Wanna cry Ransomware

Korte beschrijving van de werking Facts & figures

***Wanneer?***

*De ransomware maakte zijn eerste appearance in mei 2017. Een eerste infectie vond plaats op 12 mei 2017, in Azie rond 8 uur smorgens. Deze infectie werdt niet veroorzaakt door email phishing, zoals er gedacht werd, maar door een kwetsbare SMB poort. De SMB poort (wat in het lang Server Message Block betekend) heeft meerdere qualiteiten waarvan file sharing en toegang tot remote windows services er enkele van zijn. De malware heeft de capabiliteit om de smb poort te scannen en via hier zijn worm te versprijden.*

***Door wie ontwikkeld en In welke programmeertaal geschreven?***

*De malware werd ontwikkeld door de groep Lazarus. Dit is een cybercrime groep van een onbekend aantal leden uit Noord Korea’s Pyongyang. Park Jin Hyok werd officieel beschuldigd voor de WannaCry attacks. Hij werd betrapt toen hij een spoor van bewijs achteliet dat zijn echte identiteit linkte aan één van zijn aliases “Kim Hyon Woo”. Hij werkte ook onder de titel van “developer” en “online game developer”. Hij gaf voor deze functies aan dat hij kon coderen in Java, JSP, PHP, Flash en C++. Waarvan de laatste codetaal gebruikt werd voor het schrijven van WannaCry.*

*Bron:* [*https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/*](https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/)

*Microsoft visual C++*

***impact en aantal infecties?***

De WannaCry ransomware attack heeft ongeveer 230.000 computers geinfecteerd in meer dan 150 landen. Waaronder ook enkele grote bedrijven en duizenden ziekenhuizen. Vooral het feit dat er zo veel ziekenhuizen geinfecteerd waren, heeft gezorgd voor een grote impact. Ambulances werde omgestuurd onderweg naar patienten of mensen in nood. De ziekenhuizen verloren een grote 92 milljoen pond vanwegen de WannaCry attack. Computersystemen over heel de wereld vielen in duigen, met als gevolg wordt er geschat op een kost van 4 billjoen dollar in verlies.

**Hoe veel verdiende ze zelf?**

Ondanks het grote verlies door de impact van de malware, heeft de hacker groep maar 50.000 dollar in bitcoin verdient. De gemiddelde prijs van het decrypteren van je data is 300 – 600 dollar.