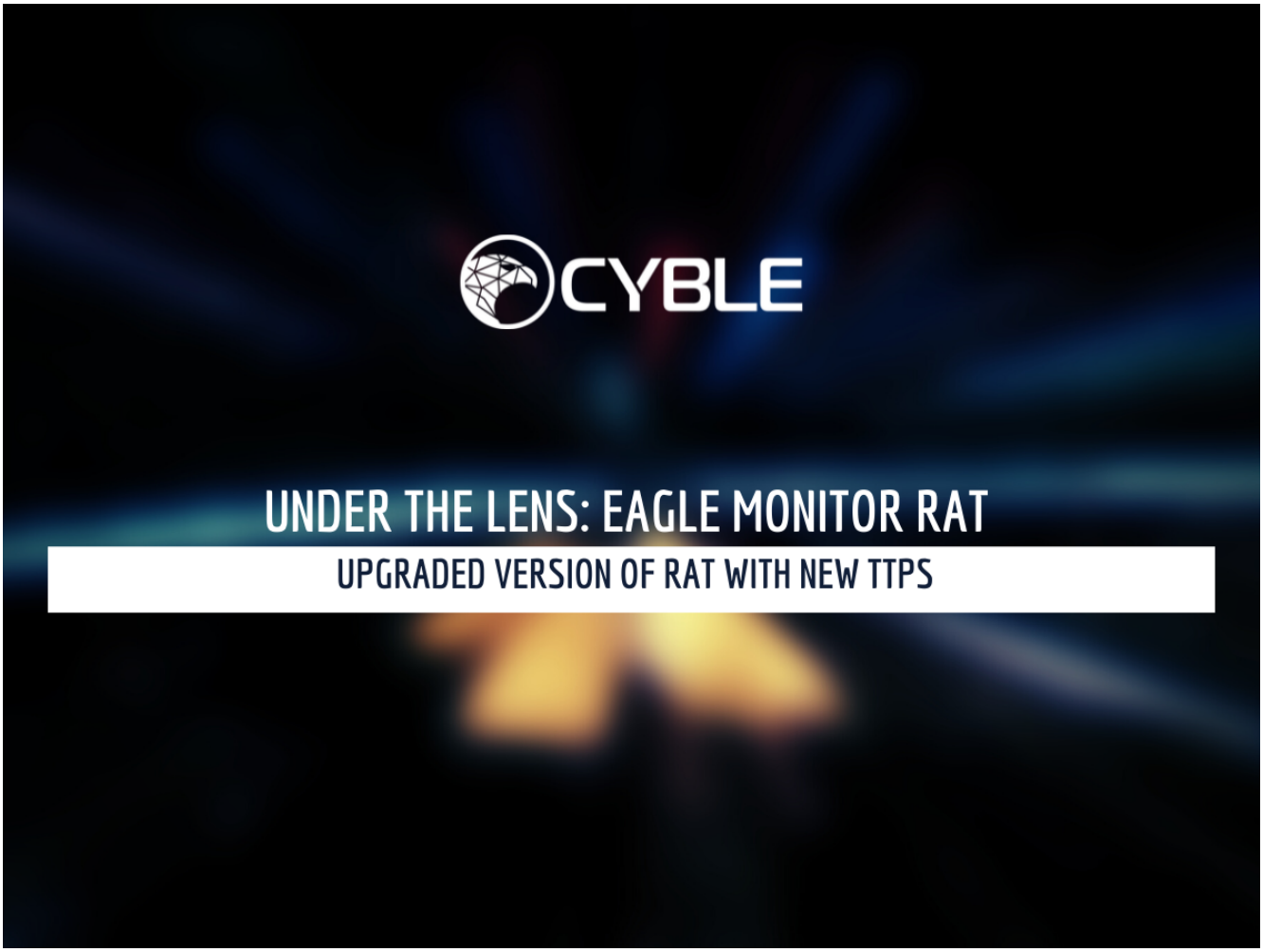
Under the lens: Eagle Monitor RAT

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

April 18, 2022



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" posted 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.

