Warning: Massive "WannaCry" Ransomware campaign launched

By Tim Berghoff

Published: 2017-06-08 · Archived: 2026-04-05 17:48:23 UTC

05/12/2017

Reading time: 8 min (2073 words)

An outbreak of the latest version of "WannaCry" has been claiming victims in several countries. The speed and ferocity of the outbreak has taken many by surprise. Researchers are as yet puzzled as to the origin of the outbreak which hit 11 countries within just three hours. So far Spain and Russia were are among those who were hit hardest.

Like a bolt from the blue

In the early morning hours (CET) of Friday, May 12, a sizeable wave of infections with the latest iteration of the WCry / WannaCry ransomware was spotted. Researchers are not sure where the sudden onslaught came from, but suspicions currently include bot nets, exploit kits, infected emails or malicious advertizing (also called *malvertizing*). In Spain, Telefónica, a major ISP, was hit with an infection on one of their internal servers. From there, things escalated to a point where IT staff are reaching out to employees to shut down their computers immediately. They were also asked to cut any VPN connections in order to stop the ransomware from ravaging more parts of the company's network. According to Spanish newspaper *El Mundo*, some utility companies had their networks affected in a similar fashion. According one data source, Russia has reported the highest number of infections.

So far the extent of the damage is unknown.

Implications

The unfolding events make it abundantly clear that ransomware is a problem for companies of all sizes.
Since utilities and telecommunications are considered "essential and critical infrastructure", adequate measures must be take to secure those.

Countermeasures

Virus signatures should be updated immediately.
G DATA customers are protected. The WannaCry ransomware is detected by all of G DATA's solutions as ***Win32.Trojan-Ransom.WannaCry.A*.**

Since the vulnerability was addressed in the March update for Windows, updates should be installed as soon as possible. In addition to this, Microsoft has also released a mitigation patch for some legacy versions of Windows which should also be applied immediately.

File-based IOCs

EXE files

"ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"
"09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa" [Win32.Trojan-Ransom.WannaCry.A]
"ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa" [Win32.Trojan-Ransom.WannaCry.A
]"2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd" [Win32.Trojan-Ransom.WannaCry.A]
"24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c" [Win32.Trojan-Ransom.WannaCry.D]
"4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982" [Win32.Trojan-Ransom.WannaCry.D]
"6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7" [Win32.Trojan-Ransom.WannaCry.D]
"b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7" [Win32.Trojan-Ransom.WannaCry.D]
"b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25 [Win32.Trojan-Ransom.WannaCry.E]

DLL:
"CYBER1be0b96d502c268cb40da97a16952d89674a9329cb60bac81a96e01cf7356830.E1E" [Win32.Trojan-Ransom.WannaCry.F]

WannaCry Batch component:
"f01b7f52e3cb64f01ddc248eb6ae871775ef7cb4297eba5d230d0345af9a5077" [BAT.Trojan-Ransom.WannaCry.C]

WannaCry VBS-component:
"51432d3196d9b78bdc9867a77d601caffd4adaa66dcac944a5ba0b3112bbea3b" [Script.Trojan-Ransom.WannaCry.B]

WannaCry Shortcut:
"a3b014598d6313c96ab511dc56028ef36f8bafde7f592a1329238718e1c29813" [Win32.Trojan-Ransom.WannaCryLnk.A]

File extension:

.wncry
Ransom note: @Please_Read_Me@.txt

https://twitter.com/malwrhunterteam/

Network-based IoCs

The "genuine" WannaCry dropper attempts to contact the following web address:

hxxp[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

This is the original "killswitch" domain.

Preview image credit: MalwareHunter

Update: May 12, 8:20 pm: WannaCry uses a leaked NSA exploit to infect machines - how to mitigate

It seems that the mechanism used by WannaCry is based on exploit code originally developed by the NSA. The Exploit is called **ETERNALBLUE** and was part of a series of files which were leaked last month.

The security flaw in SMB which made the exploit possible (also referenced in the NVD) and which was rated "critical" has been patched by Microsoft during March patch day.

G DATA strongly recommends to install all Windows updates or implement the workaround suggested by Microsoft as soon as possible.

Update: May 12, 11:20 pm

IOC list updated & Detection names added

Update: May 13, 7:30 am: train timetable displays in Germany infected, NHS declares "major incident"

First WannaCry infections were reported in the timetable displays of various train stations in Germany. The infection wave has spread across several hospitals in the UK, forcing staff to use paper-based fallbacks to maintain a basic service level. The NHS declared this a "major incident". Doctors are joining in with warnings that the WannaCry infections may cost lives.

Update: May 13, 9:15 am - Microsoft releases a mitigation patch for Windows XP, Windows 8, Server 2003 to address vulnerability

Given that there is still a large number of Windows XP installations out there (including those in critical places), Microsoft has made an unusual move and issued an update for Windows XP, Windows 8 and Windows Server 2003.

Update: May 15, 8:30 am: Accidental hero throws a wrench in WannaCry's works

A security researcher had begun analyzing WannaCry as soon as it hit the ground. During his examinations he found out that WannaCry attempts to contact a specific domain. The domain was not registered at the time, so he took it on himself to do so in order to find out what WannaCry wanted to chat about. This is a common procedure in security research.

It later turned out that the domain was in effect a "killswitch" for WannaCry. The principle is rather simple: WannaCry contacts the domain and waits for a reply. If a reply comes back, it shuts off and does not infect the system. Initially, the researcher was not aware of the fact that this killswitch existed, so the fact that this discovery helped slow down the infection wave significantly was a happy accident - many news portals refer to him as "The accidental hero of WannaCry".

