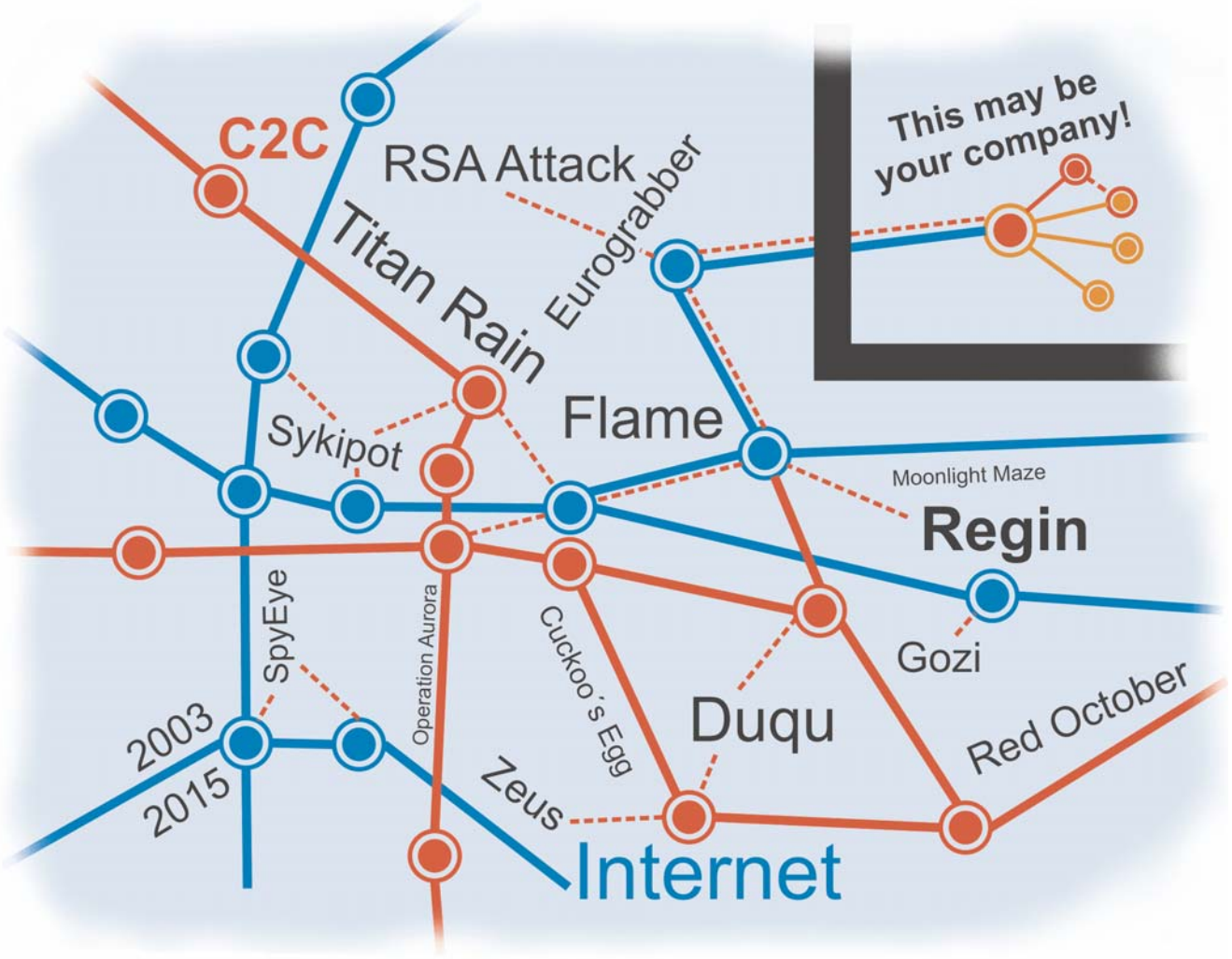
Digital Forensic Journal

1/2015 30. duben 2015



Digital Forensic Journal je odborný časopis věnovaný problematice forenzního zkoumání digitálních dat. Zabývá se nejenom problematikou samotného forenzního zkoumání, ale i dalších oblastí souvisejících s digitálními informacemi, s jejich bezpečností, ochranou, zjištěním a zkoumáním.

Znalecký ústav RAC konečně přináší český komplet

DEAT

DIGITAL EVIDENCE ACQUISITION TOOLS

DEAT je přenosná sada, obsahující kompletní sadu nástrojů pro pořizování forenzních binárních kopií dat. **DEAT** obsahuje prakticky vše, co můžete potřebovat - od sady redukcía kabelů, přes HW write-blockery pro různé typy disků nebo paměťových médií, až po speciální kopírovací zařízení.
DEAT je možné na přání vybavit i dalšími pomůckami a nástroji, které můžete na místě zajištění potřebovat.
DEAT je unikátně vybaveni nástrojem **DEAS** - forenzním bootovacím CD, které je pro účely práce na místě zajištění vytvořeno v laboratoři Znaleckého ústavu RAC.
Pomocí **DEAT** dostáváte kompletní přenosnou sadu HW a SW nástrojů pro forenzní pořizování kopií dat na místě zajištění.

Digital Forensic Journal

1/2015 30. duben 2015

Úvodník

Vážení čtenáři,

zahajujeme druhý ročník našeho časopisu. Tento ročník je ve srovnání s tím prvním neméně důležitý. Zejména proto, že tímto číslem končí podpora, kterou jsme při jeho vydávání měli z projektu Czech Cybercrime Centre of Excellence a budeme hledat jiné zdroje, které nám pomohou pokračovat. Díky vašim reakcím a vesměs pozitivní odezvě však další osud časopisu vidím optimisticky. Už teď jsou naplánovány změny, od kterých očekáváme další zkvalitnění příštích čísel. Plány jsou velké, uvidíme, co vše a v jakém časovém horizontu se nám povede zrealizovat.

Toto číslo je uvedeno velice zajímavou problematikou - Advanced Persistend Threats - sofistikované způsoby průniku do informačních systémů. Novinka to určitě není, jen odhalení a popsání těchto důmyslných a skrytých útoků nechalo na sebe nějakou chvíli čekat. Určitě stojí za přečtení, zejména specialistům na informační bezpečnost. Pokračujeme také ve slíbeném seriálu o forenzním využití logů a přidáváme první část další série článků, tentokrát o forenzní analýze SQLite databází od našich kolegů ze společnosti Belkasoft.

V poslední době také proběhlo několik důležitých akcí, ze kterých vám přinášíme informace a několik fotografií. Vy, co jste se jich zúčastnili, se tam možná najdete, těm ostatním doporučuji sledovat informační zdroje, protože podobné akce budeme určitě ještě do konce tohoto roku organizovat. Zmíním jenom dvě - závěrečná konference projektu Czech Cybercrime Centre of Excellence, která bude právě ve dnech, kdy bude vycházet toto číslo - tedy 29. a 30. dubna. Tou druhou bude 9. června Digital Forensic InfoDay, organizovaný ve spolupráci společností Risk Analysis Consultants, Compelson a FORSOLUTION Ltd.. Doufám, že se tam uvidíme.

Příjemné a užitečné čtení Vám přeje
Marián Svetlík

Obsah

Digital Forensic Journal je vydáván v kooperaci s Czech CyberCrime Centre of Excellence (C4e, www.c4e.cz) a za podpory Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs.

Risk Analysis Consultants, s.r.o.
Španělská 2
120 00 Praha 2
Tel. + 420 221 628 400
Fax + 420 221 628 401
E-mail dfj@rac.cz
Web www.rac.cz/dfj
IČ: CZ 63672774

Digital Forensic Journal (Print) ISSN 2336-4750
Digital Forensic Journal (On-line) ISSN 2336-4769
Ev. č. MK ČR: E 21 763
Ročník 2 / Rok 2015 / Číslo 3 / Vyšlo 30. 4. 2015 v Praze

Advanced Persistent Threat

Skutečná hrozba kyber-zločinců nebo počítačová hra informačních služeb ?

Jiří Hološka, Ph.D., GCFA
holoska@rac.cz
ICT Security Consultant, Digital Forensic Certified Expert, Incident Response Analyst, Risk Analysis Consultants, s.r.o.

Anotace:

Článek popisuje principy, které definují základy v současnosti asi nejnebezpečnějších způsobů průniků do informačních systémů a zneužití citlivých dat. Podrobně popisuje fenomén "Advanced Persistent Threat" (APT) a jeho životní cyklus, jako snad největší noční můru všech specialistů na bezpečnost informací. V závěru naznačuje některé možné postupy a způsoby identifikace a obrany proti těmto sofistikovaným útokům.

Definice

APT je cílený útok na vybranou organizaci nebo informační aktivum.

Advanced - kombinace známých a Zero-day zranitelností, Command and Control infrastruktura, značné znalostní i finanční zdroje, kvalitní organizace práce.

Persistent - Veškeré aktivity provedené útočníkem jsou podřízeny tomu, aby průnik do cílové organizace zůstal utajen po co nejdelší dobu; v napadené organizaci jsou vytvářeny mechanismy pro znovu infikování systému pro případ odhalení původního útoku.

Jednotlivé APT se šíří ve vlnách nebo kampaních.

Cílené kampaně:
a) patenty, výzkum, technologické know-how
b) bankovní informace
c) infrastruktura poskytovatelů služeb
d) útok za účelem poškození vybrané části kritické IT infrastruktury (STUXNET)
e) regionální kampaně – k aktivaci APT (spuštění další fáze DROPPEREM) dojde jen na systémech odpovídajícímu vybranému světovému regionu.

Na APT útoky se nespecializují jen organizované skupiny kyber-zločinců, ale nezřídka za útokem stojí různé státní agentury.

Rozdíl mezi APT a běžným útokem

APT je evolučně nejdokonalejší typ útoku, ovšem některé rysy původních přímočarých útoků byly zachovány.

Běžný útok se odehrává po lince – výběr cíle na základě znalosti využívání zranitelné technologie nebo aplikačního vybavení, identifikace slabého místa, testování nově nalezených, vzdáleně zneužitelných zranitelností (zejména na serverech). Fáze "Target research" se u plošného útoku skládá z aktivního skenování zranitelností, ať už na webových stránkách nebo přímo na serverových službách.

Mezikrok mezi klasickým útokem a APT byly různé druhy takzvaných botnetů. např. BlackHole KIT. Útoky nebyly cílené na specifickou organizaci, ale po průniku do webových serverů byl do kódu stránek vložen exploit, který infikoval návštěvníka stránek a následně se přihlásil k C2C infrastruktuře botnetu. Infikované stroje

často prohledávaly obsah pevných disků na zájmové informace, firemní data, přístupy k bankovnictví, bitcoin peněženky atd.

APT naproti tomu v první fázi útoku pasivně shromažďuje informace o organizaci, identifikuje klíčové zaměstnance, firemní procesy, sociální vazby a používané technologie, např. antivirové programy. Snaží se získat hlavičkové dokumenty a informace využitelné pro sestavení tzv. krycí historky.

APT obsahuje know-how ve formě zero-day zranitelností a kvalitního sociálního inženýrství, které umožňují kompromitaci vybraných zaměstnanců a krádež jejich identit. Tyto identity jsou využity k průzkumu firemní infrastruktury.

Další rozdíl mezi APT a běžným útokem je čas odhalení, kdy u APT je průměrná doba před objevením průniku přibližně 10 měsíců. A i tak je odhalení APT většinou otázkou upozornění třetí stranou. APT Regin byl odhalen jen díky chybě v MS Exchange mail serveru, kterou ani technici MS nebyli schopni identifikovat.

Stejně tak je rozdíl v nakládání s odcizenými daty – u pokročilých útoků je nakládání s exfiltrovanými daty podřízeno pravidlu udržet průnik do cílové organizace co nejdéle v tajnosti.

Cíle

APT jako metoda útoku je známa více jak 10 let, první útoky tohoto typu se začaly objevovat už okolo roku 2000. Na prvním místě je potřeba zmínit organizace stojící za samotnými útoky, poté bude možné lépe pochopit motivaci útočníků a definovat potenciální cíle.

V zásadě lze útočníky dělit na:

► Informační služby – zajímají se o přímý přístup k infrastruktuře poskytovatelů služeb, zpravodajským informacím (politici), nebo ke komerčnímu know how, komunikačním systémům, či k šifrovacím klíčům;

► (H)aktivisté - podobné zájmy jako informační služby s cílem odhalovat činnost politků či státních organizací;

► Kyber-zločinci - skupina zaměřená zejména na získávání finančních prostředků, popřípadě lehce zpeněžitelných informací nebo čísel kreditních karet. V komerční sféře pak cílí například na informace o nabídkách ve výběrových řízeních nebo know-how;

► Vojenské složky - cílem jsou útoky na kritickou infrastrukturu nepřátelských států nebo organizací. Útoky jsou cílené nejen na IT, ale i na fyzickou infrastrukturu s centralizovaným řízením. Příkladem může být STUXNET[1];

► Teroristické organizace - v zásadě mají stejné cíle jako vojenské složky, nicméně jejich motivace je často ideologicky či nábožensky motivovaná, proto je vhodné je zmínit odděleně.

Známé kampaně[2]

Moonlight Maze - cíl: Pentagon, NASA Department of Energy
2003 - Titan Rain - cíl: Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA
2006 - Sykipot - cíl: US, UK firmy - původ: Čína
2011 - RSA Attack - kompromitován SecurID
2012 - Flame - cíl: země blízkého východu - původ: USA, Izrael cca. 2007
2012 - Eurograbber - cíl: EU - 30 bank v EU
2014 - Regin - cíl: Belgacom
2014 - Carbanak - cíl: bankovní sektor, dopad: ztráta jedné miliardy USD
2014 - Gemalto hack - cíl: výrobce čipových karet, dopad: únik šifrovacích klíčů SIM karet

Red October, Gozi, Operation Aurora, Duqu, The Cuckoo's Egg, Zeus, SpyEye, DarkHotel,

Agent.biz, SabPub, Shamoon, Crouching Yeti, Black Energy

Obecně lze tedy tvrdit, že organizace má potenciál stát se cílem pro APT, pokud splňuje některý z následujících bodů:

a) vlastní technologické know-how
b) má přístup nebo se sama aktivně podílí na vědecko-výzkumné činnosti
c) má přístup k finančním transakcím
d) vlastní infrastrukturu s širokou uživatelskou základnou
e) provozuje službu pro uchování, přenášení nebo zpracování zpravodajsky cenných informací
f) má přístup k řídícím prvkům kritické infrastruktury

Pro příklad lze uvést útok z listopadu 2014 nazvaný Regin. Cílem se stal belgický telekomunikační operátor Belgacom, vlastník podmořských optických tras a mobilní operátor. Dle závěrů z vyšetřování nebylo cílem útoku z firmy odcizit informace, ale dostat se k přenosové infrastruktuře operátora, zejména šlo o komunikační uzly, na kterých lze provést odposlech uživatelských dat v nešifrované podobě.

