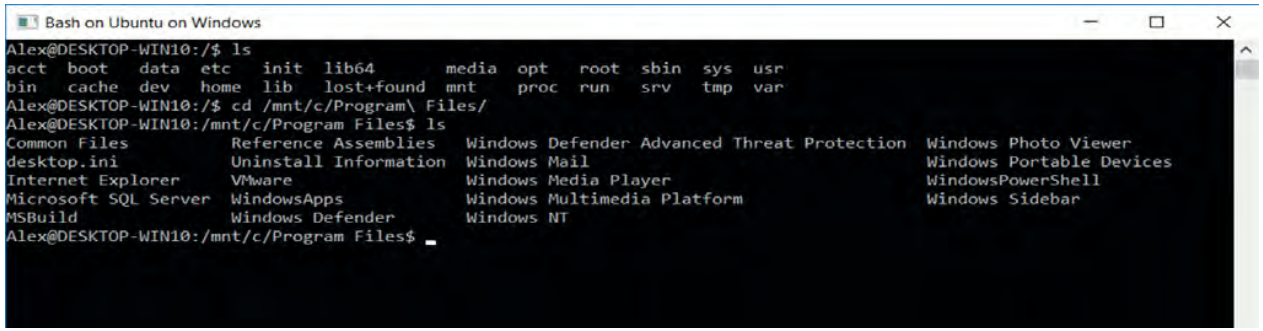
Nová hrozba Windows 10 umožňuje obejít antivirové programy

Nedávno objevená metoda útoku nazvaná bashware umožňuje obejít většinu antivirových programů. Jak velké riziko představuje a jak se může běžný uživatel bránit?

Microsoft vydal před nedávnem aktualizaci svého systému Windows 10 Fall Creators Update, ve které zpřístupnil funkci Subsystem for Linux (WSL), která byla doposud pouze betaverzí. Jedná se o nástroj, díky kterému mohou uživatelé spustit textové uživatelské rozhraní bash známé z linuxových operačních systémů. Tato funkce zjednoduší práci především vývojářům, kteří již nebudou nuceni testovat své programy na virtuálních strojích a budou moci využívat aplikace a nástroje z linuxového prostředí. To však se sebou přináší závažné bezpečnostní nedostatky.



Obr. 1: Terminálové okno bash na Windows

Výzkumný tým společnosti Check Point Software Technologies objevil novou metodu útoku zvanou „bashware“, díky které může útočník spustit jakýkoli známý malware právě pod WSL tak, aby nebyl detekovaný žádným běžným antivirovým softwarem, kontrolními nástroji nebo anti-ransomwarovými programy. [1] Útok se týká všech zařízení s operačním systémem Windows 10. Od podzimní verze Fall Creators Update je prostředí WSL dostupné (v dřívějších verzích pouze jako betaverze), ale ve výchozím nastavení je vypnuté. Přesto se Check Pointu podařilo najít způsob, jak WSL zapnout a bez vědomí uživatele spustit malware.

Linux na Windows bez virtualizace

Windows Subsystem for Linux poskytuje linuxové prostředí vedle klasického desktopového prostředí Windows. Nemá žádné grafické rozhraní, práce v něm se provádí pomocí příkazového řádku, tzv. bash, který je nejoblíbenější variantou příkazového řádku (terminálu) na linuxových systémech. Jak vypadá bash na Windows si můžete prohlédnout na obr. 1.

Vývojáři a správci operačních systémů, pro které je tato funkce primárně určena, mohou díky ní využívat linuxové nástroje (nmap, scp, awk atd.), pracovat s interprety programovacích

jazyků (např. Perl, Python) nebo spouštět linuxové aplikace. Stále ale mají k dispozici běžný systém Windows. Oproti hostování systému na virtuálním stroji má WSL značnou výhodu, protože nevyžaduje takové požadavky na výkon fyzického stroje. Z prostředí WSL lze také přistupovat k souborům systému Windows po připojení disku (nejčastěji C:\) do linuxového prostředí, čímž jsou všechny soubory přístupné v obou prostředích. [2]

