Gebruikersdag Vialis

Digitale Veiligheid

18 mei 2017

Robin de Haas

Intro – Who am I

- Commercieel Productmanager
  - Security & Compliance Monitoring
  - Threat Intelligence

- The Hague Security Delta

- TNO Defensie en Veiligheid

https://www.linkedin.com/in/robin-de-haas-3a96078/

Vanmiddag

- Uitgangspunten
- Digitalisering
- Door de ogen van een hacker
- Verschijningsvormen
- Aandachtspunten en tips

Vanmiddag

- **Uitgangspunten**
- Digitalisering
- Door de ogen van een hacker
- Verschijningsvormen
- Aandachtspunten en tips

Uitgangspunten

- Geruikersdag Vialis
- Partner van KPN in Talking Traffic
- Geen IT-publiek
- Security in relatie tot IoT
- Geen beangstigend verhaal (FUD)
- Wat zijn aandachtspunten

En toen....

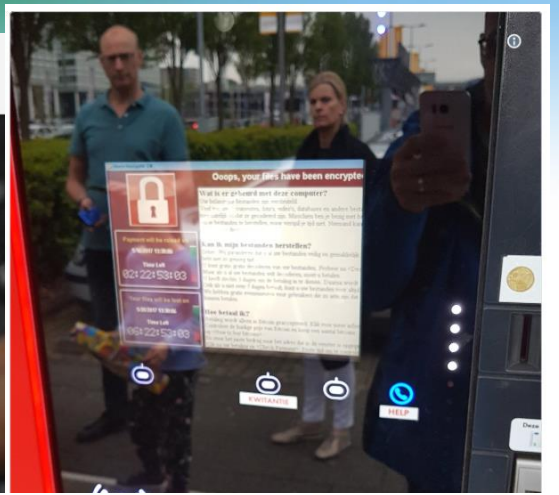
Over de hele wereld zijn meldingen gedaan van grootschalige zogenoemde ransomware-aanvallen zoals vanmiddag in Groot-Brittannië. De Britse premier May zegt dat de aanval op de Britse ziekenhuizen onderdeel is van een nog grotere internationale cyberaanval. Volgens May zijn er waarschijnlijk geen patiëntgegevens buitgemaakt bij de aanval.

NOS Nieuws Sport Uitzendingen

Cyber Security Centrum: gevolgen aanval vallen mee, wel alert blijven

MAANDAG, 09:08 BINNENLAND, TECH

De grootschalige cyberaanval die sinds vrijdagavond in m
computers heeft besmet met zogenoemde ransomware, h
nauwelijks gevolgen gehad. Directeur Zorko van het Natic
Centrum zegt dat het waarschuwingssysteem goed heeft
Nederland er daarom relatief goed vanaf is gekomen.



'Cyberaanvallen binnen twee jaar grootste bedrijfsrisico'

Gepubliceerd: 03 december 2012 13:22
Laatste update: 03 december 2012 13:26

AMSTERDAM - Cyberaanvallen zijn binnen twee jaar een groter risico voor bedrijven dan economische onzekerheid.

Dat blijkt althans uit een onderzoek onder ruim 3300 IT-specialisten door een beveiligingsbedrijf. Het is niet de eerste keer dat de risico's van cyberaanvallen voor bedrijven onder de aandacht worden gebracht.

Bijna de helft (48 procent) geeft aan dat de beveiliging tegen online diefstal van intellectueel eigendom in hun bedrijf te wensen over laat. Bovendien geeft 51 procent toe machteloos te zijn tegen serieuze pogingen van cyberspionage.

Mede daardoor geeft een derde van de IT-specialisten aan dat hij verwacht dat zijn onderneming vroeg of laat slachtoffer wordt van cyberaanvallen.

Opvallend is dat ook een derde van de ondervraagden niet op de hoogte is van de laatste trojaanse paarden en niet weet hoe gerichte aanvallen precies worden uitgevoerd.

'Veel bedrijven hebben geen enkel plan bij cyberaanval'

MAANDAG, 18:00 | BINNENLAND, BUITENLAND,

Nederlandse bedrijven worden op grote schaal getroffen door datalekken. Ruim vier op de tien ondernemingen had er de afgelopen twee jaar één of meerdere malen mee te maken.

Het aantal getroffen bedrijven ligt mogelijk nog vele malen hoger, want bijna tien procent van de ondernemingen heeft geen idee of er in de laatste twee jaar überhaupt een datalek was. Dat blijkt uit onderzoek van IT-beveiliger ESET

Vanmiddag

- Uitgangspunten
- **Digitalisering**
- Door de ogen van een hacker
- Verschijningsvormen
- Aandachtspunten en tips

Digitalisering

Toenemende data hoeveelheden

Van innovatie naar verandering

98,000+ tweets

695,000 status updates

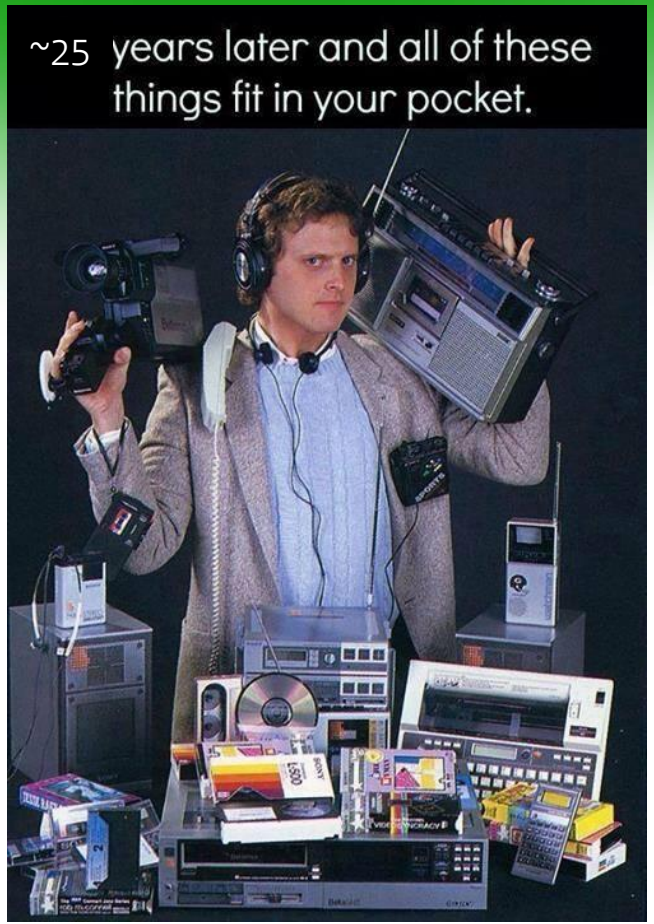
11million instant messages

698,445 Google searches

168 million+ emails sent

1,820TB of data created

217 new mobile web users



Nieuwe economische concepten

- Smart living
- Smart Homes
- Smart Cities
- Smart Grids
- Smart Logistics
- Connected driving
- .....

Internet users per 100 users	93.1
Fixed broadband subscriptions per 100 users	41.7
Mobile cellular subscriptions per 100 users	124

In 2015, it was estimated that the Dutch broader digital economy accounted for 22.9 percent or €158.01 billion (~$172.2 billion) of the total Dutch economy, and it is projected to reach 25 percent or €190.4 billion (~$207.5 billion) by 2020.[6]

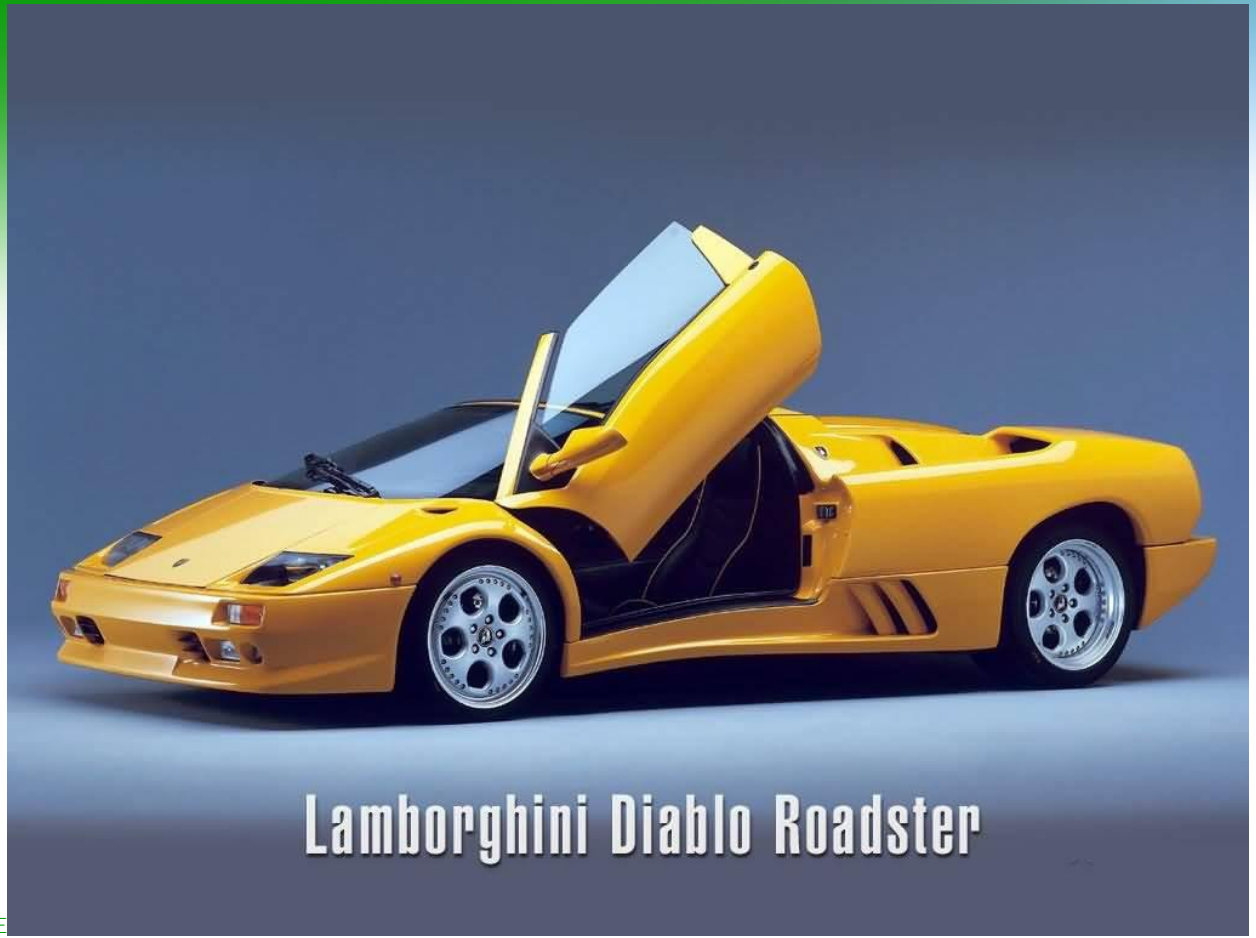
Bron:

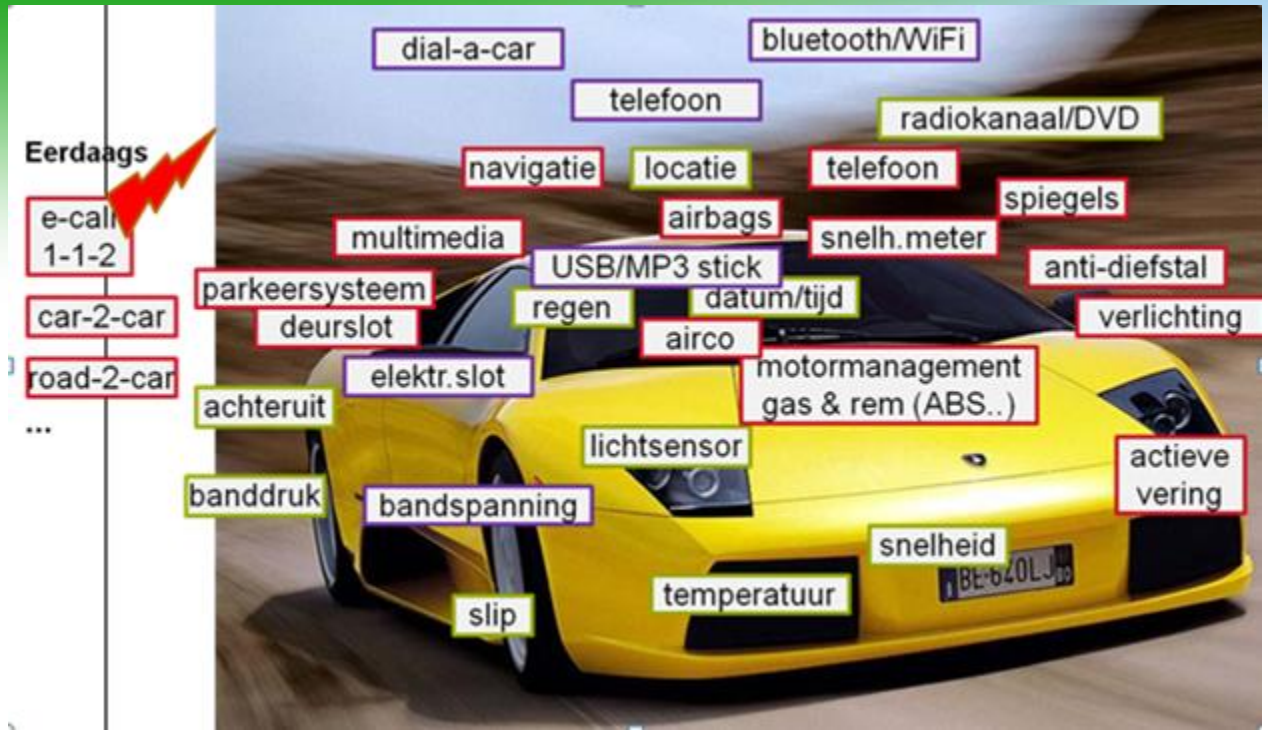
Vanmiddag

- Uitgangspunten
- Digitalisering
- **Door de ogen van een hacker**
- Verschijningsvormen
- Aandachtspunten en tips

Waarom doen hackers wat hackers doen… ?

Good & Bad…


Lamborghini Diablo Roadster




nest
1 HOUR
70


nest

Wie zijn hackers?

- Journalisten
- Statelijke actoren
- Hacktivisten / white-hat hackers
- Scriptkiddies
- Concurrenten
- Criminelen
- Onderzoekers/ethical hackers

Maar dreigingen kunnen ook komen van.....

- Ontevreden medewerkers
- Fraudeleuze medewerkers
- Supertargets
- Ingehuurd personeel
- Leveranciers
- Business partners

Enkele feiten…

- Digitale economische spionage zet NL concurrentiepositie onder druk;
- Ransomware is gemeengoed en is nog geavanceerder geworden;
- Beroepscriminelen voeren langdurige, hoogwaardige en geavanceerde operaties uit.

Tabel 1 **Dreigingsmatrix**

	Doelwitten		
Bron van Dreiging	**Overheden**	**Private organisaties**	**Burgers**
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT	Overname van ICT
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal van informatie	Diefstal van informatie	Diefstal van informatie ↘
	Verstoring van ICT ↗	Verstoring van ICT ↗	
Hacktivisten	Diefstal en publicatie van verkregen informatie ↗	Diefstal en publicatie van verkregen informatie ↗	
	Defacement	Defacement	
	Verstoring van ICT	Verstoring van ICT	
	Overname van ICT	Overname van ICT	
Interne actoren	Diefstal en publicatie of verkoop van verkregen informatie ↘	Diefstal en publicatie of verkoop van verkregen informatie ↘	
	Verstoring van ICT	Verstoring van ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal van informatie (bedrijfs-spionage)	Commercieel gebruik, misbruik of 'doorverkopen' van gegevens

kpn

De Cybersecurity kill-chain

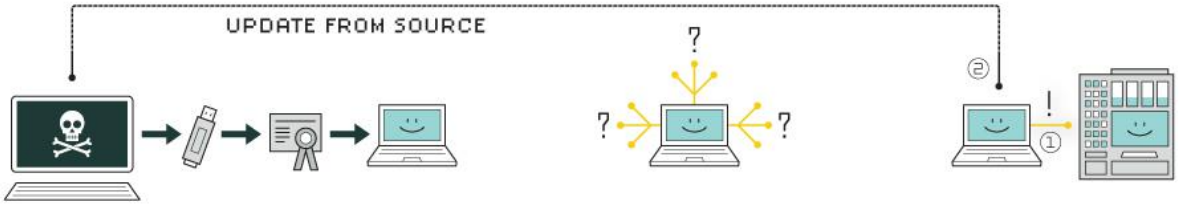
Vanmiddag

- Uitgangspunten
- Digitalisering
- Door de ogen van een hacker
- **Verschijningsvormen**
- Aandachtspunten en tips

IT?

- IT
- OT – ICS – SCADA
- IoT

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Mysterieuze malware voedt vrees voor nieuwe Stuxnet

Industriële systemen nog steeds makkelijk en onontdekt aan te vallen.

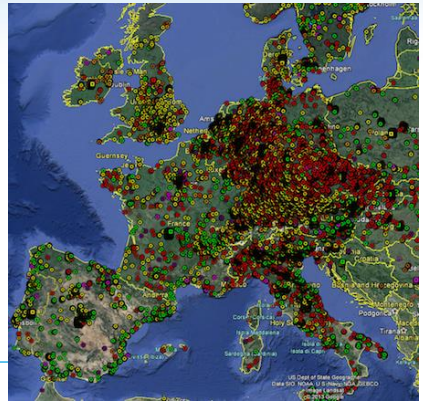
Onderzoekers hebben een malwareprogramma gevonden die ontworpen is om SCADA-systemen te manipuleren, onder meer door de echte data van dat systeem verborgen te houden voor industriële processen.

Lucian Constantin

NIEUWS 3 juni 2016

Technology in diepte…

MIVD: Nederland wekelijks doelwit cyberspionage

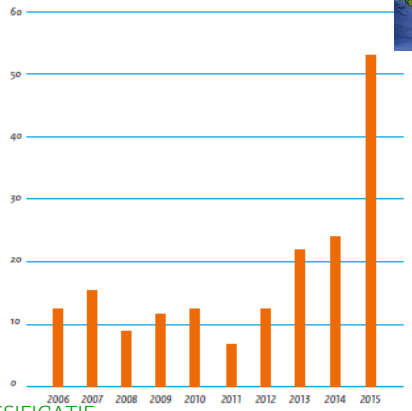


Enkele feiten industriële technologie (Kaspersky):

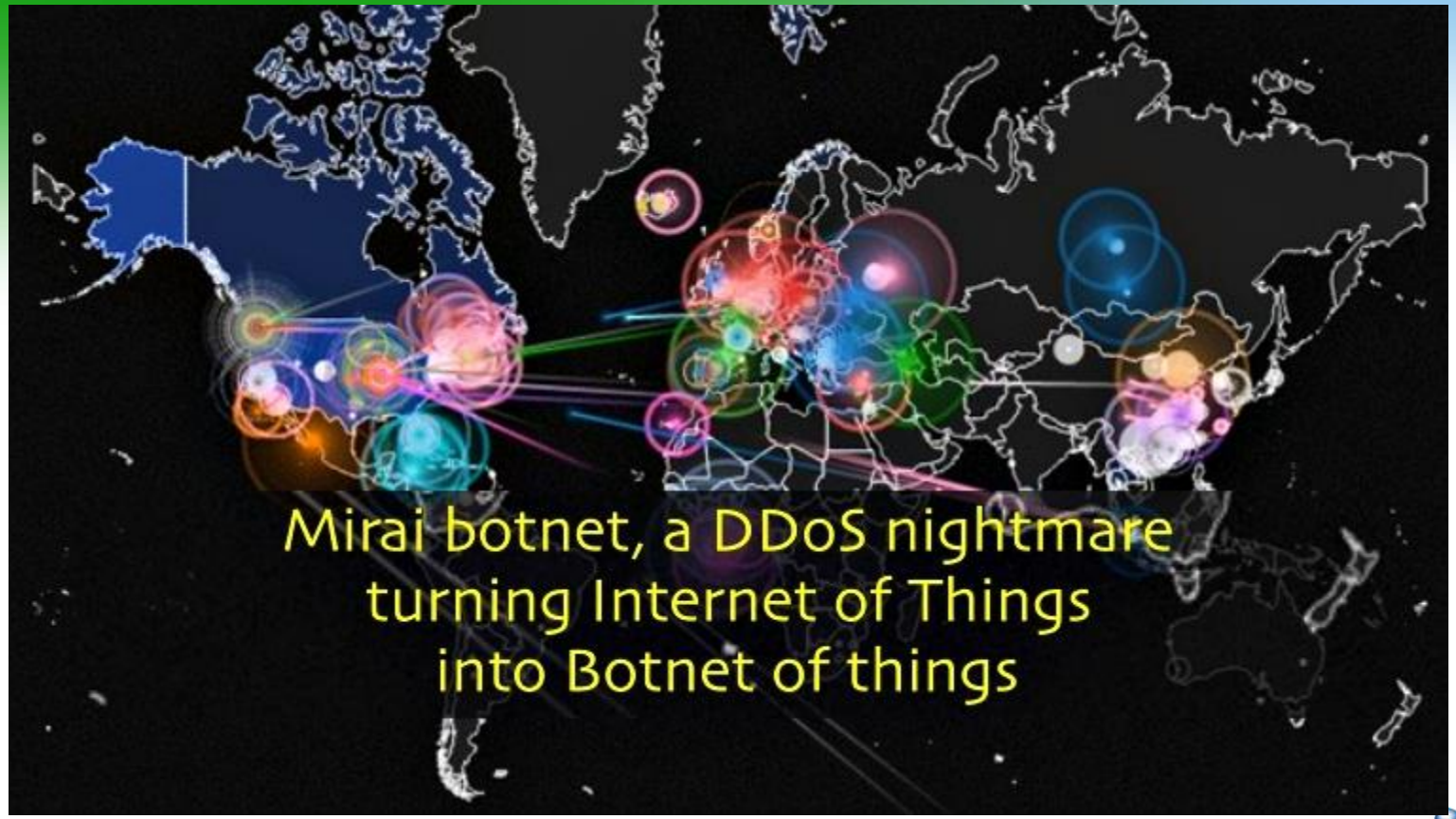
- 188.019 hosts met ICS componenten verbonden met Internet in 170 landen
- Nederland: >3500 kwetsbare hosts
- 92% heeft kwetsbaarheden
  - 230 met kritische kwetsbaarheden

- Reguliere technologie
  - Toename 0-day exploits

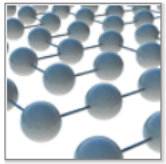
Figuur 6 **Totaal aantal bekend geworden zero-dayexploits per jaar**



Bron: Symantec.


Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

Nieuws



Mirai-botnet verspreidt zich via lek in thuisrouters

dinsdag 29 november 2016, 09:50 door **Redactie**, 3 **reacties**

De recente aanvallen op routers van internetgebruikers waardoor 900.000 klanten van Deutsche Telekom met storingen te maken kregen zijn het werk van een Mirai-botnet, zo meldt beveiligingsbedrijf **Kaspersky Lab**. De eerste versies van Mirai gebruikten nog standaard wachtwoorden die niet door de eigenaar waren veranderd om voornamelijk digitale videorecorders en ip-camera's aan te vallen.

Dit weekend werd er een nieuwe Mirai-variant waargenomen die zich op een andere manier verspreidde, aldus beveiligingsbedrijf **Fox-IT**. De variant maakt namelijk gebruik van een beveiligingslek in verschillende routers voor consumenten. Het gaat onder andere om de D1000-router van de Ierse internetprovider Eir. De kwetsbaarheid werd begin deze maand openbaar gemaakt. De aanval van de malware richt zich op een protocol dat providers gebruiken om de modems/routers van hun klanten op afstand te configureren.

In het geval de aanval succesvol is zal de Mirai-malware zich van het bestandssysteem verwijderen zodat die alleen in het geheugen aanwezig is. Vervolgens dicht de malware poort 7547 waardoor het binnenkwam. Hierna wordt de router gebruikt voor het scannen en aanvallen van andere kwetsbare routers. Aangezien de malware zich niet naar het permanente bestandssysteem van de router kan schrijven, zal het een herstart van het apparaat niet overleven. Fox-IT houdt nog in het midden of de nieuwe Mirai-versie voor de aanval op Deutsche Telekom verantwoordelijk is, maar volgens Kaspersky Lab is dit wel het geval.

Internetproviders krijgen het advies hun routers/modems zo in te stellen dat alleen verbindingen vanaf hun eigen managementinterface worden geaccepteerd en niet de hele wereld. Verder zouden gebruikers indien mogelijk de apparaten door een eigen router kunnen vervangen. Daarnaast kunnen gebruikers hun provider of leverancier benaderen met de vraag of er patches voor de problemen beschikbaar zijn.

▲ Deutsche Telekom rolt updates uit voor aangevallen routers
▼ Mozilla dicht ernstig beveiligingslek in Firefox 50

kpn


WWW
Brickerbot attacks
permanently destroying
IoT
TOLAM
.ORG
ces!

BrickerBot-malware maakt iot-apparaten vrijwel onbruikbaar

Door Sander van Voorst, vrijdag 7 april 2017 17:35, 102 reacties • Feedback

Beveiligingsbedrijf Radware heeft een nieuwe malwarevariant ontdekt, die het de naam BrickerBot heeft gegeven. De kwaadaardige software infecteert internet-of-things-apparaten en zorgt ervoor dat deze vrijwel niet meer zijn te gebruiken.

Daarbij gaat het om zogenaamde pdos-aanvallen, wat staat voor 'permanent denial of service', aldus het bedrijf. Deze vorm van aanvallen staat ook wel bekend als *phlashing*. In het geval van BrickerBot voert de malware bijvoorbeeld verschillende fdisk-commando's uit die leiden tot een beschadigd bestandssysteem door willekeurige bits te schrijven, waarna de internetverbinding wordt verbroken en het aantal *kernel threads* naar 1 omlaag wordt geschroefd. Hierdoor wordt het geïnfecteerde systeem traag en is nauwelijks nog te gebruiken.

BrickerBot wordt op dezelfde manier als de Mirai-malware verspreid, namelijk door met *brute force* telnet-toegang te verkrijgen. Volgens Radware zijn er twee botnets actief die de malware verspreiden. Het eerste, genaamd BrickerBot1, vertoonde gedurende een korte periode veel activiteit. Het tweede botnet vertoonde minder activiteit en maakte gebruik van verkeer dat afkomstig was van Tor-exitnodes. Gedurende een periode van vier dagen registreerden de *honeypots* van Radware in totaal 1895 pdos-pogingen door BrickerBot1 van enkele ip-adressen over de hele wereld.

4/21/2017

BrickerBot PDoS Attack: Back With A Vengeance

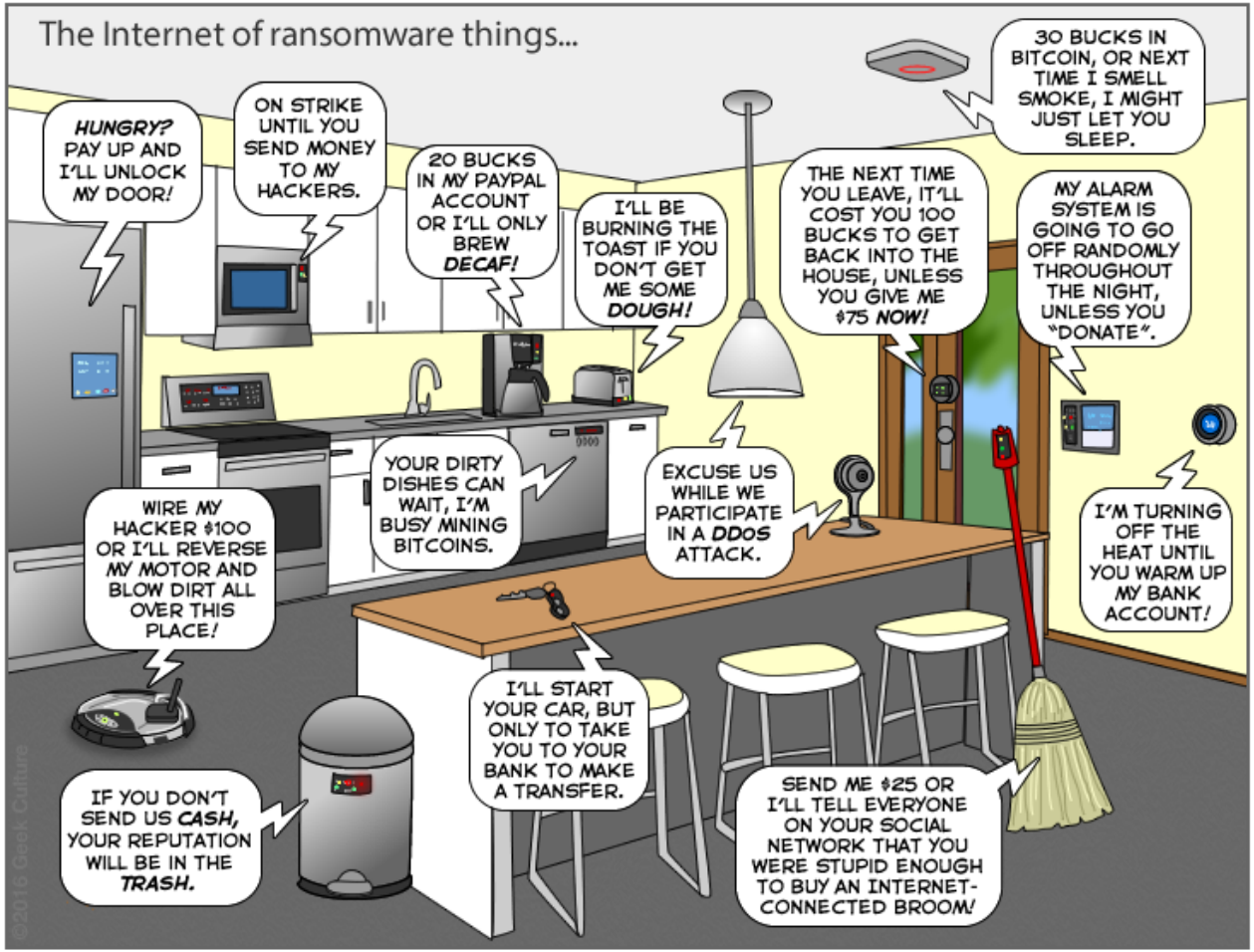
Abstract

Imagine a fast moving bot attack designed to render the victim's hardware from functioning. Called Permanent Denial-of-Service Attack (**PDoS Attack**), this form of cyber-attack is becoming increasingly popular in 2017 as more incidents involving this hardware-damaging assault occur.

In early April, Radware's Emergency Response Team identified a new botnet designed to comprise IoT devices and corrupt their storage. Over a four-day period, Radware's honeypot recorded 1,895 PDoS attack attempts performed from several locations around the world. Its sole purpose was to compromise IoT devices and corrupt their storage.

Besides this intense, short-lived bot (BrickerBot.1), Radware's honeypot recorded attempts from a second, very similar bot (BrickerBot.2) which started PDoS attack attempts on the same date – both bots were discovered less than one hour apart –with lower intensity but more thorough and its location(s) concealed by TOR egress nodes.

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

kpn

Onderwerp: Uw factuur Internetdiensten
Datum: Fri, 16 Sep 2015 12:13:58 +0200 (CEST)
Van: Paul — pfwin@yahoo.com
Aan: pfwin@yahoo.com <pfwin@yahoo.com>

Phishing mail??

kpn

Geachte heer,

In de bijlage ontvangt u de factuur van uw KPN Internetdiensten.

Bedrag en specificaties
Deze maand is uw factuur in totaal 518,41. De specificaties van de factuur vindt u in de bijlage.

Overzicht van al uw facturen in MijnKPN
Wilt u een overzicht van al uw facturen of uw persoonlijke instellingen bekijken? Klik dan hier om naar MijnKPN te gaan. Dit is uw persoonlijke en beveiligde KPN omgeving.

http://kpncom.bbvms.com/p/faq/c/2175880.html

Uitleg van uw factuur
Klik hier voor uitleg over uw factuur.

http://kpncom.bbvms.com/p/faq/c/2175880.html

http://www.kpn.com/factuur

Veelgestelde vragen
Hebt u nog vragen over uw factuur en de betaling ervan, kijk dan op kpn.com/factuur.
Hier vindt u informatie over veelgestelde vragen zoals: de opbouw van de factuur, de betalingsmogelijkheden, de factuur online bekijken en hoe u wijzigingen doorgeeft.
Met vriendelijke groet,

Bob Mols
Directeur Klantenservice
N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

Kent u KPN Compleet al? Hoe meer u combineert, hoe meer voordelen u krijgt. Kijk voor meer informatie op kpn.com/krijgmeer

De KPN Compleet voordelen zijn:

http://www.kpn.com/prive/krijg-meer/kpn-compleet.htm

KvK Den Haag nr. 2358701, NL009292056B01

Vanmiddag

- Uitgangspunten
- Digitalisering
- Door de ogen van een hacker
- Verschijningsvormen
- **Aandachtspunten en tips**

Meldplicht Datalekken

- Ingevoerd op en geldig vanaf 1 januari 2016
- Verplicht om ernstige datalekken te melden bij de Autoriteit Persoonsgegevens

AUTORITEIT
PERSOONSGEGEVENS

- Wordt dit niet gemeld of blijken beveiligingsmaatregelen niet passend genoeg?
  - Kans op een bestuurlijke boete tot € 820.000,-
  - Of tot 10% (wereldwijde) jaaromzet
- Hoofdelijke aansprakelijkheid van bestuurders

KPN SECURITY SERVICES

- KPN beveiligingsbeleid onder de loep genomen en flink aangescherpt
- De CISO office en het Security Operations Center zijn opgericht

- Veel ervaring met complexe infrastructuur en netwerken
- Continue aandacht voor verbetering door ontwikkelingen en dreigingen van buitenaf

360 graden security

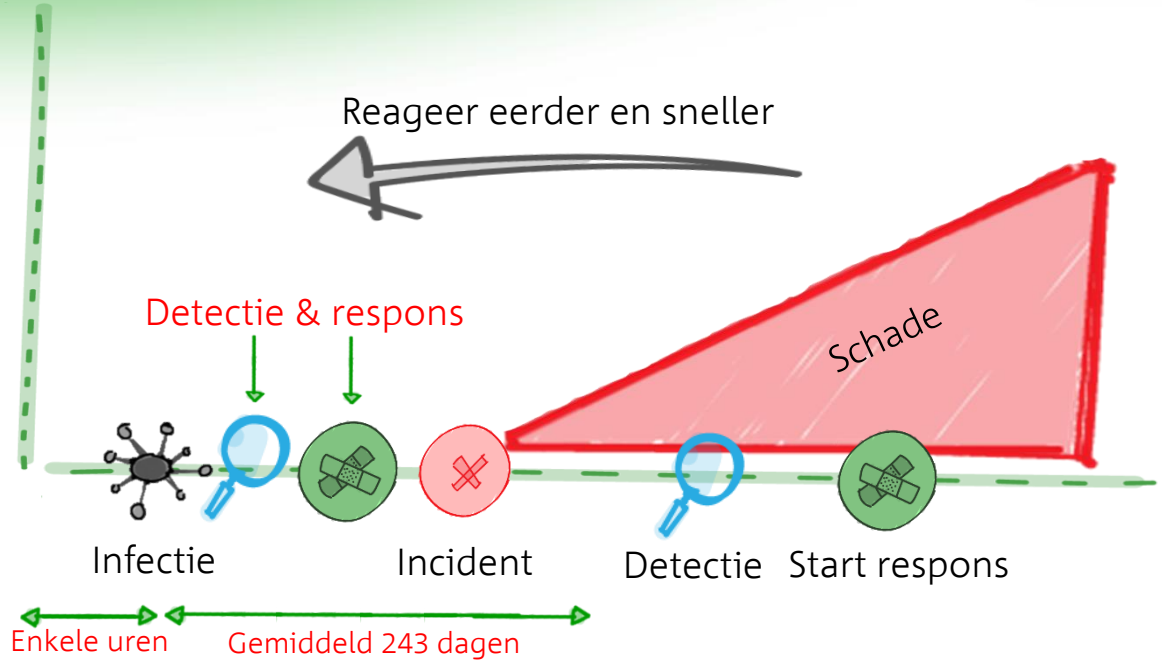
REDteam en SOC

CERT

Strategie en beleid

Senior Security Officers

Onderneem actie en voorkom schade



Vier strategische pilaren

Identity en Privacy

Secure communications

Cybersecurity

Business continuity

Kennis delen

http://corporate.kpn.com/kpn-actueel/nieuwsberichten-1/uitdagingen-en-bedreigingen-waren-nooit-groter-dan-vandaag.htm

Stel deze vraag: Bent u in control?

Wie heeft toegang tot het ICT of OT netwerk? Weet jij wie je gebruikers zijn en wat ze doen?

Hoe kwetsbaar ben je voor uitval, bedoeld of onbedoeld? Hoe snel ben je weer in business?

Kun jij kwaadwillende op jouw netwerk detecteren en identificeren? Weet jij wat er gebeurt op het netwerk?

De enige manier om effectief de organisatie te beschermen is door de security maturity lifecycle te implementeren. Sluit kwaadwillenden buiten en bescherm je business

Eerste stappen

- Awareness
- Breng in kaart wat je hebt
- Wat zijn de kroonjuwelen/kritieke processen
- Wat zijn dreigingen
- Wat zijn risico’s
- Etc

- Altijd: updates en patches!
  Voorkom kwetsbaarheden

Security by Design

Direct vanaf de start

If you can’t afford to **protect** it

then

You can’t afford to **connect** it

If all fails.....


WE LOST ALL OF OUR COMPANY DATA AND OUR BACKUPS, TOO.
SO I HACKED INTO OUR GOVERNMENT'S SECRET DATABASE WHERE THEY KEEP RECORDS OF EVERY-THING WE SAY OR DO AND GOT IT ALL BACK.
I FEEL AS IF I SHOULD BE DOING SOMETHING NOW.
NAH. EVERY-THING IS WORKING FINE.
Dilbert.com DilbertCartoonist@gmail.com
©2013 Scott Adams, Inc./Dist. by Universal Uclick
9-6-13


kpn
kpn
Dank voor uw aandacht