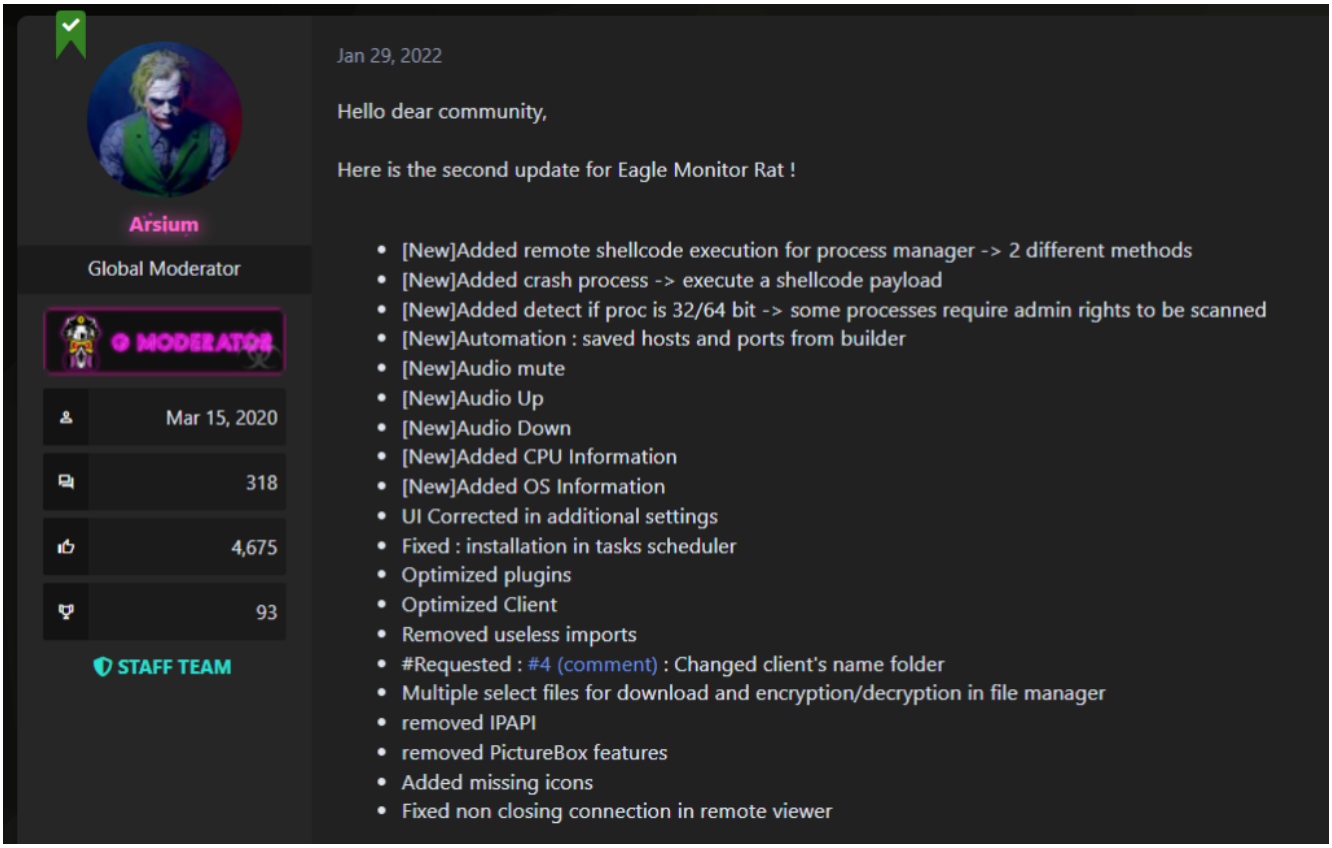


Figure 1 – Post by EagleMonitorRAT Developer

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.

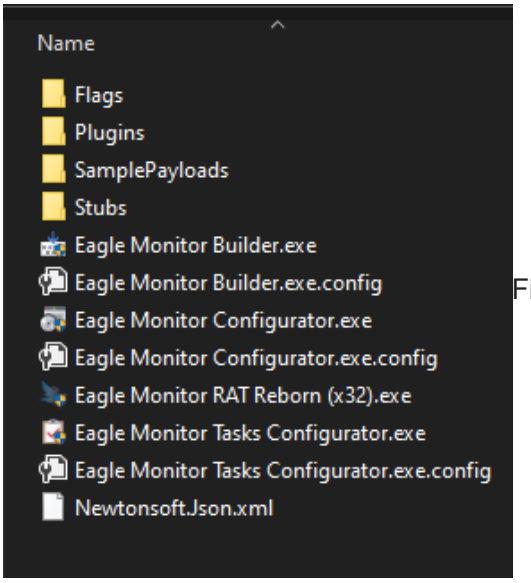


Figure 2 – Compiled Binaries for EagleMonitorRAT

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.

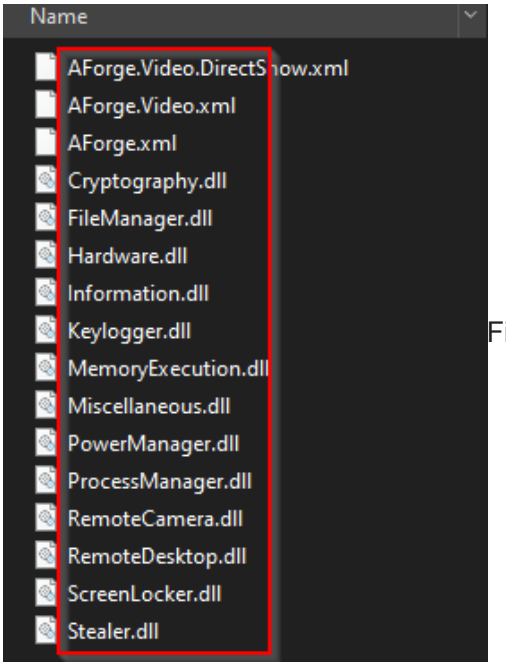


Figure 3 – List of DLL Files after compilation

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.

