Remcos Is Pairing with PrivateLoader to Extend Its Capabilities

Published: 2024-05-14 · Archived: 2026-04-06 03:22:34 UTC

Overview

This week, the SonicWall Capture Labs threat research team investigated a sample of the RemcosRAT that uses a PrivateLoader module to provide additional data and persistence on the victim's machine. By installing VB scripts, altering the registry and setting up services to restart the malware at variable times or by control, this malware is able to infiltrate a system completely and remain undetected.

Infection Cycle

The sample is detected as a 32-bit PE file with no packer or protector.

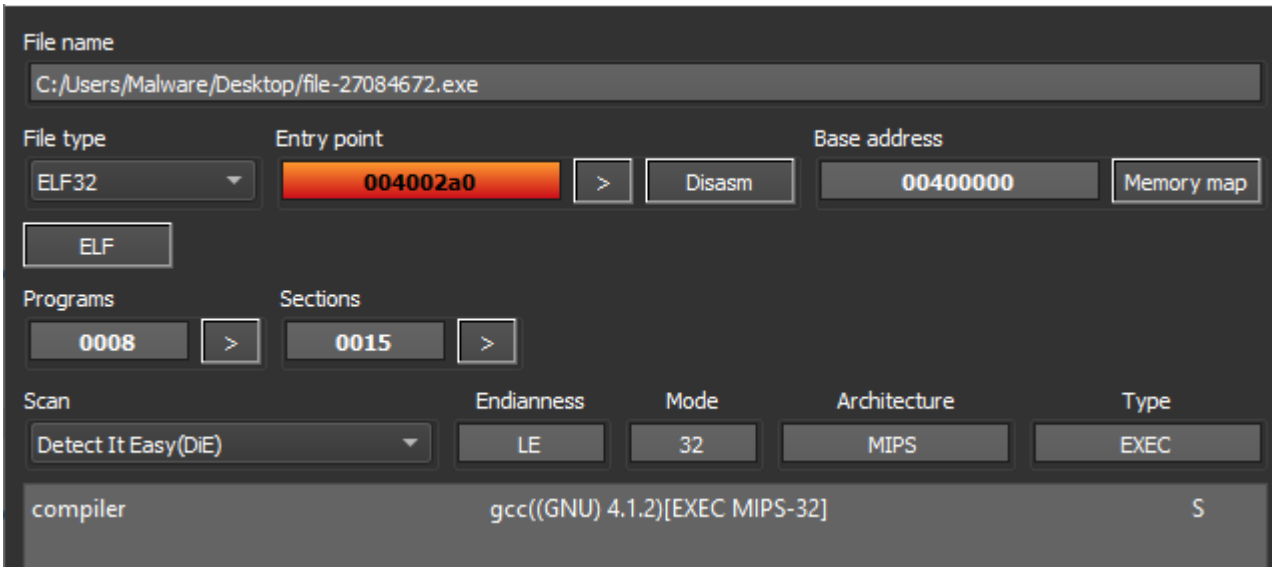
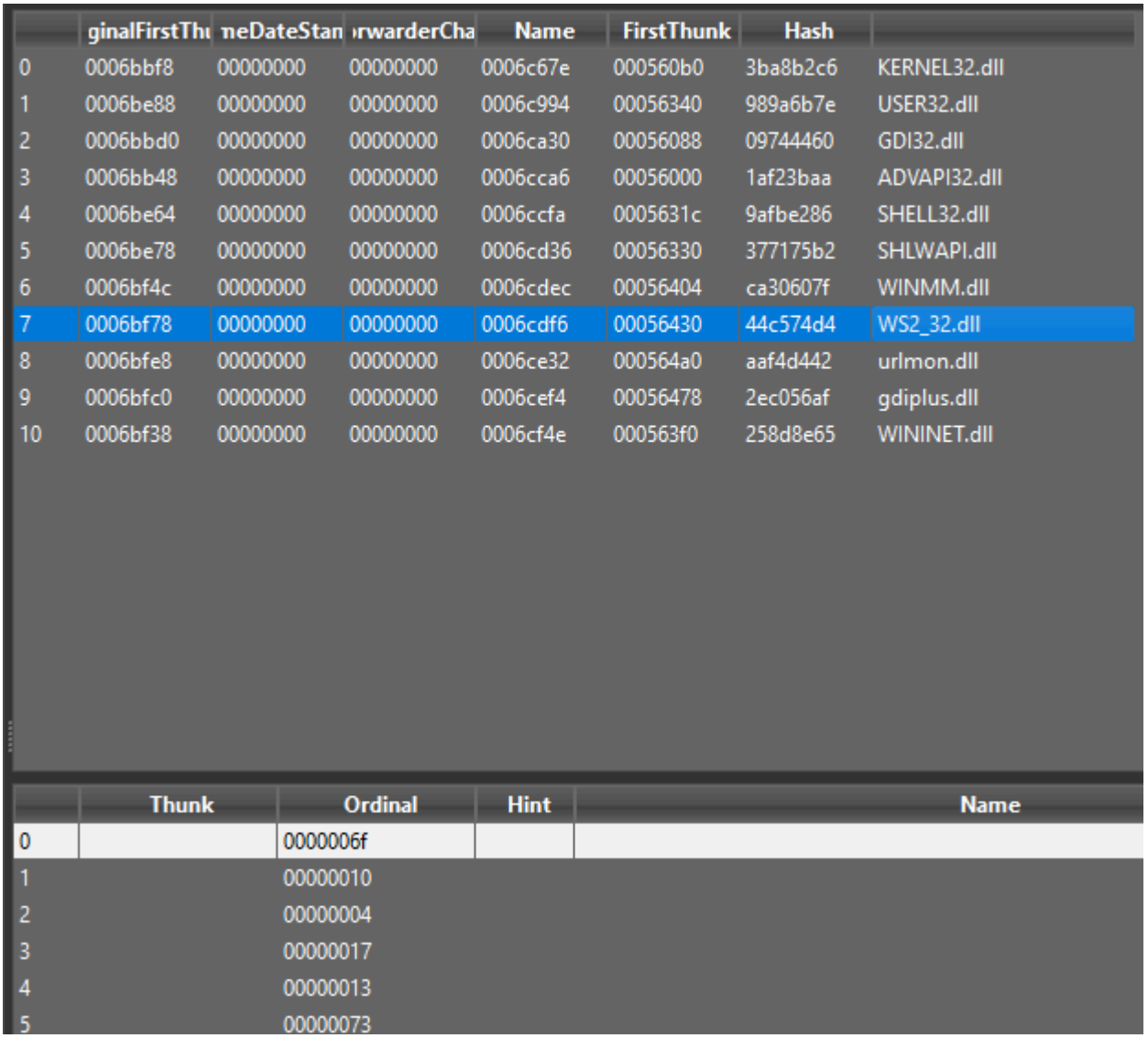


