BandarChor Ransomware

Created by:
Sudhanshu Tarale
UFID: 66177686
starale@ufl.edu
26th April, 2022

Executive Summary

- This is a ransomware with sha256 hash **CA805825DCAF51D1C45C71258F8AB2A67C4C880A1F252E1CD470832F7F867B54.**
- It is a ransomware. It encrypts the files of the user and once they try to open them, it will show a ransom message with an email id to contact.
- The malware makes changes to the keyboard layout as it makes changes to the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout** registry key.
- Makes changes to **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager** registry key. This registry key contains a list of commands to run before loading services. The malware can use this and run some malicious commands before a process starts to perhaps maintain persistence or take advantage of the functionalities that the service offers.
- **HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName** is also changed. The malware might be attempting to change the name of the local system.

Executive Summary

- Persistence is employed by the malware. It copies itself into the **C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup** folder. The script in this folder states the programs that should run when a user logs in.

7:35:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
7:35:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
7:35:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
7:35:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS

Static Analysis

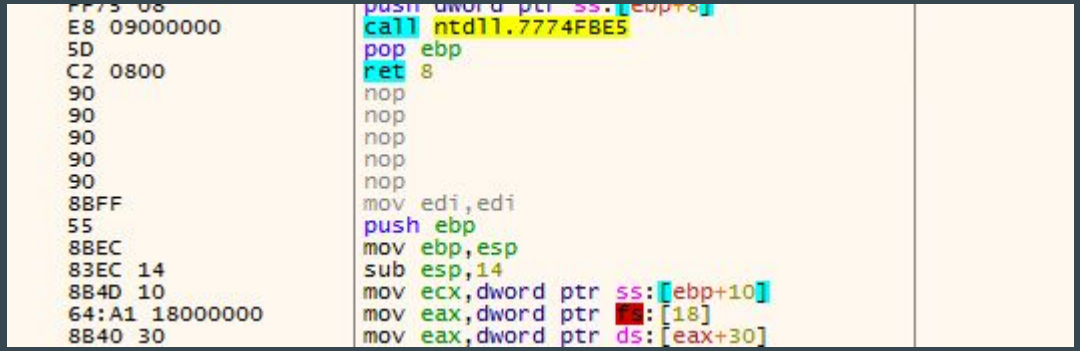
- Compilation date of the malware is **December 17th, 2014 at 15:58:25**.
- Some suspicious strings:
  - **DragFinish:** Releases memory that the system allocated for use in transferring file names to the application. Malware can use this to manipulate memory.
  - **MDIForm1,MDIForm:** MDI (Multiple-document interface) are applications that display documents to the user. In this case, we can guess that the malware is trying to display a form. Maybe it is to steal credentials by user entering it in the form or just to display some information, a message for example.
  - **SQLGetConnectAttr** gets the current settings of a connection. This further also tells us that the malware is working with SQL; maybe establishing a connection to a server.
  - **PEC2TO** is the abbreviation for PECompact packer. These are signs that the malware is packed.
  - **FastMM Borland Edition** and **2004, 2005 Pierre le Riche / Professional Software Development**: FastMM is a replacement memory manager for Embarcadero Delphi applications. This software can keep a check on the memory and it's options can be used to manipulate the memory (delete, lock, more performance, less performance etc.) Pierre le Riche is the guy who wrote this software.

Static Analysis

- Suspicious Strings (contd.):
  - **An unexpected memory leak has occurred** shows us that the malware is working with the memory of the machine being attacked.
  - **GetDiskFreeSpaceExA** retrieves information about the amount of space that is available on a disk volume.
  - **\System\currentcontrolset\control\keyboard layout:** This is a registry key which let's a user program the keyboard according to their use. For example, the key can be used to reprogram the keyboard to block the delete button from working.
  - **EIdCannotSetIPVersionWhenConnected, TIdTCPClient, BoundIP<, BoundPort<** tells us that the malware is trying to connect to some network or server.
  - **decode@india.com** seems to be an email that the attacker gives for ransom payments.
  - **ODBC32:** ODBC is an SQL administrator tool that the malware might be using to get access to the SQL server.

Static Analysis

- NOP Sled: While going through the code, we can see NOP sled. NOP sleds is a famous technique for exploiting stack buffer overflow. NOP sleds also make the malware more robust since the exact address we are aiming for may change slightly depending on the system.



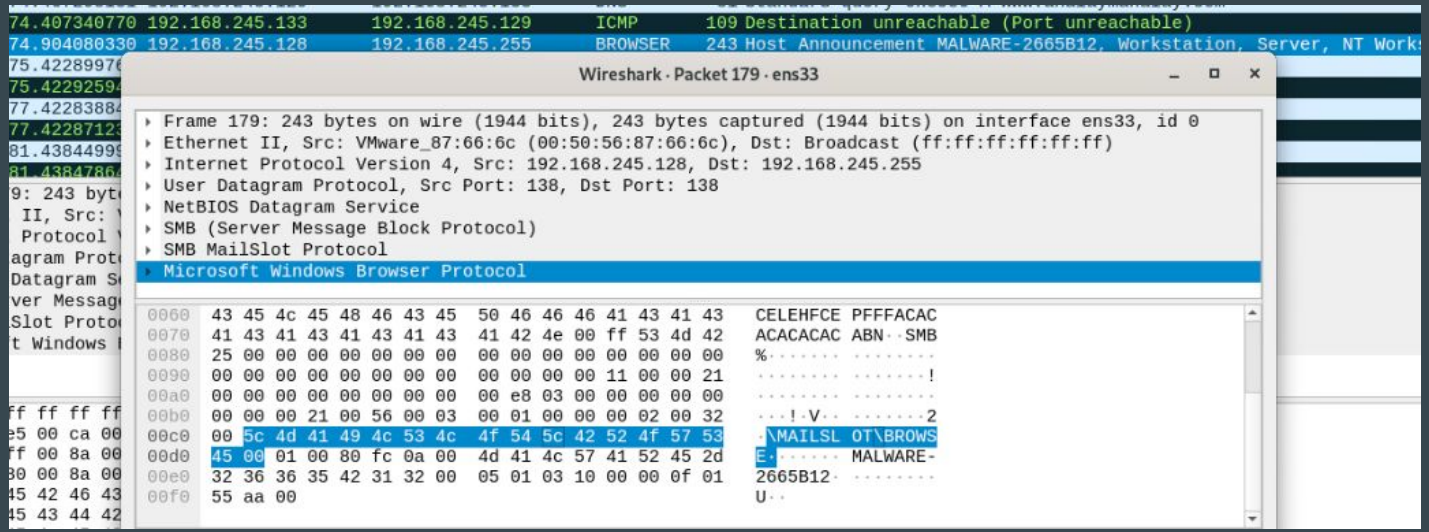
Dynamic Analysis

- Network Calls:
  - The malware contacts a certain ahalyamahalya.com

	Time	Source	Destination	Protocol	Length	Info
25	24.922610162	192.168.245.129	192.168.245.133	DNS	81	Standard query 0xabdf A www.ahalaymahalay.com
26	24.922652661	192.168.245.133	192.168.245.129	ICMP	109	Destination unreachable (Port unreachable)
27	28.924534074	192.168.245.129	192.168.245.133	DNS	81	Standard query 0x2b84 A www.ahalaymahalay.com
28	28.924570582	192.168.245.133	192.168.245.129	ICMP	109	Destination unreachable (Port unreachable)
29	29.938271062	192.168.245.129	192.168.245.133	DNS	81	Standard query 0x2b84 A www.ahalaymahalay.com
30	29.938311738	192.168.245.133	192.168.245.129	ICMP	109	Destination unreachable (Port unreachable)
31	30.938241026	192.168.245.129	192.168.245.133	DNS	81	Standard query 0x2b84 A www.ahalaymahalay.com

Dynamic Analysis

- Network Calls:
  - There is also a backup list request in wireshark which shows SMB MAILSLOT BROWSER in it's data. Mailslot is an interprocess communication method for Windows systems. One of its uses is that it can show messages as a pop up to the user.



Dynamic Analysis

- Analysis of the code: When we dump the .rsrc section of the ntdll.dll file via Ollydbg, we can see references to BitLocker Drive Encryption software and some error messages related to the local memory of the system.

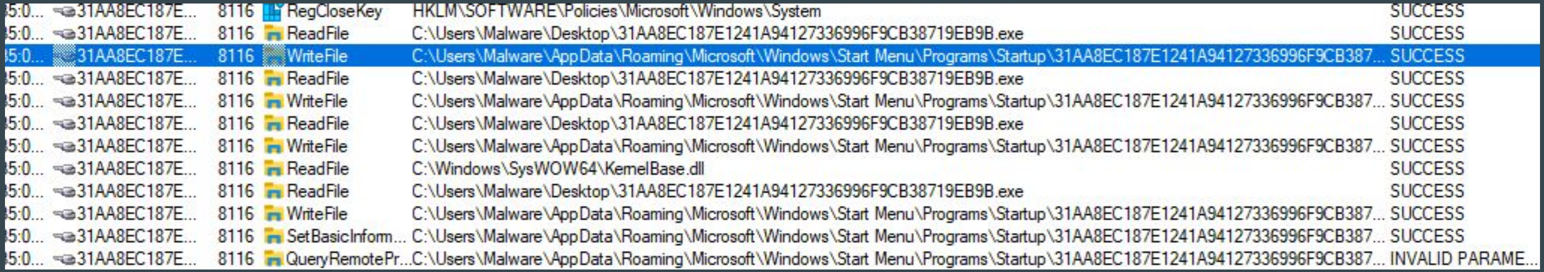
Dynamic Analysis

- Analysis of the code: When we dump the .rsrc section of the msvbvm60.dll file via Ollydbg, we can see that there are many blacklisted functions pertaining to credentials and cryptographic keys are being used.

file-offset	blacklist (643)	hint (43)	value (2563)
0x0000CC4F	x	-	CredProtect
0x0000CC5C	x	-	CredProtect
0x0000CC69	x	-	CredRead
0x0000CC89	x	-	CredReadDomainCredentials
0x0000CCA4	x	-	CredReadDomainCredentials
0x0000CCBF	x	-	CredRead
0x0000CCE0	x	-	CredUnmarshalCredential
0x0000CCF9	x	-	CredUnmarshalCredential
0x0000CD12	x	-	CredUnprotect
0x0000CD21	x	-	CredUnprotect
0x0000CD30	x	-	CredWrite
0x0000CD3B	x	-	CredWriteDomainCredentials
0x0000CD57	x	-	CredWriteDomainCredentials
0x0000CD73	x	-	CredWrite
0x0000CD7E	x	-	CryptAcquireContext
0x0000CD9F	x	-	CryptAcquireContext
0x0000CDC7	x	-	CryptCreateHash
0x0000CDD7	x	-	CryptDecrypt
0x0000CDE4	x	-	CryptDeriveKey
0x0000CDF3	x	-	CryptDestroyHash
0x0000CE04	x	-	CryptDestroyKey

Dynamic Analysis

- Persistence of Malware: Here we can see that the malware copies itself into the C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup folder. This ensures that a particular program runs when a user logs in.



5:0...	31AA8EC187E...	8116	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\System	SUCCESS
5:0...	31AA8EC187E...	8116	ReadFile	C:\Users\Malware\Desktop\31AA8EC187E1241A94127336996F9CB38719EB9B.exe	SUCCESS
5:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
5:0...	31AA8EC187E...	8116	ReadFile	C:\Users\Malware\Desktop\31AA8EC187E1241A94127336996F9CB38719EB9B.exe	SUCCESS
5:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
5:0...	31AA8EC187E...	8116	ReadFile	C:\Users\Malware\Desktop\31AA8EC187E1241A94127336996F9CB38719EB9B.exe	SUCCESS
5:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
5:0...	31AA8EC187E...	8116	ReadFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
5:0...	31AA8EC187E...	8116	ReadFile	C:\Users\Malware\Desktop\31AA8EC187E1241A94127336996F9CB38719EB9B.exe	SUCCESS
5:0...	31AA8EC187E...	8116	WriteFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
5:0...	31AA8EC187E...	8116	SetBasicInform...	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	SUCCESS
5:0...	31AA8EC187E...	8116	QueryRemotePr...	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\31AA8EC187E1241A94127336996F9CB387...	INVALID PARAME...

Indicators of Compromise

- Host based:
  - Registry keys like **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout, HKLM\SYSTEM\CurrentControlSet\Control\Session Manager, HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName are being changed.**
  - Files created/modified:

```
-----------------------------------
Files added: 1
-----------------------------------
C:\Windows\Prefetch\31AA8EC187E1241A94127336996F9-66FABBD6.pf

-----------------------------------
Files [attributes?] modified: 21
-----------------------------------
C:\Windows\appcompat\Programs\Amcache.hve.LOG2
C:\Windows\Prefetch\AgG1UAD_P_S-1-5-21-39733034-3216902470-2998706464-1000.db
C:\Windows\Prefetch\AgG1UAD_S-1-5-21-39733034-3216902470-2998706464-1000.db
C:\Windows\Prefetch\DLLHOST.EXE-4B6CB38A.pf
C:\Windows\Prefetch\PROCEXP64.EXE-657252EC.pf
C:\Windows\Prefetch\PROCMON64.EXE-E3378748.pf
C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-69C456C3.pf
C:\Windows\Prefetch\SVCHOST.EXE-47D06EA1.pf
C:\Windows\Prefetch\WMIPRVSE.EXE-E8B8DD29.pf
C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG2
C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG1
C:\Windows\System32\config\DEFAULT.LOG2
C:\Windows\System32\config\SYSTEM.LOG2
C:\Windows\System32\drivers\PROCMON24.SYS
C:\Windows\System32\wbem\Repository\INDEX.BTR
C:\Windows\System32\wbem\Repository\MAPPING2.MAP
C:\Windows\System32\wbem\Repository\OBJECTS.DATA
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
C:\Windows\System32\winevt\Logs\Security.evtx
C:\Windows\System32\winevt\Logs\System.evtx
```

Indicators of Compromise

- Network based:
  - Trying to contact www.ahalyamahalya.com
  - Packets of protocol BROWSER are being sent by the malware where the MAILSLOT functionality of windows is being used. A functionality which can show messages to the user that can be malicious.

YARA Rule

```
rule bandarchor_ransomware
{

meta:
        description="YARA Rule to detect bandarchor malware"
strings:
        $a="MSVBVM60.DLL"
        $b="MDIForm1"
        $c=" www.ahalyamahalya.com"

condition:
        ($a or $b or $c)
}
```

Thank you