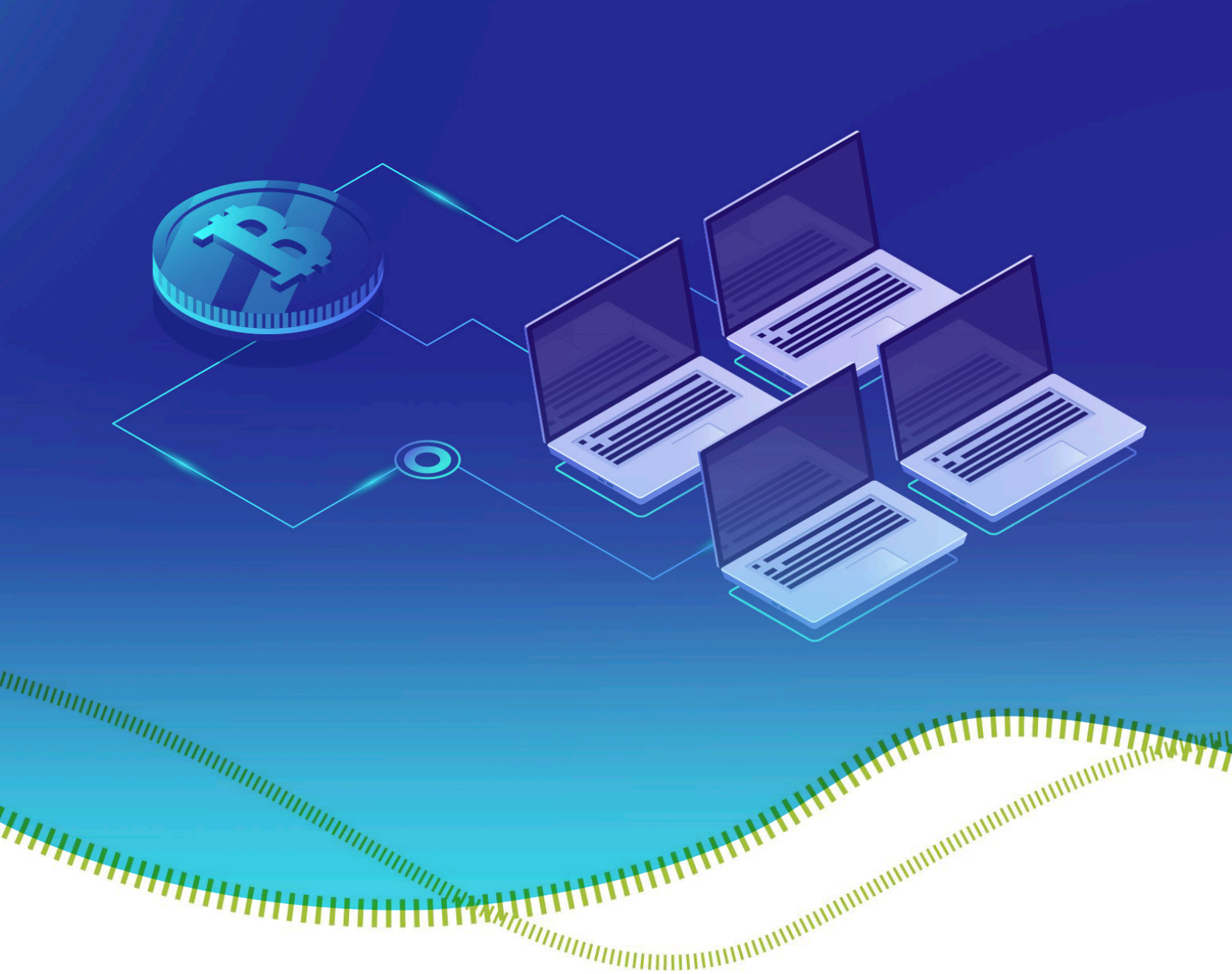


Cryptojacking

Wat is het en waarom is het belangrijk?

CERT.be
The Federal Cyber Emergency Team

The
Federal Cyber
Emergency Team

Inhoudsopgave

1 INLEIDING

Enige tijd geleden merkte CERT.be een nieuw fenomeen op: cryptojacking. CERT.be merkt 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 verwacht CERT.be dat *cryptojacking* een grotere bedreiging wordt dan *ransomware*.

In dit document bespreken we de fenomenen *in-browser mining* en *cryptojacking*.

