Security Newsletter

15 May 2017

WannaCRY ransomware is spreading like wildfire across the globe

A major ransomware attack has affected many organizations across the world reportedly including Telefonica in Spain, the National Health Service in the UK, and FedEx in the US. The malware responsible for this attack is a ransomware variant known as 'WannaCry'. What makes it so dangerous is its capacity to spread over the internet, like worms such as Conficker or Blaster did back in the day, exploiting a recently patched SMB vulnerability.

Additionally, researchers from Talos Intelligence have observed WannaCry samples making use of DOUBLEPULSAR, which is a persistent backdoor that is generally used to access and execute code on previously compromised systems. This allows for the installation and activation of additional software, such as malware. This backdoor is typically installed following successful exploitation of SMB vulnerabilities addressed as part of Microsoft Security Bulletin MS17-010, also known as "Eternal Blue". If you seem to recognize those name, it's because they all come from the recent ShadowBroker leak regarding the NSA.

Don't think it is over as we've discovered and activated a "kill switch". At the time of this newsletter, the malware is still active and things may continue to change. While the initial version contained indeed a killswitch (the malware looked up a specific domain and, if it was registered, would exit without doing any harm), some samples have been founds with this kill-switched hexedited-out of the binary. Moreover, organizations that use proxies will not benefit from the killswitch.

Organizations should ensure that devices running Windows are fully patched and deployed in accordance with best practices. Microsoft released a patch for vulnerable systems, including the out-of support Windows XP and Vista. Additionally, organizations should have SMB ports (139, 445) blocked from all externally accessible hosts.

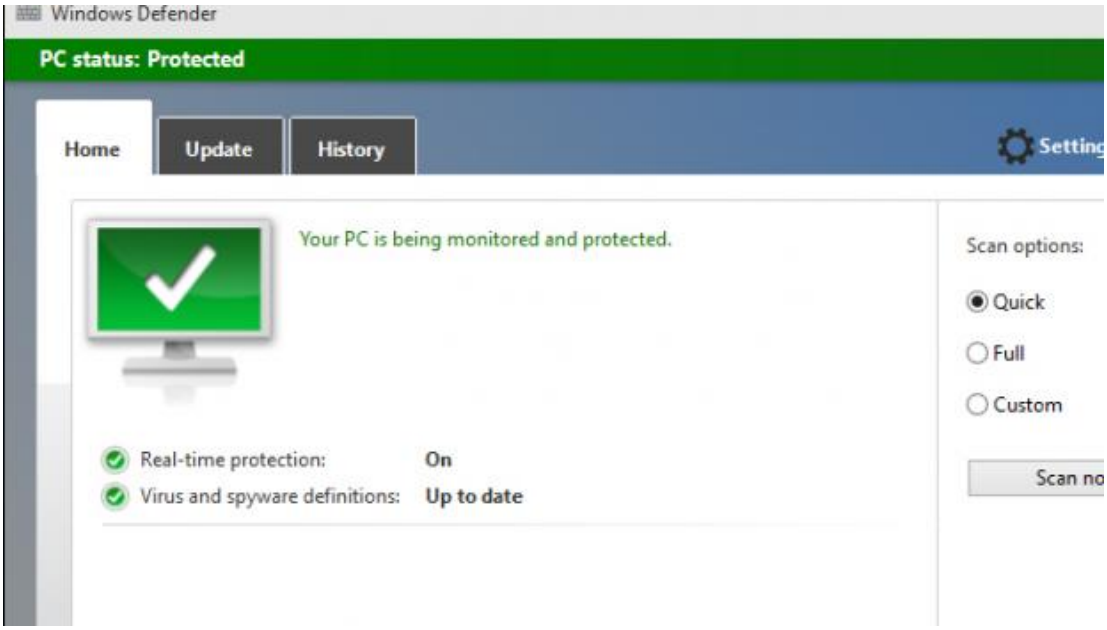
Fact sheet

Report from Talos

Report from BleepingComputers

MS Security Bulletin

Massive vulnerability in Windows Defender leaves most Windows PCs vulnerable



Microsoft on Monday patched a severe code-execution vulnerability in the malware protection engine that is used in almost every recent version of Windows (7, 8, 8.1, 10, and Server 2016), just three days after it came to its attention. Notably, Windows Defender is installed by default on all consumer-oriented Windows PCs.

