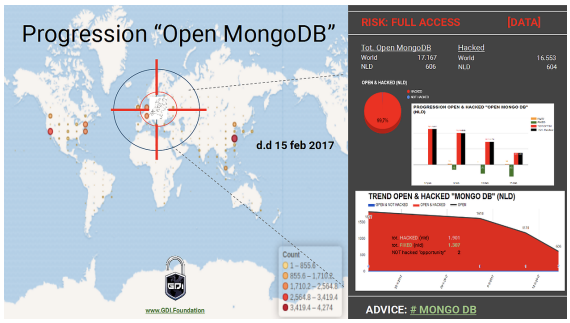
Ransomware seemingly hits faster than management can fix

February 17, 2017 | V.Toms & S. Haanen

With our project "Internet & Cyber Security Health Check" we are developing a platform that gives governments, organizations AND researchers, ethical hackers and others the opportunity to work together and share the necessary information to prevent cyber crime.

In our first prototype report we give some insight about the current situation of the Open MongoDB, hacks, the trend in fixing and solution how to fix.



Some highlights

- When making the analysis it was striking to see that the ransomware job is very sufficient. Nearly all Open MongoDB (1.913 ip's) are hacked and data is been deleted (1.911 ip's) incl. the "new" installed Open MongoDB. Seems like the attackers have an automated job. By the way, the ransomware is for sale on the Internet ($500,-).

- Although there has been quite some publicity about ransomware there were still new MongoDB installed without proper installation. They also got hacked (96 ip's). Maybe better to check the version and security notes before putting a new server in production. Saves a lot of work and annoyances in the organization.

- Another thing that makes us ponder is why hacked serwers are not taken out of production (604 ip's). I can't imagine that the ones that are hacked are all "honeypots". Maybe the owner doesn't even know that they are hit by ransomware and that the data has been deleted. Good thing, I guess, is that the deleted data doesn't have any impact on their business or other ones (?)

- It's very surprising that some organizations who were hit, did the reinstall without fixing the cause (11 ip's). They were hit by the same ransomware, again! Not very clever and I hope they will not make the same mistake the next time.

- We only could inform/ warn 1 organization based on a RD. The others were already hacked at the moment of writing the blog and doing the analyses. We hope that the RD is picked up soon by the owner, so they will be able to fix it before the ransomware hits them.

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