SECTRIO

MALWARE REPORT

Agent Tesla: Credential Stealer

Date: 19/02/2021

Meghraj Nandanwar

Agent Tesla is spyware, keylogger, and information stealer Trojan written in Microsoft's .NET language. Agent Tesla has been observed in the world since 2014, and has been active ever since. Agent Tesla is also a commercial project, whose subscription license is sold on its official website.

Overview

Agent Tesla is a Spyware that is used to spy on the victims by collecting system clipboard, credentials and other information from the infected system. New variants of the popular Agent Tesla Trojan steal credentials from target popular applications, including Google Chrome, Mozilla Firefox, Mozilla Thunderbird, Microsoft Edge, etc. It uses Process Hollowing to inject a malicious payload into the running process and can send the harvested data to command control via SMTP or FTP.

Analysis

- **Packed and Obfuscation**

The executable is packed with .NET Framework and there are only a few details available in static analysis (figure.1). We can see the Entropy of the executable file is very high which shows that the file is packed (figure.2). It also uses Delay Execution to trick the automated dynamic analysis tools (Figure.3) and also detects the virtual environment by abusing WMI to get the system information.

library (1)	blacklist (0)	type (1)	imports (1)	description
mscoree.dll	-	implicit	1	Microsoft .NET Runtime Execution Engine

name (1)	group (0)	type (1)	ordinal (0)	blacklist (0)
_CorExeMain	-	implicit	-	-

Figure 1: Library and Import Table

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy
.text	8192	661512	662016	7.74
.rsrc	671744	1544	2048	3.5
.reloc	679936	12	512	0.1

Figure 2: Entropy

Process	PID
RegSvcs.exe	1852

C:\Users\Meghraj\

#	Time of Day	Thread	Module	API
1	3:14:10.736 AM	1	clr.dll	SleepEx (71396, TRUE)
2	3:14:10.736 AM	1	KERNELBASE.dll	NtDelayExecution (TRUE, 0x010fdf1c)
3	3:15:22.278 AM	1	clr.dll	SleepEx (10000, TRUE)
4	3:15:22.278 AM	1	KERNELBASE.dll	NtDelayExecution (TRUE, 0x010fda54)

