socured
TAKING CARE

De groeiende dreiging van cybercriminaliteit

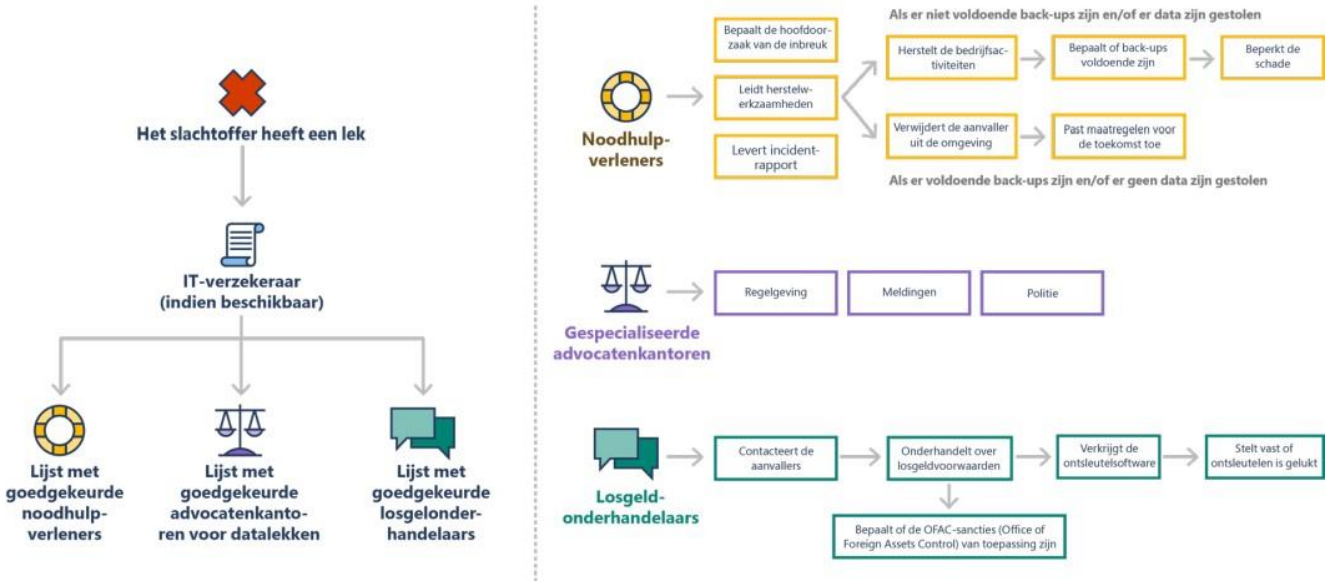
De groeiende dreiging van cybercriminaliteit

Cybercriminaliteit, ongeacht of zij door staten wordt gesteund of toegestaan, vormt een bedreiging voor de nationale veiligheid. Cybercriminelen richten zich op alle sectoren met kritieke infrastructuur, waaronder de zorg-, IT-, financiële en energiesectoren. Aanvallen met ransomware hebben steeds meer succes, verlammen overheden en bedrijven en zijn voor criminelen steeds winstgevender. De leveringsketens van cybercriminaliteit, die vaak door criminele organisaties worden opgezet, worden steeds volwassener. Zo kan iedereen de benodigde diensten kopen om met criminele activiteiten financieel gewin te behalen of een ander misdadig doel te bereiken. Geavanceerde cybercriminelen werken ook nog steeds voor overheden om te spioneren en te trainen voor het nieuwe slagveld.

De situatie is echter niet hopeloos

En we hebben de laatste tijd twee positieve trends waargenomen. Ten eerste komen meer overheden en bedrijven ervoor uit dat ze slachtoffer zijn geworden. Deze transparantie helpt op verschillende manieren. Overheden over de hele wereld begrijpen nu dat cybercriminaliteit een bedreiging voor de veiligheid vormt. De verhalen van slachtoffers plaatsen deze aanvallen in de menselijke context en maken de gevolgen duidelijk. Ze vestigen de aandacht op het probleem en maken meer betrokkenheid van incidenthulpverleners en wetshandhaving mogelijk. Omdat overheden over de hele wereld nu erkennen dat cybercriminaliteit een bedreiging voor de nationale veiligheid is, hebben ze de bestrijding ervan prioriteit gegeven. Over de hele wereld introduceren overheden nieuwe wetten voor het melden van incidenten, stellen ze interbestuurlijke werkgroepen in, wijzen ze middelen toe en zoeken ze hulp bij de particuliere sector.

