Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Middle East targeted by Earth Bogle using NjRAT malware

Date of Publication	Admiralty code	TA Number
January 18, 2023	A1	TA2023030

Summary

First Appearance: 2022
Actor Name: Earth Bogle
Target Region: Middle East and North Africa.

Actor Map

Actor Details

#1 Earth Bogle's active campaign hosts malware on public cloud storage sites like files.fm and failiem.lv. Compromised web servers also distribute NjRAT, also known as Bladabindi, a remote access trojan (RAT) malware discovered in 2013, used to gain unauthorized access and control over victim devices.

#2 The malicious file is concealed within a Microsoft Cabinet (CAB) archive file and disseminated as a "sensitive" audio file via social media, file sharing, or phishing email. The initial malicious CAB file includes an obfuscated VBS (Virtual Basic Script) dropper that is capable of delivering the next element of the attack.

#3 When the second stage payload is run, a maliciously obfuscated PowerShell script is obtained. This script dumps five files in total: two binaries, a VBS script, a PowerShell script, and a Windows batch script. Upon execution, the dropper terminates all .NET related processes. The final payload NjRAT is deployed and allows attackers to perform various intrusive operations on compromised devices.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Earth Bogle	Unknown **MOTIVE** Information theft and espionage	Middle East and North Africa.	

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 actor 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

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
T1059 Command and Scripting Interpreter	**TA0005** Defense Evasion	**TA0009** Collection	**TA0011** Command and Control
T1104 Multi-Stage Channels	**T1530** Data from Cloud Storage	**T1055** Process Injection	**T1566** Phishing
T1547 Boot or Logon Autostart Execution			

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	2f1c9ae4477f2b990ec6d084cb00c791b4e33be4828bda947f6c600239a13d0a,6bd72e80361c1be1a3cbe79f26d34855a0fd6483784b0de5f30bf36b4536a9c1,a531b9fdb6c216839451aae63cd2a13e552ac1960ae3f2e298a1c8fca54b96c3,9c2f26dcba299e0fadd6c400adc4cef030fb5b66c10cceccf2f99849871f5490,d039aebefb27b463d620f462938ade04c0492f5274d0b28a44777e6de4c80673,00d8ac438ea309ca28693b9760bf9c2a6dce079699c503f7d7ba749fdcb8f4c1,f17059c48b1f2a9f80eae8dca222d5753aa3d8d20a26bf67546a084ca79e108e,74aad1d1c94d222b5ab92efd6c7aaf1b40c3246a44917a51d6bf6f45d6f9a65b,4888c4fe2e334dcb358ca810229f1d0699c792cf8b6fbf2e1b48a66f7b2d695c,6560ef1253f239a398cc5ab237271bddd35b4aa18078ad253fd7964e154a2580,353e4e1f3e4002e3d4264ac3ede26991cf5dcbe24774e9c1eb6e2a6e2d730778,9bb8f517fd031f9c839cd54d8b6c04fb51768d778e0f640619b019d3ba1f7f55,78ac9da347d13a9cf07d661cdcd10cb2ca1b11198e4618eb263aec84be32e9c8,67c4f872bff257417a98a8bb75ac110d3ca5c7d5584f2de3c5a2337d2a948710,c03299acd37ab7c15f0d949d15f38cceacbfa817106382616e6d4064a2315942,60eeb78b09fc7fe64dde782609edc2ab4eb6daff3df1db88b054932f417e5b45,8ecc313c38eae8fa61c67bbe37532022b6deff76ae857961fc594190cff2f7a7,be979023ad6ab5427be284eac89929a9ce1d2fb83d6e28f7ce1748a4f3756e49,4c24d601bda43317eded06b0aad61fb6734e760048193779006a1030d39f5a4a,af1f23e8fbe2c39e30644bb6715dd272c4b237974124f4425ab4d90fb7b4c087,a7e2b399b9f0be7e61977b51f6d285f8d53bd4b92d6e11f74660791960b813da,4985b6e286020de70f0b74d457c7e387463ea711ec21634e35bc46707dfe4c9b

TYPE	VALUE
URLs	hxxps[:]//gpla.gov.ly/out/555555555555555555(OUT)[.]jpg hxxps[:]//gpla.gov.ly/4444488888/DFvKKnFBvI_HEX[.]jpg hxxps[:]//www.gpla.gov.ly/news/ETErpTJVDq_DEC[.]jpg hxxps[:]//gpla.gov.ly/333333/cEsITGEhOH_aaaaaa[.]jpg hxxps://www.shorturl[.]at/fkvxD
Domains	2525.libya2020.com[.]ly gpla[.]gov[.]ly

References

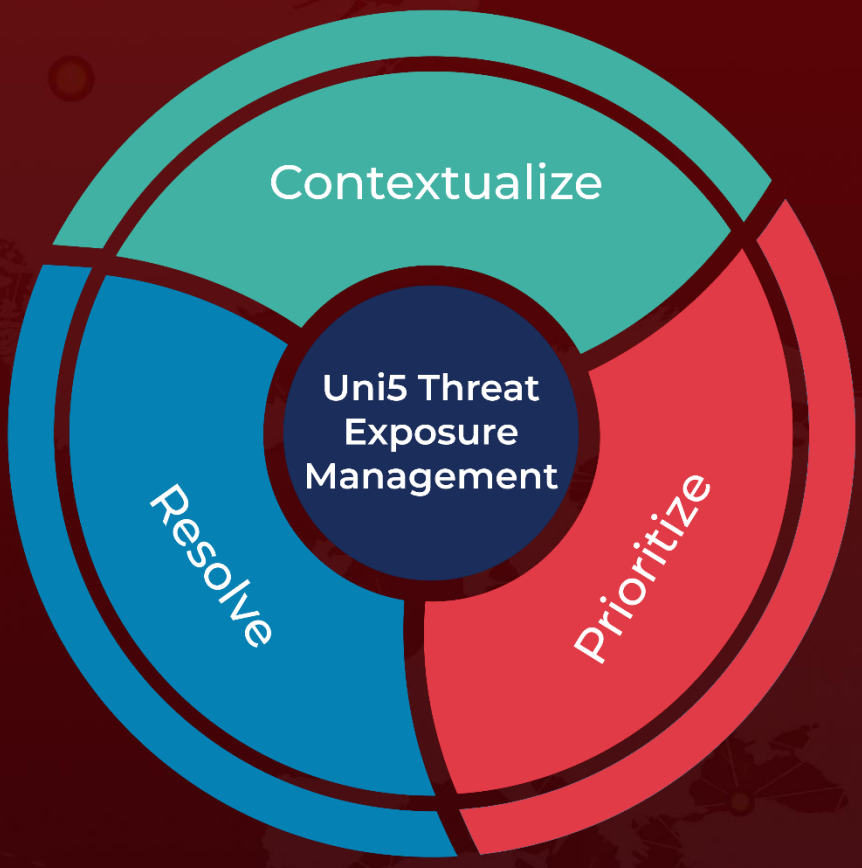
https://www.trendmicro.com/en_us/research/23/a/earth-bogle-campaigns-target-middle-east-with-geopolitical-lures.html

https://attack.mitre.org/software/S0385/

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

January 18, 2023 . 2:22 AM

More at www.hivepro.com