Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Nadere analyse Pobelka-botnet

In samenwerking met AIVD, MIVD, NCTV, OM en Politie

28 maart 2013

Inhoud

1 Inleiding

Deze rapportage beschrijft de uitkomsten van de nadere analyse van het Pobelka-botnet door de Pobelka-taskforce. In deze taskforce werken de Politie, het OM, de AIVD, de MIVD, het NCSC en de NCTV samen om nader onderzoek te doen naar de dataset die afkomstig is van de verkregen Command en Control (C&C)-server van het Pobelka-botnet, ieder op grond van de eigen bevoegdheden. Een dergelijke C&C-server dient als een spin in het web om instructies naar geïnfecteerde computers te versturen en informatie vanaf deze computers te ontvangen.

Dit gezamenlijke onderzoek is gedaan in aanvulling op de response en het onderzoek die het NCSC in december 2012 al heeft uitgevoerd na een melding van het bedrijf Digital Investigation. Het doel van dit aanvullende onderzoek is enerzijds een inschatting te maken wat de potentiële impact is op de nationale veiligheid van de gegevens in deze dataset en anderzijds beoordelen of en op welke manier aanvullende response noodzakelijk is richting slachtoffers. Hierbij is in het bijzonder aandacht voor organisaties, zowel publiek als privaat, die zich in de vitale sectoren bevinden.

Dit rapport is tot stand gekomen onder verantwoordelijkheid van de Directie Cyber Security (DCS) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

In dit aanvullende onderzoek zijn op basis hiervan de volgende drie hoofdvragen geformuleerd:

- Is de nationale veiligheid in het geding (geweest)?
- Wie is er verantwoordelijk voor het botnet?
- Is extra response noodzakelijk, in aanvulling op de in december 2012 ondernomen acties?

2 Botnets

2.1 Wat is een botnet?

Het woord 'bot' is afgeleidt van het woord robot. Een bot is een programma dat zelfstandig geautomatiseerd werk verricht. Zoekmachines gebruiken bijvoorbeeld bots om websites in kaart te brengen. Helaas kunnen bots ook voor andere doeleinden ingezet worden, voor het uitvoeren van kwaadaardige handelingen. Hiervoor worden onschuldige computers besmet met een kwaadaardig programma en wordt de bot geïnstalleerd op deze computer, waardoor deze onder controle komt van een crimineel.

Een botnet is een grote groep geïnfecteerde computers die met elkaar verbonden zijn via internet. Criminelen beheren zo'n botnet en proberen ervoor te zorgen dat er zoveel mogelijk computers geïnfecteerd worden met sofware om deze kwaadaardige handelingen uit te voeren. Deze software is niet zichtbaar voor de gebruiker van de computer omdat het op de achtergrond draait. Ook is het vaak niet herkenbaar door symptomen als een traag werkende computer. Deze kwaadaardige software wordt in eerste instantie vaak niet goed herkend door beveiligingssoftware (zoals anti-virus) of schakelt deze zelfs volledig uit.

De computer wordt onderdeel van een botnet wanneer deze besmet wordt. Dit gebeurt bijvoorbeeld door het misbruiken van kwetsbaarheden in de software die op de computer geïnstalleerd staat[1]. Deze besmetting gebeurt in veel gevallen door het bezoeken van een besmette website waar een zogenaamde 'drive-by download' plaatsvindt die deze kwetsbaarheden misbruikt, maar kan ook plaatsvinden via een bijlage bij een e-mail of door besmette USB-sticks. De 'bots' in het botnet kunnen vervolgens worden ingezet om bijvoorbeeld informatie te verzamelen van de geïnfecteerde computer, andere computers op internet aan te vallen (bijvoorbeeld DDoS) of om spam te versturen.

De bots kunnen worden aangestuurd door een of meerdere centrale computer op internet, de zogenaamde Command & Control-servers (C&C). Deze C&C-servers voorzien de bots van opdrachten en ontvangen de resultaten van deze opdrachten, bijvoorbeeld buitgemaakte inloggegevens. Deze C&C-servers zijn veelal een verzameling van verschillende computers, die vaak verspreid over de wereld staan en regelmatig verhuizen. Op deze manier wordt de criminele organisatie erachter beschermd, omdat het ontmantelen van deze infrastructuur bemoeilijkt wordt en de crimineel zich goed kan verbergen. De aanpak van botnets vereist internationale samenwerking tussen verschillende organisaties. De aanpak van het Bredolab-botnet in 2010 is hier een voorbeeld van, maar ook recenter de response op de uitbraak van Dorifel in augustus 2012.

---

[1] Het NCSC publiceert beveiligingsadviezen over software-kwetsbaarheden op haar website en op de website van De Waarschuwingsdienst . In zo'n advies wordt beschreven wat er aan de hand is, op welke systemen het impact heeft en wat er moet gebeuren om te voorkomen dat een organisatie slachtoffer wordt. Het NCSC publiceert hierop ook over actuele dreigingen zoals een veelbezochte website die malware verspreidt of een kwetsbaarheid die op grote schaal misbruikt wordt. Zie https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen

2.2 Wat is Pobelka?

Pobelka is de naam[2] van het botnet dat gebruik maakt van een softwaredistributieplatform dat 'Citadel' heet. Citadel is gebaseerd op de broncode van ZeuS, een ander platform. Citadel staat bekend als een zogenaamde 'banking trojan', oftewel een digitaal Trojaans paard dat zonder dat men het door heeft op de computer aanwezig is en primair gericht is op het manipuleren van financiële transacties tijdens het internetbankieren. Citadel is eind 2011 voor het eerst opgedoken toen de ondersteuning van andere een 'banking trojan', SpyEye, niet meer beschikbaar was[3].

