MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2022

Vypracoval: CSIRT.SK

TLP: White

Malvérom, ktorý vo februári roku 2022 opäť získal popularitu po istej dobe, sa stal ransomvér BlackByte. FBI vydala varovanie pred novou sériou útokov, pretože ransomvér opäť zosilnieva. Objavený bol už v júli roku 2021. Skupina stojaca za týmto ransomvérom sa zameriava na organizácie so sídlom v USA, a to konkrétne na organizácie patriace do kritickej infraštruktúry, vrátane vlády, financií, potravinárstva, a tiež poľnohospodárstva.

Existujú dva spôsoby ako skupina stojaca za ransomvérom BlackByte malvér používa:

- na priamy útok
- ransomvér ako služba (ransomware as a service), ktorú poskytujú iným útočníkom, ktorí zaplatili autorom malvéru za používanie ich softvéru.

Na počiatočný prístup ransomvér zneužíva zraniteľnosti ProxyShell nájdené na serveroch Microsoft Exchange. BlackByte sa zameriava na servery Microsoft Exchange, pretože mnoho organizácií využíva staršie verzie. Konkrétne ide o verzie 2013 a 2016, ktoré sú stále vo veľkej miere využívané. Ďalším dôvodom varovania FBI je skutočnosť, že skupina stojaca za BlackByte je stále úspešná s predchádzajúcimi formami ransomvérových útokov. Ransomvér však neútočí na infikované systémy, ak je nastavený jazyk ruština alebo jazyky bývalých sovietskych republík.

Varianty ransomvéru BlackByte používajú iba symetrické šifrovanie. Vo svojich skorších variantoch ransomvéru skupina distribuovala šifrovací kľúč každej obeti zo svojho riadiaceho serveru v súbore .png. Keďže pre každú obeť sa používa rovnaký šifrovací kľúč, spoločnosť Trustwave dokázala vyvinúť globálny dešifrátor. Avšak po jeho vydaní skupina útočníkov prestala doručovať kľúč obetiam a taktiež ho zmenila.

Po zašifrovaní súborov útočníci pridajú súborom príponu .blackbyte. Ransomvér zanechá rovnakú poznámku o výkupnom vo všetkých zašifrovaných adresároch a poznámka o výkupnom obsahuje adresu .onion, ktorá obeti dáva pokyny, ako zaplatiť výkupné a získať dešifrovací kľúč.

FBI na ochranu voči tomuto ransomvéru uvádza niekoľko spôsobov mitigácie:

- Implementujte pravidelné zálohovanie všetkých údajov, ukladajte ich ako offline kópie chránené heslom,
- implementujte segmentáciu siete tak, aby zariadenia vo vašej sieti boli dostupné iba zo zariadení, pre ktoré je to nevyhnutné,
- inštalujte a pravidelne aktualizujte antivírusové riešenia.

Spoločnosť Avast pri infikovaní odporúča skúsiť dešifrovací kľúč, ktorý bol vytvorený pre predchádzajúcu kampaň ransomvéru BlackByte – tu však neexistuje záruka, že tento kľúč bude funkčný.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci február riešil hlavne phishingové kampane zasahujúce jeho konštituenciu. Jednotka riešila aj prípad masívnej podvodnej kampane s motívom Sextortion, cielenej na veľkú časť zamestnancov organizácie. Ani tento mesiac nechýbala phishingová komunikácia s vloženým vláknom legitímnych správ. Kompromitácia nastala v tomto prípade mimo konštituencie CSIRT.SK. Zaznamenané boli aj prípady spear phishingu s malvérom v prílohe. Pestrosť útokov na mailservery podčiarkuje prípad pokusov o prienik zneužitím protokolu ActiveSync. CSIRT.SK ďalej riešil prípady kompromitovaných e-mailových kont, ktoré útočníci predávali na internetových fórach.

Útok, ktorý vyvolal nedostupnosť zastaranej prezentačnej webovej domény verejnej inštitúcie v rámci samospráv, podnietil vôľu urýchlene nasadiť novú verziu webu implementujúcu v súčasnosti podporované technológie.

Jednotka zaznamenala tiež prípady skenovania zraniteľností ako aj zneužite zraniteľnosti pri DDoS útoku na ciele v Ruskej federácii.

