Analýza malware pro CSIRT

Případová studie FLAB

Popis situace

Uživatelé organizace Cypherfix, a. s. jsou cílem podvodných zpráv elektronické pošty obsahujících v příloze spustitelný kód pro MS Windows. Tyto zprávy jsou doručeny do více než tří tisíc schránek firemní elektronické pošty během nedělního večera.

Následující pracovní den někteří uvědomělí uživatelé hlásí uživatelské podpoře doručení podezřelé zprávy a žádají instrukce. Bezpečnostní tým organizace (CSIRT) zjišťuje, že se jedná o podvodnou zprávu s prvky psychologického nátlaku na uživatele (sociální inženýrství), aby otevřel přílohu. Dále zjišťuje, že po spuštění souboru z přílohy dochází ke kompromitaci pracovní stanice, přičemž antivirové řešení poštovního serveru ani antivirové řešení koncových stanic neidentifikuje soubor jako závadný. Je tedy pouze na uživatelích, zda podlehnou nátlaku sociálního inženýrství a přílohu spustí. CSIRT se pouští do standardního procesu reakce na tento typ incidentu, k čemuž potřebuje mimo jiné i řadu informací týkajících se souboru v příloze.

Sami členové CSIRT však nemají dostatek volných kapacit k provedení analýzy a také se nejedná o rutinní případ, se kterým by měli dostatečné zkušenosti, proto kontaktují forenzní laboratoř sdružení CESNET.

Forenzní laboratoř FLAB

Při prvním telefonickém kontaktu jsou pracovníci forenzní laboratoře (FLAB) seznámeni s mimořádnou situací v organizaci Cypherfix, a. s. a následně probíhá úvodní konzultace. Zejména je zjišťováno, jaké informace a jak rychle CSIRT tým musí získat a jaké elektronické podklady je schopen dodat k analýze. Také je prodiskutován plán reakce na incident a podle toho konkretizovány otázky, na které mají být v rámci analýzy elektronických podkladů hledány odpovědi. Součástí je i domluva na způsobu předání elektronických podkladů.

V dalším kroku dochází k sepsání zadání (viz Příloha A) , ze kterého je zřejmé, jaké elektronické podklady byly dodány a jaké informace potřebuje organizace získat. Jsou také doplněny další relevantní informace. S jasně formulovaným zadáním se pracovníci FLAB pouštějí do práce.

Rozbor cílů

Během úvodní konzultace, probírání plánu reakce na incident a vytváření zadání bylo konstatováno, že v případě podezření na nákazu malwarem mnoha koncových stanic je potřeba nalézt informace pro realizaci následujících kroků:

- **Zamezení dalšího šíření**. Pro zastavení dalšího šíření malware technickými prostředky je nutné analyzovat průběh nákazy. Vlastní virová báze organizací používané antivirové ochrany sice malware nepozná, ale umožňuje přidat vlastní definice. Bohužel každý uživatel dostal rozdílnou přílohu a není možné pro ně vytvořit obecné pravidlo. Je však možné, že všechny doručené přílohy po spuštění provádí vždy stejné aktivity, které lze blokovat.

- **Identifikace napadených stanic**. Po zastavení útočného vektoru vzniká v dalším kroku potřeba identifikovat všechny napadené pracovní stanice, aby mohly být podrobeny nápravným opatřením. Kromě lokálních příznaků, tj. typicky změn v souborovém systému a změn v registrech, je vhodné identifikovat charakteristikou síťovou komunikaci s případnými dropzónami nebo C&C servery. Závadnou komunikaci může organizace následně vyhledat v provozně lokalizačních údajích, takže napadené stanice bude možné identifikovat bez nutnosti je fyzicky obcházet a kontrolovat.
- **Způsob nápravy**. Je třeba zjistit, jaké kroky je třeba podniknout k nápravě, tj. bezpečnému návratu napadených stanic a jejich uživatelů do běžného provozního stavu. Vzhledem k časové tísni nebude možné provést detailní analýzu činnosti malware a CSIRT tým tak bude při své reakci uvažovat také možnou kompromitaci hesel a dalších citlivých dat, která se nacházela na napadených pracovních stanicích nebo v informačních systémech, ke kterým bylo z pracovních stanic přistupováno.

