Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

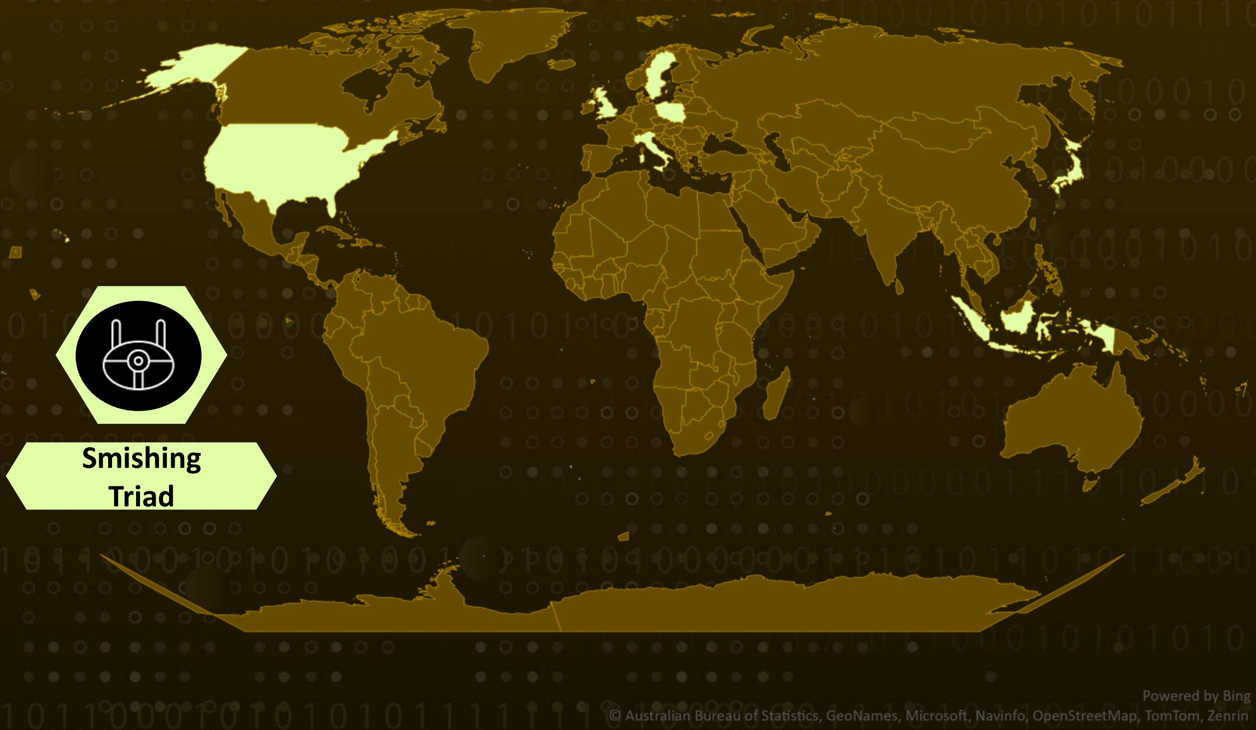
Chinese 'Smishing Triad' Group Targeting US Citizens

Date of Publication	Admiralty Code	TA Number
September 8, 2023	A1	TA2023360

Summary

First Seen: February 23, 2023
Actor Name: Smishing Triad
Attack Region: United States, United Kingdom, Poland, Sweden, Italy, Indonesia, Japan
Targeted Industry: Financial Services, Retail, E-commerce, Postal and Delivery Services, Technology, Telecommunications
Attack: Smishing Triad is a Chinese-speaking cyber-criminal group that has been conducting a large-scale smishing campaign targeting US citizens and other countries. Smishing is a form of phishing that uses text messages or iMessages to trick victims into clicking on malicious links or providing personal information.

Attack Regions


Smishing Triad
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A significant smishing campaign targeting U.S. citizens, with previous victims in U.K, Poland, Sweden, Italy, Indonesia, Japan, and other countries. The campaign, has been named "Smishing Triad“, belived to be based in China, involves sophisticated impersonations of organizations like the Royal Mail, New Zealand Postal Service, and others.

#2

Smishing, a form of phishing via text messages, tricks victims into revealing personal and financial information. In this case, the attackers use iMessage from compromised Apple iCloud accounts to deceive victims. They've also created and sold customized smishing kits on Telegram, forming a "fraud-as-a-service" network.

#3

Researchers uncovered a vulnerability in Smishing kit and was able to shed light on the threat actors and recover over 108,000 victim information. The analysis revealed Chinese signatures and a connection to Telegram user "wangduoyu8."

#4

The "Smishing Triad" not only engages in identity theft and financial fraud but also supplies other cybercriminals with tailored smishing kits. They offer subscriptions starting at $200 per month, facilitating fraudulent activities with scripts using various frameworks.

#5

The group collaborates with other cybercriminals and targets postal and delivery services worldwide. They have even developed malicious code injections targeting online shopping platforms and created counterfeit forms impersonating government agencies like the Italian Revenue Agency.

#6

The significance of this campaign lies in its use of smishing as a highly effective attack vector, taking advantage of users' trust in SMS and iMessage communication.

Recommendations

Awareness about phishing: Do not click on links in text messages from unknown senders. Be suspicious of any text messages that request personal or financial information.

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities. Regularly update antivirus and anti-malware software to ensure the latest threat definitions by the malware.

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0006** Credential Access	**TA0042** Resource Development	**TA0040** Impact
TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1589.001 Credentials	**T1589** Gather Victim Identity Information	**T1598** Phishing for Information	**T1036** Masquerading
T1078 Valid Accounts	**T1586** Compromise Accounts		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	wangduoyu[.]me wangduoyu[.]shop wangduoyu[.]site poczta-polska[.]cc ususmx[.]top ususmx[.]top ususnb[.]top ususgs[.]top ususcgh[.]top uspoddp[.]top uspsjh[.]top ususnu[.]top usushk[.]top ususcsa[.]top uspoky[.]top usplve[.]top ususcac[.]top uspshhg[.]top uspodad[.]top uspogumb[.]top uspsuiu[.]top uspshhg[.]top uspsuiu[.]top uspskkq[.]top ususuua[.]top uspodaa[.]top uspoadc[.]top uspshhg[.]top usplve[.]top usushk[.]top uspshhg[.]top ususcgh[.]top ususnu[.]top ususnb[.]top uspoddp[.]top ususuua[.]top

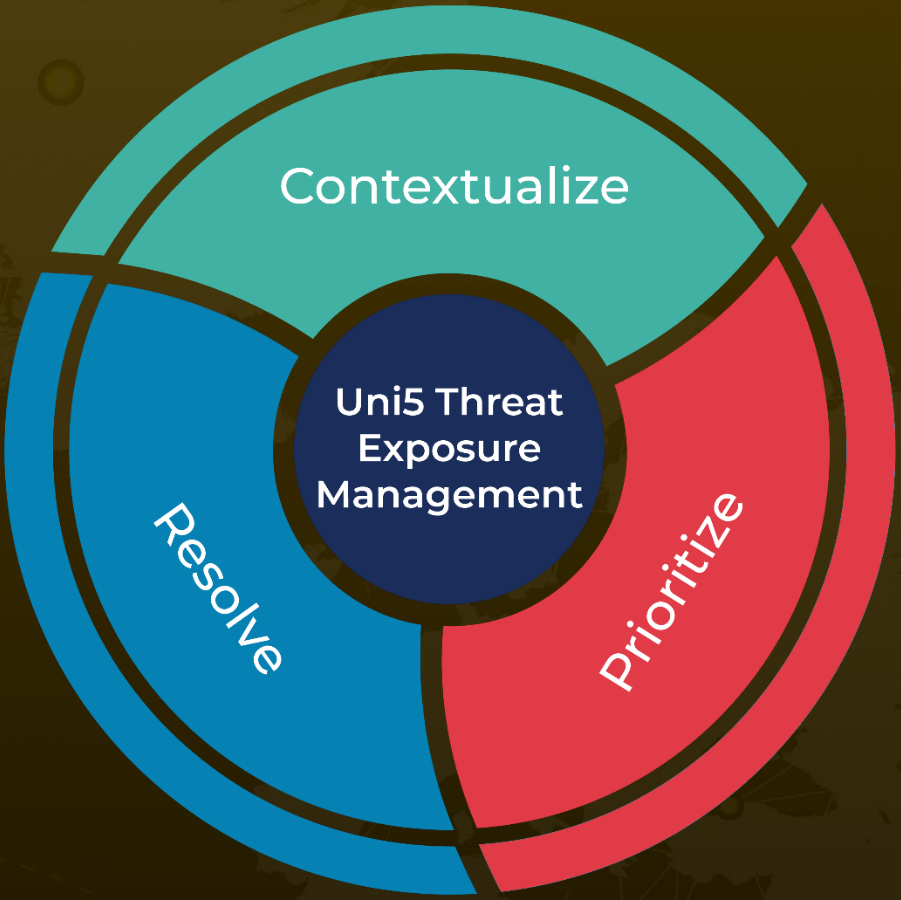
References

https://www.resecurity.com/blog/article/smishing-triad-targeted-usps-and-us-citizens-for-data-theft

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

September 8, 2023 • 6:00 AM

More at www.hivepro.com