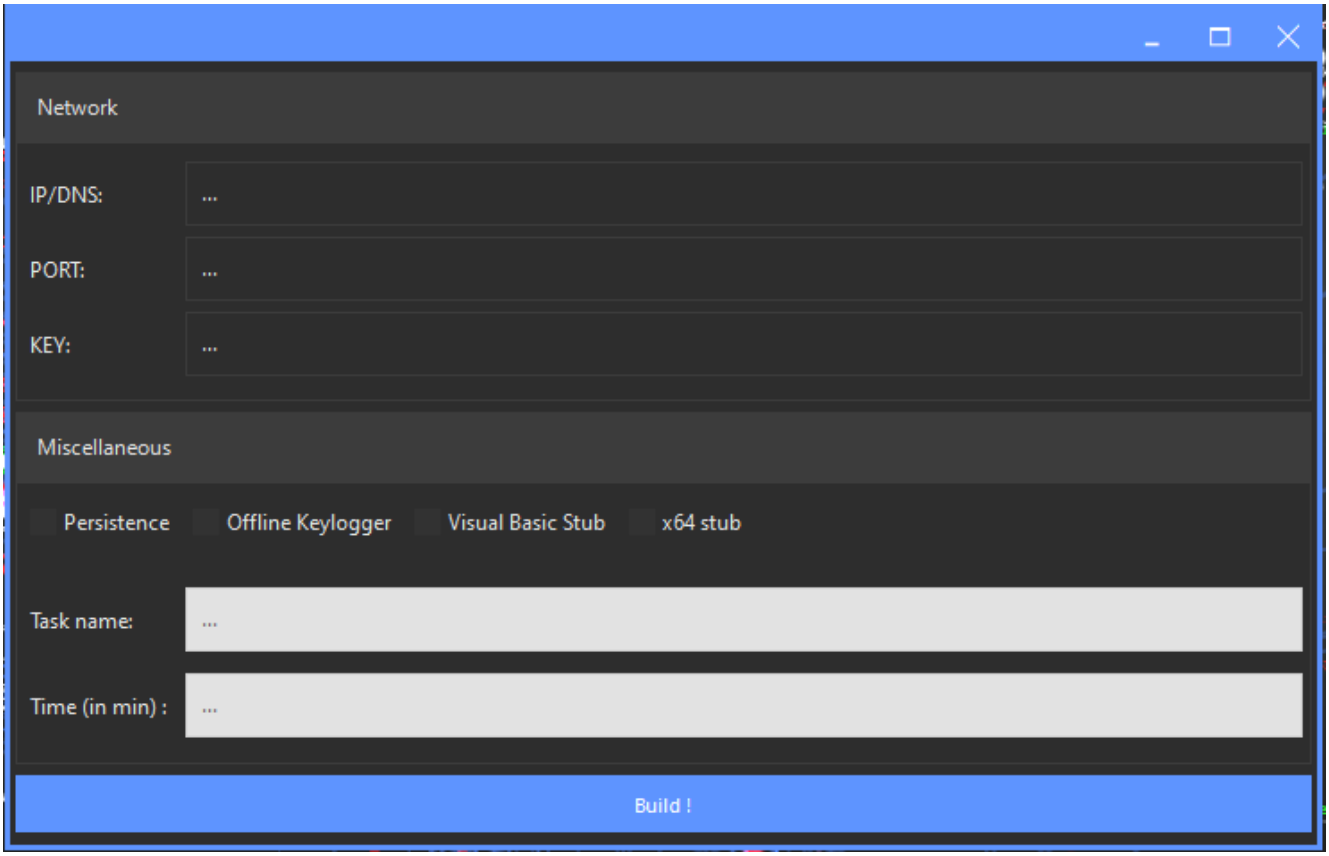


Figure 4 – EagleMonitorRAT Client Builder Panel

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.

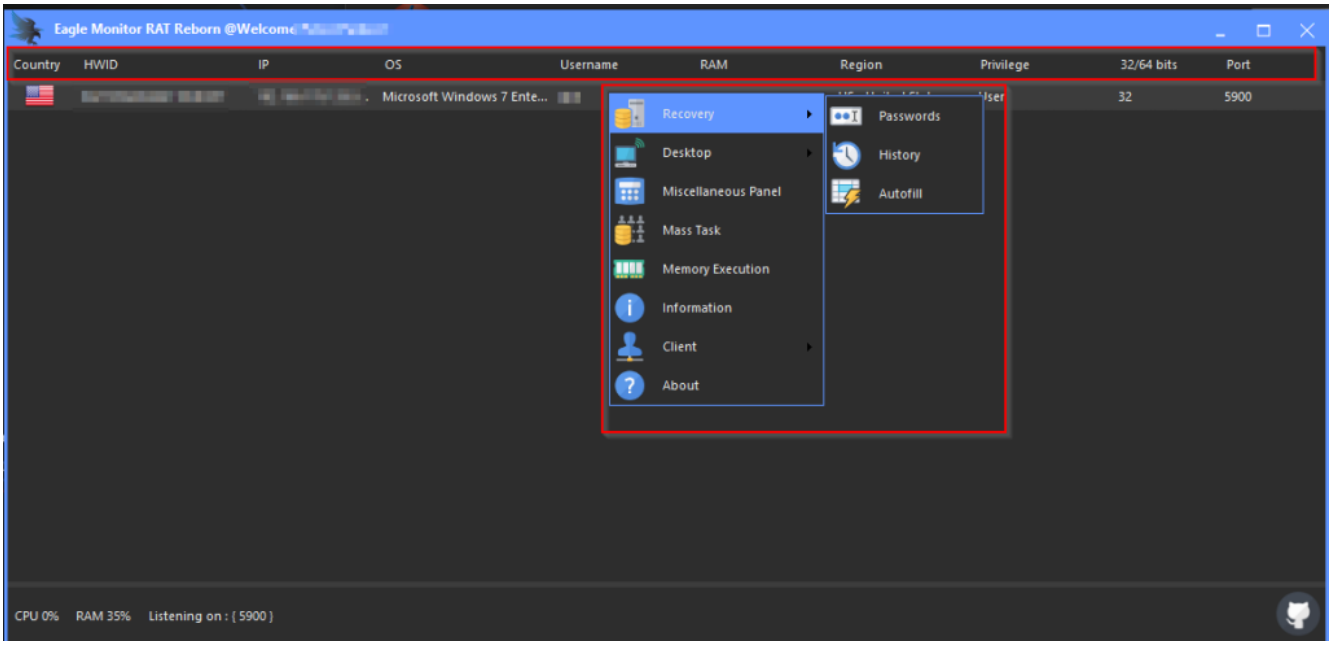


Figure 5 – Administration Panel of EagleMonitorRAT

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.

