Avaddon Ransomware: Incident Response Analysis

swascan.com/it/avaddon-ransomware/

December 28, 2020

Avaddon Ransomware: Introduzione

Avaddon Ransomware: Il Cyber **Incident Response** Team di Swascan ha analizzato la nuova famiglia di ransomware Avaddon. La prima comparsa relativa ad Avaddon risale ai primi mesi di quest'anno ma ultimamente ha incrementato la sue attività anche attraverso un "affiliation program". Infatti Avaddon rientra nei servizi Ransomware as a Service (RaaS). Come per Revil, Sodinokibi e Ryuk il gruppo criminale mette a disposizione il codice del malware, tool e strumenti a terze parti garantendosi una commissione sul "profitto" illegale ottenuto dai loro "clienti".

Un Business Model che sempre più spesso è sfruttato e utilizzato dai gruppi criminali autori di ransomware. Questo approccio permette loro di incrementare gli utili concentrandosi sull'evoluzione e aggiornamenti del codice, in questo caso del ransomware Avaddon.

Sotto attacco **Ransomware?**
Contattaci

Di seguito verranno approfonditi i seguenti temi

1. **Sintesi**
2. **Esfiltrazione dei Dati**
3. **Riscatto**
4. **Pasei Target**
5. **Sintomi**
6. **Vettori di Attacco**
7. **Modalità di attacco**
8. **Decriptazione dei dati**
9. **IoC**
10. **Incident Management**

Ransomware Avaddon: Sintesi

Nome	Avaddon
File	I file vengono modificati con estensione **.avdn**
Famiglia	Ransomware
Riscatto	Il riscatto di Avaddon è in README.txt (README.txt.avdn)

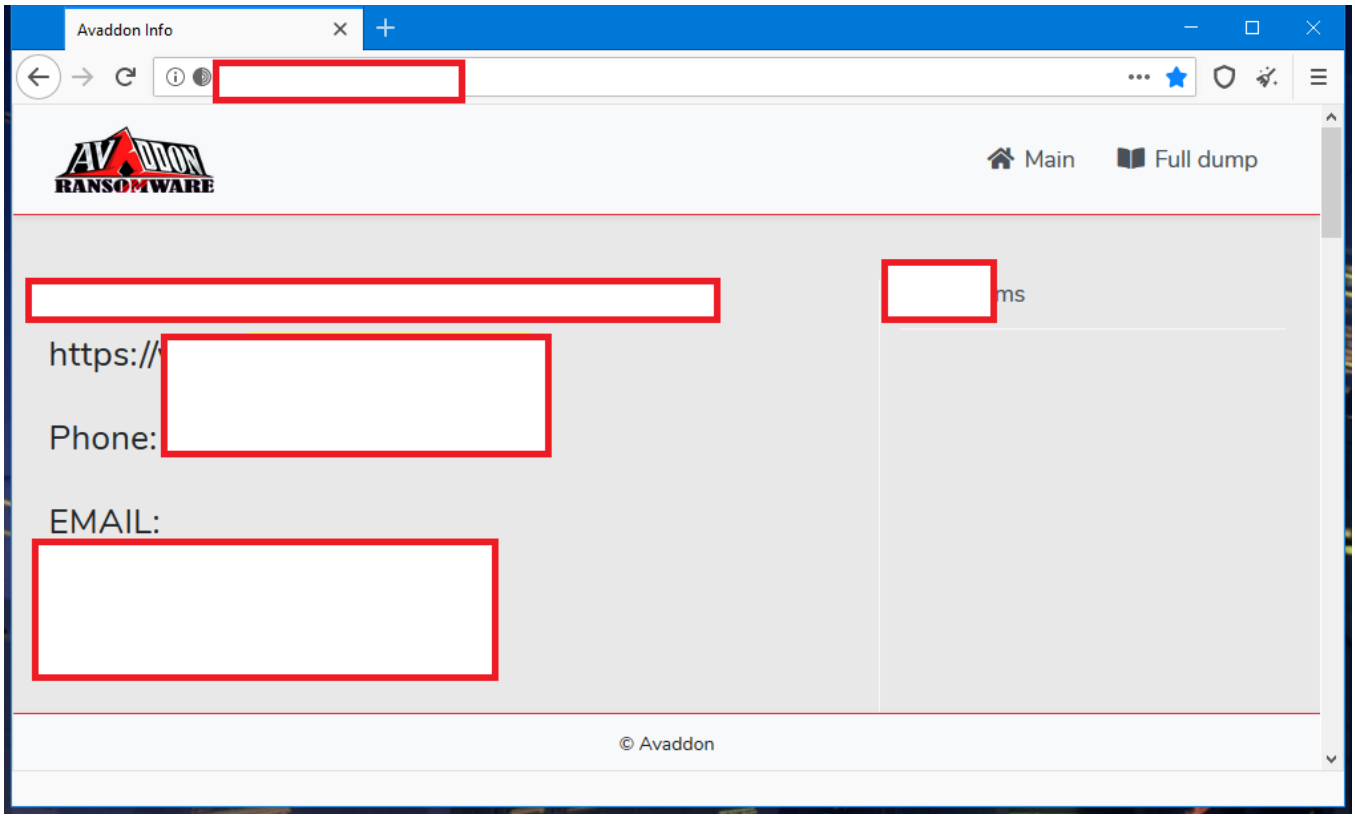
Descrizione	Crittografa dispositivi con criptografia AES e crittografa la chiave AES usando l'algoritmo RSA.
Sintomi	I file crittografati dal ransomware Avaddon hanno l'estensione file **.avdn**.
Distribuzione	Malspam, phishing, allegati email Email spam, Allegati e-mail, I file eseguibili