Figure 1: Initial detection

When looking into the sections and API calls of the file, different tools give different reports. Detect It Easy shows API calls that have been cleared (to obfuscate what they're doing), and TLS (Thread Local Storage) functionality, meaning that malicious code can be prepared or run before the main file has started at its entry point. PEStudio, however, shows all available API calls but no TLS functionality.



	ginalFirstThu	neDateStan	rwarderCha	Name	FirstThunk	Hash	
0	0006bbf8	00000000	00000000	0006c67e	000560b0	3ba8b2c6	KERNEL32.dll
1	0006be88	00000000	00000000	0006c994	00056340	989a6b7e	USER32.dll
2	0006bbd0	00000000	00000000	0006ca30	00056088	09744460	GDI32.dll
3	0006bb48	00000000	00000000	0006cca6	00056000	1af23baa	ADVAPI32.dll
4	0006be64	00000000	00000000	0006ccfa	0005631c	9afbe286	SHELL32.dll
5	0006be78	00000000	00000000	0006cd36	00056330	377175b2	SHLWAPI.dll
6	0006bf4c	00000000	00000000	0006cdec	00056404	ca30607f	WINMM.dll
7	0006bf78	00000000	00000000	0006cdf6	00056430	44c574d4	WS2_32.dll
8	0006bfe8	00000000	00000000	0006ce32	000564a0	aaf4d442	urlmon.dll
9	0006bfc0	00000000	00000000	0006cef4	00056478	2ec056af	gdiplus.dll
10	0006bf38	00000000	00000000	0006cf4e	000563f0	258d8e65	WININET.dll

