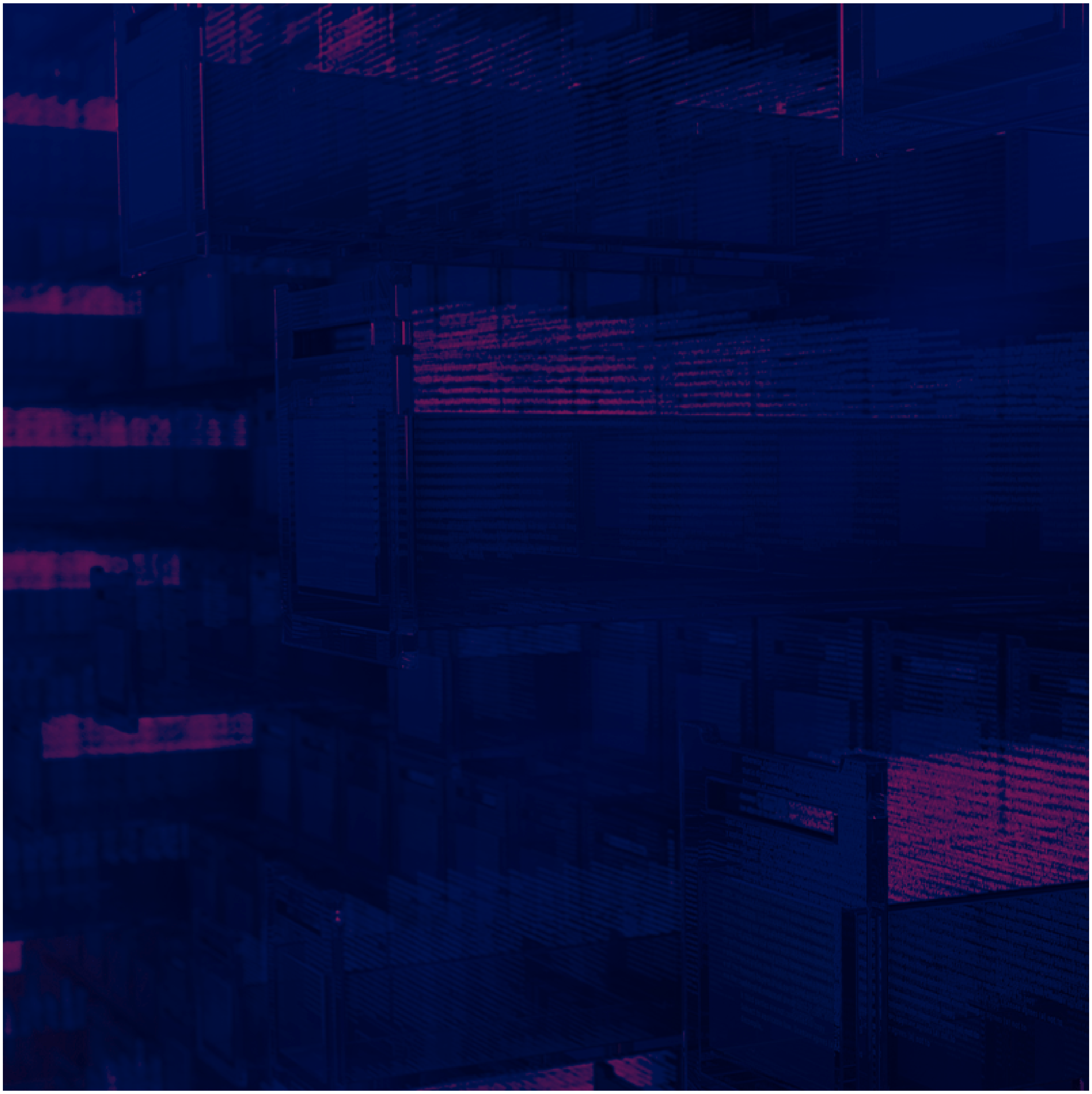
BRONZE STARLIGHT Ransomware Operations Use HUI Loader

secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

Counter Threat Unit Research Team



Thursday, June 23, 2022 *By: Counter Threat Unit Research Team*

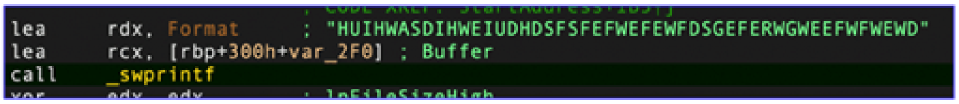
Summary

Since at least 2015, threat actors have used HUI Loader to load remote access trojans (RATs) on compromised hosts. Secureworks® Counter Threat Unit™ (CTU) researchers link two HUI Loader activity clusters exclusively to China-based threat groups. The BRONZE RIVERSIDE threat group is likely responsible for one cluster, which focuses on stealing intellectual property from Japanese organizations. The other cluster involves deployment of LockFile, AtomSilo, Rook, Night Sky, and Pandora post-intrusion ransomware. CTU™ researchers attribute this activity to the Chinese BRONZE STARLIGHT threat group.

The victimology, short lifespan of each ransomware family, and access to malware used by government-sponsored threat groups suggest that BRONZE STARLIGHT's main motivation may be intellectual property theft or cyberespionage rather than financial gain. The ransomware could distract incident responders from identifying the threat actors' true intent and reduce the likelihood of attributing the malicious activity to a government-sponsored Chinese threat group.

HUI Loader overview

HUI Loader is a custom DLL loader whose name is derived from a string in the loader (see Figure 1). The malware is loaded by legitimate programs that are vulnerable to DLL search order hijacking. HUI Loader decrypts and loads a third file containing an encrypted payload that is also deployed to the compromised host. CTU researchers have observed HUI Loader loading RATs such as SodaMaster, PlugX, Cobalt Strike, and QuasarRAT.



```
lea     rdx, Format      ; "HUIHWASDIHWEIUDHDSFSFEFWEFEWFDSGEFERWGWEEFWFWEWD"
lea     rcx, [rbp+300h+var_2F0] ; Buffer
call    _swprintf
```

Figure 1. String that starts with 'HUI' in HUI Loader samples. (Source: Secureworks)

Since early 2021, CTU researchers observed threat actors deploying HUI Loader in a cluster of activity associated with intellectual property theft. This A41APT campaign primarily targets Japanese organizations and uses HUI Loader to load the SodaMaster RAT. The victimology and tactics, techniques, and procedures (TTPs) in this campaign align with BRONZE RIVERSIDE activity. In mid-2021, CTU researchers began tracking a second cluster of activity that uses HUI Loader to load Cobalt Strike Beacon and deploy ransomware. CTU researchers attribute this second cluster of activity to the BRONZE STARLIGHT threat group. Figure 2 compares the clusters linked to HUI Loader.