Z vyšetřování vyplývá rozsah celého útoku:
- kompromitováno 120 systémů včetně 70 pracovních stanic
- kompromitovány i CISCO routery
- údajně byly kompromitovány systémy zajišťující mobilní komunikaci

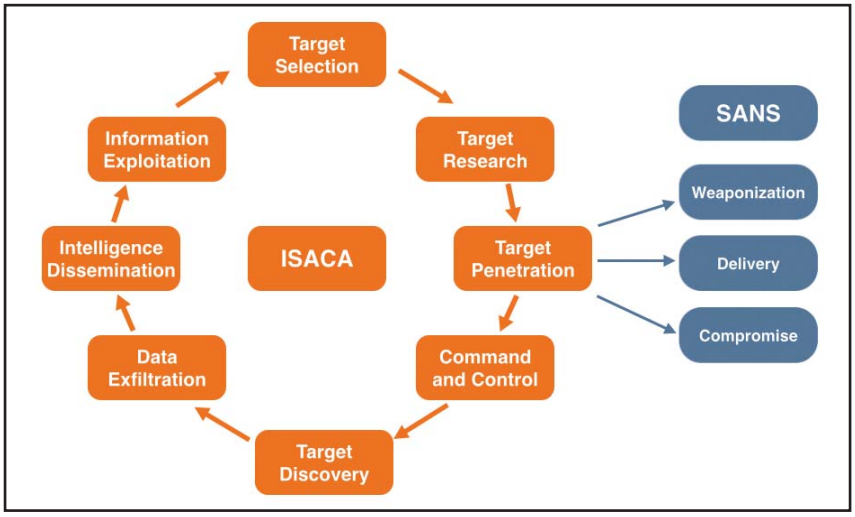
Vyšetřovatelé dále dospěli k závěru, že část důkazů o průniku mohla být odstraněna útočníkem aktivací sebedestrukčního příkazu.

Životní cyklus - APT

Pohledů na životní cyklus APT[3][4] existuje více, v obecné rovině však lze identifikovat obdobné fáze tohoto cyklu. Konkrétně to jsou Target selection, Target research, Exploitation, Target discovery a Data exfiltration. Ne nezbytně se musí shodovat názvy jednotlivých fází, nicméně obsahově jsou prakticky totožné.

Target selection - Problematika výběru cílů již byla nastíněna, nicméně je vhodné zmínit, že cíle jsou stanoveny dle priorit "zákazníků" a ty se mohou rapidně měnit v závislosti na získaných informacích nebo objevených zranitelnostech. U APT není výjimkou takzvané řetězení útoků, kdy jsou v první vlně napadeny kontraktorské či konzultantské organizace a dodavatelé technologií a teprve po vytěžení těchto znalostí se přechází na primární cíl.

Target research - Tato fáze útoku je zaměřená na získání informací o cílové organizaci. Na rozdíl od klasických útoků se mapování cíle provádí pasivním zjišťováním technologií (např. typ antiviru, firewallů, síťové infrastruktury), postupů, klíčových zaměstnanců (administrátoři, top management), identifikací dodavatelů. Mezi zájmové informace v této fázi útoku patří rozsahy IP adres, emailové adresy, sociální vazby mezi zaměstnanci, různé dokumenty obsahu-



jící aktuální corporate design a podobně.

Target penetration - Jedná se o fázi samotného průniku do cílové organizace, kdy jsou zužitkovány informace z předchozích fází pro vytvoření tzv. krycí historky (sociální inženýrství) a je sestaven exploit na míru. Po doručení exploitu je do cílového systému zavlečen malware umožňující s napadeným systémem komunikovat již bez nutnosti interakce uživatele.

Command and Control (C2C) - je název infrastruktury, kterou malware využívá pro komunikaci s útočníkem.

Target discovery - fáze útoku známá také pod pojmem "Lateral movement". Obecně je tak označován postup útočníka z jednoho stroje na druhý s cílem získat další uživatelské účty, zejména pak lokální a doménové privilegované účty. V této fázi je prováděno mapování sítě a instalce backdoorů pro případ, že primární útok bude odhalen. Pracovní stanice, na které se útočníkovi podaří přihlásit, jsou taktéž prohledány s cílem identifikovat zájmové informace.

Data exfiltration - jakmile útočník získá dostatečná oprávnění pro přístup k informačním zdrojům, začne identifikované zájmové informace shromažďovat na některé z jím ovládaných pracovních stanic nebo serverů. Zájmová data jsou komprimována a šifrována. Způsob exfiltrace, tzn. přenosu z interních systémů na některé internetové úložiště v C2C infrastruktuře, je závislý na aplikovaných data loss prevention politikách a technologiích. Může se jednat o posílání dat pomocí emailových zpráv, stejně tak i přenos na SFTP servery v síti TOR[5]. Vyloučit se nedá ani využití některé z forem steganografie, tzn. skrytých komunikačních kanálů.

Jednotlivé fáze životního cyklu nejsou pevně dané, z tohoto důvodu je zejména při porovnání manažerských a technických pohledů možné najít jinou úroveň detailu pro určité fáze.

Jako příklad lze uvést manažerský pohled ISACA[6] s důrazem na operace se zájmovými informacemi a technický pohled od SANS[7] s důrazem na techniku průniku.

Fáze definované ISACA pro nakládání s informacemi jsou pojmenovány jako Intelligence dissemination a Information exploitation:

Inteligence dissemination - nakládání s odcizenými daty tak, aby nebyl prozrazen útok nebo identifikována odcizená data; např. informační hodnota nabídky v tendru má jen velmi omezenou dobu spotřeby.

Information exploitation - fáze zneužití odcizených dat. Informační aktiva mají různou délku životnosti – od toho se odvíjí i rychlost, se kterou jsou odcizené informace využívány. Například informace o výběrových řízeních od konkurenčních firem lze zužitkovat pouze do data ukončení podávání nabídek, ovšem vývojové plány nového výrobku lze využít i za několik let. Způsob a čas zneužití informací je ovšem značně závislý na typu útočníka.

Technický pohled od SANS je spíše zaměřen na samotné provedení průniku a místo fáze Target penetration tuto oblast životního cyklu APT dělí na tři menší fáze – Weaponization, Delivery a Compromise.

Je to dáno tím, že vybudování Command and Control infrastruktury nebo frameworků pro sestavování nástrojů pro provedení útoků je velmi nákladné. Z toho důvodu jsou existující nástroje a infrastruktura nebo jejich části opětovně používány v různých kampaních. Pomocí analýzy sestavení útoku lze alespoň částečně určit původce útoku.

Dílčí části fáze Target penetration dle SANS:

Weaponization - definuje způsob nebo specifické postupy, kterými byl sestaven

daný payload, popřípadě definuje mechanizmus, jakým byl hotový exploit vložen do přenosového média (např. EXE, PDF souboru) .

Delivery - popisuje způsob přenosu exploitu od útočníka k vybrané organizaci. Mezi oblíbená přenosová média patří například emailové zprávy, infikované webové stránky, usb flash disky aj.

Compromise - fáze zabývající se samotným exploitováním cílové organizace. Jedná se o kombinaci technických zranitelností operačních systémů a sociálního inženýrství.

Fáze **Target penetration, C2C, Target discovery a Data exfiltration** jsou zajímavé z pohledu řízení incidentů, protože tyto kroky zanechávají v systémech identifikovatelné stopy, které lze při správném postupu izolovat a vytvořit tak **Indicator Of Compromise (IOC) signatury**.

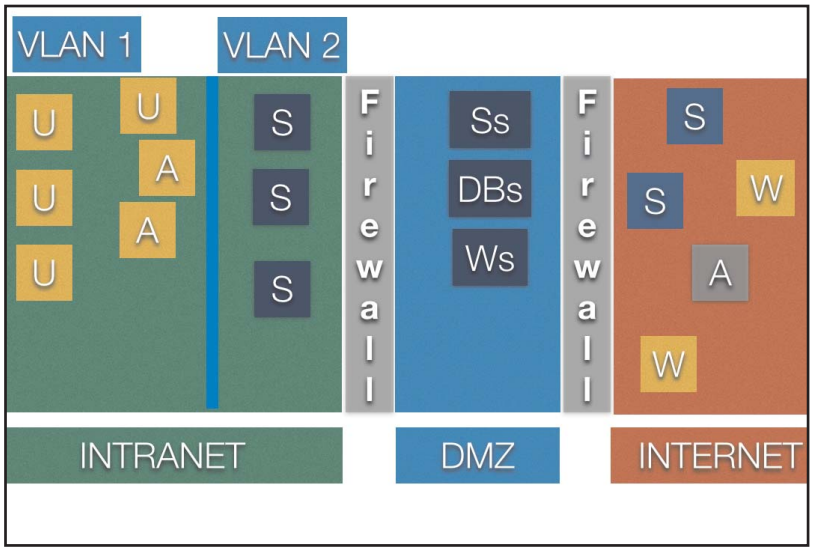
Vizualizace zjednodušené infrastruktury firemního prostředí

IT infrastruktura je v každé společnosti odlišná, ať už je to dáno druhem podnikání, nebo finančním rozpočtem. Obecně se ve firmách, tedy v těch, které bezpečnost IT berou v potaz, řeší ochrana perimetru v podobě firewallů a DMZ, segmentace intranetu pomocí VLAN a v neposlední řadě antivirová ochrana pracovních stanic.

Infrastruktura intranetu obsahuje uživatelské pracovní stanice, administrátorské pracovní stanice a servery ve vyhrazené VLAN. DMZ obsahuje webové, databázové a file servery. Internetový segment obsahuje externí servery, legitimní uživatele internetu a útočníky.

Síťová segmentace

Na následujícím obrázku je znázorněna vizualizace síťové segmentace a ochrany perimetru. Síťová segmentace definuje možnosti jednotlivý stanic a skupin stanic komunikovat mezi sebou. Dále určuje, dle jakých pravidel lze navazovat spojení mezi jednotlivými síťovými body.

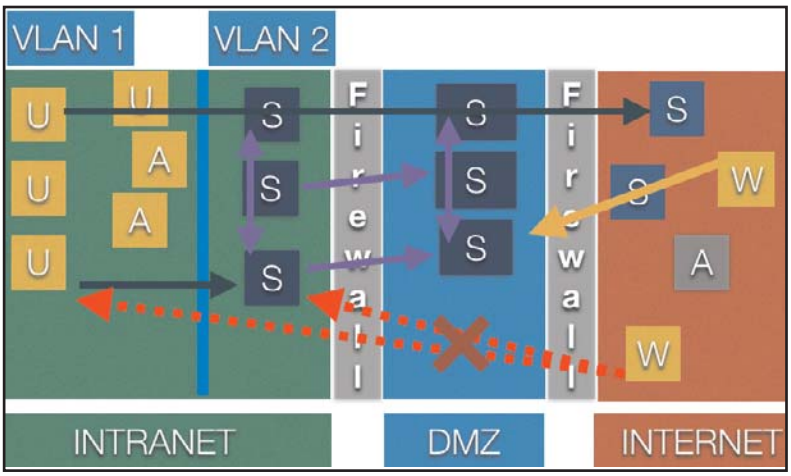


Vizualizace zobrazuje standardní členění síťové infrastruktury, včetně ochrany perimetru, kdy externí uživatelé legitimní i nelegitimní mohou přistupovat pouze na vymezené služby serverů v DMZ.

Princip spear phishing útoku

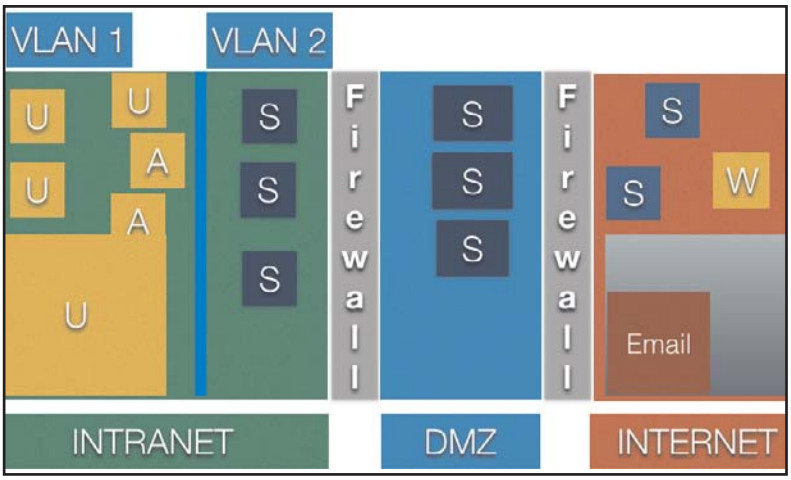
Spear phishing[8] je způsob útoku, kdy je škodlivý kód doručen oběti pomocí e-mailové zprávy ve formě přílohy nebo URL adresy odkazující na stránky se škodlivým kódem.

Možné jsou samozřejmě i kombinace obou technik, kdy je možné kombinovat různé druhy exploitů pro zvýšení pravděpodobnosti



Stejný princip byl použit pro penetrování bank APT kampaní nazvanou Carbanak (https://blog.kaspersky.com/-billion-dollar-apt-carbanak/)

průniku. Součástí delivery fáze útoku je sociální inženýrství, kdy je snahou útočníka přesvědčit oběť o legitimitě přijaté zprávy. Pro tento účel jsou využity informace z fáze Target research, ve které útočník mapoval



firemní procesy, kulturu komunikace, popř. sociální vazby vytipovaných zaměstnanců.

