GDI.Foundation treft eerste ransomware op Elasticsearch aan

January 15, 2017 | Gijs Ettes

Researchers Victor Gevers, Niall Merrigan en Matt Bromiley hebben afgelopen nacht de eerste ransomware op de populaire zoekmachinetechnologie Elasticsearch aangetroffen. De opensource zoekoplossing van Nederlandse bodem, die efficiënt enorme hoeveelheden data wereldwijd over honderdtem servers kan doorspitten, wordt wereldwijd door duizenden bedrijven gebruikt. Van kleine Nederlandse uitgevers en Bol.com, tot gigantem als Microsoftt, Netflix en Facebook.

Bij de implementatie van Elasticsearch wordt goede beveiliging regelmatig vergeten. Van de ruim 34.808 open installaties zijn tenminste 102 gehacked door cybercriminelen. In 2015 voorspelden we al dat cybercriminelen hun focus zouden gaan verleggen naar dit soort 'laaghangend fruit'.

In Nederland draaien er 688 open Elasticsearch-implementaties waarvan er 28 operationeel kritisch (SIEM) zijn. Die worden meteen als Responsible Disclosure gemeld, zodat de getroffen organisaties gepaste maatregelen kunnen treffen. GDI.Foundation zal de komende dagen extra energie steken in het opsporen en melden van Elasticsearch-implementaties die kwetsbaar zijn om 'geransacked' te worden door cybercriminelen. Ook monitoren we andere mogelijk kwetsbare en open bronnen op misbruik, om meer slachtoffers te voorkomen.

Het GDI.Foundation jaarrapport 2016 geeft aan dat er nog veel werk aan de winkel is voor 2017. Dit nieuws bevestigt dat vooruitzicht nogmaals. Voor ons is het alle hens aan dek om te voorkomen dat er nog meer data verloren gaat door slecht geconfigureerde en/of onbeveiligde databronnen. Bij de MongoDB ransomware-aanvallen van afgelopen week ging meer dan 100TB aan data verloren.

English: After MongoDB, cybercriminals are now focussing on insecure ElasticSearch installs, our researcher Victor Gevers has found. Of the 34.808 open installs at least 102 have been ransacked, and this number is rising rapidly. In 2015, we already predicted that cyber criminals would shift their attention to this kind of 'low hanging fruit'. In the following days we will devote extra attention to report vulnerabilities and prevent loss of data.

Tags: elasticsearch

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

A safer internet
for everybody and everywhere.
To protect you, me and our kids.
And prevent any misuse of information.

Contact us

Follow us

Reg.nr. 64762815/ Banknr. NL41 ABNA 0488 4071 41