Figure 3: Sleep and Delay Execution

- **Injection Flow**

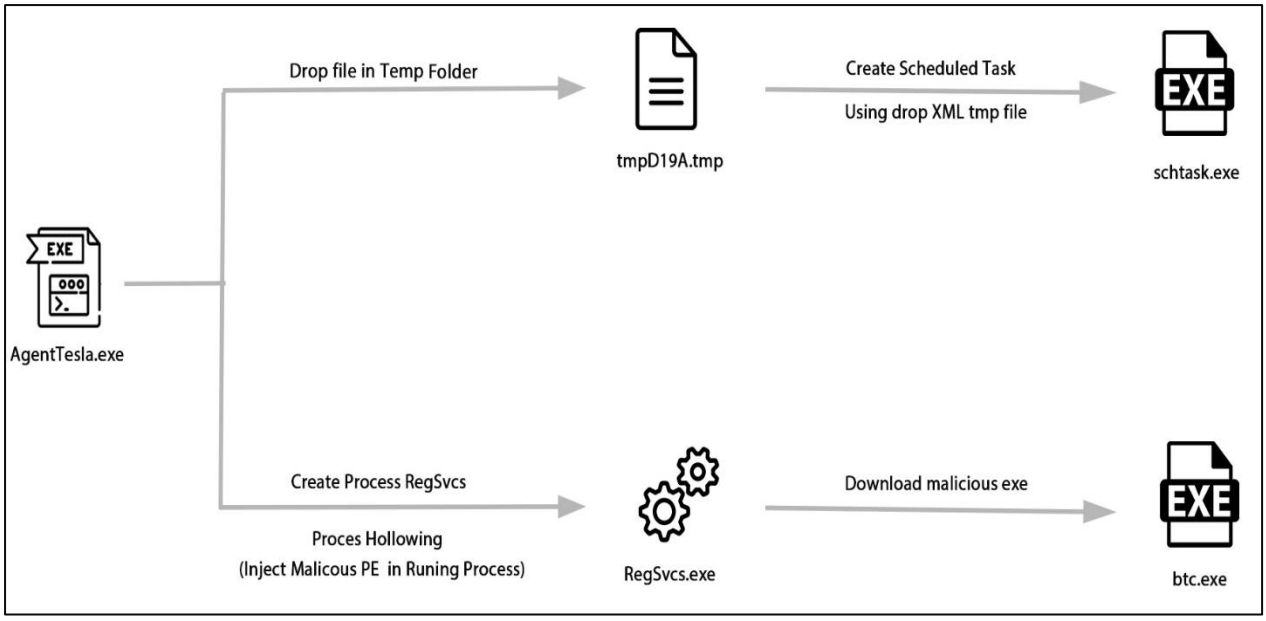


Figure 4: Injection Flow

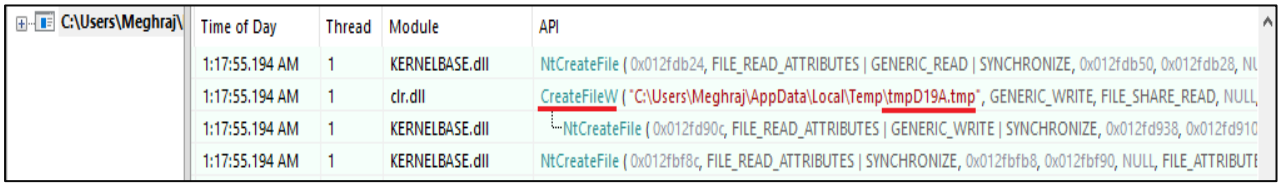


Figure 5: APIs used for creating file

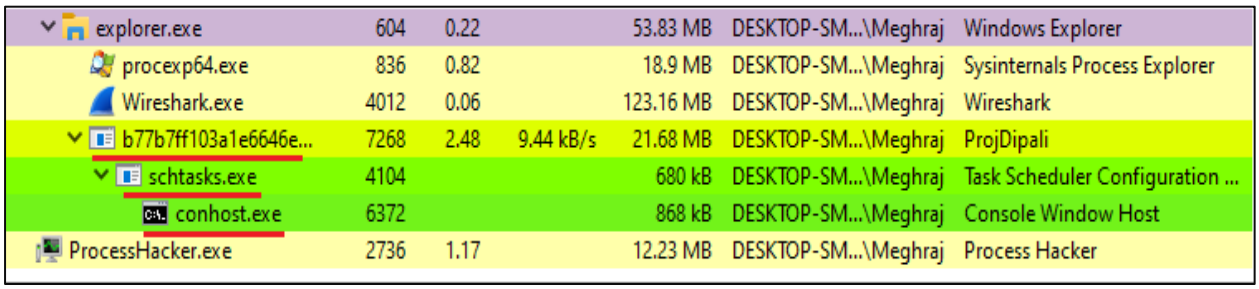


Figure 6: Creating Scheduled task for execution

- **Process Hollowing**

Agent Tesla using the process hollowing to inject malicious PE file into the running process (Figure.7).