Er is een ondergronds netwerk waar afnemers (criminelen) in contact kunnen komen met aanbieders van Citadel, die vervolgens als dienst of als software afgenomen kunnen worden. De Citadel-bots worden hoofdzakelijk gebruikt voor het manipuleren van financiële transacties tijdens het internetbankieren maar kunnen ook nieuwe software ontvangen voor andere toepassingen, zoals de installatie van ransomware[4] wat bij Dorifel[5] het geval was. Dorifel was malware die in augustus 2012 verspreid werd en naar documenten op netwerkschijven en externe media (zoals USB-sticks, externe hardeschijven) zocht en deze versleutelde. Het was de bedoeling dat door te betalen de documenten weer ontsleuteld kunnen worden.

2.3 Zijn er nog meer botnets?

Regelmatig worden er nieuwe botnets ontdekt maar er zijn geen exacte cijfers over het aantal botnets met geïnfecteerde computers in Nederland en hoeveel bots er actief zijn in deze botnets. In 2011 zijn de resultaten gepubliceerd[6] van een onderzoek dat de TU Delft in opdracht van het ministerie van Economische Zaken, Landbouw & Innovatie uitvoerde naar o.a. het tegengaan van botnets. Hierin staat dat in de geobserveerde periode, januari 2009 tot juni 2010, er 1,1 miljoen IP-adressen zijn geïdentificeerd die duiden op een mogelijk infectie. Van deze adressen waren er ongeveer 900.000 in het netwerk van de grote Nederlandse Internet Service Providers. Een conservatieve interpretatie hiervan zou duiden op ongeveer 450.000 tot 900.000 geïnfecteerde computers. Dit komt erop neer dat zo'n 5 tot 10 procent van alle Nederlandse breedband internetabonnees een geïnfecteerde computer heeft. Ook duidt de verzamelde data erop dat het aantal geïnfecteerde computers toeneemt. Geïnfecteerde computers en de botnets waar ze deel van uitmaken en bijbehorende criminaliteit horen dus het bij internet van vandaag de dag.

---

[2] Demystifying Pobelka (Fox-IT)
http://blog.fox-it.com/2013/01/11/demystifying-pobelka/

[3] Demystifying Pobelka (Fox-IT)
http://blog.fox-it.com/2013/01/11/demystifying-pobelka/

[4] Mijn computer is gekaapt en er wordt losgeld geëist, wat nu?
https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/ransomware.html

[5] NCSC publiceert factsheet naar aanleiding van Dorifel
https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-factsheet-nav-dorifel.html

[6] Internet service providers and botnet mitigation
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html

Het NCSC ontvangt regelmatig informatie[7] over geïnfecteerde computers uit diverse bronnen. Deze gegevens zijn bijvoorbeeld afkomstig van computers die door beveiligingsonderzoekers in plaats van C&C-servers op internet worden geplaatst. Deze zogenaamde 'sinkholes' registreren vervolgens de verbindingen van bots. Hierbij wordt het IP-adres waar vandaan verbinding wordt gemaakt geregistreerd die vervolgens gebruikt kan worden om de persoon of organisatie achter dat IP-adres, bijvoorbeeld via de Internet Service Provider, op de hoogte te stellen. In 2011 en het eerste kwartaal van 2012 waren er 2.400 meldingen[8] die betrekking hadden op organisaties die tot de doelgroepen van het NCSC behoren.

2.4 Welke gegevens worden er ontvreemd?

De meeste botnets zijn er op gericht om financiële transacties tijdens het internetbankieren te manipuleren om er op die manier voor te zorgen dat het geld uiteindelijk bij de criminelen terecht komt. Dit gebeurt via een zogenaamde 'Man in the Browser' (MITB). Dit betekent dat de malafide software in staat is om de gegevens die de webbrowser verstuurt en ontvangt te manipuleren zonder dat de gebruiker dit doorheeft. Doordat dit in de webbrowser gebeurt is het voor de nietsvermoedende gebruiker lastig om te herkennen. Het 'slotje', waarmee gecontroleerd kan worden of er een beveiligde verbinding is, blijft aanwezig en geeft geen waarschuwing. Via de manipulatie van financiële transacties tijdens het internetbankieren is in de eerste helft van 2012 € 27,3 miljoen verduisterd[9], een stijging van 14% t.o.v. de tweede helft van 2011.

Ook worden andere inloggegevens buitgemaakt voor diverse doeleinden. Zo kunnen inloggegevens voor internetbankieren uiteraard gebruikt worden voor het ontvreemden van geld van de bankrekening van de gebruiker die inlogt. Maar ook andere inloggegevens worden buitgemaakt waarbij er een bijzondere interesse is voor inloggegevens die gebruikt kunnen worden om het botnet uit te breiden en spam te verspreiden. Zo kunnen inloggegevens die gebruikt worden voor het onderhouden van een website, zoals voor een FTP-server[10] of voor een CMS[11], gebruikt worden om computers van bezoekers van deze websites te besmetten door een 'drive-by download'. Dit hebben we in 2012 onder andere gezien op de websites van Nu.nl[12], Telegraaf.nl[13], Weeronline.nl[14] en diverse andere

