ZAPLAŤ, NEBO SVÁ WINDOWS UŽ NIKDY NEUVIDÍŠ!

Vydírání, krádež dat: Telefonát vystrašeného čtenáře přiměl speciální tým Chipu čelit **EXTRÉMNĚ NEBEZPEČNÉMU TROJSKÉMU KONI**. Ten by brzy mohl zaútočit na mnoho dalších počítačů – třeba i na ten váš.

PETR KRATOCHVÍL, MARKUS HERMANNSDORFER

Praha, 13:00 místního času. Speciální tým Chipu přijal vystrašený telefonát. Zoufalý pan K. nás informoval o neznámém vyděrači, který zašifroval jeho disk s Windows a zároveň s ním i firemní data v hodnotě desítek tisíc korun. Vyděrač od pana K. očekával zaslání otřesně drahé „premium SMS“, po jejímž obdržení mu zašle „uvolňovací kód“, pomocí něhož by mohl být „ukořistěný“ disk s Windows opět rozšifrován. Náš úkol byl jasný: Zjistit, pomocí jakého algoritmu zločinec zašifroval disk, znovu získat přístup k disku a k firemním datům, identifikovat a usvědčit vyděrače a nakonec zabezpečit počítač pana K. před podobnými útoky v budoucnu. Na konci tohoto článku navíc najdete tipy, jak ochránit svůj vlastní počítač.

Analýza: Šifrování Windows

Praha, 14:30 místního času. Dorazili jsme na místo zločinu, do centrály malé dopravní společnosti se sídlem v Praze. Pan K. bootoval svůj počítač, ale v místě přihlašovacího okna se objevila zpráva od vyděrače v ruském jazyce. Kdyby panu K. nepomohl jeden z jeho řidičů, pocházející z oblasti východní Evropy, nikdy by požadavky pachatele nepochopil.

My jsme požádali o pomoc ruského specialistu na problematiku virů Igora Danilova, více známého pod pseudonymem Dr. Web. Ten nám nabídl další informace o škůdci v počítači pana K.: „Mohl by to být ‚Trojan.Winlock.20‘, zcela nový trojský kůň z kategorie ransomwaru (vyděračský software). Tento malware má jen jediný cíl: získání výkupného.“ Naštěstí pan Danilov už celou řadu podobných problémů řešil. I tak byl ale nepříjemně překvapen: „Až dosud se tento trojský kůň objevoval pouze v rusky mluvících oblastech. Jak se dostal do České republiky?“ Na **http://news.drweb.com**, webových stránkách specialisty na antiviry, jsme našli on-line formulář vedoucí k řešení našeho problému, který byl naštěstí v angličtině. Jednoduše jsme vložili číslo SMS ze zprávy vyděrače a obdrželi jsme, zcela zdarma, dva kódy, pomocí nichž by Windows mohla být znovu rozšifrována. Fungovalo to. Jakmile byl kód vložen, počítač pana K. začal normálně fungovat. Nebezpečí však ještě nebylo odvráceno – škůdce se stále schovával na disku.

S pomocí pana Danilova jsme však i tento problém bez námahy vyřešili. Ze všeho nejdříve jsme deaktivovali přístup k Ovládacím panelům, abychom zabránili viru v „restartování“. Pokud by měl pan K. na svém počítači nainstalovaná Windows XP Professional, šlo by vše provést jednoduše pomocí group policies. Na jeho počítači s verzí „Home“ jsme si však museli pomoci zásahem do registrů. Po kliknutí na »Start | Run« a zadání „regedit“ jsme přešli na klíč »HKEY_CURRENT_USER\Software\Microsoft\Windows\Policies\Explorer«.

Zde jsme vytvořili novou hodnotu DWORD s názvem „NoControlPanel“ a údaj hodnoty jsme nastavili na „1“. Poté jsme restartovali počítač a během bootování stiskli klávesu [F8] a zvolili „Safe mode“. Pak jsme znovu přešli do

registrů. Podle specialisty známého pod zkratkou „Dr. Web“ právě zde vir vložil nový klíč, který musí být vymazán manuálně. V sekci »HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\“Userinit“« jsme vymazali všechny položky typu „%Temp%\don[accidental string].tmp“. Následně jsme znovu spustili Windows v „běžném“ modu a nejprve jsme odstranili výše uvedenou položku v registrech, bránící přístupu k Ovládacím panelům. Tímto způsobem jsme tedy škůdce eliminovali a mohli jsme přejít k dalšímu bodu.

