ONI Ransomware Used in Month-Long Attacks Against Japanese Companies

bleepingcomputer.com/news/security/oni-ransomware-used-in-month-long-attacks-against-japanese-companies

By
Lawrence Abrams

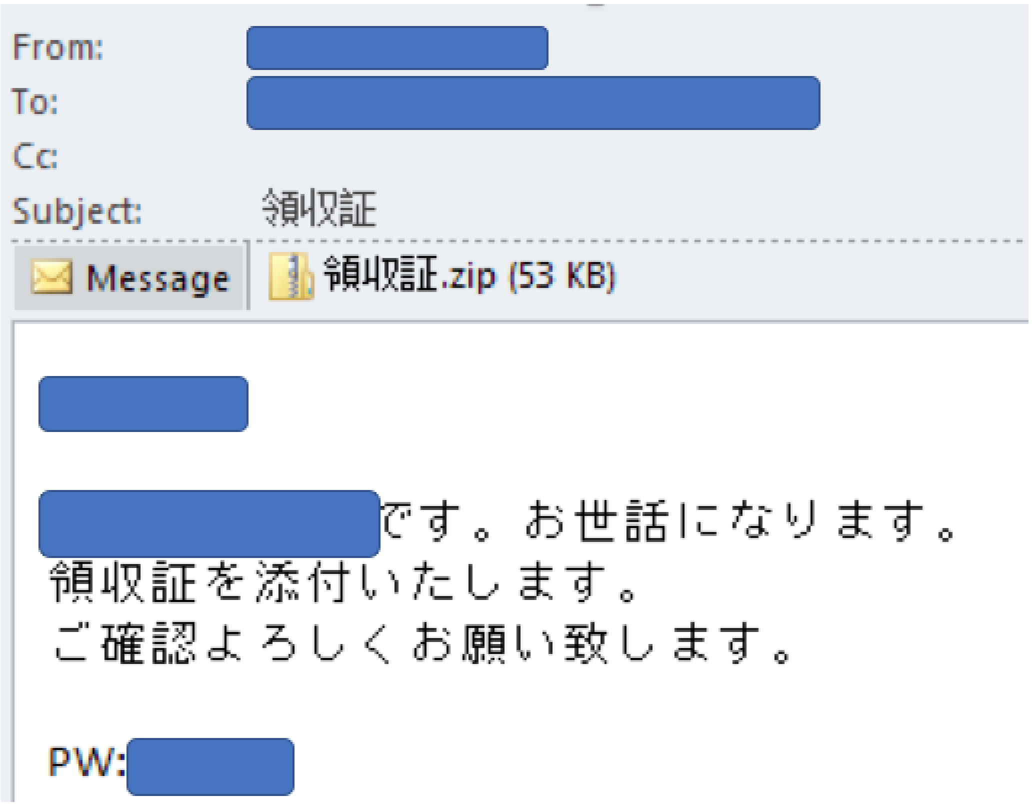
- October 31, 2017
- 09:26 AM
- 2

As more and more ransomware outbreaks are discovered, the line has become blurred in whether they are being utilized as a wiper or an actual ransomware. Such is the case with a new ransomware attack called ONI that has been used in targeted month long attacks against Japanese companies.

ONI goes phishing

It all started when security firm Cybereason analyzed some computers that were infected with a ransomware called ONI. This ransomware has been analyzed before, but it was not understood how the ONI victims were being infected. After analysis by Cybereason researchers, it was discovered that the infected computers had also been previously targeted by a spear phishing campaign that installs a RAT, or Remote Access Trojan, on the victim's computer.

These phishing emails pretend to be receipts that contain a zip attachment with a malicious Word document inside it. When a user opens the document and enables macros, a VBScript script will be launched that downloads and install a copy of the Ammyy Admin RAT onto the infected computer.



From: [redacted]
To: [redacted]
Cc:
Subject: 領収証

Message 領収証.zip (53 KB)

[redacted]

[redacted]です。お世話になります。
領収証を添付いたします。
ご確認よろしくお願い致します。

PW:[redacted]

Spear Phishing Email
Source: Cybereason

While Ammyy Admin is a legitimate remote administration tool, in this case it is being used by the attackers to gain full access to the system. According to Cybereason, they have found instances of this RAT being installed as far back as December 2016 and as recently as September 2017.