The exploit (officially dubbed CVE-2017-0290) allows a remote attacker to take over a system without any interaction from the system owner: anything that is automatically scanned by Microsoft's malware protection engine, websites, file shares, emails, could be used as an attack vector. The exploit was also "wormable," meaning they could lead to a self-replicating chain of attacks that moved from vulnerable machine to vulnerable machine.

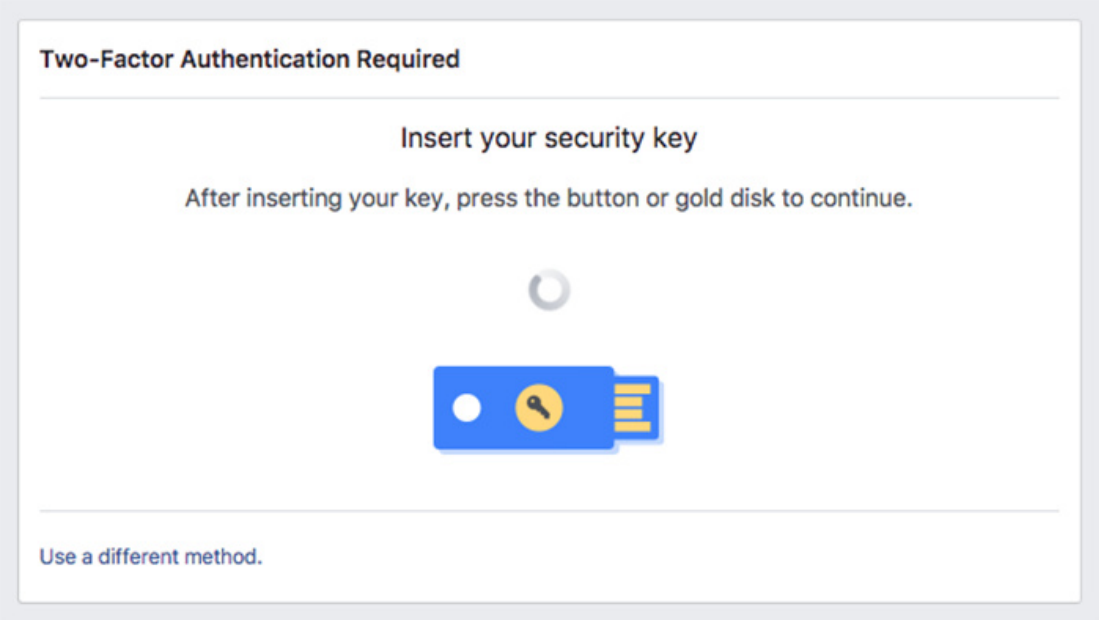
Because MsMpEng runs at the highest privilege level and is so ubiquitous across Windows PCs, this vulnerability is about as bad as it gets. Fortunately, the security researchers who discovered it—Natalie Silvanovich and Ormandy both with Google Project Zero—privately reported technical details, and last night Microsoft announced the patch. MsMpEng automatically updates every 48 hours, so disaster has probably been averted.

The security bulletin notes that Microsoft hadn't seen any public exploitation of the vulnerability.

Read More

MS Security Advisory

How to protect your Google and Facebook accounts with a security key



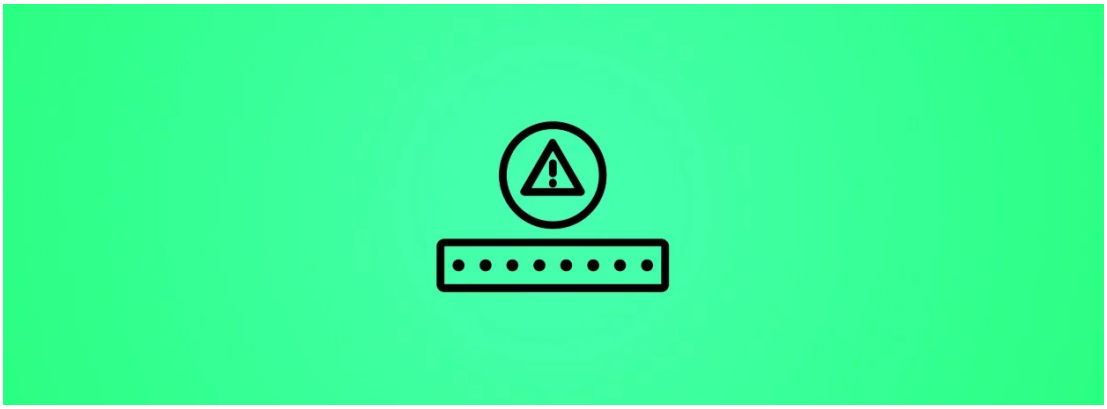
Google supports a format called FIDO Universal 2nd Factor (U2F), which it helped develop. Keys are available that work over USB, Bluetooth, and NFC, so they can be used with a smartphone or tablet in addition to a PC. They are really easy to setup and use.