Hledání: Jak vir pronikl do počítače?

Digitální škůdci, kteří proniknou na disk, většinou pocházejí z pochybných webových stránek nebo ze souborů pocházejících z P2P sítí. Zeptali jsme se pana K., zda navštívil stránky typu **www.cracks.am**, nebo zda dokonce používal programy typu Azureus. On to popíral: „Podle mého to je pro firemní počítač příliš nebezpečné.“ Na počítači nechyběl virový skener a firewall, aktivována byla i automatická aktualizace Windows. To znamená, že počítač pana K. byl vcelku slušně zabezpečen a škůdce musel do systému proniknout jinou cestou.

Všechny informace jsme si ještě ověřili pomocí nástroje BTF Sniffer (najdete ho i na DVD), který slouží k odhalování a mazání stop. Výhodou je, že tento nástroj může být spuštěn i přímo z USB, bez nutnosti instalace. Abychom získali co možná nejpřesnější obrázek o aktivitách na počítači pana K., aktivovali jsme v levé části programu všechny položky a následně jsme zvolili příkaz »File | Export all items in a text document«. Ten zajistí, že BTF-Sniffer zapíše do textového souboru každý detail o provozu počítače. Tak lze zjistit, které soubory byly otevřeny, které aplikace byly instalovány (případně kam) nebo které webové stránky byly navštíveny. Objevili jsme aktivity z USB flash disku společnosti Imation, ale pan K. si byl jistý, že nevlastní žádné zařízení od této firmy. Proto jsme chtěli zjistit podrobnější informace o USB disku: především kdy a jak často byl připojen k počítači. Tyto informace dokáže odhalit například nástroj USBDeview (také na Chip DVD). Jakmile je program spuštěn, nástroj zobrazí všechna rozpoznaná USB zařízení, bez ohledu na to, zda jsou právě připojená, nebo ne. USBDeview nám prozradil nejen „písmeno“ přiřazené USB disku, ale i jeho sériové číslo, a co je nejdůležitější, i dobu, kdy byl USB disk připojen.

V našem případě měl zobrazený časový údaj hodnotu „10:26:22“ a datum jen jeden den před úderem trojského koně. Pan K. nás ujistil, že v ten den a danou dobu byl na obchodním jednání daleko mimo společnost. V té chvíli už jsme věděli vše o infiltraci trojského koně na počítač: během nepřítomnosti pana K. někdo připojil USB disk k počítači a následně zkopíroval škůdce na disk. Zbýval nám už jen kousek k odhalení vyděrače.

Identita: Podezřelý bude odhalen

Pro následující krok je nutné mít připravené nezbytné nástroje. Stálo při nás i štěstí – shodou náhod se nám dostal do ruky i inkriminovaný disk: uklízečka ho nalezla v odpadkovém koši v opuštěné kanceláři. Do popředí seznamu možných motivů se tak dostala i pomsta uživatele kanceláře, který byl nedávno propuštěn. Pomocí důkladného vyšetřování jsme se pokusili zajistit veškeré důkazy a ukázat, jaký postup pachatel použil. Bylo tedy načase prozkoumat jeho počítač v opuštěné kanceláři...

Ochrana: Nejprve jsme bootovali podezřelý počítač pomocí Deft Linux Live CD **(www.deft-linux.net)**, založeného na Ubuntu. V BIOS jsme určili DVD mechaniku jako „First Boot Device“. Po restartu Deft nejdříve nabízí výběr jazyka, poté je do bootovací obrazovky nutné zadat „deft-gui“, aby se Linux spustil s grafickým uživatelským rozhraním. Jakmile se systém aktivoval, spustili jsme „Partition Editor“, abychom určili, které písmeno Linux přiřadil disku podezřelého. Bylo indikováno jako „sda1“. Nyní jsme si museli z tohoto datového média vytvořit tzv. forenzní zálohu, určenou pro soud. Touto metodou jsou zkopírovány dokonce i prázdné oblasti; nemění se také „časová značka“ stávajících souborů. Připojili jsme k počítači USB disk, jehož velikost byla dostačující k uložení zkopírované partition.