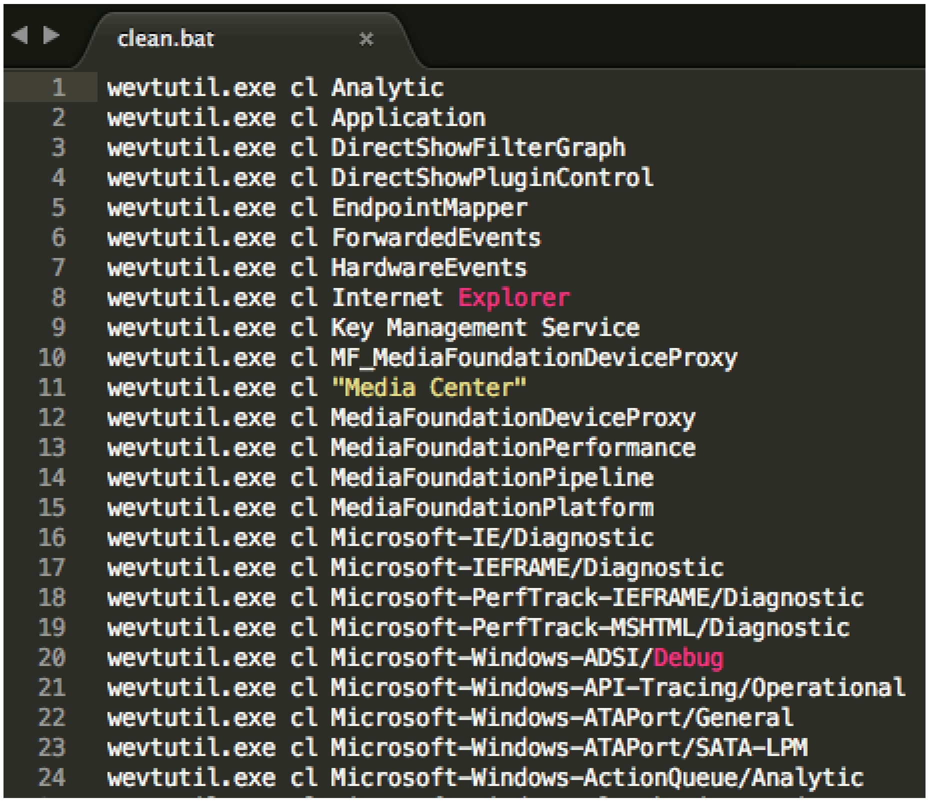
Cybereason has told BleepingComputer that all of the targets were medium-large companies and there have not been any reports of government related incidents.

Covering their tracks

Once the attackers were able to gain access to a network, they further worked on gaining access to the domain administrator account and servers. Unfortunately, at this point it becomes a bit fuzzy as to what the attackers were doing during their three to nine month access to the hacked network.

Cybereason has told BleepingComputer that "it's safe to assume that sensitive data was exfiltrated during those months of active hacking operation".

When the attackers were finished with their hacking operation, ONI Ransomware would come into play. As the attackers had access to the domain servers, they would utilize Group Policy Scripts to execute a batch file that cleaned up over 460 different event logs in order to cover their activities.



```
wevtutil.exe cl Analytic
wevtutil.exe cl Application
wevtutil.exe cl DirectShowFilterGraph
wevtutil.exe cl DirectShowPluginControl
wevtutil.exe cl EndpointMapper
wevtutil.exe cl ForwardedEvents
wevtutil.exe cl HardwareEvents
wevtutil.exe cl Internet Explorer
wevtutil.exe cl Key Management Service
wevtutil.exe cl MF_MediaFoundationDeviceProxy
wevtutil.exe cl "Media Center"
wevtutil.exe cl MediaFoundationDeviceProxy
wevtutil.exe cl MediaFoundationPerformance
wevtutil.exe cl MediaFoundationPipeline
wevtutil.exe cl MediaFoundationPlatform
wevtutil.exe cl Microsoft-IE/Diagnostic
wevtutil.exe cl Microsoft-IEFRAME/Diagnostic
wevtutil.exe cl Microsoft-PerfTrack-IEFRAME/Diagnostic
wevtutil.exe cl Microsoft-PerfTrack-MSHTML/Diagnostic
wevtutil.exe cl Microsoft-Windows-ADSI/Debug
wevtutil.exe cl Microsoft-Windows-API-Tracing/Operational
wevtutil.exe cl Microsoft-Windows-ATAPort/General
wevtutil.exe cl Microsoft-Windows-ATAPort/SATA-LPM
wevtutil.exe cl Microsoft-Windows-ActionQueue/Analytic
```