---

[7] IP-adres en tijdstip dat er contact is gemaakt

[8] Cybersecuritybeeld Nederland
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland.html

[9] Fraude internetbankieren stijgt eerste half jaar met 14%
http://www.nvb.nl/nieuws/2012/687/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14.html

[10] Server die gebruikt wordt om bestanden en webpagina's op een website te plaatsen en aan te passen

[11] Content Management System, een systeem voor het onderhouden van een website

[12] Malware verspreid via nieuwssite NU.nl
https://www.ncsc.nl/actueel/nieuwsberichten/malware-verspreid-via-nieuwssite-nu.nl.html

[13] Nieuwssite telegraaf.nl linkte naar malware
https://www.ncsc.nl/actueel/nieuwsberichten/nieuwssite-telegraaf.nl-linkte-naar-malware.html

[14] Malware bij weeronline.nl
https://www.ncsc.nl/actueel/nieuwsberichten/waarschuwingsboodschap-opgesteld-voor-weeronline.nl.html

veelbezochte websites. Ook kunnen inloggegevens voor e-mail diensten gebruikt worden om spam te versturen.

Om er zeker van te zijn dat (inlog)gegevens die via internet worden verstuurd onderschept worden, worden meestal alle gegevens die naar een website worden verstuurd (middels invoervelden op een webpagina, de zogenaamde 'POST'-data) opgevangen en opgeslagen. Deze gegevens worden rechtstreeks doorgestuurd naar de centrale C&C-server en daar opgeslagen. De gegevens die in deze 'POST'-data is heel divers, het betreft immers alle informatie die verstuurd wordt en dus ook potentieel gevoelige informatie.

3 Pobelka

Het Pobelka-botnet is een botnet dat gebruik maakt van het Citadel softwaredistributieplatform. De informatie op de verkregen C&C-server van dit botnet is in december in handen gekomen van Digital Investigation, dat een analyse van Pobelka heeft gemaakt[15]. Daarnaast is er door het anti-virusbedrijf SurfRight gepubliceerd[16] over dit botnet.

In februari 2013 komt het Pobelka-botnet opnieuw onder de aandacht in een reportage van de NOS. Journalisten hebben van Digital Investigation toegang gekregen tot de volledige dataset van 750GB die op de verkregen C&C server heeft gestaan. De reportage laat zien hoe divers de informatie is die buitgemaakt wordt en hoe gevoelig deze informatie in sommige gevallen is.

De informatie die door dit botnet is ontvreemd en het verhoogde risico door de aandacht die de dataset heeft gekregen zijn aanleiding geweest om aanvullend onderzoek te doen naar de aard van de door het botnet verzamelde informatie. Het onderzoek is er op gericht in te schatten of de nationale veiligheid in het geding is of is geweest en of er extra response noodzakelijk is richting de getroffen organisaties en andere slachtoffers. Daarnaast wordt er gekeken of er aanknopingspunten zijn voor een opsporingsonderzoek naar degene(n) die verantwoordelijk is of zijn voor dit botnet.

In dit aanvullende onderzoek zijn op basis hiervan de volgende drie hoofdvragen geformuleerd:

- Is de nationale veiligheid in het geding (geweest)?
- Wie is er verantwoordelijk voor het botnet?
- Is extra response noodzakelijk, in aanvulling op de in december 2012 ondernomen acties?

Om deze vragen te beantwoorden is de Pobelka-taskforce samengesteld waarin publieke partijen op grond van haar eigen taken en bevoegdheden samenwerken, te weten de Politie, het OM, de AIVD, de MIVD, de NCTV en het NCSC. Het NCSC heeft op grond van artikel 19 van de Wet Politiegegevens (WPG) de beschikking gekregen over de gegevens die op de verkregen C&C-server stonden en heeft het NFI gevraagd een analyse uit te voeren.

---

[15] The Pobelka Botnet - a Command and Control case study.
http://check.botnet.nu/technical.html

[16] Citadel-malwareonderzoek "Pobelka" botnet (SurfRight)
http://www.surfright.nl/nl/hitmanpro/pobelka

4 Potentiële impact van de verzamelde data

Om een goed inschatting te maken van de potentiële impact van lekken van de informatie is in de nadere analyse gekeken naar een aantal indicatoren:

- Was het botnet gericht op Nederland?
- Was er sprake van gerichte spionage?
- Welke gegevens zijn buitgemaakt?
- Was het botnet gericht op bepaalde organisaties of sectoren?
- Hoe verhoudt dit botnet zich tot andere botnets?

De geïnfecteerde computers bevinden zich bij een grote diversiteit aan organisaties in diverse sectoren, ook in sectoren die door de overheid als 'vitaal' zijn aangemerkt[17] en bij de overheid zelf. Om een betere beoordeling te kunnen geven of door deze geïnfecteerde computers de nationale veiligheid in het geding is geweest, is er een steekproef gedaan op de buitgemaakte gegevens van organisaties in de vitale sectoren die in de analyse geïdentificeerd zijn.