Ransomware Avaddon: Esfiltrazione

In caso di Data Breach causato da un cyber attack con Avaddon oltre alla crittografia dei target, è avvenuta anche l'esfiltrazione dei dati.

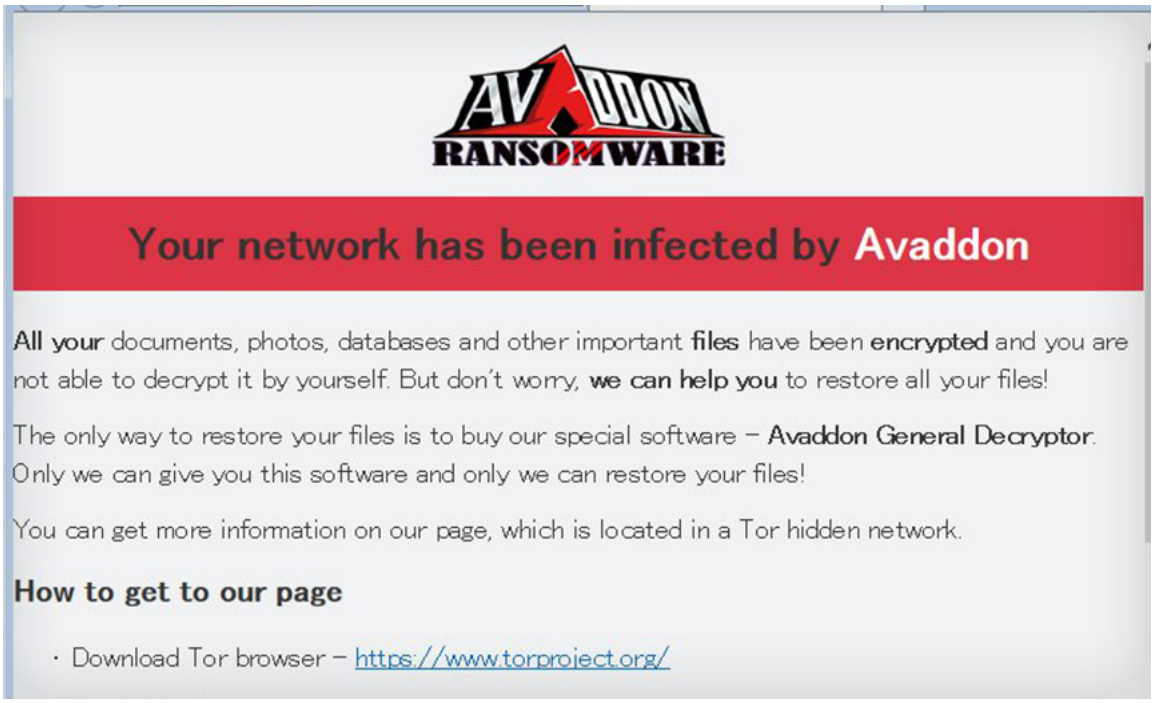
Nello specifico:

1. Esfiltrazione delle informazioni
2. Crittografia dei file
3. Possibilità di customizzare , ottimizzare e compilare il payload.
4. Pubblicazione files esfiltrati all'interno di un blog onion se non viene effettuato il pagamento previsto dal ricatto.

