MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Jún 2021

Vypracoval: CSIRT.SK

TLP: White

V mesiaci jún bola zverejnená správa od výskumníka spoločnosti Palo Alto Networks Daniela Prizmanta ohľadom malvéru Siloscape, ktorý je aktívny už viac ako rok. Je určený na kompromitáciu kontajnerov operačného systému Windows a následne zasahuje klastre Kubernetes v cloudovom prostredí. Siloscape využíva Tor proxy a doménu .onion na pripojenie sa k riadiacemu serveru.

Pre Siloscape sú charakteristické techniky ako zacielenie na bežné cloudové aplikácie ako napríklad webové servery, s cieľom získať počiatočnú podporu zneužitím známych zraniteľností. Následne po úniku z kontajnera získava možnosť vzdialene vykonať kód na základnom uzle. Malvér sa pokúša zneužiť oprávnenia uzla na šírenie v klastri, a následne nadväzuje kontakt s riadiacim serverom. Jeho cieľom je zostať neodhalený a nevystopovateľný, pričom vytvára zadné vrátka do klastra.

Malvér bol spočiatku spozorovaný v rámci kontajnerov operačného systému Linux z dôvodu popularity tohto operačného systému v cloudových prostrediach.

Vyšetrovanie riadiaceho servera ukázalo, že tento malvér je len malou časťou rozsiahlejšej kampane. Po získaní prístupu na riadiaci server Prizmant identifikoval 23 aktívnych obetí a zistil, že server hostil dokopy 313 používateľov.

Útok malvéru sa zvyčajne začína tým, že útočníci zneužijú známu zraniteľnosť na získanie schopnosti vzdialene vykonať kód v kontajneri Windows, ktorý sa potom použije na spustenie malvéru Siloscape. Ďalej malvér unikne z kontajnera, aby kompromitoval hostiteľa. Skontroluje, či má hostiteľ oprávnenie na vytváranie nových nasadení Kubernetes a pripojí sa k riadiacemu serveru pomocou prehliadača Tor. Na únik z kontajnera sa malvér vydáva za súbor „CExecSvc.exe“ a následne vytvorí symbolický odkaz na svoju kontajnerovú jednotku X s diskovou jednotkou C hostiteľa.

Spoločnosť Microsoft tiež varuje pred sériou útokov ohrozujúcou klastre Kubernetes s inštanciami strojového učenia Kubeflow (ML) s cieľom nasadiť kontajnery, ktoré budú ťažiť kryptomeny Monero a Ethereum. Na získanie počiatočného prístupu ku klastrom a následnú ťažbu útočníci využívajú verejne dostupné nástenky Kubeflow. Táto kampaň nadväzuje na podobnú kampaň z apríla 2020, ktorá tiež zneužívala klastre Kubernetes na ťažbu kryptomien. Siloscape vo všeobecnosti otvára dvere širokej škále škodlivých aktivít.

Útočníci zneužívajú aj nesprávne nakonfigurované inštancie Argo Workflows na ťažbu kryptomien. Ku klastrom získavajú prístup cez vystavené nástenky Argo Workflows. Výskumníci sú názoru, že hrozia aj útoky v širšom rozsahu, pretože na internete sú vystavené stovky takýchto inštancií.

Správcom klastrov Kubernetes odporúča spoločnosť Microsoft prejsť z Windows kontajnerov na kontajnery Hyper-V a zabezpečiť ich bezpečnú konfiguráciu, aby zabránil malvéru, ako je napríklad Siloscape, vykonávať privilegované úlohy. Správcom sa tiež odporúča, aby vynútili autentifikáciu na nástenkách Kubeflow a Argo Workflows, ak sa nedá vyhnúť ich vystaveniu na internete, a tiež monitorovali svoje prostredie.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci jún riešil najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Vyskytli sa aj cielené emailové kampane. Najzávažnejšou z nich bol pokus o podvod, pri ktorom sa útočníci zapojili do prebiehajúcej komunikácie medzi obeťou a dodávateľom. Komunikovali s obomi subjektmi, pričom predstierali identitu druhej strany. Pri incidente hrozila vysoká finančná strata zo štátnych zdrojov, rádovo v miliónoch EUR.