“Aanvallen met ransomware hebben steeds meer succes, verlammen overheden en bedrijven en zijn voor criminelen steeds winstgevender.”



DE CYBERCRIMINALITEITS-ECONOMIE EN –DIENSTEN

Door onze onderzoeken naar online netwerken van de georganiseerde misdaad, onderzoek naar aanvallen op onze klanten, onderzoek naar beveiliging en aanvallen, het volgen van bedreigingen van staten en de ontwikkeling van beveiligingstools, zien we dat de leveringsketen van de cybercriminaliteit wordt geconsolideerd en volwassen wordt. Vroeger moesten cybercriminelen alle technologie voor hun aanvallen zelf ontwikkelen. Tegenwoordig kunnen ze rekenen op een volwassen leveringsketen, waarin specialisten software en diensten maken die anderen kopen om in hun campagnes te gebruiken.

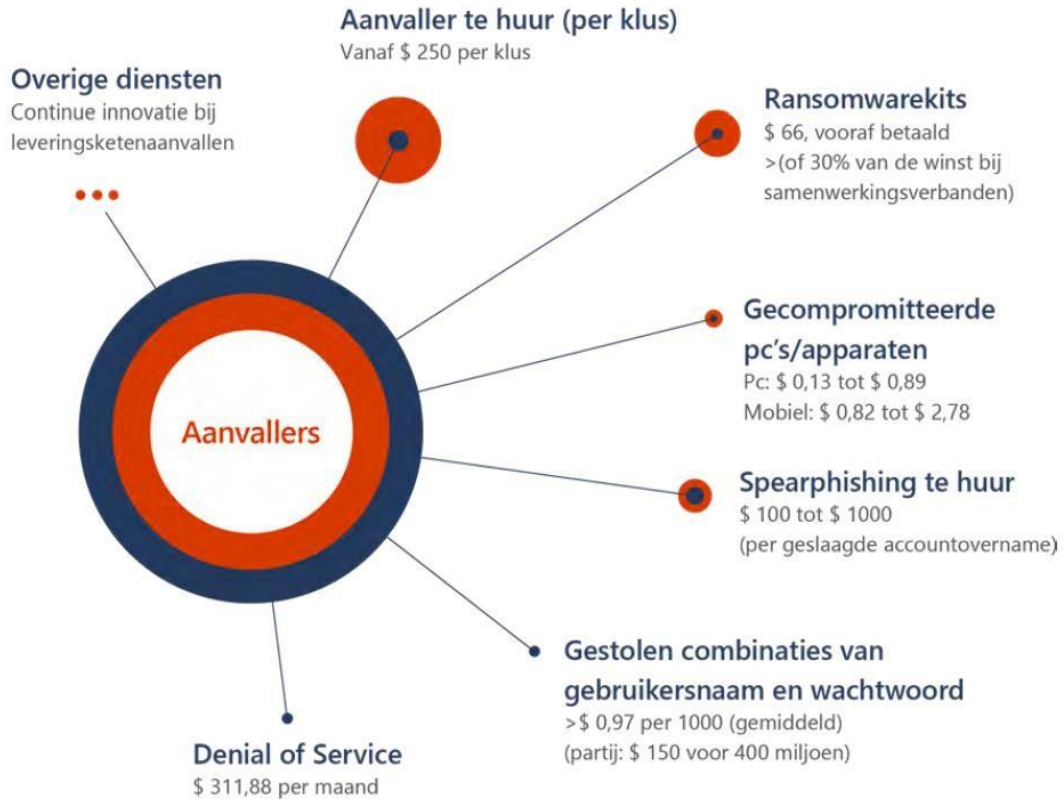
Door de toegenomen vraag naar deze diensten is er een gespecialiseerde diensteneconomie ontstaan, en kwaadwillenden gebruiken steeds meer automatisering om kosten te drukken en de schaal te vergroten. We zien bijvoorbeeld een steeds groter aanbod aan backconnectproxy's (proxy's die schakelen tussen mobiele, particuliere en datacentersystemen), naast diensten voor Remote Desktop Protocol (RDP), Secure Shell (SSH), virtuele privénetwerken (VPN's), virtuele privéservers (VPS), webshells, cPanels (een beheerdashboard voor webhosting) en andere anonimiserings-systemen. Andere voorbeelden zijn het verkopen van gestolen inloggegevens, mogelijk verkregen via phishing, het afschrapen van botnetlogboeken of andere technieken voor het verzamelen van gegevens, valse domeinnamen, phishing-als-service,