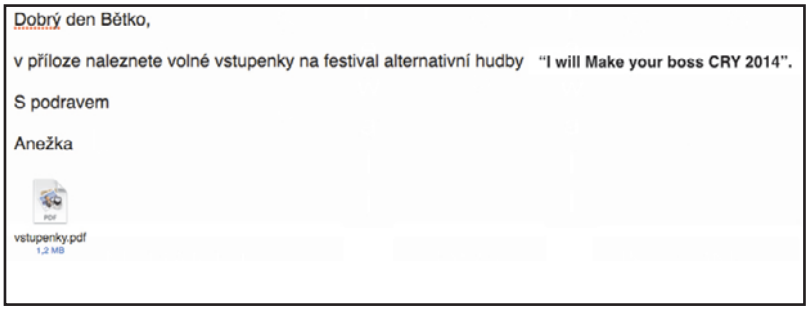
Cílem útoku je prezentovat informace posílané útočníkem v takové formě a způsobem, aby u oběti nevyvolal podezření. Digitální stopa, kterou každý aktivní uživatel internetu za sebou zanechává, je neocenitelným zdrojem informací.

Pro ilustraci útoku je použit přenos škodlivého kódu pomocí speciálně sestaveného PDF dokumentu.

Způsobů, jak provést exploit (delivery) vybraného zaměstnance, je nespočet. Mezi ty nejčastější patří spear phishing, mezi další typizované útoky patří infikování oblíbených webů oběti nástroji na bázi botnetu. Všechny mají společný cíl, a to nahrát na pracovní stanici vybraného zaměstnance programové vybavení, které umožní stažení a aktivaci dalších modulů APT. Tento miniaturní program se označuje jako dropper. Dropper se připojí na C2C infrastrukturu, stáhne modul pro další fázi útoku a zajistí, aby se nově stažená komponenta spouštěla i po restartu pracovní stanice.

Počet modulů a jejich konkrétní funkce se liší v každé vlně, vždy se ovšem jedná o nástroje umožňující přímý přístup k infikovanému stroji. Mezi oblíbené funkce patří keyloggery, modul pro vytváření kopií obrazovek (screenshotů), přístup k mikrofonu a webové kameře atd.

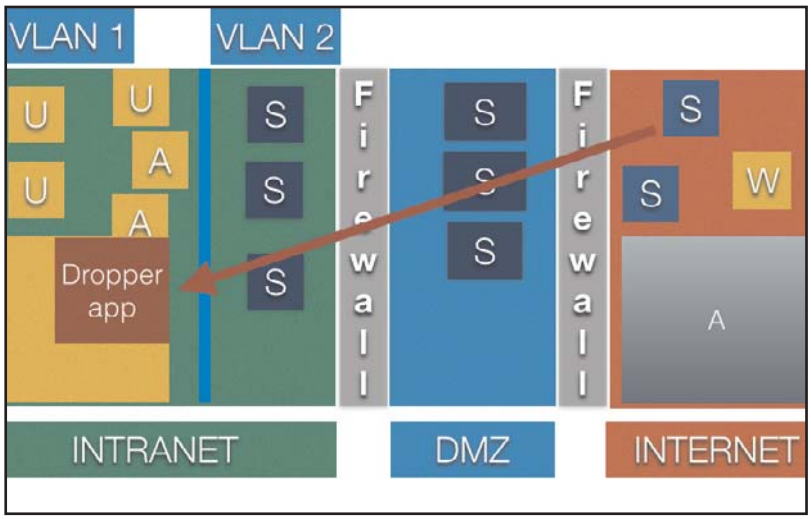
Aktivace jednotlivých modulů APT, stejně jako samotný průzkum infikované pracovní stanice, je centralizovaně řízen pomocí

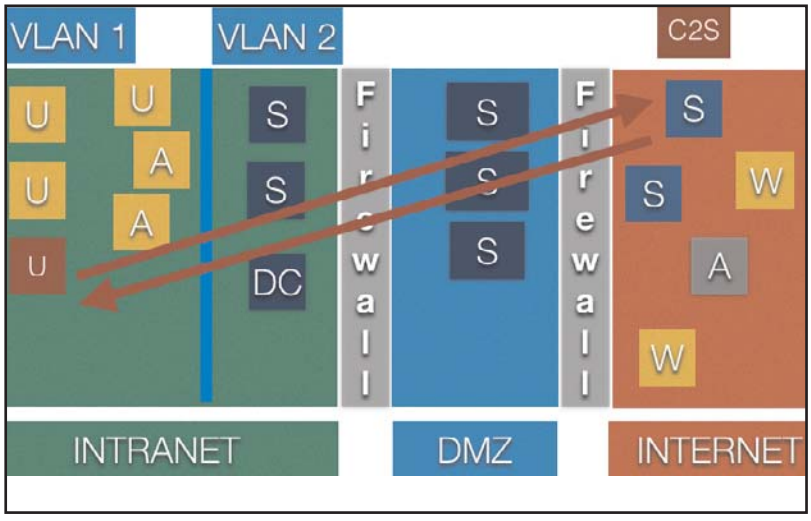


Command and Control infrastruktury (C2C). C2C se skládá ze serverů přímo v internetu, nebo v takzvaném hlubokém internetu – servery provozované v anonymizační síti TOR.

Jakmile je pracovní stanice infikována, jsou staženy moduly pro další fázi útoku, je zajištěno automatické spouštění modulů po restartu systému a je navázána komunikace s C2C, začínají pro oddělení IT Security velmi zlé časy.

Prvním krokem je zcizení identity zaměstnance na infikované pracovní stanici. Pro tento účel postačí jakákoliv lokální zranitelnost typu Local Privilege Escalation, čímž je umožněn přístup k systému na úrovni administrátora. S právy lokálního administrátora je získání aktuálního hesla přihlášeného zaměstnance otázkou sekund. S heslem lze případně odcizit i Kerberos tikety pro SSO a postup na další pracovní stanice může začít.





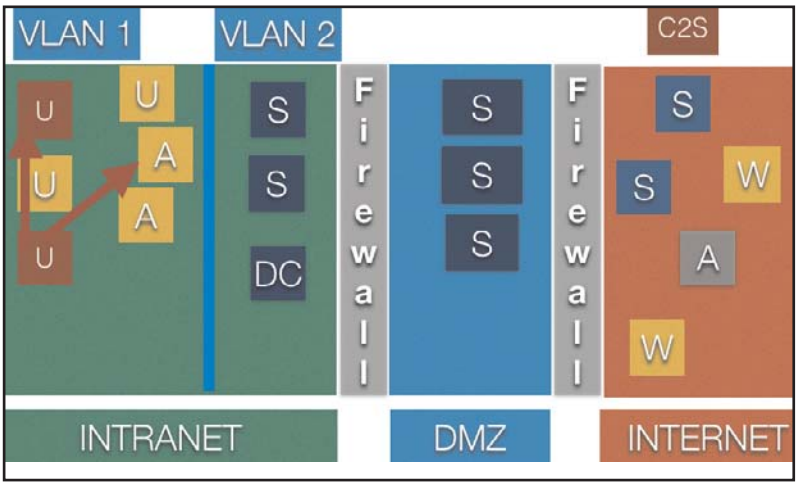
Target discovery

Fáze Target discovery životního cyklu APT definuje pohyb útočníka (lateral movement) za účelem kompromitace jednotlivých systémů v organizaci a zajištění uživatelských oprávnění a dokumentů.

Sada nástrojů využívaná útočníkem po úspěšném exploitování cílové stanice (zaměstance) se stáhne v předem připraveném balíčku z internetu. Konkrétní nástroje se v každé APT verzi (vlně) liší, ale obecně obsahují keyloggery, portforwardery[9], nástoje pro

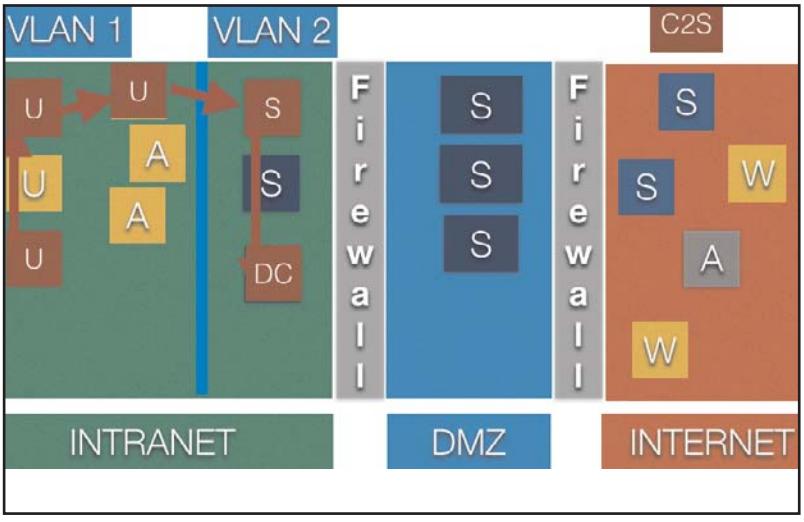
příkazovou řádku pro práci s procesy, TFTP (Trivial File Transfer Protocol)[10] servery a v neposlední řadě nástroje a exploity pro využívání lokálních zranitelností pro eskalaci oprávnění. Nicméně APT veškeré aktivity podřizuje účelu nezjistitelnosti, tj. využívá takové způsoby navazování spojení mezi pracovními stanicemi, které pokud možno odpovídají pracovním postupům skutečných zaměstnanců.

Nejjednodušší způsob přenosu dat mezi systémy je pomocí lokální sdílené složky obsahující moduly APT a spuštění těchto



modulů na vzdáleném systému s využitím nástroje PsExec.

PsExec je nástroj ze sady nástrojů Microsoft Sysinternals[11], vyvinutých pro usnadnění práce administrátorům při správě a monitoringu MS Windows. PsExec[12] umožňuje spuštění procesu na vzdáleném systému, a to i programu nasdíleného z jiného systému. Po spuštění procesu na novém systému následuje překopírování na lokální disk a zajistí se opětovné spuštění APT po restartu systému. Spojení s C2C je navázáno přímo nebo přes dříve infikované stanice. Dále je zjištěn účet aktuálně přihlášeného uživatele.



Nejvyšší dosažitelnou metou při postupu útočníka firemní sítí je získat účet s oprávněním doménového administrátora. S doménovým administrátorem lze snadno kompromitovat doménový server a tím získat neomezený přístup nejen k uživatelským datům, ale i ke skupinovým politikám.

Rozbor útoku

Vektor útoku může nabývat různých forem, od spear phishingu, přes podvržení DNS záznamů[13], přímé exploitování v kavárně až po offline exploit pomocí kompromitovaného CD nebo USB flash disku.

Cílené útoky míří v drtivé většina na konkrétní osobu, zastávající firemní roli s privilegovaným přístupem k ICT zdrojům. Dalším důvodem může být fakt, že tito zaměstnanci mají často oprávnění lokálního administrátora.

Exploitování

Zatímco servery jsou monitorovány a periodicky testovány na zranitelnosti, uživatelské stanice jsou z těchto

testů obyčejně vyjmuty. Dostupné systémové aktualizace je možné automaticky sledovat pomocí systémových nástrojů, aplikace třetích stran a jejich rozšíření (pluginy) jsou ovšem aktualizovány pouze po uvážení samotného uživatele.

Jednou z klíčových komponent programového vybavení pracovních stanic jsou webové prohlížeče a prohlížeče/editory dokumentů. Zejména neaktualizované pluginy těchto programů jsou pro útočníky příslovečné nízko visící ovoce.

Pro ilustraci lze použít nástroj Qualys BrowserCheck[14]. Níže uvedený výsledek testu ilustruje stav webového prohlížeče a jeho pluginů po třech měsících bez aktualizace.

Oblíbená kombinace pluginů pro exploitování cílových systémů je Adobe Acrobat Reader a Java Plugin, jelikož se vyskytují téměř na každé pracovní stanici. Pro útočníka není rozdíl, zda upravený dokument doručí jako přílohu emailové zprávy či pomocí URL odkazu na dokument umístěný na internetu, jelikož ten se bude v obou případech otvírat lokálně nainstalovaným prohlížečem.

Persistence

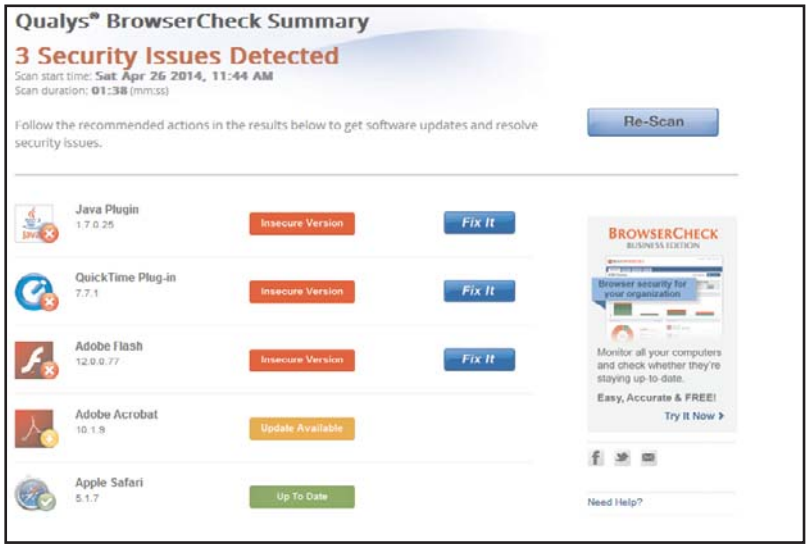
Zajišťuje lokální reaktivaci škodlivého kódu po restartu systému, například záznamem v registrech, registrací škodlivého kódu do služeb systému nebo nahrazením originální komponenty operačního systému upravenou verzí s novými funkcemi.

Persistence APT útoku se neprojevuje jen lokálně na konkrétním systému, ale i globálně v rámci organizace. Sofistikované útoky nespoléhají jen na primární vektor průniku, kterým se dostaly do organizace, ale po získání potřebných oprávnění instalují na cílové systémy backdoory pro případ, že prvotní útok bude odhalen.