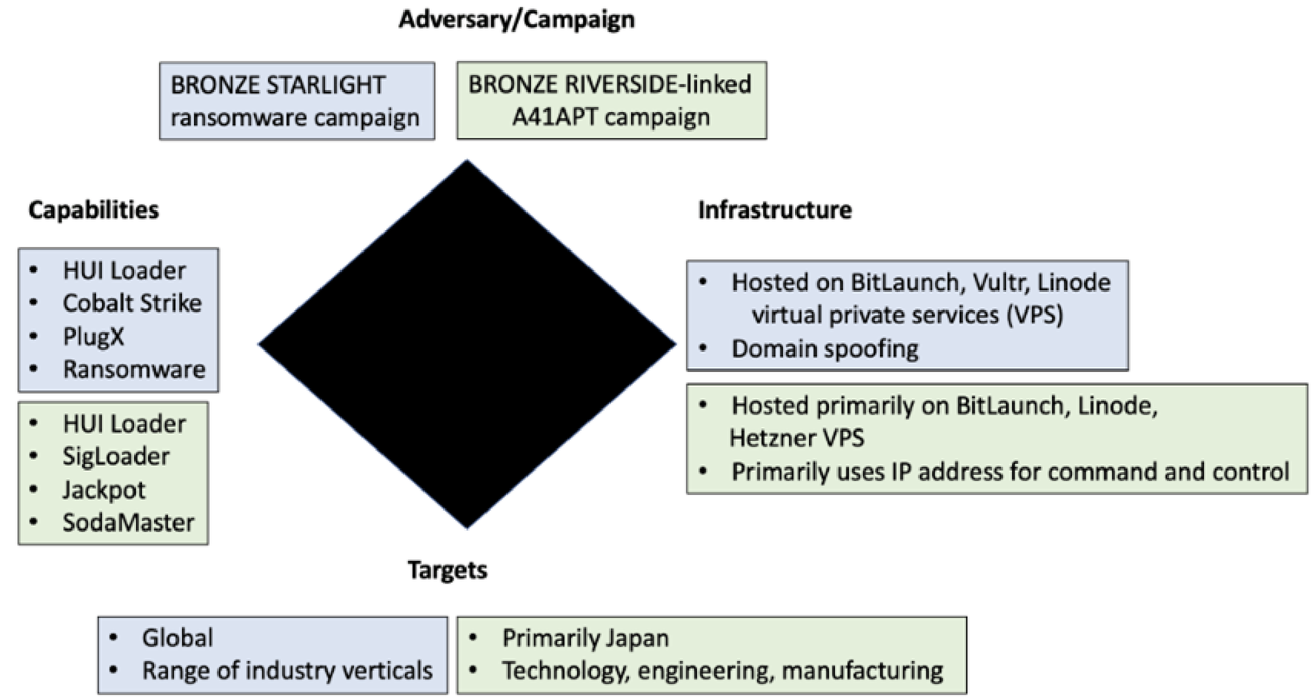

Adversary/Campaign
BRONZE STARLIGHT ransomware campaign
BRONZE RIVERSIDE-linked A41APT campaign
Capabilities
HUI Loader
Cobalt Strike
PlugX
Ransomware
HUI Loader
SigLoader
Jackpot
SodaMaster
Infrastructure
Hosted on BitLaunch, Vultr, Linode virtual private services (VPS)
Domain spoofing
Hosted primarily on BitLaunch, Linode, Hetzner VPS
Primarily uses IP address for command and control
Targets
Global
Range of industry verticals
Primarily Japan
Technology, engineering, manufacturing

Figure 2. Diamond model comparing HUI Loader clusters. (Source: Secureworks)

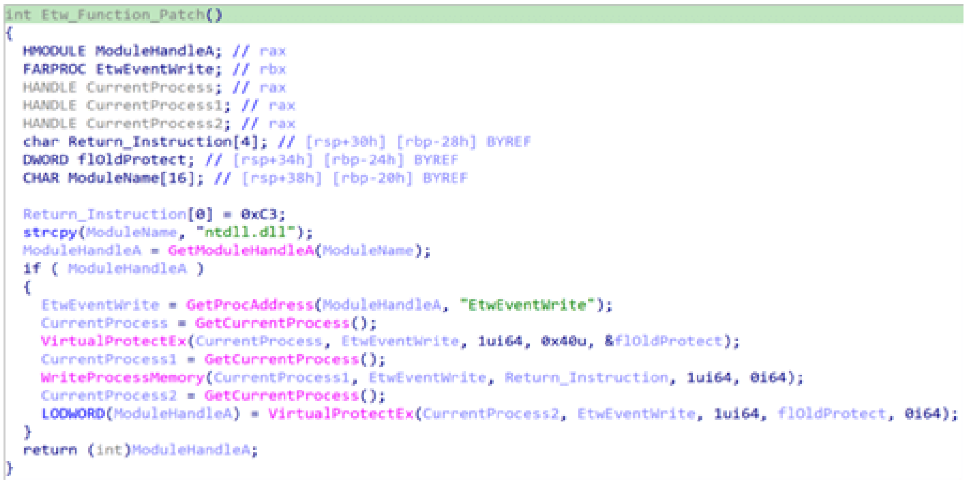
HUI Loader-linked ransomware activity

HUI Loader samples that load Cobalt Strike Beacon have been linked to LockFile, AtomSilo, Rook, Night Sky, and Pandora ransomware activity (see Table 1).

