CISCO
SECURE

The bridge to possible

Digitale weerbaarheid cruciaal een cyberaanval iedereen kan overkomen.

SLF 2022

Jan Heijdra
Security Specialist – Cisco Nederland

jheijdra@cisco.com

First thing that comes to mind when you think about Cybersecurity related to Service Logistics?

Agenda

- Digitale risico’s
  Current Threat landscape
- Organization shift towards Resilience
- Supply Chain Security
- Q & A

Disruption is happening faster than ever.

Fueling massive investments in resilience

Financial Resilience

Operations Resilience

Supply Chain Resilience

Organizational Resilience

These investments will fall short without security resilience

NCTV Cybersecuritybeeld 2021

organisaties beperkt mogelijk is. Zo is er vaak geen zicht op de mate van weerbaarheid van verschillende onderdelen van ICT-leverancierssketens. Daardoor kunnen aanvullende risico's ontstaan die niet goed in beeld zijn, bijvoorbeeld bij de inkoop en aanbesteding van producten en diensten van een leverancier waarbij sprake is van een kwetsbaarheid in een product, of waarbij een (ingehuurde) medewerker toegang heeft tot digitale processen met gevoelige informatie. Schending van de veiligheid van de

organisaties. Keteneffecten kunnen hele sectoren of zelfs de gehele maatschappij raken. Zo maakt een aanval met ransomware op een gemeente, universiteit, ziekenhuis of elektriciteitsdistributeur systemen onbruikbaar: de techniek werkt niet meer. Het gevolg daarvan is dat de gemeente haar taken niet meer naar behoren kan uitvoeren, dat onderzoek en onderwijs stil komen te liggen,

Daarnaast kunnen kwetsbare MKB deel uitmaken van de leverancierssketens van vitale processen. Tegelijkertijd neemt de afhankelijkheid van ICT-dienstverleners in het MKB toe, terwijl zij

afstand te werken doelwit geweest van aanvallen. Ook zijn processen met een digitale component ontoegankelijk gemaakt en zijn organisaties in leverancierssketens aangevallen. Er zijn veel

REUTERS

Germany issues fresh warning to banks of cyber attacks due to Ukraine war

Tue, May 31, 2022, 4:43 PM · 1 min read

NOS NIEUWS · REGIONAAL NIEUWS · VANDAAG, 19:00

Online netwerk dat malware voor mobiele telefoons verspreidde uit de lucht gehaald

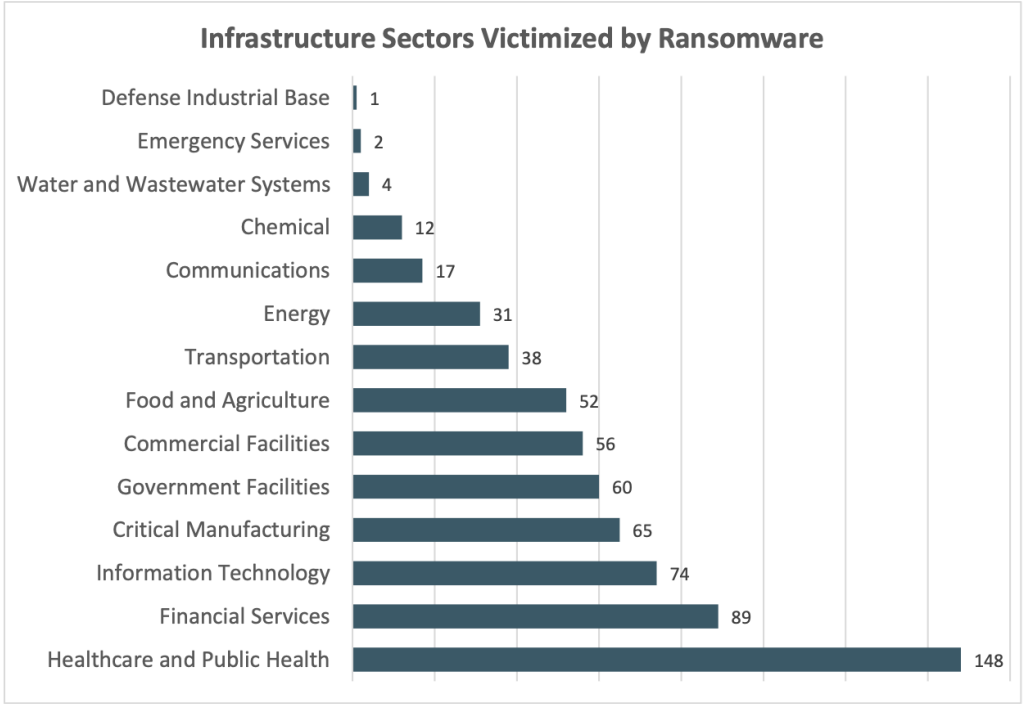
De politie Oost-Nederland heeft in samenwerking met tien landen en Europol een online netwerk dat malware verspreidt platgelegd. Volgens de politie zijn daardoor zo'n tienduizend slachtoffers losgekoppeld en ruim 6,5 miljoen spam-sms'jes per week voorkomen.

Het gaat om de malware-app FluBot. Mensen installeren de app omdat ze denken via een link in een sms naar een site te gaan waar ze een besteld pakketje kunnen volgen, maar in werkelijkheid installeren ze daar de malafide app.

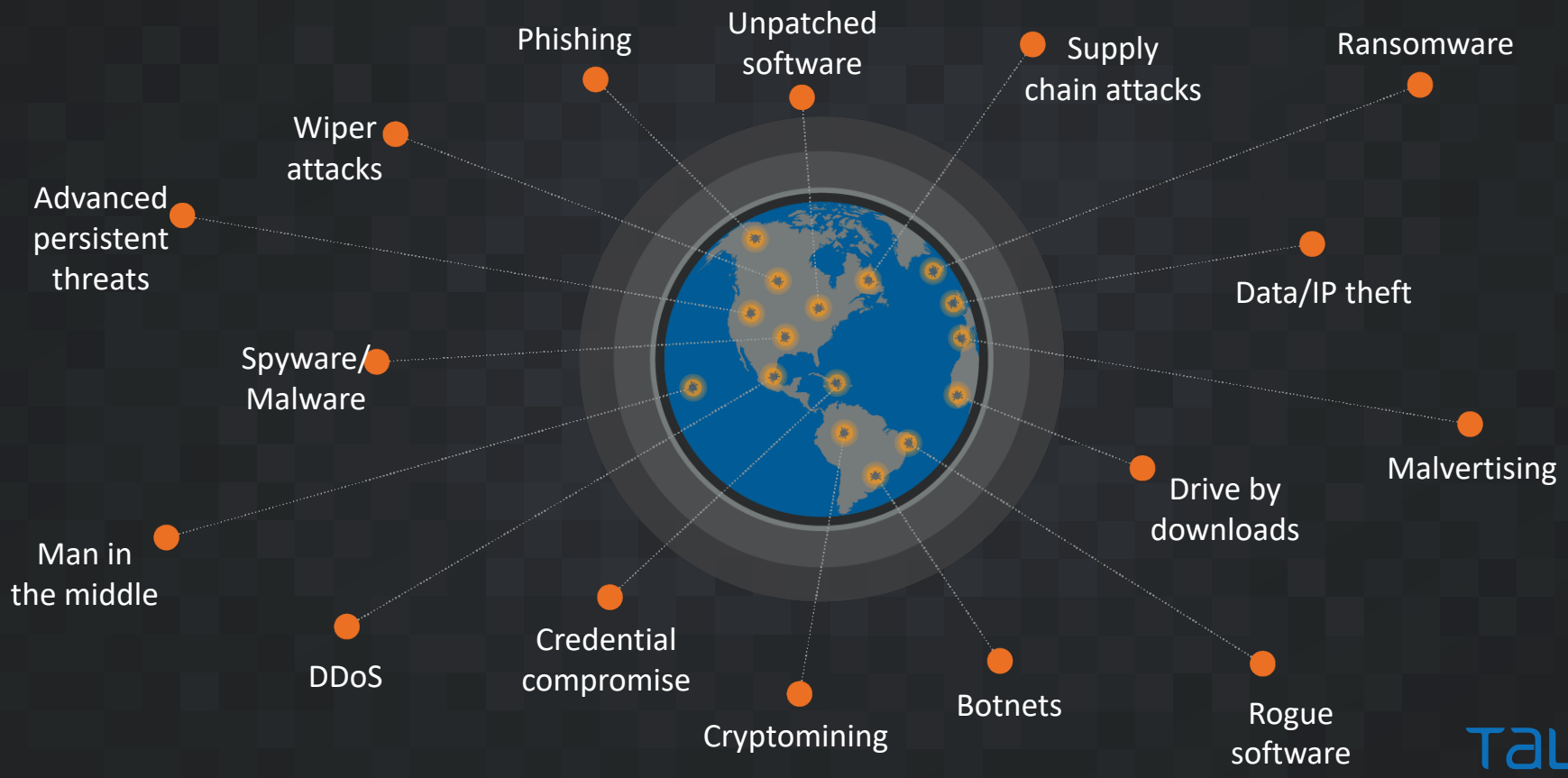
Die software kan sms'jes versturen zonder dat de gebruiker het weet en kan persoonsgegevens stelen en zelfs meekijken in bankapps. De malware werkte alleen op smartphones met Android. Vorig jaar verspreidde de kwaadaardige

FBI Cybercrime report 2021

The IC3 received 649 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021.
13



Threat Landscape



Cyber Crime

- Phishing
- Spam
- social engineering

Two Primary Actors

Nation State

- Supply chain attacks,
- partner abuse,
- etc.

Goals and methodologies are different, have to protect against both

It Starts with a Typewriter??

GUNMAN Project

- Recently Declassified
- During Height of Cold War
- First well known Supply Chain Interdiction Attack
  - Packages Intercepted by Russian Customs
    - Typewriters modified to transmit typing
    - Hollowed out solid bar
    - Wireless near-range communication
    - Only found via X-Ray of equipment

Supply chain attack examples

Target Hackers Broke in Via HVAC Company

February 5, 2014 268 Comments

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Application Security | 4 MIN READ | ARTICLE

MITRE Creates Framework for Supply Chain Security

System of Trust includes data-driven metrics for evaluating the integrity of software, services, and suppliers.

Kelly Jackson Higgins
Editor-in-Chief, Dark Reading

May 18, 2022

Basismaatregelen

Zorg dat elk systeem en elke applicatie voldoende loginformatie genereert

Pas multifactor authenticatie nodig waar nodig

Bepaal wie toegang (nodig) heeft tot uw data en diensten

Segmenteer netwerken

Versleutel opslagmedia met gevoelige bedrijfsinformatie

Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

Maak regelmatig back ups van uw systemen en test deze

Installeer software updates

Cisco Security and Trust

Defend Enterprise Business Operations

- Drive pervasive security
- Defend our global network
- Data protection and privacy
- Security awareness and education
- Report on risk and controls

Secure Our Offers

- Trustworthy technologies
- Cisco Secure Development Lifecycle
- Certifications
- Supply chain security
- Privacy by design

Industry Engagement

- Engage with key customers
- Contribute to Industry bodies and standards
- Share intelligence and leading practices
- Drive trustworthy practices & services

Questions to ask yourself

- What are you going to do when you (or a supply chain company) are breached?
  - Do you have a playbook available?
  - Do you stress test your digital envrionment?
- Which partners are you collaborating with?
  - Which requirements do you have for their level of security maturity?
  - What access do they need to your digital resources to do their job?
- Who has access to your data, when and from which location?
- Do you train your employees to be security aware?

Our Portfolio

SecureX
Platform

User

Secure Access by Duo
Multi-factor authentication

Secure Email
Email security

Device

Secure Client
Single client for access, trust, DNS, threat, query

Secure Endpoint
Endpoint Detection and Response

Secure Malware Analytics
Sandbox

AnyConnect VPN
VPN

Meraki Systems Manager
Mobile device management

Kenna
Vulnerability management

Network

Meraki MX
Campus NGFW

Secure Firewall
Enterprise

Secure Network Analytics
Network detection and response

Web Appliance
Secure web gateway

Identity Services Engine
Network access control

Cyber Vision
Industrial control security

Umbrella
Secure internet gateway/SASE

Cloudlock
Cloud application security broker

Secure Cloud Analytics
Cloud network detection and response

Apps & Data

Secure Workload
Workload protection/micro-segmentation

Secure Application
Application security

ThousandEyes
Network and application monitoring

Services

Talos Incident Response services
Incident response, threat hunting,
penetration testing, emergency response

Managed Detection and Response
Extended detection and response as a service

Advanced Services
Design, Deployment, Optimization

SECURE

Talos — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

- Duo Secure Access
- Secure E-mail

SASE/REMOTE WORKER

Unified Client| EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Observability)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall*
- ThousandEyes

On-Premises

SASE/SDWAN

Scalable| Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall*
- ThousandEyes

IoT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall*
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

*Converged multi-cloud policy

Application Security

ZERO TRUST WORKLOAD

Policy | Application Segmentation
Run-time Application Security | API Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload*
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud*
- Secure Cloud Analytics
- Secure Firewall*
- ThousandEyes