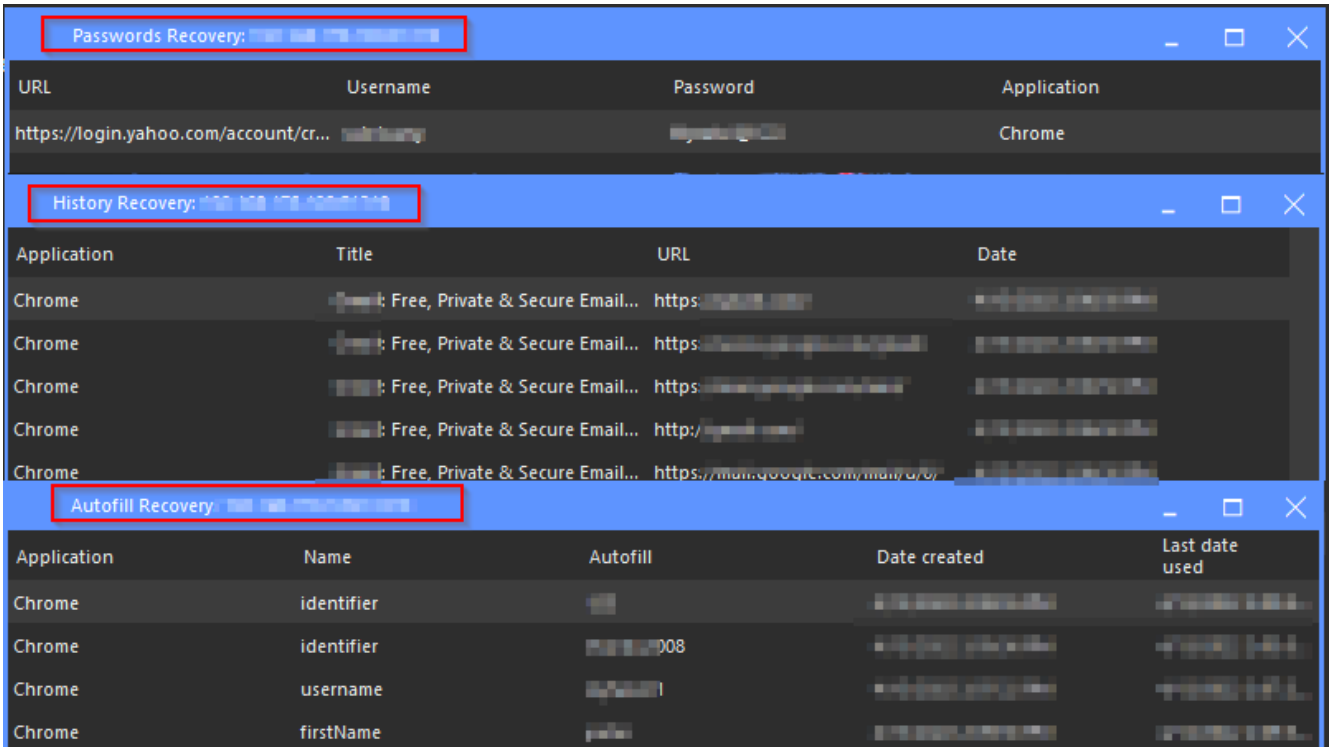


Figure 6 – Recovery Data extracted from the Recovery Option

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.

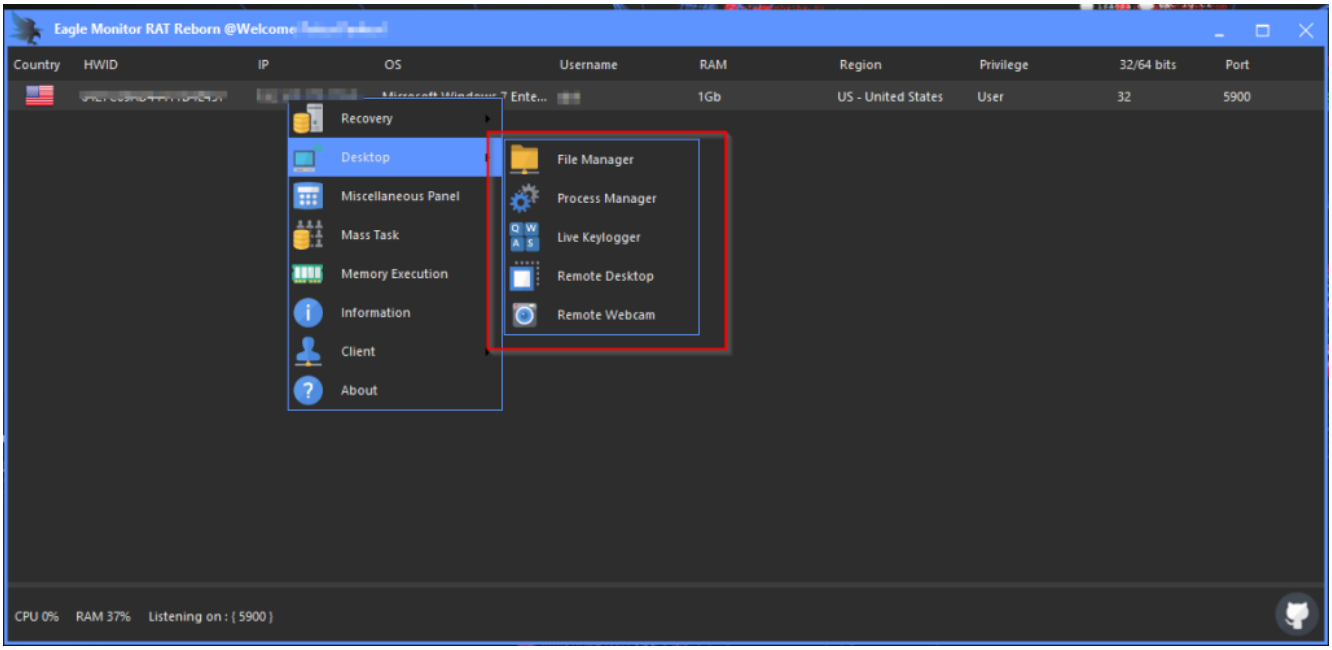


Figure 7 – Desktop Option of EagleMonitorRAT

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.

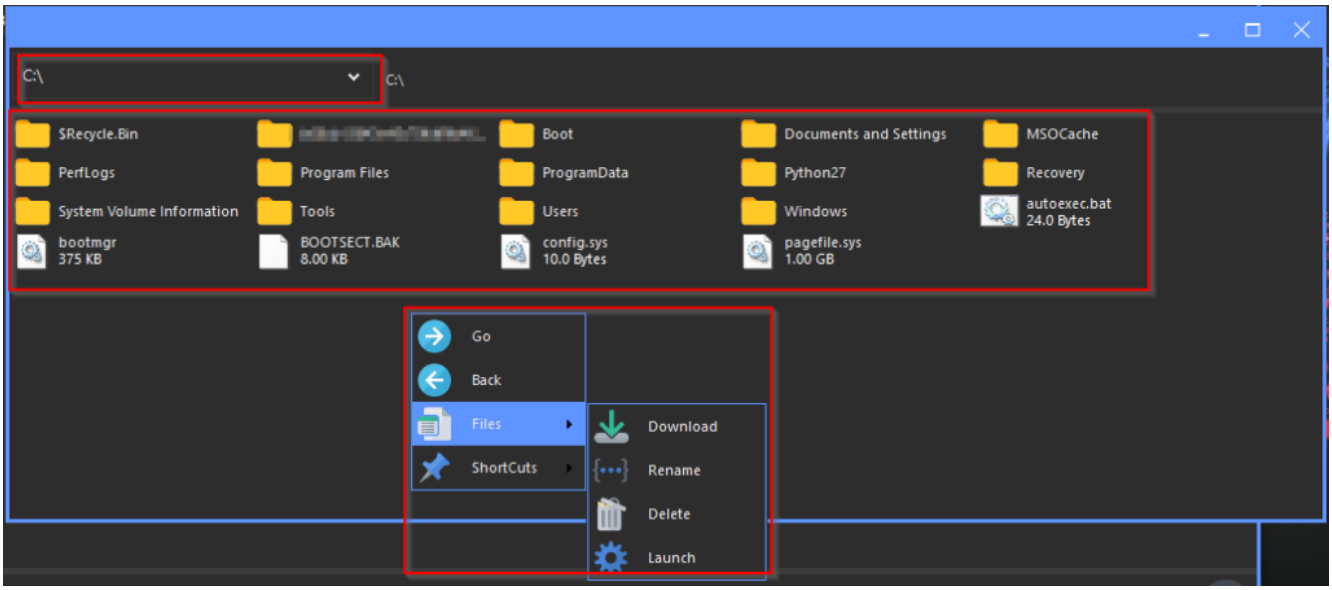


Figure 8 – File Manager Option of the RAT

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.

