Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

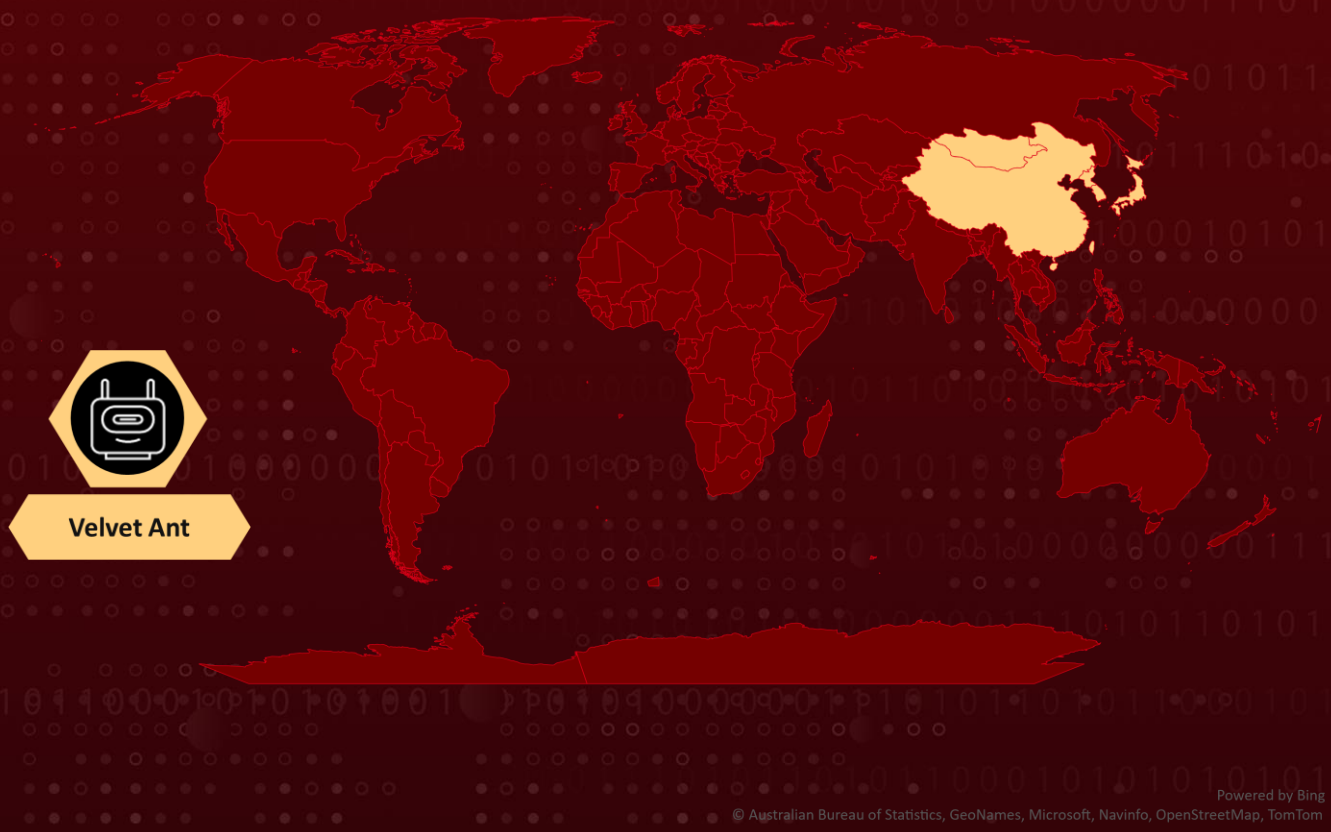
F5 BIG-IP Exploited in Three-Year Espionage Campaign by Velvet Ant

Date of Publication	Admiralty Code	TA Number
June 18, 2024	A1	TA2024233

Summary

Attack Commenced: 2023
Threat Actor: Velvet Ant
Malware: PlugX (aka Korplug)
Affected Product: F5 BIG-IP
Attack Region: East Asia
Attack: A highly sophisticated, state-sponsored cyber threat group associated with China, known as Velvet Ant, exploited F5 BIG-IP appliances to establish and sustain a persistent connection to internal networks for nearly three years, facilitating extensive data exfiltration.

Attack Regions



Attack Details

#1 A group of suspected state-sponsored threat actors linked to China, known as Velvet Ant, exploited F5 BIG-IP appliances to establish a persistent connection to an internal network and exfiltrate data from an unidentified organization in East Asia over approximately three years.

#2 Velvet Ant, a highly sophisticated threat actor, aimed to maintain long-term access to the target network for espionage purposes. One method of persistence involved utilizing a legacy F5 BIG-IP appliance exposed to the internet, which the adversaries exploited as an internal Command and Control (C&C) server.

#3 Upon discovery and remediation of one point of access, the threat actors quickly adapted and shifted to another, showcasing their agility and capability in evading detection. Velvet Ant employed multiple entry points across the victim's network infrastructure, demonstrating an in-depth understanding of the target's environment.

#4 They disabled endpoint security software before installing PlugX, a known backdoor, and utilized open-source tools like Impacket for lateral movement within the network. The attack chains prominently featured PlugX (also known as Korplug), a modular remote access trojan (RAT) widely used by espionage groups with ties to Chinese interests.

#5 PlugX is notorious for leveraging DLL side-loading to compromise devices. This campaign is particularly notable for the extraordinary efforts the threat actors undertook to maintain persistence in the target environment.

Recommendations

Control Traffic Over Management Ports: Meticulously monitor and regulate traffic over common management ports, including SMB (port 445), RPC (port 135), WinRM (ports 5985-5986), RDP (port 3389), and SSH (port 22). Restrict access to these ports exclusively to hosts with explicit authorization.

Apply Advanced Security Features: Apply Protected Process Light (PPL) to LSASS and activate Windows Credential Guard to enhance credential security and prevent unauthorized access to sensitive information.

Phase out and Upgrade Legacy Systems: Prioritize the phasing out and upgrading of legacy systems, as they are primary targets for cyberattacks due to their weaker defenses.

Deploy Endpoint Detection and Response (EDR): Implement EDR systems to enable continuous monitoring and interception of malicious actions. Ensure EDR sensors are equipped with anti-tampering features and remain operational and up-to-date.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1133 External Remote Services	T1047 Windows Management Instrumentation
T1059 Command and Scripting Interpreter	T1059.008 Network Device CLI	T1569 System Services	T1569.002 Service Execution
T1037.004 RC Scripts	T1133 External Remote Services	T1078.002 Domain Accounts	T1078.003 Local Accounts
T1574 Hijack Execution Flow	T1574.001 DLL Search Order Hijacking	T1562.004 Disable or Modify System Firewall	T1055 Process Injection
T1070.006 Timestomp	T1003.001 LSASS Memory	T1087.002 Domain Account	T1083 File and Directory Discovery

T1135 Network Share Discovery	**T1018** Remote System Discovery	**T1082** System Information Discovery	**T1016** System Network Configuration Discovery
T1021.001 Remote Desktop Protocol	**T1021.004** SSH	**T1570** Lateral Tool Transfer	**T1039** Data from Network Shared Drive
T1572 Protocol Tunneling	**T1090.001** Internal Proxy	**T1048** Exfiltration Over Alternative Protocol	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	4a0f328e7672ee7ba83f265d48a6077a0c9068d4, d80427c922db5fcd8cf490a028915485ff833666, 291bcceef6e03a9f4f0c524f1dd3a4b77d870cd8, f07272762b322cea1d8cc0845718371f1af0bd4a, 37d3665d3b803eeddfad245c0e96172b9c3e8a29, 2c5d678948938de4d10095db35390c064305413c, 6003f8042d375ec5c6d56a1d6e363e2d2cc9eb67, 1fc7b986e55f116d92e77e3b2bee86b720ffa155, 0b400eb4451c3148fa48bc72cb8a84fdcf4461d3, 49d2e3dfabd21ed4a11c6fca6236ced7b17fa97e, e6bd682c47f1a9d564f45a54427100b42e19d2e9, fc06519154e3a4b28fe16606dec05ec02dd2f647, ca7331e0c8dda90054eb941a2fdd0cc943a04fc4, 61a382b2139512f8c816ceae93ec823c88bd6eed, 8e722b2c6b114b69bd71c37759dc3410a32b7594, 35e0cbec56e6ad052c3cf53a052b254490995453, 7dc223a47fa35011d9e5ed8ef0bbeaf7bd08500f, 0667f44b8dc20d0d1b8f1a5c2fe2f8011204664b, 86a219232410f236665c51854425fbe5e37b07b3, 3faf065a9987ade102f20dd1ac6b857c7c191b97, 2b3b897dd7ef6a54bc038a9afc9d79d5989b6c5f, 44e2b73f6f5ec010681cb1fa5681ca0903f0a080, ddb59cf25b40273ef0f394c6f164923b6872d7cf, 1f2e03650afbbd10b9cff21116b7b8d9b192cee3, 3a5ea30f0ff6928a26c4e67352d0adf44dd978da, ef22dfed358bf35f702af4a14f7a646375123e05, 553674972e59e7b37a63d19556152b13bf785d71, 0e7c4f374009ff3e264d299dfc1c279bff5b6b4b, baaa29799bdbb6c1f3fc70e25c0aee4b033fefc8

TYPE	VALUE
IPv4	202[.]61[.]136[.]158, 103[.]138[.]13[.]31

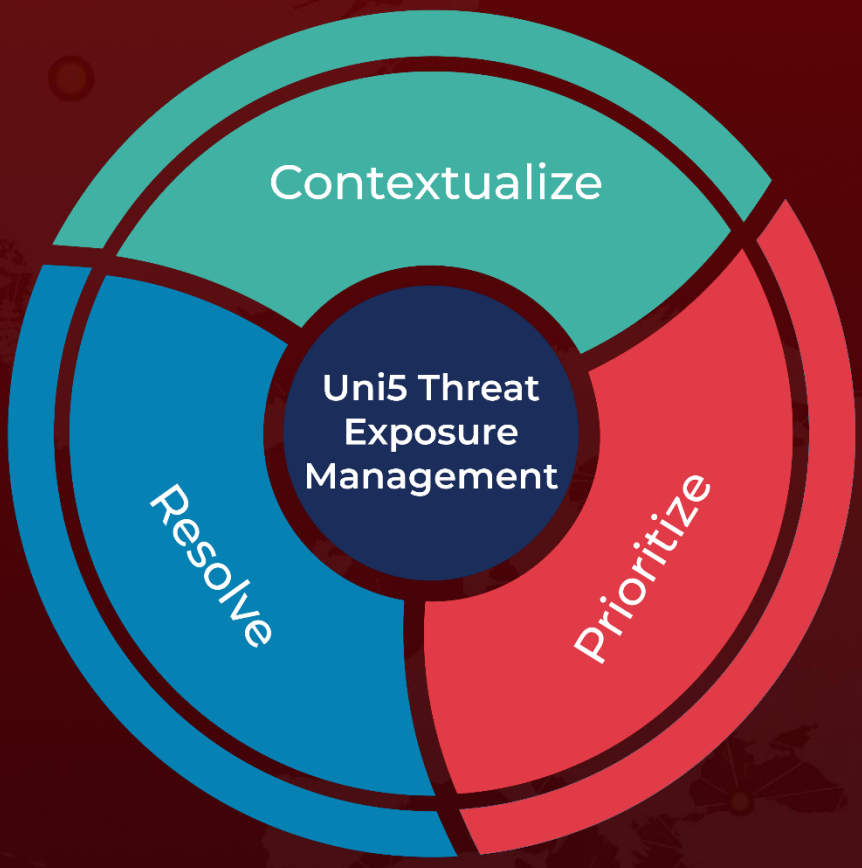
References

https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/

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

June 18, 2024 • 6:30 AM

More at www.hivepro.com