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.

Featured
Recent
Video

- 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

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.

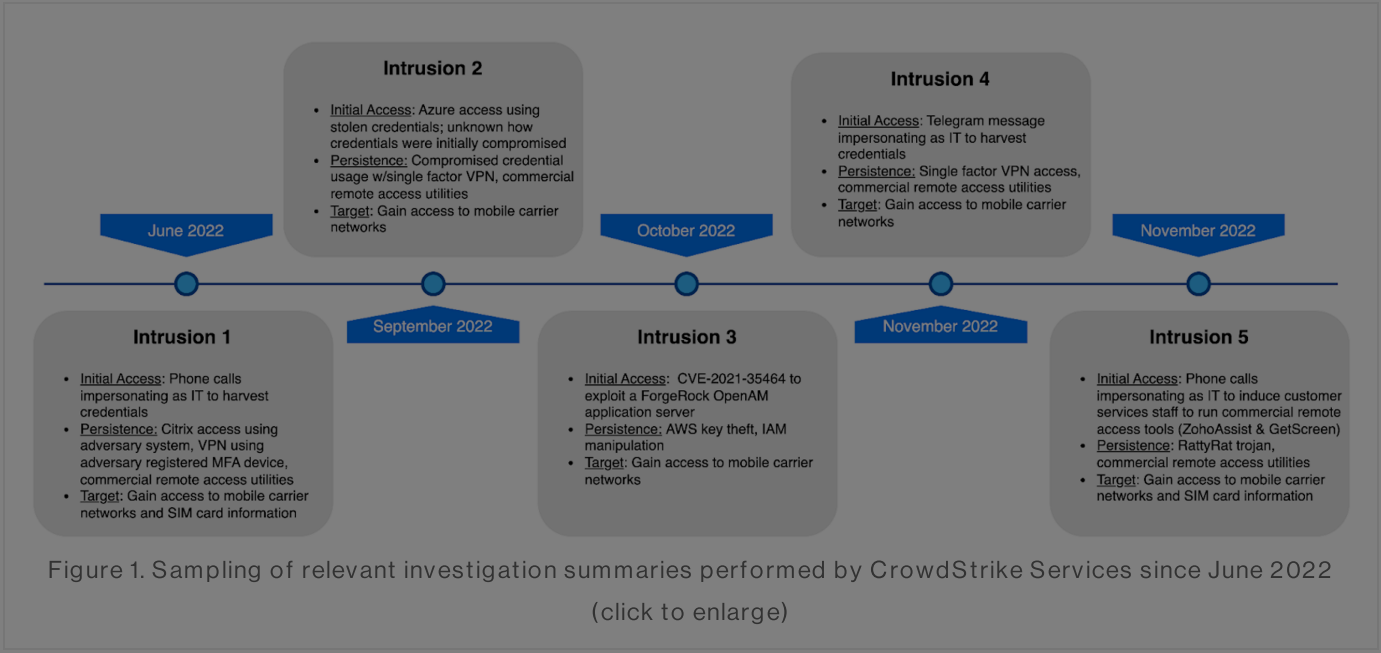

Figure 1. Sampling of relevant investigation summaries performed by CrowdStrike Services since June 2022 (click to enlarge)

Initial Access and Privilege Escalation

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

- 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)

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

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

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

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

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

100.35.70.106	Adversary ren
119.93.5.239	Adversary ren
136.144.19.51	Adversary MF
136.144.43.81	Adversary ren
141.94.177.172	Adversary ren
142.93.229.86	Adversary ren
143.244.214.243	Adversary ren
144.76.136.153	IP associated
146.70.103.228	Adversary MF
146.70.107.71	Adversary ren
146.70.112.126	Adversary ren
146.70.127.42	Adversary MF

Featured
Recent
Video

172.98.33.193	Adversary ren
173.239.204.129	Adversary MF
173.239.204.130	Adversary ren
173.239.204.131	Adversary MF
173.239.204.132	Adversary ren
173.239.204.133	Adversary ren
173.239.204.134	Adversary ren
18.206.107.24/29	Adversary adc
180.190.113.87	Failed adversa
185.120.144.101	Adversary ren
185.123.143.197	Adversary ren
185.123.143.201	Adversary ren

Featured
Recent
Video

185.202.220.239	Adversary ren
185.202.220.65	Adversary ren
185.240.244.3	Registered au
185.243.218.41	Adversary ren
185.247.70.229	Adversary ren
185.45.15.217	Adversary ren
185.56.80.28	Adversary ren
188.166.101.65	Reverse SSH
188.166.117.31	Adversary ren
188.214.129.7	Adversary ren
192.166.244.248	Adversary ren
193.2713.184	Adversary ren

198.54.133.32	Adversary ren
217.138.198.196	Adversary ren
217.138.222.94	Adversary ren
23.106.248.251	Adversary ren
2a01:4f8:200:1097::2	IPv6 associate
31.222.238.70	Adversary ren
35.175.153.217	Adversary ren
37.19.200.142	Adversary ren
37.19.200.151	Adversary ren
37.19.200.155	Adversary ren
45.132.227.211	Adversary ren
45.132.227.213	Adversary ren

Featured
Recent
Video

51.89.138.221	Adversary MF
62.182.98.170	Adversary rem
64.190.113.28	Adversary rem
67.43.235.122	Adversary rem
68.235.43.20	Adversary rem
68.235.43.21	Adversary rem
68.235.43.38	Failed adversa
82.180.146.31	Failed adversa
83.97.20.88	Adversary rem
89.46.114.164	Failed adversa
89.46.114.66	Adversary rem
91.242.237.100	Adversary rem

Featured
Recent
Video

change.m3t!!!	N/A
<redacted>.exe	3ea2d190879c8933363b222c686009b81ba8af9eb6ae36
llatZ	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e0
insomnia.exe	acadf15ec363fe3cc373091cbe879e64f935139363a8e8df
linpeas.log	N/A
linpeas.sh	N/A
lockhuntersetup_3-4-3.exe	982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46
mp	443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c
mpbec	443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c
naaNa.b64	53b7d5769d87ce6946efcba00805ddce65714a0d8045ae
ok.exe	4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e
RmaDc	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e0

Featured
Recent
Video

- *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.*

for Cybersecurity Incident Response Services

CATEGORIES

CROWDSTRIKE | BLOG

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

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

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

Sign Up

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. Cookie Notice

ABOUT COOKIES ON THIS SITE