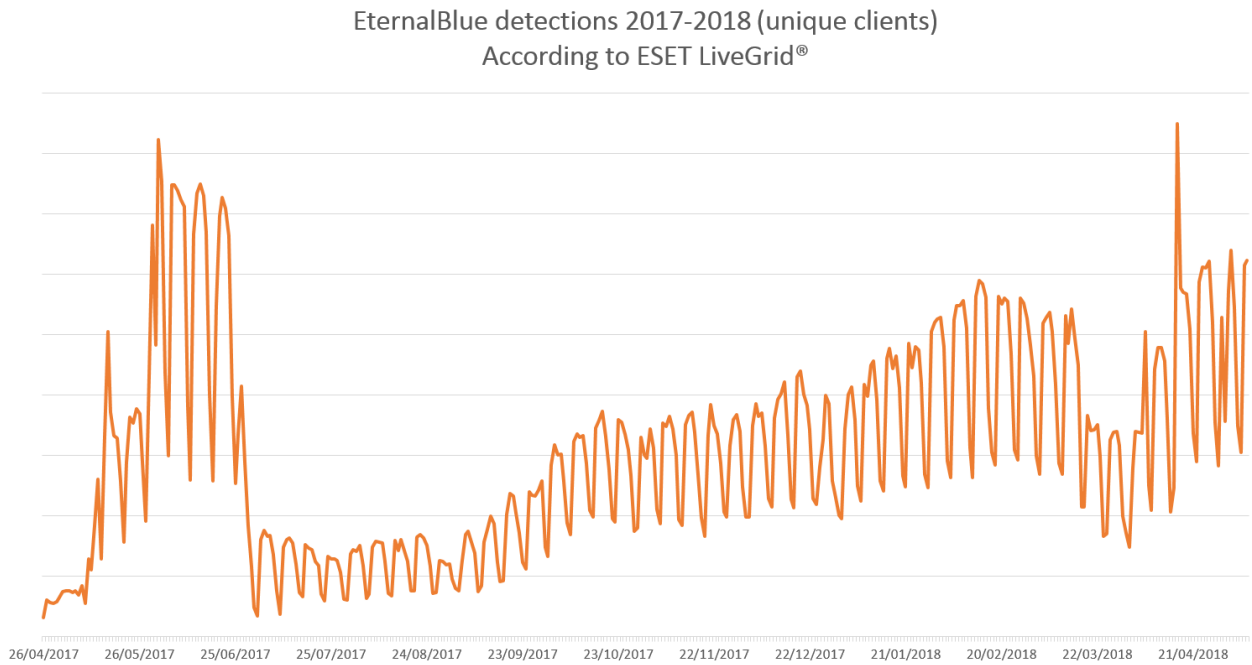
One year later: EternalBlue exploit more popular now than during WannaCryptor outbreak

The infamous outbreak may no longer be causing mayhem worldwide but the threat that enabled it is still very much alive and posing a major threat to unpatched and unprotected systems

It's been a year since the WannaCryptor.D ransomware (https://www.welivesecurity.com/2017/05/13/wanna-cryptor-ransomware-outbreak/) (aka WannaCry and WCrypt) caused one of the largest cyber-disruptions the world has ever seen. And while the threat itself is no longer wreaking havoc around the world, the exploit that enabled the outbreak, known as EternalBlue, is still threatening unpatched and unprotected systems. And as ESET's telemetry data shows, its popularity has been growing over the past few months and a recent spike even surpassed the greatest peaks from 2017.



(https://www.welivesecurity.com/wp-content/uploads/2018/05/EternalBlue2017-May2018-2.png)

The EternalBlue exploit targets a vulnerability (addressed in Microsoft Security Bulletin MS17-010) in an obsolete version of Microsoft's implementation of the Server Message Block (SMB) protocol, via port 445. In an attack, black hats scan the internet for exposed SMB ports, and if found, launch the exploit code. If it is vulnerable, the attacker will then run a payload of the attacker's choice on the target. This was the mechanism behind the effective distribution of WannaCryptor.D ransomware across networks.

