Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

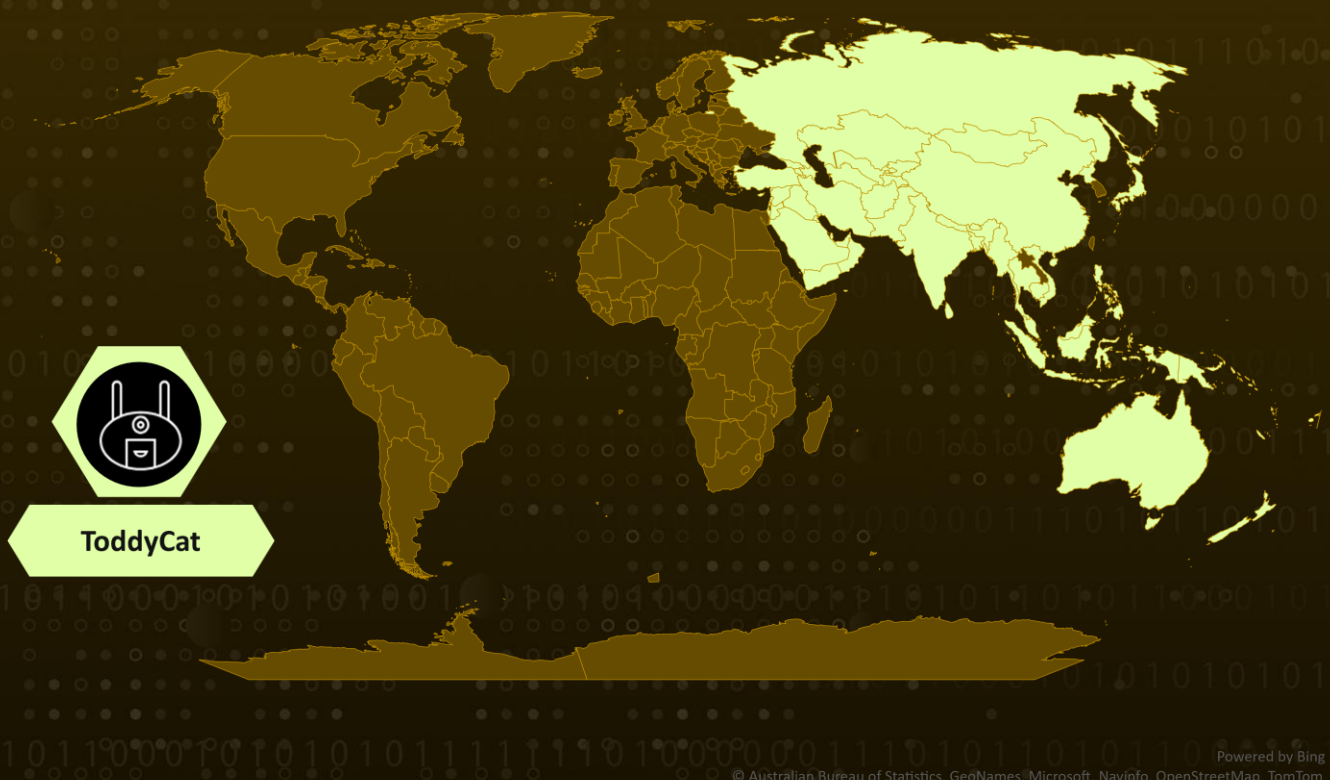
ToddyCat's Toolkit and Tactics Fueling Data Theft

Date of Publication	Admiralty Code	TA Number
April 23, 2024	A1	TA2024160

Summary

Threat Actor: ToddyCat
Attack Region: Asia-Pacific region
Targeted Industry: Government, Defense
Attack: ToddyCat, characterized by its sophisticated tactics, has surfaced with a focus on governmental entities in the Asia-Pacific region, particularly those linked to defense. Utilizing a range of tools, ToddyCat's objective is to extract sensitive data from compromised networks.

Attack Regions



Attack Details

#1 The threat actor identified as ToddyCat emerged on the radar in June 2022, demonstrating a sophisticated repertoire of tactics to infiltrate and maintain control over compromised networks. Primarily targeting governmental entities, particularly those with defense affiliations in the Asia-Pacific region, ToddyCat employs diverse tools to exfiltrate sensitive data.

#2 The latest arsenal of programs includes a combination of sophisticated data tunneling and reconnaissance software, strategically utilized following the acquisition of privileged user credentials within the compromised system.

#3 These tools facilitate covert operations, with attackers initiating a scheduled task to establish an SSH connection to a remote server. Additionally, they employ Ngrok and Krong for encryption and redirection techniques, aimed at obfuscating command-and-control (C2) traffic through designated ports on the target system.

#4 Further enhancing their capabilities, ToddyCat leverages the FRP client, a high-speed reverse proxy based on Golang, to obscure their presence, while employing Cuthead, a meticulously crafted .NET executable, to scour for documents matching specific criteria such as file extensions, filenames, or modification dates.

#5 Additionally, they utilize WAExp, a .NET application tailored to intercept and archive data associated with the WhatsApp web application, and TomBerBil, designed to extract cookies and credentials from popular web browsers like Google Chrome and Microsoft Edge. The adversaries actively employ evasion techniques to circumvent defensive measures, aiming to conceal their activities and maintain persistent access within the compromised systems.

Recommendations

Password Management: Avoid storing passwords in web browsers to prevent unauthorized access to sensitive information. Educate employees on secure password management practices and discourage password reuse across multiple services to minimize the risk of data exposure in case of a security breach.

Implement Application Whitelisting: Use application whitelisting to control the execution of unauthorized applications, thereby preventing the deployment of malicious payloads.

Enhance Firewall Restrictions: Strengthen the firewall by adding a denylist that includes resources and IP addresses linked to cloud services used for traffic tunneling. This proactive step aids in blocking potential entry points exploited by threat actors such as ToddyCat.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0010** Exfiltration
TA0011 Command and Control	**T1027** Obfuscated Files or Information	**T1105** Ingress Tool Transfer	**T1033** System Owner/User Discovery
T1041 Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1211** Exploitation for Defense Evasion
T1068 Exploitation for Privilege Escalation	**T1082** System Information Discovery	**T1555** Credentials from Password Stores	**T1090** Proxy
T1124 System Time Discovery	**T1204.002** Malicious File	**T1029** Scheduled Transfer	**T1007** System Service Discovery
T1562.004 Disable or Modify System Firewall	**T1564.001** Hidden Files and Directories	**T1053** Scheduled Task/Job	**T1055** Process Injection
T1059 Command and Scripting Interpreter	**T1021.004** SSH		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1d2b32910b500368ef0933cdc43fde0b, 5c2870f18e64a14a64abf9a56f5b6e6b, afea0827779025c92cab86f685d6429a, c7d8266c63f8aeca8d5f5bdcd433e72a, 750ef49afb88ddd52f6b0c500be9b717, 853a75364d76e9726474335bcd17e225, ba3ef3d0947031fb9ffbc2401ba82d79, 4a79a8b1f6978862ecfa71b55066aadd, 1f514121162865a9e664c919e71a6f62, 6f32d6cfaad3a956aacea4c5a5c4fbfe, 9dc7237ac63d552270c5ca27960168c3, 34985fae5fa8e9ebaa872de8d0105005
URL	hxxp[://]www.netportal.or[.]kr/common/css/main.js, hxxp[://]www.netportal.or[.]kr/common/css/ham.js, hxxp[://]23.106.122[.]5/hamcore.se2, hxxps[://]etracking.nso.go[.]th/UserFiles/File/111/tasklist.exe, hxxps[://]etracking.nso.go[.]th/UserFiles/File/111/hamcore.se2
Domain	Ha[.]bbmouseme[.]com
IPv4	103[.]27[.]202[.]85, 118[.]193[.]40[.]42

References

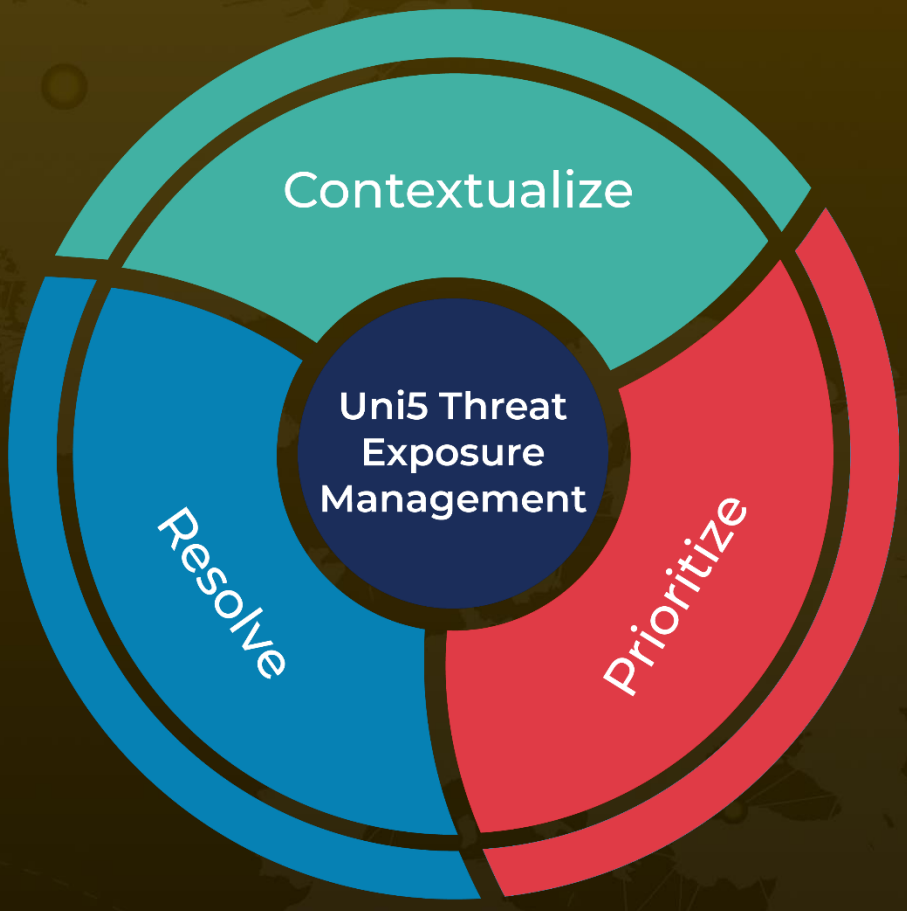
https://securelist.com/toddycat-traffic-tunneling-data-extraction-tools/112443/

https://www.hivepro.com/threat-advisory/toddycat-exploits-unknown-vulnerability-in-microsoft-exchange-servers-to-targets-entities-in-europe-and-asia/

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

April 23, 2024 • 7:00 AM

More at www.hivepro.com