Je zřejmé, že všechny informace je potřeba zjistit **ve velmi krátkém čase**, protože budou využity přímo k reakci na bezpečnostní incident.

Řešení

Zadání analýzy příloh podvodných zpráv forenzní laboratoři umožňuje bezpečnostnímu týmu napadené organizace Cypherfix, a. s. soustředit všechny své síly na reakci na bezpečnostní incident a současně přitom získat potřebné informace. Prvním krokem je informování uživatelů o nové hrozbě, což vyžaduje spolupráci CSIRT týmu s pracovištěm uživatelské podpory. Během hodiny od specifikace zadání přicházejí z forenzní laboratoře **první dílčí výsledky** – všechny analyzované přílohy pouze stahují a spouští stejný malware, podle zaslaných informací je tedy **možné upravit konfiguraci antivirového řešení** tak, aby bylo schopno blokovat závadnou činnost. Vzhledem k tomu, že používané řešení má centrální správu, je nové pravidlo ihned aplikováno na všech běžících pracovních stanicích a nebude tedy docházet k dalším kompromitacím tímto malwarem.

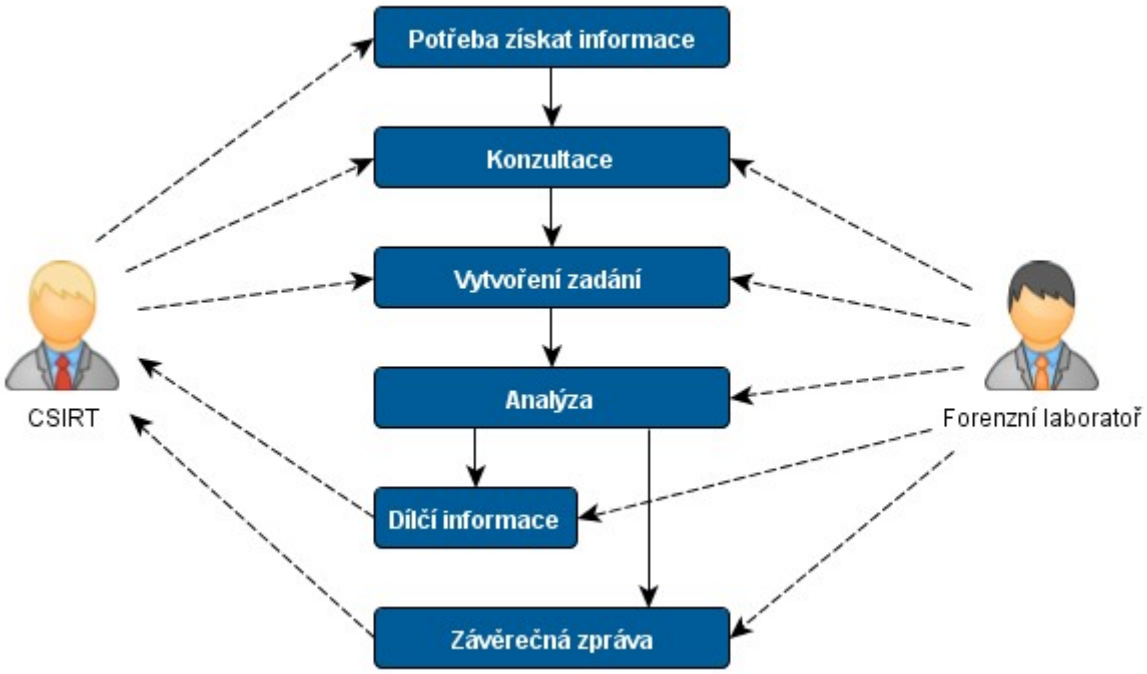
Během krátké doby je zodpovězena také druhá otázka, a to **jak identifikovat napadené pracovní stanice** – jsou identifikovány konkrétní změny v souborovém systému (nově vytvořené soubory) a změny v systémových registrech, kterými si malware chce zajistit své spuštění po restartu zařízení. Každý uživatel nebo správce pracovní stanice si tak může sám ověřit, zda byla kompromitována. Dále je předán seznam IP adres, se kterými se analyzované soubory snažily po spuštění komunikovali. Vzhledem k tomu, že síť organizace je monitorována systémem pro sběr NetFlow dat, jsou potřebné údaje k dispozici. CSIRT tým tedy může vytvořit seznam stanic i jejich uživatelů, seřadit je podle důležitosti a pustit se do části nápravných opatření. Ukazuje se, že podlehlo velmi mnoho uživatelů a počet kompromitovaných stanic násobně přesahuje běžně řešené bezpečnostní incidenty.

