Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

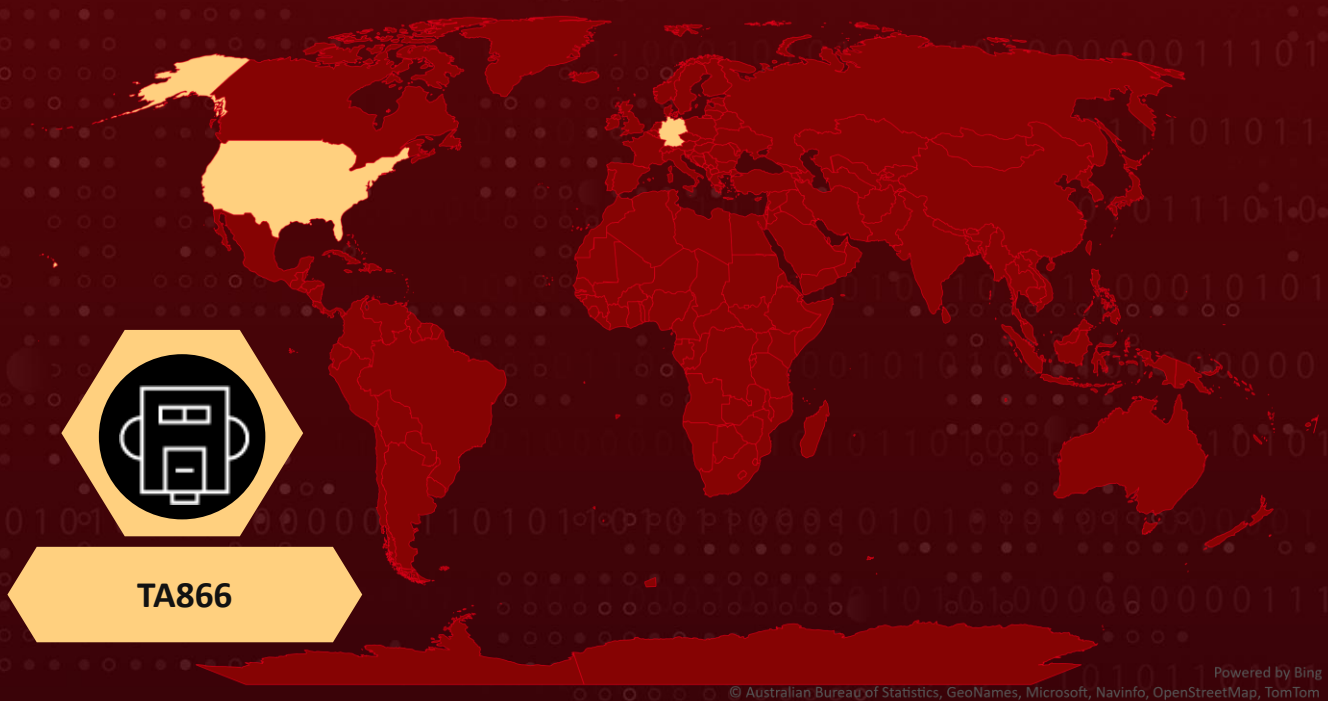
TA866 New Financially-Motivated Threat Actor Targeting US and Germany Organizations

Date of Publication	Admiralty code	TA Number
February 28, 2023	A1	TA2023107

Summary

First Appearance: October 2022
Actor Name: TA866
Target Region: United States and Germany
Target Sectors: All

Actor Map



Actor Details

#1

A new financially motivated threat actor named TA866 has been active since October 2022 and targets organizations in the United States and Germany. The attack chain starts with a malicious email containing an attachment or URL, leading to the installation of WasabiSeed and Screenshotter. TA866 is an organized actor that is able to perform attacks at scale based on their custom tools and ability to purchase tools and services from other vendors.

#2

The campaigns involve various types of malicious emails, targeting all industries, with email volumes and campaign frequency increasing drastically since November 2022. In January 2023, TA866 targeted tens of thousands of email messages over a thousand organizations in the US and Germany.

#3

The attack chain involves a multi-step process of downloading and running an MSI package containing WasabiSeed and Screenshotter, which take screenshots of the victim's screen and send them to the command and control server. The threat actor then manually examines the screenshots and places additional payloads for the WasabiSeed loop to download, such as AHK Bot and Rhadamanthys Stealer.

