Blog: progression (Not)Petya & WannaCry

July 5, 2017 | V. Toms & V. Gevers (GDI.Foundation)

What is happening?
Criminals often attack open system services which have known vulnerabilities in ransomware attacks like WannaCry and (Not) Petya which has been in the news since May until recently. During these ransomware attacks, the *EternalBlue* and *EternalRomance* exploits, which are both exploits of the NSA, were published on the 14th of April 2017 by the Shadow Brokers.

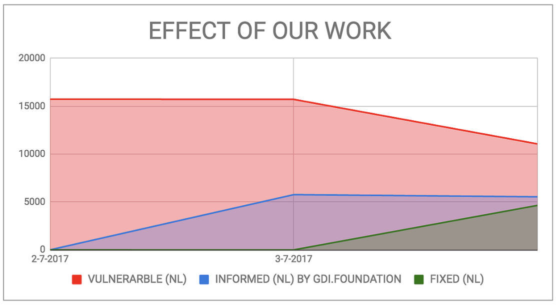
With these exploits others can gain unauthorised access to remote Windows systems and execute malicious software (like the (Not)Petya) with administrative privileges on your server.

Advice:
Protect the vulnerable server with a firewall blocking port 445 or limit the access of the service with network filtering to only accept local connections or via a VPN or a reverse proxy. You must install the MS17-010 patch!

Does our work & Cyber Security Health Dashboard help?

What do we do?
We detect & analyze high risk "criminal" opportunities, share the risk & vulnerabilities with everybody, inform the ones who are at risk and give free advice about solution(s).

Our effort & achievements so far (WannaCry & (Not) Petya [NL])



Source: GDI Public EternalBlue tracker

Sunday 2 July
Public reported our data and picked up by the Dutch press about the state of the Petrya ransomware/wiper.

At that moment there were 15.729 servers/computer systems vulnerable for the Petrya ransomware / wiper in the Netherlands. Worldwide we discovered 953.017 vulnerable servers/computer systems.

Monday 3 July
Nederland.ICT (the industry association of the ICT sector in the Netherlands) offered help informing informing the ones who are vulnerable, located in the Netherlands including smaller companies (SMB).

Tuesday 4 July
- Validating our OSINT feeds with our Nmap scans checking for the vulnerability in the Dutch IPv4 space.
- Obtaining identifying metadata of the vulnerable systems by extracting DNS records, X.509 certificate details, extract Ripe and Whois information for quick labeling "problem owners".
- Setting up a messaging platform (SendGrid) and send a bulk of verified responsible disclosures to identified owners and/or their ISP / hosting company overnight.

Result at the end of the day: 4.643 host were fixed and no longer vulnerable.

Wednesday 5 July
At the end of the day we discovered that a total of 9.294 hosts were not vulnerable anymore after warning the owners by e-mail. So these

Recent

UPDATE BLOG: progression (Not)Petya & WannaCry
July 8, 2017

Blog: progression (Not)Petya & WannaCry
July 5, 2017

Intelligence door aggregatie van open-source bronnen
April 24, 2017

Live demo "Cyber Security Health Check"
March 17, 2017

Ransomware seemingly hits faster than management can fix
February 17, 2017

Zo bescherm je je privacy bij het invullen van de Stemwijzer
February 7, 2017

GDI.Foundation treft eerste ransomware op Elasticsearch aan
January 15, 2017

GDI.Foundation genomineerd voor ISOC.nl Innovatie Award 2017
January 7, 2017

Het resultaat na 366 dagen ethisch hacken: "Security zo lek als een mandje"
January 3, 2017

Our Presentation GFCE (Hungary) & Lesson Learned Responsible Disclosure
May 9, 2016