Uit deze steekproef is gebleken dat het grootste deel van de door het botnet verzamelde gegevens betrekking hebben op algemeen beschikbare, publieke internetdiensten die door medewerkers in gebruik zijn. Een veel kleiner deel heeft betrekking op interne netwerkdiensten; zoals intranetsites, reserveringssystemen voor vergaderzalen e.d. Tijdens deze steekproef is geen informatie aangetroffen die een acuut risico vormt voor de continuïteit van getroffen organisaties of de nationale veiligheid. Wel is de aard van de informatie dusdanig dat de gegevens een basis kunnen vormen voor geslaagde gerichte aanvallen, die in potentie wel een grote impact kunnen hebben. Het is hierbij belangrijk om op te merken dat gezien het karakter van de steekproef een garantie niet te geven is. Tevens is meer kennis over de organisaties noodzakelijk om de data op de juiste manier te kunnen beoordelen. Andere bevindingen uit de steekproef zijn opgenomen in paragraaf 4.3.

4.1 Gericht op Nederland?

In het rapport[18] dat door SurfRight is opgesteld bleek al dat het overgrote deel van de geïnfecteerde computers van het Pobelka-botnet die in deze dataset voorkomen in Nederland en Duitsland staat. Dit blijkt ook uit dit onderzoek op de dataset van de verkregen C&C-server, 54,5% van de 264.339 IP-adressen [19]in de dataset zijn actief in Nederland[20] en 30,7% in Duitsland, zie ook Figuur 1. De overige IP-adressen bevinden zich in 115 andere landen verspreid over de wereld, waaronder Frankrijk (2%), de Verenigde Arabische Emiraten (1,9%) en Polen (1,6%).

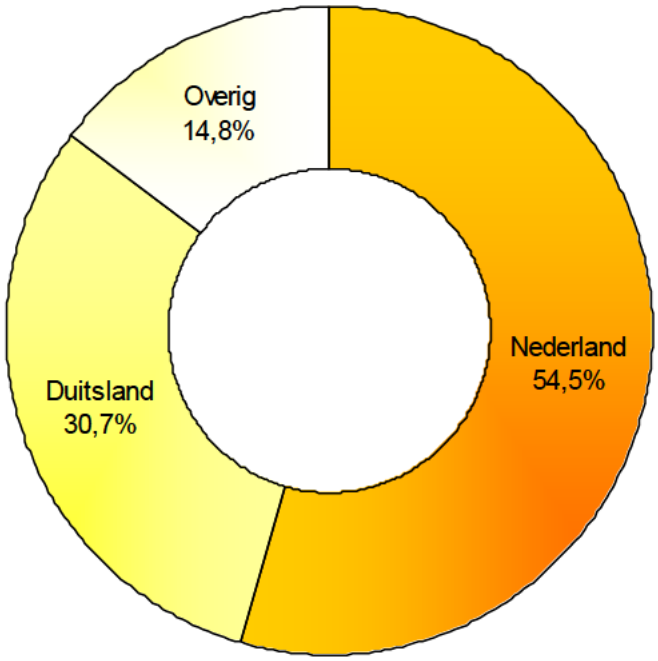
---

[17] Vitale sectoren infrastructuur
http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2010/06/25/vitale-sectoren-infrastructuur.html

[18] Citadel-malwareonderzoek "Pobelka" botnet (SurfRight)
http://www.surfright.nl/nl/hitmanpro/pobelka

[19] Het IP-adres waarmee de computer als laatste verbinding heeft gemaakt

[20] Land bepaald op basis het laatste bekende ip en geoip, afkomstig van The Shadowserver Foundation



Figuur 1: Verspreiding IP-adressen over landen

De geïnfecteerde computers zijn verspreid over verschillende campagnes. Deze campagnes zijn bedoeld om in een bepaalde periode opdrachten met specifieke doeleinden te verstrekken aan bots, bijvoorbeeld gericht op een bepaalde bank, of juist bots uit een bepaald land toe te voegen aan het botnet. Op de C&C-server zijn ook aanwijzingen gevonden waaruit blijkt dat verkeer naar bepaalde Nederlandse banken gemanipuleerd is.

Deze verschillende campagnes zijn tijdens bepaalde periodes actief geweest. De eerste campagne die gedraaid heeft vanaf de C&C-server, Mango, is gestart op 2 februari 2012 en de laatste campagne is geëindigd op 19 september 2012 (zie Tabel 1).

Tabel 1: Looptijd campagnes

Campagne	Eerst gemelde infectie	Laatst gemelde infectie
Mango	2012-02-02 19:48:10	2012-03-30 03:01:16
Lime	2012-03-22 08:23:17	2012-08-24 12:06:24
Pepper	2012-06-30 11:04:08	2012-09-19 14:16:27

Van deze computers (bots) wordt diverse informatie bijgehouden, zoals de versie van de bot, van het besturingssysteem en de taal. Maar ook worden persoonsidentificerende gegevens als IP-adres, loginnaam en logindomein opgeslagen. Er zijn 3 campagnes gevonden met daadwerkelijk geïnfecteerde computers (Zie ook Tabel 2).

Tabel 2: Geïnfecteerde computers per campagne

Campagne	Unieke IP's	Unieke bots	Unieke ldomeinen	Unieke gebruikersnamen
Lime	354.854	117.441	75.570	58.786
Pepper	213.812	68.376	47.202	35.619
Mango	151.863	53.029	37.557	26.827
Totaal	699.946	222.663	136.209	103.552

Toelichting Tabel 2: De in deze tabel genoemde aantallen zijn unieke aantallen, d.w.z. unieke IP-adressen, unieke bots op basis van bot_id, unieke Windows-domeinen en unieke gebruikersnamen. Een bot kan meerdere IP-adressen hebben gehad.

