Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

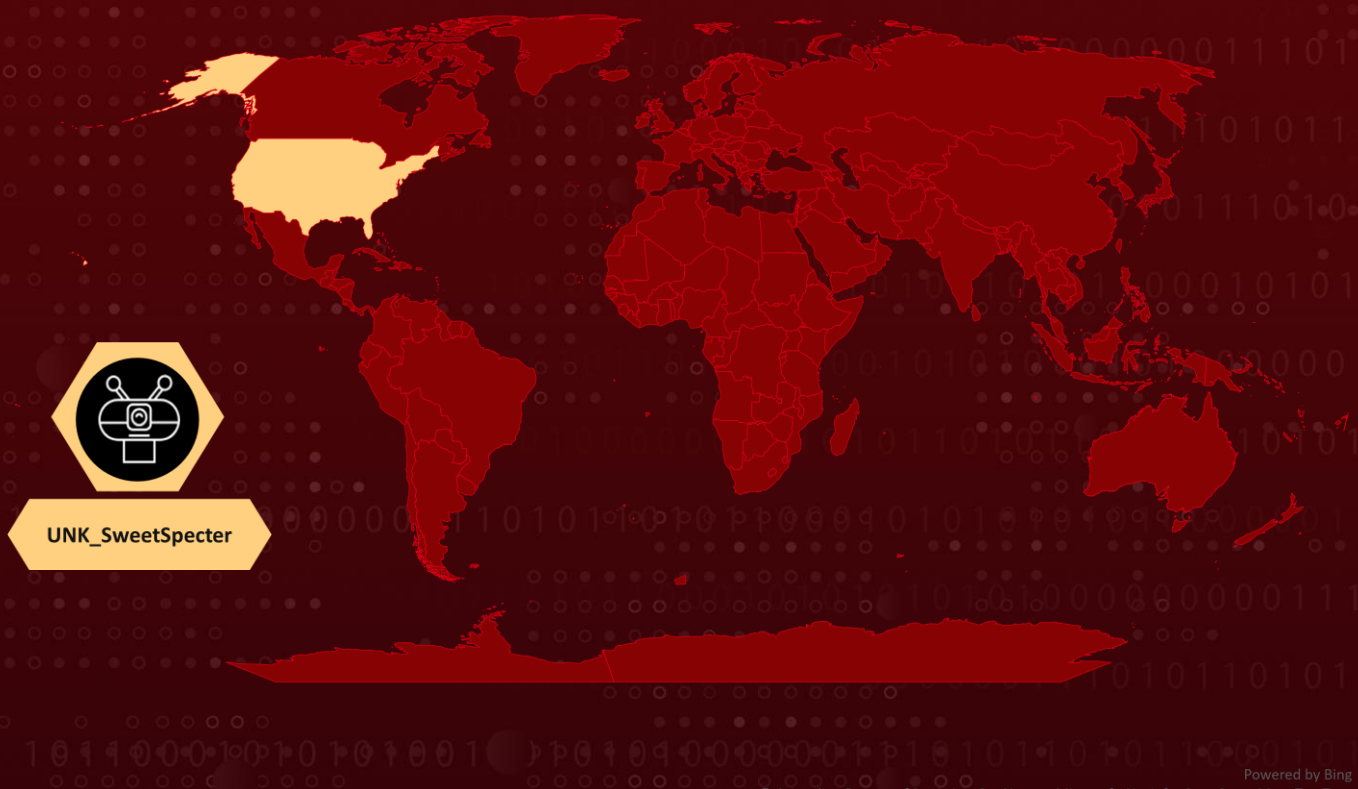
SugarGh0st RAT Infiltrates US AI Sector

Date of Publication	Admiralty Code	TA Number
May 17, 2024	A1	TA2024193

Summary

Attack Commenced: May 2024
Threat Actor: UNK_SweetSpecter
Malware: SugarGh0st RAT
Attack Region: USA
Targeted Industries: Technology, Government, Education
Attack: The May 2024 campaign, attributed to the cluster UNK_SweetSpecter, utilizes the SugarGh0st RAT, a remote access trojan customized from Gh0stRAT. Traditionally associated with Chinese-speaking threat actors, this variant has now been repurposed to target AI-related organizations.

Attack Regions



Attack Details

#1 The previously unknown threat actor, UNK_SweetSpecter, has launched the SugarGh0st RAT campaign, targeting U.S. organizations involved in artificial intelligence, spanning academia, the private sector, and government entities.

#2 SugarGh0st RAT is a customized variant of Gh0stRAT designed for remote access. In the May 2024 campaign, UNK_SweetSpecter utilized a free email account to distribute an AI-themed lure, enticing recipients to open an attached zip archive.

#3 Upon opening the zip file, a dropped LNK shortcut file executed a JavaScript dropper. The JavaScript dropper contained a decoy document, an ActiveX tool that was registered and then exploited for sideloading, and an encrypted binary, all encoded in base64.

#4 The infection sequence culminated in the deployment of SugarGh0st on the victim's system, establishing communication with a command-and-control (C2) server controlled by the attacker. UNK_SweetSpecter's objective probably was to acquire confidential information about generative artificial intelligence.

Recommendations

User Education and Awareness: Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.

Zero Trust Architecture: Adopting a zero-trust security model can help organizations mitigate the risk of insider threats and unauthorized access. Implementing strict access controls, multi-factor authentication (MFA), and continuous monitoring can prevent unauthorized users from compromising AI systems and data.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Network Segmentation and Micro-Segmentation: Segmenting the network architecture and implementing micro-segmentation can limit the lateral movement of attackers within the network. By compartmentalizing sensitive AI resources and data, organizations can minimize the impact of potential breaches.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1083 File and Directory Discovery	T1570 Lateral Tool Transfer
T1071.001 Web Protocols	T1566.001 Spearphishing Attachment	T1566 Phishing	T1490 Inhibit System Recovery
T1059 Command and Scripting Interpreter	T1082 System Information Discovery	T1574 Hijack Execution Flow	T1057 Process Discovery
T1105 Ingress Tool Transfer	T1204.002 Malicious File	T1204 User Execution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	da749785033087ca5d47ee65aef2818d4ed81ef217bfd4bc07be2d0bf105b1bf, 71f5ce42714289658200739ce0bbe439f6ef6fe77a5f6757b1cf21200fc59af7, fc779f02a40948568321d7f11b5432676e2be65f037acfed344b36cc3dac16fc, 4ef3a6703abc6b2b8e2cac3031c1e5b86fe8b377fde92737349ee52bd2604379, feae7b2b79c533a522343ac9e1aa7f8a2cdf38691fbd333537cb15dd2ee9397e
Domain	account[.]gommask[.]online
IPv4	43[.]242[.]203[.]115

References

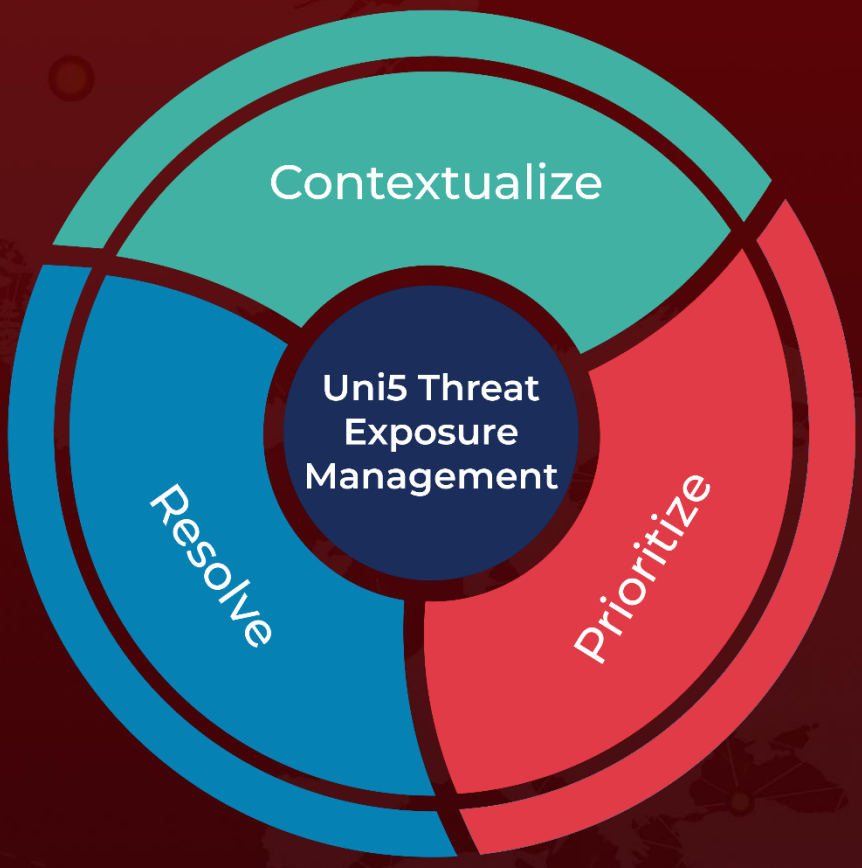
https://www.proofpoint.com/us/blog/threat-insight/security-brief-artificial-sweetener-sugargh0st-rat-used-target-american

https://www.hivepro.com/threat-advisory/sugargh0st-rat-a-customized-gh0st-variant-in-cyber-espionage/

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

May 17, 2024 • 6:00 AM

More at www.hivepro.com