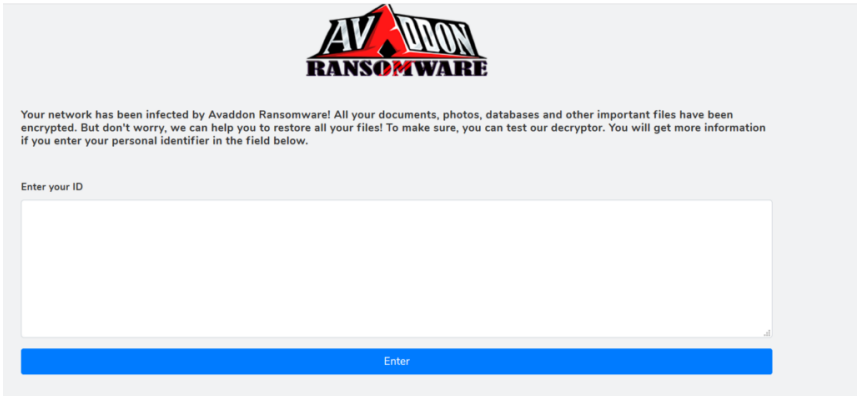


Avaddon: Richiesta di Riscatto

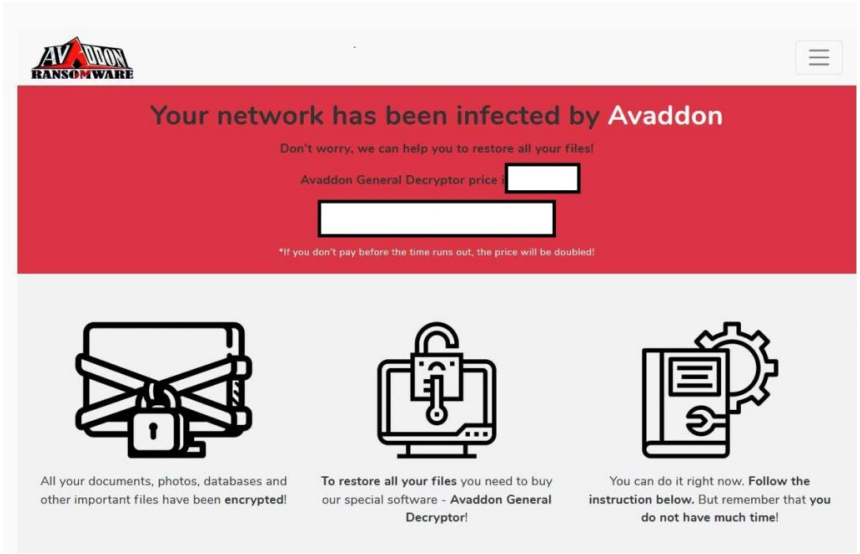
La richiesta è presente nel file **README.txt** ed invita la vittima ad accedere al sito nel dark web dei criminal hacker di Avaddon.

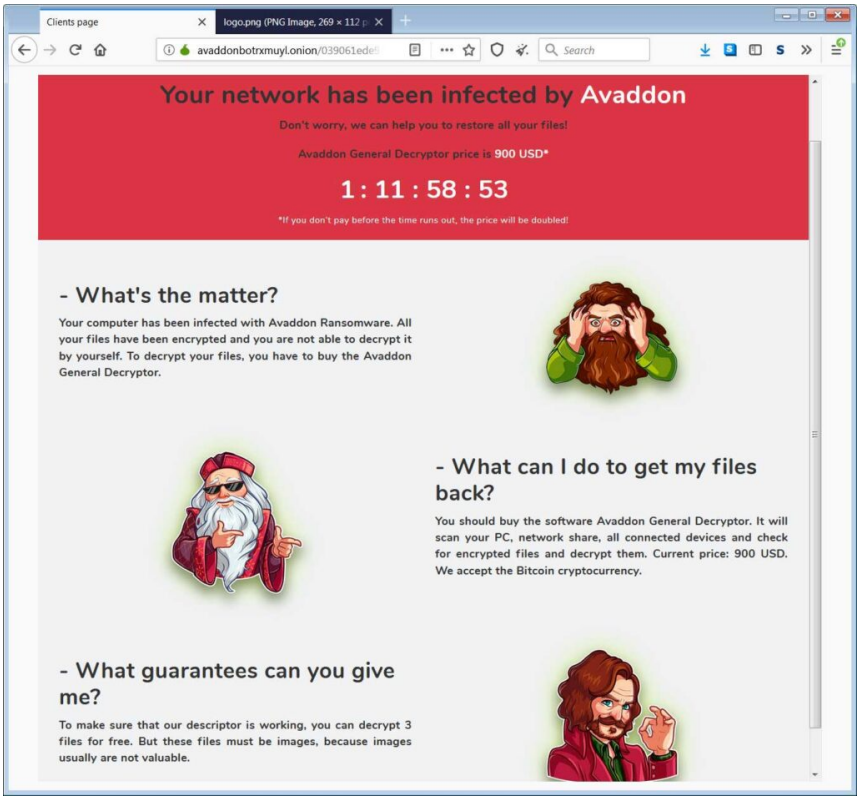


Accedendo al sito Avaddon si atterra su:



Il “servizio” dispone anche di una “Help Page” dove vengono fornite le indicazioni di dettaglio:





Area Geografica Target di Avaddon

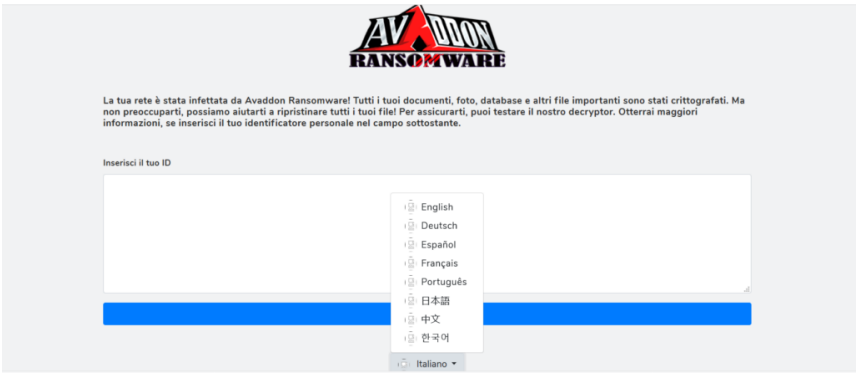
Il Ransomware Avaddon non viene eseguito se l'impostazione del dispositivo Windows è configurato per la Russia e/o Ucraina oppure se la tastiera è configurata in :

- russo
- Yakut (Russia)
- tataro
- ucraino

Avaddon non attacca i paesi appartenenti alla Comunità degli Stati Indipendenti: Armenia, Azerbaigian, Bielorussia, Kazakistan, Kirghizistan, Moldavia, Federazione Russa, Tagikistan, Turkmenistan, Uzbekistan e Ucraina .

Sembrerebbe che il motivo sia dovuto all'accondiscendenza delle autorità russe vero i criminal hacker che operano contro paesi stranieri.

Non è un caso che il sito onion di Avaddon è disponibile nelle seguenti lingue:

- 

- Italiano
- Tedesco
- Spagnolo
- Francese
- Inglese
- Portoghese

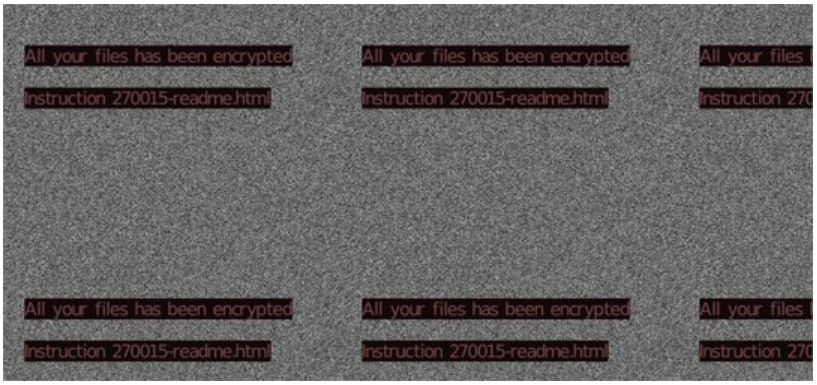
- Giapponese
- Cinese
- Coreano

Sotto attacco **Ransomware?**
Contattaci

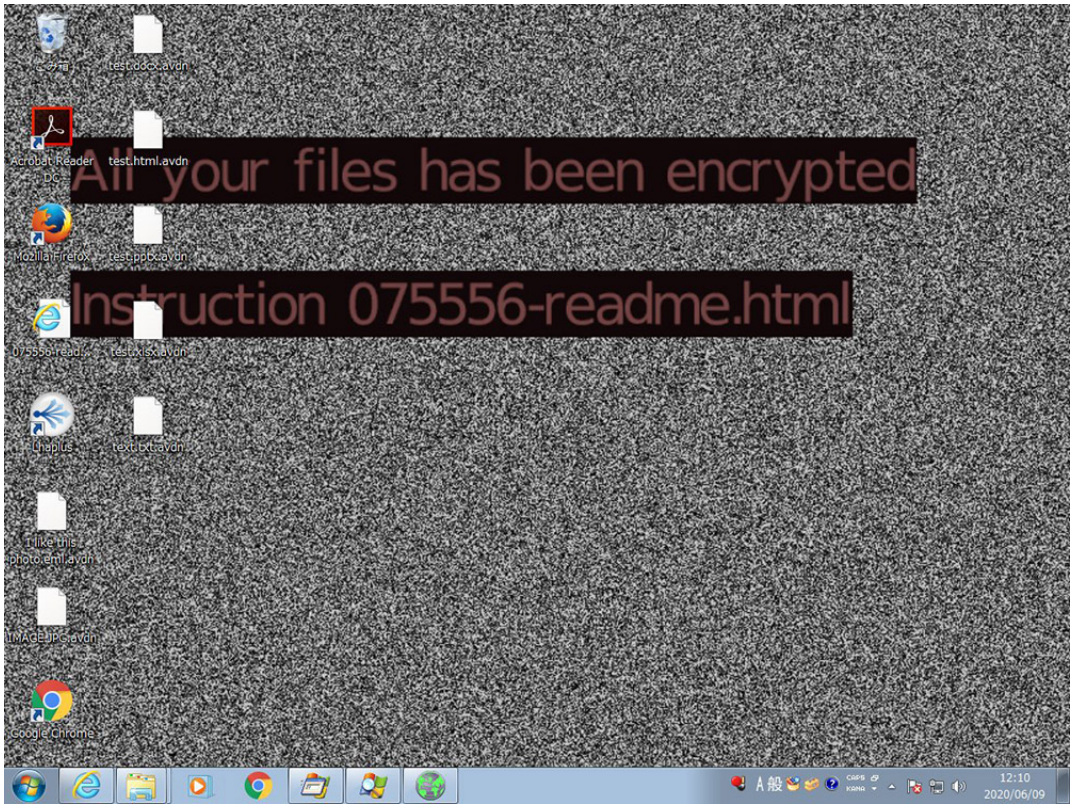
Ransomware Avaddon: Sintomi

Se nel proprio network vengono identificate tastiere con un cambio del settinge della lingua in Russo o in una delle lingue indicate precedentemente c'è un'altra probabilità che la macchina in questione è oggetto di un data breach legato ad un ransomware. E' il primo segnale di preparazione ad un cyber attack di questa tipologia di hacking. Parliamo di Avaddon, Revil, Sodinokibi, Ryuk,…

In caso di attacco con ransomware Avaddon il desktop apparirà:

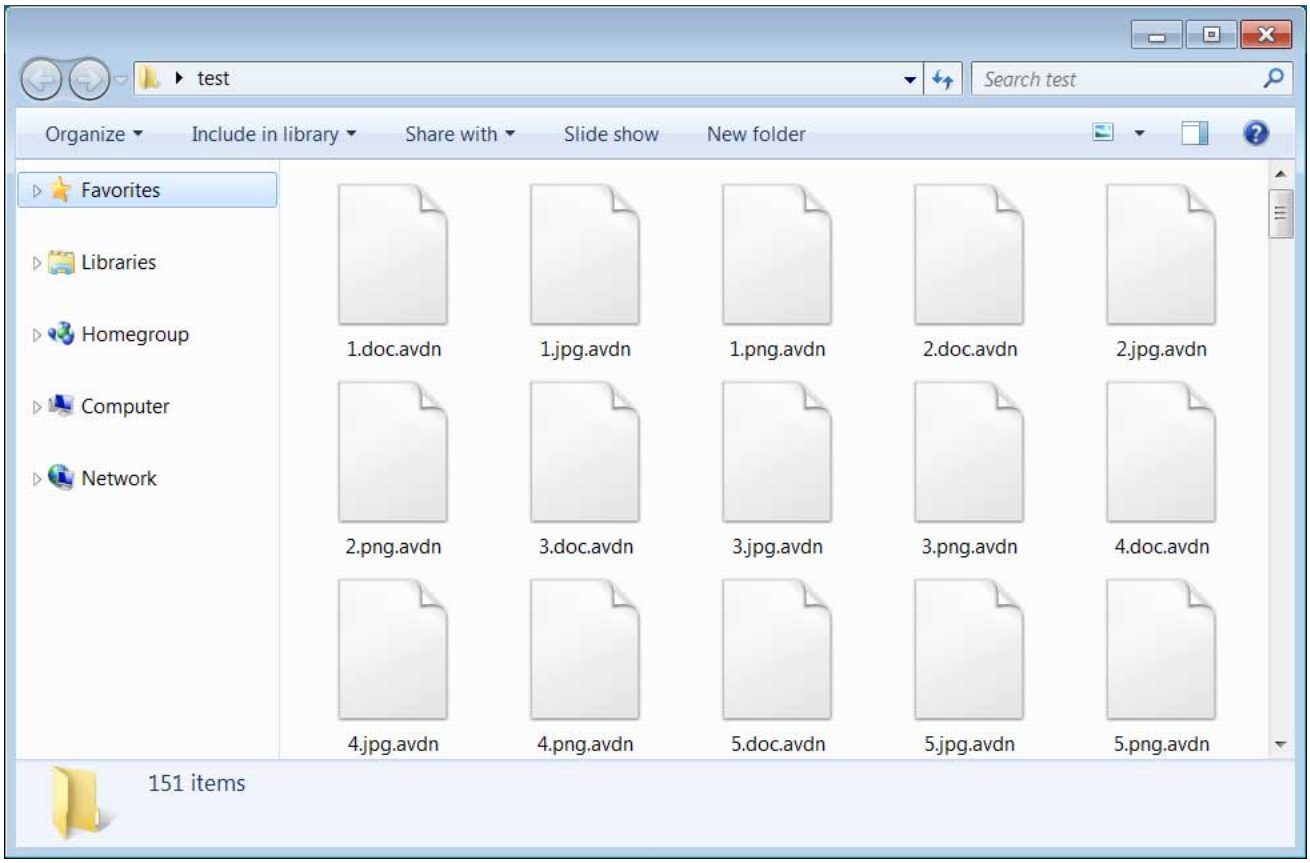


Fonte: Trend Micro



Fonte: bankinfosecurity

I file delle cartelle avranno estensione **.avn**



Fonte: bleepingcomputer

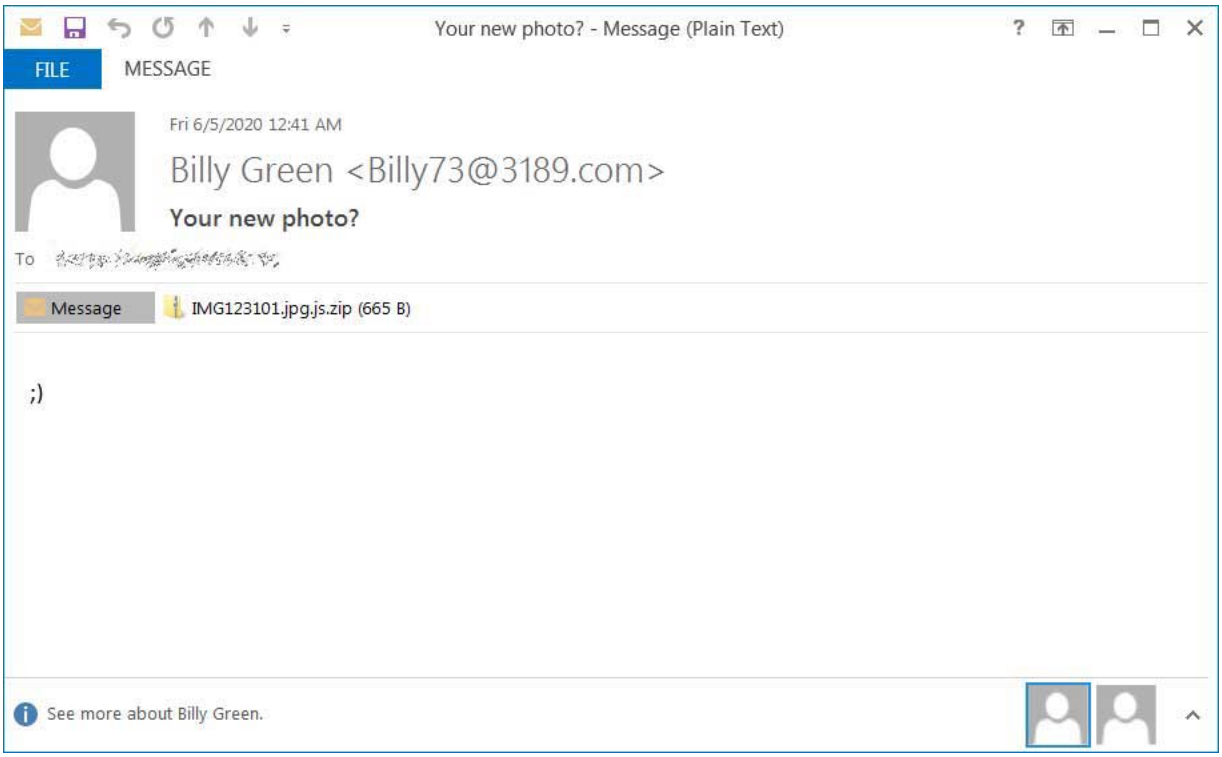
Avaddon Ransomware: Vettori di Attacco

La distribuzione del ransomware avviene principalmete attraverso due modalità:

- Social Enginering
- Sfruttamento delle Vulnerabilità note

Social Engineering

Avaddon viene principalmente diffuso tramite attività di malspam. Il **phishing** si conferma essere lo strumento e vettore di attacco più utilizzato. Le email avranno allegati con estensione .jpg.js.zip contenete un file JavaScript.



