Státní aktéři a kybernetické útoky

Ing. Dušan Navrátil

Státní aktéři a kybernetické útoky

Jsou tři životní jistoty:

Smrt

Daně

Čínský kybernetický útok

Výrok jednoho izraelského přednášejícího na školení v Izraeli.

Státní aktéři a kybernetické útoky

Pokročilá trvalá hrozba (***Advanced Persistent Threat)*** **APT je pojem z oboru kybernetické bezpečnosti. Popisuje nenápadného útočníka, obvykle národní stát, nebo státem sponzorovanou skupinu. Tato s vynaložením značných lidských a finančních zdrojů získává neoprávněný přístup k počítačové síti. Zůstává při tom po delší dobu nezjištěna. Od nedávné doby se tento termín může vztahovat i na nestátem sponzorované skupiny provádějící rozsáhlé cílené průniky za konkrétními cíli.**

Motivace aktérů těchto hrozeb je typicky politická nebo ekonomická. Každý velký sektor zaznamenal případy kybernetických útoků ze strany vyspělých aktérů s konkrétními cíli, ať už jde o krádež, špehování nebo narušení. Mezi tyto cílové sektory patří vláda, obrana , finanční služby , právní služby , průmysl, telekomunikace, akademická sféra a mnoho dalších. Některé skupiny využívají tradiční špionážní vektory, včetně sociálního inženýrství , lidské inteligence a zranitelnost získat přístup k fyzickému umístění a umožnit síťové útoky. Účelem těchto útoků je nainstalovat vlastní malware (škodlivý software).

Státní aktéři a kybernetické útoky

Medián "doba prodlevy", doba, po kterou útok APT není detekován, se mezi regiony značně liší. FireEye uvedlo průměrnou dobu setrvání pro rok 2018 v Americe na 71 dní, v regionu EMEA na 177 dní a v Asii a Tichomoří na 204 dní. Takto dlouhá doba prodlevy umožňuje útočníkům značné množství času na to, aby prošli cyklem útoku, rozšířili se a dosáhli svého cíle.

Životní cyklus útoku ATP

1. Zaměří se se na konkrétní organizace pro jeden jediný cíl
2. Pokusí se o prosazení se v prostředí (běžné taktiky zahrnují spear phishingové e-maily)
3. Použije kompromitované systémy jako přístup do cílové sítě
4. Nasadí další nástroje, které pomohou splnit cíl útoku
5. Zakryje stopy pro zachování přístupu pro budoucí iniciativy

Státní aktéři a kybernetické útoky

První velké kybernetické útoky ATP, které měly zásadní vliv na kybernetickou bezpečnost:

- **1996 Moonlight Maze – špionážní útok – cíl – NASA,Pentagon, vojenští dodavatelé, civilní akademici a řada dalších vládních agentur – ukradení obrovského množství dat – obrovské škody strategického charakteru – využití zranitelností – vybudování zadnich vrátek a přesměřování specifického síťového provozu přes Rusko – dva roky nezjištěn – doba naivity – všechny údaje pro útok zjištěny z otevřených zdrojů včetně zranitelností**

- **2003 Titan Rain – špionážní útok na informační systémy USA – DEA, Lockheed Martin, Sandia National Labotoriess, Redstone Arsenal, ,NASA a další – VB – ministerstvo obrany – tři roky neodhalen – útočník APT 1 – jednotka čínské armády 61398**

- **2007 Stuxnet – destruktivní napadání SCADA systémů sofwaru Siemens – kybernetická zbraň – útok pomocí infikované USB flash paměti – napadá PLC(programovatelné logické regulátory) – používané k řízení strojů a průmyslových procesů – využívá čtyř zranitelností zero-day – schopnost se šířit, hledání Siemens Step7software a schopnost samodestrukce – jedná se o přesné cílení – odhaduje se – práce skupiny pěti až třiceti lidí po dobu šesti měsíců – útok na centrifugy (odtředivky) na obohacování jaderného paliva v Natanzu (Irán) – zničeno asi 1000 centrifug - předpokládá se - útočník Izrael a USA**

Státní aktéři a kybernetické útoky

První velké kybernetické útoky ATP, které měly zásadní vliv na kybernetickou bezpečnost:

- **2007 Red October – špionážní malware pravděpodobně z Ruska – využíval zranitelností Microsoft Word a Excel - především získával diplomatické informace a osobní údaje – objeven v roce 2012**

