Executive Summary

The WannaCry Ransomware attack, also known as WannaDecrypr 2.0, began to proliferate in the afternoon hours of May 12, 2017 Pacific Standard Time across Europe. While initial indications were that the attack was targeting British NHS healthcare institutions in the United Kingdom, it spread quickly to other organizations and regions.

Instead of limiting themselves to one specific target type, the attackers inflicted damage across multiple industries by leveraging a leaked exploit against system vulnerabilities across a broad array of targets in order to generate profit. Analysis indicates that the attackers were likely relative amateurs that used a publicly available exploit kit affiliated with the latest NSA hack by The Shadow Brokers. Some news agencies have reported that this was the work of a state agency but the attack techniques were relatively unsophisticated. WannaCry, infected any unpatched Windows XP and above operating system targeted. The ransomware spreads like a worm leveraging Windows SMB vulnerability (MS17-010), then locks files in the computer and requires victims to pay in order to get back the control of their systems. The WannaCry ransomware attack is one of the largest on record, and has propagated to more than 140 countries. The attack infected organizations with a ransomware variant that spread via the EternalBlue exploit.

The Nyotron Attack Response Center classifies WannaCry as a "known-unknown" type attack or a variant of a previously known threat. Signatures were written for the original attack profile and a baseline established for future analysis that should have led to discovery and potential prevention by predictive antivirus platforms if the operating system updates were in place.
Table of Contents:

- About This Report 4
- Nyotron Findings 4
- Nyotron Short-term Recommendations 5
- WannaCry Timeline of Events 6
- PARANOID Execution Flow Detail 15
- Nyotron Attack Response Center Detail 16
- Summary and What To Do Now 18
About This Report
Nyotron Attack Response Center (NARC) is the global real-time crisis management and reporting authority at Nyotron, the creators of the world’s first Threat-Agnostic Defense™ technology. The NARC Team provides 24x7/365 Attack Response to Nyotron Managed Defense Services customers. Nyotron is focused on the damage phase of all attack types where damage prevention is paramount to business continuity. Nyotron provides real activity-based, not threat-based research to enterprise clients. Nyotron’s PARANOID, War Room and Managed Defense Services provide holistic protection from unknown attacks without any previous knowledge about the threat or its methodologies. Our goal is to keep our customers and the public informed of important developments in cybersecurity and to instruct on how to defend data and valuable organizational assets from damaging attacks.

Nyotron Findings

Attack Overview
Attack Description Name; WannaDecryptor 2.0 Ransomware

Operating System Versions
All outdated (MS17-010 vulnerable) Windows endpoints

Date of Attack
May 12, 2017

Current Status
Ongoing
Attack Identifiers

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>31DAB68B11824153B4C975399DF0354F</td>
</tr>
<tr>
<td>SHA1</td>
<td>14249E7FB3FB6F4B363C47D5AAE9F46DAB2083C1</td>
</tr>
<tr>
<td>SHA256</td>
<td>9b60c622546dc45cca64df935b71c26dcf4888d6fa811944dbc4e23db9335640</td>
</tr>
</tbody>
</table>

Attack Entry Point

Phishing/Exploitation

Nyotron Short-term Recommendations

- Install PARANOID or another threat agnostic protection mechanism.
- All Windows machines should apply the latest security updates provided by Microsoft.
- Brief company employees on how to spot and avoid phishing emails and potentially dangerous email attachments.
- Block access to port 445 from WAN to your organization’s internal network.
- Disable the SMEV1 Protocol.
- Remove/Disconnect vulnerable and infected machines from the network.
WannaCry Timeline of Events

Machines that expose the vulnerable SMB port, or users clicking untrusted software sent via e-mail.

The first action the malware takes is to register itself as a service to the machine.

As the image depicts, it registers itself under the name "mssecsvc2.0" with the description "Microsoft Security Center (2.0) Service." This is assumed to be done in order to make it difficult for information technology personnel to identify the faulting service straight away. Also, the command-line used for this service is "-m security" which could make it difficult for SOC analysts to identify the threat immediately. It purposefully appears to look like a legitimate service.

Detailed below is the attack-flow of the service "mssecsvc2.0":

The malware executes this service which attempts to infect connected windows machines in its local networks using the Eternal Blue doublepulsar exploit. This is done by enumerating the IP addresses of the computer and attempt the exploit against the various machines accessible.
Two threads are initially created for the network attack:
An image of the first stages of the exploit hard coded into the binaries:

The service then goes dormant for 24 hours, and then exits with error code 1.