HUI Loader filename	Payload filename	Cobalt Strike C2 domain	Ransomware
active_desktop_render.dll	desktop.ini	sc . microsofts . net	LockFile
Lockdown.dll	mfc.ini	update . ajaxrenew . com	AtomSilo
Lockdown.dll	sets5s.ini	Unknown (payload file unavailable for analysis)	Rook
Lockdown.dll	Lockdown.conf	api . sophosantivirus . ga sub . sophosantivirus . ga	Night Sky
libcef.dll	utils.dll	api . sophosantivirus . ga	Night Sky
LockDown.dll	vm.cfg	peek . openssl-digicert . xyz	Pandora

Table 1. HUI Loader and Cobalt Strike Beacon samples linked to ransomware activity.

In March 2022, CTU researchers analyzed an updated version of HUI Loader that uses the RC4 cipher to decrypt the payload. The malware sample also attempts to circumvent host-based detection and protection measures by disabling Windows Event Tracing for Windows (ETW), disabling Antimalware Scan Interface (AMSI) functions, and hooking Windows API calls (see Figure 3). CTU researchers identified code overlap between the updated HUI Loader samples and the Pandora ransomware.



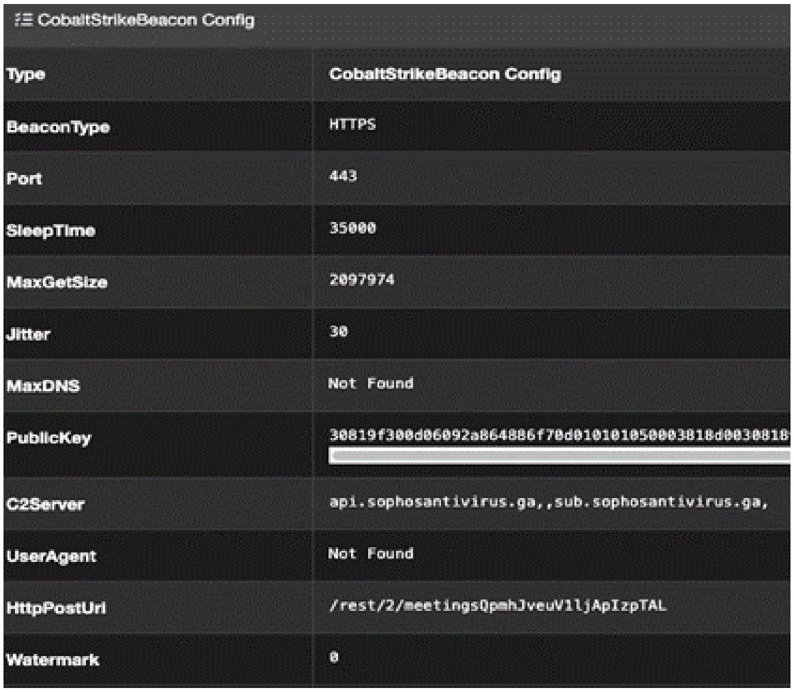
```
int Etw_Function_Patch()
{
  HMODULE ModuleHandleA; // rax
  FARPROC EtwEventWrite; // rbx
  HANDLE CurrentProcess; // rax
  HANDLE CurrentProcess1; // rax
  HANDLE CurrentProcess2; // rax
  char Return_Instruction[4]; // [rsp+30h] [rbp-28h] BYREF
  DWORD flOldProtect; // [rsp+34h] [rbp-24h] BYREF
  CHAR ModuleName[16]; // [rsp+38h] [rbp-20h] BYREF

  Return_Instruction[0] = 0xC3;
  strcpy(ModuleName, "ntdll.dll");
  ModuleHandleA = GetModuleHandleA(ModuleName);
  if ( ModuleHandleA )
  {
    EtwEventWrite = GetProcAddress(ModuleHandleA, "EtwEventWrite");
    CurrentProcess = GetCurrentProcess();
    VirtualProtectEx(CurrentProcess, EtwEventWrite, 1ui64, 0x40u, &flOldProtect);
    CurrentProcess1 = GetCurrentProcess();
    WriteProcessMemory(CurrentProcess1, EtwEventWrite, Return_Instruction, 1ui64, 0i64);
    CurrentProcess2 = GetCurrentProcess();
    LODWORD(ModuleHandleA) = VirtualProtectEx(CurrentProcess2, EtwEventWrite, 1ui64, flOldProtect, 0i64);
  }
  return (int)ModuleHandleA;
}
```

Figure 3. Updated HUI Loader code that disables ETW. (Source: Secureworks)

Ransomware C2 infrastructure

Analysis of the Cobalt Strike Beacon samples loaded by HUI Loader revealed a link between AtomSilo, Night Sky, and Pandora ransomware. The Cobalt Strike Beacons were configured with an uncommon HTTP POST URI beginning with /rest/2/meetings and a watermark value of 0 (see Figure 4). As of this publication, CTU researchers have only observed this configuration in Cobalt Strike Beacons associated with these ransomware families.



CobaltStrikeBeacon Config

Type	CobaltStrikeBeacon Config
BeaconType	HTTPS
Port	443
SleepTime	35000
MaxGetSize	2097974
Jitter	30
MaxDNS	Not Found
PublicKey	30819f300d06092a864886f70d010101050003818d0030818
C2Server	api.sophosantivirus.ga,,sub.sophosantivirus.ga,
UserAgent	Not Found
HttpPostUri	/rest/2/meetingsQpmhJveuV1ljApIzpTAL
Watermark	0

Figure 4. Cobalt Strike payload configuration information. (Source: Secureworks)

The configuration of these Cobalt Strike payloads is likely based on a modified version of a public C2 malleable profile that configures the HTTP GET request URI as ‘/functionalstatus’ and the HTTP POST URI as ‘/rest/2/meetings’. Table 2 compares the three Cobalt Strike Beacons.

Cobalt Strike C2 domain	HTTP POST URI	Ransomware
update . ajaxrenew . com	/rest/2/meetingsVDcrCtBuGm8dime2C5zQ3EHbRE156AkpMu6W	AtomSilo
api . sophosantivirus . ga sub . sophosantivirus . ga	/rest/2/meetingsQpmhJveuV1IjApIzpTAL	Night Sky
peek . openssl-digicert . xyz	/rest/2/meetingsKdEs85OkdgIPwcqbjS7uzVZKBIZNHeO4r5sKe	Pandora

Table 2. Cobalt Strike Beacon sample configuration information linked to ransomware activity.

In a January 2022 Secureworks incident response (IR) engagement, CTU researchers observed a threat actor compromising a ManageEngine ADSelfService Plus server. The threat actor exploited an authentication bypass vulnerability (CVE-2021-40539) and deployed a Meterpreter reverse shell that communicated with a C2 IP address (172 . 105 . 229 . 30). They then deployed three files to the compromised host: a legitimate Microsoft Defender executable vulnerable to DLL search order hijacking, a HUI Loader sample (mpclient.dll) that is loaded by the executable, and an encrypted Cobalt Strike Beacon (dlp.ini). CTU researchers did not observe follow-on activity.

The C2 server also hosted a legitimate VMware executable (VMwareXferlogs.exe) vulnerable to DLL search order hijacking. This executable loads a DLL (glib-2.0.dll) from the same directory. CTU researchers were unable to obtain glib-2.0.dll from this C2 server but identified other glib-2.0.dll HUI Loader samples that could be sideloaded by VMwareXferlogs.exe. An April 2022 third-party report links glib-2.0.dll HUI Loader samples that load Cobalt Strike to LockBit ransomware. However, there is not enough evidence in the report for CTU researchers to validate this claim.

The VirusTotal analysis service revealed URLs indicating the presence of glib-2.0.dll files on two servers (45 . 32 . 101 . 191 and 45 . 61 . 139 . 38). Passive DNS data shows that 45 . 61 . 139 . 38 hosted sc . microsofts . net, which is a C2 domain that third-party reporting links to LockFile ransomware activity. The 45 . 32 . 101 . 191 IP address hosted api . openssl-digicert. xyz, which has sibling domain (peek . openssl-digicert . xyz) that is linked to Pandora ransomware.

While CTU researchers do not have access to these servers, timeline analysis suggests that two HUI Loader samples uploaded to VirusTotal may have been hosted on these servers. Both samples have compile timestamps that are the close to the ‘URL first seen’ timestamp listed on VirusTotal (see Table 3). Although threat actors can trivially modify compile timestamps, the timeframe of the associated intrusion activity makes it unlikely that these timestamps were altered. The two HUI Loader samples that were possibly hosted on these servers share code with the Pandora ransomware.

Sample	First submission (VirusTotal)	Executable compile timestamp	Server/URL likely associated with the sample	URL first seen (VirusTotal)
HUI Loader sample 1	24/01/2022 08:15:29	22/01/2022 18:16:45	http: //45 . 61 . 139 . 38/glib-2.0.dll	25/01/2022 14:01:35
HUI Loader sample 2	18/03/2022 20:25:32	16/02/2022 13:01:30	http: //45 . 32 . 101 . 191/glib-2.0.dll	18/02/2022 17:28:16

Table 3. HUI Loader samples likely hosted on servers linked to ransomware activity.

Ransomware TTPs and code overlap

CTU analysis indicates that the five ransomware families linked to HUI Loader were developed from two distinct codebases: one for LockFile and AtomSilo, and the other for Rook, Night Sky, and Pandora. Based on the order in which these ransomware families appeared starting in mid-2021, the threat actors likely first developed LockFile and AtomSilo and then developed Rook, Night Sky, and Pandora.

Third-party researchers leveraged code overlap between LockFile and AtomSilo to release a decryptor for files encrypted with these ransomware families in October 2021. Other third-party reporting describes TTP overlap in LockFile and AtomSilo intrusion activity. The overlap includes identical filenames for the ransomware executable and components of the Kernel Driver Utility.

Table 4 lists feature similarities across Rook, Night Sky, and Pandora. These ransomware families appear to leverage the Babuk ransomware source code. The Babuk source code was reportedly leaked in September 2021, a few months before Rook operations began in December 2021.

Features	Rook	Night Sky	Pandora
Contains an embedded 2,048-bit RSA public key	X	X	X
Creates victim keys	X	X	X
Uses a 2,048-bit RSA victim public key	X	X	X
Encrypts each file with a different key	X	X	X
Adds a file trailer containing information required for file decryption	X	X	X
Uses a statically linked Mbed TLS library for encryption functionality	X	X	X

Features	Rook	Night Sky	Pandora
Stores encryption keys in registry	X		X
Partially encrypts large files and uses chunking	X	X	X

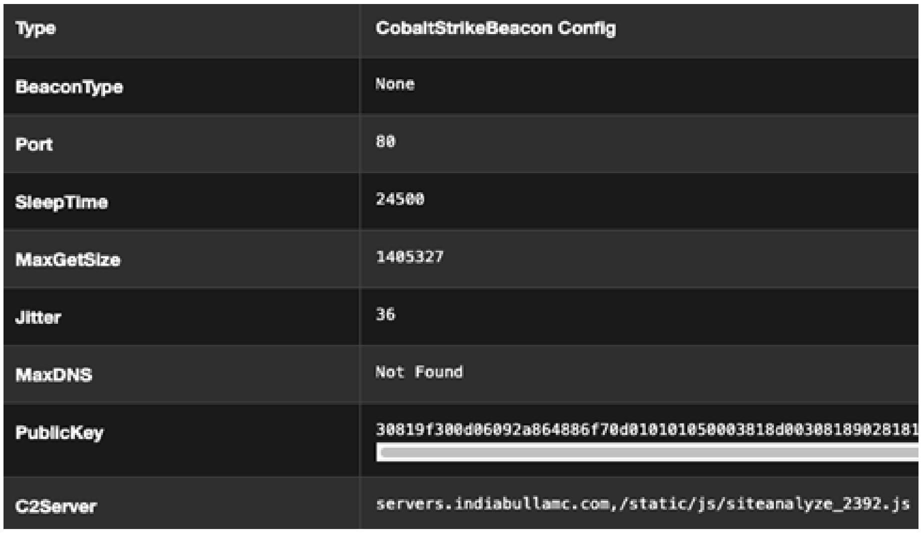
Table 4. Similarities across Rook, Night Sky, and Pandora ransomware.

The use of HUI Loader to load Cobalt Strike Beacon, the Cobalt Strike Beacon configuration information, the C2 infrastructure, and the code overlap suggest that the same threat group is associated with these five ransomware families. It is likely that BRONZE STARLIGHT is responsible for LockFile, AtomSilo, Rook, Night Sky, and Pandora intrusion activity.