Poté jsme se z Partition Editoru přepnuli na „Terminal“. Zde jsme připojili disk pomocí příkazu

```
Mount•/dev/sdb1 •/mnt
```

Ve forenzní záloze zdroj nebyl explicitně integrován, aby eliminoval náhodný zápisový přístup. Pomocí následujícího příkazu jsme zkopírovali disk podezřelého na náš USB disk:


```
dcfldd•if=/dev/sda1 of=/mnt/image.dd•
bs=4096•conv=noerror,sync
```

Prostřednictvím instrukce „bs=4096“ Linux čte a píše ve velkých blocích o 4 096 bajtech; záloha je tedy vytvořena rychle a bez jakýchkoli chyb. Poslední parametr nakonec chrání kopírovací proces před tím, aby byl přerušen v případě načtení chybných dat.

Analýza: Pátrali jsme po důkazech ve forenzní záloze. Pomocí následujícího příkazu v terminalu se zajistí, že disk nezůstane „viset“ v systému Linux:

```
mount
```

Spustili jsme nástroj Autopsy (**www.sleuthkit.org/autopsy/**) a „založili jsme“ nový případ. Přiřadili jsme mu jméno a znovu jsme ho potvrdili pomocí příkazu »New case«. Když jsme přidali „hostitele“, nezměnili jsme žádné parametry; pouze jsme vše dvakrát potvrdili pomocí tlačítka »Add Host«. Následně jsme přidali „image“ naší forenzní zálohy (/mnt/image/dd) pomocí příkazu »Add Image | Add Image file« a aktivovali jsme volby „Disk“, „Symlink“ a Volume Image“.

Pomocí kontrolního součtu MD5 si Autopsy dokáže ověřit úplnost kopie. Proto jsme

aktivovali »Calculate the hash value for this image« a nezapomněli jsme ani na volbu »Verify hash after importing«. U soudu je kontrolní součet v podstatě důkazem, že forenzní kopie byla vytvořena přesně podle pravidel. Image disku jsme připojili kliknutím na »Add«. Tento proces chvíli trvá, a to především kvůli ověřování kontrolního součtu. Po obdržení zprávy o úspěšném ověření jsme začali shromažďovat důkazy použitím příkazu »Analyze«.

Jak přesně proces analýzy probíhá, to záleží na spáchaném trestném činu. V našem případě jsme podezřelého chtěli usvědčit ze stažení trojského koně z webových stránek a z jeho zkopírování na USB.

Na podezřelém počítači jsme tedy pomocí nástroje „File Analysis“ hledali důkazy o navštívených stránkách a našli jsme HTML soubory, které směřovaly k Russian Bussines Network (specializovaná ruská obchodní síť) i k WSLabi, což je jakýsi eBay v oblasti bezpečnostních mezer a jejich zneužívání. Podezřelý si škůdce koupil právě na této stránce.

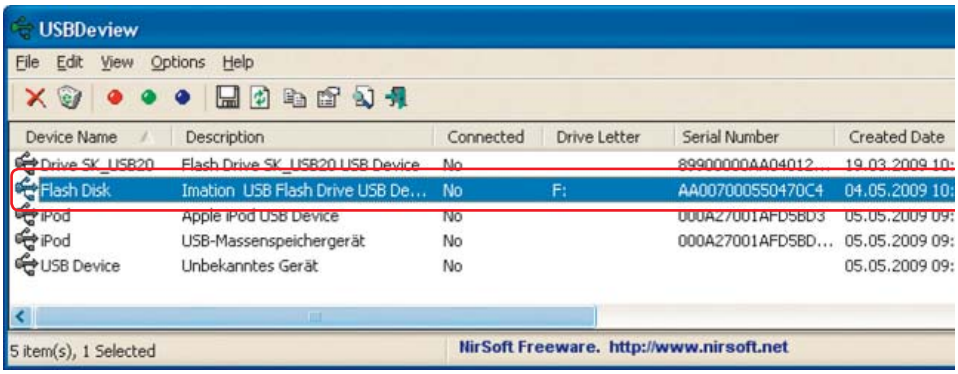
Záznamy jsme si nahráli pomocí textového editoru „Gedit“. V Autopsy jsme pomocí příkazu »File Activity Timelines | Create Data File« zjistili podrobnější informace o zvoleném časovém období – tedy kdy a co podezřelý dělal.

