Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

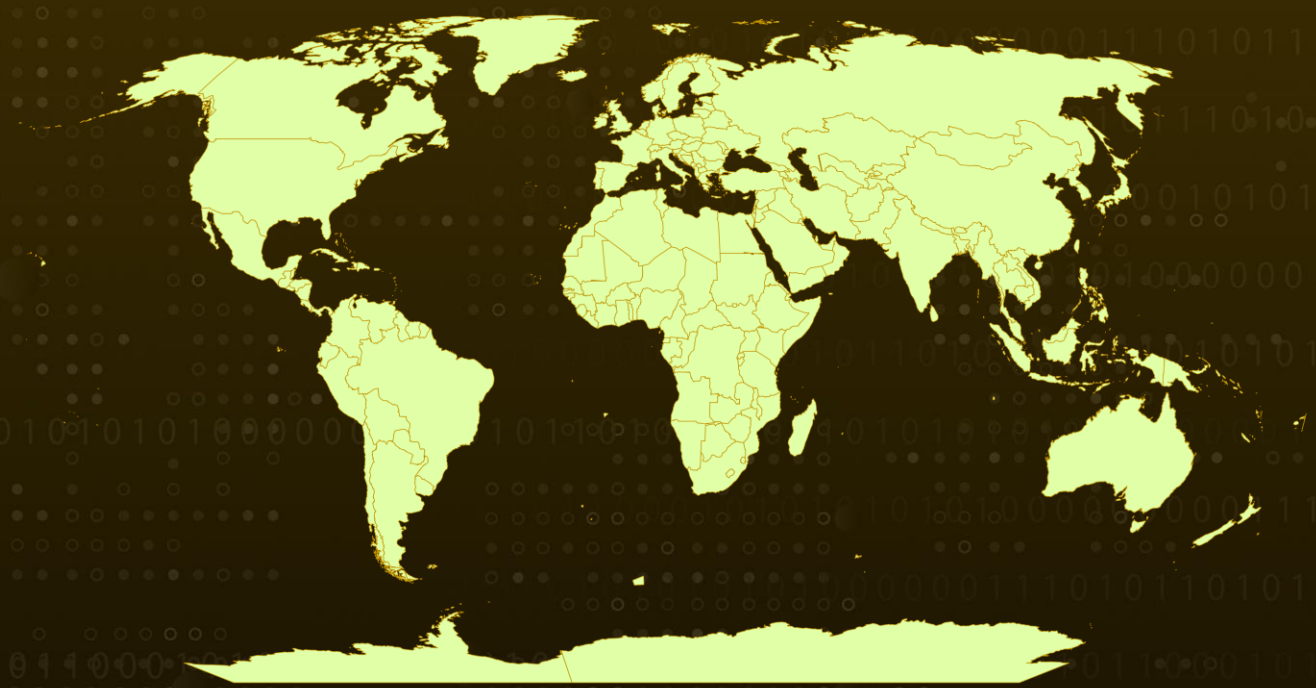
FBot's Arsenal against the SaaS Giants

Date of Publication	Admiralty Code	TA Number
January 12, 2024	A1	TA2024012

Summary

First Appearance: July 2022
Malware: FBot
Affected Platform: AWS, Office365, PayPal, Sendgrid, and Twilio.
Attack Region: Worldwide
Attack: FBot, a Python-based exploit tool, has systematically targeted critical infrastructures, spanning from web servers and cloud services to content management systems (CMS) and major Software as a Service (SaaS) platforms. Its primary objective is to infiltrate these services, acquiring credentials to subsequently monetize unauthorized access by selling it to other malicious entities.

Attack Regions



Attack Details

#1 A Python-based exploit tool, known as FBot, has systematically targeted a spectrum of critical infrastructures, including web servers, cloud services, content management systems (CMS), and prominent Software as a Service (SaaS) platforms such as Amazon Web Services (AWS), Microsoft 365, PayPal, Sendgrid, and Twilio.

#2 The overarching objective of the FBot utility is to compromise cloud-based, SaaS, and web services by acquiring credentials and subsequently capitalize on this unauthorized access by selling it to other malicious actors. Distinguished by its modest footprint in comparison to analogous tools, FBot suggests a potential origin in private development, accompanied by a more targeted approach to distribution.

