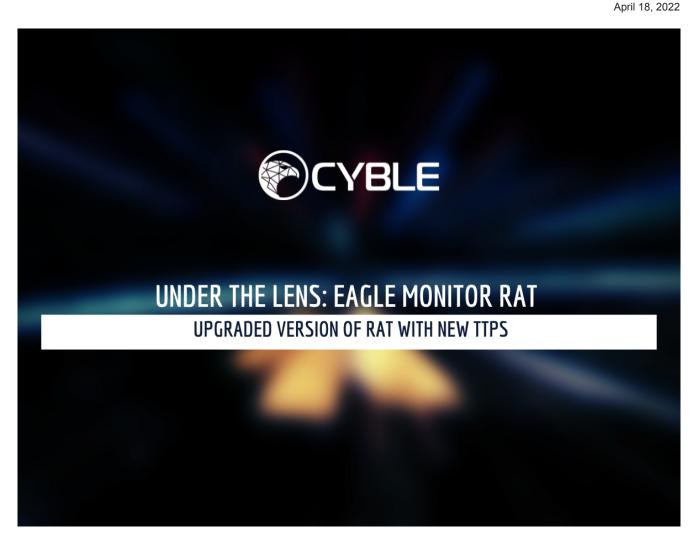
Under the lens: Eagle Monitor RAT

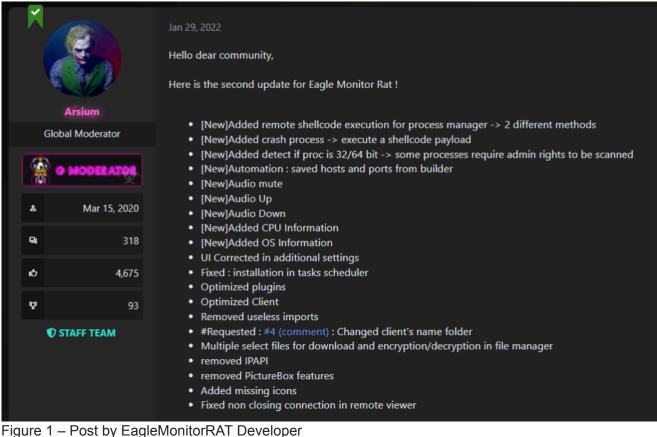
blog.cyble.com/2022/04/18/under-the-lens-eagle-monitor-rat/



Upgraded version of RAT with new TTPs

A Remote Administration Tool is a type of software that gives the attacker full control over the victims' device remotely. Using RATs, attackers can perform various tasks such as accessing files, cameras, and other resources remotely while conducting keylogging, system operations, etc.

A developer named "Arsium" <u>posted</u> a new version of this open-source RAT – EagleMonitorRAT – on GitHub. Additionally, the developer posted a link to the GitHub page of the EagleMonitorRAT to various underground dark web markets. Figure 1 shows one such post by the developer.



According to the developer, the EagleMonitorRAT is written in C# and upgraded from HorusEyesRat, which is Visual Basic .NET-based.

Cyble Research Labs has analyzed the RAT binary and panel to gain insights into the functionalities and impact of the RAT.

RAT Details

While building the solution, various executables and support plugins are compiled, including client builder plugins and an admin panel. Figure 2 shows the compiled binaries and other files.

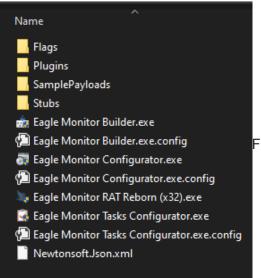
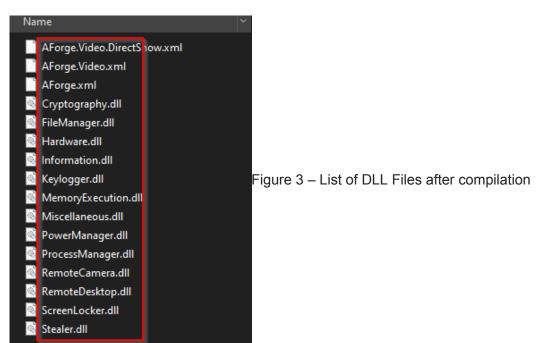


Figure 2 – Compiled Binaries for EagleMonitorRAT

Additionally, various Dynamic Link Library (DLL) files are also compiled to support operations such as file management, keylogging, etc. Figure 3 shows the support DLL files.