1.1 Wat zijn cryptovaluta?

Cryptovaluta zijn virtuele munten die sterk afhankelijk zijn van cryptologie om te kunnen functioneren. De bekendste variant is de Bitcoin, die een gedecentraliseerd digitaal cashsysteem aanbood als alternatief voor klassieke betaalsystemen. Tegenwoordig bestaan er een paar honderd verschillende cryptovaluta, maar de Bitcoin wordt dit document als voorbeeld gebruikt.

Aangezien de prijs van sommige van deze cryptovaluta snel stijgt, wint *cryptomining* terrein.

1.2 Wat is mining?

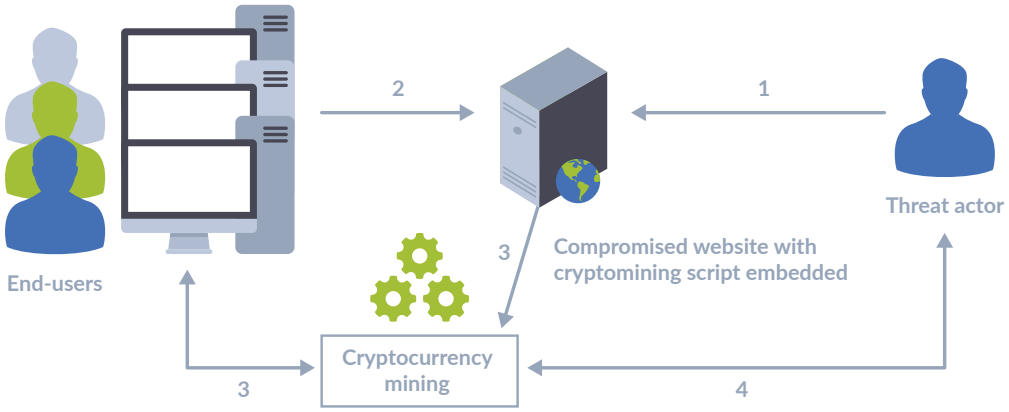
Om een Bitcoin te maken en dus geld te verdienen, moet een computer veel berekeningen uitvoeren die een grote hoeveelheid resources (CPU) vereisen. Voor deze berekeningen wordt de computer of smartphone beloond met Bitcoins. Dit proces wordt *mining* genoemd.

Aangezien het aantal berekeningen, nodig om geld te verdienen, zeer hoog is, zijn steeds meer toestellen nodig om deze berekeningen uit te voeren (een pool van apparaten).

Omdat een grotere *pool*, grotere voordelen met zich meebrengt, nemen sommige actoren op het internet miningprogramma's (scripts genaamd) op in hun websites. Dit betekent dat de bezoekers van deze websites cryptovaluta *minen* voor de eigenaar van de website. Dit gebeurt op de achtergrond, zonder dat de gebruiker zich er van bewust is.

Als de gebruiker van de website wel de toestemming geeft om te *minen* via zijn apparaat, kan je dit zien als een soort vergoeding voor het gebruik van de website en de diensten erachter. Het probleem is echter dat veel gebruikers zich er niet van bewust zijn dat hun browser gebruikt wordt om cryptovaluta te *minen*.

How cryptojacking works



Steps

1. The threat actor compromises a wesbite
2. Users connect to the compromised website ad the cryptomining script executes
3. Users start unknowinlgy mining cryptocurrency on behalf of the threat actor
4. Uppon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Source: Enisa

2 WAT IS CRYPTOJACKING?

2.1 Wat is het fenomeen cryptojacking?

Als de browser van de gebruiker wordt gebruikt om cryptovaluta te *minen* zonder de toestemming van de gebruiker, is de gebruiker het slachtoffer van *cryptojacking*.

Terwijl de *cryptominer* actief is, merkt de gebruiker 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.

2.2 Hoe kan je het opmerken?

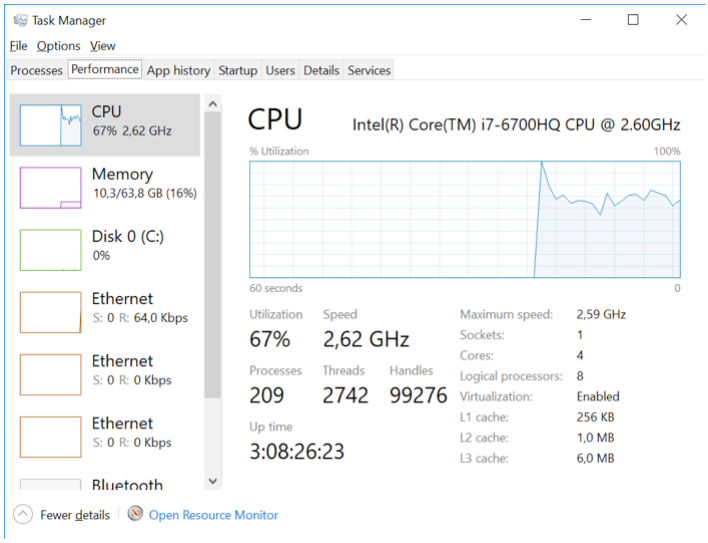
Om te zien of de browser cryptovaluta aan het *minen* is, kan je de task manager (Windows) of de activity monitor (Apple) gebruiken:

2.2.1 Windows task manager

1. Open de task manager door rechts te klikken op de taakbalk en “task manager” te selecteren.
2. Klik op “More details”.
3. Ga naar de tab “performance” om het CPU-gebruik te zien.

2.2.2 Macintosh activity monitor

1. Klik op Command+Spatiebalk om het “Spotlight search field” te activeren.
2. Typ “Activity Monitor”.
3. Druk op Return wanneer “Activity Monitor” in de resultaten verschijnt.
4. Je bevindt je nu in Activity Monitor, waar je taken kan beheren en wijzigen.



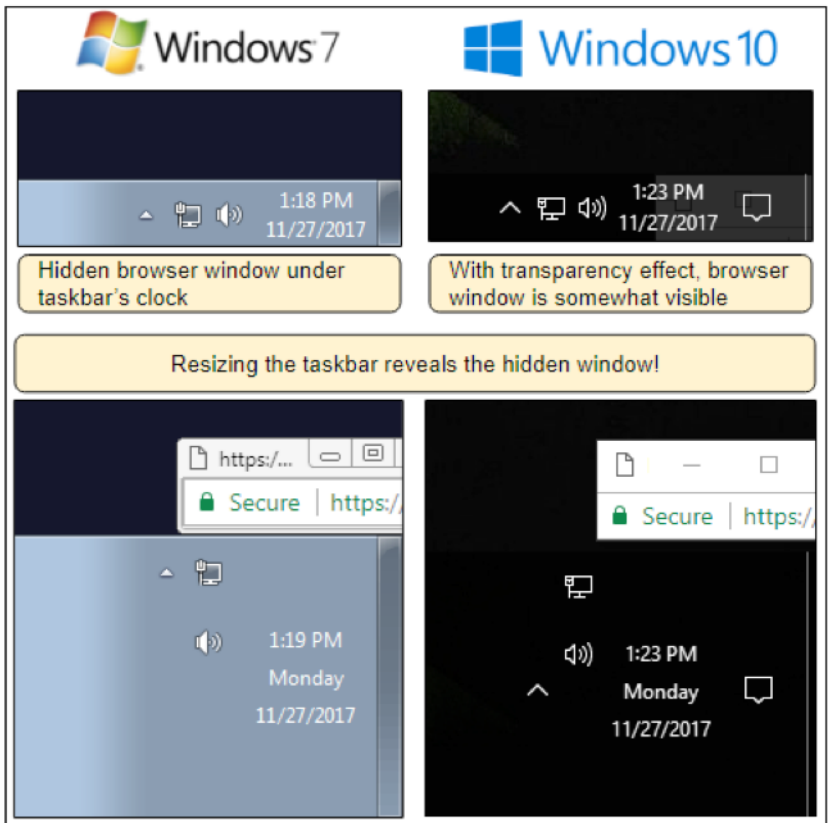
Task manager die een hoog CPU-gebruik aantoont

2.3 Hoe werkt cryptojacking?

Cryptojacking kan op verschillende manier gebeuren:

- Het script is rechtstreeks in de website opgenomen.
- Het script is opgenomen in een advertentie van een derde partij die op de website verschijnt.
- De gebruiker heeft een browser-plugin/-extensie geïnstalleerd die het script op de website uitvoert.
- Het apparaat van de gebruiker is geïnfecteerd met malware die *cryptomining* op de achtergrond uitvoert.

Onlangs is een nieuwe versie van de *cryptomining* ontdekt: een website opent een pop upvenster dat onder de taakbalk verborgen is (zie afbeelding). Dit betekent dat zelfs na het verlaten van de oorspronkelijke pagina, het mining-script de resources blijft gebruiken. Hierdoor blijft het script langer draaien, waardoor de winst voor de scriptprovider nog hoger is.



Verbogen Venster - Screenshot van blog.malwaresbytes.com

3 WAT KAN JE ERTEGEN DOEN?

Gelukkig is *cryptojacking* eenvoudig de kop in te drukken.

3.1 Internetgebruiker

- Overweeg het gebruik van een ad-blocker of een anti-virusprogramma aangezien deze voorkomen dat deze scripts draaien.
- Installeer alleen 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.
- Deactiveer onnodige browserextensies.
- Als de computer of smartphone langzamer werkt of warm wordt of als de webbrowser niet reageert, start de webbrowser opnieuw op.
- Geavanceerde gebruikers kunnen JavaScript standaard uitschakelen en alleen vertrouwde websites toestaan JavaScript te draaien.
- Controleer regelmatig of je browser nog steeds schoon is met tools zoals: https://cryptojackingtest.com.
- Informeer CERT.be door een e-mail te sturen naar cert@cert.be. Dit helpt ons bij het opvolgen van de cyberveiligheid in België.
- Aangezien je een slachtoffer bent, kan je een klacht indienen bij de lokale politie.

3.2 Eigenaar van een website

Als je klachten krijgt van gebruikers over *cryptomining* of over een langzamer werkend platform, zorg er dan voor dat je niet ongewild *mining*-scripts draait. Bovendien is dit illegaal in België zonder de toestemming van de gebruiker: er staat een gevangenisstraf op van maximaal 5 jaar (voor de eerste overtreding).

3.3 Systeembeheerder

- Blokkeer inkomend en uitgaand verkeer naar TCP- en UDP-poorten 3333, 5555, 7777, 8000 en 14444 op uw demarcatiepunt, als er geen bestaand businessdoel is.
- Deactiveer of verwijder software, poorten, protocollen en diensten die niet in gebruik zijn.
- Een zwarte lijst van domeinnamen is gepubliceerd op: http://iplists.firehol.org/

4 LEGAAL EN ILLEGAAL GEBRUIK VAN CRYPTOMINING

Het is belangrijk om een onderscheid te maken tussen het legale en het illegale gebruik van *cryptomining*, nl. *cryptojacken*. Het verschil is het akkoord en de transparantie van het *miningproces* naar de gebruiker die de cryptovaluta *minet*.

Cryptomining is een legitieme nieuwe activiteit waar bedrijven en individuen een aanzienlijke hoeveelheid CPU-energie besteden aan cryptomining, een intensief proces van computergebruik en het oplossen van gecompliceerde wiskundige problemen om een Proof of Work te verdienen, dat de volgende schakel in de keten verifieert.

Cryptojacking is een illegale vorm van cyberaanval waarbij een hacker het processorvermogen van een doelwit kaapt om cryptovaluta te *minen*. De gebruiker is zich er niet van bewust en heeft geen toestemming gegeven aan de aanvaller.

De straf wordt bepaald op basis van deze inbreuken die in het Belgische Strafwetboek zijn gedefinieerd onder:

- **Artikel 504quater Strafwetboek – Informaticabedrog**

  §1. Hij die, met bedrieglijk opzet, beoogt een onrechtmatig economisch voordeel voor zichzelf of voor een ander te verwerven, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de gegevens in een informaticasysteem te veranderen.

- **Artikel 550ter Strafwetboek - Hacking**

  §1. Hij die, terwijl hij weet dat hij/zij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert.

  §3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig BEF tot honderdduizend BEF of met een van die straffen alleen.

https://www.symantec.com/about/newsroom/press-releases/2018/symantec_0321_01
https://bittrex.com/home/markets
https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/
https://bitcoin.org/bitcoin.pdf

5 CONTACT

The Federal Cyber Emergency Team
Wetstraat 16
1000 Brussel
info@cert.be

Centre for Cyber Security Belgium
Wetstraat 18
1000 Brussel
info@cert.be

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 voor cyberveiligheid. Door het optimaliseren van de informatie-uitwisseling kunnen de bevolking, de bedrijven, de overheid en de vitale sectoren zich gepast beschermen.
www.ccb.belgium.be

Verantwoordelijke uitgever

Centrum voor Cybersecurity België, Miguel De Bruycker, Wetstraat 18, 1000 Brussel