Začiatkom krízy na Ukrajine CSIRT.SK vypracoval a rozposlal svojej konštituencii výzvu a materiál pre zvýšenie ich kybernetickej bezpečnosti. Jednotka zaznamenala tiež prípady skenovania zraniteľností ako aj zneužitie zraniteľnosti pri DDoS útoku na ciele v Ruskej federácii.

V rámci svojej proaktívnej činnosti jednotka zdieľala so svojou konštituenciou indikátory kompromitácie malvéru Trickbot a informácie o oprave kritických a závažných zraniteľností produktov spoločnosti SAP. Konkrétne organizácie varovala ohľadom potenciálne zraniteľnej služby Samba nájdenej v ich infraštruktúre. CSIRT.SK ďalej vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje.

Významné útoky vo svete

Skupina útočníkov Charming Kitten využíva vo svojich útokoch zadné vrátka PowerLess

Iránska štátom podporovaná skupina Charming Kitten (APT35) nasadzuje zadné vrátka s názvom PowerLess. Vyvinuté sú pomocou PowerShellu, pričom sú vybavené šifrovanými komunikačnými kanálmi na riadenie a umožňujú vykonávať rôzne príkazy. Malvér sa vyhýba detekcii spustením v kontexte aplikácie .NET. Analyzovaná sada nástrojov obsahuje modulárny, viacstupňový malvér, ktorý dešifruje a nasadzuje ďalšie nástroje. Pri skúmaní útokov, pri ktorých boli použité zadné vrátka PowerLess, výskumníci našli aj potenciálne spojenia s ransomvérom Memento.

Útok na Vodafone spôsobil výpadky 4G/5G siete, SMS správ a televíznych služieb

Vodafone Portugal sa stal obeťou útoku, ktorý spôsobil výpadky v celej krajine. Výpadky sa týkali 4G a 5G siete, SMS správ a televíznych služieb. Vodafone nezverejnil podrobnosti o útoku, avšak bezpečnostní experti sa domnievajú, že by sa mohlo jednať o ransomvérový útok. Vodafone má v krajine viac ako 4 milióny predplatiteľov mobilných služieb a približne 3,4 milióna zákazníkov domáceho a firemného internetového pripojenia. Spoločnosti sa podarilo obnoviť služby v krátkom časovom rozsahu.

Bezpečnostní výskumníci zaznamenali novú verziu botnetu FritzFrog

Botnet FritzFrog je aktívny už viac ako 2 roky a je známy ťažbou kryptomien. Zaznamenaná však bola nová verzia malvéru, ktorá má ďalšie funkcie ako napríklad používanie Tor proxy reťazca – kombinuje funkcie, vďaka ktorým sa odlišuje od iných hrozieb rovnakej kategórie. Útočníci sa pripravujú na pridanie aj ďalších funkcií v zameraní na servery Wordpress. Sieť senzorov spoločnosti Akamai zaznamenala približne 24-tisíc útokov, zatiaľ čo botnet si reálne vyžiadal len 1 500

obetí. Väčšina infikovaných hostiteľov je v Číne, ale medzi napadnutými systémami je aj európska televízna sieť, ruská zdravotnícka firma a rôzne univerzity vo východnej Ázii.

Skupina útočníkov MuddyWater vedie útoky voči tureckým organizáciám

Skupina útočníkov MuddyWater vedie novú kampaň zameriavajúcu sa na súkromné turecké organizácie a vládne inštitúcie. Tejto skupine sú pripisované taktiež útoky proti subjektom v strednej a juhozápadnej Ázii a mnohým organizáciám v Európe a Severnej Amerike. Útoky začínajú spearphishingovým emailom, ktorý obsahuje škodlivé súbory a tvári sa, že pochádza z ministerstva zdravotníctva alebo vnútra. V rámci útoku používajú útočníci dva infekčné reťazce, ktoré začínajú doručením súboru PDF. V prvom prípade obsahuje PDF vložené tlačidlo, ktoré po kliknutí načíta súbor XLS. Druhý reťazec využíva súbor EXE namiesto XLS.

Spoločnosť Meyer utrpela únik údajov, ktorý ovplyvnil tisícky zákazníkov

Distribútor kuchynského riadu v USA Meyer sa stal obeťou úniku údajov, ktorý ovplyvnil tisícky zákazníkov. Identifikovaný bol neoprávnený prístup k informáciám o zamestnancoch spoločnosti Meyer a tiež jej dcérskych spoločností. Uniknuté údaje mohli zahŕňať mená, fyzické adresy, dátum narodenia, etnickú príslušnosť a ďalšie citlivé informácie. Spoločnosť BleepingComputer našla na webe ransomvérovej skupiny Conti 2% uniknutých záznamov o jednotlivcoch. Skupina útočníkov však v nasledujúcich mesiacoch nezverejnila zvyšných 98 %. Nevedno však či ide zo strany útočníkov o ochotu rokovať, alebo z dôvodu straty záujmu.

Útok na spoločnosť Swissport viedol k úniku údajov

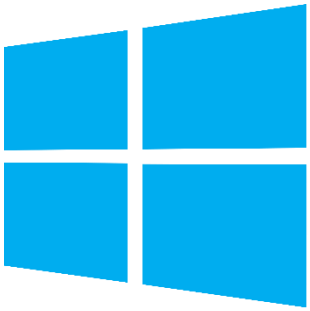
Spoločnosť Swissport International sa stala obeťou útoku ransomvéru. Útok zasiahol IT infraštruktúru spoločnosti a taktiež spôsobil meškanie 22 letov. Taktiež webová stránka spoločnosti bola na istú dobu

nedostupná. K útoku na spoločnosť sa priznala ransomvérová skupina BlackCat (ALPHV). Útočníci tvrdia, že získali až 1,6TB údajov spoločnosti Swissport. Uniknuté údaje zahŕňajú celé meno, číslo pasu, národnosť náboženstvo a ďalšie informácie pravdepodobne o kandidátoch na prácu. Členovia skupiny BlackCat potvrdili, že sú spojení s činnosťou ransomvérovej skupiny BlackMatter.

V rámci smishingovej kampane Roaming Mantis sa šíria škodlivé aplikácie pre Android

Smishingová kampaň Roaming Mantis zasiahla Európske krajiny. Jedná sa o kampaň, ktorá využíva SMS správy na distribúciu škodlivých aplikácií pre Android ako samostatné súbory APK mimo obchodu Google Play. Kampaň využíva trójskeho koňa Wroba, ktorého cieľom je ukradnúť detaily elektronického bankovníctva. Kampaň sa zameriava na používateľov vo Francúzsku a Nemecku. SMS, ktorá sa v rámci kampane šíri, obsahuje škodlivý URL odkaz. Ak používateľ klikne na odkaz prostredníctvom zariadenia iPhone, presmeruje ho to na phishingovú webovú stránku. V prípade, že používateľ používa Android, webová stránka ho vyzve, aby si nainštaloval malvér maskovaný za aplikáciu pre Android.

Nový malvér SockDetour infikuje Windows servery



Nový malvér SockDetour bol použitý ako zadné vrátka na udržanie perzistencie v rámci sietí patriacich americkým dodávateľom ministerstva obrany USA. Tieto zadné vrátka sa využívajú už od roku 2019, avšak donedávna neboli spozorované. Na infikovaných Windows serveroch funguje bez súborov a bez soketov, čo sťažuje detekciu na úrovni hostiteľa a siete. Bezpečnostní výskumníci zaznamenali, že malvér bol nasadený na Windows Server minimálne jedného amerického dodávateľa pre sektor obrany 27. júla 2021, čo viedlo k objaveniu troch ďalších obranných organizácií, na ktoré sa zamerala rovnaká skupina s rovnakými zadnými vrátkami.

V rámci útokov na Ukrajinu bol objavený malvér, ktorý ničí údaje v zariadeniach

V rámci útokov na Ukrajinu bol spoločnosťami ESET a Symantec objavený nový malvér typu „wiper“, ktorý úmyselne ničí údaje v zariadeniach takým spôsobom, aby neboli údaje obnoviteľné. Tiež znefunkčňuje operačný systém. Útoky sa týkajú nie len Ukrajiny, ale tiež Lotyšska a Litvy. Spoločnosť ESET taktiež pripravila technickú analýzu tohto malvéru a spôsob, akým zaznamenali jeho nasadzovanie. Malvér je detegovaný ako Win32/KillDisk.NCV a bol nasadený na stovkách zariadení v ukrajinských sieťach. Malvér bol skompilovaný 28. 12. 2021, čo naznačuje, že útoky mohli byť už nejaký čas plánované. Podľa analýzy spoločnosťou BleepingComputer malvér obsahuje štyri vstavané ovládače s názvom DRV_X64, DRV_X86, DRV_XP_X64 a DRV_XP_X86

Útočníci zo skupiny ModifiedElephant sa zameriavajú na aktivistov pričom podstrkujú „usvedčujúce“ digitálne dôkazy

Skupina útočníkov ModifiedElephant sa zameriava cielenými útokmi na aktivistov za ľudské práva, obhajcov ľudských práv, akademikov a právnikov po celej Indii. Útočníci sa snažia podstrčiť usvedčujúce digitálne dôkazy. Fungujú pomocou komerčne dostupných trójskych koní so vzdialeným prístupom (RAT), pričom zasielajú spearphishingové emaily so škodlivými dokumentmi na doručenie malvéru ako je NetWire, DarkComet a iné. Primárnym cieľom skupiny útočníkov je uľahčiť dlhodobé sledovanie cieľových jedincov.

V dôsledku útoku ransomvéru na spoločnosť Kronos spoločnosť Puma utrpela únik údajov

Spoločnosť Puma sa stala obeťou úniku údajov po tom, čo ransomvér zasiahol spoločnosť Kronos, ktorá je jedným zo severoamerických poskytovateľov služieb riadenia pracovnej sily. Útočníci pred zašifrovaním údajov ukradli aj osobné informácie patriace

zamestnancom spoločnosti a ich rodinným príslušníkom z cloudového prostredia Kronos Private Cloud (KPC). Dostali sa k údajom patriacim viac ako 6-tisíc jednotlivcom. Dokumenty ukradnuté počas ransomvérového útoku na Kronos zahŕňajú čísla sociálneho zabezpečenia.

- **Novo nájdený trójsky kôň typu RAT s názvom StrifeWater je prepojený s iránskou skupinou Moses Staff.**
- **Na nasadenie malvéru BazarBackdoor sú používané škodlivé csv súbory.**
- **Štátna agentúra RIPTA utrpela únik údajov, ktorý zasiahol viac ako 22-tisíc ľudí.**
- **Spoločnosť Morley Companies Inc. sa stala obeťou útoku, ktorého dôsledkom bolo šifrovanie a krádež údajov.**
- **Ransomvér Conti zasiahol spoločnosť KP Snacks, čo ovplyvnilo distribúciu tovaru do supermarketov.**
- **Americké médiá a vydavateľská spoločnosť News Corp zverejnili, že sa stali obeťou pretrvávajúceho kybernetického útoku.**
- **Trójsky kôň Medusa sa zameriava na viacero geografických regiónov, pričom kradne prihlasovacie údaje a vykonáva finančné podvody.**
- **Skupina útočníkov Kimsuky využíva vo svojich útokoch vlastné zadné vrátka s názvom Gold Dragon.**
- **APT skupina Molerats používa v špionážnej kampani implantát s názvom NimbleMamba.**
- **Distribútori malvéru sa vrátili k staršiemu triku známemu ako Squiblydoo na šírenie botov Qbot a Lokibot použitím regsvr32.exe.**
- **Na internete sa našlo viac ako 100-tisíc súborov so študentskými záznamami patriacimi British Council.**

TLP: White

- **Vo svete sa objavil nový malvér s názvom Mars Stealer, ktorý sa javí ako úprava známeho malvéru Oski.**
- **Chorvátsky telefónny operátor „A1 Hrvatska" utrpel únik údajov, ktorý zasiahol približne 200-tisíc zákazníkov.**
- **Značka športového vybavenia a oblečenia Mizuno sa stala obeťou útoku ransomvéru.**
- **Webové stránky ukrajinskej vlády a bánk sa stali obeťami DDoS útokov.**
- **FBI varuje pred útokmi typu BEC na platformy slúžiace na virtuálne stretnutia.**
- **Nový botnet napísaný v jazyku Go vyprázdňuje kryptomenové peňaženky používateľov operačného systému Windows.**
- **Na webových stránkach predajcu elektronických cigariet Element Vape sa objavil skimmer na kreditné karty.**
- **Spoločnosť AON utrpela kybernetický útok, ktorý zasiahol obmedzený počet systémov.**
- **Spoločnosť Axis Communications bola nedávno zasiahnutá kybernetickým útokom, ktorý narušil jej prevádzku.**
- **Operácia malvéru TrickBot sa zastavila po tom, čo sa jeho hlavní vývojári presunuli do skupiny ransomvéru Conti.**
- **Ukrajinský bezpečnostný výskumník odhalil viac ako 60-tisíc súkromných správ patriacich do operácie ransomvéru Conti po tom, čo sa skupina postavila na stranu Ruska kvôli útoku na Ukrajinu.**
- **Útočníci stojaci za ransomvérom Cuba zneužívajú servery Microsoft Exchange na získanie prístupu k podnikovým sieťam.**
- **Japonské závody spoločnosti Toyota boli odstavené z dôvodu podozrenia na útok.**

Závažné zraniteľnosti bežných softvérových produktov

Kritická zraniteľnosť Samba umožňuje vzdialene vykonávať kód

Populárna implementácia protokolu SMB obsahuje kritickú zraniteľnosť, ktorá umožňuje útočníkom s právami zápisu do súborov vykonávať na diaľku ľubovoľný kód. Spoločnosť Samba zároveň opravila druhú závažnú zraniteľnosť, ktorá môže viesť ku nedostupnosti služby, alebo umožniť útočníkom impersonovať existujúce služby.

Spoločnosť SAP vydala februárové záplaty – opravuje 19 zraniteľností

Spoločnosť SAP opravila 19 zraniteľností, pričom CVSS skóre sa pohybuje od 3,7 po 10. Tri kritické zraniteľnosti súvisia s knižnicou Apache Log4j v2. Ďalšie tri zraniteľnosti nazývané ICMAD objavila spoločnosť Onapsis a ovplyvňujú podnikové aplikácie SAP používajúce ICM (Internet Communication Manager).

Závažné zraniteľnosti VMWare produktov

Spoločnosť VMWare opravila 4 zraniteľnosti týkajúce sa produktov ESXi, Workstation a Fusion, ktoré zneužívajú najmä USB radiče a službu settingsd. Zraniteľnosti sú vysokej závažnosti a ich CVSS skóre sa pohybuje od 8,2 do 8,4.

Kritické zraniteľnosti Cisco

V produktoch Cisco bolo opravených 5 kritických a viacero závažných zraniteľností.
CVE-2022-20699: Zraniteľnosť v module SSL VPN smerovačov Cisco Small Business RV340, RV340W, RV345 a RV345P Dual WAN Gigabit VPN by mohla umožniť neoverenému vzdialenému útočníkovi spustiť ľubovoľný kód na postihnutom zariadení.

CVE-2022-20700 a ***CVE-2022-20701***: Viaceré zraniteľnosti vo webovom rozhraní správy smerovačov Cisco Small Business série RV by mohli umožniť vzdialenému útočníkovi povýšiť oprávnenia na administrátorské.
CVE-2022-20703: Zraniteľnosť vo funkcii overovania obrazu softvéru smerovačov Cisco Small Business série RV by mohla umožniť neoverenému miestnemu útočníkovi nainštalovať a spustiť obraz škodlivého softvéru alebo spustiť nepodpísané binárne súbory na postihnutom zariadení.
CVE-2022-20708: Zraniteľnosť vo webovom rozhraní správy zariadení Cisco Small Business RV340, RV340W, RV345 a RV345P Dual WAN Gigabit VPN by mohla umožniť neoverenému vzdialenému útočníkovi zadávať a vykonávať ľubovoľné príkazy v systéme.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Intel® Kernelflinger, Intel® Quartus®, 2021.2 IPU - Intel® Chipset Firmware, 2021.2 IPU – BIOS, Intel® PROSet/Wireless Wi-Fi, Intel® AMT Wireless a Killer™ Wi-Fi Software a Intel® AMT. Úspešným zneužitím týchto zraniteľností môže dôjsť k eskalácii privilégií, úniku informácií alebo narušeniu dostupnosti služby.

Mesačník zraniteľností Február 2022

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 Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné závažné zraniteľnosti
    - Kritická zraniteľnosť Samba umožňuje vzdialene vykonávať kód
    - Spoločnosť SAP vydala februárové záplaty – opravuje 19 zraniteľností
    - Závažné zraniteľnosti VMWare produktov

https://www.csirt.gov.sk/posts/2768.html?csrt=6423770656639699689