Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

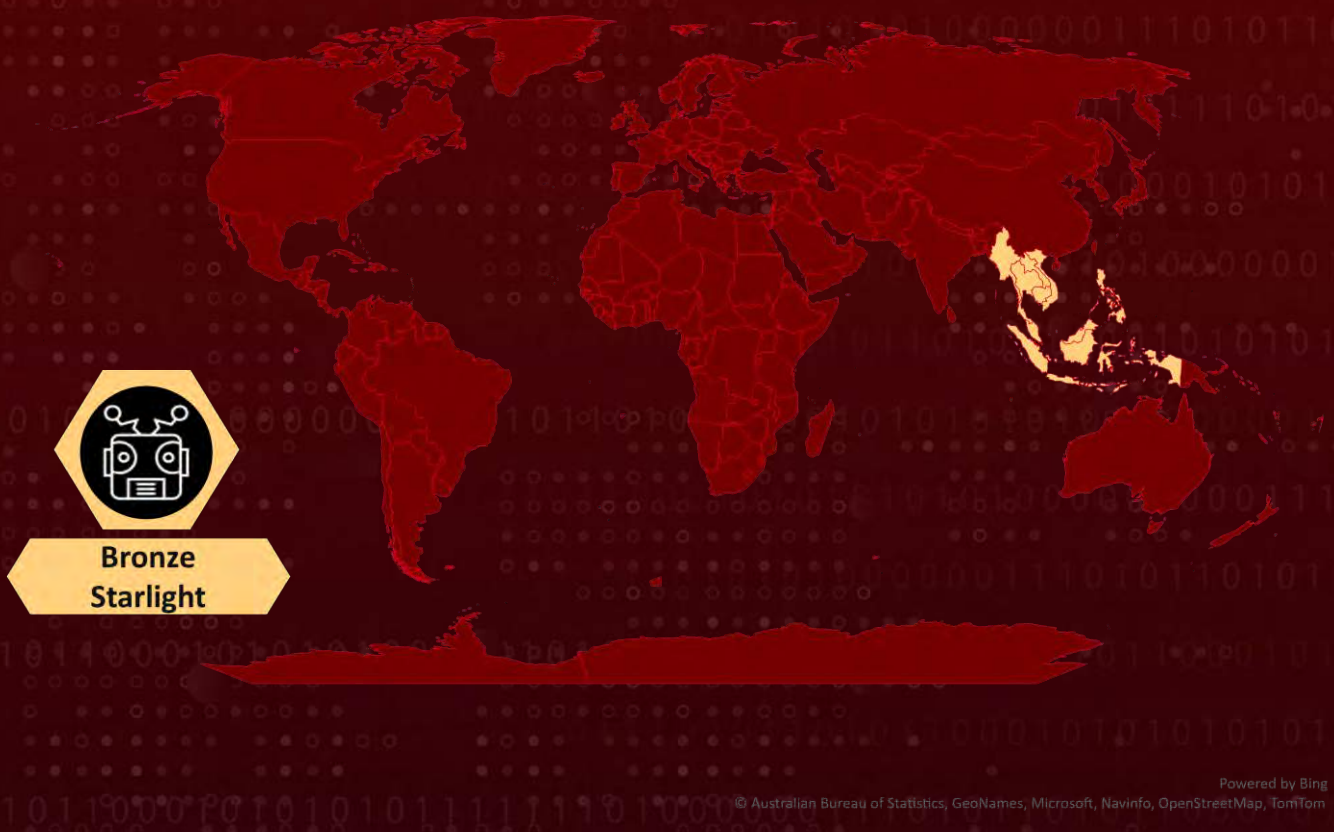
Decoding Bronze Starlight's Strategy in the Gambling Sector

Date of Publication	Admiralty Code	TA Number
August 18, 2023	A2	TA2023337

Summary

Attack Began: August 2023
Malware: HUI Loader variants
Threat Actor: Bronze Starlight (aka DEV-0401, Cinnamon Tempest, SLIME34, Emperor Dragonfly)
Attack Region: Southeast Asia
Targeted Industry: Gambling sector
Affected Platform: Windows, Linux, macOS
Attack: A cyberattack campaign stemming from China is currently focusing its efforts on the Southeast Asian gambling industry, with the objective of deploying Cobalt Strike beacons on compromised systems.

Attack Regions



Attack Details

#1 An alleged instance of Chinese malware and infrastructure is suspected to be associated with operations originating in China and targeted toward the gambling sector in Southeast Asia. The evidence indicates the potential involvement of the China-aligned BRONZE STARLIGHT group. The threat actors exploit vulnerabilities in Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan executables, utilizing DLL hijacking to deploy Cobalt Strike beacons.

#2 These attacks are characterized by their utilization of customized installers for chat programs, which serve to download a .NET malware loader. This loader is configured to retrieve a second-stage ZIP archive from Alibaba buckets. Inside this ZIP file, an executable vulnerable to DLL search order hijacking coexists alongside a malicious DLL. The execution of the loader is facilitated by the side-loading technique, capitalizing on executables susceptible to DLL hijacking. This approach orchestrates the deployment of a payload enclosed within an encrypted file.

#3 Remarkably, the loaders exhibit the behavior of terminating their execution if they are run on machines situated in countries such as the United States, Germany, France, Russia, India, Canada, or the United Kingdom. The primary objective appears to be espionage, rather than financial gains. The DLL files that are side-loaded are variants of the HUI Loader. This custom malware loader has found widespread use among China-based groups, including APT10, Bronze Starlight, and TA410.