- **2007 kybernetické útoky na Estonsko – přemístění sochy sovětského vojáka – DDoSové útoky na webowe stránky parlamentu, bank, ministerstev, novin a televizních stanic – velké množství spamu atd. – útočníci z Ruska – nejasná role státu – způsobily změnu myšlení**

- **2009 Aurora – špionážní malware využitím zero-day v Internet Exploreru – cíl americké a evropské státní organizace, dalajláma a americké podniky – zadní vrátka – napojení na řídící servery (nebyly v Číně) – prohledávání obsahu – útočník skupina Elderwood (APT 17) sídlící v Číně**

Státní aktéři a kybernetické útoky

První velké kybernetické útoky ATP, které měly zásadní vliv na kybernetickou bezpečnost:

- **2012 Shamoon – malware určený na zničení společnosti saudské Saudi Aramco (použit i proti katarské RasGaz) – destruktivní – napadá Microsoft Windows NT miware pro 32 a 64 bitovou verzi– šíří se z infikovaného počítače – maže a přepisuje data na pevném disku poškozeným obrázkem - použita hořící vlajka USA – útok v době ramadánu (zaměstnanci odjeli na dovolenou) – phishingem přes e-mail – zasaženo 30 000 počítačů – problémy v obchodování – nebyly zasaženy počítače řídící technologie – náprava - vykoupení pevných disků na světě – obnova 10 dní – útočník „Cutting Sword of Justice“**

- **2017 WannaCry – Ransomwarový útok – celosvětový útok zasáhl 150 států – počítače s OS Microsoft Windows – šifrování dat a výkupné v Bitcoinech – červ (worm) Wanna Cry – lavinovitě se šířil – během jednoho dne nakaženo 230 000 počítačů – největší problémy National Hearth Service v Anglii a Skotsku – nakaženo 70 000 zařízení – neprovedeno 20 000 výkonů – útočník Severní Korea**

Čínská lidová republika

- **Provádí především plošnou kybernetickou špionáž po celém světě – odhad - věnuje se od 50 000 do 100 000 lidí – nejsou známy destrukční útoky**

- **Od roku 2012, kdy se Si Ťin-pching stal generálním tajemníkem Komunistické strany Číny , získalo ministerstvo státní bezpečnosti větší odpovědnost za kyberšpionáž vůči Lidové osvobozenecké armádě a v současnosti dohlíží na různé skupiny APT. Podle bezpečnostního výzkumníka Tima Steffense "Prostředí APT v Číně je řízeno přístupem 'celá země', využívající dovednosti z univerzit, jednotlivců a soukromého a veřejného sektoru.„**

- **Výhody kybernetické špionáže si je Čína vědoma od počátku připojení ČLR k internetu. Využívání kyberprostoru ke sběru zpravodajských informací obchází rizika s řízením lidských agendů, včetně zatčení a odhalení zpravodajských operací. Zpravodajské operace v kyberprostoru nezahrnuji podobná rizika a poskytují státnímu aktéru možnost důvěryhodného popření i v případě, že jsou dané aktivity odhaleny.**

Čínská lidová republika

Základní údaje

- **Cíle** – klíčové vládní instituce, soukromé a státem vlastněné společnosti působící v oblasti výzkumu a vývoje informačních technologií, nevládní organizace zabývající se ČLR
- **Útočník** – Ministerstvo státní bezpečnosti a přidružené ATP skupiny, soukromé skupiny jednající ve prospěch čínské vlády, síly strategické podpory Čínské lidově-osvobozenecké armády
- **Metody** – zranitelnosti nultého dne, pkročilé spear-phishingové kampaně, útoky typu waterling day a další
- **Způsobená škoda** – kompromitace strategických informací, ohrožení konkurenceschopnosti

Čínská lidová republika

- **ČLR je v oblasti kyberprostoru známá zejména pro rozsáhlou průmyslovou špionáž. Krádeže duševního vlastnictví následně posilují úsilí Číny v prioritních obastech vědeckého a technologického rozvoje země. Průmyslová špionáž doplňujedalší, převážně legitimní prostředky prostředky k zahraniční know – how. Plán „Made in China 2025“**

- **Čínské vědecko - technologické priority jsou mj. telekomunikační technologie, satelity, big data processing, umělá inteligence a deep learnig, které jsou pravděpodobně cílem čínských ATP.**
-
- **Další prioritou je je sběr taktických a strategických zpravodajských informací. Tato priorita se začíná vyrovnávat s průmyslovou špionáží. Tato hrozba roste se zájmem o Evropu a zejména Východní Evropu. Iniciativa „Hedvábná cesta“ a „16+1 (dnes 14+1). Útoky proti ministerstvům zahraničí evropských zemí.**