The malware executes two commands “attrib +h.” used to add the “hidden” attribute to the directory it resides in and “icacls . /grant Everyone:F /T /C /Q” in order to give Full Control permissions to the user-group “Everyone” to the current directory and everything hierarchically located below it.

The malware continues to open a resource (an encrypted zip file), decrypt it (Using a hardcoded password “WNcry@2017”) and write its contents to disk.
The zip file’s contents:

<table>
<thead>
<tr>
<th>File / Directory name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg</td>
<td>Contains ransomware messages in different languages.</td>
</tr>
<tr>
<td>b.wnry</td>
<td>An image file to override the user’s Desktop image (Scare factor)</td>
</tr>
<tr>
<td>c.wnry</td>
<td>Inter-process File I/O mechanism.</td>
</tr>
<tr>
<td>r.wnry</td>
<td>Contains the classic ransomware message (Your files have been encrypted...)</td>
</tr>
<tr>
<td>s.wnry</td>
<td>Zipfile containing tor client.</td>
</tr>
<tr>
<td>t.wnry</td>
<td>An encrypted binary.</td>
</tr>
<tr>
<td>taskdl.exe</td>
<td>Executable used in the attack.</td>
</tr>
<tr>
<td>taskse.exe</td>
<td>Executable used to open @WanaDecryptor.exe on another session. (The attack starts on session 0)</td>
</tr>
<tr>
<td>u.wnry</td>
<td>A GUI application with several other uses (Explained below). (It is later renamed to @<a href="mailto:WanaDecryptor@.exe">WanaDecryptor@.exe</a>)</td>
</tr>
</tbody>
</table>
Files contained within “s.wnry”. This is a Tor client. Used to communicate with resources on the Tor network.

The file “t.wnry” is decrypted and executed. It contains binary code that encrypts files and adds the extension “.WNCRY”, as well as a crafted magic number used to identify already-encrypted files.
Following the encryption process, the software terminates various SQL, and exchange servers processes. Files that are being used by these processes are inaccessible to others. They are highly valued targets as they normally would prevent encryption of highly critical enterprise resources (Databases, mailboxes).

Shortly after, the malware changes "u.wnry" to "@WanaDecrypt@.exe" and executes it various times with different command-line arguments.

<table>
<thead>
<tr>
<th>Command Line Argument</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>fi</td>
<td>Unpacks s.wnry and instantiates to the tor client</td>
</tr>
<tr>
<td>co</td>
<td>Gets system time in a specific format and writes it to a file on the system.</td>
</tr>
<tr>
<td>vs</td>
<td>Prompts the user to delete shadow-copies</td>
</tr>
</tbody>
</table>
"@WanaDecryptor@.exe fi":

```
push esi ; File
push 1 ; Count
lea eax, [esp+00h+DestBuf]
push 00h ; ElementSize
push eax ; DestBuf
call ds:fread
push esi ; File
call ds:_imp_fclose
lea ecx, [ebp+74h]
lea edx, [ebp+6Eah]
push ecx ; int
push edx ; Execution with CommandLine “fi”
push offset aS_unryy ; s.unryy
call sub_400E90
lea eax, [esp+0Eah+Dest]
lea ecx, [esp+0Eah+DestBuf]
push eax ; Dest
lea edi, [esp+5Fh]
push offset asc_h2129h ; ‘+++’
push ecx ; int
push edi ; int
call sub_40C4F0
add esp, 30h
mov esi, eax
call sub_40C470
cmp esi, 0FFFFFFFh
jnz short loc_40B8A6
```

"@WanaDecryptor@.exe vs":

```
push 2710h ; dwMilliseconds
call ds:Sleep ; When run with vs cmdline
mov ecx, 32h
mov esi, offset aCusadminDelete ; ”/c usadmin delete shadows /all /quiet “...
lea edi, [esp+0AACH+var_990]
xor eax, eax
rep movsd
mov ecx, 0CEh
lea edi, [esp+0AACH+var_B8h]
rep stosd
mov eax, dw429FDB
mov ecx, dw429FDBh
mov [esp+0AACH+var_9C], eax
mov [esp+0AACH+var_990], ecx
call RunAsCommands
test eax, eax
jnz short loc_40B6750
```
The prompted message to delete the shadow-copies:

![User Account Control](image1.png)

