Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

China-based MirrorFace APT group targeting Japanese Political Entities

Date of Publication	Admiralty Code	TA Number
December 16, 2022	A1	TA2022301

Summary

First Appearance: June 29, 2022
Actor Name: MirrorFace
Target Region: Japan
Target Sectors: Political entities, Media, Defense, Think tanks, Academic institutions, and diplomatic organizations.

Actor Map

Actor Details

#1 A Chinese-speaking APT group named MirrorFace has started its attacks by spearphishing campaign with LODEINFO backdoor, targeting Japanese political entities since June 29, 2022 and this campaign operation is named as LiberalFace. The main motive of MirrorFace threat actor group is the exfiltration of data and espionage.

#2 After gaining initial access, LODEINFO delivers additional malware, later it exfiltrates the credentials, documents, and emails of the victim. Post-compromise activities include the command-and-control server sending commands to LODEINFO to carry out the actions in a manual or semi-manual manner.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
MirrorFace	China **MOTIVE** Exfiltration of files and Espionage	Japan	Political entities, Media, Defense, Think tanks, Academic institutions, and diplomatic organizations

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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0004 Collection	TA0011 Command and Control	TA0003 Persistence	TA0010 Exfiltration
TA0040 Impact	T1566.001 Phishing: Spearphishing Attachment	T1106 Native API	T1204.002 User Execution: Malicious File
T1559.001 Inter-Process Communication Component Object Model	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	T1112 Modify Registry	T1055 Process Injection
T1140 Deobfuscation/Decode Files or Information	T1574.002 Hijack Execution Flow DLL Side-Loading	T1082 System Information Discovery	T1083 File and Directory Discovery
T1057 Process Discovery	T1033 System Owner/User Discovery	T1005 Data from Local System	T1071.001 Application Layer Protocol: Web Protocols
T1056.001 Input Capture: Keylogging	T1113 Screen Capture	T1614.001 System Location Discovery: System Language Discovery	T1560.001 Archive Collected Data: Archive via Utility
T1114.001 Email Collection: Local Email Collection	T1132.001 Data Encoding: Standard Encoding	T1573.001 Encrypted Channel: Symmetric Cryptography	T1001.001 Data Obfuscation: Junk Data
T1041 Exfiltration Over C2 Channel	T1071.002 Application Layer Protocol: File Transfer Protocols	T1486 Data Encrypted for Impact	T1001.001 Data Obfuscation: Junk Data

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	F4691FF3B3ACD15653684F372285CAC36C8D0AEF DB81C8719DDAAE40C8D9B9CA103BBE77BE4FCE6C A8D2BE15085061B753FDEBBDB08D301A034CE1D5 0AB7BB3FF583E50FBF28B288E71D3BB57F9D1395 E888A552B00D810B5521002304D4F11BC249D8ED
IPV4	172.105.217[.]233 167.179.116[.]56 103.175.16[.]39 45.32.13[.]180 5.8.95[.]174

References

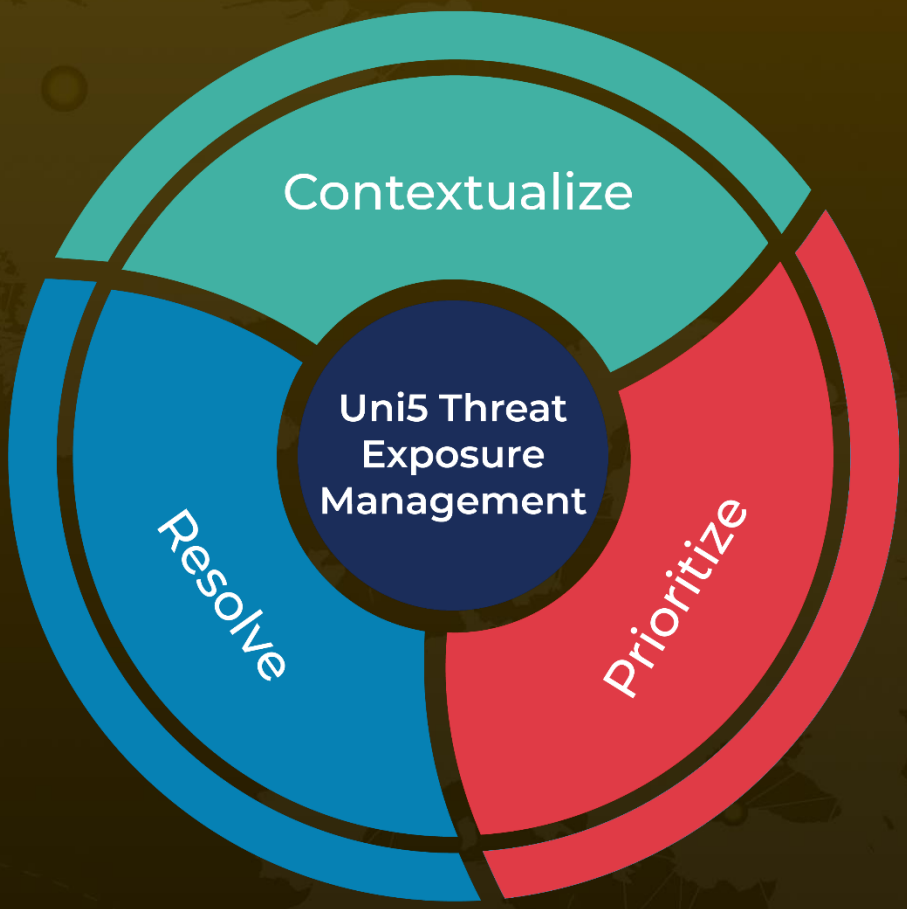
https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/

https://aavar.org/cybersecurity-conference/index.php/behind-the-mirrorface-mask-lodeinfo-malware-interfering-with-japanese-elections/

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 16, 2022 • 6:00AM

More at www.hivepro.com