	Thunk	Ordinal	Hint	Name
0		0000006f		
1		00000010		
2		00000004		
3		00000017		
4		00000013		
5		00000073		

Figure 2: Every call from ws2_32.dll has been obfuscated

functions (288)	blacklist (93)	anonymous (17)	library (11)
RegDeleteValueW	x	-	advapi32.dll
RegDeleteKeyA	x	-	advapi32.dll
ShellExecuteExA	x	-	shell32.dll
ShellExecuteW	x	-	shell32.dll
111 (WSAGetLastError)	x	x	ws2_32.dll
16 (recv)	x	x	ws2_32.dll
4 (connect)	x	x	ws2_32.dll
23 (socket)	x	x	ws2_32.dll
19 (send)	x	x	ws2_32.dll
115 (WSAStartup)	x	x	ws2_32.dll
3 (closesocket)	x	x	ws2_32.dll
12 (inet_ntoa)	x	x	ws2_32.dll
52 (gethostbyvalue)	x	x	ws2_32.dll
112 (WSASetLastError)	x	x	ws2_32.dll
11 (inet_addr)	x	x	ws2_32.dll
51 (gethostbyaddr)	x	x	ws2_32.dll
56 (getservbyport)	x	x	ws2_32.dll
15 (ntohs)	x	x	ws2_32.dll
55 (getservbyvalue)	x	x	ws2_32.dll
9 (htons)	x	x	ws2_32.dll
8 (htonl)	x	x	ws2_32.dll
URLDownloadToFileW	x	-	urlmon.dll
URLOpenBlockingStreamW	x	-	urlmon.dll
InternetOpenUrlW	x	-	wininet.dll
InternetCloseHandle	x	-	wininet.dll
InternetReadFile	x	-	wininet.dll
InternetOpenW	x	-	wininet.dll
CopyFileW		-	kernel32.dll
CreateMutexA		-	kernel32.dll
GetLocaleInfoA		-	kernel32.dll

Figure 3: A separate tool shows all hidden calls

Once functions are properly labeled, the file is shown to have the following capabilities:

- Anti-analysis/ Anti-VM
  - GetSystemTimeAsFileTime
  - GetTickCount
  - IsDebuggerPresent
  - IsProcessorFeaturePresent
  - QueryPerformanceCounter
  - QueryPerformanceFrequency
- System Enumeration
  - CreateToolhelp32Snapshot
  - EnumDisplaySettingsW
  - EnumServicesStatusW

    - EnumSystemLocalesW
    - EnumWindows
    - FindFirstFileA/Ex/W
    - FindNextFileA/Ex/W
    - GetClipboardData
    - GetCurrentProcessId
    - GetCurrentThreadId
    - GetEnvironmentStrings
    - GetLogicalDriveStringsA
    - GetLocalTime
    - GetLocaleInfoA/W
    - GetNativeSystemInfo
    - GetStartupInfo
    - GetTimeZoneInformation
    - GetUserDefaultLCID
    - GetWindowThreadProcessId
    - IsLocaleValid
    - OpenClipboard
    - RegEnumKeyA/W
    - RegEnumValueA/W
    - SystemParametersInfoW
- Monitoring
    - GetCursorPos
    - GetForegroundWindow
    - GetKeyState
    - GetKeyboardLayout
    - GetKeyboardState
    - Mouse_event
    - ReadProcessMemory
    - SetWindowsHookExA
    - waveInAddBuffer
    - waveInStart
- Process Injection
    - GetProcessId
    - GetModuleHandleA/Ex/W
    - CreateProcessA/W
    - Process32FirstW
    - ProcessNextW
    - VirtualAlloc
    - VirtualFree
    - VirtualProtect
    - WriteProcessMemory

- Persistence
    - AdjustTokenPrivilege
    - ControlService
    - GetTempFileNameW
    - LookupPrivilegeValueA
    - OpenProcess
    - OpenProcessToken
    - RegCreateKeyA/Ex/W
    - RegDeleteKeyA/Ex/W
    - RegDeleteValueA/Ex/W
    - RegSetValueA/Ex/W
    - ShellExecuteExA/W
    - WriteFile
- Communication
    - InternetOpenUrlW
    - InternetReadFile
    - URLDownloadToFileW
    - URLOpenBlockingStreamW
    - Inet_addr
    - Gethostbyaddr
    - Gethostbyvalue
    - getservbyvalue
    - Connect
    - Send
    - socket
    - Recv

Runtime shows that if security checks are not initially cleared by modules within ntdll.dll, the main portion of the executable will not be touched before it exits. No files are dropped, and nothing is injected into memory.