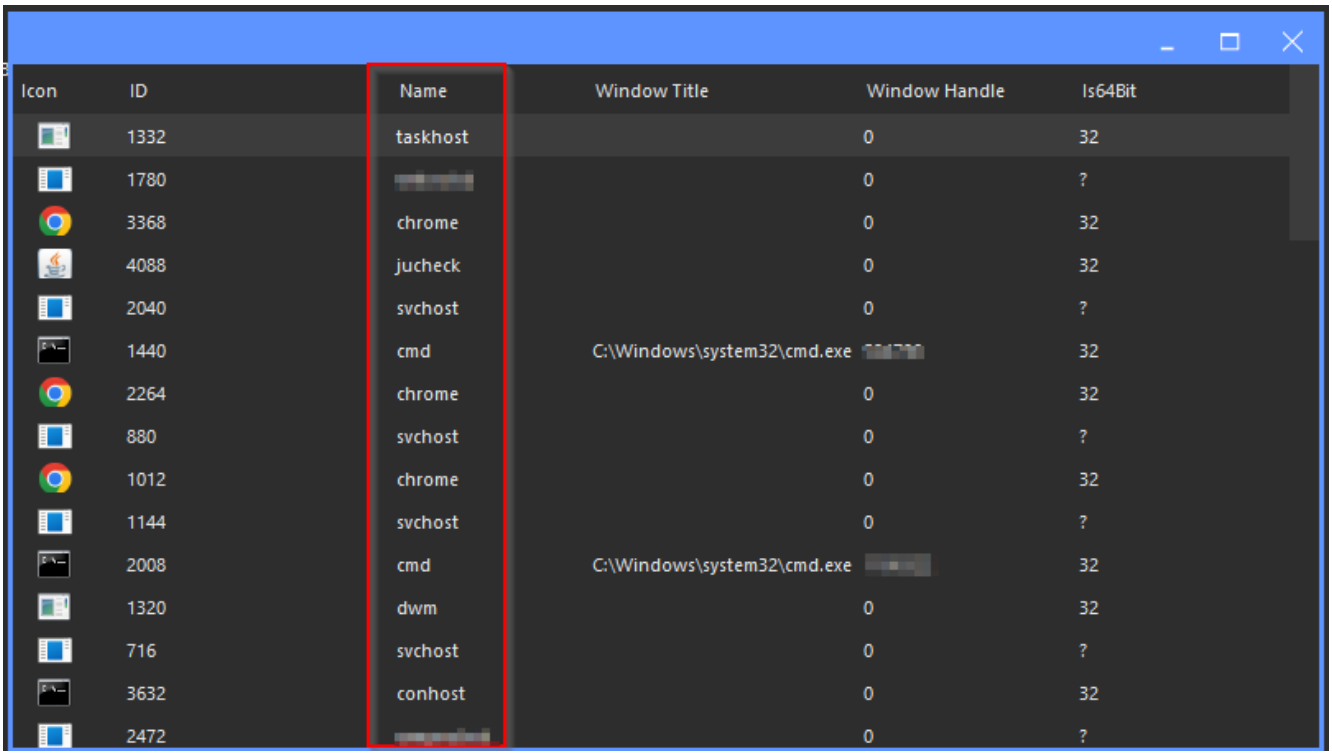


Figure 9 – Process Manager of the EagleMonitorRAT

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.