C:\Users\Meghraj\

#	Time of Day	Thread	Module	API
578	1:17:55.303 AM	1	clr.dll	VirtualAlloc (NULL, 65536, MEM_COMMIT, PAGE_READWRITE)
579	1:17:55.303 AM	1	clr.dll	CreateProcessA ("C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe", "", NULL, NULL, FALSE
580	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x008c21e8, 0x012fcd78, 4, NULL)
581	1:17:55.319 AM	1	clr.dll	VirtualAllocEx (0x0000066c, 0x00400000, 245760, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READ
582	1:17:55.319 AM	1	clr.dll	WriteProcessMemory (0x0000066c, 0x00400000, 0x055b1270, 512, 0x012fdd20)
583	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x00400000, 0x055b1270, 512, 0x012fd9d4)
584	1:17:55.319 AM	1	clr.dll	WriteProcessMemory (0x0000066c, 0x00402000, 0x054a1e00, 216576, 0x012fdd20)
585	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x00402000, 0x054a1e00, 216576, 0x012fd9d4)
586	1:17:55.319 AM	1	clr.dll	WriteProcessMemory (0x0000066c, 0x00438000, 0x0432c258, 1536, 0x012fdd20)
587	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x00438000, 0x0432c258, 1536, 0x012fd9d4)
588	1:17:55.319 AM	1	clr.dll	WriteProcessMemory (0x0000066c, 0x0043a000, 0x0432c864, 512, 0x012fdd20)
589	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x0043a000, 0x0432c864, 512, 0x012fd9d4)
590	1:17:55.319 AM	1	clr.dll	WriteProcessMemory (0x0000066c, 0x008c2008, 0x0432ca70, 4, 0x012fdd20)
591	1:17:55.319 AM	1	KERNELBASE.dll	NtWriteVirtualMemory (0x0000066c, 0x008c2008, 0x0432ca70, 4, 0x012fd9d4)
592	1:17:55.319 AM	1	KERNELBASE.dll	NtResumeThread (0x00000550, 0x012fdb00)
593	1:17:55.319 AM	1	KERNELBASE.dll	NtResumeThread (0x00000530, 0x012fd8f8)

Figure 7: Process Hollowing

```
; Attributes: bp-based frame

kernel32_CreateProcessA proc near
mov     edi, edi
push    ebp
mov     ebp, esp
pop     ebp
jmp     off_75BB14F4
kernel32_CreateProcessA endp
```

Figure 8: Create Process

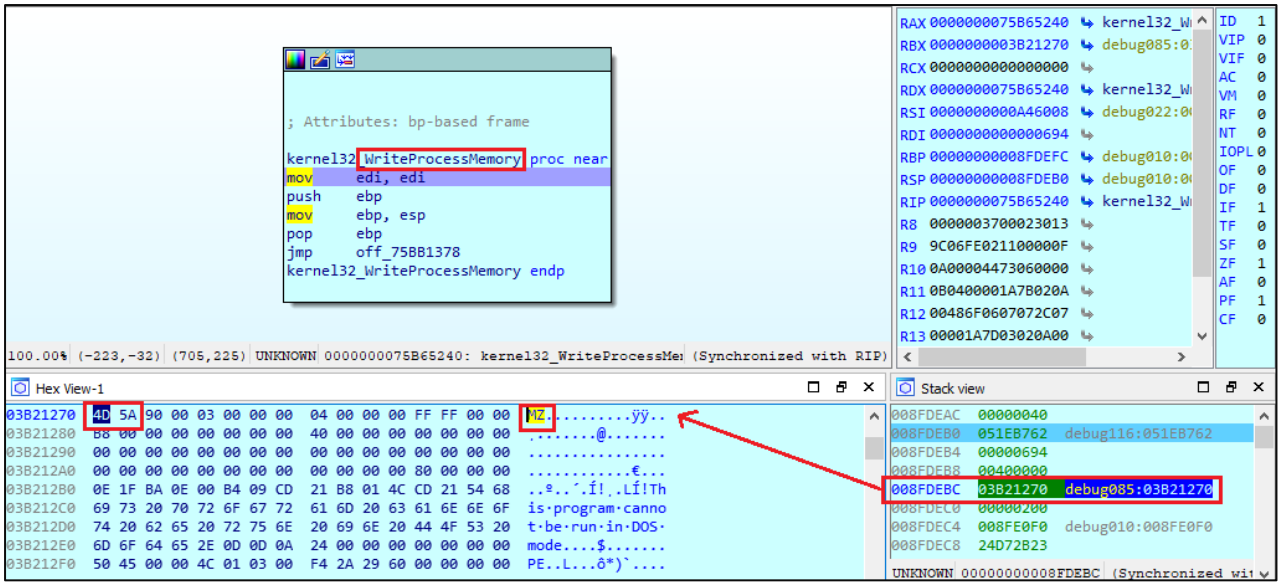
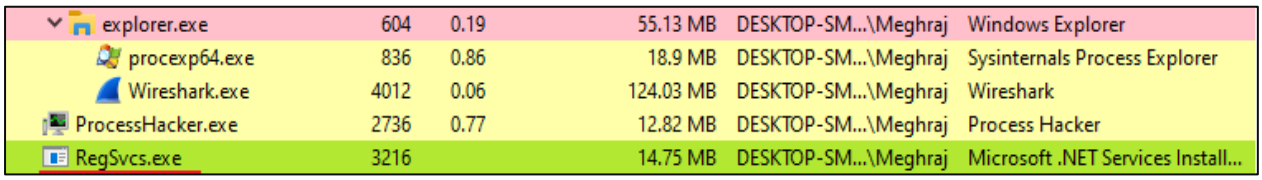


