Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Attackers target Telecommunications sector to gain network access

Date of Publication	Admiralty Code	TA Number
December 6, 2022	A2	TA2022283

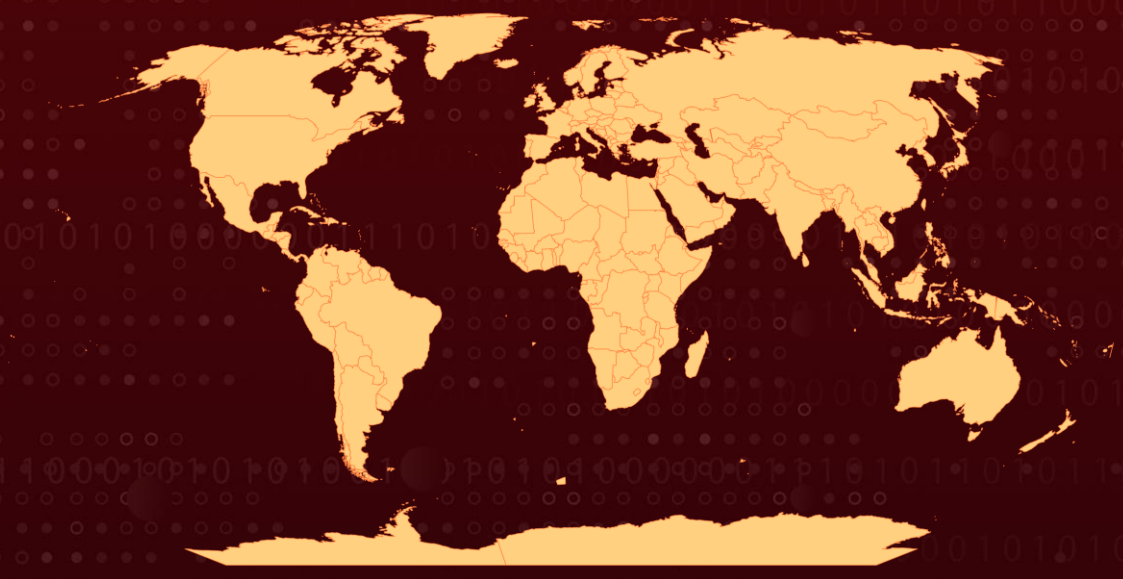
Summary

Active Since: June 2022
Attack Countries: Worldwide
Threat Actor: Scattered Spider
Attack Industries: Telecommunications and business process outsourcing(BPO)
Attack: Get access to mobile carriers' networks and perform SIM swapping.

CVE

CVE	NAME	PATCH
CVE-2021-35464	ForgeRock AM Java deserialization vulnerability	✓

Attack Regions



Attack Details

#1 To gain initial access, the adversary used social engineering to impersonate IT, staff, using phone calls, SMS, and/or Telegram. When the adversary gains access to the target environment, it performs constant activity within that environment.

#2 As mitigation measures are slowly implemented, the adversary becomes more active and sets up additional persistence mechanisms, such as VPN access and multiple RMM tools. Adversaries reverted some mitigation measures by reenabling accounts previously disabled by victims.

#3 The adversary utilized mobile carrier networks from a Telco or BPO environment and performed SIM swapping. The activity has a low confidence level of association with the SCATTERED SPIDER.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0001 Initial Access	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0008 Lateral Movement	T1040 Network Sniffing	T1036 Masquerading	T1134 Access Token Manipulation
T1566 Phishing	T1090 Proxy	T1190 Exploit Public-Facing Application	T1219 Remote Access Software
T1078 Valid Accounts	T1046 Network Service Discovery	T1593 Search Open Websites/Domains	T1210 Exploitation of Remote Services

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005 acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918 982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e 648c2067ef3d59eb94b54c43e798707b030e0383b3651bcc6840dae41808d3a9 53b7d5769d87ce6946efcba00805ddce65714a0d8045aeee532db4542c958b9f 443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58 4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93 3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08
SHA1	d8cb0d5bbeb20e08df8d2e75d7f4e326961f1bf5
MD5	56fd7145224989b92494a32e8fc6f6b6
IPV4	89[.]46[.]114[.]66 51[.]89[.]138[.]221 51[.]210[.]161[.]12 5[.]182[.]37[.]59 45[.]91[.]21[.]61 45[.]86[.]200[.]81 45[.]134[.]140[.]177