Záložní řešení nemusí obsahovat celý framework APT, ale postačí, aby se jednalo o takzvaný dropper, který v případě aktivace stáhne novou verzi z C2C nebo botnetu. Jako vhodným umístěním pro zadní vrátka se, mimo upravené systémové služby a komponenty OS, jeví také upravený firmware, a to zejména u síťových zařízení jako jsou síťové tiskárny, NAS disková pole, IP kamery. Dalším vhodným zařízením pro úpravu firmwaru jsou interní komponenty napojené na sběrnici s přímým přístupem do paměti – řadiče pevných disků, pevné disky, FireWire řadiče apod.

Lateral movement

Cílem je pokud možno nepozorovaně získat přístup k účtu doménového administrátora, identifikovat zájmové dokumenty a vytipovat vhodné zařízení pro instalaci backdoorů.



Útočník se bude snažit vytvořit si v organizaci síťový prostor, ve kterém se budou shromažďovat zájmové dokumenty, které si zde bude připravovat k exfiltraci.

Technicky může fáze lateral movement nabývat různých forem – od vzdáleného spou-

štění procesů pomocí psexec z nasdíleného adresáře, po kopírování exploitu pomocí schránky RDP[15] a lokálním spouštěním v PowerShellu. Zde již záleží na způsobu využití ICT zdrojů v cílové organizaci. Lze však konstatovat, že se útočník bude snažit svoje aktivity skrýt mezi aktivity legitimních zaměstnanců.

Indicator Of Compromise (IOC)

Rychlá identifikace APT je jediné reálně účinné protiopatření proti cíleným útokům. Obecně lze říci, že pro úspěšnou detekci APT je nutné mít nastavené procesy pro technickou analýzu jednotlivých síťových systémů a globální behaviorální analýzu stavu ICT v organizaci.

Pro tuto obecnou rovinu platí, že mezi hlavní ukazatele průniku patří:

► detekce neobvyklého síťového provozu - komunikace se zahraničními servery s malou důvěryhodností a neuvěřitelnou historií

► změny v konfiguraci firewallů na pracovních stanicích

► aktivní Man-in-the-middle útoky - například ARP poisoning

► změny v lokálních routovacích tabulkách nebo DNS záznamech

► identifikace nestandardních uživatelských přístupů - přístupy mimo pracovní dobu

► neautorizované záznamy v nástroji pro plánování automatického spouštění úloh

► existence malwaru, neznámých systémových knihoven apod.

Jednotlivé indikátory je nutné korelovat mezi sebou a vytvářet celkový pohled do uživatelských aktivit a systémových procesů.

Aktivita útočníka generuje provozní anomálie na napadených systémech. Odstranit nebo zakrýt všechny stopy po exploitování je velmi obtížné a v mnoha případech přímo nemožné. Schopnost Incident response týmu analyzovat informace ze systémů v širším měřítku je podmínkou pro identifikaci průniku.

Protiopatření

Efektivní preventivní opatření proti hrozbě APT útoků jsou téměř nerealizovatelná, preventivními opatřeními lze pouze snížit možné vektory útoků. APT využívají podobné principy jako běžné přímočaré útoky, liší se ale motivací a kombinací různých technik. Proto i protiopatření mají společné body.

V první řadě se jedná o **asset management**, neboť bez znalosti vlastních systémů a jimi poskytovaných služeb nelze provádět žádné sofistikovanější analýzy a monitoring. Následujícím krokem je **zvládnutí kontinuálního vulnerability a patch managementu**. Pro APT je typické, že prvotní útok směřuje na uživatele a pracovní stanice, proto je nutné v širším měřítku **zajistit ochranu koncových stanic**. Zejména s ohledem na používáni neautorizovaných programů a služeb, které nejsou detekovány jako hrozby antivirovými programy. Po úspěšném zvládnutí zmíněných protiopatření je vhodné zavést **sofistikované analytické nástroje pro monitoring síťového provozu, včetně behaviorální analýzy anomálií**. Nejvyšší úroveň protiopatření tvoří **nástroje pro kontextuální analýzu běžících procesů na serverech a pracovních stanicích**, které identifikují změny chování samotných procesů. Tato detekční řešení umožňují ověřovat aplikace pomocí databází od softwarových výrobců a případné anomálie testovat pomocí statické a dynamické analýzy spustitelných souborů, včetně závislostí v podobě nalinkovaných knihoven.

Pro tento stupeň analýzy je ovšem potřeba tým specialistů ve firemním nebo outsourcovaném SOC (Security Operations Center)[16].

Samostatným tématem je **ochrana VIP zaměstnanců**, neboť je jen velmi obtížné nařizovat vysokým manažerům, jak mají nakládat s ICT vybavením, příp. odebírat administrátorům lokální privilegované přístupy k jejich vlastním pracovním stanicím.

Závěr

S každým nově odhaleným cíleným útokem je stále zřejmější, že informační bezpečnost bude muset projít radikálním vývojem v oblasti zabezpečení koncových stanic, behaviorální analýzy na úrovni uživatelů, aplikačního vybavení a síťového provozu. Vytvoření vyhrazeného týmu SOC na analýzu síťových dat, kontext procesů operačních systému a analýzu malwaru, je velmi nákladné a časově náročné. Dá se proto očekávat, že na tento problém zareagují dodavatelé v oblasti penetračních testů a malware analýzy a přijdou na trh s produkty zahrnující i služby SOC center.

Přes všechna pasivní i proaktivní opatření zaměřená na potlačení hrozeb APT bude ale vždy jedinou spolehlivou ochranou firemních aktiv rychlá detekce průniku a zásah Incident response týmu.

Bibliografie

[1] http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

[2] KASPERSKY LAB. Targeted cyberattack logbook. [online]. [cit. 2015-02-08]. Dostupné z: https://apt.securelist.com

[3] LACEY, David. ISACA. Advanced persistent threats how to manage the risk to your business. Rolling Meadows, IL: ISACA, 2013. ISBN 9781604203486.

[4] CLOPPERT, Mike. Security Intelligence: Attacking the Cyber Kill Chain. In: [online]. [cit. 2015-02-05]. Dostupné z: http://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain#

[5] https://www.torproject.org/docs/faq.html.en#WhatIsTor

[6] http://www.isaca.org/about-isaca/Pages/default.aspx

[7] http://www.sans.org/about/

[8] Spear Phishers: Angling to Steal Your Financial Info. FEDERAL BUREAU OF INVESTIGATION (FBI). [online]. 2009. vyd. [cit. 2015-02-13]. Dostupné z: http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

[9] http://cs.wikipedia.org/wiki/Přesměrování_portu

[10] http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

[11] https://technet.microsoft.com/en-us/sysinternals

[12] https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

[13] http://hacking-tutorials-now.blogspot.cz/2013/09/backtrack-5-r3-dns-spoofing.html

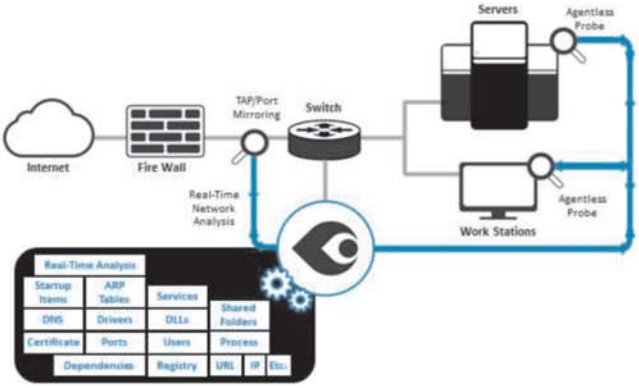
[14] https://browsercheck.qualys.com/

[15] https://msdn.microsoft.com/en-us/library/aa383015%28v=vs.85%29.aspx

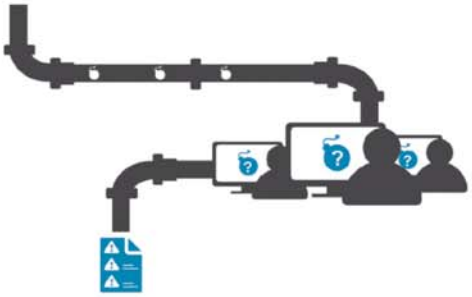
[16] http://en.wikipedia.org/wiki/Security_operations_center#SOC_of_IT

Cyber Spear Persistance

Cyber Spear Persistence je bezagentní řešení pro přesnou detekci sofistikovaných kybernetických útoků, jako např. Advanced Persistent Threats (APTs), s důrazem na minimalizaci reportování false-positive nebo nejednoznačných nálezů IT oddělení.



Po provedené analýze systém rozdělí procesy na legitimní, škodlivé, či vyžadující hlubší úroveň analýzy. Manuální analýza je prováděna na žádost klienta vyhrazeným SOC týmem, jehož služby jsou zahrnuty v rámci licence.



Cyber Spear **Persistence**

Cyber Spear
PRECISE THREAT DETECTION

Jak poznáte, že vaše organizace byla cílem sofistikovaného APT útoku?

Advanced Persistent Threat (APT) jsou cílené útoky na vybrané organizace **s cílem zajistit si trvalý přístup** (proto "persistent") k jejím aktivům. Za tímto účelem **využívají útočníci pokročilé techniky** (proto "advanced") včetně kvalitního sociálního inženýrství a tzv. zero-day zranitelností (zranitelnost, která dosud nebyla objevena nebo pro kterou dosud neexistuje patch). Pomocí těchto technik dochází ke krádeži identit vybraných zaměstnanců a tyto jsou pak využity k průzkumu firemní infratsruktury.

Obecně lze tvrdit, že organizace má potenciál stát se **cílem pro APT**, pokud splňuje některý z následujících bodů:

- vlastní technologické know-how
- má přístup nebo se sama aktivně podílí na vědecko-výzkumné činnosti
- má přístup k finančním transakcím
- vlastní infrastrukturu s širokou uživatelskou základnou
- provozuje službu pro uchování, přenášení nebo zpracování zpravodajsky cenných informací
- má přístup k řídícím prvkům kritické infrastruktury

Cílem útočníků je zůstat neodhalen co nejdelší dobu. Ze zprávy Mandiant M-Report 2015 vyplývá, že průměrná **doba od prvního průniku do jeho odhalení je dlouhých 205 dní**. Přitom pouze jedna třetina napadených organizací je schopna průnik zjistit sama, ve většině případů je odhalení APT otázka upozornění třetí stranou.

Otestujte si Vaši organizaci hned!

Nástroj CyberSpear Persistance se snaží na tuto otázku odpovědět. Při příležitosti uvedení nástroje Cyber Spear na český trh vám společnost Risk Analysis Consultants ve spolupráci s jeho tvůrci (stejní lidé stáli např. za vznikem Versafe) nabízí jedinečnou **možnost bezplatného zkušebního nasazení tohoto nástroje** v rámci Proof of Concept (PoC) přímo ve vaší organizaci.
Hlavními přednostmi nástroje Cyber Spear jsou **bezagentní řešení** (není tedy třeba instalovat agenta na každé zařízení ve vaší síti), **extrémně rychlá instalace** (ve většině případů do 2 hodin) a **minimální zátěž pro zdroje organizace**. V průběhu testování máte k dispozici veškeré funkcionality systému včetně asistence Cyber Spear Security Operations Centra (SOC). **Celý PoC je ukončen závěrečným reportem**.

Podrobnější informace o nástroji Cyber Spear Persistance a o technických podmínkách pro PoC naleznete na **www.rac.cz/CyberSpear**.

RAC®

Prodej a podporu nástroje Cyber Spear Persistance v ČR zajišťuje:
Risk Analysis Consultants, s.r.o.
Španělská 2
120 00 Praha 2
www.rac.cz
zu@rac.cz

Cyber Spear **Persistence**

XRY COMPLETE

THE ALL-IN-ONE MOBILE FORENSIC SYSTEM FROM MICRO SYSTEMATION

> CO JE XRY COMPLETE

XRY COMPLETE JE ALL-IN-ONE ŘEŠENÍ PRO MOBILNÍ FORENZNÍ ANALÝZU OD ŠVÉDSKÉ SPOLEČNOSTI MICRO-SYSTEMATION, KOMBINUJÍCÍ NÁSTROJE PRO LOGICKOU I FYZICKOU EXTRAKCI DO JEDINÉHO BALÍČKU. XRY COMPLETE UMOŽŇUJE FORENZNÍM EXPERTŮM PŘÍSTUP KE VŠEM METODÁM ZÍSKÁVÁNÍ DAT Z MOBILNÍCH ZAŘÍZENÍ.

> ŠIROKÉ MOŽNOSTI EXPORTU

>> Excel
>> Word
>> Open Office
>> XML
>> Google Earth
>> tiskové sestavy

> XRY COMPLETE OBSAHUJE

>> XRY software a licenční klíč
>> kufřík s organizérem na kabely
>> XRY komunikační jednotka
>> XRY Logical kit kabelů
>> XRY Physical kit kabelů
>> SIM id-Cloner s 12 měsíční licencí
>> 10 SIM karet pro id-Cloner
>> čtečku karet s ochranou proti zápisu
>> 12 měsíční licence
>> XACT hex prohlížeč
>> XRY Reader aplikaci
>> čistící kartáček
>> přístup k podpoře zdarma
>> veškeré upgrade SW zdarma
>> dodání kabelů k novým zařízením zdarma

> PRODEJ A PODPORA V ČR

RISK ANALYSIS CONSULTANTS, S.R.O.
Španělská 2, Praha 2
zu@rac.cz

www.rac.cz

Forenzní logy pohledem vývojáře II.

Logy jako jeden z klíčových zdrojů informací pro vyšetřování událostí v ICT

Karel Dohnal, specialista na informační bezpečnost. V roce 2013 získal certifikaci CISSP. Programování se věnuje od svých 8 let. Svůj volný čas tráví s rodinou a vařením.

Anotace:

V minulém dílu byly popsány způsoby tvorby logů a možné formáty. Druhý díl se zaměří na možnosti ukládání logů, jejich ochranu, akvizice a analýzy.