Connections to China

As of this publication, CTU researchers have not linked HUI Loader to publicly available code and have only observed HUI Loader usage in the A41APT campaign linked to BRONZE RIVERSIDE and the post-intrusion ransomware activity linked to BRONZE STARLIGHT. BRONZE RIVERSIDE (also known as APT10) is associated with the Chinese Ministry of State Security (MSS). A third-party report attributes LockFile, AtomSilo, Rook, and Night Sky ransomware activity to a Chinese threat group it calls DEV-0401. The discovery of links to PlugX and Chinese-language resources associated with the ransomware activity further support the likelihood that BRONZE STARLIGHT is based in China.

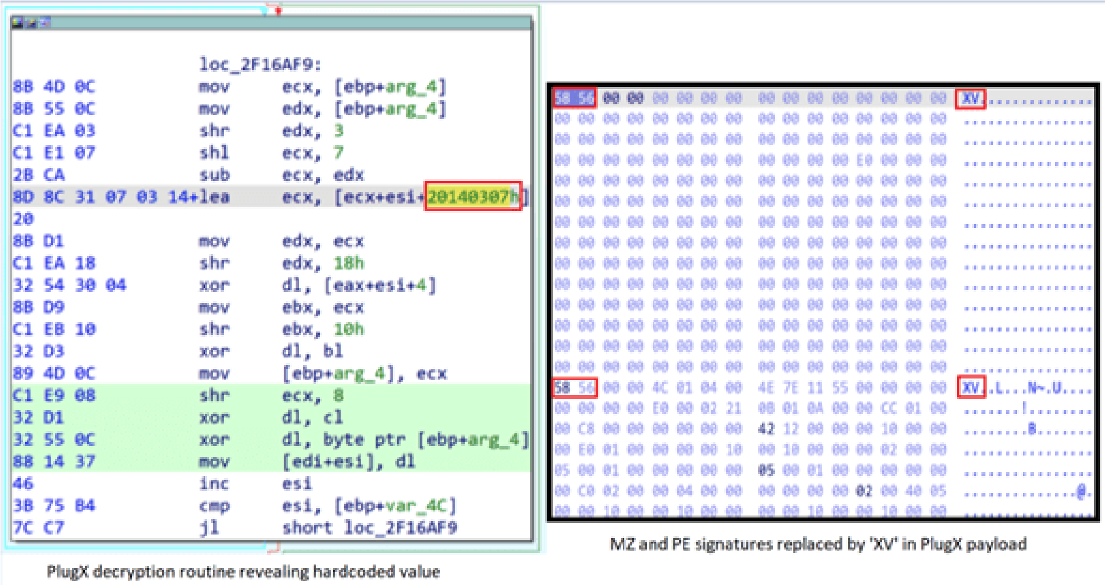
CTU analysis revealed four HUI Loader samples that decrypt and load PlugX RAT payloads. PlugX is used by multiple Chinese threat groups. One of the HUI Loader-linked PlugX samples communicates with hr . indiabullamc . com, which is a sibling domain of a BRONZE STARLIGHT Cobalt Strike C2 domain (servers . indiabullamc . com). This Cobalt Strike Beacon sends HTTP GET requests to /static/js/siteanalyze_2392.js (see Figure 5). CTU researchers identified four additional Cobalt Strike Beacons that send HTTP GET requests to the same URI. One of these Cobalt Strike Beacons communicates with cs . microsofts . net, which is a sibling of a Cobalt Strike C2 domain (sc . microsofts . net) used by LockFile.



Type	CobaltStrikeBeacon Config
BeaconType	None
Port	80
SleepTime	24500
MaxGetSize	1405327
Jitter	36
MaxDNS	Not Found
PublicKey	30819f300d06092a864886f70d010101050003818d00308189028181
C2Server	servers.indiabullamc.com,/static/js/siteanalyze_2392.js

Figure 5. Configuration information for Cobalt Strike Beacon linked to PlugX sample. (Source: Secureworks)

The indiabullamc . com domain likely masquerades as the legitimate website for an India-based company. A ransomware note uploaded to VirusTotal suggests that a company with a similar name was a LockFile victim in July 2021. Analysis of the indiabullamc . com PlugX payload revealed that it replaces the MZ signature in the MS-DOS header and the portable executable (PE) signature in the PE header with ‘XV’. This PlugX variant uses the hard-coded value 0x20140307 to generate a key to XOR-decrypt the PlugX configuration information (see Figure 6).



```
                    loc_2F16AF9:
8B 4D 0C            mov     ecx, [ebp+arg_4]
8B 55 0C            mov     edx, [ebp+arg_4]
C1 EA 03            shr     edx, 3
C1 E1 07            shl     ecx, 7
2B CA               sub     ecx, edx
8D 8C 31 07 03 14+lea     ecx, [ecx+esi+20140307h]
20
8B D1               mov     edx, ecx
C1 EA 18            shr     edx, 18h
32 54 30 04         xor     dl, [eax+esi+4]
8B D9               mov     ebx, ecx
C1 EB 10            shr     ebx, 10h
32 D3               xor     dl, bl
89 4D 0C            mov     [ebp+arg_4], ecx
C1 E9 08            shr     ecx, 8
32 D1               xor     dl, cl
32 55 0C            xor     dl, byte ptr [ebp+arg_4]
88 14 37            mov     [edi+esi], dl
46                  inc     esi
3B 75 B4            cmp     esi, [ebp+var_4C]
7C C7               jl      short loc_2F16AF9
```

PlugX decryption routine revealing hardcoded value

```
58 56 00 00 00 00 00 00  00 00 00 00 00 00 00 00  XV..............
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 E0 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
58 56 00 00 4C 01 04 00  4E 7E 11 55 00 00 00 00  XV..L...N~.U....
00 00 00 00 E0 00 02 21  08 01 0A 00 00 CC 01 00  .......!........
00 C8 00 00 00 00 00 00  42 12 00 00 00 10 00 00  ........B.......
00 E0 01 00 00 00 00 10  00 10 00 00 00 02 00 00  ................
05 00 01 00 00 00 00 00  05 00 01 00 00 00 00 00  ................
00 C0 02 00 00 04 00 00  00 00 00 00 02 00 40 05  ..............@.
00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  ................
```

