FROM THE STROZ FRIEDBERG BLOG

WERE YOU READY FOR WANNACRY?

Last week's ransomware attack was by all accounts one of the most widespread cyber events we've seen. The pace at which the malware proliferated and the scope of the impact across companies and geographies was unprecedented. As the new work week begins, it's unclear whether the worst is behind us – a "kill switch" that neutered the original version of WannaCry was discovered and registered, but new variants have already been found circulating. Our technical team is analyzing samples of WannaCry and we're monitoring this situation closely as it evolves. We plan to publish additional information and advisories in the coming days.

Below we offer more detail on the nature of the original ransomware and what you can do to protect your organization. If you have already been impacted and require assistance stopping the spread, determining the impact or recovering your data, please contact us immediately. We can help. Regardless, we strongly recommend all organizations take action now to determine: Are you ready:

+ When was the last time you reviewed your company's patch management program? Your disaster recovery and business continuity plans?

+ Can you identify where all of your mission critical data resides and whether regular backups are being made?

+ Does your cyber insurance policy provide adequate coverage? Have you taken the necessary steps to ensure you will be eligible to make a claim if your company is impacted?

+ Have you communicated with employees about the latest phishing and social engineering techniques?

+ Do you have an incident response plan in place and has it recently been tested so everyone knows what to do in the event of an attack?

+ Are all necessary technical and procedural controls in place and operating properly?

+ Has your security posture recently been assessed and tested and have you acted on the results?

What is WannaCry ransomware?

WannaCry (aka WannaCryptor and Wana Decrypt0r) is a form of ransomware being spread through an exploit called ETERNALBLUE that infects Windows computer systems via a vulnerability in the SMBv1 protocol (MS17-010, a vulnerability in Server Message Block). WannaCry targets and encrypts 176 file types, including Office documents, multimedia files, database files, amongst many others, and demands payment for a key to decrypt, or unlock, the files.

Am I impacted?

If you are running Windows computers in your environment that remain unpatched for MS17-010, you are likely at risk. Please see our guidance below on how to remediate this vulnerability and protect your organization.

What does it do and how does it do it?

This malware creates a copy of itself and executes on the vulnerable computer. Once running, the malware attempts to connect to a specific domain; if it is able to do so, it simply exits without releasing its ransomware payload (WannaCry). This "kill switch" was discovered and registered by a security researcher over the May 13th weekend effectively creating a sinkhole[1] that temporarily halted the spread of the initial version of WannaCry; however, security researchers from Kaspersky have already confirmed new WannaCry variants, and it is likely more will surface.

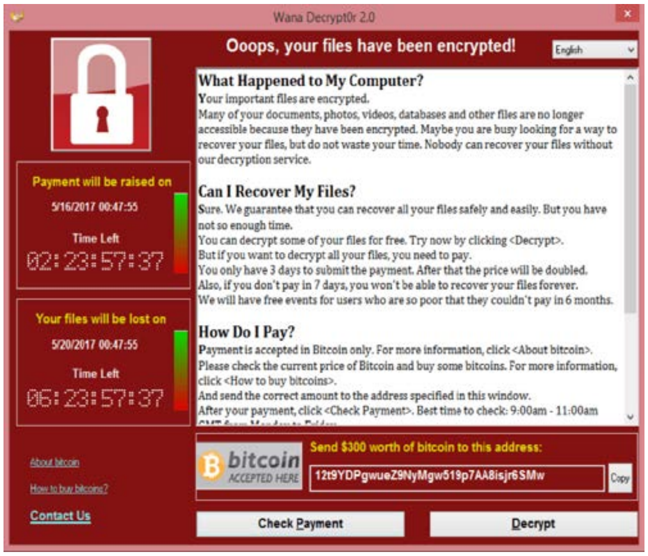
If the malware is unable to connect to the domain, it activates itself by copying and executing the WannaCry ransomware on the infected machine, which then encrypts the machine's files so they are inaccessible. The ransomware then demands payment of $300 to $600 in Bitcoin in return for a key to unlock the files.

