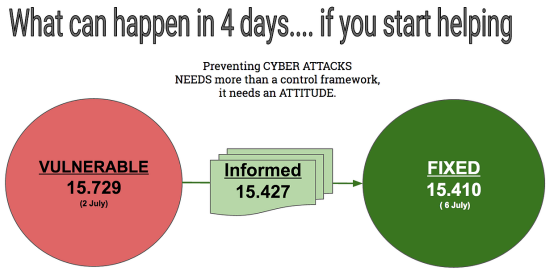
UPDATE BLOG: progression (Not)Petya & WannaCry

July 8, 2017 | V.Toms (GDI.Foundation) &V. Gevers (GDI.Foundation)

THE EFFECT & LESSONS LEARNED.



Source: GDI Public EternalBlue tracker

So did our work, efffort & Cyber Securrity Heallth Dashboard help otthers....?

From our perspective, we strongly believe our dashboard & work contributes to society. *But we are going to need help, t*o make it even more effective and to *help others who are still vulnerable across the world.*

Sharing our "Lessons Learned"

- Full *transparency* in work & status makes *joint effort and actions* possible.
- Exposure in *news & social media* helps
- Holistic approach in *working together* and give the credits to finders/ helpers.
- Always *fact check your evidence* and *use more sources.*
- Be *respectful and polite* in the communication with potential victims when informing them.
- *Less is more.* Give practical advice how to solve and make it short. The idea is that the vulnerability is being solved as soon as possible.
- *Share the evidence* of the vulnerability, only with the victims, so they are able to fact check the situation themself and take the necessary actions in a short time.
- *Helping others* is not about making money, it is about the *intention* of *your action* without expecting something in return.

==========

Whatt diid we do?

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

Scope of our action: the Netherlands

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. We discovered 953.017 vulnerable servers/computer systems Worldwide.

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 labelling “problem owners”.
- Setting up a messaging platform (SendGrid) and send a bulk of verified

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