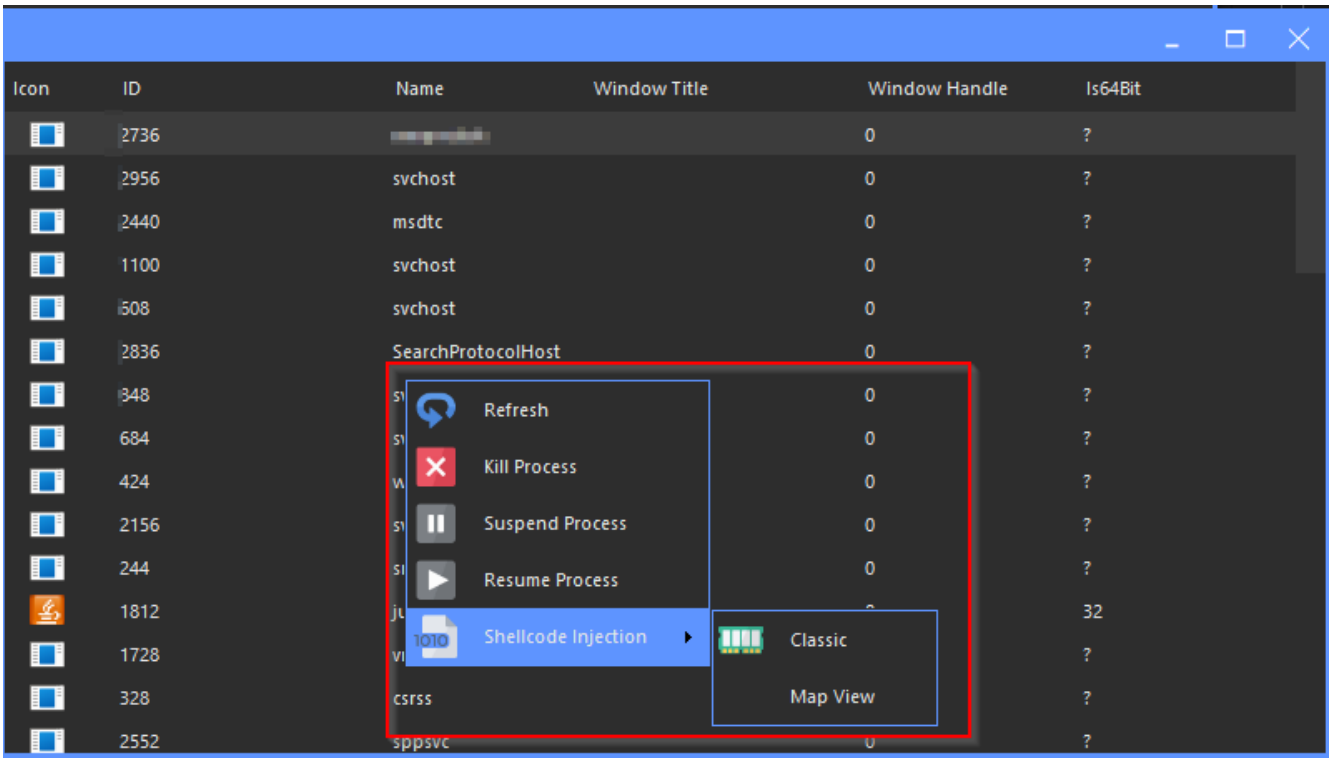


Figure 10 – Remote Shellcode Injection Option

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.