Po vybrání naši forenzní zálohy „image.dd“ jsme ještě museli přesně určit požadované časové období. Autopsy sestaví časovou linku aktivit se všemi detaily. Zaznamenány jsou například datum, čas, název a velikost získaného souboru, ID uživatele a skupiny. Nechybí ani „typicky unixovská“ poznámka o typu souboru. Jednotlivá písmena například znamenají:

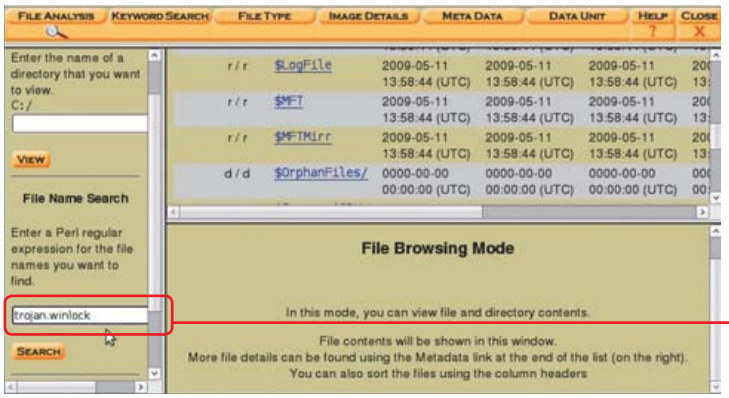
(m) modified – upravený;
(a) accessed – zpřístupněný;
(c) changed – změněný;
(b) newly created – nově vytvořený.

Autopsy všechna tato data zaznamená do textového souboru.

Tímto způsobem jsme shromáždili všechny důkazy. Už jsme tedy věděli, kdy a kam podezřelý zkopíroval libovolný soubor a také odkud trojský kůň pocházel. Aby pan K. mohl svému právníkovi poskytnout přesné detaily trestného činu, připravili jsme navíc data do speciálně navržené prezentace.



Odhalený: Na počítači oběti jsme našli záznam o použití neznámého USB flash disku.



Vyšetřování: Pomocí nástroje Autopsy jsme hledali stopy po trojském koni.

Po vybrání naši forenzní zálohy „image.dd“ jsme ještě museli přesně určit požadované časové období. Autopsy sestaví časovou linku aktivit se všemi detaily. Zaznamenány jsou například datum, čas, název a velikost získaného souboru, ID uživatele a skupiny. Nechybí ani „typicky unixovská“ poznámka o typu souboru. Jednotlivá písmena například znamenají:

(m) modified – upravený;
(a) accessed – zpřístupněný;
(c) changed – změněný;
(b) newly created – nově vytvořený.

Autopsy všechna tato data zaznamená do textového souboru.

Tímto způsobem jsme shromáždili všechny důkazy. Už jsme tedy věděli, kdy a kam podezřelý zkopíroval libovolný soubor a také odkud trojský kůň pocházel. Aby pan K. mohl svému právníkovi poskytnout přesné detaily trestného činu, připravili jsme navíc data do speciálně navržené prezentace.

ZPRACOVÁNÍ: Pro prezentace nenabízejí Autopsy či Deft Linux žádnou přijatelnou volbu, proto jsme museli použít nástroj Powerbullet Presenter (najdete ho i na našem DVD). Tento program je podobný PowerPointu od Microsoftu, oproti němu má však velkou výhodu: jakmile je prezentace vytvořena, může být snadno zkonvertována do EXE souboru pomocí příkazu

```
File | Export
```

Tento soubor pak může být spuštěn na libovolném počítači, aniž by na něm byl nainstalován software pro prezentace. Nástroj ukládá tento soubor do složky „Dokumenty\Powerbullet“, odkud jsme jej zkopírovali na USB disk. Pan K. pak už nemusí udělat nic jiného než připojit disk k počítači svého právníka a spustit prezentaci...