het op basis van criteria verzamelen van mogelijke doelwitten (bijvoorbeeld per land, sector of functie), loads (schadelijke software die wordt gebruikt om malware op een geïnfecteerde computer bij te werken), Denial of Service (DoS) en meer.

TER ILLUSTRATIE:

Op sommige markten worden door verschillende verkopers gestolen inloggegevens aangeboden voor prijzen van $ 1,00 tot $ 50,00, afhankelijk van variabelen zoals de geschatte waarde van het bedrijfsdoelwit. Het aantal websites dat deze diensten aanbiedt, het volume aangeboden inloggegevens en de verscheidenheid aan phishingkits zijn de afgelopen twaalf maanden flink toegenomen. Zelfs voor amateuristische kwaadwillenden zijn onder andere derdenrekeningen voor cryptovaluta beschikbaar (om te garanderen dat de aangeboden diensten worden geleverd). We zien dit vaak bij ransomwarecampagnes, waarbij samenwerkingsverbanden gemeengoed zijn geworden. Niet-technische cybercriminelen melden zich aan bij een ransomwaresamenwerking, waarbij de 3 samenwerkingspartners in ruil voor 30% van de omzet zorgen voor de ransomware en herstel en betaaldiensten. Vervolgens koopt de aanvaller 'loads' op een markt en gebruikt hij die om de ransomware naar de gekochte loads te sturen. Daarna kan hij rustig zijn geld binnenhalen.

Organisaties worden tegenwoordig geconfronteerd met een geïndustrialiseerde aanvalseconomie met specialisten en handel in illegale middelen. Zoals in deze momentopname van gemiddelde prijzen is te zien, zijn veel op duistere markten verkrijgbare middelen erg goedkoop, waardoor aanvallen goedkoop en eenvoudig zijn



uit te voeren (en waardoor de hoeveelheid aanvallen ook weer toeneemt).

Soms worden bepaalde diensten door groepen uit een bepaalde regio aangeboden, maar de meeste van deze cybercriminaliteitsmarkten zijn wereldwijd. Een koper in Brazilië kan phishingkits van een verkoper in Pakistan, domeinen uit de Verenigde Staten, mogelijke doelwitten uit Nigeria en proxy's uit Roemenië kopen. De prijzen voor deze diensten zijn de afgelopen paar jaar redelijk stabiel gebleken, maar net als in elke andere markt zijn ze afhankelijk van het aanbod, de vraag en externe factoren zoals de politiek.

"Niet alle aanvallen zijn succesvol. Het is essentieel dat we onze verdedigingsmechanismen blijven verbeteren, zodat er meer aanvallen mislukken en de bijbehorende kosten voor aanvallers stijgen."

BELANGRIJKSTE INZICHTEN:

- Phishingaanvallen waarbij identiteiten en wachtwoorden worden gestolen zijn goedkoop en in opkomst. Waarom zou een aanvaller inbreken als hij ook kan inloggen?
- DDoS-aanvallen (Distributed Denial of Service) voor onbeschermde websites zijn goedkoop: ongeveer $ 300 per maand.
- Ransomwarekits zijn een van de vele soorten aanvalskits die zijn gemaakt om niet technische aanvallers in staat te stellen geavanceerdere aanvallen uit te voeren.

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.

MEER LEZEN?

Ransomware: een veranderend bedrijfsmodel

Download

Phishing en andere kwaadaardige e-mails

Download

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.