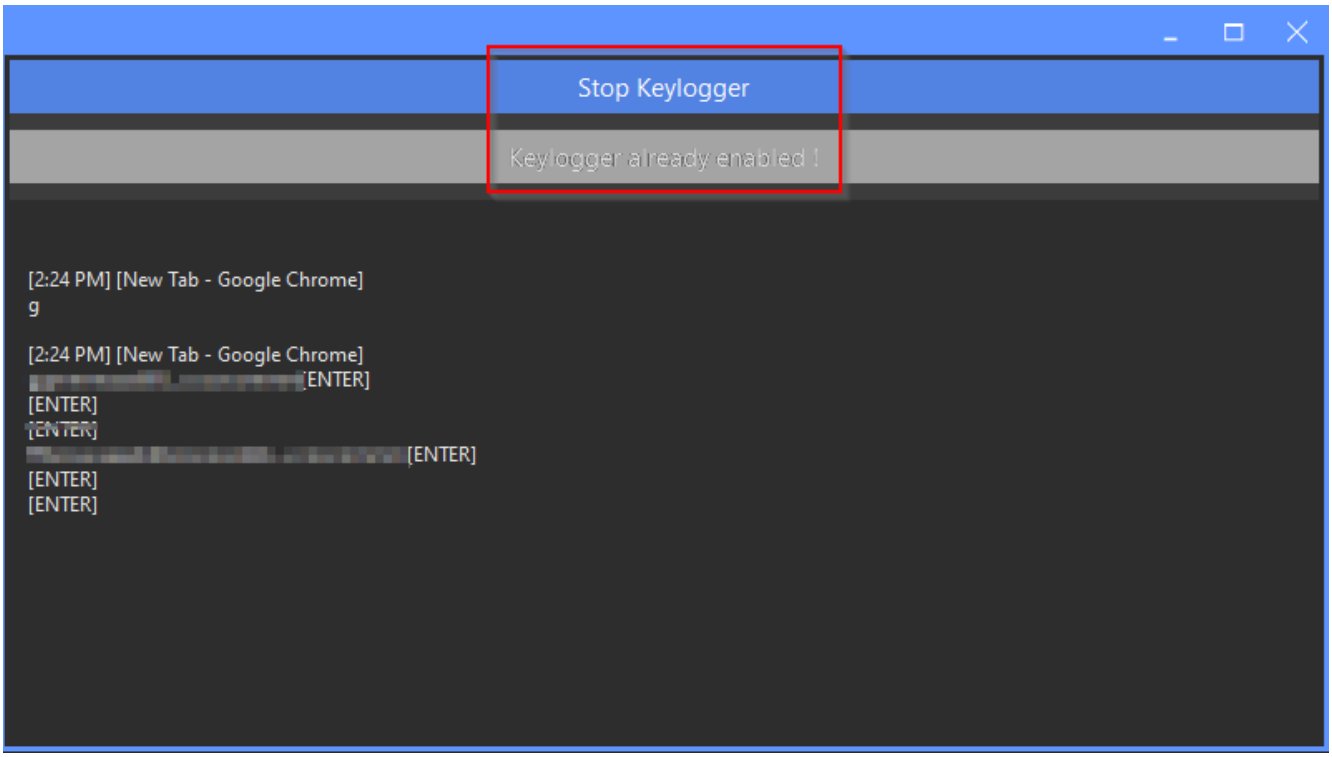


Figure 11 – Live Keylogger

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

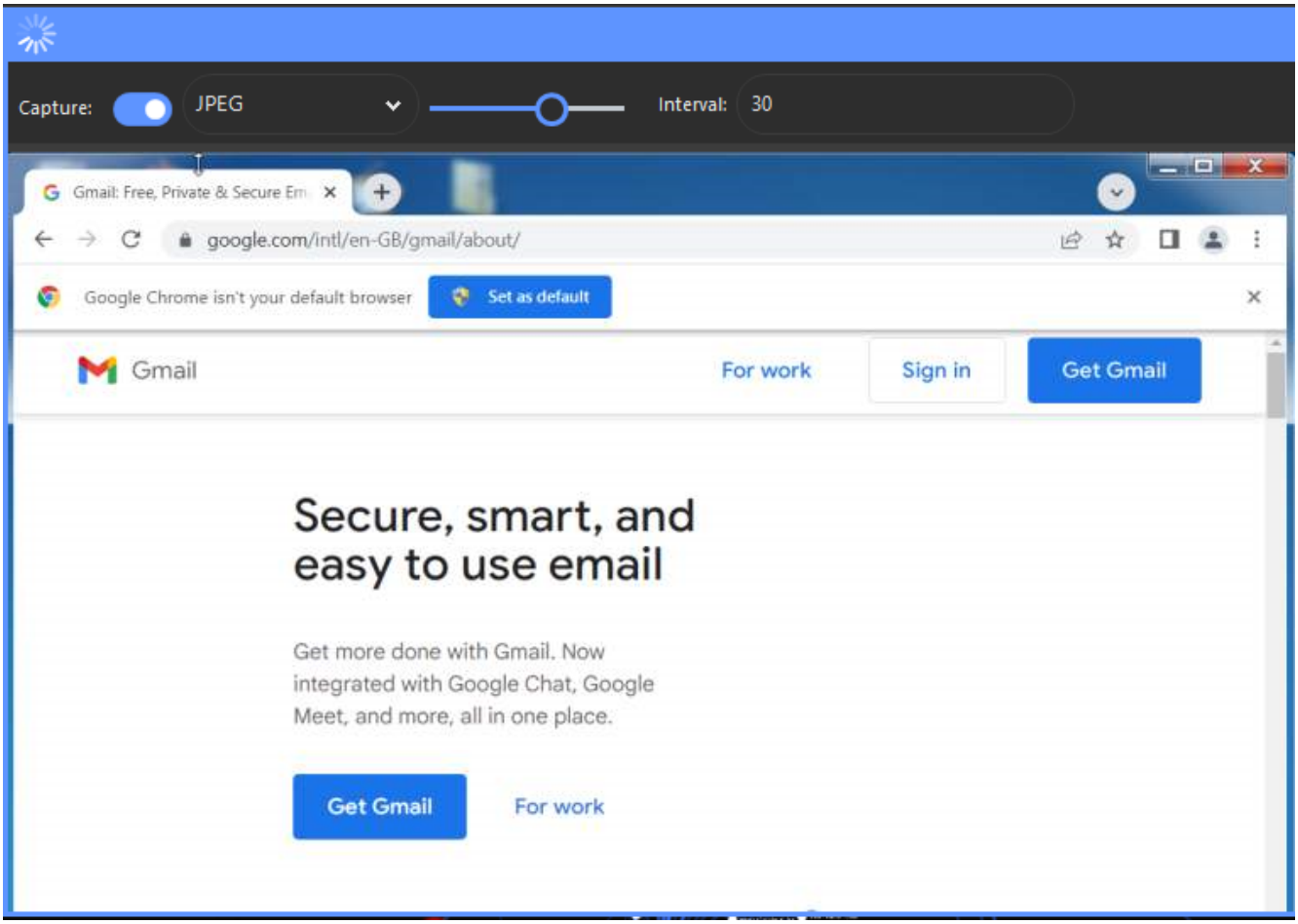


Figure 12 – Screenshot Captured by the EagleMonitorRAT

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

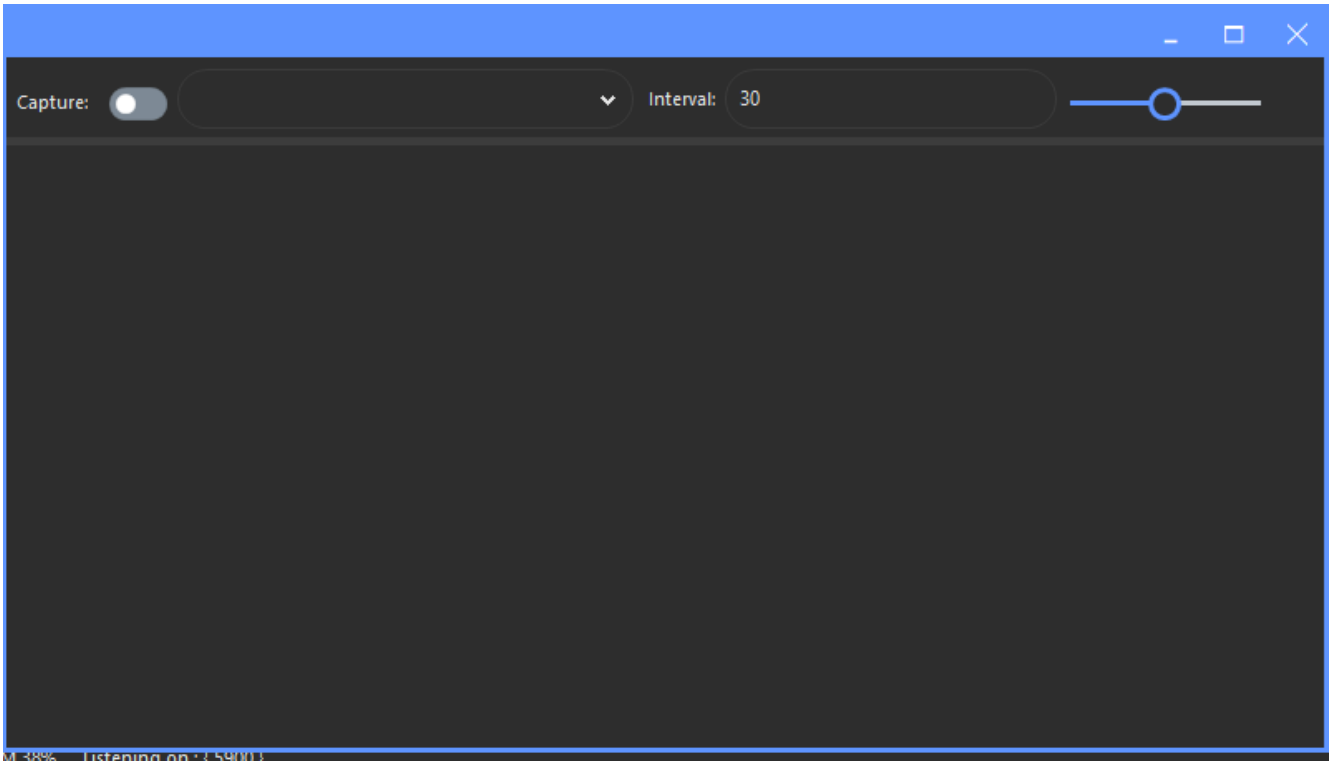


Figure 13 – Webcam Panel of the EagleMonitorRAT

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

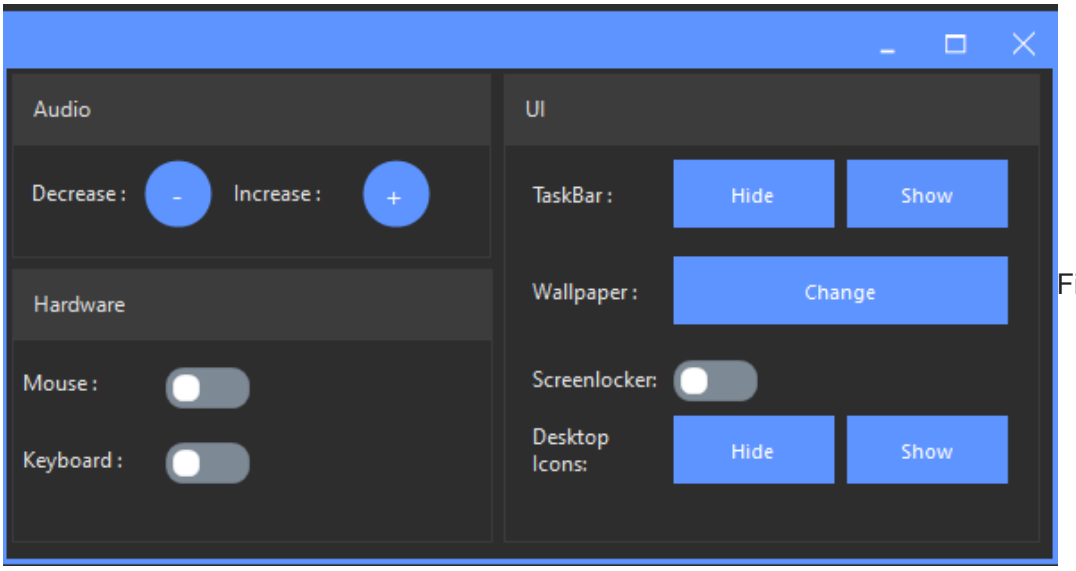


Figure 14 – Miscellaneous Options of EagleMonitorRAT