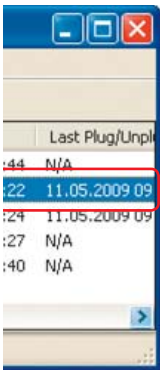
Zabezpečení: Vylepšení ochrany před sabotáží

Praha, 16.10 místního času. Odstranili jsme trojského koně, vypátrali jsme pachatele, odhalili jsme taktiku jeho zločinu a shromáždili jsme všechny důkazy tak, aby jim porozuměl i technicky méně zdatný právník či soudce. Zbývalo už udělat jen jedinou věc: zabezpečit počítač pana K. před podobnými útoky i do budoucna.

OCHRANNÁ ROZHRANÍ: Nejdříve ze všeho jsme zabezpečili USB port, protože právě zde má napadený počítač slabé místo. Mnoho kancelářských počítačů umožňuje omezení použití USB zařízení už v BIOS, což ale není případ počítače pana K. Museli jsme tedy použít nástroj DeviceLock **(www.devicelock.com)**, jehož 30denní trial verzi najdete například na **http://download.chip.eu/cz/download_cz_4388264.html**.

Plná verze programu s cenou 32 eur se nám zdá příliš drahá, ale pan K. neváhal, neboť data jeho společnosti mají podstatně větší hodnotu. Během instalace navolil všechna rozhraní, ke kterým umí DeviceLock regulovat přístup. Pod nabídkou »Lock automatically« lze zvolit například ochranu disketových mechanik, vyjímatelných disků, CD/DVD mechanik, USB portů nebo zařízení Windows Mobile. Po instalaci lze specifikovat přesné detaily přístupu v nabídce »Device Lock Service Settings Editor«.

Například při nastavení přístupu k USB portům uživatel zvolí nabídku »Device Lock Service | Devices | Permissions« a dvojitým kliknutím myší na »Removable« definuje uživatele, den a čas, kdy smí uživatel připojit zařízení k USB.



Vyděrač: Ruský trojský kůň „Winlock" učiní Windows nefunkčními a poté vyžaduje výkupné.

Čmuchal: Deft Linux obsahuje speciální forenzní nástroje, jako například Autopsy, Ophcrack nebo Nessus.

Zde lze také definovat, zda bude možné ze zařízení pouze číst, nebo na něj zapisovat, nebo z něj dokonce instalovat programy. Tímto způsobem lze řídit přístup ke všem zařízením u počítačů ve firmě. Vlastní USB disk je možné vyloučit z kontroly pomocí funkce „USB Device White List".

BLOKOVÁNÍ HACKERSKÝCH CD/DVD: Nástroj DeviceLock dokáže ochránit rozhraní počítače pouze tehdy, když je spuštěn operační systém Windows. Proti útoku hackerů pomocí speciálních „live CD" typu Ophcrack je ještě nutné nastavit v BIOS bootování pouze z pevného disku a celé nastavení chránit pomocí hesla. Pak může bootovací sekvenci a změny v BIOS provádět pouze pan K.

ŠIFROVÁNÍ DISKU: Šikovný hacker či vir se i přes všechna tato opatření může do počítače dostat. Je tedy vhodné přichystat další „překážku" – například všechna důležitá data na disku zašifrovat pomocí nástroje TrueCrypt (na Chip DVD). To lze provést například takto: Zvolte příkaz »System | Encrypt System Partition/Drive« a v průvodci vyberte »Encrypt the Windows System Partition | Single Boot«. V následném testu vám TrueCrypt zobrazí dobu požadovanou pro šifrování pomocí různých algoritmů integrovaných v programu.