Během dalších dvou hodin je předána závěrečná zpráva (viz příloha B) obsahující odpovědi na všechny položené otázky, včetně postupu, kterým byly získány. Součástí je také **návod na odstranění nákazy** – jedná se o malware, který je omezen pouze na uživatelský profil, takže není nutná kompletní reinstalace. Forenzní laboratoř však upozorňuje, že není jisté, jaký další malware mohl být na jednotlivých pracovních stanicích mezitím stažen, protože obsah dropzóny a pokyny C&C serverů se mohou v čase měnit. CSIRT tým se rozhoduje, že kompromitované stanice zaměstnanců, které má IT oddělení ve své správě, přeinstaluje, ale v doporučení pro ostatní uživatele a správce nebude reinstalaci vyžadovat.

Výsledky

Pro profesionální reakci na bezpečnostní incident potřeboval CSIRT tým informace, které však nebyl schopen zjistit vlastními silami. Obrátil se tedy na forenzní laboratoř, pro kterou je analýza chování malware běžnou činností, takže potřebné informace byly dodány rychle a v potřebné kvalitě. Na jejich základě pak mohly být provedeny jednotlivé kroky – zabránění dalším kompromitacím vhodnou úpravou centrálně spravovaného antivirového řešení, identifikace všech pracovních stanic kompromitovaných tímto malwarem na základě dat z monitoringu sítě a vytvoření interních postupů pro nápravu.

Pro bezpečnostní tým znamenalo zadání analýzy forenzní laboratoři absolvování telefonické konzultace, během které bylo vytvořeno zadání, a předání několika vzorků malware. Následně pak už byly jen přijímány požadované informace – nejprve v průběhu analýzy jen dílčí zjištění a nakonec pak kompletní závěrečná zpráva. Spolupráce CSIRT a forenzní laboratoře je schematicky znázorněna na obrázku 1.



Obrázek 1: Schéma spolupráce

Příloha A: Zadání případu

Základní informace

Identifikační údaje o případu:

Identifikátor případu	20150229
Název případu	Analýza příloh e-mailu
Datum přijetí případu	29.2.2015

Kontaktní informace pracovníka FLAB:

Pracovník FLAB	Ing. Aleš Padrta, Ph.D.
E-mail	apadrta@cesnet.cz
Telefon	+420 234 680 280

Kontaktní informace zákazníka:

Zákazník	Ing. Jan Bezpečný, Cypherfix, a. s.
E-mail	jan.bezpecny@cypherfix.cz
Telefon	---

Specifikace případu

Detailní popis případu, specifikace otázek k zodpovězení.

Pozadí případu	Do schránek elektronické pošty byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr
Doplňující informace	Všechny soubory *.scr byly přeposlány pracovníkům FLAB.
Otázky k zodpovězení	1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace? 2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci? 3. Jak lze malware z napadených stanic odstranit?
Forma předání výstupu	Výsledkem analýzy bude závěrečná zpráva v elektronické formě. Dílčí zjištění mající vliv na řešení incidentu mohou být předávány průběžně elektronickou poštou nebo telefonicky.
Požadované datum pro	Výsledky analýzy budou použity při reakci na incident, výstupy je nutno předat

předání výstupu	co nejdříve.

Podklady předané k forenzní analýze

Všechny podklady byly přeposlány zákazníkem na e-mailovou adresu apadrta@cesnet.cz.