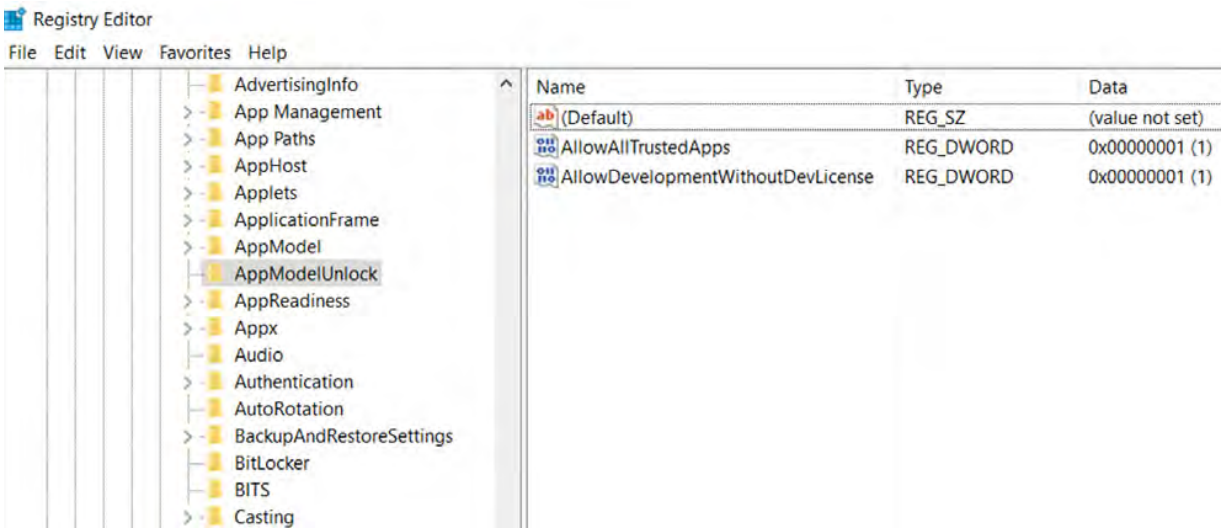
Jak obejít antivirus ve čtyřech krocích

Metoda útoku pojmenovaná bashware využívá WSL k tomu, aby spustila malware skrytým způsobem, který antivirové programy nedokážou v současné době detekovat. Funkce WSL je ve výchozím stavu vypnutá a pro její zapnutí je potřeba mít povolený vývojářský mód (tzv. developer mode). Samotný útok je rozdělený do čtyř fází. V prvním kroku se načtou komponenty WSL, dále se povolí vývojářský mód, ve třetí fázi se nainstaluje linuxové prostředí do WSL a v poslední části útoku se spustí wine proces, pod kterým poběží malware určený pro Windows.

Prvotním cílem útočníka je zjistit, jestli je na cílovém počítači spuštěná funkce WSL. Přítomnost souborů lxcore.sys a lxss.sys v adresáři ovladačů zařízení indikuje aktivní funkci WSL. Pokud soubory přítomny nejsou, funkce je vypnutá a útočník pomocí nástroje Deployment Image Service and Management (DISM) načte příslušné ovladače. K provedení tohoto kroku je potřeba, aby útočník disponoval právy lokálního administrátora. Dále je vše prováděno na pozadí a bez vědomí uživatele. Bashware poté načte komponenty potřebné ke správné funkčnosti WSL a je připraven na další krok.

Subsystem for Linux byl doposud v betaverzi, proto pro jeho spuštění bylo potřeba mít aktivovaný vývojářský mód. V nejnovější verzi Windows 10 1709 (Fall Creators Update) už to nutné není, takže pokud útočník narazí na tuto verzi, nemusí

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModelUnlock\AllowAllTrustedApps
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModelUnlock\AllowDevelopmentWithoutDevLicense



Obr. 2: Nastavení klíčů v registrech pro povolení developer módu

se spouštěním vývojářského módu zabývat. Pro dřívější verze systému výzkumníci z Check Pointu zjistili, že stačí nastavit dva klíče v registrech systému Windows, aby se stal mód aktivním. Změna nastavení registrů vyžaduje práva lokálního administrátora a změnu může provést uživatel nebo aplikace, která disponuje těmito právy. Bashware ponechá klíče změněné jen po dobu provádění škodlivých akcí, poté je vrátí na výchozí hodnotu.