Pro běžný domácí počítač lze použít „obyčejné" AES, které funguje přibližně s 43 MB/s. Pro firemní data se však doporučuje středně rychlá „AES-Twofish" (21 MB/s), protože je mnohem obtížnější ji „cracknout". Poté musí být ještě zvoleno heslo a vytvořeny dva přístupové klíče. Další krok „Rescue Disk" by neměl být přeskočen z jednoho velmi dobrého důvodu: dotaz na heslo k dešifrování disku je uložen v bootovacím sektoru datového média. V případě, že je sektor poškozen, není možné datové médium dešifrovat. Řešením tohoto problému je právě záchranné médium.

POKRYTÍ VŠECH BEZPEČNOSTNÍCH MEZER: Nakonec je nutné zabezpečit všechny mezery, které by mohly počítač ohrozit kvůli tzv. Zero-Day-Exploits. Tito škůdci na počítače útočí dříve, než bezpečnostní firmy vyvinou odpovídající „protijed". Naše ochrana se skládá ze dvou částí: Secunia Personal Software Inspektor (PSI) aktualizuje všechny stávající aplikace, jakmile se objeví známá bezpečnostní mezera. Druhá komponenta je známá jako bugging operation (odposlouchávací operace) – ta monitoruje všechny soubory a složky v síti a spustí alarm, jakmile v nich dojde k podezřelým změnám. Oba tyto programy jsou k dispozici na našem DVD.

Praha, 18:00 místního času. Speciální tým Chipu dokončil svou práci. Pan K. dodá svému právníkovi zabezpečené důkazy spolu s prezentací a díky optimálně nastavené komplexní bezpečnosti se nemusí obávat dalšího vydírání.

AUTOR@CHIP.CZ

Ochrana proti ransomwaru

Trojské koně, které se pokouší získat kontrolu nad vaším diskem, zašifrovat ho a za jeho dešifrování získat peníze, se označují jako „ransomware" (ransom je v angličtině výkupné). Těchto škůdců existuje celá řada – z těch známějších lze jmenovat například AIDS. trojan, Troj_PGPCoder.A a také námi v článku popsaný Trojan.Winlock. Podle bezpečnostních odborníků bude ransomware „hitem" příštího roku, kdy se počítačové mafie zaměří na menší a střední podniky. Na rozdíl od běžných uživatelů jsou už totiž dostatečně bohaté, zároveň však (oproti velkým firmám) obvykle nemají propracovanou IT strategii pro boj s podobnými hrozbami.

CRYZIP PRVNÍ A DRZÝ

Klasickou ukázkou fungování ransomwaru byl již jeden z jeho prvních rozšířenějších „zástupců". Škůdce známý pod jménem CryZIP (objeven v roce 2005 v laboratořích WebSense) se po proniknutí do počítače „rozhlédl", vybral si na první pohled nejdůležitější soubory (texty, tabulky, zdrojové kódy, archivy…) a přístup k nim zašifroval. Mimořádně drzé bylo použití existujícího šifrování archivů „ZIP" – útočník si ušetřil práci s vytvářením vlastního algoritmu. Nikdo už pravděpodobně nezjistí, kolik obětí zaplatilo výkupné ve výši 300 USD, nicméně jisté je, že řádění tohoto škůdce trvalo téměř rok.

VYDĚRAČI NIKDY NEODPOVÍDEJTE

Pokud je váš počítač napaden výše zmiňovaným škůdcem, nikdy boj nevzdávejte předem a neposílejte vyděrači peníze. Použijte záchranné CD s prohlížečem nebo jiný počítač a navštivte weby bezpečnostních firem. Tam lze narazit na bezpečnostní kódy, které zachrání vaše data i bez kontaktu s vyděračem. Zároveň tam také obvykle najdete instrukce, jak se škůdců zcela zbavit. Poté, co se vám to povede, použijte naše DVD a zabezpečte si počítač tak, aby se situace neopakovala. Zajímavé informace o ransomwaru lze najít například i na webu zmiňovaného Dr. Weba: **http://news.drweb.com/show/?p=1&c=5&lng=en&i=352**.

Tip: Pokud ransomware napadne váš počítač a zašifruje pouze vybrané soubory, existuje poměrně snadné řešení. Poté, co škůdce vybrané soubory zašifroval, musel je ihned smazat. Pokud tedy použijete kvalitní nástroj na obnovu smazaných dat a budete mít štěstí, můžete se vyděrači rovnou vysmát…