IT INCIDENTEN 2021

Michel Zandbergen

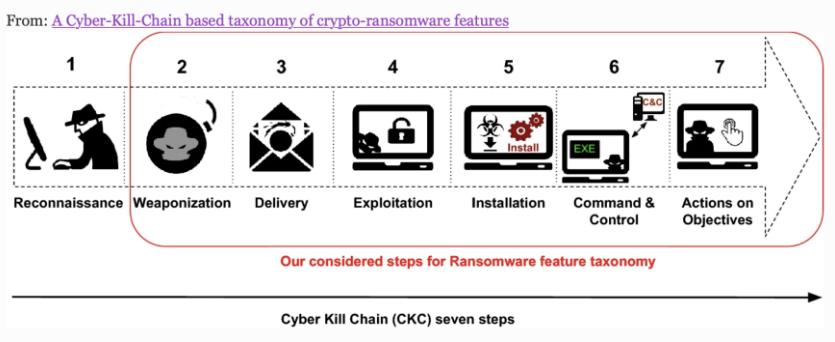
Mentimeter vraag:

- **Wat is het grootste / spraakmakendste IT security incident van 2021?**

IT SECURITY INCIDENTEN IN 2021

Ransomware Nederland	Ransomware Internationaal:	Supply chain attacks	Vulnerabilities	Datalekken
• Gelderse scholen gemeenschap, • NWO, • UVA, • Bakker Logistiek, • Mandemakers, • ROC Mondriaan, • RTL Nederland, • Zorggroep Charim, • Ijmond Werkt, • 130 Nederlandse boekhandels, • VDL Group / VDL Nedcar, • Mediamarkt, • etc. etc.	➢ **Colonial Pipeline** • JBS • Acer, • HealthService Executive Ireland, • etc.	• Solarwinds ➢ **Kaseya** • Codecov	➢ **Microsoft Exchange** ➢ **Log4j**	• Brazilian database - 223 miljoen, • Bykea Pakistan - 400 miljoen, • Facebook - 553 miljoen, • Linkedin - 700 miljoen, • Cognyte, cybersecurity analytics firm - 5 miljard records. (bron: Security magazine 9-12-2021) <u>Nederland:</u> • Alle kabels 3,6 miljoen

RANSOMWARE



Acer
Revil Ransomware
Microsoft exchange vulnerability
50 miljoen dollar losgeld gevraagd

Gemeente Hof van Twente
Wachtwoord "Welkom2020"

RTL Nederland
Inloggegevens externe beheerpartij
RTL betaald losgeld

UVA
Besmette laptop student

NWO
Malafide e-mail

Ierse gezondheidszorg
HSE - Ireland
Malafide e-mailbijlage
Directeur laat weten dat aanval de ierse gezondheidszorg al 100 miljoen euro heeft gekost

Dairy farm
Revil Ransomware
30 miljoen dollar losgeld gevraagd

JBS
Fabrieken gesloten
Betaald 11 miljoen dollar losgeld

Colonial pipeline Company
Legacy VPN met wachtwoord
Pijpelijn tijdelijk afgesloten
Betaald 4,4 miljoen dollar losgeld

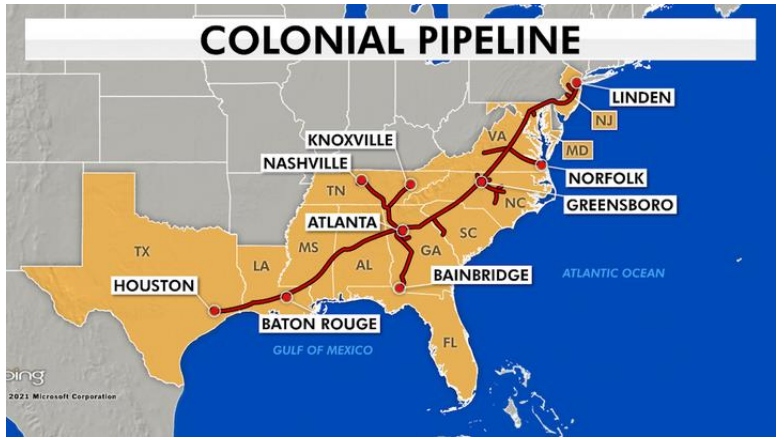
FBI
Werkwijze ransomware: meestal door misbruik remote desktop Protocol (RDP) Via:
- Brute force-aanvallen,
- misbruik inloggegevens,
- Phishingmails en
- Misbruik bekende (niet gepatchte) kwetsbaarheden.