Elektronický podklad (Data)		Evidenční číslo	001
Jméno souboru	smlouva_3C2749066380959C.scr		
Hashe souboru	MD5: ee8f9d32821517719ad919186d0e6dfd SHA1: 689886edfbd21d7a2727ed1a1a87d1572ca6d0f4		
Čas zajištění	29.2.2015 7:32 GMT+1		
Popis	Příloha k analýze.		
Způsob získání	Doručeno do schránky elektronické pošty Organizace.		
Způsob předání	Přeposláno e-mailem.		
Poznámky	---		

Elektronický podklad (Data)		Evidenční číslo	002
Jméno souboru	smlouva_5D2741865381432B.scr		
Hashe souboru	MD5: 918ab1b8cb706e70951607a9c1b8fb23 SHA1: 58f130fac8dda92b1c4ddab293b20a48c4780404		
Čas zajištění	29.2.2015 7:34 GMT+1		
Popis	Příloha k analýze.		
Způsob získání	Doručeno do schránky elektronické pošty Organizace.		
Způsob předání	Přeposláno e-mailem.		
Poznámky	---		

Elektronický podklad (Data)		Evidenční číslo	003
Jméno souboru	smlouva_4B5414799705489F.scr		
Hashe souboru	MD5: 5e6cb4f13034abc863bf11b4f3c22622 SHA1: c80dbad08d1909ce432bc55dd5407a87ff1cc373		
Čas zajištění	29.2.2015 7:42 GMT+1		
Popis	Příloha k analýze.		
Způsob získání	Doručeno do schránky elektronické pošty Organizace.		

Způsob předání	Přeposláno e-mailem.
Poznámky	---

Příloha B: Závěrečná zpráva

Manažerské shrnutí

Předané soubory (přílohy podvodného e-mailu) byly podrobeny dynamické analýze, kdy bylo zjištěno, že se jedná o druh malware zvaný dropper (zajišťuje stažení a spuštění dalšího malware). Všechny analyzované soubory, byť mají jiné názvy a jsou binárně odlišné, provádějí stejnou činnost. Na základě zjištěných změn, které malware po svém spuštění provede a síťové aktivity, byl navržen postup pro úpravu pravidel antivirového systému, způsob lokální i vzdálené identifikace kompromitovaných stanic a také navržen postup pro odstranění malware.

Základní informace o případu

Do schránek elektronické pošty organizace byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr. Vzorky (soubory) byly předán pracovníkovi FLAB elektronickou poštou.

Zadavatelem a zároveň i kontaktní osobou pro další komunikaci je Ing. Jan Bezpečný, Cypherfix, a. s. (kontaktní e-mail: jan.bezpecny@cypherfix.cz).

Vstupem pro analýzu jsou tři binární soubory – přílohy podvodného e-mailu. Detailní informace jsou uvedeny v přiloženém zadání (zde Příloha A: Zadání případu).

Cílem zkoumání je analyzovat chování příloh po jejich otevření nebo spuštění a zodpovědět následující otázky:

1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace?
2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci?
3. Jak lze malware z napadených stanic odstranit?

Průběh analýzy

Vzhledem časové naléhavosti byla pro získání požadovaných informací zvolena dynamická analýza – otevřením nebo spuštěním souboru v kontrolovaném prostředí lze pozorovat změny provedené v systému a síťové aktivity i bez detailních znalostí o formátu a obsahu souboru. Pro tuto konkrétní analýzu bylo využito připravené standardní prostředí založené na nástrojích Process Monitor, Capture BAT, Wireshark s následným předzpracováním pomocí nástroje ProcDot.

Činnost malware

Všechny analyzované soubory vykazují naprosto stejné chování, rozdílné názvy a binární obsah slouží jen ke zkomplikování automatické detekce.

Po spuštění analyzovaných souborů dojde ke

- komunikaci s IP adresou `167.aaa.bbb.160`, ze které je stažen soubor a uložen na disk do

uživatelského profilu pod názvem `ate.exe` (MD5: c1fbce4c7ed62f2474d56cd4044a36df),

- ke spuštění souboru `ate.exe`.

