Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

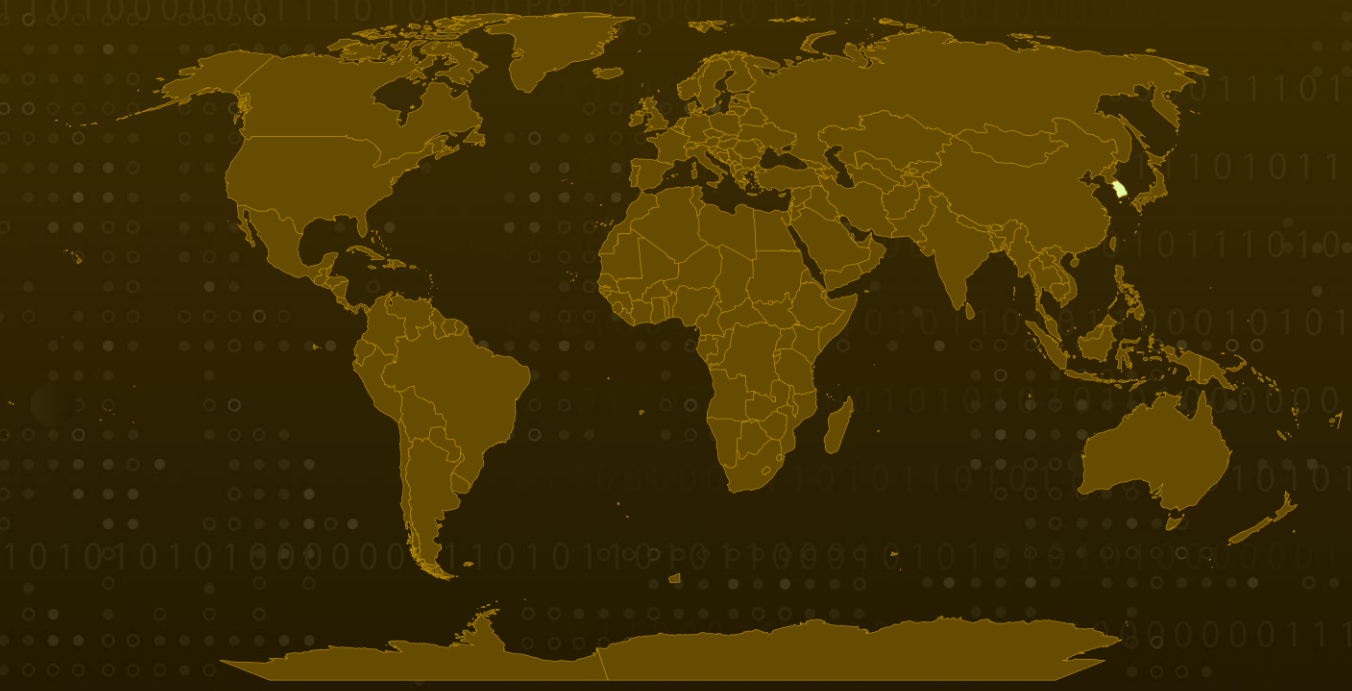
New Ransomware Campaign "TZW" Linked to GlobeImposter Targets South Korean Organizations

Date of Publication	Admiralty Code	TA Number
February 17, 2023	A1	TA2023086

Summary

Date: 2016
Attack Region: South Korea
Attack: A new ransomware campaign called TZW, linked to the GlobeImposter malware family, affecting South Korean organizations

Attack Regions



Attack Details

#1

A new ransomware campaign called TZW is affecting organizations in South Korea. The campaign is linked to the known malware family GlobeImposter, suggesting that the actors behind GlobeImposter are rebranding and updating their payloads to obfuscate their identity and sidestep crackdowns.

#2

GlobeImposter, first observed in 2016, has multiple versions and variations that have appeared over the years, and it is most often delivered via phishing emails as an attachment or a link to a malicious attachment. The ransomware has been used in conjunction with high-end cybercriminal groups, and its payloads are typically distributed via 7zip or traditional zip file archives. GlobeImposter has the ability to delete volume shadow copies, and its delivery methods and functionalities are consistent with those of the new variant TZW.

