CTB locker Virus, een serieuze bedreiging voor uw bestanden

Malware passeert bij ons dagelijks de ‘revue’, maar sinds kort komt er af en toe een virus voorbij, waarvan de werking dermate destructief is, dat we u daar **expliciet** voor willen waarschuwen.

De naam hiervan is **CTB locker** (verschijnt ook onder andere namen) en kan worden gekwalificeerd als zgn. Ransom Ware.

Wat is Ransomware?!

De toegang tot uw bestanden/computer wordt door derden (criminelen) geblokkeerd, waarbij u tegen betaling van ‘losgeld’ deze toegang weer terugkrijgt.

Waarom deze expliciete waarschuwing?!

In het verleden kwam dit fenomeen ook in vlagen voorbij (denk aan het ***politie virus***), maar in dat geval was de complete ‘schade’ te herstellen door een computerreparateur. Zowel het virus kon worden verwijderd, als toegang tot de bestanden kon worden hersteld.

Bij **CTB Locker** is verwijdering van het virus ook nog mogelijk (zelfs relatief eenvoudig), maar de gebruikersbestanden zijn na verwijdering nog steeds **versleuteld**.

Deze versleuteling is dynamisch (elke infectie creëert een unieke sleutel). Deze sleutel wordt opgeslagen op een door de criminelen beheerde server en u bent dus voor ontsleuteling volledig van deze lieden afhankelijk.

Afbeelding van CTB Locker-infectie

Daarnaast heeft het virus de neiging om ook toegankelijke externe schijven, netwerkshares, alsmede **Dropbox** en **Onedrive** bestanden te versleutelen. Dit maakt het nog erger, aangezien deze methoden veel worden gebruikt voor backups.

Voorkomen van besmetting

Besmetting vindt veelal plaats via het openen van besmette links, welke gekoppeld zijn aan e-mailberichten.

Hierbij kunt u bijvoorbeeld denken aan:

- Berichten waarin wordt aangegeven dat er een pakje voor u onderweg is.
- Een (nep)bericht van een incassobureau, waar een besmette bijlage is toegevoegd.

Wees dus zeer alert bij het openen van bijlagen. Ook besmetting via het bezoeken van geïnfecteerde sites is mogelijk!

Uiteraard is van belang dat de beveiliging van de computer up-to-date is (Windows updates en updates van de beveiligingssoftware), maar hierbij dient te worden opgemerkt dat dit geen garantie vormt voor het voorkomen van besmetting.

Vervolg: voorkoming van besmetting

Het bedrijf **FoolishIT LCC** heeft een kleine tool uitgebracht waarmee voorkomen kan worden dat het virus actief wordt (CryptoPrevent). Hierbij dient wel te worden opgemerkt dat een virus in de loop der tijd door de makers kan worden aangepast, waardoor een dergelijk programmaatje alsnog niet afdoende kan blijken te zijn.

Online Backup

Een interessante mogelijkheid om in ieder geval de gevolgen van een besmetting te verkleinen is het instellen van een Online Backup, waarbij de Backupdata niet via een stationsletter beschikbaar is.

Hierbij moet gedacht worden aan een backup die plaats vindt m.b.v. een programmaatje van de aanbieder van de Backupdienst. Het virus heeft niet zomaar toegang tot deze bestanden en kan dus ook niet zomaar de boel versleutelen.

Een bijkomend voordeel van een dergelijke backup is dat deze niet veel discipline van de gebruiker vereist, aangezien deze zelfstandig draait wanneer een internetverbinding voor handen is. Uiteraard geldt hier ook: Controleer periodiek of e.e.a. functioneert.

Bekende aanbieders van een dergelijke online backup zijn:

- KPN (Backup Online)
- Strato (Hidrive)

Na besmetting/versleuteling… wat zijn de mogelijkheden!?

Zoals eerder al opgemerkt is het verwijderen van het virus niet het grootste probleem.

Wanneer bestanden zijn versleuteld kan het zijn dat er toch nog mogelijkheden zijn om (een deel van uw gegevens) te redden:

Betaling losgeld

Bij besmetting wordt een ultimatum gesteld, waarbij u gesommeerd wordt om een bedrag naar de criminelen over te maken.

Hierna zou u een sleutel ontvangen, waarmee de bestanden weer te ontsleutelen zijn. Allereerst is het maar zeer de vraag of dit ook daadwerkelijk gebeurt.

Daarnaast zou een betaling een aanmoediging kunnen zijn om door te gaan met deze praktijken.

In de diverse bronnen die we hebben geraadpleegd heb over dit onderwerp wordt in ieder geval altijd aangeraden aangifte te doen bij de politie.

Recovery bestanden

De versleuteling vindt als volgt plaats: Het bestand wordt gekopieerd naar een versleutelde versie, waarna het origineel wordt verwijderd. Net als bij ‘normaal’ dataverlies is het mogelijk om een poging te doen deze verwijderde bestanden te recoveren. Een dergelijke recovery geeft in de praktijk wisselend succes en tevens is in de meeste gevallen de structuur van mappen verdwenen en ook vaak zijn de originele bestandsnamen kwijt.

Terughalen van vorige bestandsversies en zgn. shadowcopies

Naast een normale datarecovery kunnen er mogelijkheden zijn om oudere versies (lees: versies van voor de versleuteling) terug te halen. Dit is echter niet bij elke installatie van Windows het geval.

Een dergelijke functie kan ook beschikbaar zijn bij **Dropbox** en **Onedrive.**

Hierbij dient tevens te worden opgemerkt dat het terughalen van oude bestanden (zeker voor de normale gebruiker) een zeer tijdrovende zaak is, aangezien dit vaak 'per bestand' dient te gebeuren.

Conclusie…

Het besef dat Malware niet meer in de kinderschoenen staat is bij de meeste computergebruikers al wel aanwezig, maar de gevolgen van een **CTB Locker** infectie kunnen dermate verstrekkende gevolgen hebben dat we het erg belangrijk vinden om hier expliciet op de gevolgen te wijzen en het belang van een goede bescherming te benadrukken.

Daarnaast is het van groot belang te beseffen dat de computergebruiker zelf verantwoordelijk is voor zijn/haar data en dus ook het eventuele backuppen daarvan. Uiteraard staan we u graag met raad en daad terzijde om problemen te voorkomen en bij besmetting de gevolgen zo klein mogelijk te laten zijn. Wij kunnen echter geen enkele aansprakelijkheid erkennen bij eventueel dataverlies.