Ukládání logů

Při samotném návrhu aplikace a tím i způsobu ukládání logů je nutné vzít v potaz účel, předpokládané zatížení, množství generovaných událostí a potenciální budoucí rozvoj. Obzvláště poslední zmíněné je nejdůležitější. Při špatném rozhodnutí se dostavují komplikace ve formě nedostatečných kapacit anebo naopak příliš složitého kódu.

Pro systémy, které jsou geograficky i síťově blízko sebe, je vhodnější centralizované ukládání. Během zasílání zpráv nedochází k velkým časovým prodlevám a všechny logy jsou shromážděny na jedno místo. Navíc případné LMI systémy [1] provádějící zpracování přijatých informací vše ukládají do databází podle předdefinovaných klíčů, čímž markantně usnadní následné vyhledávání. Tento benefit je však také největší nevýhodou. Indexy zabírají místo, musí se udržovat a jejich sestavování je zdrojově i časově náročné.

Pro globálně působící společnosti je centralizovanost překážkou. Aby byly odezvy systémů směrem k zákazníkům co nejmenší, je nutné mít vše distribuované minimálně v rámci kontinentů. Pokud by systémy běžící v Severní Americe, Asii, či Austrálii měly posílat své provozní informace do České republiky, lze počítat při silném zatížení se zahlcením front díky latenci a ztrátovosti paketů. Následný dominový kolaps na sebe nenechá dlouho čekat. Pro takové prostředí je vhodnější ukládat informace v lokálním datovém centru, případně předzpracovat a pouze výsledky posílat do centrálního uložiště pro další analýzy. Takový postup však může znamenat časovou prodlevu mezi vznikem bezpečnostního incidentu a jeho detekcí.

Pro forenzního analytika je centralizovanost při hledání souvislostí v celém systému obrovskou výhodou šetřící čas. Avšak z pohledu provozu jde o potenciální „Single Point Of Failure“ [2], kdy jeho selháním může dojít k zastavení chodu aplikace. Rozhodnutí by se proto mělo vždy odvíjet od účelu, zatížení a budoucího rozvoje aplikace. Bohužel ne vždy ve prospěch analytiků. Dobrá dokumentace může tento nedostatek kompenzovat.

Syslog

Standardizovaný protokol určený pro záznam událostí převážně v textové podobě, který odděluje zdroj událostí (systém, aplikaci) od ukládání a případně zpracování. Jeho přesný popis lze nalézt v RFC 5424 [3]. Data lze posílat buď s využitím TLS [4], nebo skrz UDP [5], který je ze své podstaty sice rychlejší (neprovádí se sestavení sezení), ale také nespolehlivý (UDP pakety mohou být zahozeny).

Protokol je implementován ve všech systémech a existuje mnoho knihoven pro různé programovací jazyky. Z pohledu programátora jde o velmi jednoduchý systém. Jediné, co je nutné znát pro efektivní práci, je vytvořit si pravidla, která budou popisovat použití identifikátorů zdroje (v protokolu označované jako „Facility“) a důležitosti (priority). Pro samotný obsah zpráv je vhodné použít buď jeden z některých standardů, o kterých bylo psáno v minulém článku anebo se v rámci týmu dohodnout na vlastním a pevně jej dodržovat (a zdokumentovat).

Logy databázových systémů

Databázové systémy jsou schopny tvořit jak textové logy, které se týkají provozu (připojení uživatelé, pomalé dotazy, chybový log, apod.), tak i binární, které se týkají databázových změn (vytvoření tabulky, změna dat v tabulce, atd.) a používají se hlavně při replikaci nebo obnově stavu.

V databázovém systému MySQL je standardně textové logování vypnuté vyjma zaznamenávání chyb a pomalých dotazů, které slouží pro zlepšení výkonnosti. Pokud je systém v režimu master-slave anebo master-master, lze z něj získat binární log.

Z pohledu forenzní analýzy je nejzajímavější zkoumání textových logů a následně binárních, protože binární logy obsahují pouze změny dat a struktur. Dotazy typu SELECT se v něm neobjeví.

Následující výtažek z textového logu zachycuje průběh extrakce dat:

```
Time                 Id Command    Argument
150207 18:54:29      89 Connect    shop@localhost on
                     89 Query      select @@version_comment limit 1
150207 18:54:34      89 Query      SELECT DATABASE()
                     89 Init DB    shop
150207 18:54:38      89 Query      select number from cards into outfile 'd:\\www\\cc.txt'
```

7. února 2015 v 18:54:29 (časová zóna není v záznamech zanesena, je potřeba ji získat z nastavení systému) se do databáze připojil uživatel `shop` z rozhraní `localhost`. Jde tedy o přístup vyvolaný z lokálního prostředí. V 18:54:34 došlo k otevření databáze `shop` a o 4 vteřiny později k extrakci sloupce `number` do souboru `d:\www\cc.txt`.

Log nezachycuje skutečnost, jestli k extrakci dat skutečně došlo. Databázový systém mohl zamezit vytvoření souboru z důvodu chybějících oprávnění. K zodpovězení této otázky je potřeba získat informace z dalších systémů. Podle záznamů výše jde pravděpodobně o webový server ukládající informace o platebních nebo věrnostních kartách (úvaha je založena na jménu uživatele shop a na skutečnosti, že došlo k přihlášení přes `localhost`, což indikuje, že na stejném serveru běží webový server a skripty přistupují do databáze; není zohledněna skutečnost, že nemusí být naplněny požadavky PCI SSC DSS [6]). Pokud byl poskytovaný obsah webovým serverem uložen v adresáři `d:\www\` a v tzv. access logu by byl nalezen záznam s URI souboru, odpovědí `200` a nenulovou délkou, pak byla data nejen úspěšně extrahována, ale také zcizena. Dalším vodítkem pak je i skutečnost, že logy webového serveru obsahují i IP adresu, ze které požadavek přišel.

V binárním logu takovou aktivitu nelze najít, protože nedošlo k modifikaci žádné tabulky či dat. Následující ukázka zachycuje změnu nad tabulkou `cards`:

```
BEGIN
/*!*/;
# at 199
#150207 19:19:31 server id 1  end_log_pos 313 CRC32 0x26f3d741  Query  thread_id=1
exec_time=0 error_code=0

use `shop`/*!*/;
SET TIMESTAMP=1423333171/*!*/;
update cards set number='xxxxxxxxxxxxxx'
/*!*/;

# at 313
#150207 19:19:31 server id 1  end_log_pos 344 CRC32 0x3ce532c0  Xid = 8
COMMIT/*!*/;
```

Na rozdíl od textového logu binární log nezachycuje, který uživatel změnu provedl. Je to z toho důvodu, že binární logy jsou primárně určeny k replikaci změn a k tomu se používá dedikovaný databázový účet. Informace o autorovi změny je tím pádem zbytečná.

Pokud databázový systém provádí nějaké logování, je pravděpodobnější, že je zakládán binární log než textový zachycující všechny operace nad databází. Avšak jakákoliv informace je užitečná při skládání celkového obrazu.

Akvizice logů

Lokální síť

Většina logů se získá společně s pořízením digitálního obrazu disku, popř. disků při zajišťování digitálních stop. Je ideální se seznámit i s topologií sítě a službami, které jsou v dané síti poskytovány.

Ve vysoce zabezpečených sítích je možné také narazit na monitorovací službu, která zaznamenává veškerý síťový provoz anebo provádí kontrolu obsahu – tzv. DLP systémy [7]. Tyto systémy mohou při analýze poskytnout cenný zdroj informací. Většinou jsou založeny na databázovém systému, ve kterém lze snadno a rychle vyhledávat.

Vzdálená síť

Aktuálně jsou hojně využívány tzv. Cloudové služby [8]. Jde o formu pronajímání hardwaru, výkonu, platformy, služby, aplikace, uložiště, někdy také označovanou termínem SaaS. Pro vývojáře a firmy jde o zajímavý koncept, kdy snadným způsobem lze zajistit výpočetní výkon a následně provést instalaci aplikace. Problém nastává v případě akvizice logů z daného systému. Nejenže je vlastněn třetí osobou, která má sídlo většinou v zahraničí, ale také na jednom systému může běžet více aplikací nebo být umístěna data i osob, které nejsou předmětem analýzy. V takovém případě nezbývá než se obrátit na provozovatele služby.

Ochrana logů

V drtivé většině případů, kdy je log v textové podobě, není přítomna žádná interní ochrana. Jejich integrita a dostupnost je založena na přístupových oprávněních na úrovni ope-

račního systému, nebo následně pomocí hashů. Výjimečně se lze potkat s digitálním podpisem.

Systémy založené na UNIX

U UNIX systémů je lze nalézt ve složce `/var/log/` a všechny aplikace by měly ukládat své logy do tohoto adresáře nebo ještě lépe do vytvořeného podadresáře.

Každá distribuce řeší oprávnění individuálně. Například v distribuci Ubuntu je chráněn oprávněními

```
drwxrwxr-x root  syslog
```

což znamená, že pouze systémový superuživatel `root` a členové skupiny `syslog` mohou provádět modifikaci nad adresářem, všichni ostatní mohou číst jeho obsah. V distribuci CentOS má adresář oprávnění

```
drwxr-xr-x root  root
```

takže pouze `root` je oprávněn provádět změny nad adresářem. Uvnitř adresáře se pak nacházejí různé podadresáře a soubory služeb běžících v systému, které jsou chráněny individuálními nastaveními.

Nejzajímavějšími logy z forenzního pohledu jsou:

`/var/log/syslog` nebo `/var/log/messages` obsahující zprávy ze Syslog služby,

`/var/log/secure` obsahuje informace vztahující se k autorizace a autentizaci,

`/var/log/wtmp` nebo `/var/log/utmp` obsahují informace o aktuálně přihlášených uživatelích v systému.,

`/var/log/btmp` a `/var/log/faillog` obsahují informace o neúspěšných pokusech o přihlášení,

`/var/log/httpd/` nebo `/var/log/apache2`, či `/var/log/lighttpd/` jsou nejčastější adresáře, ve kterých lze nalézt provozní logy webového serveru,

`/var/log/audit/` je adresář, do kterého systém standardně ukládá informace o změnách v systému, pokud je auditovaní povoleno.

Windows

Systém Windows vývojářům nabízí centralizovaný Správce událostí (Event manager), do kterého lze zasílat aplikační informace. Další alternativou je, že se aplikace postará o ukládání logů sama. Výhody každého přístupu byly popsány v minulém díle.

Pokud se vývojář rozhodne nevyužít Správce událostí, potom má několik míst, kam ukládat své logy:

► Do adresáře s aplikací, ale zde může dojít k problémům s přístupovými oprávněními, pokud aplikace neběží jako služba anebo je spuštěna uživatelem s nedostatečnými oprávněními nad adresářem, ve kterém je aplikace nainstalována (Standardní uživatel).

► Do adresáře označovaný jako AppData (zpravidla `C:\Users\%username%\AppData\`; přesné umístění je uloženo v systémové proměnné `%APPDATA%`) [9].

► Do tzv. TMP adresářů a to buď systémového (zpravidla `C:\WINDOWS\TEMP`) anebo uživatelského, který je uložen v uživatelském AppData adresáři (zpravidla `C:\Users\%username%\AppData\Local`

\Temp). Pokud je zvolena tato možnost, je nutné vzít v potaz, že jde o prostor určený pro ukládání dočasných informací a může být kdykoliv vymazán.

► Poslední možnost, která je krajně uživatelský nepřívětivá, je ukládání informací na Plochu uživatele.

Určitě je vhodné se zmínit, že programátor může uložit citlivé informace do tzv. alternativního datového streamu (ADS) v NTFS, který je uživateli a forenznímu analytikovi bez hlubšího zkoumání skryt. Základní informace o ADS lze nalézt v [10]. Avšak takový způsob logování je silně nepraktický, protože standardní uživatel není schopen takový log připojit do reportu. Nicméně, jeho existence by měla vzbudit v analytikovi okamžitý zájem.

Kontrolní součty

Textové i binární logy lze ochránit před jednoduchou manipulací pomocí kontrolních součtů. Log se rozdělí na bloky (může být i celý soubor), ke kterým se provede součet libovolnou jednosměrnou hashovací funkcí (např. MD5, SHA1, SHA256, SHA512, atd.) Nevýhodou takového přístupu je, že potenciální útočník po změně provede přepočet a nahradí kontrolní součet novou hodnotou.

Menší vylepšení pak spočívá v zavedení sdíleného tajemství, které je známo pouze aplikaci generující logy a čtecímu softwaru. Toto sdílené tajemství (většinou řetězec náhodných znaků) se připojí k bloku a aplikuje se hashovací funkce. Tento přístup dokáže eliminovat změny, pokud útočník neprovedl dekompilaci programů a nenalezl tajemství i místo, kam se vkládá před hashováním. Ale aby takový postup měl smysl, sdílené tajemství se musí udržet mezi generátorem logů a čtečkou, což jde proti masivnějšímu používání.

Mnohem elegantnější je zavedení digitálního podpisu [11]. Z bloku dat se spočítá kontrolní součet některou z výše uvedených funkcí, který se následně zašifruje privátním klíčem. Takový postup zajistí integritu a nepopiratelnost. Nevýhodou je časová náročnost pro výpočet a nutnost chránit privátní klíč.

Archivace

Dobrou ochranou logů je také jejich archivace. Čím dříve jsou zkopírovány na zálohovací médium, tím menší čas má útočník pro modifikaci logů. Archivy mohou být při přenosu šifrovány nebo digitálně podepsány, jak bylo popsáno v předchozí kapitole, protože v celém systému jsou správci zálohování, kteří mají přístup k zálohám a zálohovaným systémům.

Alternativou i vhodným doplňkem k zálohovacím médiím je ukládání logů do cloudových řešení a tzv. „off-site“ lokací.

Analýza logů

Analyzovat logy je nejen tzv. „best-practice“ pro odhalení narušení bezpečnostního perimetru a podvodů, ale také tzv. „must have“ v určitých prostředích. Například v systémech, ve kterých se pracuje s informacemi z platebních karet, musí být splněn požadavek PCI DSS (v současné době ve verzi 3) [12]. Společnosti, které jsou veřejně obchodovatelné v USA nebo obchodující na území Spojených států, musí splňovat požadavky kladené zákonem Sarbanes – Oxley [13] zaměřeným především na oblast účetnictví.

