Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 251 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 augustus 2012

Naar aanleiding van het verzoek van het lid Gesthuizen (SP) om geïnformeerd te worden over het Dorifelvirus, wil ik u, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, met deze brief informeren over de stand van zaken omtrent dit virus. Het gaat hierbij om de karakteristieken en werkwijze van het virus en de recente activiteiten van het Nationaal Cyber Security Centrum (NCSC) om dit virus te bestrijden.

Karakteristieken van het Dorifel-computervirus

Een computervirus, zoals het Dorifel- computervirus, is een vorm van schadelijke software (malware). Het is een computerprogramma dat zich in een systeem kan nestelen met als doel schade aan te richten, in dit geval door office documenten aan te passen. Het Dorifel virus heeft zich in eerste instantie verspreid via systemen die al in een eerder stadium geïnfecteerd zijn met een variant van een ander virus, het zogenaamde Citadel virus, dat op zijn beurt weer een variant op het Zeus virus is.

Computers geïnfecteerd met het Citadel virus maken onderdeel uit van een Citadel botnet. Met dit Citadel botnet kan actief malware zoals Dorifel worden verspreid. Een botnet is een verzameling van geïnfecteerde computers van nietsvermoedende slachtoffers, dat centraal bestuurd kan worden door criminelen en de infrastructuur vormt voor veel vormen van cybercriminaliteit. Dit Citadel botnet heeft nu bijvoorbeeld de instructie gekregen om het Dorifel virus te downloaden.

Het Dorifel virus kan zich los van Citadel verder verspreiden via besmette documenten, bijvoorbeeld gedeeld via netwerkschijven of e-mail, waardoor ook systemen die geen Citadel besmetting hebben geïnfecteerd kunnen raken. De inhoud van de originele bestanden wordt door het virus veranderd waardoor deze bestanden niet meer leesbaar zijn. De inhoud van de originele bestanden wordt door het virus versleuteld, maar niet vernietigd. Vervolgens worden andere gebruikers die het getroffen document openen ook geïnfecteerd met het Dorifel virus. Zo kan het virus

kst-26643-251
ISSN 0921 - 7371
's-Gravenhage 2012

zich verspreiden in omgevingen waar gezamenlijk gewerkt wordt aan documenten, zoals overheids- en bedrijfsnetwerken. Op dit moment is er nog geen andere activiteit waargenomen. Of en wat voor activiteiten het virus verder kan ontplooien wordt verder onderzocht.

Stand van zaken

Sinds de eerste meldingen bestrijdt het Nationaal Cyber Security Centrum (NCSC) het Dorifel virus, de gerelateerde malware en de gebruikte infrastructuren (het Citadel botnet) voor de verspreiding hiervan.

Het Dorifelvirus is voor het eerst op dinsdag 7 augustus jl. verspreid. Op woensdagmiddag 8 augustus jl. heeft het NCSC de eerste meldingen van dit virus binnen gekregen via verschillende private- en overheidspartijen. Deze relatief late meldingen houden verband met het feit dat de infectie pas actief wordt na een herstart van het computersysteem. In reactie op de eerste meldingen van het virus heeft het NCSC een uitgebreid onderzoek gestart om de karakteristieken van het virus in kaart te brengen en meer inzicht te krijgen in de verspreidingsgraad van de malware en de mate waarin organisaties zijn getroffen. Naar aanleiding van de meldingen van het Dorifelvirus heeft het NCSC op woensdag 8 augustus een waarschuwing uitgestuurd binnen de overheid en richting de vitale sectoren. Daarnaast zijn ook de aangesloten partijen binnen het NCSC geïnformeerd. Het blijkt dat naast de overheid ook bedrijven zijn getroffen door het Dorifelvirus. Toen verdere verspreiding zichtbaar werd is ook actief via de media gecommuniceerd.

Vanaf woensdag 8 augustus zijn in ieder geval 30 instellingen waaronder gemeenten, bedrijven en universiteiten getroffen door het Dorifelvirus. Voor wat betreft de Rijksoverheid hebben de ministeries aan de RijksCIO gerapporteerd dat besmetting is opgetreden bij het Rijksinstituut voor Volksgezondheid en Milieu (RIVM, twee PC's), het Koninklijk Meteorologisch Instituut (KNMI, 3 PC's), het ministerie van Onderwijs, Cultuur en Wetenschappen (OCW, 6 PC's), het ministerie van Economische Zaken, Landbouw en Innovatie (EL&I, 10 PC's en twee servers) en op één PC op het separate studentennetwerk van de Nederlandse Defensie Academie (NLDA). Genoemde organisaties geven aan dat de besmetting is bestreden, dat besmette bestanden zijn geïsoleerd en worden geschoond en dat bedrijfscontinuïteit van de organisaties niet in het geding is geweest. Hoewel niet uit te sluiten, zijn er geen aanwijzingen dat het virus zich via de websites van betroffen organisaties verder heeft verspreid en dat er persoonsgegevens van burgers zijn gelekt. Er is voorts geconstateerd dat er vanuit een systeem van de Kustwacht contact is geweest met een internetmachine welke het virus verspreidde maar van een besmetting is vooralsnog geen sprake. Dit Kustwacht systeem is in quarantaine genomen en uit voorzorg opgeschoond.

Daarnaast is uitgebreid in de media aan de orde geweest dat dienstverlening bij een aantal gemeenten is getroffen. De verspreiding van het Dorifelvirus heeft een impact op de bedrijfsvoering van deze organisaties gehad. Dit heeft op lokaal niveau in een aantal gevallen geleid tot de tijdelijke stoplegging van de uitvoering van verschillende publieke taken om het virus te verwijderen.

Op dit moment is nog een aantal van de getroffen instellingen bezig met het verwijderen van het virus van de eigen systemen en bestanden. Sinds vrijdagochtend 10 augustus zijn er bij het NCSC geen nieuwe meldingen meer binnengekomen. Daar het Dorifelvirus pas geactiveerd wordt bij het opstarten van systemen is het niet uit te sluiten dat het Dorifelvirus zich komende weken nog zal manifesteren.

Momenteel wordt samen met verschillende onderzoekspartijen de werking van het virus bekeken. Het onderzoek richt zich nu voornamelijk op de omvangrijke internationale infrastructuur die is gebruikt om Dorifel te verspreiden (het Citadel botnet). Er wordt actief opgetreden om de resterende dreiging die uitgaat van deze infrastructuur, en daarop gefaciliteerde malware, weg te nemen en de criminele operatie te verstoren. Te nemen maatregelen worden geïnventariseerd en gedeeld om het virus te bestrijden. De IP-adressen die betrokken zijn bij verspreiding van het Dorifel virus zijn op verzoek van het NCSC, met medewerking van Internet Service Providers onbereikbaar gemaakt. Tevens zijn het Openbaar Ministerie en Politie begonnen met een strafrechtelijk onderzoek naar de dader(s) achter dit netwerk. Recent zijn in de media berichten verschenen dat ook cliënten van banken getroffen zijn door het Citadel botnet waarlangs ook het Dorifelvirus is verspreid. Op basis van het huidige inzicht van het NCSC betreft het de computers van enkele honderden cliënten. In overleg met het NCSC zullen de banken hun getroffen cliënten actief benaderen.

NCSC

Het NCSC werkt samen met zijn publieke- en private partners aan de bestrijding van de malware en de ondersteuning van getroffen instanties. Op de websites NCSC.nl en waarschuwingsdienst.nl plaatst het NCSC informatie en beveiligingsadviezen om besmetting te voorkomen en over hoe het virus verwijderd kan worden.

Het NCSC heeft zich sinds de eerste melding van het Dorifelvirus gericht op:

1. Het inzichtelijk krijgen van de oorsprong en werking van de malware;
2. Meer informatie verkrijgen over de verspreiding van de malware;
3. Het coördineren van activiteiten en het bieden van handelingsperspectief om de malware te bestrijden;
4. Het actief nemen van beschermingsmaatregelen voor het onschadelijk maken van onderliggende command en control structuren (bijvoorbeeld, het onbereikbaar laten maken van IP-adressen door Internet Service Providers).

Tot slot

De komende periode blijft mijn ministerie zich richten op het onderzoek naar de aard en omvang van dit virus. Het NCSC werkt hiertoe intensief samen met de getroffen organisaties, bedrijven en personen uit de cyber security gemeenschap. Wanneer uit dit onderzoek relevante conclusies kunnen worden getrokken, zal ik uw Kamer hierover informeren.

Als laatste kondig ik u aan dat ik op korte termijn mijn toezegging gestand zal doen en u de uitkomst van mijn inventarisatie naar noodzakelijke nieuwe strafrechtelijke opsporingsbevoegdheden op het internet in het algemeen zal toezenden. Doel van deze nieuwe wetgeving is het juridisch kader voor de opsporing en vervolging van cybercrime meer toe te snijden op de door de diensten, die zijn belast met de opsporing en vervolging van cybercrime, gesignaleerde behoeften.

De minister van Veiligheid en Justitie,
I. W. Opstelten