- **Příprava informačního bojiště pro budoucího „informativního“ konfliktu, který se bude vyznačovat intenzivním nasazením metod informačního (včetně útoků v kyberprostoru) a elektronického způsobu boje (např. rušení signálů).**

Čínská lidová republika

Právní podpora státu:

- **Zákon o státní bezpečnosti – definuje rámcovou povinnost jednotlivců a organizací podílet se na zajištění státní bezpečnosti.**
- **Zákon o kontrašpionážní činnosti definuje povinností podílet se na sběru důkazů o špionážní činnosti. Zákon se vztahuje i na aktivity mimo teritorium ČLR.**
- **Zákon o kybernetické bezpečnosti určuje povinnost provozovatelům sítí spolupracovat v otázkách státní bezpečnost.**
- **Zákon o státní zpravodajské činnosti určuje povinnosti jednotlivců a organizací podílet se na zpravodajské aktivitě a práva orgánů podílejících se na zpravodajské činnosti součinnost vyžadovat.**
- **Společnou charakteristikou všech uvedených regulací je jejich velmi široké a vágní pojetí z hlediska definice pojmů jako je např. „státní bezpečnost“ či „špionážní aktivita“. To umožňuje státním orgánům aplikovat dotyčné zákony v závislosti na aktuální potřebě.**
- **Právní systém ČLR také obsahuje mechanizmy přímého vlivu Komunistické strany Číny na dění v nominálně soukromých společnostech skrze povinnost ustanovení stranických buněk.**

Čínská lidová republika

Příklad životního cyklu čínského kybernetického útoku – činnost útočníka:

- **Počáteční kompromitace** – proveden pomocí sociálního inženýrství a spear phishingu přes e-mail, pomocí zero-day apod. Další populární metodou infekce je umístění malwaru na webovou stránku, kterou zaměstnanci oběti pravděpodobně navštíví.
- **Vytvoří si pevnou půdu pod nohama** – umístí software pro vzdálenou správu do sítě oběti, vytvoří síťová zadní vrátka a tunely umožňující utajený přístup k její infrastruktuře.
- **Eskaluje oprávnění** – použije exploity a prolomení hesel k získání administrátorských práv nad počítačem oběti a případně je rozšíří na účty administrátorů domény Windows.
- **Interní průzkum** – shromažďujte informace o okolní infrastruktuře, vztazích důvěryhodnosti, struktuře domény Windows .
- **Přesune se do strany** – rozšiřuje kontrolu na další pracovní stanice, servery a prvky infrastruktury a provádí na nich sběr dat.
- **Udržuje přítomnost** – zajišťuje nepřetržitou kontrolu nad přístupovými kanály a přihlašovacími údaji získanými v předchozích krocích.
- **Dokončuje misi** – exfiltrujte ukradená data ze sítě oběti.

Čínská lidová republika

Čínské APT

- PLA Unit 61398 (také známý jako APT1, Puter Panda – útok Titan Rain)
- PLA Unit 61486 (také známý jako APT2)
- Buckeye (také známý jako APT3)
- Red Apollo (také známý jako APT10)
- Numbered Panda (také známý jako APT12)
- APT15
- DeputyDog (také známý jako APT17, Elderwood – operace Aurora)
- Codoso Team (také známý jako APT19)
- Wocao (také známý jako APT20)
- APT 27
- PLA Unit 78020 (také známý jako APT30 and Naikon)
- Zirconium (také známý jako APT31)
- Periscope Group (také známý jako APT40)
- Double Dragon (také známý jako APT41, Winnti Group, Barium, nebo Axiom)
- Dragonbridge
- Hafnium
- LightBasin (také známý jako UNC1945)
- Tropic Trooper

Čínská lidová republika

Popis některých čínských APT:

- **Jednotka PLA (Peoples Liberation Army) 61486 (APT2) (– jednotka ČLOA Čínská lidově-osvobozenecká armáda) – většina kybernetických útoků zaměřena na americký, evropský a japonský letecký a satelitní průmysl – útok Titan Rain 2003 - ??přisouzen útok Hades 2013 – krádeže dat celé řady zbrojních programů – Pac-3 Patriot, Hight Altitude Area Defence (protiraketový systém), F/A Super Hornet, UH 60 Black, F-35 Joint Strike Fighter – ovlivnil vývoj čínských letounů 5. generace J-20, J-31**