#3 FBot is primarily designed to empower threat actors to hijack cloud, SaaS, and web services, with a secondary emphasis on acquiring accounts to orchestrate spamming attacks. The salient features of FBot include the orchestration of credential harvesting tailored for spamming assaults, tools for hijacking AWS accounts, and functionalities facilitating attacks on PayPal and diverse SaaS accounts.

#4 In addition to generating API keys for AWS and Sendgrid, FBot incorporates an array of capabilities, encompassing the generation of random IP addresses, execution of reverse IP scanning, and validation of PayPal accounts along with their associated email addresses. Notably, FBot does not delete the compromised account leveraged by the attacker for initial access. The tool also exhibits several attributes strategically aimed at targeting payment services and SaaS configurations.

Recommendations

Enhanced Credential Security: Regularly update and strengthen passwords for all accounts, especially those associated with cloud services, SaaS platforms, and web servers. Enable multi-factor authentication (MFA) to add a layer of security.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect any suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Vendor Security Assessment: If relying on third-party services like SaaS platforms, perform regular security assessments on their infrastructure and practices. Verify the security measures implemented by vendors, especially those handling sensitive data.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
T1526 Cloud Service Discovery	T1580 Cloud Infrastructure Discovery	T1098 Account Manipulation	T1136.003 Cloud Account
T1530 Data from Cloud Storage	T1212 Exploitation for Credential Access	T1098.001 Additional Cloud Credentials	T1496 Resource Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	1ad78e99918fd66ed43d42a93d2f910a2173b3c5, 2becd32162b2b0cb1afc541e33ace3a29dad96f1, 8ba3fca4deada6dbdc94b17a0c3c55a0b785331e

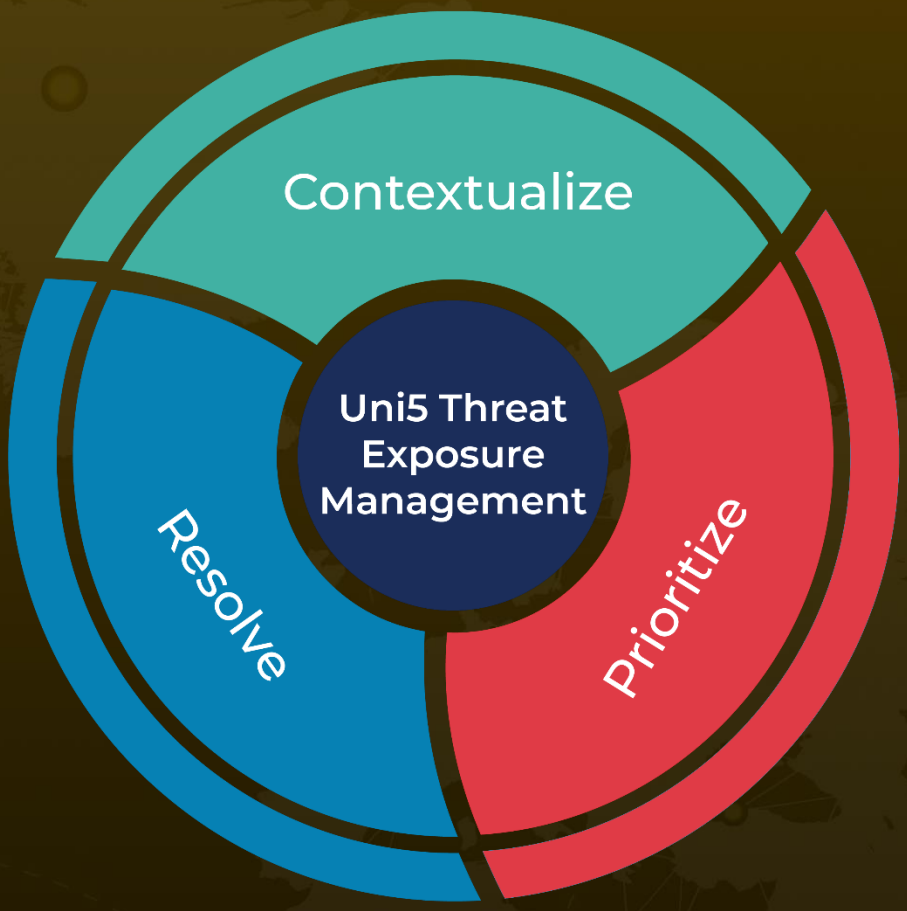
References

https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/

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

January 12, 2024 • 4:00 AM

More at www.hivepro.com