Handleiding Conti-ransomware
- Translated by CISCO Talos
- Comprehensive documentation
- Several ways to Hunt for administrator access
- Tools listed Cobalt strike, OSINT, windows utilities, use of Adfind and whoami to gain info, etc
- Instructions on CVE-2020-1472 zerologon exploitation
- Isight in approach may help in prevention

Bron: blog talosintelligence.com 2-9-2021

COLONNIAL PIPELINE

Largest cyberattack on an oil infrastructure target in the history of the United States



Explanation

- The company's system transports roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard. 45% of fuel along East Coast, 50 million Americans depend on the fuel.
- Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network
- The VPN account, which has since been deactivated, didn't use multifactor authentication. The account's password has since been discovered inside a batch of leaked passwords on the dark web.
- Colonial paid the hackers, who were an affiliate of a Russia-linked cybercrime group known as DarkSide, a $4.4 million ransom shortly after the hack.
- FBI, Homeland, CISA, TSA, etc all involved. Part of ransomware recovered by FBI

Impact

- Pipeline shut down as a precaution as they did not know extend of infiltration into pipeline operating systems.
- Fuel shortages began to occur at filling stations amid panic buying.
  - 71% of filling stations running out of fuel in Charlotte on May 11 and
  - 87 percent of stations out in Washington, D.C. on May 14.
  - Average fuel prices rose to their highest since 2014, reaching more than $3 a gallon.
- President Joe Biden declared a state of emergency on May 9.

Lessons Learned

- MFA (Multi Factor Authentication) voor admin accounts
- Crisis oefeningen

KASEYA

Explanation

- Managed Serviceproviders gebruiken KASEYA VSA software om systemen van klanten te beheren.
- Dutch Institute for Vulnerability Disclosure had een deel van de vulnerabilities ontdekt en gemeld, Kaseya was bezig patches te maken.
- De aanvallers wisten de (zeroday) vulnerabilities uit te buiten in de VSA-software om zo de authenticatie te omzeilen en commando's uit te voeren. Zo konden ze ransomware op endpoints zetten.
- REvil is de naam van de ransomwaregroepering die de aanval opeist. REvil sloeg toe onafhankelijkheids-weekend op het moment dat Security Operation Centers dunbezet waren.
- REvil biedt zijn gijzelsoftware aan als ransomware-as-a-service. Criminelen kunnen de malware, inclusief de achterliggende command-and-controlservers, huren in ruil voor een deel van de opbrengst.
- Kaseya heeft niet betaald. Een security firma heeft de decryptie code achterhaald met hulp FBI.

Kaseya › Other › Informational

Important Notice July 2nd, 2021

We are experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers only as of 2:00 PM EDT today.

We are in the process of investigating the root cause of the incident with an abundance of caution but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us.

Impact

- Victims in 17 countries, including the U.K., South Africa, Canada, New Zealand, Kenya and Indonesia.
  60 service providers en circa 1500 klanten aangevallen.
- Supermarktketen Coop, heeft in Zweden honderden supermarkten moeten sluiten. Dat kwam omdat de betaalprovider voor de kassa's en zelfscankassa's was getroffen.
- Het Dutch Institute for Vulnerability Disclosure heeft samengewerkt met 'partners' en met de Nederlandse autoriteiten en het NCSC om het aantal geïnfecteerde servers 'terug te brengen naar nul'.

Lessons Learned

- Toegang MSP veilig inrichten (bv via VPN)
- Verify security MSP's

MICROSOFT EXCHANGE

Explanation

- Set of zero day vulnerabilities known as Proxylogon
- ProxyLogon consists of four flaws (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) that can be chained together to create a pre-authentication remote code execution (RCE) exploit – meaning that attackers can take over servers without knowing any valid account credentials. This gives them access to email communications and the opportunity to install a web shell for further exploitation within the environment.
- Allows an attacker bypassing the authentication and impersonating as the admin. As a result, an unauthenticated attacker can execute arbitrary commands on Microsoft Exchange Server through an only opened 443 port!
- The Exchange On-Premises Mitigation Tool, which installs the specific updates protecting against the threat, runs a malware scan which also detects installed web shells, and removes threats that were detected;

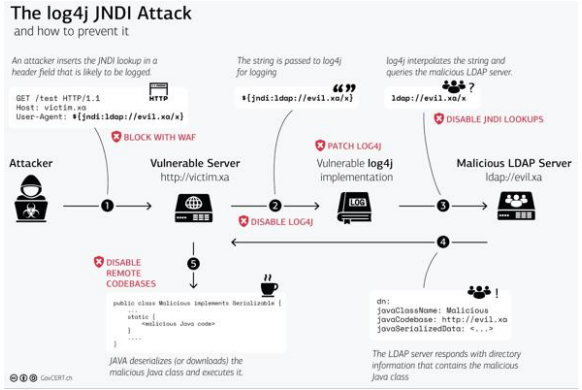
Impact

- Within one week, at least 30,000 U.S. organizations and hundreds of thousands of organizations worldwide have fallen victim to an automated campaign run by HAFNIUM that provides the attackers with remote control over the affected systems.
- Security company ESET identified "at least 10" advanced persistent threat groups. Ransomware cybergangsexploit vulnerability a.o.: Revil & DearCry,
- Attackers continue to have access to the server until the web shell, other backdoors and user accounts added by attackers are removed
- Package for exploiting the vulnerability published to the Metasploit application and on Github.