U2F is currently only supported by two browsers, Google Chrome and Opera. Together, they account for about two-thirds of desktop browsing and are available on Windows, macOS, and Linux, so a good portion of the market is covered, but if you prefer Firefox, Safari, or another browser, you'll need to switch.

Yubico has a helpful matrix on its site detailing compatibility, and there are a couple of listings of sites that support security keys and the standards they use.

Read More

Upcoming NIST Guideline Advocates Simpler Rules for Online Passwords



The US National Institute of Standards and Technology (NIST) is preparing to issue a new Digital Identity Guideline, which unlike its previous editions, will take a softer stance on the complexity of online passwords.

The current draft of the NIST Digital Identity Guideline reveals some of the changes coming next year. These recommendations are important, as they are widely accepted and followed by most government agencies and enterprises around the US, and even around the globe.

The changes show a relaxation of recommended password policies. This relaxation comes after several studies have shown that users tend to use simpler passwords the more complex password rules become. Instead, company should favour the length of the password, blacklist password obtained from previous breach corpuses and use random generators to define initialisation password.

Another major change is to finally stop asking users to change password every three months, but instead ask them to change if there is evidence of compromise. Regular password change for no good reason only leads to weaker passwords in the long run.

Read More

Mac video app HandBrake – now with free spyware

Crooks managed to break into one of the download servers of a popular open-source video converter program called HandBrake. The crooks then uploaded a hacked version of the official Mac download. As a result, anyone who installed or reinstalled HandBrake Version 1.0.7 recently may have ended up with malware known as OSX/Proton-A.

Proton, which targets macOS, does all kinds of nasty behavior, including stealing passwords, keylogging, exfiltrating files and enabling remote access log-in. When this file is being executed, what appears to be a legitimate dialog box appears and asks for the user's password in order to install some "additional codecs." But it is actually to read your KeyChain where MacOS stores your passwords.

If you downloaded the Handbrake Version 1.0.7 DMG outside the timeframe listed above, you are fortunate: you missed the infectious window. If you downloaded the DMG within the infectious window timeframe, you have a 50% chance of being OK, because only the mirror server was hacked. But if you did get infected, and you did find that dreaded proton.zip file, you need to assume the worst: that the crooks know some or all of your passwords.

Read More

Malware details

Security Assessment of OpenVPN

Quarkslab was hired by OSTIF to perform a security assessment of OpenVPN 2.4.0. Quarkslab focused on code and cryptography assessment. Results are briefly described in this blog post, and full report is available at its end.

The review targeted version 2.4.0 and was performed by 3 engineers between 15 February 2017 and 7 April 2017, for a total of 50 man days of effort. Issues were reported to the OpenVPN team and have been fixed in OpenVPN 2.4.2. Only one high severity vulnerability has been found, it allowed to DoS the service with specially crafted packets.

Since the beginning of the project, OpenVPN has followed the best practices for secure development. For examples, wrappers are used to avoid handling strings and buffers directly, assertions are used to avoid that the program ends up in an inconsistent state, secure functions of the C language are used, etc. Best practices of development make the discovery of memory corruption vulnerability unlikely. If vulnerabilities were to be found, logical or cryptographic bugs would be more likely.

Read More

Full report

Game of Thrones makes its stars two-factor their emails now

HBO's Game of Thrones has always had to cope with bizarre threats to secrecy around its plot details — drones flying over set, rogue set photographers, its own actors accidentally posting scripts to Instagram. Then there's the unavoidable obsessive fan interest, which turn things like the length of Kit Harington's hair and a sighting of Rory McCann hanging out in a hotel lobby into spoilers. But now that the show is moving past the story of George R.R. Martin's A Song of Ice and Fire for the first time with season 7, HBO is taking security even more seriously.

In a recent interview with Express, actress Nathalie Emmanuel, who plays Daenerys' BFF Missandei, said the cast was required to set up two-factor authentication on their email accounts this year. They only received digital copies of the script through these accounts, and weren't allowed to print them.

She also mentioned that any notes they received during rehearsal weren't permitted to leave the set: "You might get given rehearsal notes on set, but you have to sign for and return them before you leave. If you don't, people will chase you until you give them back!"

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.