Russische criminelen krijgen volgens computerspecialisten al jaren bescherming van het Kremlin

Hackers stelen miljoenen van Citibank

Russische hackers hebben tientallen miljoenen dollar gestolen door in te breken in het computersysteem van de Amerikaanse financiële instelling Citibank, zegt de krant *The Wall Street Journal*. De bende in kwestie krijgt volgens beveiligingsfirma's al jaren bescherming van de Russische overheid.

DOOR RONALD MEEUS

BRUSSEL • De software die voor de hackings werd gebruikt, werd ook ingezet bij zware cyberaanvallen op servers van de Estse en Georgische overheid in respectievelijk 2007 en 2008. Er waren toen ook sterke vermoedens dat die aanvallen 'besteld' waren door het Kremlin.

De Amerikaanse veiligheidsdienst FBI onderzoekt een computerinbraak die zich wellicht enkele maanden geleden al heeft voorgedaan in de systemen van de Amerikaanse financiële groep Citibank. De inbrekers slaagden erin om via elektronische weg tientallen miljoenen dollar te stelen, zegt de zakenkrant *The Wall Street Journal*. Sporen van de aanval werden afgelopen zomer pas ontdekt, maar de inbraak zelf kan al veel ouder zijn. De zaak wordt nu onderzocht door de FBI en de National Security Agency, een andere veiligheidsdienst van de Amerikaanse overheid.

Ondertussen ontkent Citibank in alle toonaarden dat er ingebroken is in zijn computersystemen en dat er geld is gestolen van de rekeningen van de bank. Het bedrijf stuurde gisterochtend ook een - ondertussen op het internet gelekte - memo naar alle werknemers, waarin staat dat ze het nieuws staalhard moeten ontkennen als klanten vragen stellen.

Maar dat is het algemene beleid bij Citibank, zegt *The Wall Street Journal*: het bedrijf is de afgelopen twee decennia namelijk al enkele keren het slachtoffer geweest van computeraanvallen, en komt sindsdien niet graag meer in het nieuws. In 1994 slaagde een hacker er al eens in om 10 miljoen dollar te ontvreemden van Citibank, en die gebeurtenis werd een ware pr-ramp toen de bank daar openlijk over communiceerde. Sindsdien houdt Citibank, en daarmee ook de meeste andere Amerikaanse banken, haar mond dicht als er een geslaagde hackingaanval is geweest.

Black Energy

Volgens de gegevens van de FBI leidde het spoor van de computeraanval naar internetadressen die tot in 2007 werden gebruikt door een notoire Russische hackersbende. Het Russian Business Network voerde zelf heel wat internetaanvallen uit, maar levert ook de nodige software voor andere hackergroeperingen en beschikt over een groot zogeheten 'botnet': een netwerk van duizenden door een virus geïnfecteerde pc's van nietsvermoedende gebruikers, die kunnen worden ingezet bij een internetaanval.

BEVEILIGINGSEXPERT EDDY WILLEMS:

Er zijn sterke aanwijzingen dat de bende banden onderhoudt met de corrupte cenakels van de Russische overheid

Heel wat beveiligingsfirma's, waaronder het gezaghebbende Amerikaanse bedrijf VeriSign en de in Tokio gebaseerde groep Trend Micro, zeggen ook dat de bende contacten onderhield met de Russische overheid, en dat ze daardoor speciale bescherming genoot. "Er zijn sterke aanwijzingen dat ze banden onderhouden met de corrupte cenakels van de Russische overheid", zegt beveiligingsexpert Eddy Willems van het Europese computerbeveiligingscentrum Eicar. "Alleen: er zijn geen staalharde bewijzen die bruikbaar zouden zijn in een rechtbank. Bovendien zijn ook de kopstukken van de groep nog niet geïdentificeerd."

In 2007 verdween de groep ook ineens van de radar, toen haar activiteiten - het beschikbaar stellen van inbraaksoftware, maar ook het versturen van spam en het leveren van kinderporno - te veel aandacht kreeg. Maar de afgelopen maanden waren er verscheidene aanwijzingen dat bepaalde leden opnieuw actief zijn. "Een groot deel van hun activiteiten werd verplaatst naar China en een aantal andere landen", zegt Willems. "Dat maakt het nog moeilijker om hen in het oog te houden, of om te achterhalen waarmee ze gelinkt zijn."

Ook de software die werd gebruikt voor de aanval op het computersysteem van Citibank is van Russische makelij. Het programma Black Energy, dat eveneens wordt verkocht door de Russische hackergroep, is al enkele jaren in gebruik om aanvallen op specifieke sites te coördineren, en de recentste versie maakt het ook mogelijk belangrijke gegevens zoals bankrekeningen en wachtwoorden los te peuteren uit de aangevallen computersystemen.

Digitale oorlogsvoering

Het programma dook ook op in de onderzoeken die werden uitgevoerd na hackeraanvallen op overheidssites in Estland en Georgië, respectievelijk in 2007 en 2008. Ook bij die twee gebeurtenissen, die volgens de meeste beveiligingsexperts pal op de grens zaten tussen gewone informaticacriminaliteit en digitale oorlogsvoering, werd beweerd dat de Russische overheid in de schaduw de touwtjes in handen had.

Zeker in het geval van Georgië was het bijzonder verdacht. De internetaanvallen gebeurden precies op hetzelfde moment als een conventionele Russische aanval op het land. "Het is simpelweg ondenkbaar dat dat een toeval is", opperde Eka Tkeshelashvili, de Georgische nationale veiligheidschef, in maart van dit jaar tijdens een topconferentie over landsbeveiliging in de Amerikaanse stad Washington DC. "Er zijn een hoop aanwijzingen dat de aanvallen werden georganiseerd door de Russische overheid."