Interestingly, according to ESET's telemetry, EternalBlue had a calmer period immediately after the 2017 WannaCryptor campaign: over the following months, attempts to use the EternalBlue exploit dropped to "only" hundreds of detections daily. Since September last year, however, the use of the exploit has slowly started to gain pace again, continually growing and reaching new heights in mid-April 2018.

One possible explanation for the latest peak is the Satan ransomware campaign (https://bartblaze.blogspot.sk/2018/04/satan-ransomware-adds-eternalblue.html) seen around those dates, but it could be

connected to other malicious activities as well.

We must stress that the infiltration method used by EternalBlue is not successful on devices protected by ESET. One of the multiple protection layers – ESET's Network Attack Protection module – blocks this threat at the point of entry. This can be compared to a silent knocking on the door at 2 a.m. testing if someone is still up. As such activity is most likely driven by malicious intentions, the entrance is securely sealed off to keep the intruder out.

This was true during the WannaCryptor outbreak on May 12, 2017 as well as all previous (https://www.welivesecurity.com/2017/05/17/wannacryptor-wasnt-the-first-to-use-eternalblue/) and subsequent attacks by malicious actors and groups.

EternalBlue has enabled many high-profile cyberattacks. Apart from WannaCryptor, it also powered the destructive Diskcoder.C (aka Petya, NotPetya and ExPetya) attack in June 2017 as well as the BadRabbit ransomware campaign in Q4 2017 (https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/). It was also used by the Sednit (https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf) (aka APT28, Fancy Bear and Sofacy) cyberespionage group to attack Wi-Fi networks in European hotels (https://www.bleepingcomputer.com/news/security/russian-cyberspies-are-using-nsa-tools-to-target-european-hotels/).

The exploit has also been identified as one of the spreading mechanisms for malicious cryptominers (https://www.bleepingcomputer.com/news/security/new-massminer-malware-targets-web-servers-with-an-assortment-of-

exploits/). More recently, it was deployed to distribute the Satan ransomware campaign, described only a few days after ESET's telemetry detected the mid-April 2018 EternalBlue peak.

The EternalBlue exploit was allegedly stolen from the National Security Agency (https://www.nsa.gov/) (NSA) probably in 2016 and leaked online on April 14, 2017 by a group dubbed Shadow Brokers. Microsoft issued updates that fixed the SMB vulnerability on March 14, 2017, but to this day, there are many unpatched machines in the wild.

This exploit and all the attacks it has enabled so far highlight the importance of timely patching (https://www.welivesecurity.com/2018/04/19/patching-shut-window-unpatched/) as well as the need for a reliable and multi-layered security solution that can block the underlying malicious tool.

Ondrej Kubovič (https://www.welivesecurity.com/author/okubovic/) 10 May 2018 - 02:57PM

Similar Articles

(https://www.welivesecurity.com/2018/05

(https://www.welivesecurity.com/2018/04

two-zero-days/)

A tale of two zero-days (https://www.welivesecurity.com/2018/05/15/tale-two-zero-days/)

update-analysis-zebrocy/)

Sednit update: Analysis of Zebrocy (https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/)

Discussion

0 Comments WeLiveSecurity.com 1 Login

Recommend Share Sort by Best

Start the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy

Contact Us (https://www.welivesecurity.com/contact-us/)

Sitemap (https://www.welivesecurity.com/sitemap/)

Our Experts (https://www.welivesecurity.com/our-experts/)

ESET (https://eset.com)

How To (https://www.welivesecurity.com/category/how-to/)

Categories (https://www.welivesecurity.com/categories/)

RSS Configurator (https://www.welivesecurity.com/rss-configurator/)

News Widget (https://www.welivesecurity.com/news-widget-generator/)

()

Privacy policy (https://www.welivesecurity.com/privacy/)

Legal Information (https://www.welivesecurity.com/legal-information/)

Copyright © ESET, All Rights Reserved