Po spuštění souboru `ate.exe` dojde

- k zajištění persistenci zapsáním příslušné hodnoty do registrového klíče `HKCU\software\Microsoft\Windows\CurrentVersion\Run`,
- k nastavení koše (recycle bin) na neukládání smazaných souborů změnou registrového klíče `HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{vol-ID}`,
- ke snaze o překlad doménového jména `pxxxxxnet.com`,
- odeslání zprávy na IP adresu odpovídající výsledku překladu uvedeného doménového jména. V době testování šlo o IP `197.ccc.ddd.71`, ale cílová IP adresa se může v čase měnit (fast flux DNS). Bez dalších informací získaných např. ze systému PassiveDNS nelze určit IP adresu pro jiný čas.

Během doby testování neproběhla žádná další síťová komunikace. Dále bylo zjištěno, že pokud je zablokováno vytvoření souboru `ate.exe`, nedojde ke kompromitaci a proce je ukončen.

Vytvořené soubory

```
C:\Users\<username>\AppData\Local\Temp\ate.exe
```

Detekované změny v registrech

```
HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{vol-ID} ... NukeOnDelete=00000001

HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Run ... pchealth=C:\Users\<username>\AppData\Local\Temp\ate.exe
```

Síťová komunikace

```
http://167.aaa.bbb.160/~ate.exe
```

Všechny změny jsou prováděny pouze v rozsahu uživatelského profilu.

Detekce kompromitovaných pracovních stanic

Pro detekování stanic, které byly tímto malwarem napadeny, je možné použít následující možnosti:

- Z logu netflow
  - Navázání komunikace s IP adresou `167.aaa.bbb.160`
- Lokální změny
  - Existence hodnoty (v registrovém klíči `HKCU\...Current Version\Run`)

    `pchealth=C:\Users\<username>\AppData\Local\Temp\ate.exe`
  - Existence souboru

    `C:\Users\<username>\AppData\Local\Temp\ate.exe`

Náprava kompromitovaných pracovních stanic

Postup pro odstranění analyzovaného malware je následující:

1. Restartovat počítač a přihlásit se jako administrátor.
2. Navrátit změny, které malware provedl
   a) Zrušit celý profil napadeného uživatele a vytvořit mu nový
   b) Ručně vrátit změny v registrech a smazat vytvořené soubory

Vzhledem k tomu, že činnost malware byla analyzována jen v krátkém časovém úseku a jeho veškerá činnost jakožto i případné další pokyny z C&C nejsou známy, lze doporučit přeinstalování celého zařízení.

Shrnutí

Všechny analyzované přílohy vykonávají shodnou činnost i když mají různá jména a jsou binárně rozdílné. Jedná o tzv. dropper, který stáhne malware z URL `http://167.aaa.bbb.160/~ate.exe` a spustí jej.

Analýza činnosti se vztahuje k malware dostupnému ke dni 30.2.2015 kolem 8:20, v současné době se na daném URL může vyskytovat jiný soubor.

Změny, které analyzovaný malware provádí, jsou omezeny na uživatelský profil. Stačí tedy obnovit profil uživatele, případně ručně vrátit všechny zmíněné změny, tj. pod jiným uživatelem smazat vytvořené soubory a odstranit nové položky v registrech. Vzhledem k tomu, že na jiných stanicích a v jiném čase se stažený malware může chovat jinak, nelze obecně vyloučit jeho rozšíření mimo uživatelský profil. V takovém případě je doporučeno přeinstalovat celou infikovanou pracovní stanici.

Odpovědi na položené otázky

Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace?

Vytvořit generické pravidlo přímo pro soubor z přílohy není možné, ale je možné blokovat vytvoření a spuštění souboru, do kterého dropper ukládá stahovaný malware. Vždy se jedná o stejný soubor, stejného jména ve stejném adresáři. Pravidlo pro blokování může být tedy založeno jak na hashi souboru tak i na jeho názvu.

Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci?

Napadené stanice je možno identifikovat lokálně podle existence charakteristických klíčů v registrech a podle přítomnosti konkrétního souboru. Dropper komunikuje vždy s konkrétní IP adresou a následně stažený malware pak s IP adresami, které v dané době odpovídají nalezenému doménovému jménu.

Jak lze malware z napadených stanic odstranit?

Postup pro nápravu stanice je popsán v kapitole „Náprava kompromitovaných stanic“.