The malware creates a VBS script file and executes it, used to hide some of its execution steps:

```
Set ob = wscript.createobject("scripts.shell")
ob.run "\"echo SET oe = os.replacedirectory("\"C:\Users\username\Desktop\Malware\\"\",\"C:\\Program Files\\\Malware\\"\")\" > vbs
ob.run "\"echo DELETE /s /q /a /f \"\"C:\\Program Files\\\Malware\\"\"\" > vbs
ob.run "\"echo \"\" > vbs
ob.run "\"\"> vbs
```

```
Eventually it also adds itself to registry for persistence.

The malware needs to propagate a GUI window to the interactive user. It does that by executing "taskse.exe" with the command-line argument "@WanaDecryptor@.exe". Notice that this software is now executed without arguments as opposed to previously. This means that it will now create a GUI window and display the results of the attack to the user.

Taskse.exe is executed:

Lastly, @WanaDecryptor@.exe executes its GUI window:
The ransomware window pops up:

![Ransomware Window](image)

**PARANOID Execution Flow Detail**

Simplified Execution Flow:

Prevention mode:

![Execution Flow Diagram](image)

Malware does not continue further to next stages after preventing the encryption attempt.
The Nyotron Attack Response Center Detail

The WannaCry attack has had a strong infection rate across broad geographies, it’s full effect has likely not yet been realized, and propagation is expected to increase as the malware authors work to change their infection techniques. While the attack’s scale is exceptional, WannaCry was not the most dangerous zero-day exploit type attack, nor did it use an extraordinary method for intruding or vectoring into an organization. The attacker used a publicly available exploit; a simple yet effective entry vector which worked well because their targets were unpatched and or, were too dependent on predictive technology defense mechanisms.

The attack’s success rate suggests that organizations should prepare for additional variant attacks from the same malware authors.
In general, when speaking about remote code execution vulnerabilities in Microsoft products (especially in Windows), the scope of infected endpoints will most-likely be very large, simply because there are plenty of vulnerable targets that don’t or cannot pay attention to security updates.

Updating your operating system may seem like the obvious solution, but when you’re on the IT front lines in the real world of budgets, time constraints, and business operations, organizations fall behind the patch management curve. Applying your service packs, hotfixes and special security updates must be a priority, especially if organizations plan to continue to use predictive technologies as their only malware defensive layer against known and known-unknown variant threats. Without security patch updates, predictive solutions will not be able to respond effectively to attacks of this nature. Finely tuned phishing techniques will continue to leave organizations vulnerable to attack. Countermeasures should include training for personnel on how to avoid suspected phishing links, emails and other entry vector mechanisms. Consider publishing a corporate best practices guide on how to avoid risky web and email content.

There is a persistent and real danger to prepare for in the form of a truly never-seen-before ransomware attack with this same level of scale. While this has not yet been realized, we recommend taking the appropriate defensive measures now to defend your assets from damage.

Based on the success of WannaCry ransomware alone, we foresee that a malware author will create a truly unknown-unknown attack, or an attack in which no evidence or indicators of previous malicious intent exist. This type of sophisticated attack will easily evade unpatched and patched operating systems and predictive defense technologies will likely be blinded without that comparator, that breadcrumb of historical evidence to identify the threat.
Summary and What To Do Now

Nyotron’s senior security scientists recommend defending against this type of attack by first ensuring that all operating system patches including service packs, hotfixes and special security updates are current. Once updated, predictive technologies such as artificial intelligence, machine learning, or behavioral analysis could be used to detect and stop most variant attacks. Predictive threat chase engines require updated operating system components, and rely on previously seen predictive behaviors, mathematics, or intelligence schemes to detect and prevent malware variants like WannaCry.

If your real-world business challenges dictate that you will always be behind that operating system patch-update curve, then Nyotron highly recommends selecting a deterministic malware defense system that ignores your patch update status and protects you from damage; data manipulation, encryption, and exfiltration regardless of operating system status. Threat agnostic solutions offer protection and near zero exposure to damage. These solutions can quickly identify and stop today’s known, known-unknown attacks like WannaCry ransomware, and the more dangerous unknown-unknown attacks expected in the days ahead.

*This attack was successfully prevented by PARANOID’s Threat-Agnostic Defense™ regardless of the patch status.*

About Nyotron

*Nyotron is a privately held cybersecurity company that has developed a disruptive threat-agnostic defense technology to cope with the biggest challenge of today’s digital era — the unknown threat. PARANOID is designed to prevent targeted and advanced national-level cyber-attacks on high-profile enterprises, and it does so without any previous knowledge about the threat or its methodologies. Based on a unique last-line-of-defense approach, the company’s technology is designed to protect enterprise data and critical assets by mitigating threats that are able to outsmart all security layers. Nyotron’s customer base includes all major industries.*