Hackersbende licht Amerikaanse bedrijven op met vervalste buitenlandse papieren

Internetfraude met Belgisch paspoort

BRUSSEL ● Een bende Oost-Europese hackers heeft Amerikaanse bedrijven miljoenen dollars afhandig gemaakt via een hacking-aanval. Een van de tussenpersonen die vervolgens zorgde dat de fondsen bij het hoofd van de bende terechtkwamen, opereerde onder een vals Belgisch paspoort.

DOOR RONALD MEEUS

De Amerikaanse overheid arresteerde eergisteren 37 personen van Oost-Europese origine die bankrekeningen van Amerikaanse bedrijven en organisaties plunderden, en de fondsen uit die hackings vervolgens doorstuurden naar het brein achter de bende. Eerder deze week werden in Groot-Brittannië elf criminelen opgepakt die er een soortgelijke operatie hadden opgezet.

De cybercriminelen waren al sinds 2008 actief in de Verenigde Staten, en hielden al die tijd een ingenieuze 'muilezeloperatie' draaiende. Ze kwamen het land binnen met een speciaal visum dat de Amerikaanse overheid uitreikt aan buitenlanders die in de VS willen studeren of er een bedrijfsopleiding willen volgen. Het visum geeft hen het recht om meerdere maanden in het land te blijven. Vervolgens gebruikten ze valse paspoorten om rekeningen te openen bij banken daar. Daarna speelden ze voor 'money mule' voor de echte hackers, die vanuit Oost-Europa inbraken op de computers van hun slachtoffers via de hackingsoftware Zeus.

Via de inbraak werden bankgegevens losgeweekt. Daarmee werd vervolgens ingelogd op het internetbankieraccount van de slachtoffers. Er werden bedragen van de rekeningen gehaald die net onder de 10.000 dollar lagen, om de transactie minder te laten opvallen. Het geld werd overgemaakt naar de rekeningen die de muilezels onder een valse identiteit hadden opgezet. Bijna onmiddellijk na de inbraak haalden de tussenpersonen in de Verenigde Staten vervolgens het geld in cash van de rekening, via een geldautomaat of een loketbezoek.

De daders maakten gebruik van meerdere vervalste paspoorten, waarmee ook verschillende bankrekeningen werden geopend. Een van hen gebruikte bijvoorbeeld een clandestien Grieks en Belgisch paspoort (dat laatste onder de valse naam 'Françoise Lewenstadd') om meerdere rekeningen te openen bij Amerikaanse retailbanken als Bank of America en JP Morgan Chase. De buitenlandse paspoorten waren een extra manier om minder op te vallen. "De beslissing om Belgische en Griekse paspoorten te nemen is wellicht een erg specifieke keuze geweest", zegt Eddy Willems, een expert in computerbeveiliging bij beveiligingsbedrijf G Data. "Een nagemaakt Amerikaans paspoort is riskant, omdat het risico groter is dat een bankbediende de onvolmaaktheden erin zal ontdekken. En een Oost-Europees paspoort doet dan weer te snel vragen rijzen. Dus ligt de keuze voor minder 'verdachte' landen, zoals België, voor de hand."

Eddy Willems (expert computerbeveiliging): 'Een nagemaakt Amerikaans paspoort is riskant, één uit een land als België is minder verdacht'

Hoe het geld vervolgens bij de hoofden van de bendes terechtkwam stond niet in de arrestatieverslagen die bij de Amerikaanse media terechtkwamen, maar de normale modus operandi bij dit soort fraudes is dat het geld wordt doorgestuurd via geldtransfersystemen als Western Union, die gewoon bereikbaar zijn door een geldbedrag in cash af te leveren op het postkantoor. De muilezels nemen ook eerst een paar procenten af voordat ze de grotere som doorsturen.

Het gebruik van fysieke stromannen is een typische strategie in dit soort fraudes, en dient vooral om de kopstukken en de hackers die voor hen werken buiten schot te houden. Transacties binnen de landsgrenzen worden ook minder snel opgepikt door de fraudedetectors in het computersysteem van de banken.