StoneStop)
- Bring your own vulnerable driver ([BYOVD](#))
 - BYOVD makes it possible for an attacker with administrative control to bypass Microsoft signed driver requirement by exploiting vulnerability in a driver e.g. (CVE-2015-2291) in the Intel Ethernet diagnostics driver, Check <https://www.loldrivers.io/>

Malicious Drivers

Vulnerable Drivers

Bring your own Virtual Machine - BYOVM

- VMWare Virtual Machines that are powered on manually from the command line
 - Hidden from the usual mechanisms, like vCenter
 - Without security tools, could be used to target without any detections
- Create new virtual machines in Cloud
 - Not using organizations default tools, no security monitoring, end point security software etc



Prepare:

- Build detection rules to detect any new Virtual machine creation

Detect:

- Hunt for Virtual machines, using tools like VirtualGHOST

Respond:

- Kill any new virtual machines created recently

It only takes one unmanaged system

- You have EDR everywhere? Really? How about
 - That Windows XP, 2003 that does not support EDR
 - That developer who has a VM they are using to test stuff
 - Old Linux systems
 - Attackers' system that connected over the SFA VPN?
- Once Attacker is on an unmanaged system, they can often map network drives and encrypt them over the network
 - Technically encryption happens on the system without EDR



Prepare

- Deploy EDR, upgrade systems or isolate them

Walls have ears – Operational Security

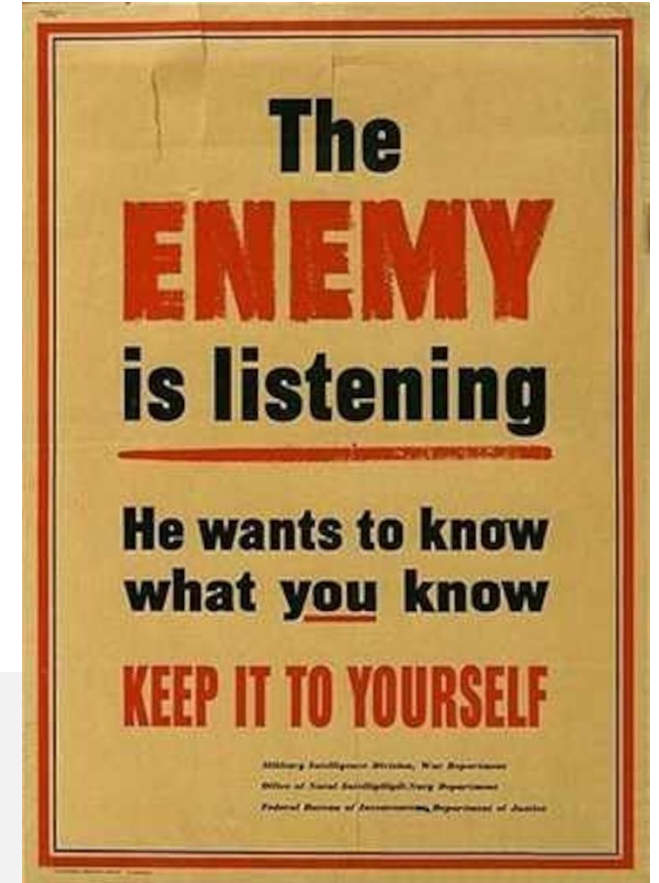
- Next Gen eCrime threat actors are Operational Security aware Are you?
 - Joining Incident Response calls, reviewing JIRA tickets
 - Lurking and leveraging Communication channels (Slack, Teams) to gain access, change TTPs
 - Creating email rules to forward emails from IDAM, Cloud and security vendors to the actors to monitor communications

Prepare

- Ensure you have OOB communication plan for your security team

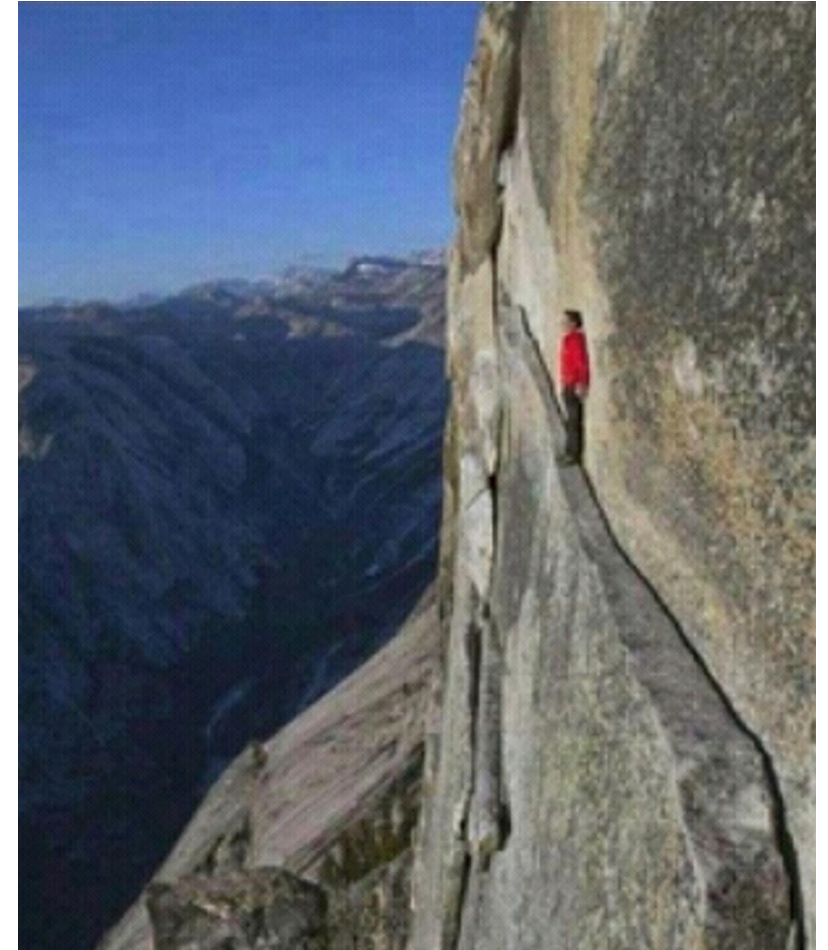
Respond

- Assume your communication mechanisms are compromised
- Verify anyone who joins your teams/zoom calls
- Create a Google Workspace only for response if operational security is a concern
- Review for newly created transport and forwarding rules in your email service provider



Living on the Edge - LOTE

- Targeting of edge devices has increased
 - [Firewalls](#), [VPN devices](#), [Email security gateways](#)
 - [Palo Alto](#), [Ivanti](#), [FortiGate](#), [Barracuda](#)
- Often no visibility and difficult to secure and analyse
- Off late, several vulnerabilities have been identified in these devices
- Threat Actors exploit these vulnerabilities to deploy persistence mechanisms
 - WebShells, Tunnelling tools, stealing credentials, adding accounts..



Remote Monitoring and Management Tools

- Legitimate **RMM tools**, to blend in with approved IT activities, bypassing security controls
- At scale, remote management capabilities = **Advanced Remote Access Trojans with Enterprise Support**
- Automation, Remote Control, System Administration

Prepare

- Only use one approved RMM tool, you just need one!
- Block all other RMM tools using EDR/Network controls

Respond

- Hunt for and remove any un-approved RMM tools in the environment
- EDR, Network Telemetry, Asset Inventory



Software-Defined Networks

- Easy to use and deploy, Software defined network, Create Exit nodes
- Work similarly to SOCKS proxy, providing uninhibited access to a network
- More scalable and feature rich than RMM tools



I am here for \$\$\$\$

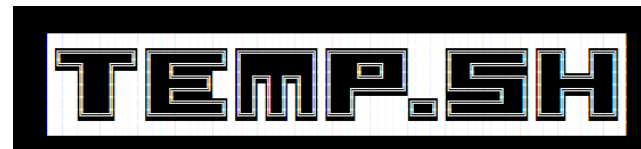
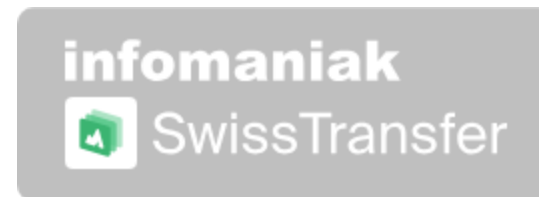


Exfiltration > Encryption

- More attackers are performing exfiltration as the only extortion method
- Sometimes deleting data after exfiltration
- Targeting
 - code repositories, document management and storage systems
 - SharePoint, SQL databases, cloud storage buckets
- Data exfil using legit backup solutions to steal files, Veeam, AFI Backup, CommVault
- Exfiltration to Cloud often using management clients
 - Data movement platform, Azure Data Factory, AWS DataSync, AWS Transfer Family and automated pipelines