Lessons Learned

- Belang effectief patch management
- Check for indicators of compromise

LOG4J



Explanation

- Log4j (Logging) is a fundamental feature of most software, which makes Log4j very widespread. Log4j is used by tens of thousands of software packages.
- Log4shell is a critical vulnerability, rated a 10 out of 10 on the Common Vulnerability Scoring System, or CVSS, due to the potential impact that it can have if leveraged by attackers. Details of the vulnerability can be found under the heading CVE-2021-44228.
- On December 9th, the PoC exploit for the notorious Log4Shell vulnerability (CVE-2021-44228) leaked on GitHub.
- Jen Easterly, director of the U.S. Cybersecurity & Infrastructure Security Agency, called Log4Shell the most serious vulnerability she's seen in her career.

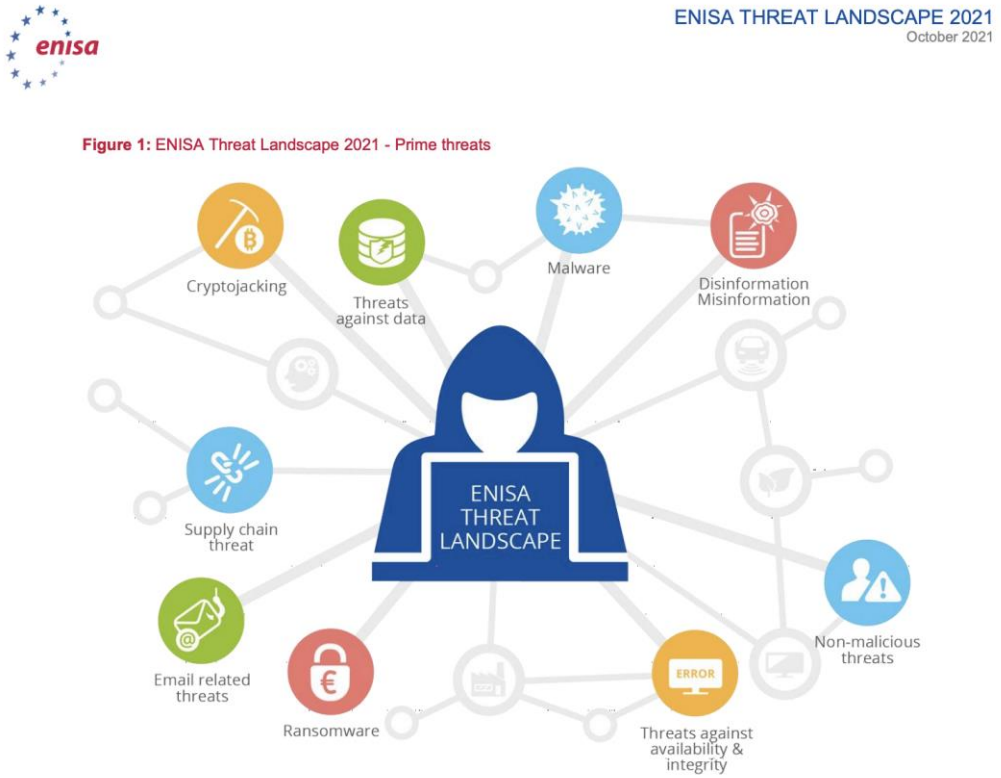
Impact

- More than 35,000 Java packages, amounting to over 8% of the Maven Central repository, have been impacted by the log4j vulnerabilities
- Cybersecurity company Akamai Technologies Inc. has tracked (in the U.S) more than 10 million attempts per hour to exploit the Log4j vulnerability.
- Microsoft Threat Intelligence Center observed access brokers leveraging the Log4Shell flaw to gain initial access to target networks that were then sold to other ransomware affiliates.
- Cyberattack Belgium ministry of Defense. Mail shut down for serveral days. (log4j exploit)
- One of the largest Vietnamese crypto trading platforms, ONUS, recently suffered a cyber attack

Lessons Learned

- Belang configuratie management
- Belang vulnerability scanning tools en Patchen
- Onderzoek Indicators of Compromise regarding the Log4j vulnerability

IT SECURITY INCIDENTEN 2022 ?



Verwachtingen:

- Groei/continuering Ransomware as a service
- Toename supply chain-aanvallen leveranciersketen
- Toename aanvallen op clouddiensten
- Mobile malware
- Nieuwe Vulnerabilities (open source) software
- Nieuwe datalekken
- New exploits van “oude” hacks

Mentimeter vraag:

- **Welke les heb je het afgelopen jaar geleerd (van security incidenten)?**