TYPE	VALUE
IPV4	45[.]132[.]227[.]213 37[.]19[.]200[.]155 37[.]19[.]200[.]151 37[.]19[.]200[.]142 31[.]222[.]238[.]70 23[.]106[.]248[.]251 217[.]138[.]222[.]94 217[.]138[.]198[.]196 198[.]54[.]133[.]52 198[.]54[.]133[.]45 198[.]44[.]136[.]180 195[.]206[.]105[.]118 194[.]37[.]96[.]188 193[.]37[.]255[.]114 193[.]27[.]13[.]184 192[.]166[.]244[.]248 188[.]214[.]129[.]7 188[.]166[.]117[.]31 188[.]166[.]101[.]65 185[.]56[.]80[.]28 185[.]45[.]15[.]217 185[.]247[.]70[.]229 185[.]240[.]244[.]3 185[.]202[.]220[.]65 185[.]202[.]220[.]239 185[.]195[.]19[.]207 185[.]195[.]19[.]206 185[.]181[.]102[.]18 185[.]163[.]109[.]66 185[.]123[.]143[.]197 185[.]120[.]144[.]101

Patch Link

https://backstage.forgerock.com/knowledge/kb/article/a47894244

References

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

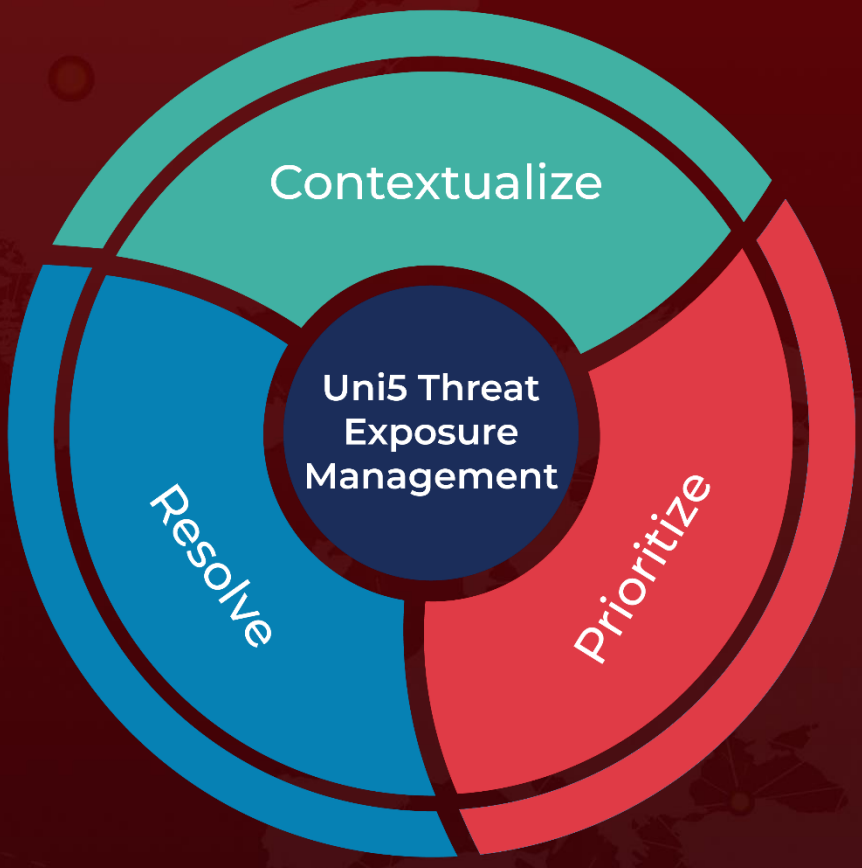
https://otx.alienvault.com/pulse/638ed7de06391c71d4d7fb7b

https://www.bleepingcomputer.com/news/security/sneaky-hackers-reverse-defense-mitigations-when-detected/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 6, 2022 . 4:15 AM

More at www.hivepro.com