Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies

December 02, 2022 | Tim.Parisi | From The Front Lines

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.

CATEGORIES

Cloud & Application Security 104
Counter Adversary Operations 184
Endpoint Security & XDR 307
Engineering & Tech 78
Executive Viewpoint 162
Exposure Management 84
From The Front Lines 190
Identity Protection 37
Next-Gen SIEM & Log Management 91
Public Sector 37
Small Business 8

CONNECT WITH US

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.

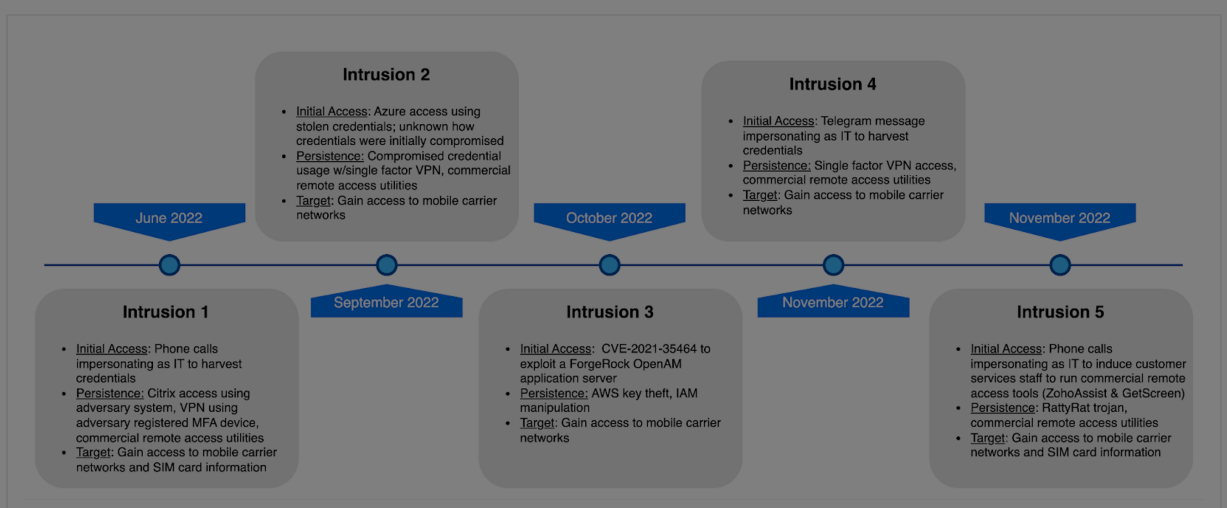

Figure 1. Sampling of relevant investigation summaries performed by CrowdStrike Services since June 2022 (click to enlarge)

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

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

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

- 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

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

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

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	Bac
100.35.70.106	Adv
119.93.5.239	Adv
136.144.19.51	Adv
136.144.43.81	Adv
141.94.177.172	Adv
142.93.229.86	Adv
143.244.214.243	Adv

146.70.45.166	Adv
146.70.45.182	Adv
152.89.196.111	Adv
159.223.213.174	Adv
162.118.200.173	Adv
169.150.203.51	Adv
172.98.33.195	Adv
173.239.204.129	Adv
173.239.204.130	Adv
173.239.204.131	Adv
173.239.204.132	Adv
173.239.204.133	Adv
173.239.204.134	Adv
18.206.107.24/29	Adv
180.190.113.87	Fail
185.120.144.101	Adv
185.123.143.197	Adv
185.123.143.201	Adv
185.123.143.205	Adv
185.123.143.217	Adv
185.156.46.141	Adv
185.181.102.18	Adv
185.195.19.206	Adv
185.195.19.207	Adv
185.202.220.239	Adv
185.202.220.65	Adv

185.56.80.28	Adv
188.166.101.65	Rev
188.166.117.31	Adv
188.214.129.7	Adv
192.166.244.248	Adv
193.27.13.184	Adv
193.37.255.114	Adv
194.37.96.188	Adv
195.206.105.118	Adv
195.206.107.147	Adv
198.44.136.180	Azu
198.54.133.45	Adv
198.54.133.52	Adv
217.138.198.196	Adv
217.138.222.94	Adv
23.106.248.251	Adv
2a01:4f8:200:1097::2	IPv
31.222.238.70	Adv
35.175.153.217	Adv
37.19.200.142	Adv
37.19.200.151	Adv
37.19.200.155	Adv
45.132.227.211	Adv
45.132.227.213	Adv
45.134.140.171	Adv

51.89.138.221	Adv
62.182.98.170	Adv
64.190.113.28	Adv
67.43.235.122	Adv
68.235.43.20	Adv
68.235.43.21	Adv
68.235.43.38	Fail
82.180.146.31	Fail
83.97.20.88	Adv
89.46.114.164	Fail
89.46.114.66	Adv
91.242.237.100	Adv
93.115.7.238	Adv
98.100.141.70	Adv
aws-cli/1.19.59 Python/3.9.2 Linux/5.10.0-kali5-amd64 botocore/1.27.43	UA

Host-Based IOCs

IOC	SHA256
change.m31!!!	N/A
<redacted>.exe	3ea2d190879c8933363b222c686009b81ba8af
IlatZ	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f
insomnia.exe	acadf15ec363fe3cc373091cbe879e64f9351393
linpeas.log	N/A
linpeas.sh	N/A
lockhuntersetup_3-4-3.exe	982dda5eec52dd54ff6b0b04fd9ba8f4c566534
mp	443dc750c35afc136bfea6db9b5ccbdb6adb63c

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.*

Related Content

CrowdStrike Named a

How to Defend Employees

The Anatomy of an ALPHA

« How Falcon OverWatch Hunts for Out-of-Band Application Security Testing

CrowdStrike Services Helps Organizations Prioritize Patching Vulnerabilities with CrowdStrike Falcon Spotlight »