Quick look at Nazar's backdoor - Capabilities

Published: 2020-04-23 · Archived: 2026-04-05 15:18:40 UTC

Intro

Yesterday at a virtual edition of OPCDE Juan Andrés Guerrero-Saade disclosed to the world part of his research on threat groups listed in `Lost in Translation`, a leak of Equation Group tools done by Shadowbrokers in 2017. Shortly after he published an analysis on his blog and shared hashes. During the talk Juan mentioned that he doesn't really know what the piece of malware, belonging to Nazar APT, actually does so we put some time to find out.

EYService

EYService (**2fe9b76496a9480273357b6d35c012809bfa3ae8976813a7f5f4959402e3fbb6**) is a main part of the backdoor and its the one we took a look at. This a passive backdoor that relies on, now discontinued, Packet Sniffer SDK (PSSDK) from Microolap. We wont go into details of communication and how packets from and to c2 are build, this will be a subject of following posts. Instead we will present capabilities of this malware. All magic is happening in `00404F10h` where we can find a big if-else tree with various commands id.

Command	Action	Comments
311	prepare/execute keyloger	loads %WINSYSDIR%\hodll.dll calls `instalhook` and `removehook` from it, saves data to %WINSYSDIR%\report.txt
139	shutdown os	calls ole object via rclsid: F6E5B398-E3DF-496B-A2AD-C20FEA30DBFE, riid: DBCB4B31-21B8-4A0F-BC69-0C3CE3B66D00 - registerd by godown.dll
189	prepare/take screen shot	loads ViewScreen.dll, calls SaveBitmapToPNGFile, saves screenshot to %CWD%\z.png
119	prepare/record audio	using mixer* WINAPI, saves recorded audio to %WINSYSDIR%\music.mp3
199	list drives	Enumerates drives, saves results to %WINSYSDIR%\Drives.txt
200	list files	Enumerates files on drive, save results to %WINSYSDIR%\Files.txt
201	read file	
209	remove file	
499	list programs	Its done by enumerating HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall, results are

Command	Action	Comments
		saved to %WINSYSDIR%\Programs.txt
599	list available devices	
999	ping	sends back pong
555	get os info	sends back windows version and computer name
315	disable audio recording	
312	disable keyloger	
313	disable screenshot	
666	set unused flag	

Update 27.04.2020

Quick update regarding commands **555**, **999**, **139**

- 999 - ping
- 555 - get os info
- 139 - shut down system via godown.dll

Conclusion

In this short post we showed a capabilities of a malware used by Nazar APT, clearly designed with espionage purposes. Stay tune for next part about abusing IP and TCP protocol in order to smuggle commands. In the meantime if you have an interesting piece of malware and need someone to take a look at it don’t hesitate to contact us - contact@malwarelab.pl

---