Analysis of an Intrusion Campaign Targeting Telco and BPO Companies

crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Tim Parisi December 2, 2022

CrowdStrike Services reviews a recent, extremely persistent intrusion campaign targeting telecommunications and business process outsourcing (BPO) companies and outlines how organizations can defend and secure their environments.

- CrowdStrike Services has performed multiple investigations into an intrusion campaign targeting telecommunications and business process outsourcing (BPO) companies.
- The end objective of this campaign appears to be to gain access to mobile carrier networks and, as evidenced in two investigations, perform SIM swapping activity.
- Initial access is varied: Social engineering using phone calls and text messages to impersonate IT personnel, and either directing victims to a credential harvesting site or directing victims to run commercial remote monitoring and management (RMM) tools.
- These campaigns are extremely persistent and brazen. Once the adversary is contained or operations are disrupted, they immediately move to target other organizations within the telecom and BPO sectors.
- Organizations should focus on identity-based security through authentication restrictions and secure multifactor authentication (MFA) configurations to most effectively disrupt this campaign.
- CrowdStrike Intelligence has attributed this campaign with low confidence to the SCATTERED SPIDER eCrime adversary.

Since June 2022, CrowdStrike Services, CrowdStrike Falcon OverWatch™ and CrowdStrike Intelligence teams have observed an increase in the targeting of Telco and BPO industries. These investigations appear to be tied to a financially-motivated campaign with links to an adversary CrowdStrike tracks as SCATTERED SPIDER. This blog will

discuss the ongoing campaign in greater detail, highlighting the various techniques used by the adversary to gain and maintain access, and evade detection and response, as well as what organizations should be aware of to best defend and respond to this campaign.

Background

In this attack campaign, the adversary demonstrates persistence in trying to gain access to victim environments and performs constant, and typically daily, activity within the target environment once access is gained. It is imperative for organizations to swiftly implement containment and mitigation actions if this adversary is in the environment. In multiple investigations, CrowdStrike observed the adversary become even more active, setting up additional persistence mechanisms, i.e. VPN access and/or multiple RMM tools, if mitigation measures are slowly implemented. And in multiple instances, the adversary reverted some of the mitigation measures by re-enabling accounts previously disabled by the victim organization.

Also of note, as CrowdStrike assisted one organization through the investigation and to a successful containment phase, the adversary moved onto other organizations in the same vertical. CrowdStrike was subsequently engaged to support the new victim organizations battling against the same campaign, as evidenced by overlapping indicators of compromise (IOCs) and techniques.

In all observed intrusions, the adversary attempted to leverage access to mobile carrier networks from a Telco or BPO environment, and in two investigations, SIM swapping was performed by the adversary.

Below is a summary timeline outlining a sampling of intrusions CrowdStrike Services responded to along with corresponding findings.

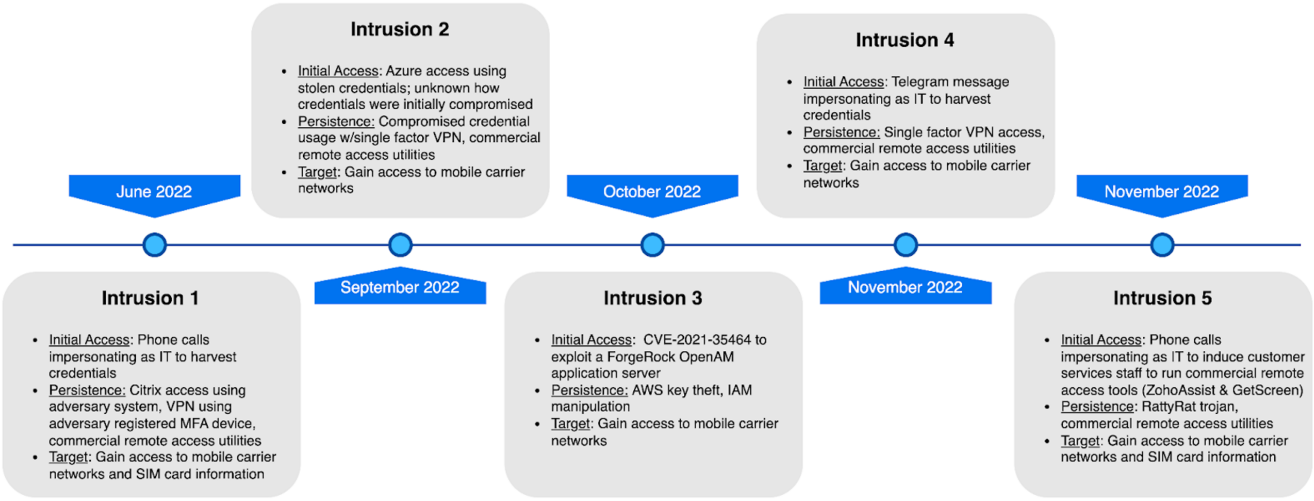

Figure 1. Sampling of relevant investigation summaries performed by CrowdStrike Services since June 2022 (click to enlarge)