This is good news of course: new infections are stopped in their tracks. There are two major caveats about this, though: the killswitch only works on machines which were not previously infected. It cannot "clean" an infected system and it will not bring back encrypted files. Also, the killswitch domain will not work if the to-be-infected machines are located behing a proxy server.

Still, the slowdown allowed security staff to breathe a sigh of relief, albeit a cautious one.

Update: May 15, 8:50 am: "Brace for impact"

As mentioned previosly, the full extent of the infection wave may only become apparent this Monday morning when workers return to their offices. Therefore users should pay really close attention to any messages they see on screen and alert their IT department immediately as soon as a ransom note appears on screen.

It is also goes without saying that email attachments should be treated with utmost caution, especially if they were received after Thursday, May 11.

Update: May 16, 3:00 pm: Some things are not adding up - Copycats give researchers trouble - Attribution attempts

Although many researchers are warning that "this is not over yet", there are some things that strike us as odd around WannaCry. First and foremost, the intention of any ransomware campaign is to rake in as much money as possible in the shortet amount of time. With the infection count at over 200,000 and counting, one would expect the attackers' Bitcoin wallets almost bursting at the seams. However, only three BTC wallets have been identified so far and they only have a meager 60.000 dollars to show between them. Even if we calculate this in a very conservative manner and assume that about 2,5% of the victims actually pay up, we should still at least be looking at seven-figures in Bitcoins. That does not seem to be the case, though, which opens up room for speculations.

There are several possibilities as to why there does not seem to be any money transferred. For instance, the people behind the ransomware attack may not have anticipated that their creation would be so wildly successful and were just overwhelmed by the infection rates - triggering decryption in WannaCry's case is a manual process which on this scale requires a lot of resources.

To make life even more difficult, there are large numbers of "copycat" version circulating. After many people had gotten their hands on a sample, they started experimenting with it. In some cases, they disabled the killswitch domain, in other cases its URL is changed. Some of the versions would not even work as other modifications were made in the file. Those modifications often "break" a file and make it unusable for infecting a machine. At the time of this writing, several hundred modified versions of the file have been counted by G DATA and were also added to our detection database.

As with any man-made event that causes great damage, the question of "who done it?" inevitably comes up. This case is no different. Some researchers point out that some routines of the malware bear characterisitics that were seen in attacks by an APT group called Lazarus. At this point we cannot rule out this possibility, but neither can we confim it.

Update: May 17, 9:45 am: Copycats vs. Duplicates

As mentioned in our previosu update, numerous updates of the WannaCry files are in circulation at this time. We need to distinguish several categories here:

- Variations of the original file with the killswitch removed
- Variations with a modified killswitch domain
- Variations without ransomware components; those are able to spread without performing any malicious activities on a system.
- "Real" copycats which imitate the ransom note of Wannacry, but do not have any connection to WannaCry on the technical side.

Correction:
Contrary to what was mentioned in the previous update, the decryption components do not need to be created manually as they are part of the malware already. However, the decryption process must still be triggered manually by the attackers.

Update: 17.05., 10:00 Uhr - IoC list updated

Killswitch domain added under "Network-based IoCs"

Update: May 18, 12:30 pm: parking garages in Germany hit with WannaCry - distribution method still unclear

According to current reports, the payment systems in some German parking garages are affected by the WannaCry infection wave. The company that rund the parking garages has not issued a statement about how much money was lost due to the outage, but this example show very clearly what a direct effect a ransomware infection can have on everyday operations. This development is problematic for another reason: should the outage continue for longer, traffic jams may develop because it is now impossible to keep track of how much parking space (if any) is left in the garage. This would cause drivers to attempt entering a (full) parking garage.

The exact mehtod used by WannaCry to spread this rapidly is still unclear. However, at this point it seems unlikely that email attachments were used as a vessel. As previously reported, WannaCry uses a security flaw in the fil and folder sharing protocol of Microsoft Windows. This akes it possible to distribute the malware over the internet as the protocol is usually not filtered out by ISPs. This makes an infection more likely if a system is connected directly to the internet with this feature enabled. Note, though, that this is also based on conjecture, but for a definitive answer, more information is needed.

Update: May 18,12:30 pm: Makers of WannaCry are speaking up

The message some victims of WannaCry are starting to see right now (Image credit: Twitter / Thijs Bosschert)

As we have learned about an hour ago, some victims of the WannaCry infection are getting messages on their screens which appear to come from the attackers. The message asks victims to send the attackers their unique Bitcoin ID one hour prior to making the payment to speed up the process of receiving their decryption key.

This is the first time since the infection wave has started that the attackers seem to speak up. We had already suspected that they may have been overwhelmed by their own success and had difficulties coping with it.

What is still unclear, though, is where the ransom payment are supposed to go - up to now, only three BTC wallets have been identified that were associated with the attackers.

We still strongly discourage making any ransom payments.

Update: June 8, 12:00 pm: WannaCry is still no blunt axe

Reports from the Health & Human Services department clearly show that despite its famed kill switch the danger from WannaCry is not over. Since machines in several hospitals are still affected, HHS experts advise affected organizations to rebuild (or reimage) affected systems and to install the latest updates as quickly as possible. Even though the kill switch prevents WannaCry's ransomware module to kick in and encrypt files, the worm part of WannaCry is not affected by this - WannaCry remains on the lookout for vulnerable machines.

Related articles:

Share Article

Source: https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign