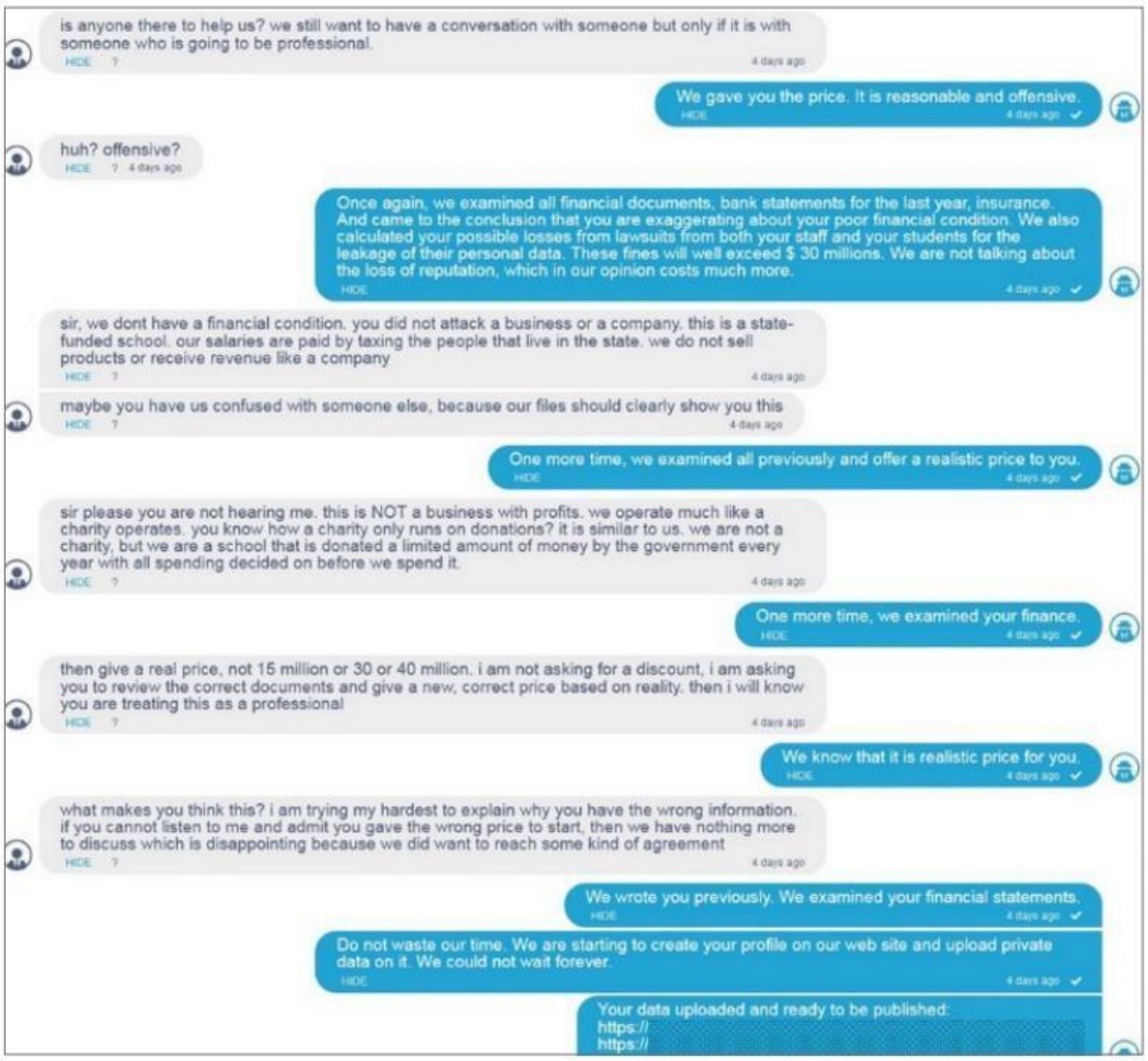
socured
TAKING CARE

Ransomware: een veranderend bedrijfsmodel

Ransomware: een veranderend bedrijfsmodel

Het bedrijfsmodel voor ransomware is in feite uitgegroeid tot een inlichtingenoperatie: criminelen doen onderzoek naar het beoogde slachtoffer om een optimale hoeveelheid losgeld te eisen. Zodra een crimineel een netwerk infiltreert, kan hij data stelen en financiële documenten en verzekeringspolissen bestuderen. De criminelen vragen niet alleen losgeld voor het ontgrendelen van de systemen van het slachtoffer, maar ook voor het niet openbaar maken van de gestolen data van het slachtoffer. Zodra ze deze informatie hebben verzameld en geanalyseerd, bepalen ze een 'passend' losgeldbedrag. De onderhandelings-chat hieronder met een openbare school om in ruil voor geld een sleutel voor het ontsleutelen van Conti-ransomware op het netwerk van de school te geven, laat zien wat voor onderzoek de crimineel voorafgaand aan de onderhandeling heeft uitgevoerd.

Chat van een ransomwareonderhandeling



Hier legt de crimineel uit dat “we alle financiële documenten, bankafschriften van het afgelopen jaar en verzekeringen hebben bekeken. En we zijn tot de conclusie gekomen dat u de slechte financiële situatie overdrijft. We hebben ook uw mogelijke verliezen door rechtszaken van zowel uw personeel als scholieren voor het lekken van hun persoonsgegevens berekend. Deze boetes zullen meer dan $ 30 miljoen bedragen. En dan hebben we het nog niet eens over reputatieverlies gehad, wat naar onze mening meer kost.”

De lat om aan deze criminele bedrijfstak deel te nemen, ligt laag. Om van deze misdaden te profiteren, heeft een crimineel geen specifieke programmeervaardigheden nodig. De ransomwaresector heeft zich ontwikkeld tot een industrie waarin ransomware als dienst wordt aangeboden en op basis van informatie over en onderzoek naar mensen wordt ingezet. Het is niet meer alleen het domein van malwaredevelopers; de bedrijfsstructuur is eerder modulair. Malwaredevelopers rekruteren hackers met toegang tot netwerken en beloven in ruil daarvoor een deel van de winst. Criminelen kunnen malware kopen, toegang krijgen tot specifieke netwerken en zich richten op specifieke sectoren. Dit is in feite een criminele organisatie waarin elk lid voor bepaalde expertise wordt betaald. In het voorbeeld hieronder, waarin de stromen cryptovaluta worden gevolgd, zien we hoe een criminele onderneming haar ‘winst’ heeft opgesplitst, waarbij ongeveer 15% naar de developer/manager gaat en 75% naar de aanvaller. Waar de ransomware ook wordt ingezet, de aanvallers eisen meestal een betaling met een cryptovaluta via cryptoportemonnees.

“Malwaredevelopers rekruteren hackers met toegang tot netwerken en beloven in ruil daarvoor een deel van de winst.”

Hoewel de onderliggende blockchain-technologie de stromen cryptovaluta transparant maakt, blijven de eigenaren van de portemonnees pseudoniem. Toch hebben ze nog altijd in- en uitgangen voor het crypto-ecosysteem nodig. Uiteindelijk moet de crimineel aan het einde van de blockchain een transactie toevoegen om de winst te verzilveren. Binnen het crypto-ecosysteem zijn meerdere partijen actief om aan losgeld gerelateerde transacties en betalingen mogelijk te maken.

Deze tussenpersonen bestaan vaak in rechtsgebieden met overheden die in het verleden niet bereid waren om met de Verenigde Staten en andere landen samen te werken. Het zijn deze tussenpersonen die de stroom illegaal verkregen inkomsten uit ransomware faciliteren. De particuliere sector (via civiele rechtszaken) en de overheid (via vervolging, wetshandhaving en internationale samenwerking), kunnen gecoördineerd optreden tegen deze tussenpersonen om het betaalproces te verstoren.

WEL OF NIET BETALEN?

Na een ransomwareaanval liggen bedrijven vaak volledig plat: met hun beveiligingssystemen is geknoeid, hun back-ups zijn verwijderd, hun data zijn versleuteld en hun gebruikers kunnen niet inloggen. Terwijl de activiteiten stilliggen en de verliezen oplopen, is het belangrijk om niet te vergeten dat het betalen van losgeld niet garandeert dat de activiteiten worden hersteld, en ook toekomstige aanvallen niet voorkomt. Bovendien hebben we te maken met een klassieke 'tragedie van de meent'. Hoewel het voor afzonderlijke slachtoffers misschien logisch is om voor hun eigen voordeel (het herstel van essentiële bedrijfsactiviteiten) te betalen, zorgt de betaling er ook voor dat dit schadelijke bedrijfsmodel groeit.

Losgeldbetalingen kunnen deze vicieuze cirkel in gang houden:

- Het bedrijfsmodel van de afpersers wordt versterkt, wat ook weer meer criminelen aantrekt. De criminelen verdienen veel geld, en een deel daarvan gebruiken ze voor onderzoek en ontwikkeling (O&O) om hun tools te verbeteren en toegang tot mogelijke slachtoffers te kopen. Sommige ransomwareteams hebben aanzienlijke budgetten voor O&O en het kopen van zerodays. Sommige teams hebben bijvoorbeeld genoeg budget om $ 1 miljoen of zelfs meer per zeroday uit te geven. Terwijl sommige geavanceerde ransomwareteams zerodays kopen, richten andere zich op traditionele manieren om toegang tot netwerken van slachtoffers te krijgen.
- De ransomwaretools worden geautomatiseerder en effectiever, zodat de criminelen hun aanvallen kunnen opschalen, versnellen en verfijnen, terwijl de aanvallen minder inspanningen kosten.

Hou rekening met het volgende:

- Gemiddeld krijgen organisaties die losgeld hebben betaald maar 65% van hun data terug, waarbij 29% niet meer dan de helft terugkrijgt.
- De ontsleutelingssoftware bevat fouten en kan de grootste, meest essentiële bestanden (groter dan 4 GB) vaak niet ontsleutelen.
- Bestanden ontsleutelen gaat langzaam en is arbeidsintensief: de meeste klanten ontsleutelen alleen de meest essentiële bestanden en herstellen de rest van een back-ups.
- Het herstellen van data maakt sabotage door de aanvallers niet ongedaan.
- Het herstellen van data beschermt systemen niet tegen toekomstige aanvallen.
- Organisaties moeten nagaan of losgeldbetalingen in hun land legaal zijn.

Wereldwijd stellen overheden rapportage-vereisten voor ransomwarebetalingen op, sommige leggen boetes op als aan bepaalde partijen betalingen worden gedaan en sommige overwegen op ransomwarebetalingen illegaal te maken

VOORBEELD: CONTI-RANSOMWARE

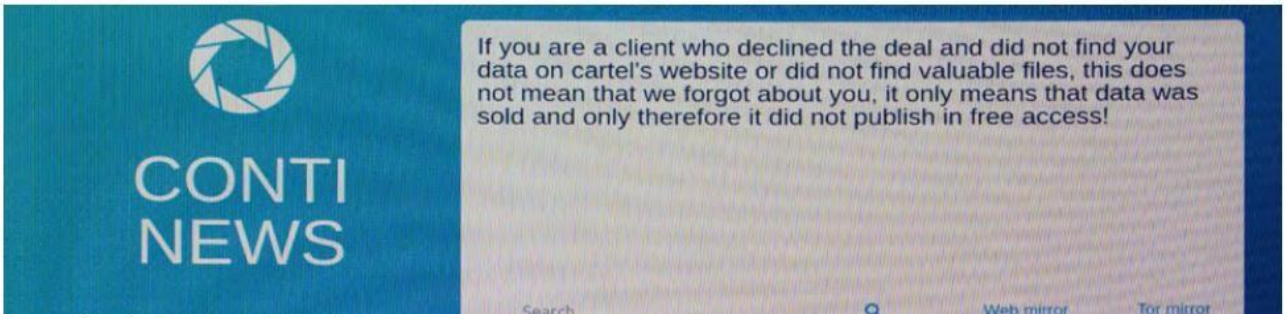
De Conti-ransomware werd rond juli 2020 voor het eerst waargenomen. Bij Conti werd gebruikgemaakt van dubbele afpersing, waarbij het slachtoffer zowel voor de gijzeling als voor het publiceren van gestolen data wordt afgeperst. Conti is ook een ransomware-als-service (RaaS), een abonnementsdienst waarmee gebruikers makkelijk toegang hebben tot tools voor het maken van ransomware en ransomware zelf. Abonnees betalen een percentage van het losgeld aan de developer van de ransomware en de crimineel die de aanval heeft uitgevoerd. Conti krijgt meestal via andere bedreigingen zoals Trickbot, IcedID of Zloader toegang tot het netwerk van het slachtoffer. Eenmaal in het netwerk gebruikt Conti een configureerbare verkenningsmodule waarmee het interne netwerken kan scannen op netwerkshares en andere waardevolle doelen. Zodra Conti wordt ingeschakeld, worden door gebruikers aanpasbare data en databases op basis van lijsten met bestandsextensies versleuteld. Zodra de versleuteling is voltooid, wordt in elke bestandsmap een losgeldbrief met instructies voor de gebruiker over contact met de aanvallers achtergelaten:

Losgeldbrief

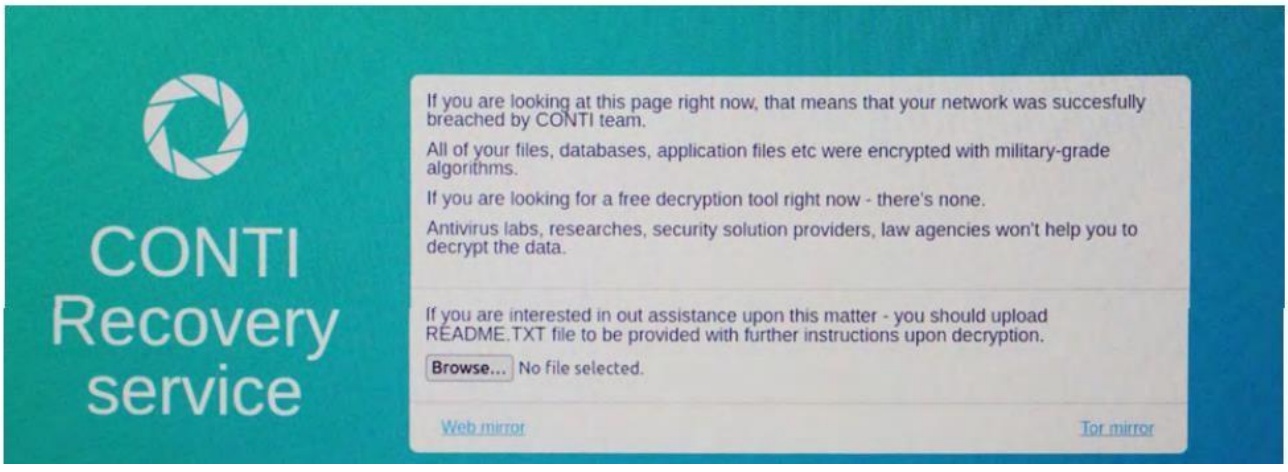
```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be
recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try
it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of
charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti                                                                    .onion/

HTTPS VERSION :
https://contirecovery.top/

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on
out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
---END ID---
```

Nu moet de gebruiker het tekstbestand met de losgeldbrief uploaden naar de herstelwebsite die in de brief wordt vermeld. De brief bewijst de versleuteling en maakt het slachtoffer identificeerbaar voor de aanvallers.

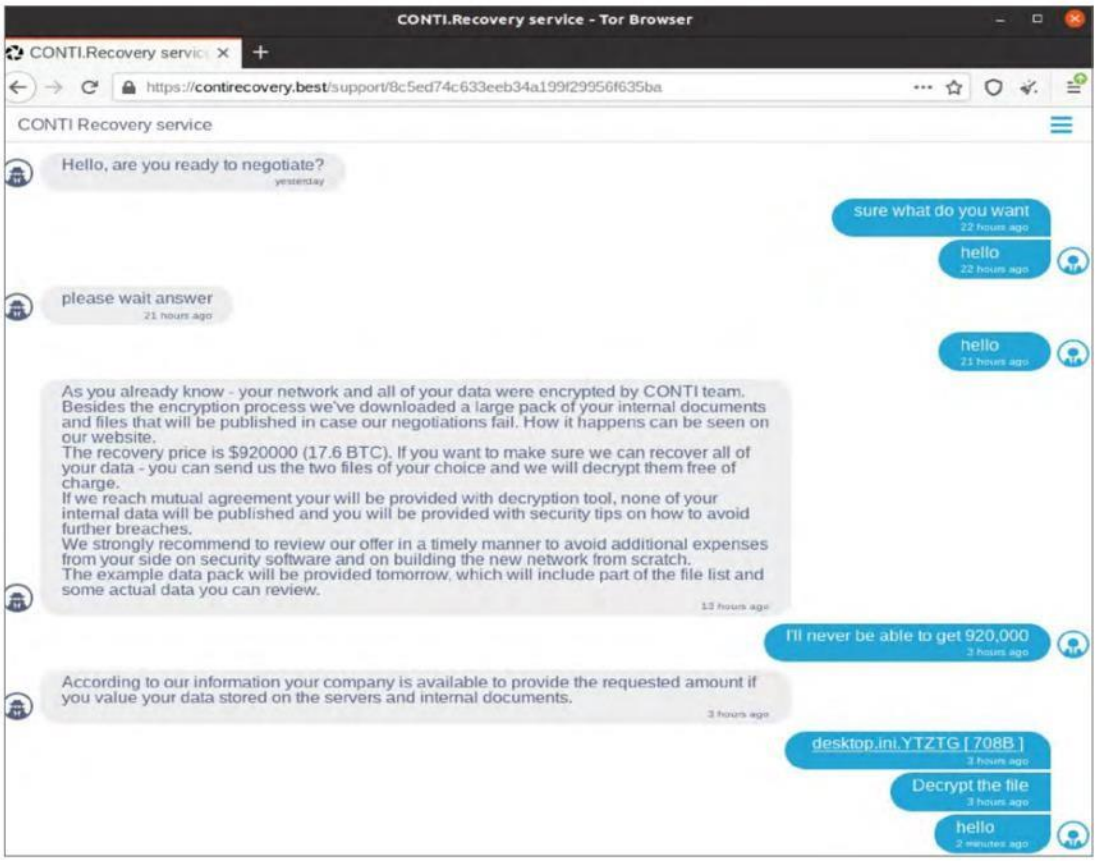
Conti News-website



Herstelwebsite voor losgeld



Chat na het uploaden van de losgeldbrief



De onderhandelingsfase wordt gestart door de aanvaller, die kan bewijzen dat hij elk bestand dat het slachtoffer aanlevert kan ontsleutelen. Nadat een definitief losgeld is overeengekomen, noemt de aanvaller een Bitcoinportemonneeadres waarnaar het slachtoffer de betaling moet sturen. Op de website Conti News staan nu honderden slachtoffers met verschillende voorbeelden van hun privégegevens.

DE SITUATIE IS VERANDERD

Ransomware en afpersing groeien enorm. Om je organisatie tegen ransomware te beschermen, raden we het volgende aan:

Stel een herstelplan op:

Door het moeilijker te maken om systemen te benaderen en verstoren, zijn er voor aanvallers minder financiële prikkels. Bovendien kan je organisatie hiermee makkelijker zonder losgeldbetaling van een aanval herstellen.

Beperk de reikwijdte van de schade:

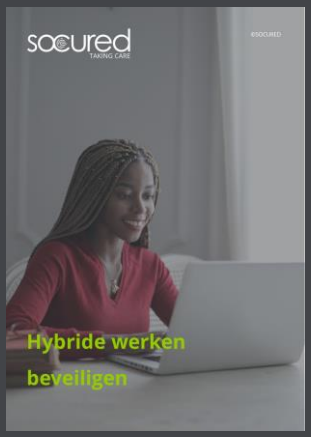
Zorg dat het aanvallers meer moeite kost om toegang tot meerdere bedrijf kritische systemen te krijgen. Dit maakt het voor een aanvaller die het netwerk binnendringt moeilijker om zich binnen het netwerk te bewegen en waardevolle data te vinden om te versleutelen.

Versleutel ook inactieve data en zorg dat back-up en herstel nauwgezet worden uitgevoerd.Zo zijn data, zelfs als ze worden gestolen, versleuteld en voor de aanvallers niet echt nuttig. Zelfs als de aanvaller je data onverhoopt versleutelt, heb je een goede back-up om te herstellen, zodat je bedrijfscontinuïteit wordt gehandhaafd.

Maak binnendringen moeilijker:

Met standaardmaatregelen voor cyberbeveiliging wordt het voor aanvallers moeilijker om het netwerk binnen te dringen. De belangrijkste van deze maatregelen is het gebruik van meervoudige verificatie (MFA). Dit is belangrijk om toegang moeilijker te maken, maar de implementatie duurt wel langer en maakt deel uit van een breder beveiligingstraject. Andere maatregelen, zoals patches snel toepassen en een juiste configuratie, kunnen worden genomen om kwetsbare toegangspunten te vinden en af te sluiten.

MEER LEZEN?



Hybride werken beveiligen

Download

Phishing en andere kwaadaardige e-mails

Download

BEDANKT VOOR HET LEZEN VAN DEZE WHITEPAPER. HEEFT U NOG VRAGEN OVER HET ONDERWERP?

Neem dan gerust contact met ons op via info@socured.nl of 020 708 55 65.

Socured
Klokkenbergweg 50A
1101 AP AMSTERDAM-ZO
Tel.: 020 708 55 65
info@socured.nl
www.socured.nl

Onderdeel van Socia

Over Socured

Socured is gevestigd in Amsterdam en is onderdeel van Socia. Socia helpt al meer dan 15 jaar haar klanten op het gebied van IT en heeft inmiddels een mooie voetafdruk achtergelaten bij veel bedrijven in Nederland als het gaat om IT-diensten.