Fonte: Bleepingcomputer

Scaricando ed eseguendo il file allegato viene attivata la PowerShell associata e tramite riga di comando BITSAdmin viene scaricato il payload del ransomware Avaddon. A questo punto il ransomware procede alla crittografia dei file del dispositivo e alla modifica del desktop.

Vulnerabilità

La presenza di vulnerabilità sui sistemi esposti sono una opportunità per qualsiasi attaccante. La vulnerabilità più usata è la presenza di RDP esposti senza disdegnare vulnerabilità note e o facilmente exploitabili.

Modalità di attacco Avaddon

Con l'esecuzione del payload del ransomware Avaddon inizia la crittografia dei file :

- File di programma (x86) \ Microsoft \ Exchange Server
- Programmi \ Microsoft SQL Server
- Programmi \ Microsoft \ Exchange Server
- Programmi (x86) \ Microsoft SQL Server

Procede con il terminare i processi adibiti principalmente al recupero dei file, di backup, scansione antivirus e le attività pianificate:

Servizi terminati:

- ccEvtMgr
- ccSetMgr
- Culserver
- dbeng8
- dbsrv12
- DefWatch
- Intuit.QuickBooks.FCS
- msmdsrv
- QBCFMonitorService
- QBIDPService

Inoltre blocca i processi :

- BCFMonitorService.exe
- 360doctor.exe
- axlbridge.exe
- 360se.exe

- fdlauncher.exe
- GDscan.exe
- Culture.exe
- Defwatch.exe
- fdhost.exe
- httpd.exe

Il ransomware Avaddon elimina e/o rende difficile il recupero delle copie di backup aggiungendo i processi:

- 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 Elimina Shadows / All / Quiet

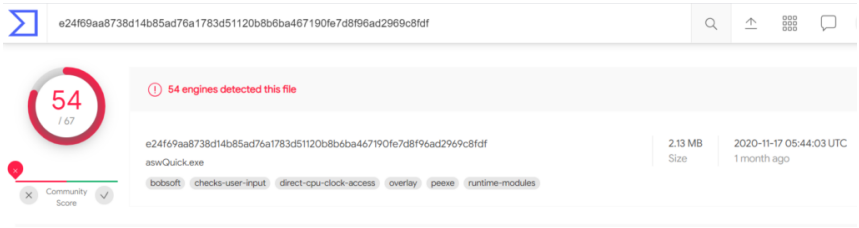
Decriptazione Avaddon e Recovery dei dati

L'algoritmo di crittografia utilizzato dal ransomware Avaddon, come per tutti i ransomware di nuova generazione, rende impossibile la decriptazione dei file unitamente al recovery dei dati se non si dispone di backup non "colpiti" dal ransomware stesso.

Le uniche possibilità per il recupero dei file è di disporre della chiave di decriptazione. In alcuni casi è possibile recuperare parte dei dati presenti in Database di grandi dimensioni operando e sfruttando un limite tecnico dei sistemi ransomware. Anche in questo caso non parliamo di decryptor.

Indicatori di Compromissione del Ransomware Avaddon

MD5 ccede1200a6e8eff54a358fa1e6d119a
SHA-1 e62fbe82dc5c1efbdecfd94791e023002d3c178b
SHA-256 e24f69aa8738d14b85ad76a1783d51120b8b6ba467190fe7d8f96ad2969c8fdf