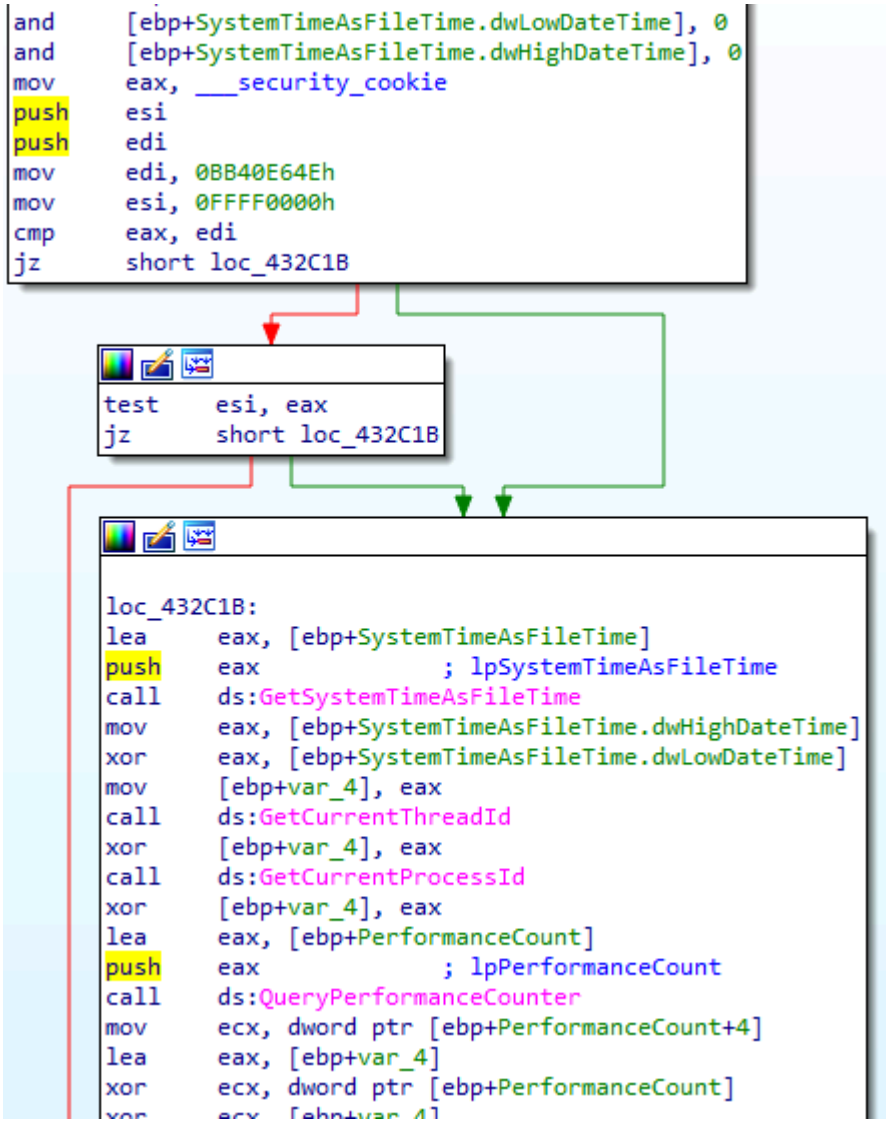


Figure 4: Beginning of the security check function

Once security has been passed, which consists of VM, locale, timezone and analysis tool enumeration, two files are dropped.

- C:\Users\user\AppData\Local\Temp\install.vbs
- C:\Users\user\AppData\Roaming\data\notepads.exe

Notepads.exe is a copy of the parent executable placed for persistence. The script contains the following four lines and is deleted once executed – there is no check on whether or not this action is successful. The script will simply delete itself if it is run before ‘notepads.exe’ is dropped.