Figure 9: Injecting Malicious Payload

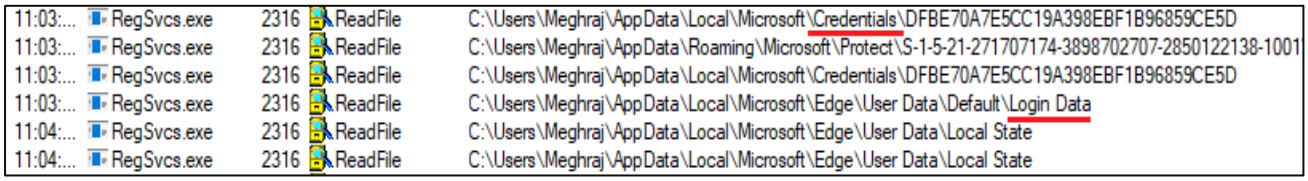
- After Injecting Malicious payload into RegSvcs.exe, packed malware process terminates itself. Malwares do this to hide themselves.



explorer.exe	604	0.19	55.13 MB	DESKTOP-SM...\Meghraj	Windows Explorer
procexp64.exe	836	0.86	18.9 MB	DESKTOP-SM...\Meghraj	Sysinternals Process Explorer
Wireshark.exe	4012	0.06	124.03 MB	DESKTOP-SM...\Meghraj	Wireshark
ProcessHacker.exe	2736	0.77	12.82 MB	DESKTOP-SM...\Meghraj	Process Hacker
RegSvcs.exe	3216		14.75 MB	DESKTOP-SM...\Meghraj	Microsoft .NET Services Install...

Figure 10: Injected Malicious Process

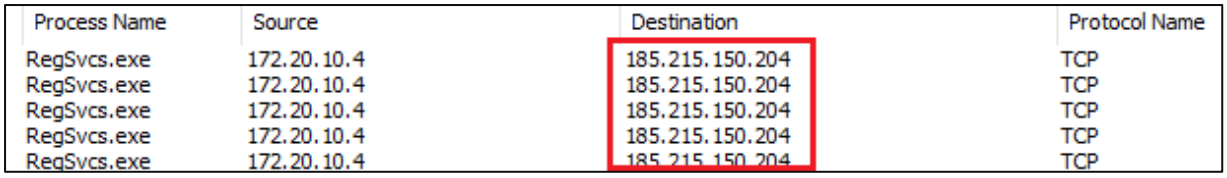
- **Credential Stealing**
  Injected malicious process reading the files which stores the credential of the user. Agent Tesla has the capability to steal credentials of various applications such as Browser, Mail, FTP, etc.



11:03:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
11:03:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Roaming\Microsoft\Protect\S-1-5-21-271707174-3898702707-2850122138-1001
11:03:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
11:03:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Local\Microsoft\Edge\User Data\Default\Login Data
11:04:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Local\Microsoft\Edge\User Data\Local State
11:04:...	RegSvcs.exe	2316	ReadFile	C:\Users\Meghraj\AppData\Local\Microsoft\Edge\User Data\Local State

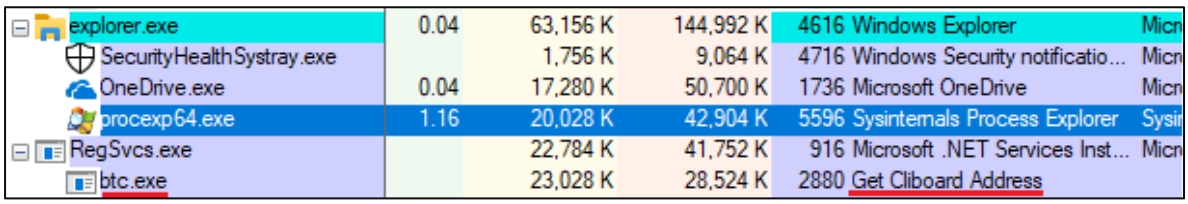
Figure 11: Reading Credentials stored in local computer.

