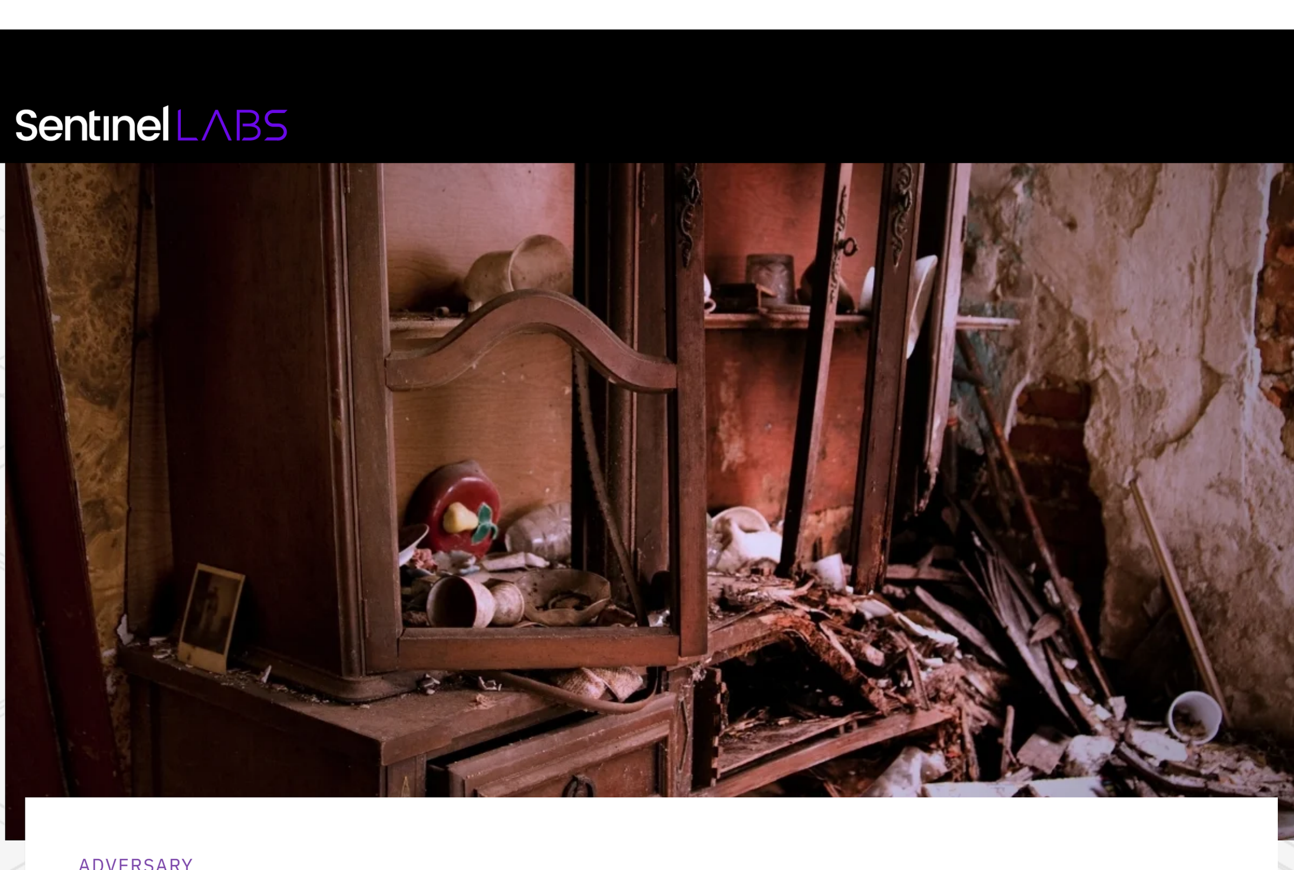
SentinelLABS



ADVERSARY

Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector

ALEKSANDAR MILENKOSKI / AUGUST 17, 2023

By Aleksandar Milenkoski and Tom Hegel

Executive Summary

- SentinelLabs has identified suspected-Chinese malware and infrastructure potentially involved in China-associated operations directed at the gambling sector within Southeast Asia.
- The threat actors drop Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan executables vulnerable to DLL hijacking to deploy Cobalt Strike beacons.
- We've observed related malware using the signature of a likely stolen code signing certificate issued to PMG PTE LTD, a Singapore-based vendor of Ivacy VPN services.
- Indicators point to the China-aligned BRONZE STARLIGHT group; however, the exact grouping remains unclear due to the interconnected relationships among various Chinese APT groups.

Overview

Thriving after China's crackdown on its Macao-based gambling industry, the Southeast Asian gambling sector has become a focal point for the country's interests in the region, particularly data collection for monitoring and countering related activities in China.

We observed malware and infrastructure likely related to China-aligned activities targeting this sector. The malware and infrastructure we analyze are related to indicators observed in Operation ChattyGoblin and are likely part of the same activity cluster. Operation ChattyGoblin is ESET's name for a series of attacks by China-nexus actors targeting Southeast Asian gambling companies with trojanized Comm100 and LiveHelp100 chat applications.

The targeting, used malware, and C2 infrastructure specifics point to past activities that third parties have linked to the China-aligned BRONZE STARLIGHT group (also known as DEV-0401 or SLIME34). This is a suspected Chinese 'ransomware' group whose main goal appears to be espionage rather than financial gain, using ransomware as means for distraction or misattribution. Team T5 has also reported on BRONZE STARLIGHT's politically-motivated involvement in targeting the Southeast Asian gambling industry.

Despite the indicators observed, accurate clustering remains challenging. The Chinese APT ecosystem is plagued by extensive sharing of malware and infrastructure management processes between groups, making high confidence clustering difficult based on current visibility. Our analysis has led us to historical artifacts that represent points of convergence between BRONZE STARLIGHT and other China-based actors, which showcases the complexity of a Chinese threat ecosystem composed of closely affiliated groups.

Background

ESET reported that a ChattyGoblin-related attack in March 2023 targeted the support agents of a gambling company in the Philippines. In the attack, a trojanized LiveHelp100 application downloaded a .NET malware loader named `agentupdate_plugins.exe`. The final payload was a Cobalt Strike beacon using the `duckducklive[.]top` domain for C2 purposes. The hash of this malware loader was not disclosed.

We subsequently identified malware loaders that we assess are closely related to those observed as part of Operation ChattyGoblin and are likely part of the same activity cluster – a .NET executable also named `agentupdate_plugins.exe` and its variant `AdventureQuest.exe`.

This association is based on naming conventions, code, and functional overlaps with the sample described in ESET's report. Although we cannot conclusively determine whether the `agentupdate_plugins.exe` we analyzed is the same as that reported by ESET, we note that one of its VirusTotal submissions is dated March 2023 and originates from the Philippines. This aligns with the geolocation of the target and the timeline of the ChattyGoblin-related attack involving `agentupdate_plugins.exe`.

The Malware Loaders

`agentupdate_plugins.exe` and `AdventureQuest.exe` deploy .NET executables based on the SharpUnhooker tool, which download second-stage data from Alibaba buckets hosted at `agenfile.oss-ap-southeast-1.aliyuncs[.]com` and `codewavehub.oss-ap-southeast-1.aliyuncs[.]com`. The second-stage data is stored in password-protected zip archives.

The zip archives downloaded by `agentupdate_plugins.exe` and `AdventureQuest.exe` contain sideloading capabilities. Each of the archives we were able to retrieve consists of a legitimate executable vulnerable to DLL search order hijacking, a malicious DLL that gets sideloaded by the executable when started, and an encrypted data file named agent.data.

The executables are components of the software products Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan. The malicious DLLs masquerade as their legitimate counterparts: They export functions with the same names, such that specific functions, when invoked by the legitimate executables, decrypt and execute code embedded in the data files. The data files we could retrieve implement Cobalt Strike beacons.

Zip archive	Archive content	Final payload
adobe_helper.zip (agentupdate_plugins.exe)	Adobe CEF Helper.exe libcef.dll agent.data (not available)	/
cefhelper.zip (AdventureQuest.exe)	identity_helper.exe msedge_elf.dll agent.data	Cobalt Strike C2: www.100helpchat[.]com
Agent_bak.zip (AdventureQuest.exe)	mfeann.exe LockDown.dll agent.data	Cobalt Strike C2: live100heip[.]com

The `100helpchat[.]com` and `live100heip[.]com` C2 domains follow the naming convention of the LiveHelp100 trojanized application used in operation ChattyGoblin, possibly to make malicious network activity look like legitimate LiveHelp100 activity.

`agentupdate_plugins.exe` and `AdventureQuest.exe` implement geofencing based on the ifconfig.co IP-based geolocation service. The loaders are meant to stop their execution if they are run on a machine located in the United States, Germany, France, Russia, India, Canada, or the United Kingdom. This may indicate that the threat actors have no interest in intrusions in these countries for this campaign. Due to errors in implementation, the geofencing fails to work as intended.

Stolen Ivacy VPN Certificate

`AdventureQuest.exe` is signed using a certificate issued to the Ivacy VPN vendor PMG PTE LTD:

- Thumbprint: 62E990CC0A26D58E1A150617357010EE53186707
- Serial number: 0E3E037C57A5447295669A3DB1A28B8A.

Ivacy has been present on the market since 2007 and attracts users with low-price offerings.

It is likely that at some point the PMG PTE LTD singing key has been stolen – a familiar technique of known Chinese threat actors to enable malware signing. VPN providers are critical targets, since they enable threat actors to potentially gain access to sensitive user data and communications.

At the time of writing, we have not observed any public statements by PMG PTE LTD clarifying the circumstances that have led to the use of their signing keys for signing malware. The DigiCert Certificate Authority has revoked the compromised certificate after a public discussion on the issue.

HUI Loader

The malicious DLLs `libcef.dll`, `msedge_elf.dll`, and `LockDown.dll` distributed by `agentupdate_plugins.exe` and `AdventureQuest.exe` are HUI Loader variants. HUI Loader is a custom malware loader shared between several China-nexus groups. The loader is executed through sideloading by legitimate executables vulnerable to DLL hijacking and stages a payload stored in an encrypted file. HUI Loader variants may differ in implemented payload staging and execution techniques as well as additional functionalities, such as establishing persistence and disabling security features.

`libcef.dll`, `msedge_elf.dll`, and `LockDown.dll` closely resemble HUI Loader variants observed in a string of cyberespionage and ransomware operations that third parties have linked to APT10, TA410, and BRONZE STARLIGHT.

Threat actor	Description
BRONZE STARLIGHT *Aliases*: DEV-0401, SLIME34	A China-based ransomware operator active since 2021. The group is known for deploying a variety of ransomware families, such as LockFile, AtomSilo, NightSky, LockBit 2.0, and Pandora, and shares tooling with APT10. BRONZE STARLIGHT's main goal is suspected to be espionage rather than financial gain, using ransomware as means for distraction or misattribution.
APT10 *Aliases:* BRONZE RIVERSIDE, MenuPass	A China-nexus cyberespionage group active since at least 2009. The group focuses on targeting entities considered strategically important by the Chinese state.
TA410	A China-nexus cyberespionage group loosely linked to APT10, tracked as a distinct entity. The group is mostly known for targeting the US utilities sector and Middle Eastern governments.

APT10 and TA410 Operations

The `cef_string_map_key` function of `libcef.dll` downloaded by `agentupdate_plugins.exe` references the `C:\Users\hellokety.ini` file.

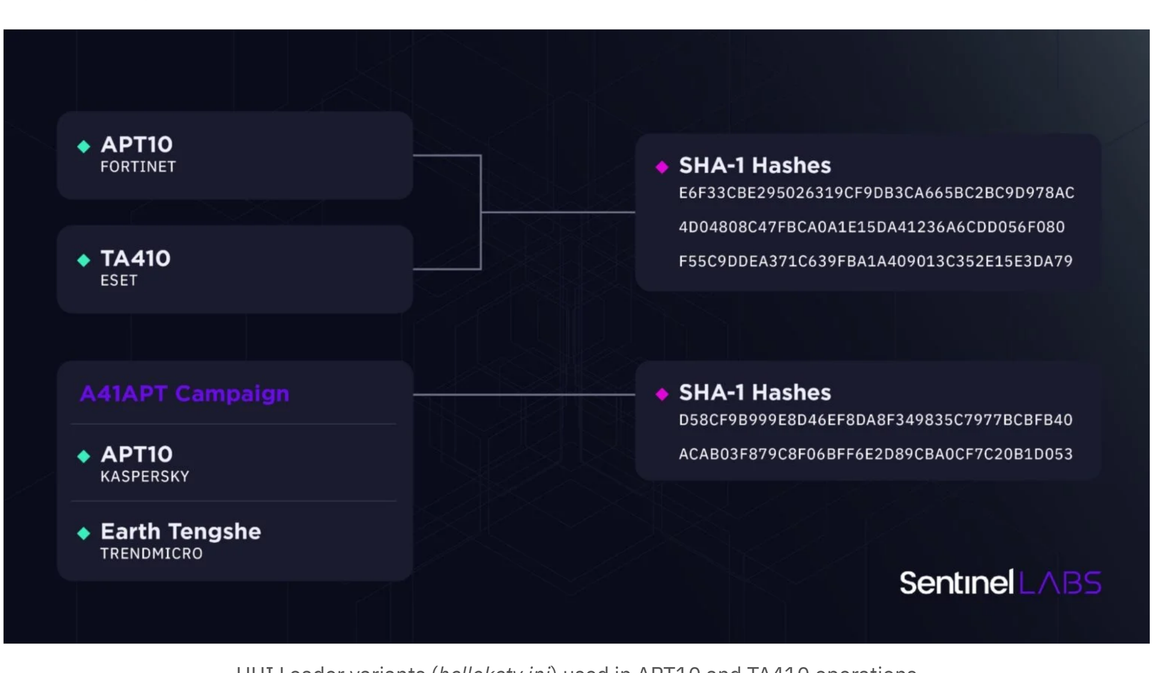
```
void __noreturn cef_string_map_key()
{
  FILE *v0;
  int v1;
  char *v2;
  char v3[1024];

  v0 = fopen("c:\\users\\hellokety.ini", "a");
  v1 = 0;
  v2 = getenv("EINFO_INDENT");
  [...]
  fprintf(v0, "%s", v3);
  ExitProcess(0);
}
```

The *cef_string_map_key* function

HUI Loader variants with this exact artifact have been reported as part of several cyberespionage operations:

- enSilo (now Fortinet) has disclosed cyberespionage activities in Southeast Asia observed in April 2019 and attributed them with medium confidence to APT10.
- Researchers from Macnica, Secureworks, and Kaspersky have presented on A41APT campaign activity conducted throughout 2021. A41APT is a long-running cyberespionage campaign targeting Japanese companies and their overseas branches. Kaspersky has attributed earlier A41APT activity (from March 2019 to the end of December 2020) with high confidence to APT10. TrendMicro has attributed A41APT activity over 2020 and 2021 to a group they track as Earth Tengshe, noting that Earth Tengshe is related to APT10 with some differences in employed TTPs.
- ESET has presented on TA410 activities, noting the `hellokety.ini` artifact in this context. ESET also notes the possibility of misattribution the April 2019 activities reported by Fortinet to APT10 instead of TA410.



HUI Loader variants (*hellokety.ini*) used in APT10 and TA410 operations

BRONZE STARLIGHT Operations

Since around 2021, HUI Loader variants have been deployed in operations involving the ransomware families LockFile (Symantec, 2021; NSFOCUS, 2021), AtomSilo (Sophos, 2021), NightSky (Microsoft, 2021), LockBit 2.0 (SentinelLabs, 2022), and Pandora (TrendMicro, 2022). Some of these operations have been attributed to BRONZE STARLIGHT by the organizations disclosing them and all of them collectively by Secureworks. All of these ransomware families have been noted by Microsoft as being part of the BRONZE STARLIGHT arsenal in time intervals aligning with those of the previously mentioned operations.

C2 Infrastructure

The Cobalt Strike C2 GET and POST URIs associated with the Operation ChattyGoblin domain `duckducklive[.]top` contain `/functionalStatus` and `/rest/2/meetings`, respectively. Their uncommon full forms closely resemble those observed by Secureworks in AtomSilo, Night Sky, and Pandora operations they attribute to BRONZE STARLIGHT. The researchers reported that, as of June 2022, they had not seen this Cobalt Strike configuration associated with other ransomware families. The threat actors have likely adapted a public Cobalt Strike malleable C2 profile available in a Github repository of the user `xx0hcd`.

Cobalt Strike C2 POST URI	Relation
/rest/2/meetingsmCRW64qPFqLKw7X56lR41fx	Operation ChattyGoblin
/rest/2/meetingsVDcrCtBuGm8dime2C5zQ3EHbRE156AkpMu6W	AtomSilo
/rest/2/meetingsQpmhJveuV1ljApIzpTAL	Night Sky
/rest/2/meetingsKdEs85OkdgIPwcqbjS7uzVZKBIZNHeO4r5sKe	Pandora

The C2 GET and POST URIs associated with the `www.100helpchat[.]com` and `live100heip[.]com` domains we observed contain `/owa` followed by character strings. The format of these strings resembles those in the URIs associated with `duckducklive[.]top` and also those reported in past BRONZE STARLIGHT activities. It is likely that the threat actors have adapted another open source Cobalt Strike malleable C2 profile, which is also available in a Github repository of the user `xx0hcd`.

Domain	Cobalt Strike C2 URIs
live100heip[.]com	GET: /owa/Z7bziD-BDtV9U1aLS9AhW4jyN1NEOelTEi POST: /owa/LAC9kgQyM1HD3NSIwi–mx9sHB3vcmjJJm
www.100helpchat[.]com	GET: /owa/aLgnP5aHtit33SA2p2MenNuBmYy POST: /owa/XF0O-PjSCEslnDo51T0K4TOY

The Cobalt Strike profiles associated with the `duckducklive[.]top`, `www.100helpchat[.]com`, and `live100heip[.]com` domains share a C2 port number (`8443`) and a watermark (`391144938`). The earliest record of `duckducklive[.]top` becoming active is dated 24 Feb 2023. The earliest records of `live100heip[.]com` and `100helpchat[.]com` becoming active are dated 24 Feb 2023 (overlapping with that of `duckducklive[.]top`) and 28 Feb 2023, respectively.

The three domains are each hidden behind CloudFlare, who were quick in remediation after we reported the service abuse. In this case, however, the actors revealed their true-hosting locations due to an OPSEC mistake in their initial deployment of the domain's SSL certificates on their Alibaba Cloud hosting servers at `8.218.31[.]103`, `47.242.72[.]118`, and `47.242.159[.]242`.

Certificates use on Alibaba IPs

While the analysis of the Cobalt Strike profiles provides links to previous BRONZE STARLIGHT activities, an assessment of the specific group attribution based on current intelligence should be treated with caution. It is noteworthy that Chinese cyber espionage threat actors are progressively refining their operational tactics in manners that obfuscate clear attribution through publicly available intelligence sources alone.

To illustrate this concept, consider the scenario where a broader array of domains imitating various brands may be interconnected, such as those publicly documented involving the BRONZE STARLIGHT, TA410, and APT10 threat actors. Examples include `microsofts[.]net`, `microupdate[.]xyz`, `microsofts[.]info`, `microsofts[.]org`, `miscrosofts[.]com`, `microsofts[.]com`, `kaspresksy[.]com`, t`encentchat[.]net`, and `microsoftlab[.]top`.

Conclusion

China-nexus threat actors have consistently shared malware, infrastructure, and operational tactics in the past, and continue to do so. The activities this post discusses illustrate the intricate nature of the Chinese threat landscape.

Better understanding of this landscape is essential for keeping up with its dynamics and improving defense strategies. Achieving this necessitates consistent collaborative and information sharing efforts. SentinelLabs remains dedicated to this mission and continues to closely monitor related threats.

Indicators of Compromise

Files (SHA1)

Indicator	Description
09f82b963129bbcc6d784308f0d39d8c6b09b293	agentupdate_plugins.exe
1a11aa4bd3f2317993cfe6d652fbe5ab652db151	LockDown.dll
32b545353f4e968dc140c14bc436ce2a91aacd82	mfeann.exe
4b79016d11910e2a59b18275c786682e423be4b4	Adobe CEF Helper.exe
559b4409ff3611adaae1bf03cbadaa747432521b	identity_helper.exe
57bbc5fcfd97d25edb9cce7e3dc9180ee0df7111	agentdata.dat
6e9592920cdce90a7c03155ef8b113911c20bb3a	AdventureQuest.exe
76bf5ab6676a1e01727a069cc00f228f0558f842	agentdata.dat
88c353e12bd23437681c79f31310177fd476a846	libcef.dll
957e313abaf540398af47af367a267202a900007	msedge_elf.dll

Second-Stage Data URLs

https[://]agenfile.oss-ap-southeast-1[.]aliyuncs.com/agent_source/temp1/cefhelper.zip	AdventureQuest.exe
https[://]agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp2/agent_bak.zip	AdventureQuest.exe
https[://]agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp3/adobe_helper.zip	agentupdate_plugins.exe
https[://]codewavehub.oss-ap-southeast-1.aliyuncs[.]com/org/com/file/CodeVerse.zip	AdventureQuest.exe

C2 Domains

www.100helpchat[.]com	Cobalt Strike
live100heip[.]com	Cobalt Strike

C2 IP Addresses

8.218.31[.]103	Cobalt Strike
47.242.72[.]118	Cobalt Strike

ADVERSARY

ALEKSANDAR MILENKOSKI

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs, with expertise in reverse engineering, malware research, and threat actor analysis. Aleksandar has a PhD in system security and is the author of numerous research papers, book chapters, blog posts, and conference talks. His research has won awards from SPEC, the Bavarian Foundation for Science, and the University of Würzburg.