A client builder is used to compile the binary, which will be delivered to users to compromise a target machine. The client binary may be delivered to users using various initial infection vectors such as spam email etc. The builder has an option to specify the IP address of the server, port, and key. Figure 4 shows the client builder.

		_	×
Network			
IP/DNS:			
PORT:			
KEY:			
Miscellaneous			
Persistence	Offline Keylogger Visual Basic Stub x64 stub		
Task name:			
Time (in min) :			
	Build !		

Figure 4 – EagleMonitorRAT Client Builder Panel

EagleMonitorRAT has a server panel for managing victim devices. The panel shows country, hardware ID, operating system details, username, available RAM, privilege, region etc. Additionally, the panel has various options to manage as well for performing several operations in the infected device.

The Admin panel of EagleMonitorRAT includes operations such as:

- recovery
- desktop
- miscellaneous panels
- mass tasks
- memory execution
- information
- client

Figure 5 shows the administration panel of EagleMonitorRAT.

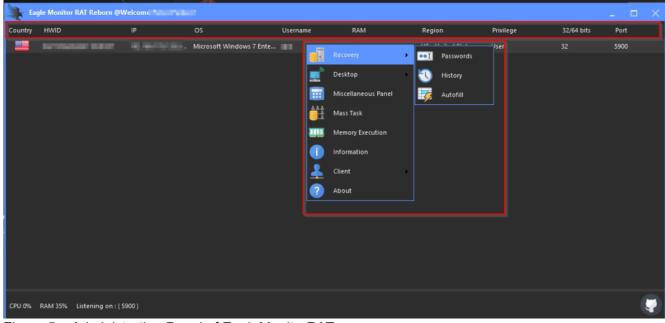


Figure 5 – Administration Panel of EagleMonitorRAT

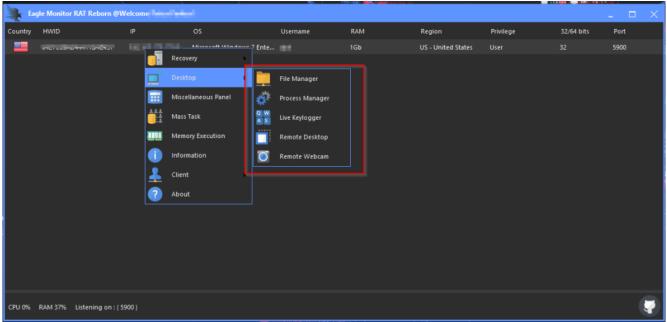
In the recovery option of EagleMonitorRAT, there are three different options – passwords, history, and autofill.

The Recovery option works as an information stealer which extracts usernames, passwords, and browser history. Figure 6 shows stolen information retrieved using the Recovery menu from the victim's machine.

Passwords Recovery:				-		\times
URL	Username	Password	Applica	ition		
https://login.yahoo.com/account/	/cr	Nyahi (PC)	Chrome			
History Recovery:	Laber 14			-		×
Application	Title	URL	Date			
Chrome	Free, Private & Secure	Email https://		101034		
Chrome	: Free, Private & Secure	Email https://	appear and and			
Chrome	: Free, Private & Secure	Email https://	and a second	1000		
Chrome	: Free, Private & Secure	Email http:/	470,000	-		
Chrome	: Free, Private & Secure	Email https://main.googre.com	/1101/0/0/	and the		
Autofill Recovery				-		\times
Application	Name	Autofill	Date created	Last o used	date	
Chrome	identifier		100000000000000000000000000000000000000			н.,
Chrome	identifier	208	10000300000		81 H S	6 B.
Chrome	username	nghanan -	******			ы.,
Chrome	firstName	participant de la construcción de la constr	100000-000000			

Figure 6 – Recovery Data extracted from the Recovery Option

The Desktop menu option of EagleMonitorRAT has 5 different suboperations – file manager, process manager, live keylogger, remote desktop, and remote webcam. Refer to Figure 7.





The File Manager menu option of EagleMonitorRAT gives TAs the functionality to manage files in the specific directory of the infected device, as shown below.