Fonte: Virustotal

IP Contattati

· 68.232.34.200

· 93.184.221.240

· 93.184.220.29

· 13.68.93.109

· 2.19.194.146

· 23.56.184.216

· 13.107.4.52

· 67.26.19.254

· 2.19.194.161

· 67.26.25.254

· 8.247.205.126

Url Contattati

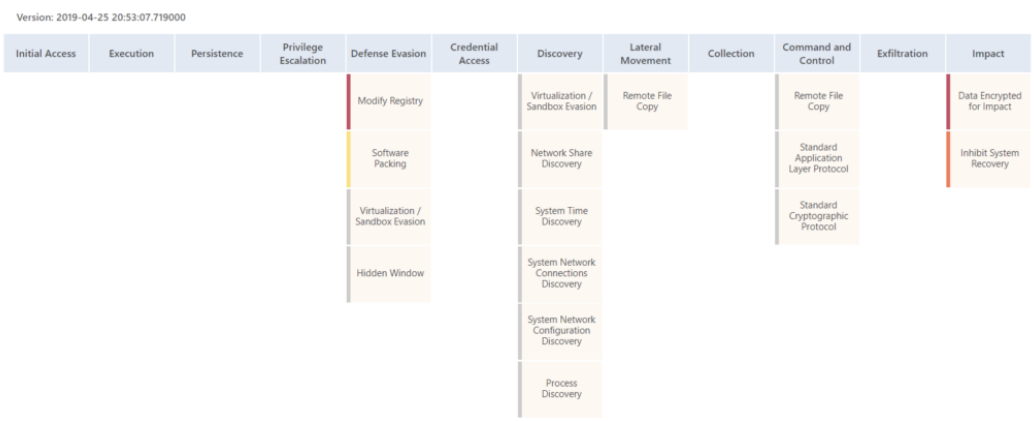
- http://api.myip.com/

- http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom/nYB45SPUEwQU5Z1ZMIJHWMys+ghUNoZ7O
- http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Secure%20Server%20CA%202.1.crl
- http://download.windowsupdate.com/c/msdownload/update/others/2019/12/30378685_721206c65081222488d2fae7cc6ecbca9e5025d4.cab
- http://download.visualstudio.microsoft.com/
- http://download.windowsupdate.com/d/msdownload/update/others/2019/08/29692004_8adad4cd466b76f1bfa96233d6832d8a2bbd477a.cab
- http://download.windowsupdate.com/c/msdownload/update/others/2019/10/30015113_f0ac1db5f98499f074c0e673eb42b34311dfe078.cab
- http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fbd360b9b6522e8f
- http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl
- http://download.windowsupdate.com/d/msdownload/update/others/2019/08/29632392_bfa3183dbb37e66f0fd8e68624b74472de3794ea.cab
- http://download.windowsupdate.com/c/msdownload/update/others/2020/05/31702887_c66d1f08687e7d20809c993d2cddb293957f3ae6.cab
- http://sls.update.microsoft.com/

Avaddon Threats

Severity	Operation	Count
5/5	Defense Evasion	Bypasses Windows User Account Control (UAC)
5/5	User Data Modification	Encrypts content of user files
5/5	Reputation	Known malicious file
4/5	User Data Modification	Modifies Windows automatic backups
3/5	Anti Analysis	Tries to evade debugger
2/5	Obfuscation	Resolves APIs dynamically to possibly evade static detection
2/5	Defense Evasion	Sends control codes to connected devices
2/5	Anti Analysis	Tries to detect debugger
1/5	Anti Analysis	Tries to detect analyzer sandbox
1/5	Mutex	Creates mutex
1/5	Discovery	Reads SMB connection information
1/5	Hide Tracks	Creates process with hidden window
1/5	Network Connection	Performs DNS request
1/5	Obfuscation	Overwrites code
1/5	System Modification	Creates an unusually large number of files
1/5	Network Connection	Downloads file
1/5	Network Connection	Connects to HTTP server
1/5	Network Connection	Connects to HTTPS server
0/5	Discovery	Enumerates running processes

Avaddon Mitre Attack



Fonte: Vmray

Incident Management

L'**Incident Management** di un Data Breach da ransomware prevede le seguenti azioni immediate di Mitigation e Eradication.

1.
    1. Isolare la rete compromessa. Non spegnere i sistemi per garantire l'integrità delle evidenze digitali.D
    2. Determinare se nel web, darkweb e deep web sono pubbliche email/pwd aziendali compromesse (**Domain Threat Intelligence)**
    3. Determinare e identificare eventuali Botnet relative al network aziendale(**Cyber Threat Intelligence)**
    4. Effettuare l' Analisi dell'integrità dell'Active Directory
    5. Forzare il cambio delle password di dominio e applicative
    6. Revoca e riemissione di eventuali certificati (VPN, Firma Digitale, ecc.).Analisi dell'integrità dell'Active Directory
    7. Effettuare la segmentazione delle reti
    8. Installare sistemi di EDR e NDR
    9. Attivare il servizio di **Soc as a Service**
    10. Effettuare attività di digital investigation attraverso l'analisi dei Logs

Cyber Security News 28/12/2020
Cyber Security News 29/12/2020