Organizations should understand that machines already infected with WannaCry will not get their files back just because the "kill switch" described above was registered. There is currently no known method for breaking the ransomware's encryption. As discussed below, organizations may be able to circumvent the ransomware if proper backup copies of impacted files exist and can be properly restored once all infected systems have been patched.

How do I know if my organization is infected with WannaCry?

If the ransomware is activated on an infected system, two prevalent actions will occur:

1. A user's files will become encrypted with the extension ".WCRY" ".WNCRY" and/or ".WNCRYT", and will not be accessible
2. The decryptor tool (Wana Decrypt0r) will run automatically and display the following ransom message on an infected machine:



What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Can it spread from machine to machine?

Yes. WannaCry's worm-like behavior and its ability to easily propagate across the organization make this a particularly dangerous strain of ransomware. The malware spreads from the infected computer by scanning other computers and systems on the network, and over the internet, and infecting these connected machines by exploiting the same vulnerability, all without any user action. Essentially, it only takes one infected user on a network to put the whole organization at risk.

[1] Tactic used by researchers to redirect traffic from the infected machines to a self-controlled system.

What should you do to protect yourself?

We suggest the following best practices you can adopt and implement to protect your organization from WannaCry:

+ One of the most important things you can do immediately (if you haven't already) is patch all affected Windows systems against the vulnerability in SMB server. Microsoft released Microsoft Security Bulletin MS17-010 for remediating the vulnerability and has also made patches available for otherwise unsupported Windows systems (XP, Server 2003 and Windows 8) that are also affected. If you cannot patch directly, TrendMicro suggests using a virtual patch to help mitigate the threat.

+ If patching is not possible, organizations should consider segregating machines that cannot be patched - for example at least blocking access to SMB ports on these machines (TCP/445 and TCP/139).

+ Organizations should also ensure SMB ports (TCP/445 and TCP/139) are blocked at the firewall and appropriate network devices for inbound traffic.

As noted earlier the version of WannaCrypt that was circulating last week had a "kill switch" logic condition that checked with the command and control (C2) domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com before deciding whether to encrypt the system. A security researcher working with law enforcement has now registered this domain. We recommend companies allow outbound traffic to this C2 domain to continue; or sinkhole the domain internally by redirecting traffic to an internal server. Both solutions will help take advantage of this flaw in the WannaCry code and maximize visibility into systems that are compromised.

+ Given that we have already seen the attack evolve, customers should consider additional defenses to stop the spread of WannaCry and other SMBv1 attacks by disabling the SMB protocol altogether on systems that do not require it and disabling SMBv1 on machines that do. We would advise against enabling unneeded services to limit the ways an attacker could exploit a vulnerability in your IT environment.

+ Organizations may also consider additional measures such as deploying the NoMoreCry Tool from CCN-CERT, which prevents the execution of the WannaCry ransomware **(NOTE: It does not clean already infected systems)**.

+ Like many other ransomware families, WannaCry calls "vssadmin.exe" to delete Volume Shadow Copies. Organizations may want to consider as both a short and long term recommendation to rename that executable to something more unique so that WannaCry (and other ransomware) cannot use the executable to delete Volume Shadow Copies -- which would otherwise prevent any chance of a quick system recovery. Relatedly, once the step above is performed, organizations should consider enabling Volume Shadow Copies on all systems in case of infection and have a cold archive backup that is disconnected from the network. This should allow restore of any files affected by ransomware.

+ As in many cases of malware, infection can occur via spam and other social engineering / phishing campaigns. Remind the people in your organization to take great care when clicking on any links in email and only open files from trusted sources (and even then confirm that the email and file are legitimate). The organization should also ensure that its end point solution can protect systems from email-based malware and enable the solution if it is not already working.

For additional recommendations, we recommend you read the recently released TrendMicro guidance.

About

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. Our focus is on cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; intellectual property; and due diligence. Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

STROZ FRIEDBERG
an Aon company

AON
Empower Results®