K zapnutí developer módu je potřeba nastavit hodnotu DWORD na 1 pro dva klíče (viz obr. 2).

Na pozadí se poté vyhledá a nainstaluje balíček pro developer mód. Následně je vyžadován restart počítače. To pro útočníka disponujícího právy lokálního admina není problém, může buď restartovat počítač ručně a „natvrdo“, nebo zobrazit uživateli hlášku, ve které bude žádost o restartování počítače z důvodu např. „instalace aktualizací“.

Nyní je WSL i vývojářský mód zapnutý. Dalším krokem je stáhnutí a instalace souborového systému pro Linux. K tomu slouží příkaz Lxrun s parametrem /install. Útočník spustí Lxrun.exe, ten stáhne systém Ubuntu 16.04 a nainstaluje ho do WSL. Tento proces nevyžaduje práva lokálního administrátora, je legitimní a běží na pozadí.

Nyní má útočník k dispozici plně připravené linuxové prostředí vedle systému Windows. Aby mohl spustit malware určený pro systémy Windows, musí nainstalovat program, který umožní programům určeným pro Microsoft Windows běžet

na operačních systémech založených na Linuxu. Jedním ze zástupců těchto „emulátorů“ je program Wine.

Útočník nainstaluje Wine do systému WSL (nejsou potřeba práva lokálního administrátora) a provede konverzi malwaru ve formátu EXE (klasický formát spouštěcích souborů na Windows) programem Wine tak, aby mohl být malware spuštěn v linuxovém prostředí. Všechny systémové příkazy, které malware vykoná, budou speciálními ovladači převedeny na windowsovské systémové příkazy a budou vykonány v systému Windows. Systém Windows vidí, že příkazy přicházejí z WSL, což je legitimní aplikace, takže nepovažuje její chování za škodlivé. Tímto způsobem může útočník spustit např. ransomware, který zašifruje všechny soubory na počítači, aniž by byl detekován antivirovým programem.

Pico procesy

Abychom mohli správně porozumět tomu, proč může být aktivita malwaru pomocí této techniky utajená před antivirovými a jinými bezpečnostními programy, musíme si vysvětlit, jak funguje překlad příkazů z Windows na Linux a zpět.

Pokud se podíváme na problematiku podrobněji, základem téměř každého programu je možnost využívat funkce operačního systému. Žádost o využití těchto funkcí se nazývá systémové volání. Na operačních systémech Microsoft Windows poskytuje podobné funkce Windows API.

Spustitelné soubory v operačních systémech Windows mají obvykle formát EXE, v linuxových systémech ELF (Executable and Linkable Format). Oba formáty jsou navzájem nekompatibilní, takže bylo potřeba vymyslet způsob, jak ve Windows spustit ELF soubory. Za tímto účelem byly vytvořeny tzv. pico procesy.

Pico procesy jsou „kontejnery“ pro spouštění ELF souborů na Windows. Systémové volání pocházející od ELF souboru je pomocí pico providera (poskytovatele) předáno ovladačům lxcore.sys a lxss.sys, které přeloží linuxové systémové volání do rozhraní Windows API a z pohledu ELF souboru emulují jádro systému Linux – kernel. Tímto způsobem jsou přeložená systémová volání z WSL do Windows, což umožňuje spouštět linuxové programy pomocí WSL na Windows. [3]

Antiviry bashware nedetekují, ale proč?

Microsoft si po vydání betaverze WSL uvědomil, že existují některé scénáře, kdy uživatel nebo škodlivý program může obejít zabezpečení systému Windows, např. antivirový program nebo bránu firewall tím, že spustí malware pod systémem WSL. Antivirové programy nedokážou monitorovat chování aplikace spuštěné v systému WSL. Uživatelé, kteří tuto funkci v beta testování zkoušeli, požadovali možnost zakázat ve WSL přístup k internetu, omezit nebo úplně zakázat přístup k určitým souborům a složkám, nebo dokonce znemožnit instalaci funkce WSL.

