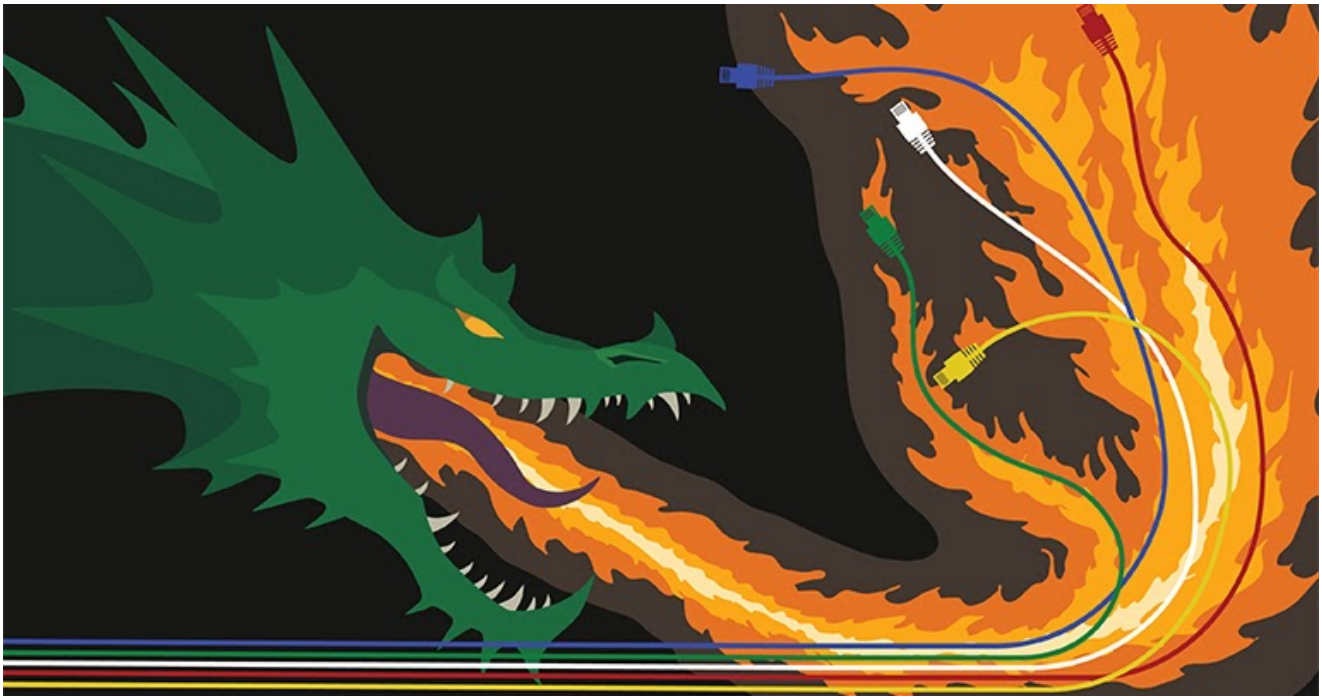
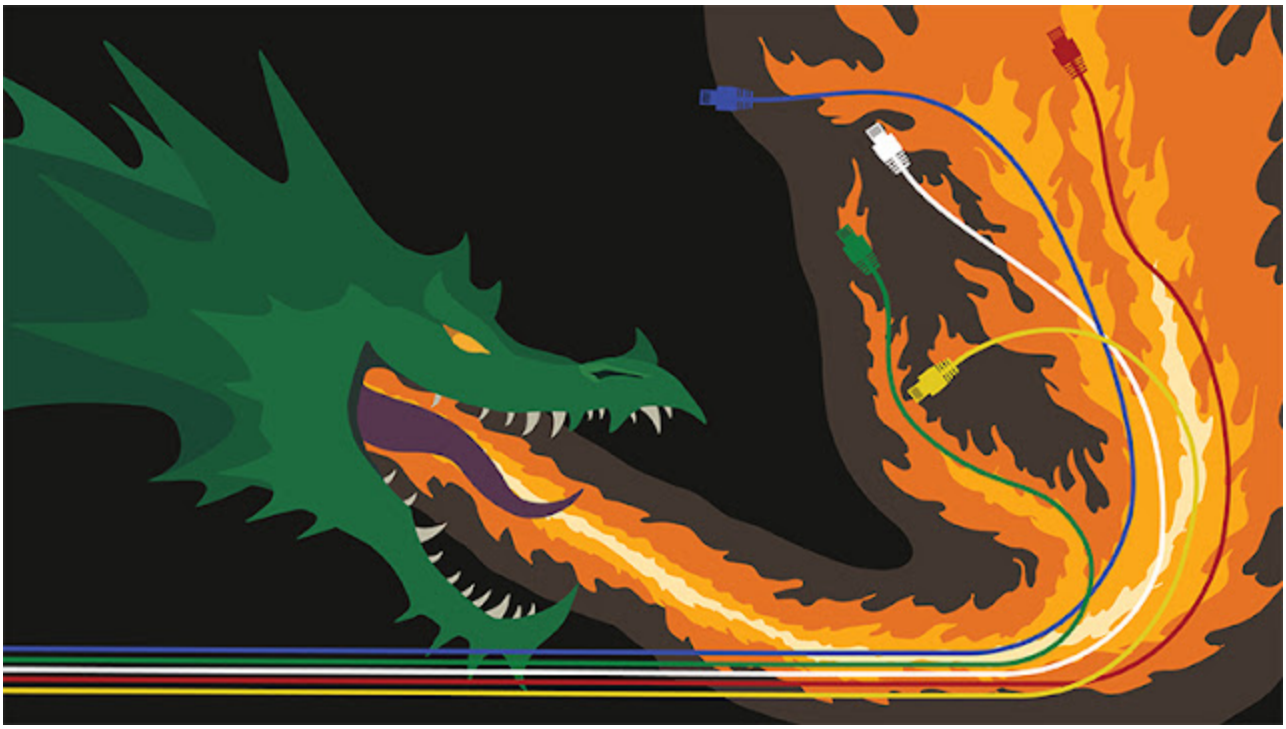
New Ransomware Variant "Nyetya" Compromises Systems Worldwide

blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html



Note: *This blog post discusses active research by Talos into a new threat. This information should be considered preliminary and will be updated as research continues.*

Update 2017-07-06 12:30 EDT: Updated to explain the modified DoublePulsar backdoor.



Since the SamSam attacks that targeted US healthcare entities in March 2016, Talos has been concerned about the proliferation of malware via unpatched network vulnerabilities. In May 2017, WannaCry ransomware took advantage of a vulnerability in SMBv1 and spread like wildfire across the Internet.

Today a new malware variant has surfaced that is distinct enough from Petya that people have referred to it by various names such as Petrwrap and GoldenEye. Talos is identifying this new malware variant as Nyetya. The sample leverages EternalBlue, EternalRomance, WMI, and PsExec for lateral movement inside an affected network. This behavior is detailed later in the blog under "Malware Functionality". Unlike WannaCry, Nyetya does not appear to contain an external scanning component.

The identification of the initial vector is still under investigation. We have observed **no use** of email or Office documents as a delivery mechanism for this malware. We believe that infections are associated with software update systems for a Ukrainian tax accounting package called MeDoc. Talos is investigating this currently.

Given the circumstances of this attack, Talos assesses with high confidence that the intent of the actor behind Nyetya was destructive in nature and not economically motivated. Talos strongly recommends users and organizations decline to pay the ransom. Any attempts to obtain a decryption key will be fruitless as the associated mailbox used for payment verification and decryption key sharing has been shut down by the posteo.de. This renders any successful payment as useless as there is no method of communication available for this actor to use to verify payments from victims or distribute decryption keys once ransom

payments have been received. There is also no method used by the malware to directly connect to command and control for remote unlocking.

Recovery of User Credentials

Nyetya requires user credentials to spread itself laterally via the PsExec and WMI vectors (which are detailed in the "Malware Functionality" section). Talos has identified three ways Nyetya can obtain these credentials.

First, credentials can be manually passed in via a command line argument. Here is the syntax:

```
rundll32.exe C:\Windows\perfc.dat,#1 60 "username:password"
```

A second method consists to use the CredEnumerateW Windows API.