MZ and PE signatures replaced by 'XV' in PlugX payload

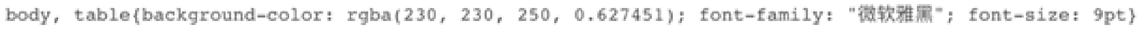
Figure 6. Analysis of PlugX sample linked to LockFile ransomware activity. (Source: Secureworks)

PlugX ‘XV’ samples can be grouped into sub-versions based on the hard-coded value in the decryption routine. One of the other PlugX payloads loaded by HUI Loader was uploaded to VirusTotal in 2017 and was not the same sub-version as the indiabullamc . com payload. The remaining two samples were the same sub-version as the indiabullamc . com payload and were observed in attacks targeting Southeast Asian organizations in April 2019. CTU researchers are unable to corroborate the BRONZE RIVERSIDE attribution based on the information in the report, but the TTPs align with Chinese threat group activity.

PlugX source code has allegedly been leaked online. However, it is unclear which variant was leaked and if it has been used by threat groups outside of China. It is unlikely that the indiabullamc .com PlugX sub-version is used widely across distinct threat groups or even across multiple Chinese threat groups. The links connecting LockFile ransomware activity, HUI Loader, and a specific PlugX sub-version associated with Chinese threat group activity suggest that the threat group responsible for the HUI Loader-linked ransomware activity has access to malware developed by Chinese government-sponsored threat groups.

During an October 2021 Secureworks incident response engagement, CTU researchers observed likely ransomware precursor activity that overlapped with third-party reporting of LockFile activity. The engagement revealed that the threat actors exploited the ProxyShell vulnerabilities in a Microsoft Exchange server to deploy a web shell. They then ran a PowerShell wget command to download an unidentified file from a server at IP address 45 . 91 . 83 . 176, which the third-party report links to LockFile activity. This server with this IP address reportedly used a Chinese-language configuration during the LockFile ransomware campaign. Although CTU researchers cannot corroborate this claim, VirusTotal reported that the server returned a web page displaying an error message in Chinese.

CTU researchers identified additional artifacts that indicate attribution to a Chinese-speaking threat group. The inclusion of uncommon Subject DN and Issuer DN fields in an SSL certificate associated with Pandora ransomware C2 infrastructure suggest it was likely generated following instructions on a Chinese-language blog for setting up Cobalt Strike SSL certificates. CTU researchers also detected a Chinese character font in a ransom note dropped by Night Sky ransomware (see Figure 7).



```
body, table{background-color: rgba(230, 230, 250, 0.627451); font-family: "微软雅黑"; font-size: 9pt}
```

Figure 7. Reference to a Chinese font family in a Night Sky ransom note. (Source: Secureworks)

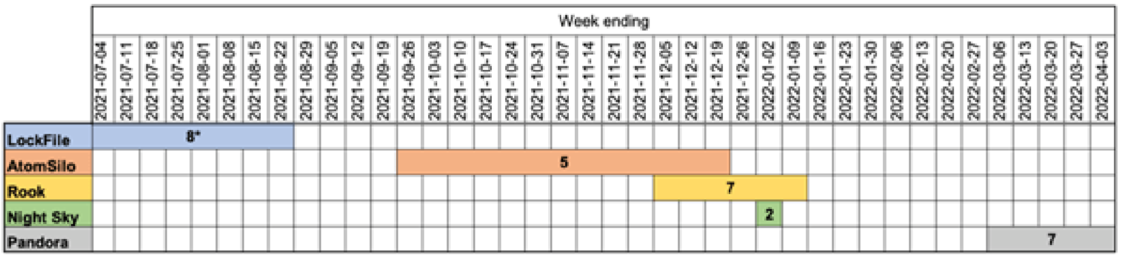
Links between BRONZE STARLIGHT and BRONZE UNIVERSITY

A January 2022 Secureworks incident response engagement revealed that BRONZE STARLIGHT compromised a server running ManageEngine ADSelfService Plus and deployed HUI Loader with a Cobalt Strike Beacon. CTU researchers observed the Chinese BRONZE UNIVERSITY threat group active on the same network with overlapping timeframes. Around mid-November 2021, BRONZE UNIVERSITY compromised this server to deploy ShadowPad malware and stayed active on the network until January 2022. In addition to deploying ShadowPad, BRONZE UNIVERSITY harvested credentials, moved laterally within the network, and compressed sensitive data for exfiltration. The intrusion activity attributed to BRONZE STARLIGHT began in late November 2021 and ended in early December 2021.

CTU researchers did not observe additional BRONZE STARLIGHT activity after the threat actors deployed and executed HUI Loader to load a Cobalt Strike Beacon. It is unclear why BRONZE STARLIGHT suspended its intrusion activity. The simultaneous and continued operations by another Chinese threat group on the same network suggests that the two groups may have deconflicted their post-intrusion activity. This scenario assumes collaboration and knowledge sharing between the groups. It could indicate that BRONZE STARLIGHT participates in government-sponsored intelligence-gathering efforts rather than being a purely financially motivated threat group.

Targeting and victimology

The operational cadence and victimology of LockFile, AtomSilo, Rook, Night Sky, and Pandora deployments do not align with conventional financially motivated cybercrime operations. In each case, the ransomware targets a small number of victims over a relatively brief period of time before it ceases operations, apparently permanently (see Figure 8). The number of victims is unclear, as leak sites often do not list victims who pay ransoms early.



* Estimate based on open source reporting

Figure 8. Timeline of ransomware activity and number of victims listed on each ransomware leak site. (Source: Secureworks)

Cybercrime groups sometimes rebrand their ransomware, often in response to law enforcement or government actions. For example, the GOLD WATERFALL threat group rebranded its Darkside ransomware to BlackMatter likely as a result of law enforcement scrutiny following the Colonial Pipeline attack. Similarly, GOLD DRAKE made several changes to its Hades ransomware to hinder attribution and enable victims to circumvent payment sanctions imposed by the U.S. Treasury Department. Due to the overhead associated with retooling and the impact on revenue, cybercriminals tend to only make these adjustments when they are necessary for continued operations. These pressures typically do not apply to the BRONZE STARLIGHT ransomware families. While the release of an AtomSilo and LockFile decryptor may have prompted the group to create a ransomware family based on Babuk's source code, the decision to limit the ransomware use to brief, targeted deployments is likely to prevent security researchers from clustering activity and identifying trends. The rapid changes in the ransomware landscape make it unlikely that researchers will investigate obsolete ransomware.