Microsoft na jejich požadavky odpověděl vydáním Pico API, rozhraním, které mohou výrobci bezpečnostního softwaru využít k monitorování pico procesů a ke splnění výše uvedených požadavků. [4] Ačkoli je toto rozhraní dlouhou dobu dostupné, většina antivirových společností tuto funkci do svých produktů ještě nezakomponovala.

Co vše může útočník napáchat ve firmě?

Získá-li útočník přístup ke koncové stanici, je to samozřejmě problém. Když se na to ale podíváme s nadhledem, správně fungující společnost s dostatečnými bezpečnostními mechanismy by mělo být těžké ohrozit kvůli kompromitaci koncové stanice.

Všechna důležitá data by měla být na serverech, na něž by běžný uživatel neměl mít přístup. Takže samotná možnost obejití antiviru na koncové stanici nemusí být pro firemní síť tak vážným problémem. Pravidelně se však ve firmách setkáváme se špatně nastavenými bezpečnostními postupy. Uživatelé jsou na svých počítačích přihlášeni pod účtem, který má přístup také na servery, administrátoři k běžné práci využívají účet doménového administrátora apod.

Jakmile útočník získá přístup ke koncové stanici, odvíjí se riziko od typu uživatele, který je na zařízení přihlášen. Pokud se jedná o běžného uživatele, který nedisponuje žádnými vyššími oprávněními, útočník má omezené možnosti. Může spustit např. ransomware a zašifrovat vše, k čemu má uživatel přístup. Pozor na to, že uživatel může mít přístup také ke sdíleným diskům. Pokud má právo zapisovat, může ransomware zašifrovat i data na sdílených discích. K využití bashwaru je

potřeba práv lokálního admina, takže můžeme předpokládat, že útočník jimi disponuje. S tímto oprávněním je již infikovaná stanice plně v moci útočníka. Může se dostat ke všem souborům na počítači nebo odchytávat síťovou komunikaci.

Má-li útočník při průniku do sítě štěstí a kompromituje stanici, na které je přihlášený uživatel s právy doménového administrátora, dopad útoku na firemní síť se rapidně zvyšuje. Útočník může vyextrahovat otisky hesel ze systému a získat přístupové údaje, díky kterým se dostane do všech systémů v síti.

Přestože se útočník dostane „pouze" na stanici, kde je přihlášený klasický uživatel, riziko získání práv doménového administrátora přetrvává. Zásahem do systému, který způsobí chybu, může uživatele donutit, aby zavolal na firemní helpdesk a vyžádal si vzdálenou pomoc. Administrátoři se často kvůli pohodlnosti připojují přes účet doménového admina, a tím vystavují tento účet riziku kompromitace. Pokud se tímto účtem administrátor připojí na koncovou stanici např. pomocí funkce vzdálené plochy, útočník opět může získat heslo a využít ho stejným způsobem jako v předchozím případě.

Je-li útočník schopný a má znalosti sociálního inženýrství (předpokládejme, že obě vlastnosti splňuje), dříve nebo později získá ta správná oprávnění, protože po celou dobu svého útoku není monitorován bezpečnostním softwarem instalovaným na koncové stanici, a má tak téměř neomezený čas.

Jak moc je hrozba reálná?

Pokud se na problém bashwaru podíváme z pohledu útočníka, je tato metoda přesně tím, čeho chce dosáhnout. Útočník není kontrolovaný antivirovým programem a veškerá jeho činnost, resp. činnost malwaru, je před antivirem skryta. Samozřejmě existují i jiné metody, jak antivirové programy obejít. Jsou ovšem velmi náročné a ne vždy se útočníkovi jeho počínání podaří. Dnešní bezpečnostní software má totiž skvělé sebeobranné funkce. Proto může tato technika útočníkovi velmi usnadnit práci.