Finally, Perfc.dat contains three embedded executables in its resource section which are compressed with zlib. Two of the executables are used to recover user credentials (32 and 64 bits) while the third one is the PsExec binary. The executables related to credential recovery are dropped as a temporary files in the user's %TEMP% folder and run with a named pipe parameter (containing a GUID). The main executable communicates with the dropped executable using this named pipe. For example:

```
C:\WINDOWS\TEMP\561D.tmp, \\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}
```

The dropped .tmp executable seems to be based on Mimikatz, a popular open source tool used for recovery of user credentials from computer memory using several different techniques. ***However, Talos has confirmed that the executable is not specifically the Mimikatz tool.***

The recovered credentials are then used for launching malware on the remote system using WMIC and PsExec. This is detailed below.

Malware Functionality

Perfc.dat contains the functionality needed to further compromise the system and contains a single unnamed export function referred to as #1. As part of the propagation process, the malware enumerates all visible machines on the network via the NetServerEnum API call and then scans for an open TCP 139 port. This is done to compile a list of devices that expose this port and may possibly be susceptible to compromise.

Nyetya has several mechanisms that are used to propagate once a device is infected:

1. EternalBlue - the same exploit used by WannaCry.
2. EternalRomance - an SMBv1 exploit leaked by "ShadowBrokers"
3. PsExec - a legitimate Windows administration tool.
4. WMI - Windows Management Instrumentation, a legitimate Windows component.

These mechanisms are used to attempt installation and execution of perfc.dat on other devices to spread laterally.

For systems that have not had MS17-010 applied, the EternalBlue and EternalRomance exploits are leveraged to compromise systems. The exploit launched against the victim system depends on the operating system of the intended target.

- EternalBlue
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 7
- EternalRomance
  - Windows XP
  - Windows Server 2003
  - Windows Vista

The two exploits drop a modified version of DoublePulsar which is a persistent backdoor running in kernel space of the compromised system. The developer modified only few bytes from the original version but this modification allowed it to evade network detection and the open source DoublePulsar scanning tools available on the Internet. The modification can be divided in 3 parts:

- The attacker modified the command codes:

Original Command Code	Nyetya Command Code	Purpose
0x23	0xF0	PING
0x77	0xF1	KILL
0xC8	0xF2	EXEC

- The attacker modified the response codes:

Original Response Code	Nyetya Response Code	Purpose
0x10	0x11	OK

0x20	0x21	CMD_INVALID
0x30	0x31	ALLOCATION_FAILURE

- The attacker modified where the response code is stored in the SMB response packet. In the original version of DouplePulsar, the code was stored in the MultiplexID field (offset 0x1E). In the Nyetya version, the response code is stored in a reserved field (offset 0x16) which is normally set to 0x0000

We implemented a specific NGIPS / Snort rule to detect this DoublePulsar variant: 43459.

PsExec is used to execute the following instruction (where w.x.y.z is an IP address) using the current user's windows token (from the "Recovery of User Credentials" section above) to install the malware on the networked device.

```
C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe
C:\Windows\perfc.dat,#1 60
```