Jednotka zaznamenala kompromitáciu zariadenia v infraštruktúre organizácie vo svojej konštituencii, z ktorého útočníci spustili skenovanie okolitých dostupných systémov. Zariadenie bolo obnovené zo záloh a boli zmenené prístupové údaje.

Ani v tomto mesiaci sa konštituencii CSIRT.SK nevyhýbali vishingové telefonáty z falšovaných telefónnych čísiel vrátane slovenských predvolieb, s klasickou tematikou technickej podpory spoločnosti Microsoft.

CSIRT.SK v rámci svojej proaktívnej činnosti kontaktoval organizácie, ktoré využívali z internetu dostupné zariadenia cez protokol RDP a varoval ich pred možnými hrozbami z toho vyplývajúcimi. Vo všeobecnosti jednotka odporúča v prípade potreby vzdialeného prístupu k zariadeniu tento prístup zabezpečiť pomocou VPN.

Jednotka zachytila informáciu o aktuálnej ponuke falošných slovenských dokladov na darkwebových fórach. O tejto skutočnosti informovala NBÚ. Tiež priamou cestou upozornil na kritickú zraniteľnosť služby Windows Print Spooler CVE-2021-1675. Varovanie rozposlala jednotka ohľadom útoku na spoločnosť Kaseya, ktorý zasiahol aj jej vyše 1500 zákazníckych organizácií a ohľadom kampane skupiny APT31, cielenej na malé routre. Svojej konštituencii poskytla aj IoC pre kontrolu a blokovanie.

Významné útoky vo svete

Spoločnosť Adata sa stala obeťou útoku, čo malo za následok únik údajov o veľkosti 1,5TB

Spoločnosť Adata bola po útoku ransomvéru nútená uviesť svoje systémy do režimu offline. Skupina Ragnar Locker tvrdí, že ukradla 1,5 TB citlivých údajov zo siete pred nasadením samotného ransomvéru. Útočníci ako dôkaz na svojej stránke uverejnili iba snímky obrazovky s ukradnutými súbormi a priečinkami. Ukradnuté boli dôverné súbory, schémy, finančné údaje, zdrojové kódy SVN a Gitlab, právne dokumenty, dohody o mlčanlivosti a ďalšie. Neskôr útočníci zverejnili odkazy na stiahnutie 13 archívov, ktoré dokopy obsahovali viac ako 700GB odcudzených údajov.

Spoločnosti Electronic Arts unikli údaje o veľkosti 750GB

Herná spoločnosť Electronic Arts (EA) bola napadnutá útočníkmi, ktorí tvrdia, že ukradli približne 750GB údajov, ktoré zahŕňajú zdrojové kódy a nástroje na debugovanie. Útočníci tvrdia, že ukradli celý zdrojový kód hry FIFA, údaje o herných klientoch EA a tiež body, ktoré sa používajú ako mena v hre. Tieto body útočníci častokrát využívajú na „pranie špinavých peňazí“. Zdieľali tiež snímky obrazovky s výpismi adresárov a zdrojovým kódom ako dôkaz, že ukradnuté informácie sú legitímne.

Reťazec rýchleho občerstvenia McDonald’s sa stal obeťou útoku

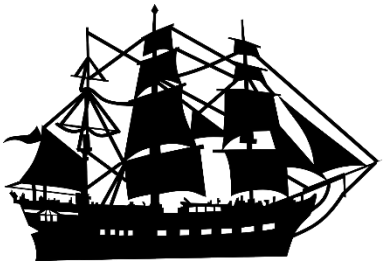
Reťazec rýchleho občerstvenia McDonald’s potvrdil únik údajov po tom, čo útočníci narušili jeho systémy a ukradli údaje o zákazníkoch a zamestnancoch z USA, Južnej Kórey a Taiwanu. Uniknuté údaje zahŕňali osobné údaje ako meno, emailová adresa a telefónne čísla zákazníkov, zatiaľ čo platobné údaje ostali neodhalené. Spoločnosť investovala do implementácie viacerých bezpečnostných systémov, vďaka ktorým rýchlo

identifikovali a obmedzili neoprávnenú aktivitu v ich sieti.

Audi a Volkswagen utrpeli únik údajov, ktorý sa týka 3,3 milióna zákazníkov

Spoločnosti Audi a Volkswagen utrpeli únik údajov, ktorý ovplyvnil približne 3,3 miliónov zákazníkov. Uniknuté údaje môžu zahŕňať kontaktné údaje ako meno a priezvisko, poštová adresa, emailová adresa a telefónne číslo, ale tiež citlivejšie informácie ako čísla sociálneho zabezpečenia, identifikačné čísla vozidla, čísla pôžičiek a podobne. Viac ako 95% zahrnutých citlivých údajov boli čísla vodičských preukazov. Keďže údaje Audi a Volkswagen boli dlho nezabezpečené (v období od augusta 2019 do mája 2021), nedá sa povedať, koľko ľudí mohlo získať neoprávnený prístup k týmto údajom.

Špeciálny malvér bráni užívateľom v prístupe k pirátskym webovým stránkam



Výskumníci objavili malvér, ktorý užívateľom bráni v prístupe k webovej stránke The Pirate Bay, ktorá slúži na nelegálne sťahovanie obsahu chráneného autorským právom. Malvér sa nesnaží ukradnúť heslá, ani nevydiera používateľa. Úpravou súboru „hosts“ blokuje možnosť navštevovať pirátske webové stránky. Malvér sa distribuuje prostredníctvom serverov v rámci aplikácie Discord alebo prostredníctvom pirátskych torrentov. Po spustení sa pripojí na vzdialený server, ktorý je pod kontrolou útočníka a odošle meno falošného pirátskeho softvéru, ktorý používateľa infikoval. Útočník tiež môže vidieť IP adresu, z ktorej pristupoval používateľ na web.

Útočníci sa nabúrali na webovú stránku spoločnosti Eggfree Cake Box odkiaľ odcudzili čísla kreditných kariet

Britská sieť obchodov Eggfree Cake Box sa stala obeťou útočníkov, ktorí sa nabúrali na web tejto spoločnosti a ukradli čísla kreditných kariet. Neoprávnená tretia strana získala prístup na webovú stránku Cake Box a

umiestnila na ňu malvér. Pomocou neho útočníci mohli získať informácie, ktoré zákazníci poskytujú pri nakupovaní online. Keď zákazníci uskutočnili nákup na infikovanej stránke, skripty odoslali na vzdialené servery ovládané útočníkmi údaje ako meno a priezvisko, emailovú adresu, poštovú adresu a informácie o platobnej karte vrátane kódu CVV. Pravdepodobne sa jedná o útok typu MageCart.

Dve cloudové databázy spoločnosti Wegmans Food Markets boli verejne dostupné na internete

Obchodný reťazec Wegmans Food Markets informoval svojich zákazníkov o tom, že dve jeho cloudové databázy boli verejne dostupné na internete z dôvodu problému s konfiguráciou. Odhalené informácie zahŕňali mená, adresy, telefónne čísla, dátumy narodenia, emailové adresy, heslá a podobne. Informácie o platobných alebo kreditných kartách neboli v rámci tohto incidentu odhalené. Spoločnosť obmedzila prístup útočníkovi vynútením obnovenia hesla pre všetky ovplyvnené účty, aby sa zabránilo budúcim prihláseniam.

„8 sekundový“ únik údajov ovplyvnil 123 zamestnancov spoločnosti AmeriGas

Americký poskytovateľ propánu AmeriGas utrpel únik údajov, ktorý trval 8 sekúnd a ovplyvnil 123 zamestnancov. Únik súvisí s kompromitovaním spoločnosti J. J. Keller, čo je dodávateľ zodpovedný za poskytovanie služieb spoločnosti AmeriGas. Medzi tieto služby patrí pomoc spoločnosti AmeriGas pri vykonávaní kontrol vodičských preukazov, testovanie drog a alkoholu u vodičov a podobne. Zamestnanec spoločnosti J. J. Keller sa stal obeťou phishingového emailu, čo viedlo ku kompromitácii účtu. Odhalené údaje obsahovali rodné čísla, čísla vodičských preukazov, dátumy narodenia a podobne. V súčasnosti nič nenasvedčuje tomu, že by boli nejaké informácie o zamestnancoch zneužité.

Útočníci zo Severnej Kórey napadli vnútorné siete Kórejského inštitútu pre výskum atómovej energie

Kórejský inštitút pre výskum atómovej energie (KAERI), vládou sponzorovaný ústav pre výskum a aplikáciu jadrovej energie v Južnej Kórei, potvrdil, že ich vnútorné siete boli napadnuté útočníkmi zo Severnej Kórey. Útočníci sa do siete dostali zneužitím zraniteľnosti VPN. Prístupové záznamy potvrdzujú, že 13 neoprávnených IP adries získalo prístup do internej siete prostredníctvom VPN. Jedna z IP adries je spájaná so skupinou Kimsuky (Thallium, Black Banshee, Velvet Chollima), ktorá sa pomocou phishingových útokov zameriava na ďalšie juhokórejské vládne agentúry.

Trójsky kôň ChaChi sa zameriava na americké školy

Trójsky kôň ChaChi, napísaný v programovacom jazyku Go, sa po útokoch na vládne agentúry zameral na americké školy. ChaChi bol zaznamenaný v prvej polovici roku 2020 voči francúzskym miestnym vládnym orgánom. Malvér je schopný vykonávať typické činnosti RAT (Remote Access Trojan), vrátane vytvárania zadných vrátok, tunelovania DNS, využívania proxy SOCKS a podobne. Názov ChaChi je odvodený od dvoch bežne dostupných nástrojov Chashell a Chisel, ktoré malvér používa počas útokov.

Spoločnosť Mercedes-Benz USA utrpela únik údajov, ktorý sa týkal menej ako 1000 zákazníkov

Mercedes-Benz

Spoločnosť Mercedes-Benz USA sa stala obeťou úniku údajov, ktorý ovplyvnil niekoľko jej zákazníkov. Uniknuté údaje sa týkali menej ako 1000 zákazníkov, pričom odhalené boli informácie o kreditných kartách, čísla sociálneho zabezpečenia a čísla vodičských preukazov. Údaje unikli z dôvodu nedostatočného zabezpečenia inštancie cloudového úložiska. Uniknuté informácie sa týkali zákazníkov webových stránok predajcov a Mercedes-Benz z obdobia medzi 1. januárom 2014 a 19. júnom 2017.

Útok ransomvéru na spoločnosť FujiFilm ovplyvnil časť vnútornej siete

Spoločnosť FujiFilm sa stala obeťou útoku ransomvéru, pričom bola nútená vypnúť časť svojej siete. Kybernetický útok konkrétne utrpelo ústredie nachádzajúce sa v meste Tokyo. Útok ransomvéru pravdepodobne súvisí s tým, že spoločnosť FujiFilm bola minulý mesiac infikovaná trójskym koňom Qbot. Skupina stojaca za malvérom Qbot v súčasnosti spolupracuje so skupinou stojacou za ransomvérom REvil. Aj keď je ransomvér aktívny už od roku 2012, pozornosť si získal hlavne vďaka útoku na spoločnosť Colonial Pipeline.

- **Americké ministerstvo spravodlivosti sa zmocnilo domén používaných pri phishingových útokoch na USAID.**
- **„Have I Been Pwned“ začalo spoluprácu s FBI.**
- **FBI potvrdila, že za útokmi na JBS stojí ransomvér REvil.**
- **Na servery Microsoft Exchange sa zameriava ransomvér Epsilon Red.**
- **The Steamship Authority – trajektová doprava v Massachusetts, bola zasiahnutá ransomvérom.**
- **Výskumníci objavili nový malvér nazývaný SkinnyBoy, ktorý spájajú so skupinou APT28.**
- **Zdravotnícke centrum na Floride utrpelo údajný útok ransomvéru, ktorý prinútil dve nemocnice uviesť časť svojej siete do režimu offline.**
- **CD Projekt oznámil, že po internete kolujú dáta ukradnuté počas februárového útoku ransomvéru.**
- **Spoločnosť Navistar sa stala obeťou útoku, pri ktorom došlo k ukradnutiu údajov z jej siete.**

- **FBI a AFP vytvorili falošnú chatovaciu platformu „An0m“ na odhaľovanie a usvedčovanie zločincov.**
- **Španielske ministerstvo práce a sociálnej ekonomiky (MITES) sa stalo obeťou kybernetického útoku.**
- **Malvér SteamHide sa vyskytuje v profilových obrázkoch na hernej platforme Steam.**
- **Nová skupina útočníkov Gelsemium je spájaná s útokom na emulátor NoxPlayer.**
- **Kvôli nesprávnej konfigurácii cloudových služieb bolo vystavených viac ako miliarda záznamov patriacich spoločnosti CVS Health.**
- **Nový spyware sa zameriava na používateľov aplikácie Telegram a Psiphon VPN v Iráne.**
- **Britská právnická firma Gateley potvrdila únik údajov.**
- **Útočníci získali prístup k osobným, finančným a zdravotným informáciám zákazníkov lodnej spoločnosti Carnival.**
- **Agent Tesla RAT sa vracia s phishingovou kampaňou súvisiacou s očkovaním proti COVID-19.**
- **Kliniku reprodukčnej medicíny v oblasti Atlanty zasiahol útok ransomvéru. Odhalené boli záznamy o približne 38-tisíc pacientoch.**
- **Ransomvér DarkRadiation sa zameriava na inštancie operačného systému Linux a Docker.**
- **Záznamy zhruba 500-tisíc pacientov očnej kliniky v Iowe mohli byť ukradnuté v rámci útoku ransomvéru.**

Závažné zraniteľnosti bežných softvérových produktov

V doplnku Fancy Product Designer pre Wordpress sa nachádza kritická aktívne zneužívaná zraniteľnosť

Útočníci sa zameriavajú na zero-day zraniteľnosť v doplnku Fancy Product Designer pre Wordpress. CVSS skóre tejto zraniteľnosti je 9.8. Chyba existuje z dôvodu, že doplnok nemá zavedené dostatočné kontroly a z dôvodu, že existujúce kontroly je možné ľahko obísť. Útočník by mohol na webovú stránku nahrať škodlivé súbory.

Závažné zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Cisco StarOS, SD-WAN softvér, Webex Player pre Windows a MacOS, Webex Network Recording Player pre Windows a MacOS, FTD softvér, AnyConnect Secure Mobility Client pre Windows a ďalšie. Úspešným zneužitím týchto zraniteľností môže dôjsť napríklad k úniku informácií, získaniu administrátorských oprávnení, obídeniu autorizácie, vykonávaniu ľubovoľného kódu, eskalácii privilégií alebo narušeniu dostupnosti služby.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Intel® NUC Firmware, DSA, Security Library, Server Board M10JNP2SB, 2021.1 IPU – BIOS, RealSense™ ID, 2021.1 IPU - Intel® VT-d, FPGA OPAE Driver a Thunderbolt™ Controller. Zneužitím zraniteľností môže dôjsť k narušeniu dostupnosti služby a eskalácií privilégií prostredníctvom sieťového alebo lokálneho prístupu.

Mesačník zraniteľností Jún 2021

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java

https://www.csirt.gov.sk/posts/2141.html?csrt=6334625290407285558