BRONZE STARLIGHT operated LockFile as a traditional ransomware scheme but adopted the name-and-shame model for the other ransomware operations. It is possible that the change provided a more plausible means of exfiltrating data. The threat actors may also have decided that the public profile would be more effective as a distraction from their true operational objectives. Pandora is the only ransomware with a leak site as of April 14, 2022, listing five victims. Two earlier victims were removed. Descriptions of each company include anonfiles . com links to ZIP files containing allegedly stolen data.

As of mid-April, a total of 21 victims had been listed across the AtomSilo, Rook, Night Sky, and Pandora leak sites. CTU researchers estimate that approximately 75% would be of interest to Chinese government-sponsored groups focused on espionage based on the victims' geographic locations and industry verticals. The victims include pharmaceutical companies in Brazil and the U.S., a U.S.-based media organization with offices in China and Hong Kong, electronic component designers and manufacturers in Lithuania and Japan, a law firm in the U.S., and an aerospace and defense division of an Indian conglomerate. The five victims that were not likely targeted for espionage include two real estate companies in the Americas, two small financial institutions in the U.S., and a small interior design company in Europe. One victim of Rook ransomware was a bank in Kazakhstan, which strongly suggests that the threat actors are not based in the Commonwealth of Independent States (CIS). There is an unspoken universal agreement among Russian-speaking ransomware groups not to target entities in those jurisdictions.

The number and nature of LockFile victims is unclear. Third-party reporting suggests that victims represented verticals such as manufacturing, financial services, legal, and engineering, and that most were located in the U.S. and Asia. CTU researchers identified two victims that are consistent with the targeting of a Chinese government-sponsored espionage-focused threat group: a financial services organization in India and a local government entity in the U.S.

Victimology does not provide conclusive attribution. Chinese government-sponsored threat groups have broad targeting, so any ransomware operation could include victims of potential Chinese interest. Conversely, Chinese government-sponsored groups using ransomware as a distraction would likely make the activity resemble financially motivated ransomware deployments. However, the combination of victimology and the overlap with infrastructure and tooling associated with government-sponsored threat group activity indicate that BRONZE STARLIGHT may deploy ransomware to hide its cyberespionage activity. While Chinese government-sponsored groups have not historically used ransomware, there is precedent in other countries. For example, North Korea deployed WCry (also known as WannaCry) for financial gain, the Russian IRON VIKING threat group used NotPetya for its destructive capabilities, and the Iranian COBALT FOXGLOVE threat group used Pay2Key and N3tw0rm ransomware as a destructive wiper against entities in Israel.

BRONZE STARLIGHT likely uses ransomware in these incidents to achieve the following tactical objectives:

- Destroy evidence: Encrypting data destroys forensic evidence of espionage activities, making it much more challenging for victims to properly assess the threat and protect themselves.
- Distract investigators: Ransomware can significantly impact a compromised organization and can consume all incident response efforts. Pressure to return to normal business operations could prevent victims from detecting suspicious activity that does not directly relate to the ransomware.
- Exfiltrate data: Name-and-shame ransomware exfiltrates data, with an emphasis on proprietary or sensitive information. As this data is also targeted in espionage operations, the ransomware operation could mask the threat actors' motivation.

Conclusion

BRONZE STARLIGHT compromises networks by exploiting vulnerabilities in network perimeter devices, including known vulnerabilities for which patches are available. The threat actors deploy HUI Loader to decrypt and execute a Cobalt Strike Beacon for command and control. They then deploy ransomware and exfiltrate sensitive data from the victim’s environment.

Both the exploitation of known vulnerabilities and the use of the Cobalt Strike for command and control provide opportunities to detect and prevent BRONZE STARLIGHT intrusion activity before exfiltration or ransomware deployment. Network defenders should implement a robust patch management process to address network perimeter vulnerabilities in a timely manner. However, breaches can occur even with preventative measures in place. Reactive measures such as a robust and tested incident response plan, real-time network monitoring and alerting, and an extended detection and response (XDR) solution are crucial for minimizing the impact of ransomware and other malicious activity.

Threat indicators

The threat indicators in Table 7 can be used to detect activity related to BRONZE STARLIGHT. Note that IP addresses can be reallocated. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
b16bb2f910f21e2d4f6e2aa1a1ea0d8b	MD5 hash	HUI Loader used in likely ransomware campaign (lockdown.dll)
a75e9b702a892cc3e531e158ab2e4206b939f379	SHA1 hash	HUI Loader used in likely ransomware campaign (lockdown.dll)
8502852561fcb867d9cbf45ac24c5985fa195432b542dbf8753d5f3d7175b120	SHA256 hash	HUI Loader used in likely ransomware campaign (lockdown.dll)
809fcab1225981e87060033d72edaeaf	MD5 hash	Encrypted Cobalt Strike Beacon loaded by HUI Loader (vm.cfg)
64f5044709efc77230484cec8a0d784947056022	SHA1 hash	Encrypted Cobalt Strike Beacon loaded by HUI Loader (vm.cfg)
62fea3942e884855283faf3fb68f41be747c5baa922d140509237c2d7bacdd17	SHA256 hash	Encrypted Cobalt Strike Beacon loaded by HUI Loader (vm.cfg)
peek.openssl-digicert.xyz	Domain name	Cobalt Strike C2 server used in HUI Loader intrusion
a4a6abf4ed4c9447683fba729a17197b	MD5 hash	HUI Loader used in likely ransomware campaign (glib-2.0.dll)