Kromě manuální revize, která je vhodná na menší množství logů, anebo na detailní zkoumání konkrétních nálezů, je praktičtější nasazení automatizovaných systémů. Jejich architektura je založena na jednom z následujících principů:

► Bez agenta – logy jsou zasílány/sbírány do definovaného kolektoru, ve kterém se provádí analýza.

► S agentem (též známé jako Host-based IDS) – na hlídaném zařízení, systému je nainstalován specializovaný software (agent), který permanentně monitoruje vybrané oblasti (registry, systémové adresáře, logy) a provádí analýzu. Výsledek je pak zaslán do monitorovacího systému nebo je upozorněna obsluha.

Komerčně používané systémy v sobě obsahují předdefinovanou sadu pravidel, většinou jde buď o řetězce nebo regulární výrazy, které definují závažnost události a někdy i automatizované provedení protiakce (zablokování účtu, IP adresy, apod.) Některé systémy dokáží zvyšovat závažnost v čase (např. pokud bylo provedeno 10 neúspěšných přihlášení do systémů v posledních 30 vteřinách pro uživatele `root`, potom jde pravděpodobně o útok hrubou silou).

Poměrně vyčerpávající doporučení, které se zabývá problematikou Log Management systémů, vydal National Institute of Standards and Technology (NIST) pod označením SP 800-92 [14].

Závěr

Zvolit správný způsob ukládání s ohledem na předpokládaný budoucí vývoj je těžké. Při návrhu je vhodné začlenit i integritní kontrolu. Nejjednodušší je po rotaci logu připojit kontrolní součet a soubory uložit mimo provozní systém.

Pro včasnou detekci narušení bezpečnostního systému je vhodné zvážit implementaci automatizovaného analyzátoru logů s možností spuštění protiakce a vyhlášení poplachu.

Další díl bude zaměřen na útoky proti logům, jak je poznat a jak se bránit.

Bibliografie

Log management. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2015 [cit. 2015-02-01]. Dostupné z: http://en.wikipedia.org/wiki/Log_management

Single point of In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/Single_point_of_failure

GERHARDS, R. RFC 5424: The Syslog Protocol. ADISCON GMBH. RFC 5424 [online]. 2009 [cit. 2015-02-01]. Dostupné z: http://tools.ietf.org/html/rfc5424

Transport Layer Security. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-07]. Dostupné z: http://cs.wikipedia.org/wiki/Transport_Layer_Security

User Datagram Protocol. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-07]. Dostupné z: http://cs.wikipedia.org/wiki/User_Datagram_Protocol

PCI SSC Data Security Standards Overview. PCI SECURITY STANDARDS COUNCIL, LLC. Official Source of PCI DSS Data Security Standards

Documents and Payment Card Compliance Guidelines [online]. © 2006 - 2015 [cit. 2015-02-07]. Dostupné z: https://www.pcisecuritystandards.org/security_standards/index.php

Data loss prevention software. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-07]. Dostupné z: http://en.wikipedia.org/wiki/Data_loss_prevention_software

Cloud computing. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-07]. Dostupné z: http://en.wikipedia.org/wiki/Cloud_computing

Co je složka AppData?. MICROSOFT. Windows [online]. © 2015 [cit. 2015-02-11]. Dostupné z: http://windows.microsoft.com/cs-cz/windows-8/what-appdata-folder

Pomoc a podpora. MICROSOFT. How To Use NTFS Alternate Data Streams [online]. © 2015 [cit. 2015-02-11]. Dostupné z: http://support.microsoft.com/kb/105763/en-us

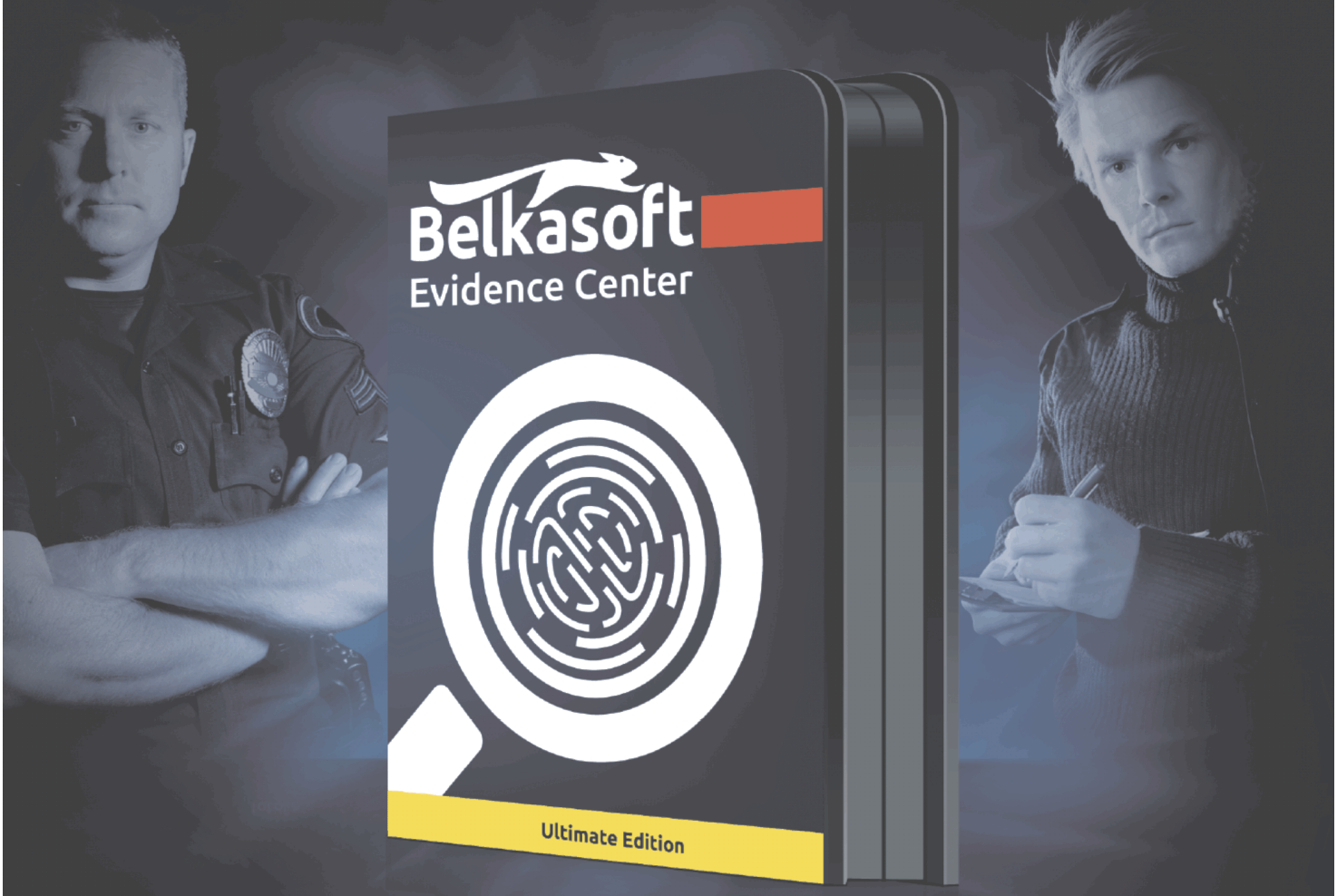
Public-key cryptography. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-11]. Dostupné z: http://en.wikipedia.org/wiki/Public-key_cryptography

Requirement 10: Track and monitor all access to network resources and cardholder data. Payment Card Industry (PCI) Data Security Standard [online]. Listopad 2013, s. 82-88 [cit. 2015-02-12]. Dostupné z: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Sarbanes–Oxley Act. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-02-12]. Dostupné z: http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

KENT, Karen a Murugiah SOUPPAYA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology [online]. 2006 [cit. 2015-02-12]. NSIT SP 800-92. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Why new Belkasoft Evidence Center 2015



Is a forensic tool of choice around the globe? *

* Purchased by several thousands of forensic investigators in around 70 countries worldwide

Belkasoft
forensics made easier

Prodej a podporu v ČR a SR zajišťuje:
Risk Analysis Consultants, s.r.o.
Španělská 2
120 00 Praha 2
zu@rac.cz
www.rac.cz

RAC®

C4e CyberCrime Training March 2015

Intezivní pětidenní školení C4E pro Policii ČR

Ing. Marián Svetlík st., vedoucí Znaleckého ústavu RAC, soudní znalec v oboru Kriminalistika, specializace Kriminalistická počítačová expertíza.

Anotace:

České centrum excelence pro kybernetickou kriminalitu (C4e) zorganizovalo ve spolupráci s Odborem bezpečnostního výzkumu a policejního vzdělávání MV ČR intenzivní komplexní pětidenní školení v oblasti kybernetické kriminality pro vybrané zástupce různých policejních složek.

Úvod

Školení bylo původně domlouváno pro specifickou skupinu účastníků - pro učitele policejních škol - jako jeden z výstupů projektu Czech Cybercrime Centre of Excellence (C4e).

Po obsahové stránce bylo připraveno jako průřezové, od problematiky právních a procesních aspektů práce s elektronickými, resp. digitálními důkazy, přes otázky spolupráce policejních složek se specialisty na informační bezpečnost, a to zejména ve vztahu k Zákonu o kybernetické bezpečnosti (ZoKB), až konečně na otázky konkrétní práce s digitálními stopami, od jejich identifikace, zajištění, manipulace, přes procesní a technické otázky expertíz digitálních stop a jejich znaleckého zkoumání a konče využitelností digitálních důkazů při vyšetřování různých druhů trestné činnosti.

Původní cílová skupina posluchačů - učitelů policejních škol - byla vybrána ze dvou důvodů:

► jednak to bylo proto, že záměrem tohoto školení bylo dostat základní pozantky problematiky kybernetické kriminality a práce s digitálními stopami právě do prostředí policejních škol, aby byly dány základy pro jejich předávání co nejširší skupině policistů;

► druhým důvodem byl zájem, který učitelé policejních škol sami projevili právě v této oblasti a původně se sami

Tak, dost povídání, už nám zbývá tak nanejvýš 5 minut, abychom stihli ten začátek...

přihlásili k nabídce C4e na pořádání takovýchto školení. Navíc sami iniciativně připomínkovali prvotní nabídku a vznášeli další praktické požadavky na obsah takvého školení.

Nakonec školení, z pohledu sestavy účastníků, dopadlo docela jinak. Dalo by se říci, že téměř na poslední chvíli se na školení přihlásili další zájemci téměř ze všech důležitých policejních útvarů. Nás to z jedné strany potěšilo, protože jsme přesvědčeni o důležitosti problemaitky pro policejní práci. Z druhé strany nás to postavilo před situaci, kdy bylo nutné v rámci domluveného programu upravit na poslední chvíli obsah a rozsah jednotlivých témat a přizpůsobit, v rámci daných možností, novým posluchačům i způsob a míru detailu výkladu.

K programu

Celé školení bylo naplánováno na pět dní. Abychom příliš nevytrhávali účastníky z jejich náročného pracovního programu, rozdělili jsme celé školení do dvou týdnů. V prvním týdnu to byly tři dny (23. - 25. března) a v dalším týdnu zbylé dva dny (30. a 31. března).

První den školení byl věnován právním a procesním otázkám kybernetické kriminality a související problematice. Konkrétně se jednalo o pondělí 23. 3. 2015, kdy hlavním tématem byly právní a procesní problematika digitálních stop a digitálních důkazů při odhalování a vyšetřování kyberkriminality a specifika této trestné činnosti.

Z přednášek pracovníků Ústavu práva a technologií Právnické fakulty Masarykovy univerzity lze zmínit představení výsledků práce C4e na problematice vytvoření společného jazyka (slovníku) vyšetřovatelů a specialistů informační bezpečnosti. Problém spočívá v tom, že byť se věcně jedná o stejnou věc, vyšetřovatelé mluví jazykem trestního zákona a technici používají k popisu toho samého odbornou terminologii, a proto si navzájem velice často nerozumí. Přitom těsná spolupráce obou je nutná. Byly probrány i další okruhy otázek. Praktické problémy byly řešeny díky výkladu státního zástupce pana Píše, který podrobně mluvil o aktivitách státního zastupitelství v této oblasti, což

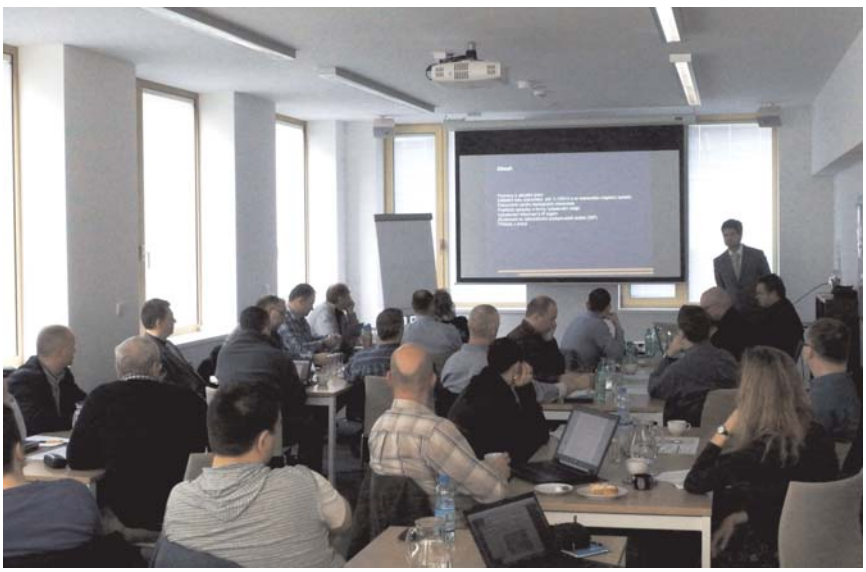
Je nakročeno správným směrem k vytvoření společného jazyka právníků a techniků

Právníci s techniky se teď už lehce domluví

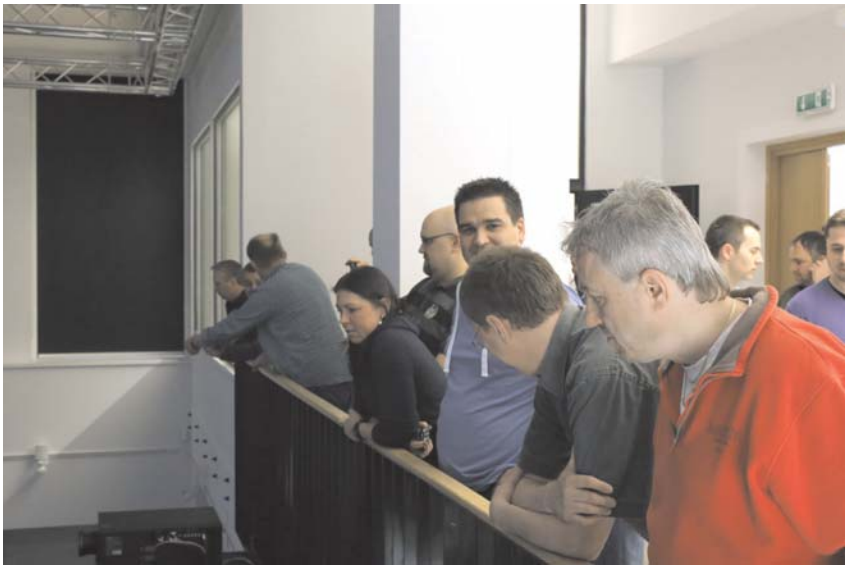
bylo pro posluchače nesmírně důležité. Další přednášející vysvětlovali např. mezinárodní souvislosti kybernetické kriminality.