Initial Access and Privilege Escalation

In most of the investigations CrowdStrike performed, initial access was achieved through social engineering, where the adversary leveraged phone calls, SMS and/or Telegram to impersonate IT staff. The adversary instructed victim users to either navigate to a credential-harvesting website containing the company logo and enter their credentials, or download a RMM tool that would allow the adversary to remotely connect and control their system. If MFA was enabled, the adversary would either engage the victim directly by convincing them to share their one-time password (OTP), or indirectly by leveraging MFA push-notification fatigue. This is when an adversary continuously prompts MFA to the victim user until they accept the MFA push challenge.

In another investigation, the adversary leveraged compromised credentials from a victim user and authenticated to the organization's Azure tenant. Using this access, the adversary instantiated Azure VMs to conduct credential theft activity and lateral movement to on-premises systems.

In a third tactic observed in another investigation, the adversary leveraged CVE-2021-35464 to exploit a ForgeRock OpenAM application server, which front-ends web applications and remote access solutions in many organizations (a patch for this CVE was released in October 2021). In this example, the adversary showcased their knowledge of AWS. Leveraging AWS Instance Roles to assume or elevate privileges from the Apache Tomcat user, the adversary would request and assume permissions of an instance role using a compromised AWS token. As shown in Figure 2, the adversary used elevated privileges to execute the open-source LINpeas privilege escalation utility.

```
Source Process User: tomcat | Source Process Command Line: curl -s -f -H
X-aws-ec2-metadata-token: <redacted>==
http://169.254.169.254/latest/meta-data/iam/security-credentials/<redacted>Ins
tanceRole-<redacted> | Source Process Parent Process: sh linpeas.sh | Source
Process Parent Process Start Time: 2022-10-XXTXX:XX:XXZ | Event Type: IP
Connect | Source Process Start Time: 2022-10-XXTXX:XX:XXZ | Destination IP:
<redacted> | Target file Path:
```

Figure 2. Adversary curl command leveraging an AWS Instance Role for privilege escalation, running the LinPEAS privilege escalation tool

Persistence and Remote Access Tactics

CrowdStrike incident responders observed that in many cases, the adversary gained access to the organization's MFA console to add their own devices (as an additional device per user) as trusted MFA devices. The devices would be assigned to compromised users for whom they had captured credentials. This technique, performed by taking advantage of user self-enrollment policies with the MFA provider, allowed the adversary to maintain a deeper and less obvious level of persistence instead of simply installing a remote access trojan to maintain access.

In almost all investigations, the adversary used a wide variety of RMM tools to maintain persistent access such as the list below:

- AnyDesk
- BeAnywhere
- Domotz
- DWservice
- Fixme.it
- Fleetdeck.io
- Itarian Endpoint Manager
- Level.io
- Logmein
- ManageEngine
- N-Able
- Pulseway
- Rport
- Rsocx
- ScreenConnect
- SSH RevShell and RDP Tunnelling via SSH
- Teamviewer
- TrendMicro Basecamp
- Sorillus
- ZeroTier

Because these tools are not nefarious or malicious in nature, they do not typically generate alerts and are not typically blocked by endpoint detection and response (EDR) technology. However, the combination of Falcon EDR telemetry with human analysis from OverWatch and incident responders painted a clear picture of the adversary's actions. During active hands-on-keyboard activity at most the intrusions CrowdStrike Services responded to, the adversary would often deploy multiple RMM tools and would quickly deploy another one if the organization blocked the previously used utilities.

Another tactic seen throughout multiple investigations is the adversary following a generic `DESKTOP-<7 alphanumeric characters>` naming pattern when using their own systems to connect to victim organization VPNs. And when creating systems in the victim organization's virtual desktop infrastructure, the adversary followed a pattern mimicking the victim organization's naming conventions.