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

TA0007 Discovery	TA0004 Privilege Escalation	TA0003 Persistence	TA0009 Collection
TA0005 Defense Evasion	TA0040 Impact	T1070.004 File Deletion	T1027 Obfuscated Files or Information
T1005 Data from Local System	T1202 Indirect Command Execution	T1486 Data Encrypted for Impact	T1070 Indicator Removal
T1112 Modify Registry	T1012 Query Registry	T1083 File and Directory Discovery	T1027.002 Software Packing
T1082 System Information Discovery	T1490 Inhibit System Recovery	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution:

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	4585da0ff7a763be1a46d78134624f7cd13e6940 14be1c43fbfb325858cda78a126528f82cf77ad2 dc98b516c9c589c2b40bc754732ad5f16deb7c82 d034880d1233d579854e17b6ffad67a18fb33923 858f3f7f656397fcf43ac5ea13d6d4cbe7a5ca11 9a080cd497b8aa0006dc953bd9891155210c609c 8c64e820a4c5075c47c4fbaea4022dc05b3fd10b 3326708ba36393b1b4812aa8c88a03d72689ac24 cf5ab37612f24ed422a85e3745b681945c96190e cf21028b54c4d60d4e775bf05efa85656de43b68

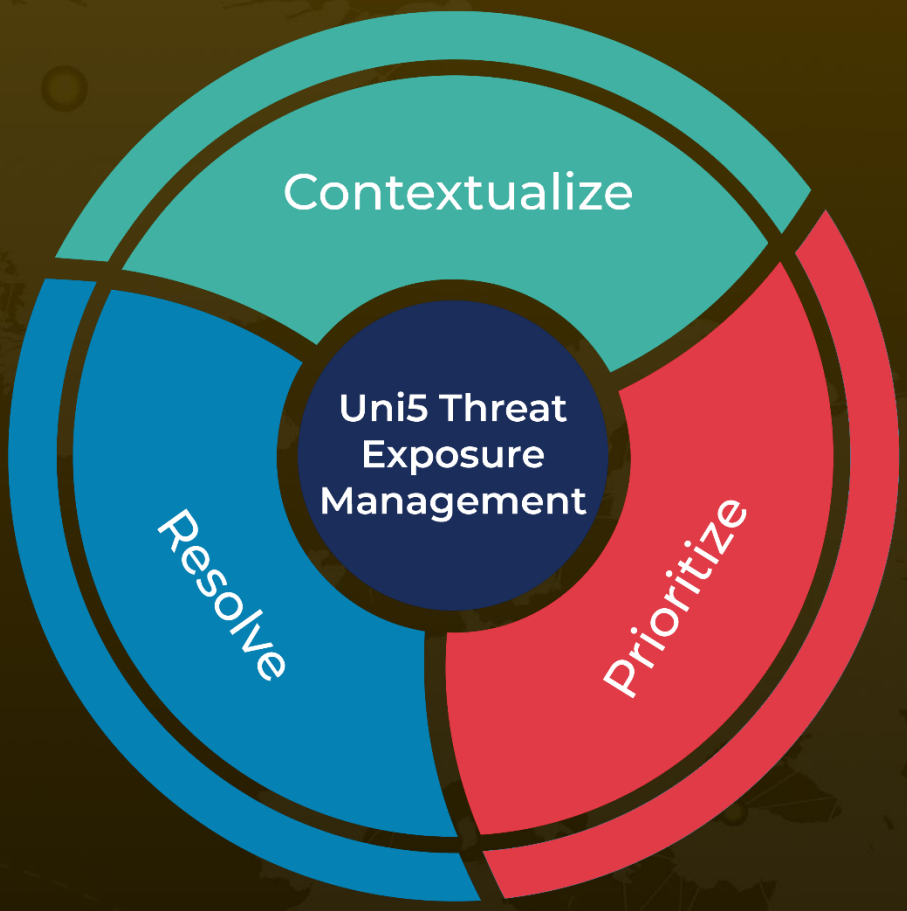
References

https://www.sentinelone.com/blog/recent-tzw-campaigns-revealed-as-part-of-globeimposter-malware-family/

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

February 17, 2023 • 1:00 AM

More at www.hivepro.com