Druhý den školení byl pod záštitou specialistů Ústavu výpočetní techniky Masarykovy univerzity a byl věnován technické stránce vyšetřování internetové kriminality. Vysvětleny byly procesy, které souvisí s reakcemi na bezpečnostní incidenty, základní postupy z pohledu digitálních stop, identifikace podezření z trestné činnosti při řešení bezpečnostních incidentů, zajišťování digitálních stop třetí stranou, co by měl umět a dělat „information security manager“ (člen CERT) a co by od něj měla/mohla požadovat policie. Byly popsány praktické zkušenosti z vyšetřování několika případů zneužití internetu a kroků, které byly podniknuty ze strany specialistů na informační bezpečnost - CERT týmu Masarykovy univerzity - která je jedním z průkopníků těsné spolupráce s OČTŘ.

Velice zajímavou částí tohoto dne bylo praktické cvičení, kdy si účastníci na vlastní kůži zkusili práci na unikátním



Zkušenosti státního zastupitelství jsou pro policii důležité.



Tam dole, kam z galerie všichni upínají zrak, je ten zázrak - sál a zároveň laboratoř KYPO

systému pro analýzu dějů v počítačových sítích - cvičení na "Kybernetickém polygonu" KYPO. Pravda, necvičili v samotných prostorách laboratoře KYPO, protože prostory laboratoře ještě vlastně ani nebyly v době školení dokončeny. Samotnou laboratoř KYPO ve stavu před dokončením a oficiálním uvedením do provozu si účastníci jen prohlédli. Cvičení samotné probíhalo v učebně, protože systém KYPO umožňuje vzdálené připojení účastníků i přes internet, tudíž účastníci nemusí jezdit cvičit do Brna, ale mohou se zdokonalovat i na dálku.

KYPO je skutečně unikát, nejenom v českém, ale vlastně i v celosvětovém měřítku. Obdobných systémů je ve světě jen několik. KYPO umožňuje v přísně kontrolovaném a monitorovaném virtuálním prostředí jednoduše simulovat prakticky libovonlnou síťovou konfiguraci a na takovémto modelu zkoumat a procvičovat různé situace, kybernetické útoky, šíření virů a samozřejmě také procvičovat vědomosti a dovednosti v boji proti takovým kriminálním aktivitám.

Další tři dny školení patřili digitálním

KYPO se díky vzdálenému přístupu dočasně "přestěhovalo" do učebny

Ano, šedivá je teorie, i teorie digitální stopy

stopám, jejich identifikaci, zajišťování, manipulaci, zkoumání a využití získaných digitálních důkazů ve vyšetřování. Všechny tři dny proběhli pod záštitou experů Znaleckého ústavu RAC.

Důležitým aspektem digitálních stop je skutečnost, že jejich využití ve vyšetřování se nevztahuje pouze na případy informační nebo kybernetické kriminality, jak jsou definovány tresním zákonem. Digitální data jsou v současnosti důležitým zdrojem kriminalisticky relevantních informací při vyšetřování prakticky libovoného druhu trestné činnosti.

Aby bylo možné zařadit digitální stopy do systému kriminalistických stop, byly podány základy teorie digitální kriminalistické stopy a byly podrobně popsány a vysvětleny základní vlastnosti digitální stopy.

Podrobně byly vysvětleny zásady a pravidla práce s digitálními stopami, která právě vycházejí z popsaných vlastností. Značná pozornost byla věnována právě zajišťovacím úkonům, protože nezajištěná stopa neposkytne očekávané informace a špatně zajištěná stopa může poskytnout informace zkreslující nebo dokonce falešné.

Od teorie k prvním praktickým krokům

Přípravu bych v žádném případě nepodceňoval...

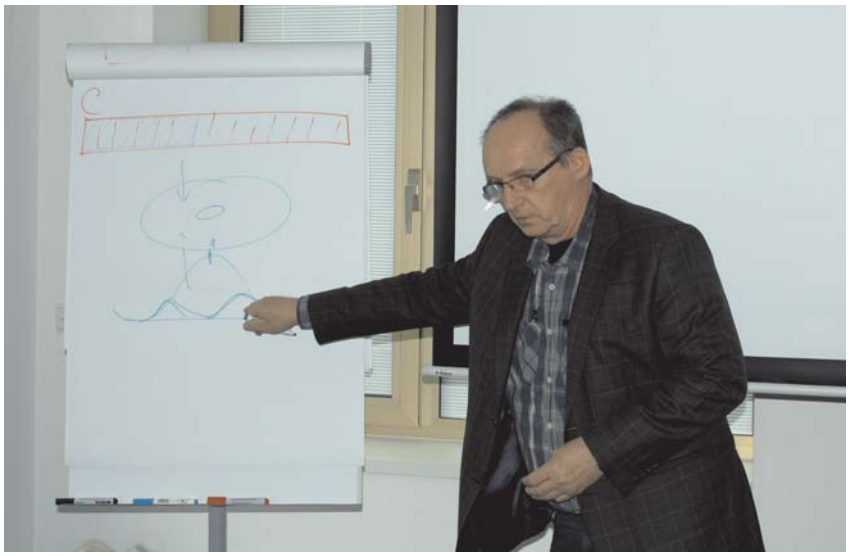
Jako jeden z klíčových parmetrů úspěchu při práci s digitálními stopami byla podrobně popsána etapa důkladné přípravy. Nejenom vědomosti, zkušenosti a dovednosti, nejenom relevantnost a celistvost digitálních stop, ale vůbec samotná příprava na práci s digitálními stopami je pro jejich efektivní využití při vyšetřování důležitým prvkem.

Podobně byly dopodrobna popsány a vysvětleny i další etapy práce s digitálními stopami.

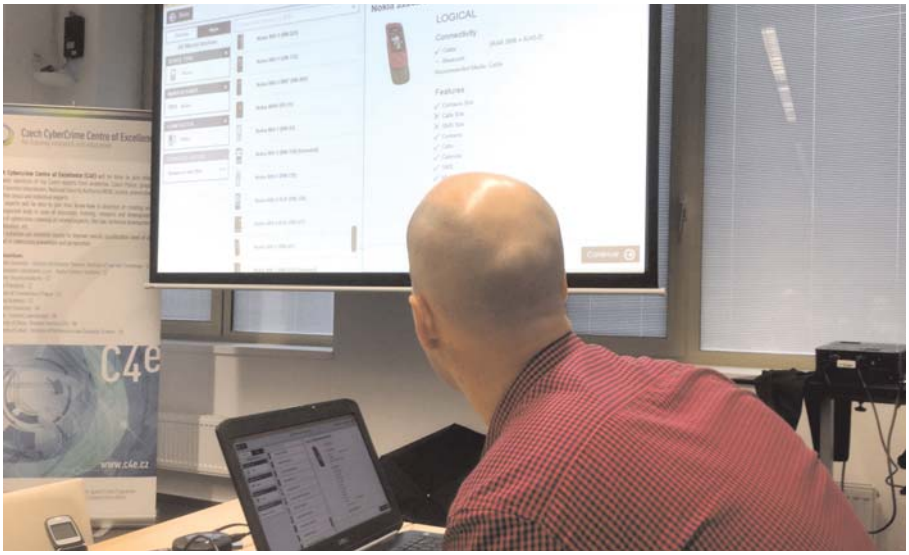
Školení probíhalo v pracovní atmosféře. Množství dotazů a připomínek z praxe svědčilo o velkém zájmu posluchačů i o tom, že problematika digitálních stop je nanejvýš aktuální a potřeba obdobných školení je pro praktickou policejní práci důležitá.

Vznesené dotazy se týkaly velice různorodého spektra problémů. Od vysloveně teoretických úvah z oblasti fyzikálních principů práce prostředků výpočetní techniky, přes technické a procesní otázky až po metodiky řízení činností techniků a expertů.

Přínosem školení také bylo to, že mnoho otázek bylo zodpovězeno samotnými



Že by ten zelený létající talíř vyhloubil až takový kráter?



Vše je pod kontrolou, na plátně se zobrazuje skutečně ten mobil, co má.

účastníky školení. Z tohoto pohledu bylo vlastně užitečné, že nakonec byli účastníci z různých součástí policie s různými zkušenostmi z práce s digitálními stopami. To umožňovalo praktickou výměnu poznatků nejenom směrem k účastníkům, ale i mezi nimi samotnými.

Závěr

Přestože školení probíhalo intenzivně celých pět dní, potvrdilo se, že to stačilo pouze k podání základních, přehledových informací a poznatků. Problematika digitálních stop, jejich vytěžitelnost a použití při vyšetřování kybernetické kriminality a vlastně i celého spektra jiných trestných činů je nesmírně široká.

Ukazuje se, že **právní, procesní, technické, forenzní a kriminalistické aspekty digitálních stop nejsou zatím systematicky propracované**, nehledě na to, že jejich důležitost byla v průběhu celého školení potvrzována nejenom přednášejícími, ale zejména prakticky všemi účastníky.

Některé dotazy daly skutečně zabrat, ale ve výsledku to stálo za to...

V žádném případě to však neznamená, že by jednotlivé vědomosti účastníků byly jakkoliv zpochybňovány. Naopak, **prakticky každý účastník školení projevil značné zkušenosti a vědomosti ve své oblasti**. Problém je však pravděpodobně v tom, že:

► Jednotlivé vědomosti, poznatky a zkušenosti účastníků **netvoří ucelený systém**, ze kterého by, jako ze základní vědomostní a poznatkové báze, měli jednotliví specialisté vycházet podle konkrétního profesního zaměření a specifiky vykonávané práce.

► Mnohdy **unikátní poznatky a zkušenosti vycházejí z nutnosti ad-hoc** vyřešit zadaný problém bez systematického začlenění a odpovídající návaznosti na další rozvoj nebo na spolupracující součásti.

► Nesystematický přístup způsobuje, že (lidské, materiální, finanční) **prostředky se čerpají někdy neefektivně**, používají se na činnosti, které se, bez znalosti systematického začlenění a uceleného pohledu na problematiku, se mohou ukázat jako zbytečné nebo neúměrné řešenému problému.

Pravděpodobně to ale není chybou účastníků ani ostatních součástí Policie ČR. Již několikrát a na několika místech bylo zdůrazňováno, že problematika informační společnosti, digitálních informací, jejich zneužití, ale i využití digitálních dat při vyšetřování a postihování trestné činnosti je komplexní vědecký a společenský problém, který vyžaduje ucelený přístup napříč všemi oblastmi, do kterých zasahuje.

Právě realizované školení bylo náznakem takového propojení všech oblastí, které se na problematice vyšetřování trestné činnosti spojené s informačními a komunikačními prostředky podílejí. Právo, proces, technologie, kriminalistika a forenzní vědy musí být v tomto případě účelně a efektivně propojeny nebo spíše vhodně spojeny do uceleného systému vědomostí a poznatků.

Není to problematika jednoduchá a pravděpodobně zatím nikdo nezná její jednodoché a přímočaré řešení, nejenom u nás, ale ani ve světě. Ale nehledě na to, jak budeme definovat informační společnost, problematika života společnosti v prostředí digitálních technologií je aktuální a vyžaduje systémové řešení.

Náznakem takového řešení bylo právě popsané školení. Jsem přesvědčen, že všichni účastníci, ale i přednášející, jsou si vědomi této potřeby, potřeby pokračovat v tomto nebo podobném formátu výměny a předávání zkušeností a poznatků napříč všemi zmíněnými oblastmi. Je však zcela zřejmé, že diskutovat a předávat poznatky je potřebné, ale nedostatečné. Je také nutné vytvořit a podporovat snahy všech zainteresovaných (aniž bych předesílal, že právě C4e má ve svém poslání řešit tyto otázky) soustřeďovat tyto poznatky, podrobovat je kritické analýze, přebírat intenzivně zkušenosti ze světa, neustále a systematicky zkoumat vývoj v této a souvisejících oblastech a vytvářet podmínky pro systémové a systematické řešení tohoto komplexního a multidisciplinárního problému.

C4e Cybercrime Training 2015 byl organizován v rámci projektu Czech CyberCrime Centre of Excellence for training, research and education a s podporou Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Digital Forensic InfoDay III Bratislava

První setkání RAC a našich slovenských kolegů - specialistů digitální forenzní analýzy

Ing. Marián Svetlík st., vedoucí Znaleckého ústavu RAC, soudní znalec v oboru Kriminalistika, specializace Kriminalistická počítačová expertíza.

Anotace:

Společnost Risk Analysis Consultants, s.r.o., jako klíčový partner Českého centra excelence pro kybernetickou kriminalitu (C4e) a za významné pomoci Znaleckého ústavu Elektrotechniky a informatiky FEI Slovenské technické univerzity v Bratislavě, pokračovala v organizaci populárních akcí typu DigitalForensic InfoDay, tentokráte už potřetí a tentokráte v Bratislavě.