									-	□ ×
C:\		✓ C:\								
	\$Recycle.Bin	internet internet	ananat. 📄	Boot		Documents	and Settings	MSOCache		
	PerfLogs	Program Files		ProgramData		Python27		Recovery		
	System Volume Information	Tools		Users		Windows		autoexec.bat 24.0 Bytes		
Q)	bootmgr 375 KB	BOOTSECT.BAK 8.00 KB	0	config.sys 10.0 Bytes	4	pagefile.sys 1.00 GB				
L										
			🗩 Go							
			G Back							
			Files	• 🛃	Download					
			ShortCuts	; {•••}	Rename					
				<u> </u>	Delete					_
				*	Launch					

Figure 8 – File Manager Option of the RAT

The Process Manager menu options show the details of the running process of the infected device, such as Icon, ID, Name, Window Title, Window Handle, and Is64Bit. Figure 9 shows the Process Manager.

					_ 🗆 X
lcon	ID	Name	Window Title	Window Handle	Is64Bit
	1332	taskhost			32
	1780			0	
O	3368	chrome		0	32
<u></u>	4088	jucheck		0	32
	2040	svchost		0	
P-	1440	cmd	C:\Windows\system32\cmd.exe	104710	32
O	2264	chrome		0	32
	880	svchost		0	
O	1012	chrome		0	32
	1144	svchost		0	
-	2008	cmd	C:\Windows\system32\cmd.exe		32
	1320	dwm		0	32
	716	svchost		0	
-	3632	conhost		0	32
	2472	second at		0	?

Figure 9 – Process Manager of the EagleMonitorRAT

The shellcode injection menu option of the EagleMonitorRAT gives attackers an option to perform shellcode injection remotely in the infected device. Refer to Figure 10.

					_	
lcon	ID	Name	Window Title	Window Handle	Is64Bit	
	2736	and the second se				
	2956	svchost				- 1
	2440	msdtc				
	1100	svchost				
	508	svchost				
	2836	SearchProtocolHost		0		
	348	si 🕢 Refresh				
	684	51				
	424	w 🔀 Kill Process				
	2156	sı 🚺 Suspend Pr	rocess			
	244	si 🕟 Resume Pro	ocess			
<u></u>	1812	ju 1010 Shellcode I	njection	Classia	32	
	1728	vi ¹⁰¹⁰ Shellcode I	njection	Classic		
	328	csrss		Map View		
	2552	sppsvc			?	

Figure 10 – Remote Shellcode Injection Option

The EagleMonitorRAT has a live keylogger functionality to remotely capture the victim system's keystrokes. Figure 11 shows the keylogger menu operation of the RAT.

		-	\times
	Stop Keylogger		
	Keylogger aiready enabled !		
[2:24 PM] [New Tab - Google Chrome] g [2:24 PM] [New Tab - Google Chrome] [ENTER] [ENTER] [ENTER] [ENTER] [ENTER]			

Figure 11 – Live Keylogger

The Remote Desktop functionality captures screenshots of the victim system remotely at predefined intervals. Figure 12 shows the captured screen.

W.						
Capture: 🚺 JPEG 🔹 🗸	Interval: 30					
G Gmail: Free, Private & Secure Em × +			~		•	x
← → C			@ ☆			E
Set as default browser					,	×
M Gmail	For work	Sign in	Get Gr	nail		Â
Secure, smart, a easy to use ema Get more done with Gmail. Now integrated with Google Chat, Googl Meet, and more, all in one place.	il					

Figure 12 – Screenshot Captured by the EagleMonitorRAT

This RAT has a menu option to remotely capture the webcam feed of the infected system as well. Figure 13 shows the webcam panel.

				_ C	⊐ ×
Capture:	✓ Inte	rval: 30	-	-0-	_

Figure 13 – Webcam Panel of the EagleMonitorRAT

The EagleMonitorRAT has miscellaneous menu options to perform other remote operations such as hiding the taskbar, changing wallpapers, sound management, etc., as shown below.

			_ □	×	
Audio	UI				
Decrease : - Increase : +	TaskBar :	Hide	Show		
Hardware	Wallpaper :	Cha	inge		Figure 14 –
Mouse :	Screenlocker:				
Keyboard :	Desktop Icons:	Hide	Show		

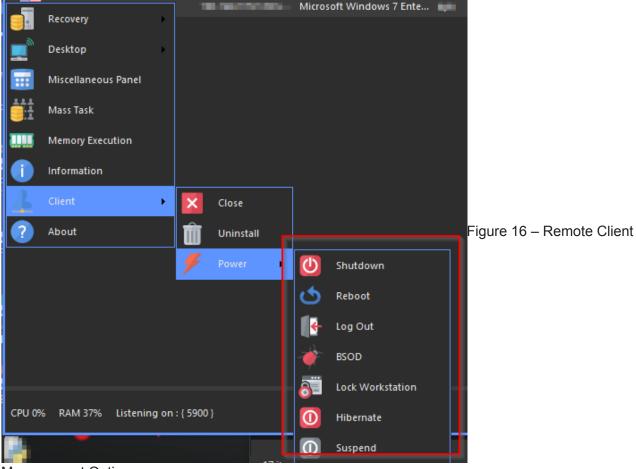
Miscellaneous Options of EagleMonitorRAT

EagleMonitorRAT also has a menu option to discover the network connection and get the CPU information of the infected system. Figure 15 shows the network connection and CPU information.