Cloud based storage solutions for exfil

- Use whatever organization is using or whatever works
 - Dropbox, SharePoint Online, OneDrive, Google Drive, Proton drive etc
 - AWS S3 buckets, temp.sh, Backblaze, File.io, Transfer.sh, Swisstransfer.sh, Simpletransfer.online. mega.io
 - RClone, WinSCP, FileZilla



Exfiltration > Encryption - ETL Tools

- Install and use Extract, Transform, and Load (ETL) tools to collect data from compromised cloud environments to a centralized database



Prepare

- Monitor for usage of ETL services with cloud applications and ensure usage is approved

Hypervisor Jackpotting

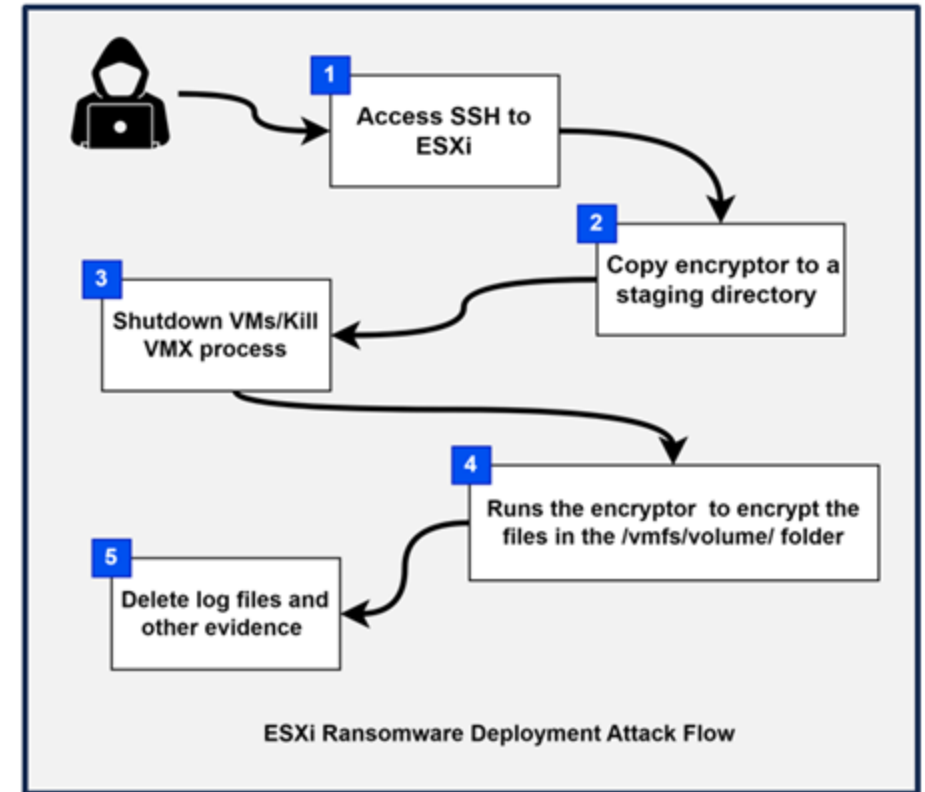
- **Hypervisor** systems remain a very valuable target with custom ransomware

Prepare

- Enable VMWare Lockdown mode

Respond

- Isolate Virtual infrastructure using Firewalls
- Remove identity integration with Active Directory and proactively rotate credentials for local accounts
- Only manage ESXi through vCenter
- Disable SSH to access ESXi



Evolving Extortion Tactics





- Reaching out to Victims
 - Some Attackers reach out via SMS, emails to victims, employees, customers, vendors, letting them know that they have the data, and the victim is not paying
- A Threat Actor reached out to the U.S. Securities and Exchange Commission (SEC) against an alleged victim
- Leaking data publicly in parts as a pressure tactics

Call to Action for Monday

- Identity is the key to a secure environment
 - Use phishing resistant Multi Factor Authentication
- Secure your Hypervisors
- Improve Cloud Security including monitoring capability
- Remember visibility and capability to respond is a superpower
- If under attack, respond fast and with ruthlessness

Thanks for listening!

Presentation deck available at rudrasec.io/talks

 **Anurag Khanna**
 **@khannaanurag**
www.linkedin.com/in/khannaanurag