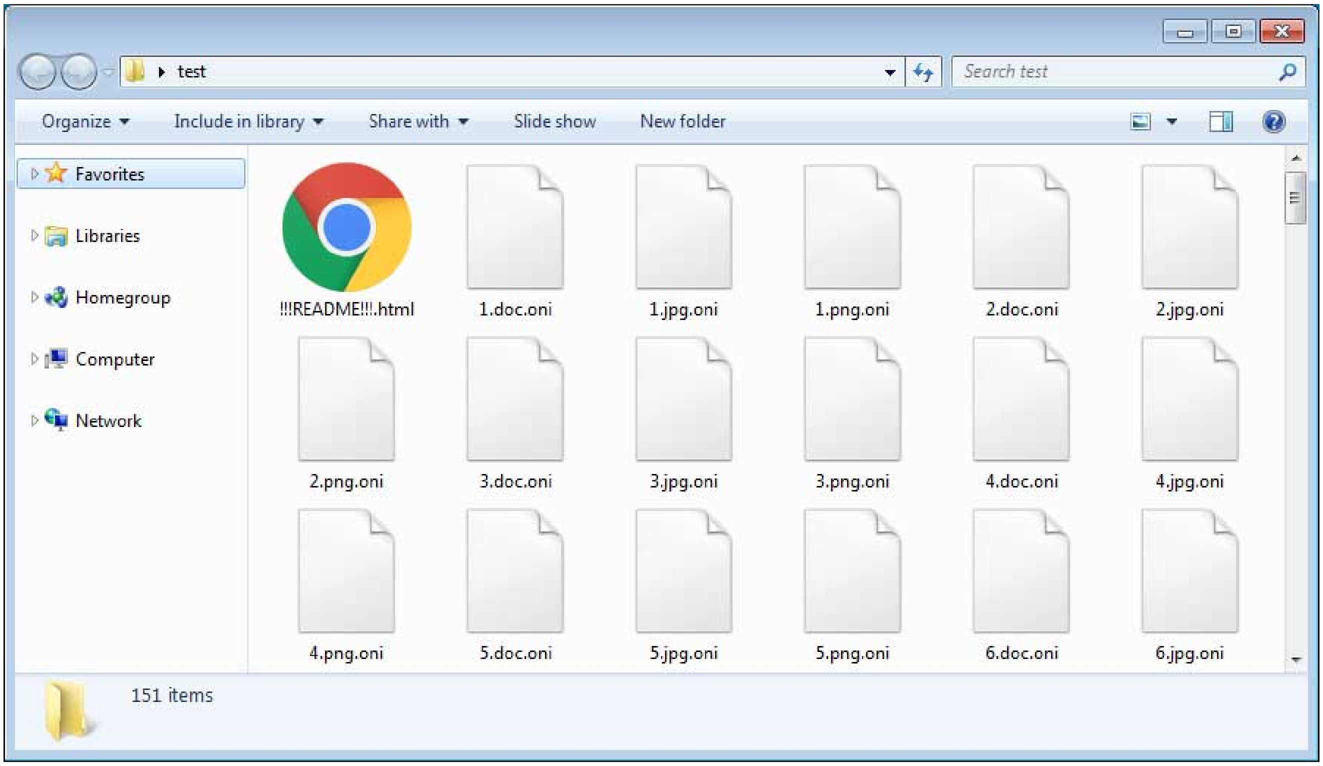
Clearing Event Logs
Source: Cybereason

This same script would also deploy the ONI ransomware on computers in order to encrypt files and to possibly further obfuscate the activities of the attackers.

ONI Ransomware: A Ransomware or a Wiper?