The adversary has also targeted VMware ESXi hypervisors. In one investigation, the adversary installed the open-source *rsocx* reverse proxy tool and Level remote monitoring and management tool (RMM) on an ESXi appliance. In another investigation, the adversary executed the open-source port scanner tool RustScan from a Docker container running on an ESXi appliance. We have released the CrowdStrike Services ESXi Triage Collection and Containment Quick Reference Guide, which includes best practices to secure ESXi instances.

Throughout all investigations, the adversary used a variety of ISP and VPN providers to access victim Google Workspace environments, AzureAD and on-premises infrastructure. Many IP addresses originating from these ISPs were observed throughout the multiple investigations performed by CrowdStrike Services. Two of the most common ISPs CrowdStrike observed the adversary operating from were M247 and Digital Ocean. In each investigation, CrowdStrike leveraged Obsidian, a CrowdStrike Store partner, to implement custom ISP detections and restrictions in O365, AzureAD, Google Workspace and other software-as-a-service (SaaS) environments to quickly respond to, and further secure victim environments.

Reconnaissance and Lateral Movement

The adversary operates across Windows, Linux, Google Workspace, AzureAD, M365 and AWS environments. They have also accessed SharePoint and OneDrive environments for reconnaissance information, specifically searching for VPN information, MFA enrollment information, "how to" guides, help desk instructions and new hire guides.

In one investigation, the adversary accessed Azure Active Directory and performed bulk downloads of group members and users. By doing so, they were able to identify privileged users, along with the email addresses and AD attributes of all users within the victim tenant. Additional techniques employed by the adversary during this investigation included domain replication, lateral movement via Windows Management Instrumentation (WMI) using Impacket, SSH tunneling and various remote access tools.

In some investigations, the adversary downloaded tools using victim organization systems from sites such as file[.]io, GitHub, and paste[.]ee. The site transfer[.]sh was used by the adversary to perform data exfiltration of reconnaissance information.

In another investigation, an open source tool called `aws consoler` was used by the adversary to create temporary federated credentials for non-existent users issued by identity and access management (IAM) users. Federated Credentials help obfuscate which AWS credential is compromised and enables the adversary to pivot from the AWS CLI to console sessions without the need for MFA.

Mitigations and Containment Measures

In all investigations performed by CrowdStrike incident responders, the faster the organization implemented swift and bold security measures, the faster the adversary activity ceased. These containment and mitigation measures focused on secure identity and MFA controls and configurations, as highlighted below.

CrowdStrike Falcon Identity Threat Protection

- CrowdStrike Services leveraged Falcon Identity Threat Protection (ITP) in all related investigations as one of the primary detection and mitigation vehicles.
- Enable Falcon ITP rules to enforce restrictions on where privileged accounts can authenticate to and from (e.g., specific system to system only, blocking all RDP access, etc.)
- Enforce MFA challenges for privileged account authentication across all access methods (e.g., PowerShell, RDP, etc.)
- Monitor for ITP alerts regarding anomalous use of accounts, stale account usage, custom detection rules, DCsync and other domain replication activity.
- Identify compromised and at-risk accounts and credentials via custom rules and queries.
- Maintain good Active Directory hygiene monitoring and review any newly created accounts, modified groups or re-enabled accounts.
- Leverage the Protected Users Security Group in Active Directory to guard against NTLM used for privileged accounts.
- Real-time alerting for known compromised credential detection.

CrowdStrike Falcon Insight XDR and Obsidian

- CrowdStrike incident responders leveraged CrowdStrike Store partner Obsidian to implement custom ISP detections and restrictions in O365, AzureAD, Google Workspace and other SaaS environments from where the adversary was sourcing their activity.
- Configure alerts and blocks of unauthorized and/or anomalous RMM tools via custom indicators of attack (IOAs) as the adversary used a wide variety of RMM tools in each investigation.

CrowdStrike Falcon Complete and Falcon OverWatch

Effectively defending against advanced attackers takes technology as well as the skilled judgment of seasoned incident handlers, working 24/7 in order to respond quickly and effectively. Organizations looking to get the most value out of their CrowdStrike Falcon® platform investment should consider partnering with Falcon Complete[1] to provide their award-winning MDR services. The Falcon Complete team provides management, monitoring, and rapid response leveraging the Falcon platform, combining endpoint protection and identity protection in one turnkey solution.

Multifactor Authentication

- Implement MFA everywhere possible, especially for accounts that have access to third-party environments.
- Disable MFA simple push notifications in place of number-matching MFA where possible, or use One Time Passcodes with manual entry.
- Avoid unsupervised MFA self-enrollment or reset, and disallow any self-enrollment from external IP space.
- Allow only one trusted MFA device per user.
- Implement a global password reset and KRBTGT account reset twice per domain if compromise is suspected.

AWS Token Pivoting

- Ensure IMDSv2 is enabled on all EC2 instances to the extent possible (many products unfortunately still do not support v2).
- Enable GuardDuty in all active regions (GuardDuty has detections for abuse of EC2 instance credentials outside of an EC2 instance).
- Deprecate static IAM user access keys in favor of IAM roles where possible.

Azure

Enforce Azure Conditional Access Policies (CAP):

- Block legacy authentication
- Restrict logon by geographic region
- Enforce multifactor authentication for all users
- Enforce compliant devices

Network Access Controls

VPN host checking or other Network Access Control technology can limit the adversary's ability to log in remotely from non-organizational hosts.

General Vigilance

- Ensure user accounts, especially those with access to sensitive company information and/or access to mobile carrier networks, are assigned Principle of Least Privilege policies within all identity management applications e.g., Active Directory, Group Policy Objects, Identity Access Management, etc.
- Due diligence should be performed by internal security teams to ensure company insiders remain at a minimal risk of purposely supporting the adversary.
- Be cognizant of endpoint security tool bypass attempts. In many of the investigations CrowdStrike performed, the adversary attempted to bypass AV or EDR security tools on the endpoints.

Notes

1. CrowdStrike recently demonstrated the value of Falcon Complete in the first close-book MITRE ATT&CK® Evaluations for Security Service Providers, achieving the highest detection coverage (99%) by conclusively reporting 75 of the 76 adversary techniques.

Indicators of Compromise (IOCs)

Many of the passwords, file names, ISPs and IOCs listed below have been observed across multiple investigations tracked in this campaign. Some of the passwords, file names and system-associated domains used by the adversary are inappropriate and xenophobic and have been omitted from this article.

Also of note is the campaign has used a minimal amount of command and control (C2) malware, and therefore there are few host-based IOCs. The theme of the tactics and techniques used has been identity-focused, where the adversary leverages compromised credentials to access SaaS applications, or perform remote access using the victim organization VPN or RMM tools to carry out their objectives.

While the IP addresses listed below were seen in use by the adversary, stand-alone indicator IPs are considered low-fidelity. CrowdStrike is sharing the list below to provide information that may lead to actionable queries for security teams, however hits on these IP addresses may not indicate true positives. As with implementing any network traffic restrictions, caution should be exercised if blocking any of the network-based IOCs.

Network-Based IOCs

IOC	Background
100.35.70.106	Adversary remote access
119.93.5.239	Adversary remote access
136.144.19.51	Adversary MFA registration
136.144.43.81	Adversary remote access
141.94.177.172	Adversary remote access

142.93.229.86	Adversary remote access
143.244.214.243	Adversary remote access
144.76.136.153	IP associated with transfer.sh used for data exfil
146.70.103.228	Adversary MFA registration
146.70.107.71	Adversary remote access
146.70.112.126	Adversary remote access
146.70.127.42	Adversary MFA registration
146.70.45.166	Adversary remote access
146.70.45.182	Adversary remote access
152.89.196.111	Adversary remote access
159.223.213.174	Adversary remote access
162.118.200.173	Adversary remote access
169.150.203.51	Adversary remote access
172.98.33.195	Adversary remote access
173.239.204.129	Adversary MFA registration
173.239.204.130	Adversary remote access
173.239.204.131	Adversary MFA registration
173.239.204.132	Adversary remote access
173.239.204.133	Adversary remote access
173.239.204.134	Adversary remote access
18.206.107.24/29	Adversary added CIDR range as an AWS security group to allow inbound traffic
180.190.113.87	Failed adversary login
185.120.144.101	Adversary remote access
185.123.143.197	Adversary remote access
185.123.143.201	Adversary remote access
185.123.143.205	Adversary remote access
185.123.143.217	Adversary remote access
185.156.46.141	Adversary remote access
185.163.109.66	Adversary remote access
185.181.102.18	Adversary remote access
185.195.19.206	Adversary remote access
185.195.19.207	Adversary remote access