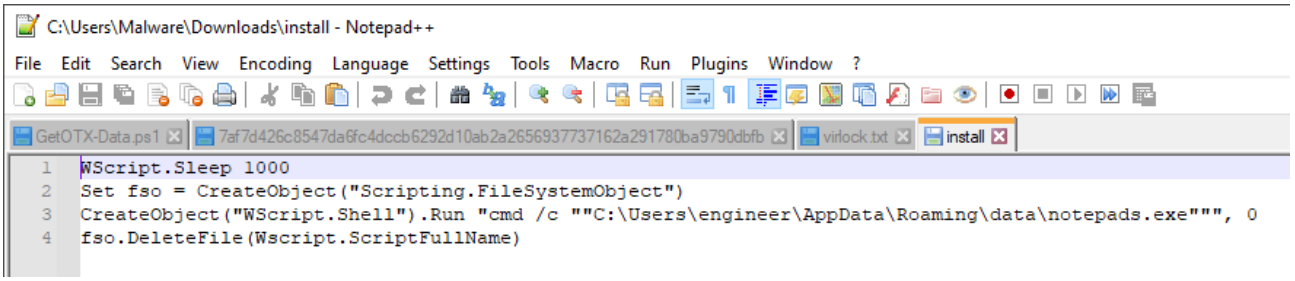


Figure 5: Install.vbs contents

User security access is then checked. If applicable, Windows User Access Control is disabled with the following command to allow for privileged access:

/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f

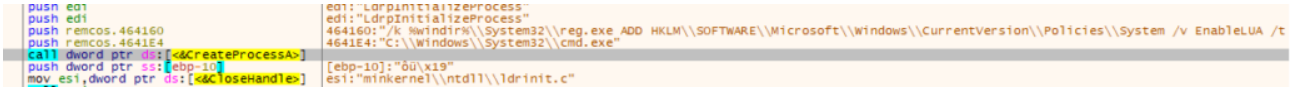


Figure 6: UAC is disabled

At this point, the system is enumerated fully and hooks are implemented to track keystrokes, mouse actions, audio and screen grabs. Targeted software includes browsers by searching the following locations for logins and cookie data, as well as the clipboard data being pulled:

\AppData\Local\Google\Chrome\User Data\Default\Login Data

\AppData\Local\Google\Chrome\User Data\Default\Cookies

\AppData\Roaming\Mozilla\Firefox\Profiles\

\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

\AppData\Local\Microsoft\Edge\

\Opera Software\Opera Stable\

\User Data\Default\Network\Cookies

This information is stored in ‘logins.json’ and ‘key3.db’, also seen in the screenshot below.

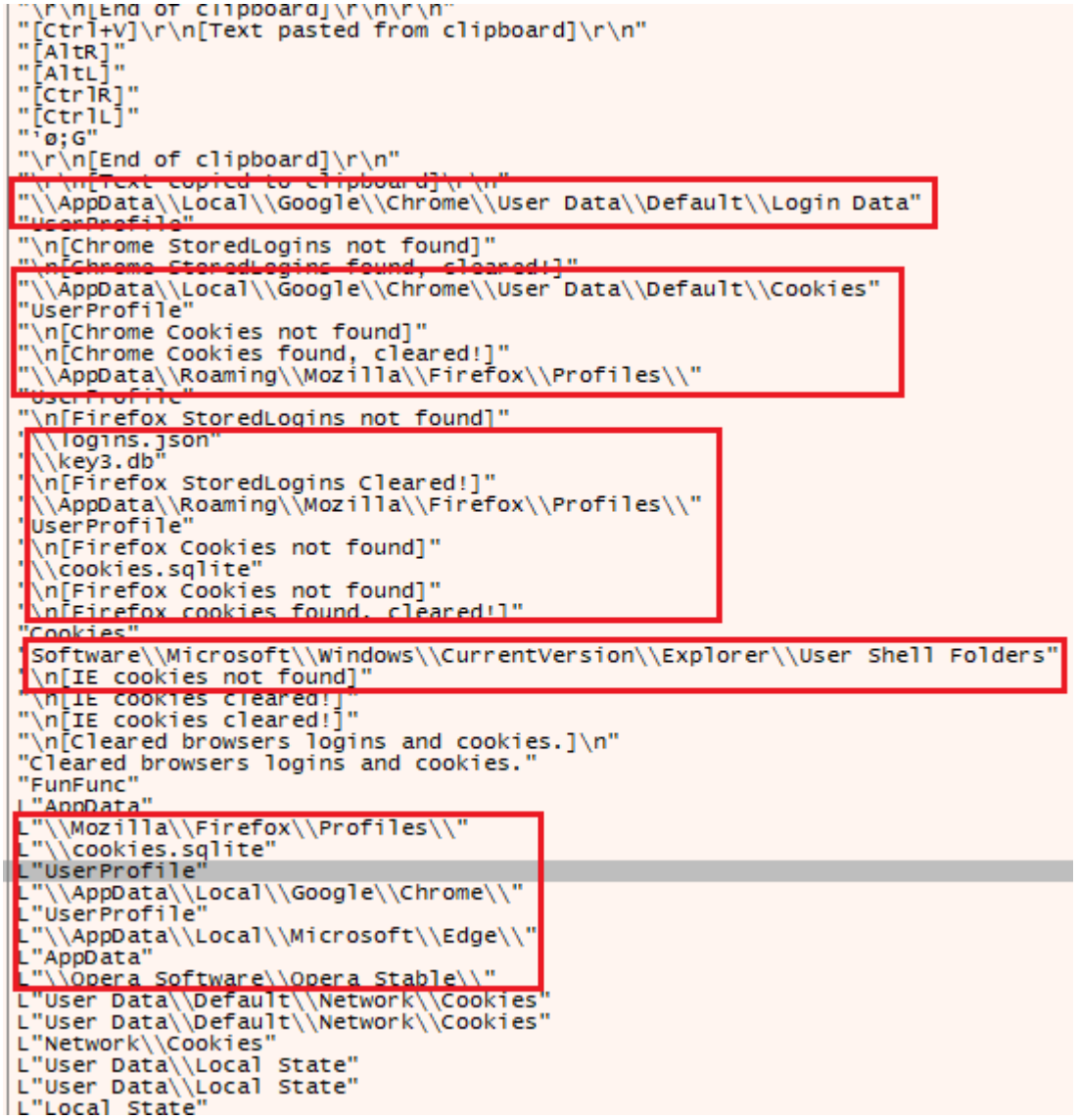


Figure 7: Browser paths and storage files

Once complete, ‘notepads.exe’ will open a socket on the system and reach out to two URLs. The first is a GET request to geoplugin(dot)net/json.gp, which returns geographic information pertaining to the victim’s IP address. The second is to nuevosremcs.duckdns.org. Once a connection is made, a config file is created and sent to the server. Here is the configuration observed during runtime:

{

"Host:Port:Password": "nuevosremcs.duckdns.org:9090:1",

"Assigned name": "Nuevos",

"Connect interval": "1",

"Install flag": "Enable",

"Setup HKCU\Run": "Enable",

"Setup HKLM\Run": "Enable",

"Install path": "AppData",

"Copy file": "notepads.exe",

"Startup value": "system32",

"Hide file": "Disable",

"Mutex": "Rmc-WRNU47",

"Keylog flag": "1",

"Keylog path": "Application path",

"Keylog file": "logs.dat",

"Keylog crypt": "Disable",

"Hide keylog file": "Disable",

"Screenshot flag": "Disable",

"Screenshot time": "10",

"Take Screenshot option": "Disable",

"Take screenshot title": "",

"Take screenshot time": "5",

"Screenshot path": "AppData",

"Screenshot file": "Screenshots",

"Screenshot crypt": "Disable",

"Mouse option": "Disable",

"Delete file": "Disable",

"Audio record time": "5"

}

At this point the C2 has assumed control and can remotely stop, start and engage further monitoring or file downloads for other functionality.

SonicWall Protections

To ensure SonicWall customers are prepared for any exploitation that may occur due to this malware, the following signatures have been released:

- PrivateLoader

IOCs

Parent sample / Notepads.exe: 27bb3968cc18fb0df5b14e6d1b805552

Install.vbs: a7fe45cc57afb3dba91ab77483fffa0a

Mutex Created

- \Sessions\1\BaseNamedObjects\Rmc-WRNU47

IP Addresses

- 246.82.10
- 237.33.50

URLs

- http://geoplugin.net/json.gp
- duckdns.org