RAC InfoDay

V minulém čísle tohoto časopisu jsme podrobněji popsali akce typu Digital Forensic InfoDay (DFID). Ani tento bratislavský se v principu od těch ostatních příliš neodlišoval. Ale v něčem přece.

Koncem minulého roku jsme navázali těsnější spolupráci se Slovenskou technickou univerzitou v Bratislavě, přesněji řečeno se Znaleckým ústavem elektrotechniky a informatiky FEI STU (ZUEI). Co je zajímavé je skutečnost, že impulzem k této těsné spolupráci byl právě první DFID v květnu loňského roku, kde jsme se potkali s p. Osterem, který je gestorem vzdělávání slovenských znalců právě za obor informatiky. A tam vznikla myšlenka spolupráce a i organizace DFID na Slovensku.

DFID III, Bratislava, 10. dubna 2015

Od nápadu nebylo daleko k realizaci a 10. dubna 2015 jsme se sešli v Bratislavě, v hotelu Apollo, na třetím DFID.

Společně se ZUEI se nám povedlo před akcí oslovit široké spektrum potenciálních zájemců o tuto akci a je potřebné zdůraznit, že aniž bychom vyvinuli néja-

Pan profesor Smola, ředitel ZUEI FEI STU, osobně přivítal účastníky DFID

Pro pochopení souvislosí jsme začali i trochou teorie

kou výjimečnou aktivitu vůči zvaným hostům, nakonec jsme byli dokonce přinuceni některé zájemce odkázat na příští DFID, protože kapacita konferenčních prostor byla beznadějně zaplněna.

Úvod DFID měl také lehce slavnostní nádech. Při příležitosti první společné akce Znaleckého ústavu RAC a ZUEI FEI STU přišel přivítat a pozdravit účastníky také ředitel ZUEI, pan profesor Smola.

Pak už přišly na řadu odborné přednášky. I tady jsme provedli změny oproti předchozím DFID. Čistě praktické přednášky a představování nástrojů a prostředků pro digitální forenzní analýzu bylo doplňováno i pasážemi z teorie digitálních stop.

Zajišťování digitálních stop patří ke klíčovým činnostem

Představení NUIXu na Slovensku proběhlo z těch nejkvalifikovanějších úst

Naši slovenští kolegové také měli trochu víc štěstí v tom, že (na rozdíl od našeho druhého DFID v ČR) se nám nakonec povedlo zajistit účast experta společnosti NUIX, Andrease Friberga, který dopoledne podrobně představil na našem trhu nový produkt pro digitální forenzní analýzu, NUIX Investigator.

Zájemci také měli možnost si odpoledne s Andreasem pohovořit o detailech NUIXu i separátně a povyzvídat další podrobnosti, specifika konkrétní implementace nebo si nechat vysvětlit případné nejasnosti.

Musím také přiznat, že nejenom účastníci akce, ale i my jsme tuto možnost využili a dozvěděli se mnohé ze zákulisí a i přímo z kuchyně, kde se tento uni-

Pan Andreas Friberg podrobně objasnil základní koncept analytického nástroje

Program DFID byl doplněn dalšími forenzními nástroji, včetně nástroje XRY pro analýzu mobilů

kátní a velice výkonný forenzní analytický nástroj připravuje. O některé z poznatků se s vámi podělíme při příležitosti některého příštího DFID.

Účastníkům byly představeny i další nástroje, které jsou pro účely digitální forenzní analýzy běžně používány. Naši slovenští kolegové projevovali zájem zejména o produkty Belkasoft Evidence Center a Internet Evidence Finder, ale samozřejmě, i díky profesionálnímu představení, NUIX byl jedním z lídrů jejich zájmu.

Závěr

Jak již bylo uvedeno, náš třetí DFID, tentokráte v Bratislavě, se vyznačoval

Pozornost účastníků svědčila o aktuálnosti poskytovaných informací

Příjemná atmosféra napomáhala neformálním diskusím

i několika odlišnostmi oproti těm předchozím. Kromě toho, že byl první na Slovensku, bylo znatelné, že pro účastníky to byla akce ojedinělá svou náplní i poskytnutými informacemi.

Přirozeně jsme využili nejenom oficiální program, ale i diskuse při přestávkách k neformálním rozhovorům s účastníky. Tito nám jednoznačně potvrdili, že DFID je akce, která na Slovensku ještě nebyla a že pro převážnou většinu účastníků byla unikátní, podnětná a ve svém důsledku i velice užitečná.

Jako první akce tohoto druhu na Slovensku byl tento DFID trochu stručnější, v průběhu jednoho dne jsme se mohli věnovat pouze některým aspektům digitální forenzní analýzy a nebyl dostatek času zacházet do podrobností. Tuto skutečnost jsme diskutovali s našimi partnery ze ZÚEI FEI STU a domlouvali jsme pokračování v organizaci DFID na Slovensku s tím, že bychom společně vytipovali aktuální témata, která bychom příště chtěli představit podrobněji.

RAC Digital Forensic InfoDay vol III v Bratislavě byl organizován v rámci projektu Czech CyberCrime Centre of Excellence for training, research and education a s podporou Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Forenzní analýza SQLite databází

Často opomíjená oblast forenzní analýzy

David Makeev, Nikita Timofeev, Oleg Afonin, Yuri Gubanov - Belkasoft.

(do českého jazyka se souhlasem autorů přeložil Marián Svetlík jr.)

Anotace:

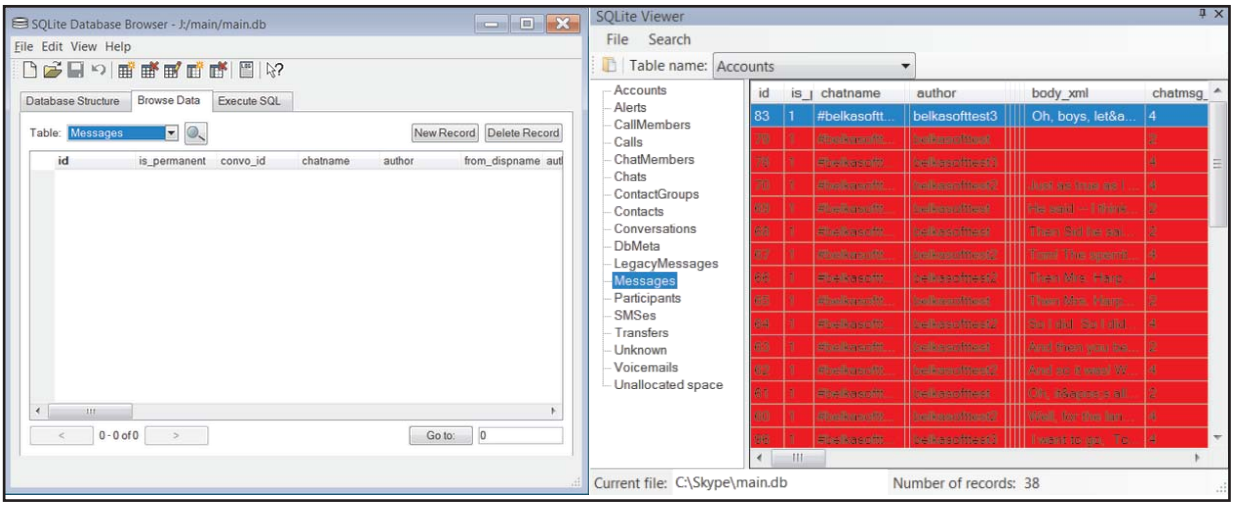
SQLite je populární databázový formát využívaný většinou mobilních i desktopových aplikací. V SQLite formátu ukládají data různé aplikace pro iOS i Android, stejně jako celá řada desktopových i mobilních webových prohlížečů (vč. Chromu a Firefoxu) a instant messengerů (např. Skype, WhatsApp).

Úvod

Forenzní analýza SQLite databází je často opomíjena a omezuje se pouze na jednoduché zobrazení databáze v příslušném prohlížeči. Nevýhodou takového přístupu je neschopnost běžných prohlížečů přistupovat k nedávno smazaným záznamům. V tomto článku se proto z forenzního pohledu podíváme blíže na jednu z funkcí SQLite databází – tzv. freelisty.

Freelisty – přístup ke smazaným záznamům

Nejprve se podívejme, jak SQLite ukládá a spravuje data. Platné záznamy jsou ukládány v jednom databázovém souboru. Tento soubor je rozdělen na stránky o pevné délce, která je specifikována v hlavičce souboru. Každá z těchto stránek může mít jednu z mnoha funkcí (vč. ukládání samotných dat), kterou jí přidělí SQLite engine. Jednotlivým stránkám jsou pak přidělena čísla vzestupně od jedničky.



Rozdíl v zobrazení smazaných zpráv z databáze při použití standardního SQLite prohlížeče a Evidence Center SQLite Viewer

SQLite databáze může obsahovat jednu nebo více nepoužívaných stránek, které byly vytvořeny jako rezerva pro budoucí využití a neobsahují žádná smysluplná data. Nepoužívané stránky jsou v rámci databázového souboru ukládány v tzv. freelistech.

Freelisty jsou používány k uchovávání nových nebo naopak smazaných stránek, dokud tyto nejsou přepsány novými daty. Do té doby tyto stránky reálně existují, nelze k nim však přistoupit prostřednictvím regulérních prostředků databázového enginu. Přitom tyto stránky mohou z pohledu forenzní analýzy obsahovat důležité informace, např. smazané SMS zprávy nebo chatové konverzace. Proto je zpřístupnění informací z freelistů velmi podstatné.

Standardní databázové prohlížeče a SQLite komponenty neumožňují přístup k informacím uložených ve freelistech, proto je více než žádoucí mít v rámci forenzní laboratoře k dispozici nástroj, který tento přístup umožní.

SQLite Recovery and Analysis Tool

Belkasoft Evidence Center je komplexní forenzní nástroj, který se osvědčil v mnoha zemích. Kromě jiných funkcí přichází také s nativním SQLite parsováním, což umožňuje forenznímu expertovi spolehlivou extrakci dat z SQLite databází včetně výše zmíněných informací z freelistů.

Tuto funkcionalitu si můžete vyzkoušet v rámci trial verze na `http://belkasoft.com/trial`.

V další části našeho článku se z pohledu forenzní analýzy podíváme na další vlastnost SQLite databází, tzv. Write Ahead Logy, které obsahují čerstvě vložené a dosud nevykonané příkazy, které mohou rovněž být zdrojem forenzně cenných informací.

Celý článek v angličtině si můžete přečíst na `http://belkasoft.com/en/sqlite-analysis`

Pokyny pro autory

Digital Forensic Journal je odborný časopis, který se věnuje problematice forenzního zkoumání digitálních dat.

Přijímáme články jak specializované, které se věnují konkrétním technickým problémům, tak i informacím v širších souvislostech z oblasti obecných otázek znaleckého zkoumání.

Věnujeme se doporučením a metodickým pokynům, pozornost věnujeme také použití digitální forenzní analýzy v trestně-právních otázkách ale i v procesu šetření bezpečnostních incidentů ICT. Nevyhýbáme se tématiky bezpečnosti ICT ve vztahu k šetření bezpečnostních incidentů, jakož i dalších oblastí použití digitální forenzní analýzy.

Rukopisy jsou přijímány elektronicky na adrese dfj@rac.cz ve všech běžných datových formátech.

Struktura příspěvků je dána v zásadě podle toho, jak jsou uvedeny příspěvky v aktuálním čísle, tedy název, autor (pozice a kontaktní e-mail), anotace a samotný obsah článku. Doporučujeme členit kapitoly a podkapitoly nanejvýše do tří úrovní. Rozsah článku není v principu omezen, doporučujeme nepřesáhnout 10 stran. Obrázky a grafiku vložte do textu příspěvku, aby bylo zjevné jejich umístění v textu a navíc přiložte jako samostané soubory v dostatečné kvalitě.

Případné obsahové nebo technické připomínky redakce k příspěvku budou individuálně projednány s autorem. Příspěvky v zásadě neprocházejí jazykovou korekturou, autor odpovídá za obsah a za věcnou a gramatickou správnost příspěvku.

Příspěvky, které nebudou splňovat výše uvedené základní požadavky, nebudou publikovány.

Rozhodnutí o publikaci příspěvku je ve výhradní kompetenci vydavatele.

Tableau TD2u Forensic Duplicator

Nový TD2u duplikátor s rozhraními

- USB 3.0
- SATA
- SAS
- IDE

Každý TD2u KIT obsahuje

- TD2u forenzní duplikátor
- TP5 univerzální kompaktní adaptér
- 3M > molex-4 napájecí kabel
- SATA signální kabel
- univerzální SAS/SATA signální a nápájecí kabel (3x)
- 3M > SATA napájecí kabel
- IDE signální kabel
- USB-A > mini USB-B kabel
- utěrku na displej

Podpora množství rozhraní

Již čtvrtá generace duplikátorů Tableau provádí imaging dat ve vysokých rychlostech, které přesahují až 15GB/min při současném vypočítávání MD5 a SHA-1 hashí. TD2u umožňuje zajištění digitálních stop ze zařízení s rozhraním USB 3.0, SATA a IDE/PATA. Dále může uživatel vytvářet obraz SAS disků za použití stejného TDP6 modulu, který se používá u TD1 a TD2 duplikátorů.

Nabitý funkcemi

TD2u dokáže vytvořit jednu (1:1), dvě (1:2), nebo tři (1:3) kopie zdrojových disků. Mezi základní funkce patří disk-to-disk (klon) a disk-to-file (image) duplikace, formátování, mazání, výpočet kontrolních sum MD5 a SHA-1, HPA/DCO detekce a odstranění a kontrola prázdného disku. TD2u vytváří výstupy ve formátech DD, .e01, .ex01 a .dmg. Stejně jako u všech produktů společnosti Tableau, firmware TD2u je upgradovatelný skrz Tableau firmware update (TFU) funkci.

Prodej a podporu v ČR a SR zajišťuje:
Risk Analysis Consultants, s.r.o.
Španělská 2
Praha 2
zu@rac.cz
www.rac.cz

Digital Forensic Journal
ISSN (Print): 2336-4750
ISSN (On-line): 2336-4769