Antivirový program	Detekce při stahování (wget)	Detekce při přístupu (cat, nano)
Avast Internet Security	✓	✗
ESET Internet Security	✓	✓
McAfee Total Protection	✗	✗
Microsoft Windows Defender	✓	✓

Tab. 1: Test detekce vybraných antivirových programů

K tomu, aby mohl útočník bashware využít, musí nejdříve zapnout vývojářský mód (týká se všech verzí do Windows 10 Fall Creators Update). Ten je ve výchozím nastavení vypnutý a k jeho zapnutí je potřeba oprávnění lokálního admina. Pro motivovaného útočníka, který disponuje penězi i časem, není problém tato práva získat. Často útočníci zneužívají špatně nakonfigurované služby třetích stran nebo chybějící patche. Na jaře se objevil ransomware WannaCry, který využíval zranitelnosti způsobené chybějícím patchem MS17-010. Tato zranitelnost umožňovala získat práva lokálního admina a ještě dnes se s ní stále setkáváme. Zkrátka existují způsoby, jak může útočník získat práva, díky kterým zapne vývojářský mód.

Druhý nutný předpoklad je ten, že koncová stanice poběží na Windows 10. Ačkoli jsou desítky mezi námi již přes dva roky, firmy na ně přecházejí spíše pomaleji. Současný podíl Windows 10 mezi operačními systémy činí necelých 30 % (výzkum společnosti Net Applications, září 2017), takže šance, že útočník narazí na stanici s Windows 10, je 1:3. Navíc se s každou novou verzí Windows zvyšuje zabezpečení operačního systému, takže fakt, že WSL je funkce dostupná až ve Windows 10, je další překážkou.

Různé názory na problematiku

Může se zdát, že některá vyjádření k tomuto riziku jsou zbytečně zveličená. Podle vyjádření na blogu společnosti Check Point, která tuto metodu útoku objevila, ze dne 11. září 2017, se jedná o „alarmující metodu, která umožňuje jakémukoli známému malwaru obejít dokonce i nejběžnější bezpečnostní řešení". Jak již bylo uvedeno, je potřeba najít stanici se správným operačním systémem a poté získat práva lokálního admina k využití této metody útoku.

Podle portálu The Register i samotný Microsoft tvrdí, že hrozba představuje pouze malé riziko pro uživatele systému Windows 10. Poukazuje na to, že je nutné nejdříve zapnout vývojářský mód (který je ve výchozím nastavení vypnutý), poté nainstalovat potřebné komponenty, restartovat počítač a nainstalovat WSL.

Stejný názor na rizikovost útoku bashware zastává i antivirový výrobce Trend Micro. Ve svém prohlášení na webu z 18. září 2017 uvádí, že útok je možný pouze za velmi specifických podmínek, přesto dodává, že by uživatelé neměli brát žádnou hrozbu na lehkou váhu.

Testování detekce

V době, kdy společnost Check Point vydala zprávu popisující techniku bashware, nedokázala „většina předních antiviro-

vých a bezpečnostních produktů na trhu“ malware skrytý metodou bashware detekovat. My jsme se při testování zaměřili na produkty určené pro domácí uživatele. Vybrali jsme tři společnosti, které mají podle výzkumu společnosti OPSWAR ze září 2017 na trhu s antivirovými produkty největší zastoupení – Avast, ESET a McAfee. Dále jsme do testování zahrnuli i vestavěný Windows Defender společnosti Microsoft.

Jako testovací jsme vybrali soubor eicar.com.txt, který obsahuje textový řetězec určený pro testování antivirových programů. Není nijak nebezpečný, ale antiviry ho detekují jako virus. Nejdříve jsme zjišťovali, jestli je antivirový program schopný detekovat stažení souboru pomocí příkazu wget. Druhá metoda testovala detekci při práci se souborem pomocí příkazů cat a nano. Výsledky testování jsou zobrazeny v tabulce 1 na předchozí straně.

Důvodem, proč některé produkty detekují škodlivý soubor pouze při stahování, může být, že mají implementovánu funkci pro kontrolu síťové komunikace, která pochází právě z WSL, ale nikoli celé rozhraní Pico API.

Podle výsledků našeho testování je zřejmé, že výrobci bezpečnostních řešení již začali s úpravou svých produktů tak, aby zajistili monitorování pico procesů, a tím udělali metodu bashware neúčinnou. Samozřejmostí je, že Windows Defender od Microsoftu umí malware detekovat, protože samotný Microsoft je výrobcem WSL a rozhraní Pico API.

Riziko tu je, ale...

Jak vyplývá z názorů odborné veřejnosti a předních výrobců bezpečnostních řešení, většina z nich je velmi skeptická, co se týče tohoto útoku. V první řadě bychom si měli říct, že bashware není zranitelností. Funkce WSL je naprogramována správně a důvod, proč je tato metoda útoku možná, je ten, že výrobci bezpečnostních řešení se dostatečně nevěnovali zabezpečení této funkce. Bashware sám o sobě neotevírá vrátka útočníkovi, „pouze“ mu ulehčuje práci a bezpečnostním týmům ztěžuje detekci.

Jakmile antivirové společnosti implementují bezpečnostní mechanismy, které budou monitorovat pico procesy, bashware již nebude mít budoucnost, protože ho zachytí každý antivirový nebo jiný bezpečnostní program.

Jak se může uživatel bránit v tuto chvíli?

Do doby, než váš bezpečnostní software bude schopen detekovat útok touto metodou, není žádná stoprocentní ochrana. Check Point ukázal, že i když je vývojářský mód vypnutý, útočník ho dokáže zapnout a poté nainstalovat komponenty potřebné pro spuštění WSL. [1] Pokud výrobce vašeho bezpečnostního řešení ještě nestihl implementovat ochranu do svých produktů, nezbývá vám nic jiného než čekat. V nejbližší době by měly mít všechny antivirové společnosti ve svých produktech obsažené rozhraní pro ochranu před malwarem spuštěným přes WSL.

Jako uživatelé však můžeme útočníkovi ztížit nebo téměř znemožnit získání potřebných práv pro zapnutí developer módu. Řiďme se obecnými bezpečnostními pravidly: používat aktualizovaný antivirový program, pravidelně aktualizovat operační systém a programy třetích stran, neotevírat podezřelé soubory a nevyžádané e-maily, používat dostatečná hesla. Tímto způsobem minimalizujeme riziko jakéhokoli útoku, nejen pomocí metody bashware.

Závěr

Možnost obejít antivirový program je pro útočníka velmi lákavá, avšak k využití bashwaru vede dlouhá cesta s překážkami. Zatím to nevypadá, že by technika bashware mohla způsobit závažné zvýšení počtu útoků na uživatele. Navíc bychom se během relativně blízké doby měli dočkat aktualizovaných antivirových programů a jiných bezpečnostních řešení schopných tuto metodu detekovat a zablokovat. Někteří výrobci již tuto funkci do svých produktů přidali.

David Pecl
David.Pecl@aec.cz

David Pecl

Bezpečnostní specialista se zaměřením na ochranu koncových stanic a serverů ve společnosti AEC a.s. V současné době se věnuje také detekci zranitelností a oblasti mobilní bezpečnosti.

POUŽITÉ ZDROJE

[1] ELBAZ, Gal a Dvir ATIAS. Beware of the Bashware: A New Method for Any Malware to Bypass Security Solutions [online]. [cit. 2017-10-12]. Dostupné z: https://research.checkpoint.com/beware-bashware-new-method-malware-bypass-security-solutions
[2] COOLEY, Sarah. Windows Subsystem for Linux Documentation [online]. [cit. 2017-10-12]. Dostupné z: https://msdn.microsoft.com/en-us/commandline/wsl/about
[3] HAMMONS, Jack. Pico Process Overview [online]. [cit. 2017-10-12]. Dostupné z: https://blogs.msdn.microsoft.com/wsl/2016/05/23/pico-process-overview
[4] HAMMONS, Jack. WSL Antivirus and Firewall Compatibility [online]. [cit. 2017-10-12]. Dostupné z: https://blogs.msdn.microsoft.com/wsl/2016/11/01/wsl-antivirus-and-firewall-compatibility
[5] COOLEY, Sarah. Windows 10 Installation Guide [online]. [cit. 2017-10-12]. Dostupné z: https://msdn.microsoft.com/en-us/commandline/wsl/install_guide