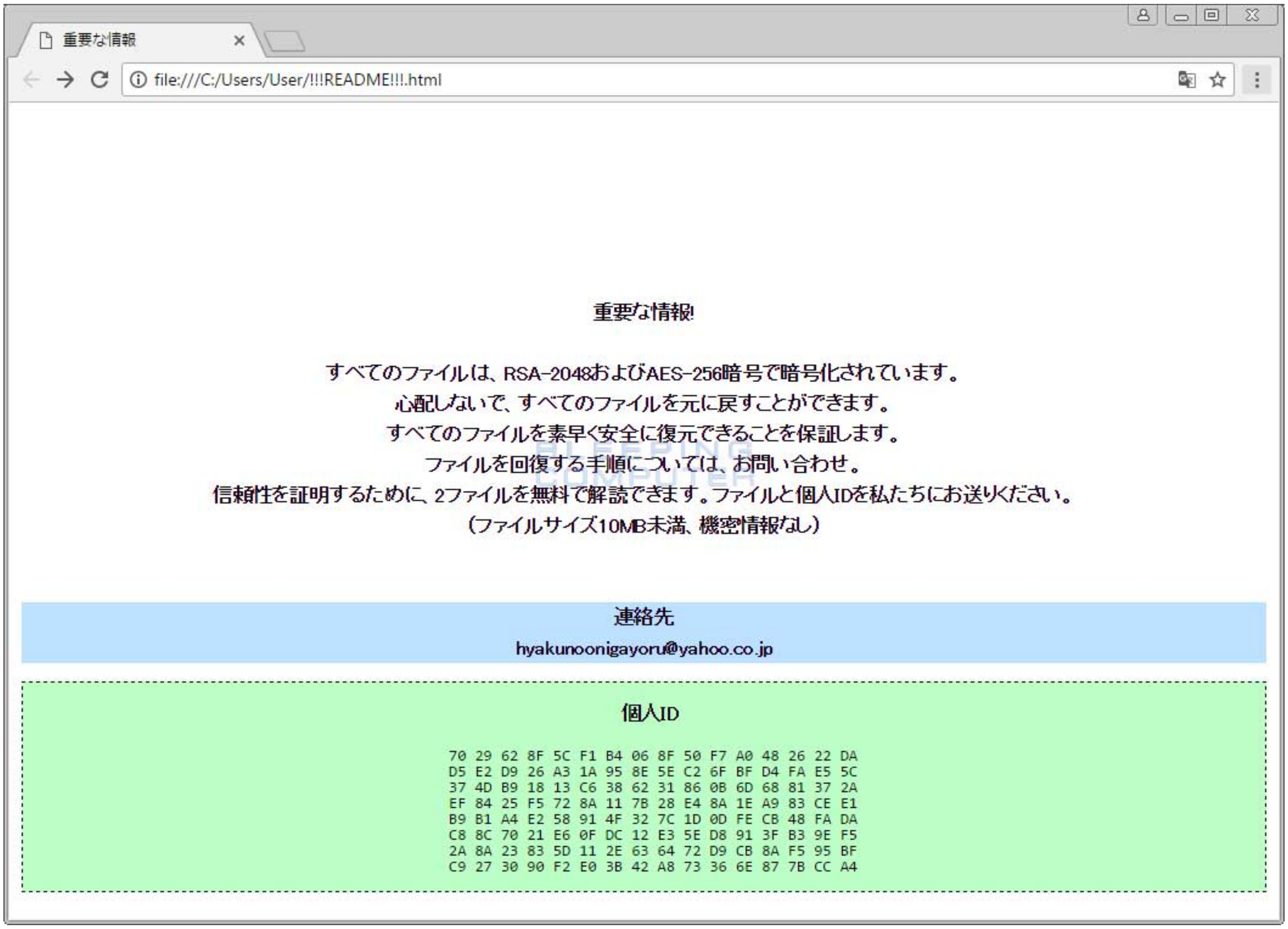
An interesting aspect of this attack was that the attackers used two different versions of the ONI Ransomware. One version, which was used to mostly target non-critical computers, is a GlobeImposter variant that acts as a user mode encryptor.

When installed, ONI Ransomware would encrypt the computer's files and append the **.oni** extension to encrypted files as shown below.



Encrypted Folder

When done, victims would then find a ransom note named **!!!README!!!!.html** located in folders where files were encrypted. These ransom notes contain basic information on what happened to the victim's files and an email that can be used to contact the attackers for payment instructions.



重要な情報!

すべてのファイルは、RSA-2048およびAES-256暗号で暗号化されています。
心配しないで、すべてのファイルを元に戻すことができます。
すべてのファイルを素早く安全に復元できることを保証します。
ファイルを回復する手順については、お問い合わせ。
信頼性を証明するために、2ファイルを無料で解読できます。ファイルと個人IDを私たちにお送りください。
(ファイルサイズ10MB未満、機密情報なし)

連絡先
hyakunoonigayoru@yahoo.co.jp

個人ID

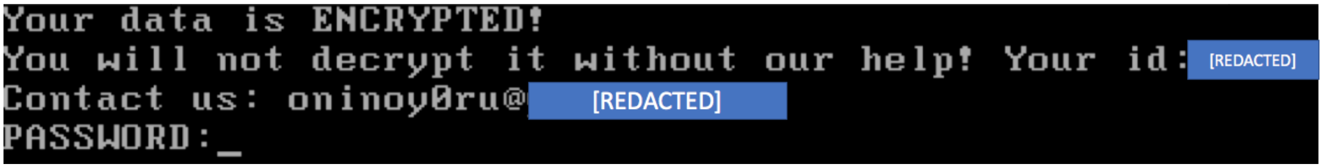
```
70 29 62 8F 5C F1 B4 06 8F 50 F7 A0 48 26 22 DA
D5 E2 D9 26 A3 1A 95 8E 5E C2 6F BF D4 FA E5 5C
37 4D B9 18 13 C6 38 62 31 86 0B 6D 68 81 37 2A
EF 84 25 F5 72 8A 11 7B 28 E4 8A 1E A9 83 CE E1
B9 B1 A4 E2 58 91 4F 32 7C 1D 0D FE CB 48 FA DA
C8 8C 70 21 E6 0F DC 12 E3 5E D8 91 3F B3 9E F5
2A 8A 23 83 5D 11 2E 63 64 72 D9 CB 8A F5 95 BF
C9 27 30 90 F2 E0 3B 42 A8 73 36 6E 87 7B CC A4
```

ONI Ransom Note

This is all standard procedure for GlobeImposter ransomware variants.

It gets more interesting, though, when Cybereason discovered that the attackers were also using another ransomware on certain computers. This ransomware is being called MBR-ONI because it encrypts the actual as it encrypts the actual file system and then replaces the MBR, or Master Boot Record, with a password protected lock screen that is displayed before Windows boots.

It does this by utilizing the legitimate DiskCryptor program, which was recently used by the Bad Rabbit Ransomware attack, to encrypt the file system and requires a password to make it accessible again.



```
Your data is ENCRYPTED!
You will not decrypt it without our help! Your id:[REDACTED]
Contact us: oninoy0ru@[REDACTED]
PASSWORD:_
```

MBR-ONI Lock Screen
Source: Cybereason

According to Cybereason, MBR-ONI was only deployed on active directory servers or "critical assets".

Unlike the NotPetya attack which would not allow decryption of the file system, ONI and MBR-ONI are legitimate ransomware infections that can be decrypted if the victim acquires the decryption key. While Cybereason has told BleepingComputer that there have been no reports of victim's paying the ransom or even contacting the attackers, the way these ransomware were used is not commonly done.

The question remains as to whether the attackers were using ONI to earn some extra money after they finished their attack, to make computers and files inaccessible to cover their traces, or maybe even both. Only time will tell.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

Hashes:

```
SHA256: 9bba34947b9b2f9d52aeb45b342637ce93d6683bbf8e352da53dae053da37ae6
(GlobeImposter Variant)
```

Files associated with ONI:

```
!!!README!!!.html
```

ONI Ransom Note (Japanese):

```
重要な情報！

すべてのファイルは、RSA-2048およびAES-256暗号で暗号化されています。
心配しないで、すべてのファイルを元に戻すことができます。
すべてのファイルを素早く安全に復元できることを保証します。
ファイルを回復する手順については、お問い合わせ。
信頼性を証明するために、2ファイルを無料で解読できます。ファイルと個人IDを私たちにお送りください。
(ファイルサイズ10MB未満、機密情報なし)


連絡先
hyakunoonigayoru@yahoo.co.jp
```

ONI Ransom Note (English Translation):

```
Important information!

All files are encrypted with RSA - 2048 and AES - 256 ciphers.
Do not worry, you can restore all the files.
We guarantee that all files can be safely restored quickly and safely.
For instructions on recovering files, contact us.
To prove reliability, you can decipher two files for free. Please send us the file and personal ID.
(File size less than 10 MB, no confidential information)


contact information
hyakunoonigayoru@yahoo.co.jp
```

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-

  Amigo-A - 4 years ago

  """Ammyy Admin is a legitimate remote administration tool"""
  It should be noted that the utility Ammyy Admin and sites of the company "Ammyy" Ltd. were many, many times compromised, hacked, infected.

  https://www.esetnod32.ru/company/press/center/eset-avtory-buhtrap-osvoili-apt-ataki/
  https://securelist.ru/blog/issledovaniya/28900/lurk-a-danger-where-you-least-expect-it/
  http://news.softpedia.com/news/ammyy-admin-website-compromised-to-spread-cerber-3-ransomware-508330.shtml

-

  Amigo-A - 4 years ago

  Cylance assert that file %Temp%\qfjgmfgmkj.tmp - special file that prohibits the re-installation of this encryptor. So it can be used for protection.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: