MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Január 2022

Vypracoval: CSIRT.SK

TLP: White

Spoločnosť Kaspersky 20. januára 2022 oznámila, že výskumníci odhalili tretí prípad bootkitu s názvom MoonBounce pre firmvér UEFI (Unified Extensible Firmware Interface). MoonBounce bol prvýkrát spozorovaný na jar 2021, pričom so značnou istotou bol pripísaný skupine útočníkov APT41. Jedná sa o čínsky hovoriacich útočníkov, ktorí sú známi minimálne od roku 2012.

Na rozdiel od FinFisher a ESPecter, ktoré sa zameriavajú na EFI System Partition (ESP), novoobjavený rootkit – spolu s LoJax a MosaicRegressor – sa zameriava na flash pamäť SPI, čo je nevolatilné externé úložisko. Oproti dvom predošlým bootkitom (LoJax, MosaicRegressor) sa MoonBounce javí ako pokročilejší, komplikovanejší a tiež sofistikovanejší.

Kód firmvéru UEFI je zodpovedný za spustenie zariadenia a odovzdanie riadenia softvéru, ktorý načíta operačný systém. Ak firmvér obsahuje škodlivý kód, potom sa tento kód vykoná ešte pred spustením operačného systému, čo sťažuje jeho odstránenie. Nie je možné ho odstrániť preformátovaním pevného disku ani preinštalovaním operačného systému.

MoonBounce bol nájdený v UEFI komponente s názvom CORE_DXE. Tento komponent inicializuje dátové štruktúry a funkčné rozhrania, ktoré sú potom volané inými ovládačmi DXE.

Pôvodný vektor infekcie UEFI zatiaľ nie je známy, avšak spoločnosť Kaspersky zistila, že útočník pridal škodlivý kód a ovládač režimu jadra do novovytvorenej časti v kompromitovanom obraze firmvéru, aby sa zmocnil zavádzania infikovaného počítača.

Výskumníci spoločnosti Kaspersky taktiež odhalili niekoľko škodlivých zavádzačov a post-exploitačných malvérov, napríklad ScrambleCross, Sidewalk, Mimikat_ssp alebo Microcin. Útočníci v rámci kampane vykonávali archiváciu súborov, zhromažďovanie informácií o sieti a podobne. Zdá sa, že ich cieľom bol laterálny pohyb, exfiltrácia údajov a tiež špionážna činnosť. Celú správu z objavenia tohto bootkitu, jeho podrobnejší popis a indikátory kompromitácie nájdete na tejto webovej stránke.

Firma Binarly v nezávislej analýze poznamenala, že MoonBounce bol vytvorený pre hardvér súvisiaci so systémom MSI z roku 2014, a že malvér mohol byť do napadnutého stroja doručený buď fyzickým prístupom, alebo následnými úpravami softvéru, ktoré vyplynuli z nedostatku adekvátnej ochrany SPI.

Medzi hlavné odporúčania, ktoré vydala spoločnosť Kaspersky na ochranu pred bootkitmi UEFI ako je napríklad MoonBounce sú pravidelná aktualizácia firmvéru UEFI, používanie firmvéru od dôveryhodných predajcov a povolenie Secure Boot (najmä BootGuard a Trust Platform Modules - TPM, ak je to možné).

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci január riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Jednotka riešila tiež prípady kompromitovaných e-mailových schránok zamestnancov niekoľkých verejných organizácií v Slovenskej republike, ktoré útočníci ponúkali na predaj na internetových obchodoch. Stretla sa aj so sofistikovaným phishingovým útokom s pravdepodobným cieľom získať citlivé údaje z cieľovej organizácie. Útočníci podvrhli odosielateľa ako zahraničnú štátnu organizáciu, o čom sme informovali príslušnú jednotku CSIRT.

Významnú rolu v januári zohrala aj kampaň šíriaca malvér Trickbot. Jednotka informovala inštitúcie, ktorých infraštruktúra komunikovala s IP adresami zariadení infraštruktúry Trickbot. Preverenie ukázalo, že vo všetkých prípadoch komunikácia predstavovala iba pokusy o prístup na webové služby z internetu a neboli odhalené stopy vedúce k podozreniu na infekciu.

CSIRT.SK zaznamenal aj prípad ransomvéru, ktorý infikoval niekoľko pracovných staníc a aspoň jeden server verejnej organizácie.

Jednotka v januári informovala svoju konštituenciu o viacerých závažných zraniteľnostiach, ktoré odhalila pri svojej proaktívnej činnosti alebo jej boli nahlásené. Jednalo sa o zraniteľnosti kategórie SQL injection a cross-site scripting na webových stránkach organizácií, zraniteľnosti CMS platforiem a sieťových bezpečnostných prvkov, či možnosť prístupu ku súborovému systému zariadení vystavených do internetu. CSIRT.SK riešil tiež prípad zneužitia zraniteľnosti vedúceho ku prieniku na mailserver a rozposielaniu spamových emailov. Po reštartovaní servera a nainštalovaní aktualizácií sa útok neopakoval. Únik údajov nebol potvrdený.

V rámci svojej proaktívnej činnosti jednotka zdieľala so svojou konštituenciou indikátory kompromitácie malvéru WhisperGate a Trickbot, či informáciu o oprave kritických a závažných zraniteľností produktov spoločnosti Microsoft. 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

Nový malvér s názvom SysJoker sa zameriava na operačné systémy Windows, MacOS a Linux

Výskumníci zo spoločnosti Intezer objavili nový backdoor s názvom SysJoker, ktorý sa zameriava na Windows, MacOS ale aj Linux. Malvér je schopný vyhnúť sa detekcii na všetkých troch operačných systémoch. Napísaný je v jazyku C++. SysJoker zhromažďuje informácie o stroji pomocou príkazov Living off the Land (LOtL). Na zaznamenávanie výsledkov príkazov používa rôzne dočasné textové súbory. Malvér si vytvára perzistenciu v systéme pridaním nového kľúča do registrov. Taktiež komunikuje s C&C serverom.

Webová stránka ShopGoodwill.com obsahovala zraniteľnosť, čo malo za následok vystavenie údajov

Americká nezisková organizácia Goodwill sa stala obeťou úniku údajov. Zraniteľnosť na webovej stránke ShopGoodwill.com spôsobila, že sa útočníci dostali k osobným údajom, čo ovplyvnilo účty zákazníkov tohto elektronického obchodu. Spoločnosť však potvrdila, že neunikli žiadne informácie o platobných kartách. Vystavené údaje zahŕňali meno, priezvisko, emailovú adresu, telefónne číslo a poštovú adresu. Zraniteľnosť, ktorá spôsobila vystavenie týchto osobných údajov, bola podľa organizácie opravená.

Útočníci napadli webové stránky verejných ukrajinských inštitúcií

Webové stránky patriace rôznym ukrajinským verejným inštitúciám boli napadnuté a následne uvedené do režimu offline. Medzi dotknuté inštitúcie patria ministerstvo zahraničných vecí, pôdohospodárstva, školstva a vedy, bezpečnosti a obrany a online portál kabinetu ministrov. V dôsledku masívneho kybernetického útoku dočasne nefungovali webové stránky týchto inštitúcií, pričom mohli obsahovať

správu, ktorá informovala o tom, že všetky údaje o občanoch boli kompromitované. Polícia však potvrdila, že v dôsledku týchto útokov neboli ohrozené žiadne osobné údaje, a že cieľom týchto správ bolo vystrašiť občanov. Napadnutých bolo 15 webových stránok, ktoré boli zraniteľné voči CVE-2021-32648.

Ransomvér White Rabbit je spájaný so skupinou útočníkov FIN8

Nedávne výskumy ukázali, že za novou rodinou ransomvéru White Rabbit by mohli stáť útočníci z APT skupiny FIN8. Ransomvér sa šíri pomocou malého súboru o veľkosti 100kB a vyžaduje zadanie hesla na dešifrovanie škodlivého obsahu. Po spustení ransomvér prehľadá všetky priečinky a zašifruje súbory, pričom vytvára súbory s informáciou o výkupnom s názvom test.txt.scrypt.txt. Pri šifrovaní vynecháva systémové priečinky, aby sa predišlo znefunkčneniu operačného systému. Útočníci sa vyhrážajú zverejnením alebo predajom ukradnutých údajov. Ransomvér využíva verziu backdooru Badhatch (Sardonic), ktorý je spájaný práve so skupinu FIN8.

Malvér BHUNT sa zameriava na krádež kryptopeňaženiek

Spoločnosť Bitdefender objavila nový malvér BHUNT, ktorý kradne kryptopeňaženky. Zameriava sa na obsah, heslá a bezpečnostné frázy. Malvér je zabalený a šifrovaný použitím Themida a VMProtect, čo bráni analytikom vykonávať reverzné inžinierstvo a analýzu. Malvér je podpísaný digitálnym podpisom ukradnutým od spoločnosti Piriform. BHUNT je injektovaný do explorer.exe a do napadnutého systému je pravdepodobne doručený pomocou KMSpico, čo je nástroj na nelegálnu aktiváciu produktov od spoločnosti Microsoft. Najviac infikovaných používateľov je z Indie, avšak zasiahnutý je celý svet.

Útoky typu „watering hole“ prekvapili návštevníkov webovej stránky prodemokratickej rozhlasovej stanice v Hongkongu

Nový malvér DazzleSpy sa zameriava na používateľov operačného systému MacOS a návštevníkov webovej stránky prodemokratickej rozhlasovej stanice v Hongkongu pomocou útokov typu „watering hole“. Útok tohto typu zahŕňa infikovanie legitímnej webovej stránky malvérom, ktorý sa zameriava na demografické údaje stránky a v niektorých prípadoch na konkrétne IP adresy. Webová stránka obsahuje škodlivý prvok iframe, ktorý mieri na doménu kontrolujúcu verziu OS a postupuje do ďalšej fázy, ktorá načíta škodlivý Javascript kód. Zneužívaná je zraniteľnosť CVE-2021-1789 v prehliadači Safari verzie nižšej ako 14.1.

Webová stránka internetového obchodu Segway obsahovala škodlivý skript Magecart

Internetový obchod Segway sa stal obeťou útoku. Obsahoval škodlivý skript Magecart, ktorý umožňoval útočníkom ukradnúť informácie o zákazníkoch a ich platobných kartách. Útočníci kompromitovali webovú stránku – do internetového obchodu pridali JavaScript kód, ktorý predstieral, že zobrazuje autorské práva stránky. Skript však načítal externý favicon, ktorý obsahoval škodlivý skript na krádež údajov z platobnej karty. Spoločnosť Malwarebytes tvrdí, že útočníci zodpovední za tento útok sú súčasťou skupiny Magecart Group 12, ktorá kradne údaje o kartách minimálne od roku 2019.

Červený kríž utrpel útok, ktorého dôsledkom bola krádež údajov o viac ako 515-tisíc ľuďoch

Medzinárodný výbor Červeného kríža (International Comittee of the Red Cross – ICRC) sa stal obeťou kybernetického útoku. Útočníci ukradli údaje viac ako 515-tisíc ľudí z programu „Restoring Family Links“, ktorý pomáha zjednotiť rodiny rozdelené vojnou, katastrofou alebo migráciou. Medzinárodný výbor Červeného kríža vyzval útočníkov, aby nezverejňovali, nezdieľali, nepredávali ani nepoužívali ukradnuté

údaje, keďže patria ľuďom, ktorí už trpia a sú veľmi zraniteľní. Nie je známe, kto vykonal útok na spoločnosť uchovávajúcu ich údaje. Počas vyšetrovania útoku boli systémy a webová stránka programu uvedené do režimu offline.

Fínsko čelilo phishingovému útoku na Facebook Messenger a infikovaniu zariadení spywarom Pegasus

Zariadenia fínskych diplomatov boli infikované spywarom Pegasus v rámci kyberšpionážnej kampane. Po kompromitácii zariadení z nich útočníci mohli kradnúť dáta. Údaje prenášané alebo uložené v telefónoch diplomatov sú buď verejné, alebo sú utajované na najnižšej úrovni utajovaných skutočností, avšak niektoré informácie môžu podliehať diplomatickej dôvernosti. Špionáž na týchto diplomatov je vraj už ukončená. Fínsko taktiež čelilo phishingovým podvodom cez Facebook Messenger, ktoré mohli viesť ku krádeži účtov.

Malvér pre Android s názvom BRATA bol obohatený o funkcie ako sledovanie GPS a iné

Malvér pre Android BRATA obohatil svoje funkcie o sledovanie GPS, schopnosť používať viacero komunikačných kanálov a o funkciu, ktorá je schopná vykonať obnovu továrenských nastavení na vymazanie stôp útočníka. Malvér bol prvýkrát zaznamenaný v roku 2019. Najnovšie verzie sa zameriavajú na používateľov elektronického bankovníctva vo Veľkej Británii, Poľsku, Taliansku, Španielsku a ďalších krajinách. Vyhľadáva prítomnosť antivírusového riešenia na zariadení a pokúša sa vymazať bezpečnostné nástroje predtým, ako exfiltruje dáta. Obnovu továrenských nastavení útočníci vykonávajú po úspešnej kompromitácii alebo po zistení, že aplikácia beží vo virtuálnom prostredí.

Po útoku na Finalsite bolo uvedených do režimu offline približne 5-tisíc webových stránok škôl

Poskytovateľ služieb školským webovým stránkam Finalsite sa stal obeťou útoku ransomvéru. Dôsledkom bolo narušenie prístupu k webovým stránkam tisícok škôl po celom svete. Útok zabránil školám odosielať upozornenia ohľadom zatvorenia kvôli počasiu alebo koronavírusu. Bezpečnostný tím Finalsite identifikoval prítomnosť ransomvéru na určitých systémoch v rámci siete. Poskytovateľ služieb okamžite podnikol kroky na zabezpečenie systémov a zabránenie činnosti ransomvéru. Vypol svoje systémy, aby zabránil šíreniu útoku, čo malo za dôsledok, že približne 5-tisíc školských webových stránok bolo uvedených do režimu offline. Neexistujú žiadne dôkazy o kompromitácii údajov.

- **Malvér pre iOS môže predstierať vypnutie alebo reštart zariadenia za účelom sledovania kamery alebo mikrofónu.**
- **Bankový malvér Zloader zneužíva overovanie podpisu od spoločnosti Microsoft na injektovanie kódu do podpísanej systémovej DLL knižnice.**
- **Verejný zdravotnícky systém Broward Health sa stal obeťou útoku, ktorý zasiahol viac ako 1,3 milióna jedincov.**
- **Chemická spoločnosť Element Solutions sídliaca na Floride utrpela kybernetický útok.**
- **Portugalská spoločnosť Grupo Impresa sa stala obeťou skupiny „Lapsus$“, ktorá zaútočila na jej online služby.**
- **Služba Flexbooker potvrdila únik údajov, ktorý zahŕňal informácie o viac ako 3,7 miliónoch účtov.**
- **Ransomvér Night Sky sa zameriava na podnikové siete.**
- **Online lekáreň Ravkoo so sídlom v Spojených štátoch sa stala obeťou úniku údajov.**

- **Spoločnosť QNAP varuje pred ransomvérom, ktorý sa zameriava na vystavené NAS zariadenia.**
- **Malvér FluBot sa aj naďalej vyvíja – nové kampane distribuujú malvér ako Flash Player.**
- **Nákupná platforma PulseTV potvrdila potenciálny únik údajov, ktorý sa týka 200-tisíc ľudí.**
- **Škodlivý inštalačný súbor pre Telegram distribuuje malvér Purple Fox.**
- **UScellular potvrdil únik údajov po útoku na fakturačný systém.**
- **Botnet Abcbot je prepojený so skupinou Xanthe.**
- **Medical Review Institute of America (MRIoA) sa stal obeťou útoku, ktorý ohrozil údaje 134-tisíc ľudí.**
- **Ransomvér TellYouThePass sa znovu objavil a zameriava sa na viac operačných systémov.**
- **Kampaň GootLoader sa zameriava na infikovanie zariadení zamestnancov právnických a účtovných spoločností malvérom.**
- **Microsoft varuje pred deštruktívnym malvérom na vymazávanie dát, ktorý sa maskuje ako ransomvér používaný pri útokoch proti viacerým organizáciám na Ukrajine.**
- **Módny gigant Moncler potvrdil únik údajov po útoku ransomvéru BlackCat.**
- **Marketingová spoločnosť RRD potvrdila krádež údajov pri útoku ransomvéru Conti.**
- **Obchodovacia platforma Crypto.com potvrdila napadnutie 483 účtov, pričom bolo ukradnutých 34 miliónov dolárov.**
- **Stránka OpenSubtitles sa stala obeťou úniku údajov 7 miliónov používateľov.**
- **Emotet používa nekonvenčné formáty IP adries, aby sa vyhol detekcii.**

Závažné zraniteľnosti bežných softvérových produktov

Spoločnosť Microsoft opravila 97 zraniteľností, z toho 9 kritických a 6 zero-day

Spoločnosť Microsoft vydala balík opráv Patch Tuesday, v ktorom opravila 97 zraniteľností. Deväť z nich bolo označených ako kritické a 88 ako závažné. Až 6 z týchto zraniteľností je typu zero-day. Zneužitím týchto zraniteľností môže dôjsť napríklad k vzdialenému vykonaniu kódu, eskalácii privilégií alebo narušeniu dostupnosti služby. Avšak jedna z najnovších aktualizácií pre Windows Server (KB5009624, KB5009557 a KB5009555, KB5009566 a KB5009543) spôsobuje problémy s doménovými radičmi. Preto je potrebné zvážiť jej nasadenie.

PwnKit – závažná zraniteľnosť vyskytujúca sa v predvolených inštaláciách rôznych distribúcií Linuxu

Závažná zraniteľnosť PwnKit (CVE-2021-4034), ktorá sa môže vyskytovať vo všetkých distribúciách Linuxu, môže viesť k eskalácii privilégií až na oprávnenia root. Nachádza sa v programe pkexec komponentu PolicyKit, ktorý je možné použiť na vykonávanie príkazov s právami používateľa root.

Spoločnosť Apple vydala bezpečnostné záplaty, ktorých súčasťou je oprava zero-day zraniteľnosti

Spoločnosť Apple vydala bezpečnostnú záplatu (iOS 15.3 a macOS Monterey 12.2), ktorá opravuje viacero zraniteľností – medzi nimi je aj CVE-2022-22587. Apple uvádza, že táto chyba mohla byť aktívne zneužívaná. Súvisí s poškodením pamäte v komponente IOMobileFrameBuffer, čo by mohlo viesť k vzdialenému vykonaniu kódu s oprávneniami jadra.

Kritické zraniteľnosti Cisco

V produktoch Cisco bolo opravených 7 kritických a viacero závažných zraniteľností. Prvé 4 súvisia s knižnicou Apache Log4j2.
CVE-2021-44228: Funkcie JNDI Apache Log4j2 nechránia pred útočníkom kontrolovaným LDAP a inými koncovými bodmi súvisiacimi s JNDI.
CVE-2021-44832: Apache Log4j2 Thread Context Message Pattern a Context Lookup Pattern sú zraniteľné voči DoS útoku.
CVE-2021-45046: Apache Log4j2 nie vždy chráni pred nekonečnou rekurziou pri vyhodnocovaní vyhľadávania.
CVE-2021-45105: Apache Log4j2 je zraniteľná voči RCE cez JDBC Appender, keď útočník riadi konfiguráciu.
CVE-2022-20648: Zraniteľnosť vo funkcii ladenia pre Cisco RCM pre softvér Cisco StarOS by mohla umožniť neoverenému vzdialenému útočníkovi vykonať akcie ladenia, ktoré by mohli viesť k sprístupneniu dôverných informácií, ktoré by mali byť obmedzené.
CVE-2022-20649: Zraniteľnosť v Cisco RCM pre softvér Cisco StarOS by mohla umožniť neoverenému vzdialenému útočníkovi vzdialene vykonať kód v aplikácii s rootovskými oprávneniami v kontexte nakonfigurovaného kontajnera.
CVE-2022-20658: Zraniteľnosť vo webovom rozhraní správy Cisco Unified Contact Center Management Portal (Unified CCMP) a Cisco Unified Contact Center Domain Manager (Unified CCDM) by mohla umožniť overenému vzdialenému útočníkovi povýšiť svoje oprávnenia na správcu.

Mesačník zraniteľností Január 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
    - Spoločnosť Microsoft opravila 97 zraniteľností, z toho 9 kritických a 6 zero-day
    - PwnKit – závažná zraniteľnosť vyskytujúca sa v predvolených inštaláciách rôznych distribúcií Linuxu

https://www.csirt.gov.sk/posts/2733.html?csrt=15600245697994209535