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.

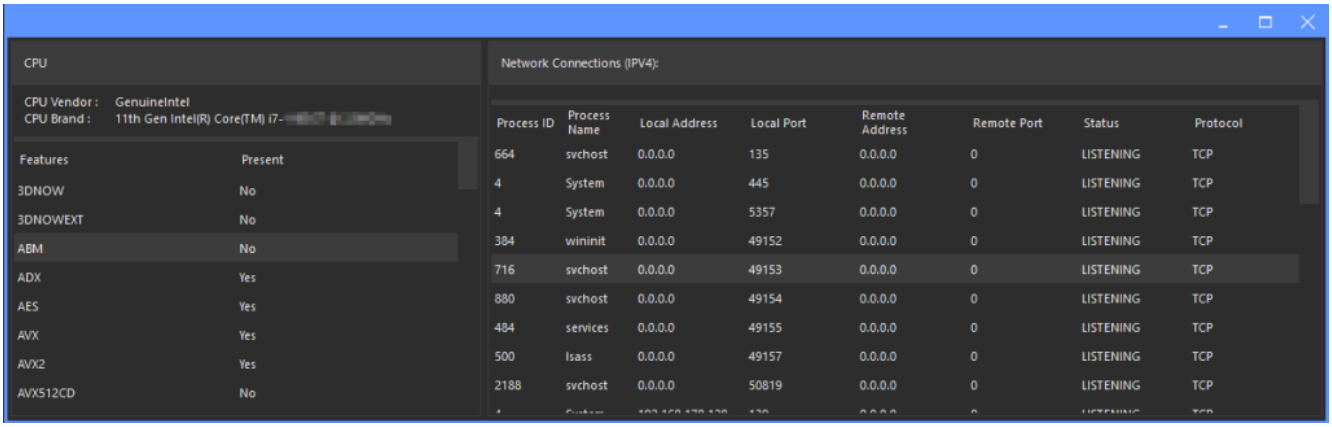


Figure 15 – Network connection and CPU Monitoring

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.

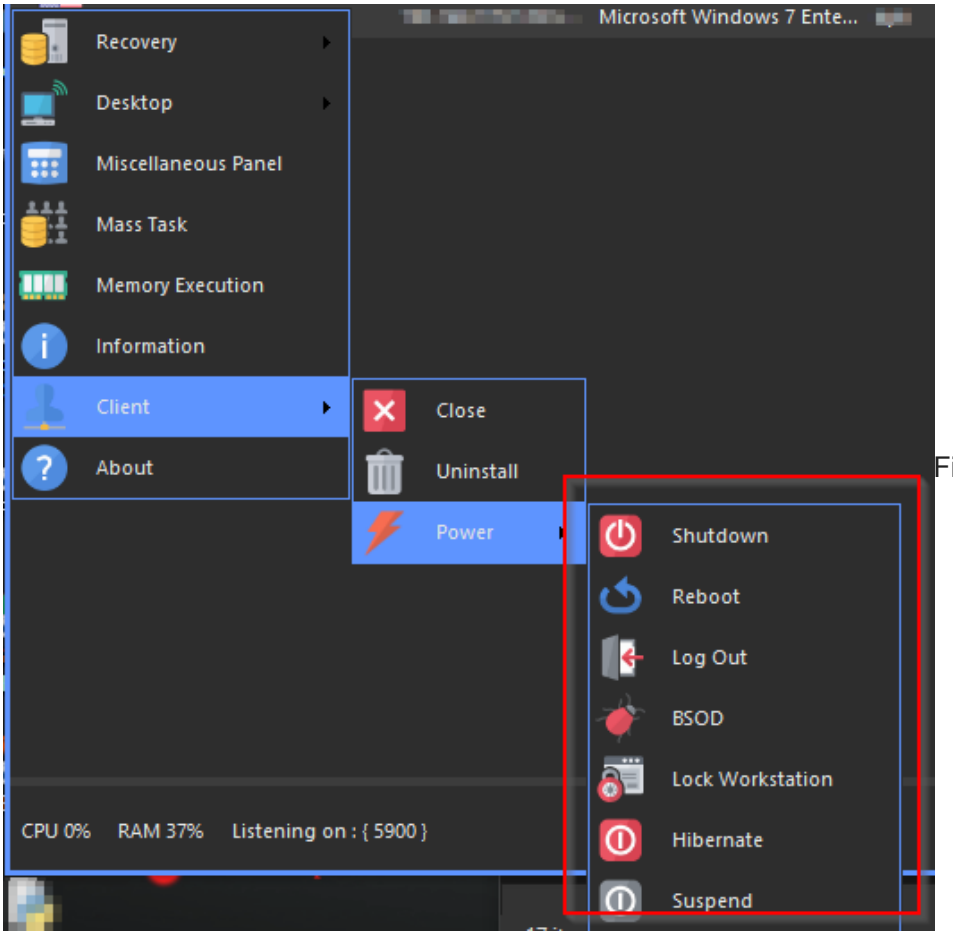


Figure 16 – Remote Client Management Option

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.

MITRE ATT&CK® Techniques

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

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**