Dat deze campagnes gericht zijn op een bepaald land of bepaalde landen is niet vreemd, zo is er bij criminelen een voorkeur voor landen waar mensen veel actief zijn op internet, er veel en snelle internetverbindingen zijn en voor criminelen niet onbelangrijk; waar veel gebruik wordt gemaakt voor internetbankieren. In Nederland wordt samen met Finland het meest gebruik gemaakt van internetbankieren in Europa[21].

Om een campagne succesvol te maken spelen ook andere zaken een rol. Als een campagne bijvoorbeeld gericht is op een bepaalde Nederlandse bank moet er verkeer van Nederlandse computers gemanipuleerd worden. Deze computers zijn oorspronkelijk geïnfecteerd en toegevoegd aan een botnet door bijvoorbeeld op een Nederlandse website een 'drive-by download' te plaatsen. Om het geld vervolgens het land uit te sluizen zijn er ook Nederlandse bankrekeningen en dus Nederlandse 'money mules'[22] nodig. Om succesvol te zijn is de hele keten van belang en moet deze hele keten dus soepel verlopen. De campagne richten op meerdere landen maakt het moeilijker om controle te houden over de hele keten.

4.2 Was er sprake van gerichte spionage?

De informatie die door het Pobelka-botnet en Citadel in het algemeen wordt buitgemaakt is gevoelig. Immers, alle informatie die men via de webbrowser verstuurd wordt afgevangen en verstuurd naar de C&C-server. Zoals al eerder aangegeven is het primaire doel van Citadel-botnets het manipuleren van financiële transacties, alle overige gegevens die worden verzameld kunnen beschouwd worden als 'bijvangst'. Delen van deze bijvangst worden vaak ook, in bulk, gebruikt en doorverkocht. Het gaat hier bijvoorbeeld om inloggegevens voor populaire websites, zoals Facebook of Twitter, maar ook voor de eerder genoemde CMS-beheerpagina's. Het onderzoek geeft geen aanleiding om het Pobelka-botnet anders te classificeren. Dit wordt onderschreven door de onderzoekers van AIVD, MIVD en NFI. Hieronder wordt dit verder onderbouwd.

Er zijn verschillende soorten informatie die door een botnet verzameld kunnen worden. Een overzicht van de data die door het Pobelka-botnet is verzameld is opgenomen in Tabel 3. De tabel geeft weer welke soorten informatie er verzameld kunnen worden en welke er ook verzameld zijn. Als informatie niet verzameld is dan staat hier een '-'. Het aantal keren dat HTTP- en HTTPS-gegevens zijn

[21] Nederland in Europese top met internetbankieren http://www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2012/2012-3662-wm.htm

[22] Iemand dia via zijn/haar eigen bankrekening geld naar criminelen (in het Buitenland) sluist

bemachtigd ondersteunt dat het botnet zich met name heeft gericht op webverkeer. Een omschrijving van een aantal belangrijke soorten gegevens is te vinden in de Toelichting Tabel 3.

Tabel 3: Aantal keren dat soorten gegevens gerapporteerd zijn

Soorten gegevens	Mango	Lime	Pepper	Totaal
Cookies or browsers	41.854	35	-	41.889
File	-	-	-	0
HTTP	129.639.408	426.206.467	156.009.926	711.855.802
HTTPS	16.617.829	26.377.682	8.074.887	51.070.398
LUHN10 request	-	-	-	0
FTP Login	29.175	99.406	43.435	172.016
POP3 Login	2.430.450	14.554.558	4.031.659	21.016.667
Files	-	-	-	0
Keylogger	-	-	-	0
Grabbed UI	-	-	-	0
Grabbed Data [HTTP]	-	-	-	0
Grabbed Data Winsocket	-	-	-	0
Grabbed Data FTP Client	5.175	6.385	4.356	15.916
Grabbed Data Email	21.553	91.126	37.253	149.932
Grabbed Data Other	-	-	-	0
Command Line Result	66.731	170.354	78.581	315.666
Installed Software	2	186.732	1	186.735
Installed Firewall	1	161.241	-	161.242
Installed AntiVirus	1	165.707	-	165.708

Toelichting Tabel 3: Omschrijving soorten gegevens

File, Files – Opgevangen bestanden
HTTP - Aantal afgevangen post requests verstuurd via een HTTP-verbinding (web browser)
HTTPS - Aantal afgevangen post requests verstuurd via een beveiligde HTTPS-verbinding (web browser)
LUHN10 request - Een formule om bepaalde gegevenspatronen af te vangen, bijvoorbeeld creditcardnummers
Keylogger - De malafide software vangt alle toetsaanslagen af
FTP Login, Grabbed Data FTP Client - Afgevangen en/of gevonden FTP inloggevens
POP3 Login, Grabbed Data E-mail - Afgevangen inloggegevens voor e-mail
Command Line Result - Resultaat van bepaalde commando's die op het systeem zijn uitgevoerd, zoals door Windows in het geheugen bewaarde (NetBIOS) computernamen op het nabije netwerk en de netwerkconfiguratie (ipconfig)
Installed Software, Installed Firewall, Installed AntiVirus – Verzamelde informatie over geïnstalleerde en/of geactiveerde software op het systeem

Er is onderzocht of er gericht gezocht is naar bepaalde soorten informatie of bepaalde documenten of dat er verkeer naar bepaalde websites is afgevangen anders dan websites van bepaalde banken. Op basis van de door het botnet verzamelde gegevens en de opdrachten die door de beheerder van het botnet zijn afgegeven is er op dit moment geen aanleiding om aan te nemen dat dit het geval is.

