Information Security: Wanna Decryptor (WNCRY) Ransomware Explained

Posted by Bob Rudis May 12, 2017
Mark the date: May 12, 2017.

This is the day the "ransomworm" dubbed "WannaCry" / "Wannacrypt" burst — literally — onto the scene with one of the initial targets being the British National Health Service. According to The Guardian: the "unprecedented attack… affected 12 countries and at least 16 NHS trusts in the UK, compromising IT systems that underpin patient safety. Staff across the NHS were locked out of their computers and trusts had to divert emergency patients." A larger estimate by various cybersecurity firms indicates that over 70 countries have been impacted in some way by the WannaCry worm. As of this post's creation time, a group with the Twitter handle @0xSpamTech has claimed responsibility for instigating the attack but this has not yet been confirmed.

What is involved in the attack, what weakness(es) and systems does it exploit, and what can you do to prevent or recover from this attack? The following sections will dive into the details and provide guidance on how to mitigate the impact from future attacks.

What is "Ransomware"?

Ransomware
"malicious software which covertly encrypts your files – preventing you from accessing them – then demands payment for their safe recovery. Like most tactics employed in cyberattacks, ransomware attacks can occur after clicking on a phishing link or visiting a compromised website." (https://www.rapid7.com/solutions/ransomware/)

However, WannaCry ransomware deviates from the traditional ransomware definition by including a component that is able to find vulnerable systems on a local network and spread that way as well. This type of malicious software behavior is called a "worm" and the use of such capabilities dates back to 1988 when the Morris Worm spread across the internet (albeit a much smaller neighborhood at the time).

Because WannaCry combines two extremely destructive capabilities, it has been far more disruptive and destructive than previous cases of ransomware that we've seen over the past 18-24 months.

While the attackers are seeking ransom — you can track payments to their Bitcoin addresses:

- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

here: https://blockchain.info/address/ — there have been reports of this also corrupting drives, adding a destructive component as well as a ransom-recovery component to the attack.

What Systems Are Impacted?

WannaCry only targets Microsoft Windows systems and is known to impact the following versions:

- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016
- Windows XP (

However, all versions of Windows are likely vulnerable and on May 13, 2017 Microsoft issued a notification that included links to patches for all impacted Windows operating systems — including Windows XP.

As noted, Windows XP is impacted as well. That version of Windows still occupies a 7-10% share of usage (as measured by NetMarketshare):

and, this usage figure likely does not include endpoint counts from countries like China, who have significant use of "aftermarket" versions of Windows XP and other Windows systems, making them unpatchable.

The "worm" component takes advantage of a Remote Code Execution (RCE) vulnerability that is present in the part of Windows that makes it possible to share files over the network (known as "Server Message Block" or SMB). Microsoft released a patch -MS17-010 - for this vulnerability on March 14th, 2017 prior to the release of U.S. National Security Agency (NSA) tools (EternalBlue / DoublePulsar) by a group known as the the Shadow Brokers. Rapid7's Threat Intelligence Lead, Rebekah Brown, wrote a breakdown of this release in a blog post in April.

Vulnerability detection tools, such as Rapid7's Metasploit, have had detection capabilities for this weakness for a while, with the most recent Metasploit module being updated on April 30, 2017.

This ransomworm can be spread by someone being on public Wi-Fi or an infected firm's "guest" WiFi and then taking an infected-but-not-fully-encrypted system to another network. WannaCry is likely being spread, still, by both the traditional phishing vector as well as this network worm vector.

What Can You Do?

- Ensure that all systems have been patched against MS17-010 vulnerabilities.
- Identify any internet-facing systems that have not been patched and remediate as soon as possible.

- Employ network and host-based firewalls to block TCP/445 traffic from untrusted systems. If possible, block 445 inbound to all internet-facing Windows systems.
- Ensure critical systems and files have up-to-date backups. Backups are the only full mitigation against data loss due to ransomware.

NOTE: The Rapid7 Managed Detection & Resoponse (MDR) SOC has developed detection indicators of compromise (IOCs) for this campaign, however we are only alerted once the malware executes on a compromised system. This is not a mitigation step.

UPDATE - May 15, 2017: For information on how to scan for, and remediate, MS17-010 with Nexpose and InsightVM, please read this blog.

A Potentially Broader Impact

We perform regular SMB scans as a part of Project Sonar and detected over 1.8 million devices responding to full SMB connection in our May 3, 2017 scan:

Some percentage of these systems may be Linux/UNIX servers emulating the SMB protocol but it’s likely that a large portion are Windows systems. Leaving SMB (via TCP port 445) open to the internet is also a sign that these systems are not well maintained, and are also susceptible to attack.

Rapid7’s Heisenberg Cloud — a system of honeypots spread throughout the internet — has seen a recent spike in probes for systems on port 445 as well:

Living With Ransomware

Ransomware has proven to be an attractive and lucrative vector for cybercriminals. As stated previously, backups, along with the ability to quickly re-provision/image an impacted system, are your only real defenses. Rapid7 has additional resources available for you to learn more about dealing with ransomware:

- Understanding Ransomware: https://www.rapid7.com/resources/understanding-ransomware/
- Ransomware FAQ: https://community.rapid7.com/community/infosec/blog/2016/03/22/ransomware-faq-av oiding-the-latest-trend-in-malware

If you’d like more information on this particular ransomworm as seen by Project Sonar or Heisenberg Cloud, please contact research [at] rapid7 [dot] com.

Many thanks to the many contributors across Rapid7 who provided vital information and content for this post.

For more information and resources on WannaCry and ransomware, please visit this page.
35343 Views Tags: microsoft, windows, worms, ransomware, wannacry, wannacrypt, ms017-010

Russ Verbofsky
May 17, 2017 3:32 PM
I have shared this article with members of the New Mexico State Security Users Group. The groups consist of CISOs and CSOs of state agencies within the New Mexico State Government. The article is well done and concise.

Tengku Alif
May 17, 2017 6:02 AM
Very informative article. Thank you!

Jet Chan *in response to* *Bob Rudis* *on page 4*
May 16, 2017 12:08 AM
Agreed. During the outbreak, awareness is too late or rather slow to see the result. Action (or Re-action) should come first.

Austin Murphy
May 15, 2017 11:17 PM
Thanks

Bob Rudis *in response to* *ironjack11* *on page 4*
May 15, 2017 9:08 PM
Awareness does no good with a worm. There is no confirmation that the primary infection vector for WCry was a phishing e-mail and the post needed to focus on things more centric to WCry.

We did make sure that Awareness was covered in the links provided, so it's there, but not directly in this blog post.

ironjack11
May 15, 2017 8:09 PM
I'm a little surprised and a little disappointed that under your category "What can you do" you don't mention security awareness training.

Aziz Hafid
May 15, 2017 7:58 PM
Thanks

jeremy W

May 15, 2017 5:20 PM

Thanks for the post. We were so bogged down with identify, patch, validate that we overlooked a major mitigation: backups. This post was a friendly reminder so thank you.

Sylvain Drapeau

May 15, 2017 3:47 PM

Again, an great recap explaining the why, how, where and when.

Thanks a lot Bob Rudis !