- **Jednotka PLA 61398 (APT2) – vojenská jednotka – útoky na americké soukromé dodavatelské firmy MO – útok na indickou armádu – 2006 operace RAT - OSN – Mezinárodní olympijský výbor - 2009 operace GhostNet - ambasády, MZV, tibetská exilová komunita, vládní úřady, NATO**

- **Red Apollo (APT 10) – napojená na Ministerstvo státní bezpečnosti (MSS) – akademická sféra – krádež 130 000 osobních údajů personálu amerického námořnictva (2016) – Filipíny (2019) – Japonsko(2020) – Indie (2021)**

Čínská lidová republika

Popis některých čínských APT:

- **Numbered Panda (APT 12) – napojen na ČLOA – cílem Východní Asie včetně Taiwanu**
- **APT 40 – cíl vládní organizace, společnosti včetně universit v širokém spektru včetně biomedicíny, robotiky a námořního výzkumu**
- **Double Dragon – „hackři v pronájmu“ – zabývají se špionáží technologií i kyberkriminalitou, (krádež nejméně 20 000 dolarů na pomoc COVID-19 v USA – 2022) – dvojí zaměstnání – symbióza**
- **Hafnium – napojení na MSS - 2021- narušení Microsoft Exchange Server**
- **LightBasin – cílí na protokoly a technologie telekomunikačních operátorů**

Čínská lidová republika

Popis některých čínských APT:

- **APT15 – 2013 – Operace Ke3Chang – útoky proti ministerstvům zahraničí evropských zemí**

- **Čínské ATP? – 2014 - OPM Hack – kybernetický útok na sítě na vládní Office of Personnel Managment (OPM) – obdoba českého NBÚ – úřad pro provádění bezpečnostních prověrek – ukradeno bylo několik milionů formulářů SF-86, které obsahovaly osobní údajích shromážděné při bezpečnostních prověrkách, včetně otisků prstů milionů lidí – útočníci pronikli prostředím OPM do serveru ministerstva vnitra – odcizili dalších 4,2 mil. osobních údajů a otisky prstů - nedozírné následky – CIA stáhla řadu důstojníků z Číny, kteří pracovali pod krytím – nutná ochrana některých lidí- zatím do roku 2025 – odhadované náklady na ochranu 1 miliarda dolarů – nejprve útočníci pronikli do manuálů a informací o architektuře IT systému - systém napojen na internet – dva subdodavatelé služeb bezpečnostních prověrek – USIS a KeyPoint – při útoku použity ukradené přihlašovací údaje KeyPointu – již před útokem bylo OPM kritizováno za špatné bezpečnostní postupy.**

Ruská federace

- **Rusko v minulosti velmi využívalo špionáže, průmyslové špionáže, politických vražd, sabotáží, destruktivních útoků, desinformačních kampaní, ovlivňování veřejného mínění a voleb, v zahraničí které dodnes provádí klasicky.**
- **Dnešní prostředí nových technologií a zejména internetu umožňuje tyto operace provádět mnohem efektivněji a levněji a umožňuje vézt efektivně hybridní válku.**
- **Rusko je velkým inovátorem ve vedení hybridní války.**
- **V kyberšpionáži jsou průkopníkem.**
- **Kybernetické destruktivní útoky používají ve velké míře a dlohoudobě zejména na Ukrajině, překvapivě jsou méně účinné než se očekávalo. Vede to k celosvětovému pokroku v obraně proti nim.**
- **Nemá informační technologie, které se používají v západních IS výjimka (Kasperský ?)**
- **Úspěšné ve vedení desinformačního boje a ovlivňování veřejného mínění v zahraničí pomocí internetu.**
- **Bezpečné pro soukromé skupiny, které provádějí kybernetické útoky za účelem finančního zisku. Symbioza se státními orgány.**

Ruská federace

Popis některých ruských APT:

- **Fancy Bear (APT 28) – ruská ZS GRU – útoky na Gruzii,zakavské státy, Ukrajinu, NATO, vojenští dodavatelé MO USA, bílý dům, Demokratická národní výbor, německý a francouzský parlament, OBSE, francouzký prezident Macron, TV5Monde, desítky nepřátel Putina v zahraničí, Světová antidopingová agentura, IAAF, Konstantinopolský ekumenický patriarchát a další- využívají zero-day exploit, spear phishing a malware**
- **Cozy Bear (APT 27) – ZS SVR nebo GRU – diplomatické orgány a vládní organizace – Demokratický národní výbor (nezávisle spolu s Fany Bear – nevěděly o sobě) – americké think-tanky a neziskovky – norské a nizozemské státní organizace – vakcíny proti COVID19 – útok na dodavatelský řetězec aktualizace obchodního softwaru SolarWinds Orion**
- **Bersek Bear - ZS FSB – zaměření na sledování a průzkum infrastruktury veřejných služeb, zejména zásobování vodou (USA, Německo)- municipality a další**
- **Sandworm – jednotka 74455- kybervojenská jednotka GRU – kyberútok na ukrajinskou rozvodnou síť (prosinec 2015 a rok 2016) – kyberútoky na Ukrajinu pomocí malwaru NotPtay**
- **Gamaredon – útoky na celém světě – leden 1922- Ukrajina**

Ruská federace

- **Popis některých ruskýc kyberútoků:**

- **Estonsko 2017- DDoS útok**
- **Útok na Gruzii – spolu s kinetickým útokem masívní DDoS útoky a změna webových stánek– cyberútoky začaly týden před zahájenim útoku na stránky tiskových agentur**
- **Útoky na Ukrajinu - Útoky na automatizovaný systém "Volby", červen 2014 - První hacknutí ukrajinské elektrické sítě, prosinec 2015. Útoky prosinec 2015. Útoky pomocí trojského viru BlackEnergy na energetické společnosti na Ukrajině, které dodávají energii regionům Kyjev, Ivano-Frankivsk a Černovice. Jednalo se o první úspěšný kybernetický útok na rozvodnou síť.- Druhé hacknutí ukrajinské elektrické sítě, prosinec 2016. - Paralýza státní pokladny Ukrajiny, prosinec 2016 - Kybernetické útoky na Ukrajinu z roku 2017, Hromadný hackerský útok na dodavatelský řetězec, červen 2017 s použitím viru Petya - Kybernetický útok na Ukrajině 2022 , útoky na webové stránky ukrajinské vlády, leden 2022, jeden den poté, co selhala americko-ruská jednání o budoucnosti Ukrajiny v NATO – cybernetické útoky předcházející a doprovázející útok na Ukrajinu**

Irán

Iránské útoky zřejmě byly vyprovokovány, kybernetickým útokem na jaderné zařízení v Natanzu v červnu 2010.

- **Operace Ababil – DoS útoky na finanční instituce v USA od roku 2012**
- **Team Elfin – APT 33 – vazba na íránskou vládu – cíle letecký, vojenský a petrochemický průmysl - používá mazací program ShapeDhift podobný Shamoon**
- **Kitten Helix (ATP 34) – kyberšpionáž,sabotáž – cíle jsou finanční energetický, telekomunikační a chemický průmysl**
- **Charming Kitten (APT 35) – vládní – útočí na e-maily**

Severní Korea

Přestože Severní Korea občas trpí hladomorem, vyvinula jaderné zbraně, vyvíjí mezikontinentální rakety a je schopna podnikat sofistikované kybernetické útoky

Kybernetické operace jsou považovány za nákladově efektivní způsob, jak si Severní Korea zachovat asymetrickou vojenskou možnost, a také za prostředek ke shromažďování zpravodajských informací; jeho hlavní zpravodajské cíle jsou Jižní Korea, Japonsko a Spojené státy.

Bureau 121 je severokorejská agentura pro kybernetické války a hlavní jednotka Generálního úřadu pro průzkum severokorejské armády . Provádí útočné kybernetické operace, včetně špionáže a kybernetické finanční kriminality.

Bureau 121 je největší (více než 600 hackerů) a nejsofistikovanější jednotka. Bureau 121 jr osazeno některými z nejtalentovanějších počítačových expertů Severní Koreje a je řízeno korejskou armádou. Přeběhlík uvedl, že agentura má asi 1800 specialistů. Mnoho pracovníků úřadu jsou ručně vybraní absolventi Univerzity automatizace v Pchjongjangu a stráví pět let školením. Odhad z roku 2021 naznačoval, že v Bureau 121 může být více než 6 000 pracovníků, přičemž mnozí z nich působí v jiných zemích, jako je Bělorusko, Čína, Indie, Malajsie a Rusko. Zatímco tito specialisté jsou rozptýleni po celém světě, jejich rodiny mají doma zvláštní privilegia.