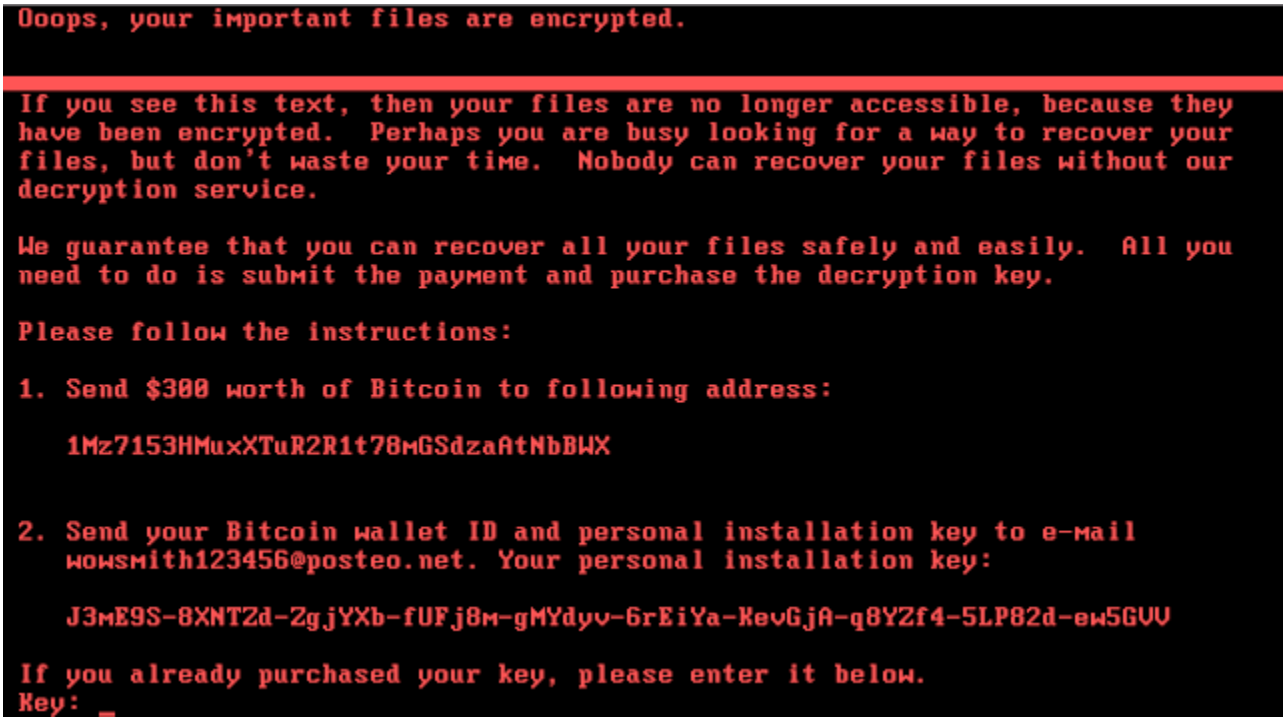
WMI is used to execute the following command which performs the same function as above, but using the current user's username and password (as username and password), retrieved from the "Recovery of User Credentials" section above.

```
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call
create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"
```

Once a system is successfully compromised, the malware encrypts files on the host using 2048-bit RSA encryption. Additionally, the malware cleans event logs on the compromised device using the following command:

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl
Application & fsutil usn deletejournal /D %c:
```

Nytetya attempts to obtain administrative privileges (SeShutdowPrivilege and SeDebugPrivilege) for the current user through the Windows API AdjustTokenPrivileges. If successful, Nyetya overwrites the boot sector on PhysicalDrive0 without first saving a copy. If overwriting the boot sector fails, Nyetya instead wipes the first ten sectors of the disk drive. Additionally, if Nyetya finds a process file name hash of 2E214B44 on the system, it will also wipe the first ten sectors of the disk drive. Talos has identified that this hash is referring to avp.exe, which corresponds to Kaspersky Anti-virus. Systems that have the boot sector overwritten will see this message when restarting their systems.



Screenshot of a system compromised by Nyetya.

Note that regardless of whether Nyetya is successful in overwriting the boot sector or not, it will proceed to create a scheduled task via schtasks to reboot the system one hour after infection.

Without analyzing the key generation or key storage components, Talos believes that the actors behind Nyetya did not intended for the boot sector or the ten sectors that are wiped to be restorable. Thus, Nyetya is intended to be destructive rather than as a tool for financial gain.

Mitigation and Prevention

There are several ways customers can mitigate and prevent Nyetya from impacting your environment.

- First and foremost, we strongly recommend that customers who have NOT yet already applied MS17-010 to go do so immediately. Given the severity of the vulnerability and the widely available tools that exploit it, leaving this vulnerability unpatched is unwise.
- Ensure you have anti-malware software deployed on your systems that can detect and block the execution of known malicious executables.
- Implement a disaster recovery plan that includes backing up and restoring data from backup devices that are kept offline. Adversaries frequently target backup mechanisms to limit the possibilities a user may be able to restore their files without paying the ransom.
- Disable SMBv1, if possible, on networks and move to a more updated version of SMB. (SMBv2 was introduced with Microsoft Vista)

- Organizing your networks in a number of well-defined logical segments, and allowing access to network assets only to those users and systems within a segment may help with containing outbreaks of self-spreading worms such as Nyetya.

As Nyetya attempts to overwrite the boot sector on an infected machine, Talos tested using MBRFilter to prevent any changes being allowed to the system boot sector. This test proved successful and the machine boot sector remained intact in a good state. For users or enterprises that can do so, we recommend using MBRFilter. Note that MBRFilter is an open source project from Talos and no warranties or guarantees are provided.

Coverage

Cisco customers are protected from Nyetya via the following products and services.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	N/A
Email Security	N/A
Network Security	✔
Threat Grid	✔
Umbrella	N/A
WSA	N/A

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Network Security appliances such as NGFW, NGIPS, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Email and web have not been identified as attack vectors at this time. Additionally, there are no known C2 elements related to this malware at this time. The malware, if transferred across these systems on your networks, will be blocked.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

NGIPS / Snort Rules

The following NGIPS / Snort rules detect this threat:

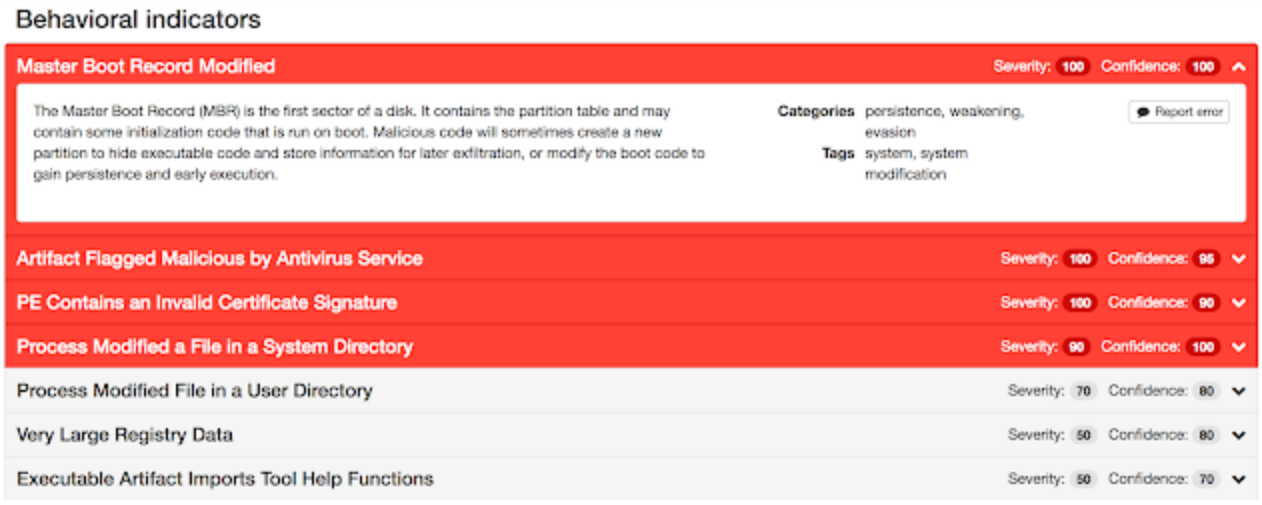
- 42944 - OS-WINDOWS Microsoft Windows SMB remote code execution attempt
- 42340 - OS-WINDOWS Microsoft Windows SMB anonymous session IPC share access attempt
- 41984 - OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type confusion attempt
- 43459 - MALWARE-CNC Win.Trojan.Doublepulsar variant successful ping response

The following NGIPS / Snort rules are also indicators of infection traffic:

- 5718 - OS-WINDOWS Microsoft Windows SMB-DS Trans unicode Max Param/Count OS-WINDOWS attempt
- 1917 - INDICATOR-SCAN UPnP service discover attempt
- 5730 - OS-WINDOWS Microsoft Windows SMB-DS Trans Max Param OS-WINDOWS attempt
- 26385 - FILE-EXECUTABLE Microsoft Windows executable file save onto SMB share attempt
- 43370 - NETBIOS DCERPC possible wmi remote process launch

Threat Grid

Threat Grid is capable of detecting malware samples related to Nyetya as malicious.



Indicators of Compromise (IOCs)

AMP Coverage

W32.Ransomware.Nyetya.Talos

SHA256

- 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998 (password stealer)