27 aug 2018 -16:05

CERT.be waarschuwt voor nieuw fenomeen: cryptojacking

Afgelopen maanden merken wij een nieuw fenomeen op: cryptojacking. We zien zowel een toename van het aantal infecties als van de complexiteit ervan. Het aantal waarnemingen van coinminers bij eindgebruikers is in 2017 met 8500 procent toegenomen. Aan dit tempo verwachten wij dat cryptojacking een grotere bedreiging wordt dan ransomware. Daarom publiceren wij een brochure over cryptojacking met informatie voor ICT professionals, maar ook voor de eindgebruiker. Ook op de website www.safeonweb.be publiceren we informatie voor de modale internetgebruiker. Je wapenen tegen cryptojacking is immers niet zo moeilijk.

Wat is cryptojacking?
Om te begrijpen wat cryptojacking is, moet je begrijpen wat cryptomunten zijn en hoe je er geld mee kan verdienen. Cryptomunten zijn virtuele munten. Er bestaan momenteel honderden cryptomunten maar bekendste variant is de Bitcoin.
Om een Bitcoin of een andere cryptomunt te verkrijgen en dus geld te verdienen, moet een computer veel berekeningen uitvoeren die een grote hoeveelheid energie (CPU) vereisen. Voor deze berekeningen wordt een computer of smartphone beloond met Bitcoins. Dit proces wordt cryptomining genoemd.
Aangezien het aantal berekeningen, nodig om geld te verdienen, zeer hoog is, zijn steeds meer toestellen nodig om deze berekeningen uit te voeren. Net daarom proberen miners toegang te krijgen tot jouw toestel om het dan zonder jouw medeweten te kunnen gebruiken om cryptomunten te verzamelen. Als dit gebeurt, spreken we over cryptojacking.
Hoe kan je cryptojacking opmerken?
Op het ogenblik dat de cryptojacker actief is, merk je een zeer hoog gebruiksniveau van de grafische kaart en/of CPU op. De browser verbruikt dan 40% of meer van het beschikbare computervermogen. Dit betekent dat de computer of smartphone langzamer werkt, de batterij sneller leeg raakt en de temperatuur van het apparaat stijgt zolang het script loopt. Bovendien leidt een hogere belasting van het apparaat tot een hogere elektriciteitsrekening.
Wat kan je doen om cryptojacking te voorkomen?
• Gebruik een anti-virusprogramma en eventueel een adblocker
• Installeer enkel browserextensies/-plugins die je vertrouwt en die worden aangeboden door een vertrouwde app-store (Google Play, Microsoft store etc.).
• Controleer regelmatig de geïnstalleerde extensies en verwijder de extensies die niet langer nodig zijn. Hoe meer extensies, hoe groter de kans op kwaadaardige extensies of een kwetsbaarheid, dus zorg ervoor dat ze tot een minimum beperkt blijven.
Wij volgen het fenomeen van cryptojacking permanent op. Bedrijven of gebruikers die slachtoffer zijn, kunnen dit melden bij cert@cert.be.

https://www.safeonweb.be/nl/mijn-toestel-wordt-gebruikt-voor-cryptojacking

(Einde persbericht)
Over het CERT.be
Het Federal Cyber Emergency Team (CERT.be), is de operationele dienst van het Centrum voor

Cybersecurity België (CCB), die de overheid, de vitale diensten en de ondernemingen ondersteunt bij de preventie, coördinatie en bijstand bij cyberincidenten. www.cert.be
Over het Centrum voor Cybersecurity België
Het Centrum voor Cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in België. Het CCB stelt tot doel het superviseren, het coördineren en het waken over de toepassing van de Belgische strategie betreffende cyberveiligheid. Door het optimaliseren van de informatie-uitwisseling zullen de bevolking, de bedrijven de overheid en de vitale sectoren zich gepast kunnen beschermen.
www.ccb.belgium.be

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be