Severní Korea

Nejznámější útoky:

- **2013 - kybernetické útoky v Jižní Koreji - útok na více než 30 000 počítačů v Jižní Koreji, na banky a vysílací společnosti a také webové stránky jihokorejské prezidentky Park Kun-hje – DDoS útoky, krádeže a mazání dat - infikování tisíců jihokorejských smartphonů zákeřnou herní aplikací škody 750 mil dolarů.**

- **2014 – útok na Sony Pictures – krádeže dat – útočníci nepozorovaně působili 2 měsíce – poté zveřejnili citlivá osobní data a kopie dosud neuvedených filmů – plány na budoucí filmy scénáře apod. – mázání infrastruktury Sony - Během útoku skupina požadovala, aby Sony stáhla svůj tehdy připravovaný film *The Interview*, komedii o spiknutí s cílem zavraždit severokorejského vůdce Kim Čong-una, a vyhrožovala teroristickými útoky v kinech, kde se film promítal. Poté, co se mnoho velkých amerických divadelních řetězců rozhodlo nepromítat *The Interview* v reakci na tyto hrozby, Sony se rozhodla zrušit formální premiéru filmu a mainstreamové uvedení a rozhodla se přeskočit přímo na digitální verzi ke stažení, po níž bude následující den následovat omezené uvedení v kinech.**

Severní Korea

- **2016 - Bangladéšská bankovní loupež - krádež, ke které došlo v únoru 2016 - kybernetičtí útočníci vydali 35 podvodných pokynů prostřednictvím sítě SWIFT k nezákonnému převodu téměř 1 miliardy USD z účtu Federální rezervní banky v New Yorku patřícího Bangladesh Bank, centrální bance Bangladéše - pět z třiceti pěti podvodných pokynů bylo úspěšných při převodu 101 milionů USD, přičemž 20 milionů USD bylo vysledováno na Srí Lanku a 81 milionů USD na Filipíny - Federální rezervní banka v New Yorku zablokovala zbývajících třicet transakcí ve výši 850 milionů USD kvůli podezření vyvolanému chybně napsaným pokynem - všechny peníze převedené na Srí Lanku byly získány zpět - od roku 2018 však bylo získáno zpět pouze přibližně 18 milionů USD z 81 milionů USD převedených na Filipíny - většina peněz převedených na Filipíny šla na čtyři osobní účty, které drželi jednotlivci, a ne do společností nebo korporací**

Severní Korea

- **2017- Ransomwarový útok WannaCry - celosvětovým kybernetickým útokem v květnu 2017 ze strany ransomwarového šifrovacího červu WannaCry , který se zaměřoval na počítače s operačním systémem Microsoft Windows šifrováním dat a vyžadováním výkupného v kryptoměně Bitcoin - šířilo se pomocí EternalBlue - exploitu vyvinutého Národní bezpečnostní agenturou Spojených států (NSA) pro systémy Windows. EternalBlue byl ukraden a zveřejněn skupinou s názvem The Shadow Brokers měsíc před útokem. Zatímco Microsoft již dříve vydal záplaty k uzavření exploitu, velká část šíření WannaCry pocházela od organizací, které je neaplikovaly, nebo používaly starší systémy Windows, jejichž životnost již skončila - Odhaduje se, že útok zasáhl více než 300 000 počítačů ve 150 zemích , přičemž celkové škody se pohybovaly od stovek milionů až po miliardy dolarů - Jednou z největších agentur zasažených útokem byly nemocnice National Health Service v Anglii a Skotsku a mohlo být zasaženo až 70 000 zařízení – včetně počítačů, MRI skenerů , chladniček pro skladování krve a divadelních zařízení. Dne 12. května musely některé služby NHS odmítnout nekritické případy nouze a některé sanitky byly odkloněny. Ačkoli samotný útok byl zastaven již 12. května je odhadováno, že nemohlo být provedeno 19000 zdravotnických výkonů.**

Severní Korea

- **2021 – odhadují se zisky z krádeže kryptoměn 429 mil. dolarů**

- **2022 - odhadují se zisky z krádeže kryptoměn 1,7 miliard dolarů (44% z celkem ukradených v hodnotě 3,8 miliard dolarů)**
- **2023 – odhadují se zisky 1 miliarda dolarů**

Pozn. Severní Korea utržila v roce 2020 na exportu zboží 142 mil. dolarů.

Útoky státních aktérů v České republice

- **??? DDoS útoky v roce 2013**
- **Útoky na Ministerstvo zahraničních věcí**
- **DDos útoky v rámci postoje ČR k válce na Ukrajině**

Dotazy?
Diskuze!