- RegSvcs.exe downloads the malicious executable btc.exe from the IP address 185.215.150.204.



Process Name	Source	Destination	Protocol Name
RegSvcs.exe	172.20.10.4	185.215.150.204	TCP
RegSvcs.exe	172.20.10.4	185.215.150.204	TCP
RegSvcs.exe	172.20.10.4	185.215.150.204	TCP
RegSvcs.exe	172.20.10.4	185.215.150.204	TCP
RegSvcs.exe	172.20.10.4	185.215.150.204	TCP

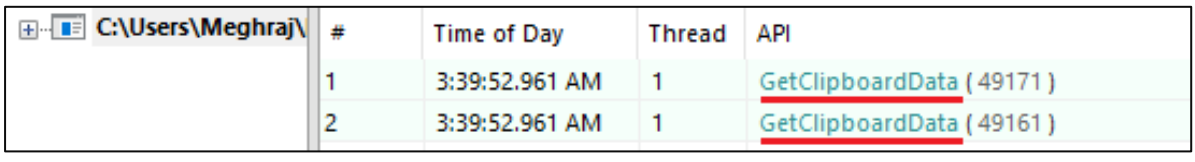
Figure 12: Network Activity



explorer.exe	0.04	63,156 K	144,992 K	4616 Windows Explorer	Micr
SecurityHealthSystray.exe		1,756 K	9,064 K	4716 Windows Security notificatio...	Micr
OneDrive.exe	0.04	17,280 K	50,700 K	1736 Microsoft OneDrive	Micr
procexp64.exe	1.16	20,028 K	42,904 K	5596 Sysinternals Process Explorer	Sysi
RegSvcs.exe		22,784 K	41,752 K	916 Microsoft .NET Services Inst...	Micr
btc.exe		23,028 K	28,524 K	2880 Get Cliboard Address	

Figure 13: Malicious Executable

- btc.exe reads the content of the clipboard to acquire all the data victim copied in their clipboard.



C:\Users\Meghraj\

#	Time of Day	Thread	API
1	3:39:52.961 AM	1	GetClipboardData (49171)
2	3:39:52.961 AM	1	GetClipboardData (49161)

Figure 14. API used by btc.exe to get clipboard data.

- Sending Harvested data from the infected system to command control via SMTP.

RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	172.20.10.4	mail.hermanusbearings.co.za	TCP
RegSvcs.exe	mail.hermanusbearings.co.za	172.20.10.4	TCP

Figure 15: Command Control

Network Activity

Activity	Address	Protocol
Download Malicious Payload	185.215.150.204	HTTP
Send Harvested Credential	mail.hermanusbearings.co.za	SMTP

Sample Details

File	Hash Value (MD5)
Packed Sample	B77B7FF103A1E6646E7525A5D4CFDEE9
RegSvcs.exe	2867A3817C9245F7CF518524DFD18F28
btc.exe	ABE8943DEA79BFECB7728DEB44846FE3

MITRE Attack Techniques

TACTIC	ID	NAME
Execution	T1047	Windows Management Instrumentation
Persistence	T1053	Scheduled Task/Job
Persistence	T1547.001	Registry Run Key / Startup Folder
Defense Evasion	T1055	Process Injection
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1027.002	Software Packing
Defense Evasion	T1497	Virtualization/Sandbox Evasion
Credential Access	T1003	OS Credential Dumping
Discovery	T1082	System Information Discovery
Collection	T1005	Data from Local System
Collection	T1114	Email Collection
Collection	T1115	Clipboard Data
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1573	Encrypted Channel

Sectrio Protection

Sectrio detects the Spyware-Trojan malware as 'SS_AI_Trojan_PE'.

Our Honeypot Network

This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 72 cities across the world. These cities have at least one of the following attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 12 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Sectrio. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.