Gedurende de tijd dat het botnet actief was en de besmette systemen onder controle van de beheerder van het botnet waren, waren deze bruikbaar voor het organiseren van aanvallen of informatievergaring op andere systemen op het interne netwerk van de organisaties, afhankelijk van de door de organisaties gebruikte netwerkarchitectuur en beveiligingsmaatregelen.

4.3 Welke gegevens zijn buitgemaakt?

De buitgemaakte gegevens zijn heel divers. Persoonidentificerende gegevens, bedrijfsinformatie (zoals concurrentiegevoelige informatie), informatie over de computer en kwetsbaarheden in software gebruikt door de getroffen organisatie of persoon hebben voor verschillende actoren een grote waarde en worden soms voor grote bedragen verhandeld. Kant-en-klare informatieverzamelingen die relatief eenvoudig te verhandelen zijn, zijn op deze manier steeds vaker te koop, zoals bijvoorbeeld creditcardgegevens. Persoonsidentificerende gegevens kunnen op eenzelfde manier verhandeld worden maar ook gebruikt worden voor identiteitsfraude of voor het misleiden van mensen, bijvoorbeeld met behulp van 'social engineering'.

In deze paragraaf wordt verder ingegaan op een aantal soorten van gegevens die zijn buitgemaakt.

4.3.1 Inloggegevens

Het botnet verzamelt inloggegevens die de gebruiker van een geïnfecteerde computer gebruikt. In de meeste gevallen gaat het hier om gebruikersnamen en wachtwoorden die verstuurd worden via de invoervelden van een formulier op een website, zoals bij het inloggen op een webmail-omgeving. Naast deze informatie wordt er ook informatie inloginformatie verzamelt via HTTP en HTTPS 'Basic Authentication' op websites, voor het lezen van email (POP3) en voor het uitwisselen van bestanden (FTP/FTPS). Deze gegevens zijn terug te vinden in Tabel 3 onder 'FTP Login', 'POP3 Login' en 'Grabbed Data FTP Client'. Op deze wijze zijn in totaal 232.989 verschillende inloggegevens verzameld. In Tabel 4 is weergegeven hoeveel gegevens er per type zijn buitgemaakt, HTTP en HTTPS zijn in deze tabel terug te vinden onder 'Grabbed Data FTP Client'

Tabel 4: Unieke verzamelde inloggegevens per type

Type inloggegeven	Hoeveelheid verzamelde gegevens
FTP	52.764
FTPS	27
HTTP	47
HTTPS	6
POP3	180.145
Totaal	232.989

Omdat de malafide software alle gegevens verzamelt die via de webbrowser verstuurd worden, worden ook alle inloggegevens verzameld die worden gebruikt in invoervelden op webpagina's. In veel bedrijfsomgevingen wordt er gebruik gemaakt van Outlook Web Access (OWA) om op een gemakkelijker manier via internet toegang te hebben tot de zakelijke e-mail omgeving. Bij de analyse is er specifiek gegevens naar dit verkeer. Het botnet heeft, naast de inloggegevens, 206.221 verschillende e-mailberichten verzameld. Het is belangrijk om hierbij op te merken dat berichten die in een mailbox zijn opgeslagen in veel gevallen zeer vertrouwelijk van aard zijn.

4.3.2 Informatie over netwerkomgeving

De malafide software verzamelt informatie over het systeem en de omgeving van het systeem. Dit is in Tabel 3 te vinden onder 'Command Line Result'. Het gaat hier ondermeer om de informatie die Windows opslaat voor het verbinding maken met diensten en apparaten op het interne netwerk waar de computer zich in bevindt. Het gaat hier om netwerknamen (NetBIOS) die door Windows in het geheugen bewaard worden.

Ook is bij een bot IP-informatie (ipconfig) terug te vinden. Het betreft hier IP-adressen van netwerkadapters die in het geïnfecteerde systeem aanwezig zijn, dit zijn IP-adressen die door deze computer op het lokale netwerk gebruikt worden. Op basis hiervan is er geen aanleiding om aan te nemen dat er actieve netwerkverkenning heeft plaatsgevonden. Echter levert dergelijke informatie bij netwerken die 'plat' zijn, oftewel niet opgedeeld in bepaalde subnetwerken, wel een goed beeld op van het netwerk en de servers en diensten die aanwezig zijn op dit netwerk. Deze informatie kan door een kwaadwillende die kennis heeft van de omgeving en organisatie waarin een geïnfecteerde computer staat, gebruikt worden bij een geavanceerde aanval op deze organisatie.

4.3.3 Informatie over geïnstalleerde software en draaiende processen

Er wordt ook informatie verzameld over de software die er op de computer geïnstalleerd staat. Dit is in Tabel 3 te vinden onder de noemer 'Installed Software'. In combinatie met de informatie over de netwerkomgeving zijn dit gevoelige gegevens. Het geeft weer welke software er in een organisatie aanwezig is en waar bij een aanval (zowel van binnen- als van buitenaf) misbruik van gemaakt kan worden.

Door de malware wordt ook informatie verzameld over de draaiende programma's (processen) die op het systeem actief zijn. Het gaat hier in de meeste gevallen om legitieme processen die op een Windows-systeem aangetroffen kunnen worden. Echter zijn er in een aantal gevallen ook procesnamen aangetroffen die erop kunnen wijzen dat er ook andere malware op het systeem aanwezig was op het moment dat de procesinformatie verzameld is.

4.4 Was het botnet gericht op bepaalde organisaties of sectoren?

Op basis van de diversiteit van getroffen systemen en buitgemaakte gegevens is er op dit moment geen reden om aan te nemen dat het botnet specifiek gericht was op specifieke overheden, sectoren of organisaties.

4.5 Hoe verhoudt dit botnet zich tot andere botnets?

Op basis van de buitgemaakte gegevens zijn er geen aanwijzingen gevonden dat de aard van dit botnet anders is dan andere vergelijkbare (Citadel-)botnets. Het is primair gericht op het manipuleren van financiële transacties bij internetbankieren.

Dat het botnet gericht is op een bepaald land is niet uitzonderlijk omdat juist het functioneren van de gehele keten voor de fraude afgestemd moet zijn op dat land. Zoals al uitgelegd in paragraaf 4.1 is het bij het richten van campagnes op meerdere landen moeilijker om controle te houden over de hele keten.

Qua omvang is het met 264.339 in de dataset aangetroffen IP-adressen [23]groter dan bijvoorbeeld het Citadel-botnet dat gebruikt werd om Dorifel[24] te verspreiden, waar 188.282 verschillende IP-adressen zijn aangetroffen. Belangrijke kanttekening hierbij is dat het hier de voor het NCSC op dat moment beschikbare informatie betreft en dat de looptijd van campagnes verschilt.

---

[23] Het IP-adres waarmee de computer als laatste verbinding heeft gemaakt

[24] NCSC publiceert factsheet naar aanleiding van Dorifel
https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-factsheet-nav-dorifel.html

5 Verantwoordelijken botnet

Op basis van de aard van het botnet en de door het botnet buitgemaakte gegevens kan aangenomen worden dat het om (beroeps)criminelen gaat die uit zijn op financieel gewin door hoofdzakelijk inloggegevens te ontvreemden en financiële transacties tijdens het internetbankieren te manipuleren.

Op dit moment doet de Politie onder leiding van het Openbaar Ministerie onderzoek naar de verantwoordelijken voor het Pobelka-botnet.

6 Aanvullende response

In de dataset zijn op basis van zoekcriteria, zoals organisatienamen, domeinnamen die gebruikt worden door organisaties en veel gebruikte trefwoorden, organisaties in vitale sectoren en andere slachtoffers geïdentificeerd. De informatie die is verkregen na de oproep[25] aan organisaties in de vitale sectoren om extra informatie beschikbaar te stellen is hier ook bij gebruikt.

Op basis van de resulterende dataset en het onderzoek achten wij het van belang om getroffen organisaties te informeren. Een organisatie kan vervolgens zelf bepalen welke maatregelen getroffen moeten worden. Organisaties zijn zelf namelijk het beste toegerust om een inschatting te maken van de impact van het lekken van de gegevens en of verdere analyse gedaan moet worden.

Bij de aanvullende response zijn een aantal aandachtspunten van belang:

- de data is sterk verouderd, de eerste infecties stammen uit februari 2012, hierdoor is de situatie ten opzichte van het moment dat een computer geïnfecteerd is geraakt, waarschijnlijk sterk veranderd;
- logbestanden, die in sommige gevallen benodigd zijn om geïnfecteerde systemen te vinden, zijn niet meer beschikbaar;
- hoewel het tot op zekere hoogte te bepalen is van wie een geïnfecteerde computers is, kan het NCSC niet bepalen van wie de informatie is die in de dataset zijn verzameld. Eigenaren van de geïnfecteerde systemen moeten ervan uitgaan dat alle data op die computer gecompromitteerd is en ook hetgeen via de webbrowser verstuurd is;
- de computer is mogelijk nog steeds onderdeel van dit, of een ander botnet.

[25] Media-aandacht voor Pobelka-botnet
https://www.ncsc.nl/actueel/nieuwsberichten/media-aandacht-voor-pobelka-botnet.html

7 Conclusies en bevindingen

Dit document is het resultaat van de taskforce Pobelka waarin de Politie, het OM, de AIVD, de MIVD, de NCTV en het NCSC nader onderzoek hebben gedaan naar de dataset die afkomstig is van de verkregen Command en Control (C&C)-server van het Pobelka-botnet. Het NFI heeft op verzoek van het NCSC de analyse van de data uitgevoerd.

De AIVD heeft zich in het onderzoek naar het Pobelka-botnet uitsluitend gericht op de vraag of er sprake is geweest van spionageactiviteiten door statelijke actoren. Om deze vraag te beantwoorden heeft de AIVD IP-adressen en samenhangende technische kenmerken en informatie die de relateren zijn aan overheidsinstellingen en vitale sectoren geanalyseerd. Uit de onderzoeksresultaten is gebleken dat er geen aanwijzingen zijn voor spionageactiviteiten door statelijke actoren.

De focus van de MIVD in het onderzoek naar het Pobelka-botnet is er op gericht vast te stellen of er (digitale) spionageactiviteiten hebben plaatsgevonden gericht op militair relevante aspecten, inbegrepen de Nederlandse defensie-industrie. In dit kader is in de dataset geen gerubriceerd materiaal aangetroffen. Weliswaar is een aantal maal een term als 'NATO SECRET' geconstateerd, echter niet als inhoudelijke kwalificatie van gegevens, maar als gespreksonderwerp binnen sociale media. Ook onderzoek naar andere specifiek Defensie-relevante steekwoorden heeft tot dusver niet tot verontrustende resultaten geleid. Verder heeft de MIVD gezocht naar IP-adressen en e-mailadressen die te relateren zijn aan Defensie. Het aangetroffen IP-verkeer is overwegend te herleiden naar het zogenaamde internet op de legering (IODL)[26]. In relatie tot IP-adressen van de defensie-industrie is ook een aantal hits geconstateerd, maar hierin zijn geen veiligheidsrisico's aangetroffen. In de dataset zijn eveneens e-mailadressen van Defensie aangetroffen. Deze zijn vooral te verklaren doordat contactlijsten, bevattende dergelijke adressen, van getroffen systemen buiten Defensie door het botnet zijn buitgemaakt. Uit deze eerste onderzoeksresultaten komen geen activiteiten naar voren die duiden op digitale spionage op militaire relevante aspecten.

Op dit moment doet de Politie onder leiding van het Openbaar Ministerie onderzoek naar de verantwoordelijken voor het Pobelka-botnet. Omwille van dit lopende onderzoek kunnen er geen nadere mededelingen worden gedaan.

In het onderzoek van het NFI is opgemerkt dat de drie campagnes niet gericht zijn geweest op specifieke overheden, bedrijven of andere organisaties. Als echter op een juiste manier misbruik wordt gemaakt van de buitgemaakte gegevens dan is de schade potentieel groot. Ook bevatten de door het botnet verzamelde gegevens zeer veel gegevens die direct impact hebben op de privacy van personen.

Het NCSC heeft geconstateerd dat het Pobelka-botnet zich primair heeft gericht op de manipulatie van financiële transacties tijdens het internetbankieren op voornamelijk Nederlandse en Duitse computers. Hierbij is er veel bijvangst met gevoelige informatie buitgemaakt. Tijdens de in het onderzoek uitgevoerde

[26] Een *wellfare* voorziening van Defensie aan haar medewerkers om op hun slaapverblijf op defensieterreinen privé gebruik te kunnen maken van internet

steekproef is geen informatie aangetroffen die een acuut risico vormt voor de continuïteit van getroffen organisaties of de nationale veiligheid. Wel is de aard van de informatie dusdanig dat de gegevens een basis kunnen vormen voor geslaagde gerichte aanvallen, die in potentie een grote impact kunnen hebben. In de nadere analyse zijn getroffen organisaties geïdentificeerd naast de al geïnformeerde partijen, het NCSC gaat deze organisaties informeren.

7.1 Bevindingen

Hieronder treft u de belangrijkste bevindingen van de nadere analyse aan:

- Het Pobelka botnet was, net als andere Citadel-botnets, primair gericht op het manipuleren van financiële transacties om geld weg te sluizen.
- Als bijvangst zijn er veel gevoelige gegevens van verschillende aard buitgemaakt, deze gegevens zijn hoofdzakelijk afkomstig uit 'POST'-data (gegevens die via invoervelden in de webbrowsers verstuurd worden).
- IP-adressen van geïnfecteerde computers in het Pobelka-botnet zaten hoofdzakelijk in Nederland (54,5%) en Duitsland (30,7%).
- De campagnes op de verkregen C&C-server van het Pobelka-botnet zijn actief geweest tussen 2 februari 2012 en 19 september 2012.
- Op basis van de door het botnet verzamelde gegevens en de opdrachten die door de beheerder van het botnet zijn afgegeven is er op dit moment geen aanleiding om aan te nemen dat er gericht gezocht is naar bepaalde soorten informatie of bepaalde documenten.
- Op basis van de diversiteit van getroffen systemen en buitgemaakte gegevens is er op dit moment geen reden om aan te nemen dat het botnet gericht was op specifieke overheden, sectoren of organisaties.
- De door het botnet buitgemaakte gegevens vormen geen acuut risico voor de continuïteit van getroffen organisaties of de nationale veiligheid. Wel is de aard van de informatie dusdanig dat de gegevens een basis kunnen vormen voor geslaagde gerichte aanvallen, die in potentie wel een impact kunnen hebben op de continuïteit van de dienstverlening van deze organisaties.
- Er zijn geen aanwijzigen gevonden dat er actieve netwerkverkenning heeft plaatsvonden, wel is bepaalde netwerkinformatie buitgemaakt.
- De door het botnet verzamelde gegevens bevatten zeer veel gegevens die direct impact kunnen hebben op de privacy van personen.
- Op basis van de aard en de buitgemaakte gegevens van het botnet mag aangenomen worden dat het om (beroeps)criminelen gaat.
- De Politie doet op dit moment onder leiding van het Openbaar Ministerie onderzoek naar de verantwoordelijken voor het Pobelka-botnet.
- Uit de onderzoeksresultaten uit de analyse van de AIVD is gebleken dat er geen sprake is van spionageactiviteiten door statelijke actoren.
- Uit de onderzoeksresultaten van de MIVD blijken vooralsnog geen activiteiten die duiden op (digitale) spionage jegens het ministerie van Defensie, de defensie-industrie of ten aanzien van onderwerpen met een militaire relevantie in het algemeen.
- In het onderzoek van het NFI is opgemerkt dat de drie campagnes niet gericht zijn geweest op specifieke overheden, bedrijven of andere organisaties. Wanneer op een juiste manier misbruik wordt gemaakt is de schade echter mogelijk wel groot.
- Op basis van de resulterende dataset en het onderzoek achten wij het van belang om getroffen organisaties te informeren.