									_ □	×
CPU		Network C	onnections	(IPV4):						
CPU Vendor : CPU Brand :	GenuineIntel 11th Gen Intel(R) Core(TM) i7-	Process ID	Process Name	Local Address	Local Port	Remote Address	Remote Port	Status	Protocol	
Features	Present	664	svchost	0.0.0.0		0.0.0.0		LISTENING	тср	
3DNOW	No		System	0.0.00	445	0.0.00		LISTENING	тср	
3DNOWEXT	No		System	0.0.00	5357	0.0.0.0		LISTENING	тср	
ABM	No	384	wininit	0.0.0.0	49152	0.0.0.0		LISTENING	тср	
ADX	Yes		svchost	0.0.00	49153	0.0.0.0		LISTENING	тср	
AES	Yes	880	svchost	0.0.00	49154	0.0.0.0		LISTENING	тср	
AVX	Yes	484	services	0.0.0.0	49155	0.0.0.0		LISTENING	тср	
AVX2	Yes	500	lsass	0.0.0.0	49157	0.0.0.0		LISTENING	тср	
AVX512CD	No	2188	svchost	0.0.0.0	50819	0.0.0.0		LISTENING	тср	
			e	100 100 170 100	100		^	HETENING	TCO	

Figure 15 – Network connection and CPU Monitoring

The RAT panel has a menu option to remotely shutdown, reboot, log out, BSOD, lock the workstation, hibernate and suspend the victim's system. Figure 16 showcases these options.



Management Option

Conclusion

RATs have steadily become stealthier and more efficient with new techniques in place. Various cybercriminals and Advanced Persistent Threat Groups have leveraged RATs in the past.

Cyble has observed data breaches in high-profile organizations due to such threats. Since EagleMonitor is an open-source RAT, it is possible that threat actors could create and deploy custom variations for future attacks. Organizations and individuals should thus continue to follow industry best cybersecurity practices.

Our Recommendations:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.

• Enable Data Loss Prevention (DLP) Solutions on the employees' systems.

Tactic	Technique ID	Technique Name
Execution	<u>T1204</u>	User Execution
Privilege Escalation	<u>T1543</u> T1055	Create or Modify System Process Process Injection
Credential Access	<u>T1555</u> <u>T1539</u> <u>T1552</u> <u>T1528</u>	Credentials from Password Stores Steal Web Session Cookie Unsecured Credentials Steal Application Access Token
Collection	<u>T1113</u> <u>T1123</u> <u>T1119</u> <u>T1005</u> <u>T1056</u>	Screen Capture Audio Capture Automated Collection Data from Local System Input Capture
Discovery	<u>T1518</u> <u>T1124</u> <u>T1007</u> <u>T1083</u> <u>T1046</u>	Software Discovery System Time Discovery System Service Discovery File and Directory Discovery Network Service Scanning
Command and Control	<u>T1071</u>	Application Layer Protocol
Exfiltration	<u>T1041</u>	Exfiltration Over C2 Channel

MITRE ATT&CK® Techniques

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
6c172f7329eb3d18eb59de21aa065ee4 12b61e975fa830fee6ea04e66cb07b5db6c4477b b1422ef3148f49247b207d4c167cc54c6d3c65d408910470b252ea178eaa66c8	Md5 SHA-1 SHA- 256	Eagle Monitor RAT Reborn (x32).exe
6d269bc0b0a986e6e437bc9a33c6c95a 47e45dd7e64fe23dd9cb88a3545cee7b9014239c 8cc10fff94267bd402ef92cf0e886120803a3d46f90e821bc28fe0f5b2606082	Md5 SHA-1 SHA- 256	Eagle Monitor Builder.exe
c179251bae0044413c32b224895bf103 b6d646d9ae87eefc4dc271f3e0419f43bdb2c94f 7b09df73e2551317e2547391361b579899cfcfd3304aab7fe4808858822be3f4	Md5 SHA-1 SHA- 256	Client.exe