Recommendations

- Implement robust encryption for data at rest and in transit, enforce multi-factor authentication and strict access controls to limit system access to authorized personnel, and bolster security through advanced endpoint protection to thwart unauthorized access and malware threats.
- Consider segmenting networks to isolate critical systems, reducing the attack surface and containing the impact of potential compromises on less critical assets.
- Utilize behavior-based analysis tools capable of detecting unusual activities on endpoints. Implement application whitelisting or control mechanisms to permit the execution of authorized applications exclusively on systems.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**T1053** Scheduled Task/Job
T1129 Shared Modules	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1027** Obfuscated Files or Information
T1027.002 Software Packing	**T1036** Masquerading	**T1070.006** Timestomp	**T1140** Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	**T1562.001** Disable or Modify Tools	**T1010** Application Window Discovery	**T1012** Query Registry
T1057 Process Discovery	**T1083** File and Directory Discovery	**T1560** Archive Collected Data	**T1071** Application Layer Protocol
T1095 Non-Application Layer Protocol	**T1573** Encrypted Channel	**T1018** Remote System Discovery	**T1082** System Information Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	09f82b963129bbcc6d784308f0d39d8c6b09b293, 1a11aa4bd3f2317993cfe6d652fbe5ab652db151, 32b545353f4e968dc140c14bc436ce2a91aacd82, 4b79016d11910e2a59b18275c786682e423be4b4, 559b4409ff3611adaae1bf03cbadaa747432521b, 57bbc5fcfd97d25edb9cce7e3dc9180ee0df7111, 6e9592920cdce90a7c03155ef8b113911c20bb3a, 76bf5ab6676a1e01727a069cc00f228f0558f842, 88c353e12bd23437681c79f31310177fd476a846, 957e313abaf540398af47af367a267202a900007

TYPE	VALUE
URLs	hxxps[://]agenfile.oss-ap-southeast-1[.]aliyuncs.com/agent_source/temp1/cefhelper.zip, hxxps[://]agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp2/agent_bak.zip, hxxps[://]agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp3/adobe_helper.zip, hxxps[://]codewavehub.oss-ap-southeast-1.aliyuncs[.]com/org/com/file/CodeVerse.zip
Domains	tencentchat[.]net, kaspresksy[.]com, www.100helpchat[.]com, miscrosofts[.]com, microupdate[.]xyz, microsofts[.]org, microsofts[.]net, microsofts[.]info, microsofts[.]com, microsoftlab[.]top, live100heip[.]com, duckducklive[.]top, 100helpchat[.]com
IPv4	8.218.31[.]103, 47.242.72[.]118

References

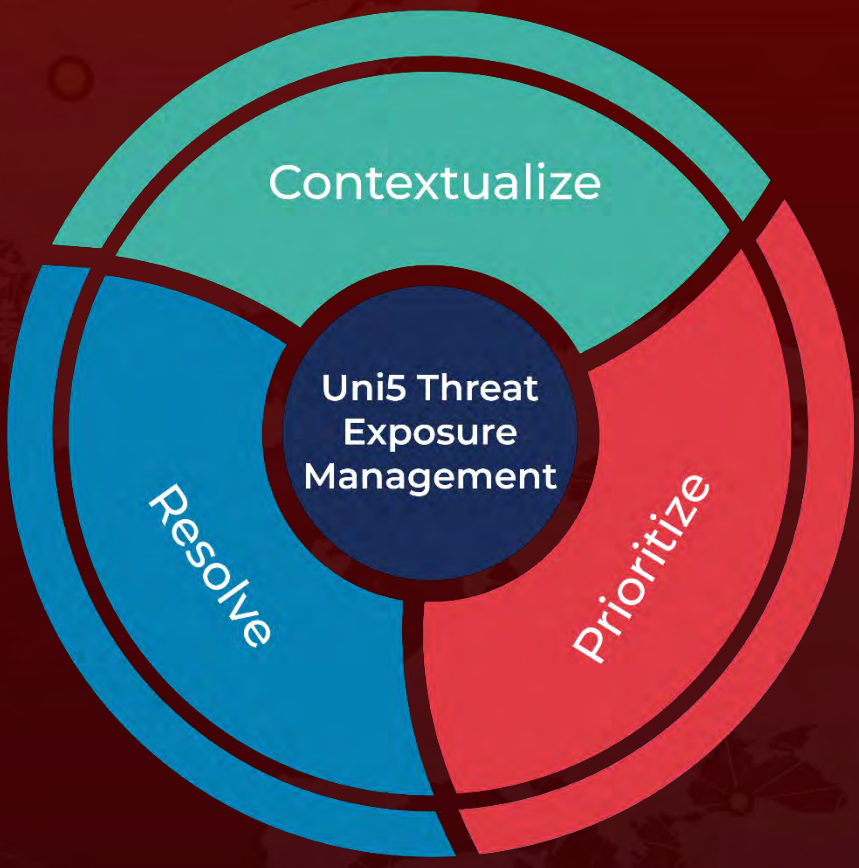
https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/

https://www.hivepro.com/bronze-starlight-uses-loader-malware-to-deploy-ransomware/

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 18, 2023 • 6:30 AM

More at www.hivepro.com