185.202.220.239	Adversary remote access
185.202.220.65	Adversary remote access
185.240.244.3	Registered authenticator app and adversary VPN logins
185.243.218.41	Adversary remote access
185.247.70.229	Adversary remote access
185.45.15.217	Adversary remote access
185.56.80.28	Adversary remote access
188.166.101.65	Reverse SSH tunnel
188.166.117.31	Adversary remote access
188.214.129.7	Adversary remote access
192.166.244.248	Adversary remote access
193.27.13.184	Adversary remote access
193.37.255.114	Adversary remote access
194.37.96.188	Adversary remote access
195.206.105.118	Adversary remote access
195.206.107.147	Adversary remote access
198.44.136.180	Azure MFA registration
198.54.133.45	Adversary remote access
198.54.133.52	Adversary remote access
217.138.198.196	Adversary remote access
217.138.222.94	Adversary remote access
23.106.248.251	Adversary remote access
2a01:4f8:200:1097::2	IPv6 associated with transfer.sh used for exfil
31.222.238.70	Adversary remote access
35.175.153.217	Adversary remote access
37.19.200.142	Adversary remote access
37.19.200.151	Adversary remote access
37.19.200.155	Adversary remote access
45.132.227.211	Adversary remote access
45.132.227.213	Adversary remote access
45.134.140.171	Adversary IP used to download documents from victim SharePoint
45.134.140.177	Adversary remote access

45.86.200.81	Adversary remote access
45.91.21.61	Adversary remote access
5.182.37.59	Adversary remote access
51.210.161.12	Adversary remote access
51.89.138.221	Adversary MFA registration
62.182.98.170	Adversary remote access
64.190.113.28	Adversary remote access
67.43.235.122	Adversary remote access
68.235.43.20	Adversary remote access
68.235.43.21	Adversary remote access
68.235.43.38	Failed adversary login activity
82.180.146.31	Failed adversary login activity
83.97.20.88	Adversary remote access
89.46.114.164	Failed adversary login activity
89.46.114.66	Adversary remote access
91.242.237.100	Adversary remote access
93.115.7.238	Adversary remote access
98.100.141.70	Adversary remote access
aws-cli/1.19.59 Python/3.9.2 Linux/5.10.0-kali5-amd64 botocore/1.27.43	UA associated with aws_consoler used by the adversary

Host-Based IOCs

IOC	SHA256	Background
change.m31!!!	N/A	Password used by adversary extensively
<redacted>.exe	3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08	Packed Fleet Deck binary
IIatZ	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005	Backconnect TCP malware used to read and execute shellcode from C2, executed via OpenAM exploit

insomnia.exe	acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918	Prevents a system from entering sleep mode
linpeas.log	N/A	LINPeas Local Privilege Escalation Enumeration tool output log
linpeas.sh	N/A	LINPeas Local Privilege Escalation Enumeration tool
lockhuntersetup_3-4-3.exe	982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e	File unlocking tool (for deletion of locked files)
mp	443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58	“Midgetpack” packed binary used to establish connections to 67.43.235.122 on ports 4444 and 8888
mpbec	443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58	“Midgetpack” packed binary used to establish connections to 67.43.235.122 on ports 4444 and 8888
naaNa.b64	53b7d5769d87ce6946efcba00805ddce65714a0d8045aeee532db4542c958b9f	Backconnect TCP malware used to read and execute shellcode from C2, executed via OpenAM exploit
ok.exe	4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93	Binary with same name as other adversary tooling to prevent system from sleeping

RmaDc	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005	Backconnect TCP malware used to read and execute shellcode from C2
rsocx.exe	648c2067ef3d59eb94b54c43e798707b030e0383b3651bcc6840dae41808d3a9	SOCKS5 bind/reverse proxy

Acknowledgements

CrowdStrike would like to thank all of the dedicated employees on the CrowdStrike Intelligence, Endpoint Recovery Services, Falcon OverWatch and Incident Response teams for supporting all of the investigations in this campaign, spending countless late nights, weekends and intense “firefights” detecting and mitigating active hands-on-keyboard activity.

Additional Resources

- *Read about adversaries tracked by CrowdStrike in 2021 in the 2022 CrowdStrike Global Threat Report and in the 2022 Falcon OverWatch™ Threat Hunting Report.*
- *Learn more about how CrowdStrike Services can help your organization prepare to defend against sophisticated threats, respond and recover from incidents with speed and precision, and fortify your cybersecurity practices.*
- *Learn how CrowdStrike Falcon® Identity Protection products reduce costs and risks across the enterprise by protecting workforce identities.*
- *Check out this live attack and defend demo by the Falcon Complete team to see Falcon Identity Threat Protection in action.*
- *Watch this video to see how Falcon Identity Threat Protection detects and stops ransomware attacks.*
- *Watch an introductory video on the CrowdStrike Falcon® console and register for an on-demand demo of the market-leading CrowdStrike Falcon® platform in action.*
- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*