#4

The URLs used in the campaign lead to 404 TDS, a Traffic Distribution System that is likely a shared or sold tool due to its involvement in a variety of phishing and malware campaigns. The domains used in the campaign were previously registered, expired, and then re-sold to the TDS operator.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
TA866	Unknown	United States and Germany	All
	MOTIVE		
	Financial gain		

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

TA0002 Execution	TA0005 Defense Evasion	TA0011 Command and Control	TA0003 Persistence
TA0008 Lateral Movement	TA0004 Privilege Escalation	TA0009 Collection	TA0042 Resource Development
T1204.002 User Execution: Malicious File	T1210 Exploitation of Remote Services	T1036.007 Masquerading: Double File Extension	T1140 Deobfuscate/Decode Files or Information
T1566 Phishing	T1586 Compromise Accounts	T1027 Obfuscated Files or Information	T1113 Screen Capture
T1204.001 User Execution: Malicious Link	T1059.007 Command and Scripting Interpreter: JavaScript	T1546.016 Event Triggered Execution: Installer Packages	T1055.003 Process Injection: Thread Execution Hijacking
T1218.007 System Binary Proxy Execution: Msiexec			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	southfirstarea[.]com peak-pjv[.]com otameyshan[.]com thebtcrevolution[.]com annemarieotey[.]com expresswebstores[.]com styleselect[.]com mikefaw[.]com fgpprlaw[.]com duncan-technologies[.]net black-socks[.]org virtualmediaoffice[.]com samsontech[.]mobi footballmeta[.]com gfcitservice[.]net listfoo[.]org duinvest[.]info shiptrax24[.]com repossessionheadquarters[.]org bluecentury[.]org moosdies[.]top
SHA256	d934d109f5b446febf6aa6a675e9bcc41fade563e7998788824f56b3cc16d1ed 29e447a6121dd2b1d1221821bd6c4b0e20c437c62264844e8bcbb9d4be35f013 292344211976239c99d62be021af2f44840cd42dd4d70ad5097f4265b9d1ce01 02049ab62c530a25f145c0a5c48e3932fa7412a037036a96d7198cc57cef1f40 d0a4cd67f952498ad99d78bc081c98afbef92e5508daf723007533f000174a98 6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc 322dccd18b5564ea000117e90dafc1b4bc30d256fe93b7cfd0d1bdf9870e0da6 1f6de5072cc17065c284b21acf4d34b4506f86268395c807b8d4ab3d455b036b 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 3db3f919cad26ca155adf8c5d9cab3e358d51604b51b31b53d568e7bcf5301e2

TYPE	VALUE
URLs	hxxp[:]//109[.]107.173.72/%serial% hxxp[:]//79[.]137.198.60/1/ke.msi hxxp[:]//109[.]107.173.72/screenshot/%serial% hxxp[:]//89[.]208.105.255/%serial%-du2 hxxp[:]//89[.]208.105.255/%serial% hxxp[:]//89[.]208.105.255/download?path

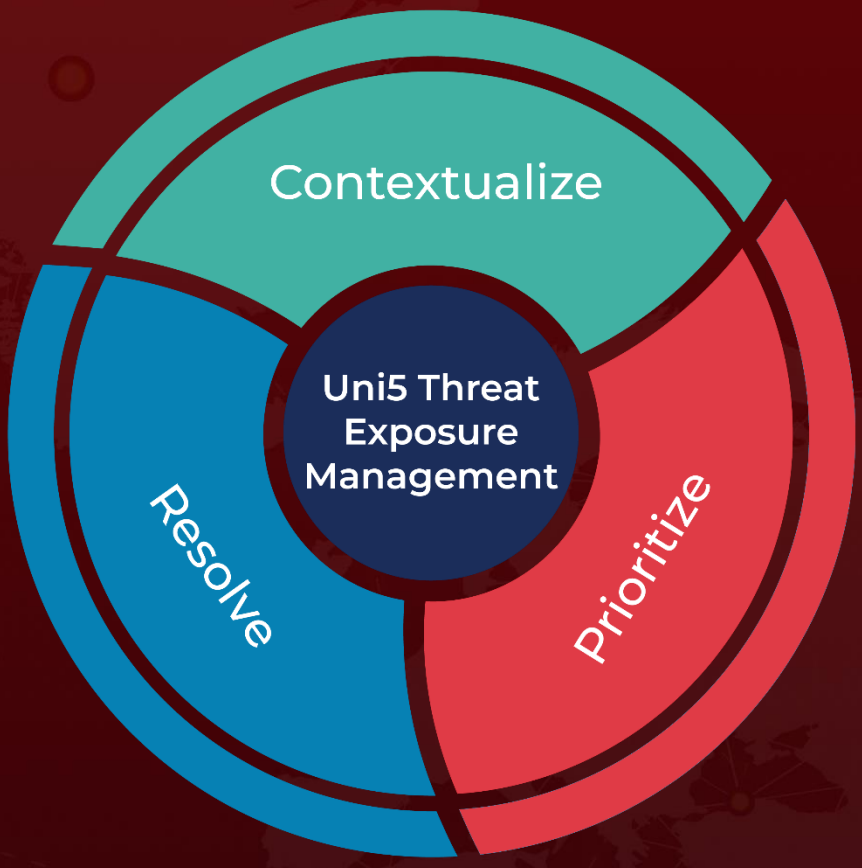
References

https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

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

February 28, 2023 . 3:00 AM

More at www.hivepro.com