Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

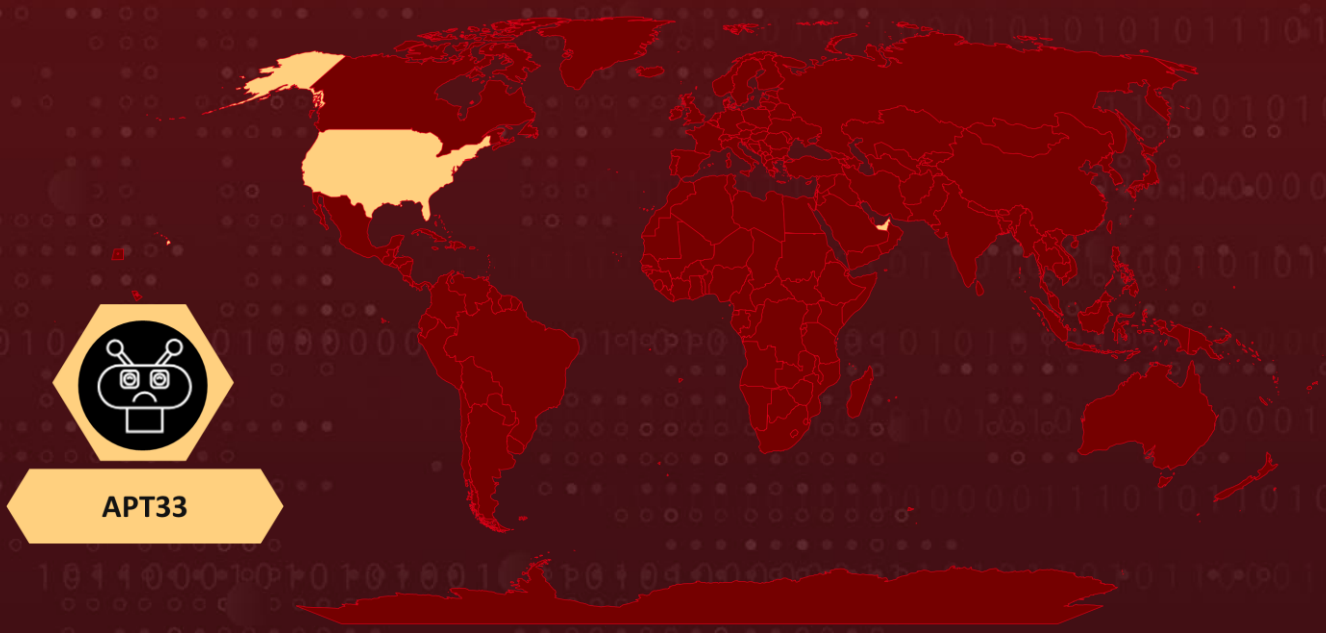
APT33 Unleashes Custom Tickler Malware Targeting the US and UAE

Date of Publication	Admiralty Code	TA Number
August 30, 2024	A1	TA2024335

Summary

Attack Discovered: July 2024
Attack Region: United States and the United Arab Emirates
Affected Industries: Government, Defense, Satellite, Oil and Gas Sectors
Malware: Tickler
Actor: APT33 (aka Refined Kitten, Elfin, Magnallium, Holmium, ATK 35, TA451, Cobalt Trinity, Peach Sandstorm, Yellow Orc, Curious Serpens)
Attack: The Iranian group APT33 has recently been observed using a new malware strain, dubbed Tickler, to backdoor the networks of various organizations in the United States and the United Arab Emirates. Tickler is a custom, multi-stage backdoor that enables attackers to maintain persistent access and deploy additional malware onto compromised systems, thereby extending their control over the targeted environments. In these attacks, APT33 leveraged Microsoft Azure infrastructure for command-and-control (C2) purposes.

Attack Regions



Attack Details

#1 The Iranian state-sponsored threat actor **APT33** aka Peach Sandstorm, developed a sophisticated, multi-stage backdoor known as Tickler, which was discovered in July 2024. This malware was deployed in targeted attacks against organizations in the United States and the United Arab Emirates, aligning with Peach Sandstorm's objectives of intelligence gathering and cyber espionage.

#2 Since February 2023, APT33 has conducted password spray attacks against thousands of organizations, targeting companies and individuals in the defense, satellite, and higher education sectors. This tactic involves attempting to authenticate numerous user accounts using a single password or a list of commonly used passwords, exploiting weak or reused credentials. APT33 employs these attacks to breach high-value targets, utilizing platforms like LinkedIn for reconnaissance. After successful authentication, the group uses commercial VPN services to obscure their activities and avoid detection.

#3 APT33 has notably used compromised educational accounts to establish their operational infrastructure. They either accessed existing Azure subscriptions associated with these accounts or created new ones to host their malicious infrastructure. The attacker-controlled Azure resources served as operational nodes, facilitating APT33's activities against high-value targets.

#4 In July 2024, two samples of the Tickler backdoor were identified, highlighting APT33’s ongoing efforts to infiltrate and sustain access to targeted systems through advanced techniques. The first Tickler sample was found gathering network information from the infected host and transmitting it to a command-and-control (C2) server via an HTTP POST request, helping the threat actor map the network environment.

#5 Second Tickler Sample was discovered as sold.dll, a Trojan dropper that retrieves additional malicious payloads from the C2 server. This includes a backdoor for remote access, a batch script for persistence, and legitimate files used for DLL Sideloading of the malware’s capabilities.

#6 Tickler is coded in 64-bit C/C++ and possesses capabilities to gather system information, list directories, execute commands, delete files, manage sleep intervals, and upload files from the C2 server to the compromised system. This comprehensive functionality underscores the sophisticated nature of APT33's operations and their continued commitment to maintaining stealthy, persistent access to targeted networks. Organizations should remain vigilant and proactively enhance their security measures to defend against such advanced threats.

Recommendations

Remain Vigilant: Avoid clicking on suspicious links or visiting untrusted websites, as they may harbor malicious content. Be cautious when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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.

Create Strong Passwords: Ensure your passwords are long (at least 12 characters), include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid common words and predictable patterns. Regularly updating your passwords (e.g., every 3-6 months) can help protect your accounts in case of a data breach.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0010 Exfiltration	**TA0011** Command and Control	**T1110** Brute Force	**T1110.003** Password Spraying
T1059 Command and Scripting Interpreter	**T1082** System Information Discovery	**T1070** Indicator Removal	**T1070.004** File Deletion
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1078** Valid Accounts	**T1078.004** Cloud Accounts

T1589 Gather Victim Identity Information	**T1598** Phishing for Information	**T1586** Compromise Accounts	**T1586.003** Cloud Accounts
T1608 Stage Capabilities	**T1566** Phishing	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading
T1016 System Network Configuration Discovery	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1585** Establish Accounts
T1585.003 Cloud Accounts	**T1083** File and Directory Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	subreviews[.]azurewebsites[.]net, satellite2[.]azurewebsites[.]net, nodetestservers[.]azurewebsites[.]net, satellitegardens[.]azurewebsites[.]net, softwareservicesupport[.]azurewebsites[.]net, getservicessuports[.]azurewebsites[.]net, getservicessupports[.]azurewebsites[.]net, getsupportsservices[.]azurewebsites[.]net, satellitespecialists[.]azurewebsites[.]net, satservicesdev[.]azurewebsites[.]net, servicessupports[.]azurewebsites[.]net, websupportprotection[.]azurewebsites[.]net, supportsoftwarecenter[.]azurewebsites[.]net, centersoftwaresupports[.]azurewebsites[.]net, softwareservicesupports[.]azurewebsites[.]net, getsdervicessupoortss[.]azurewebsites[.]net
SHA256	7eb2e9e8cd450fc353323fd2e8b84fbbdfe061a8441fd71750250752c577d198, ccb617cc7418a3b22179e00d21db26754666979b4c4f34c7fda8c0082d08cec4, 5df4269998ed79fbc997766303759768ce89ff1412550b35ff32e85db3c1f57b, fb70ff49411ce04951895977acfc06fa468e4aa504676dedeb40ba5cea76f37f, 711d3deccc22f5acfd3a41b8c8defb111db0f2b474febdc7f20a468f67db0350

References

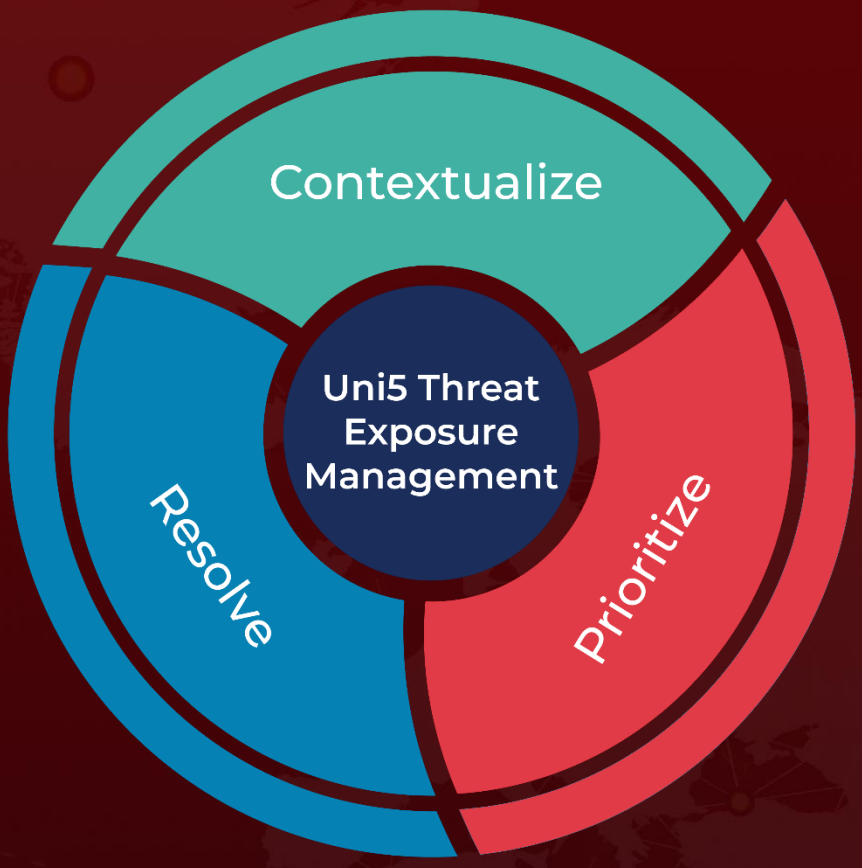
https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/

https://hivepro.com/threat-advisory/apt-33-uses-password-spray-campaigns-to-infiltrate-organizations/

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

August 30, 2024 • 6:50 AM

More at www.hivepro.com