Indicator	Type	Context
ead02cb3f6b811427f2635a18398392bc2ebca3a	SHA1 hash	HUI Loader used in likely ransomware campaign (glib-2.0.dll)
b0fb6c7eecbf711b2c503d7f8f3cf949404e2dd256b621c8cf1f3a2bdfb54301	SHA256 hash	HUI Loader used in likely ransomware campaign (glib-2.0.dll)
4c3c7053ec145ad3976b2a84038c5feb	MD5 hash	Cobalt Strike Beacon loaded by HUI Loader (vmtools.ini)
3246867705e8aad60491fe195bcc83af79470b22	SHA1 hash	Cobalt Strike Beacon loaded by HUI Loader (vmtools.ini)
15b52c468cfd4dee4599ec22b1c04b977416fbe5220ab30a097f403903d28a3a	SHA256 hash	Cobalt Strike Beacon loaded by HUI Loader (vmtools.ini)
api.wensente.xyz	Domain name	Cobalt Strike C2 server used in HUI Loader campaign
0c4a84b66832a08dccc42b478d9d5e1b	MD5 hash	Pandora executable with similar code as HUI Loader lockdown.dll sample
160320b920a5ef22ac17b48146152ffbef60461f	SHA1 hash	Pandora executable with similar code as HUI Loader lockdown.dll sample
5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b	SHA256 hash	Pandora executable with similar code as HUI Loader lockdown.dll sample
bde2a3c8e034d30ce13e684f324c6702	MD5 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
a413f4bcb7406710b76fabdaba95bb4690b24406	SHA1 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
f04f444d9f17d4534d37d3369bf0b20415186862986e62a25f59fd0c2c87562f	SHA256 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
f259765905cd16ff40132f35c85a862a	MD5 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
d9efd4c4e1fb4e3d4a171c4ca0985839ad1cdee9	SHA1 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
7fe5674c9a3af8413d0ec71072a1c27d39edc14e4d110bfeb79d1148d55ce0b6	SHA256 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
update.microsoftlab.top	Domain name	Cobalt Strike C2 server used in HUI Loader campaign

Indicator	Type	Context
69ef2d7f9ed29840b60a7fd32030cbd1	MD5 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
b24e254f6fdd67318547915495f56f8f2a0ac4fe	SHA1 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
91f8805e64f434099d0137d0b7ebf3db3ccbf5d76cd071d1604e3e12a348f2d9	SHA256 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
577a47811b3c57a663bcbf2aab99c9e3	MD5 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
dbc48357bfbe41f5bfdd3045066486e76a23ad2d	SHA1 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
70225015489cae369d311b62724ef0caf658ffdf62e5edbafd8267a8842e7696	SHA256 hash	Cobalt Strike Beacon loaded by HUI Loader (mpc.tmp)
api.microsoftlab.xyz	Domain name	Cobalt Strike C2 server used in HUI Loader campaign
b0175b09e58d34689a7403abed2ae2f5	MD5 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
46a9b419d73a518effbc19c3316d8a20cff9ce4a	SHA1 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
5b5cd007fb96eef68d3d123eba82a4e4dfce50cdf3b05fe82bfa097870c09903	SHA256 hash	HUI Loader used in possible ransomware activity (mpclient.dll)
f3355c8f43dada5a62aab60089c03d1e	MD5 hash	Cobalt Strike Beacon loaded by HUI Loader (dlp.ini)
5df448af3f7935c3f4a2904b16af9ea00d13cb0c	SHA1 hash	Cobalt Strike Beacon loaded by HUI Loader (dlp.ini)
c7a515276883a03981accfac182341940eb36071e2a59e8fb6cb22f81aa145ae	SHA256 hash	Cobalt Strike Beacon loaded by HUI Loader (dlp.ini)
update.microupdate.xyz	Domain name	Cobalt Strike C2 server used in HUI Loader campaign
update.ajaxrenew.com	Domain name	Cobalt Strike C2 server used in HUI Loader campaign
172.105.229.30	IP address	Meterpreter C2 server linked to BRONZE STARLIGHT
45.61.139.38	IP address	Hosting HUI Loader malware linked to BRONZE STARLIGHT
45.32.101.191	IP address	Hosting HUI Loader malware linked to BRONZE STARLIGHT

Table 5. Indicators for this threat.

References

Abrams, Lawrence. “Babuk ransomware's full source code leaked on hacker forum.” Bleeping Computer. September 3, 2021. https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/

Avast. “Avast releases decryptor for Atom Silo and LockFile ransomware.” October 27, 2021. https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/

Gallagher, Sean and Singh, Vikas. “Atom Silo ransomware actors use Confluence exploit, DLL side-load for stealthy attack.” SOPHOS Labs. October 4, 2021. https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/

Gatlan, Sergiu. “Free decryptor released for Atom Silo and LockFile ransomware.” Bleeping Computer. October 27, 2021. https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-atom-silo-and-lockfile-ransomware/

Hunter, Ben. “Uncovering New Activity By APT10.” Fortinet. October 15, 2019. https://www.fortinet.com/blog/threat-research/uncovering-new-activity-by-apt-

Jie, Ji. “Insights into Ransomware Spread Using Exchange 1-Day Vulnerabilities 1-2.” NSFOCUS. September 26, 2021. https://nsfocusglobal.com/insights-into-ransomware-spread-using-exchange-1-day-vulnerabilities-1-2/

Kersten, Max and Elias, Marc. “PlugX: A Talisman to Behold.” March 28, 2022. https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/plugx-a-talisman-to-behold.html

Microsoft Threat Intelligence Center (MSTIC). "Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability." December 11, 2021. https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

S2W Talon. “Atomsilo x Lockfile: Atomsilo copied BlackMatter and Cerber for operating the double extortion site.” September 24, 2021. https://medium.com/s2wblog/atomsilo-x-lockfile-atomsilo-copied-blackmatter-and-cerber-for-operating-the-double-extortion-site-7fb5aaac5f21

Symantec. “LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers.” August 20, 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows

Tsai, Orange. “From Pwn2Own 2021: A New Attack Surface on Microsoft Exchange - ProxyShell!” August 18, 2021. https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell

United States Department of Justice. “Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.” December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Wosar, Fabian (@fwosar). “BlackMatter decryptor characteristics indicate a Darkside rebrand.” Twitter. July 31, 2021, 12:15 pm. https://twitter.com/fwosar/status/1421504819890634754

Yanagishita, Hajime, et al. “What We Can Do against the Chaotic A41APT Campaign.” Japan Security Analyst Conference 2022. January 27, 2022. http://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf