Forenzní audit živých

V současné době přibývá systémů, které nelze z nejrůznějších důvodů vypnout. Zároveň se zvyšují objemy dat, které se při vypnutí počítače neukládají, a tradiční metody forenzního zkoumání je tedy nemohou zachytit. Moderní forenzní postupy se proto začínají věnovat i analýze tzv. živých systémů, tedy analýze běžících zařízení nebo informačních systémů.

Tradiční forenzní metody se při analýze informačních systémů soustřeďují na pevné disky a podobná úložiště dat. Prvním krokem forenzní analýzy je vytvoření tzv. forenzní (binární) kopie uložených dat[1]. Používané metody předpokládají, že jsou příslušné systémy v okamžiku tvorby forenzní kopie vypnuté. Další kroky forenzní analýzy pak probíhají na vytvořených kopiích. Informační systémy však stále více interagují s okolním prostředím a řada informací o této komunikaci, která může být pro forenzní zkoumání velmi důležitá, je uložena v paměti počítače, která se při jeho vypnutí maže (tzv. volatilní pamět). Tyto informace mohou být velmi důležité pro interpretaci informací uložených na disku. Data uložená ve volatilní paměti nám mohou mimo jiné poskytnout kontext pro data uložená na disku. Informují nás o spuštěných procesech, přihlášených uživatelích nebo síťových připojeních. Kromě toho obsahuje volatilní paměť informace, které nebyly zapsány na disk, protože jsou toho času ve vyrovnávací paměti. Všechny tyto informace mohou mít z hlediska forenzní analýzy velký význam.

Dalším problémem je skutečnost, že některé informační systémy nelze z nejrůznějších důvodů pro účely forenzního zkoumání vypnout. V takových případech je třeba přistoupit k jejich analýze za chodu.

Situaci dále komplikuje rychle rostoucí kapacita datových úložišť. V důsledku toho je tradiční kopírování časově stále náročnější a v některých případech dokonce nemožné. Podle [1] není manuální analýza dat efektivní už pro disky o velikosti nad 1 GB. V těchto případech však lze použít automatizované nástroje, které pomohou analýzu provést. Pro úložiště dat o velikosti nad 1 TB už je i analýza pomocí nástrojů velmi zdlouhavá a neefektivní.

Všechny tyto důvody vedou ke stále častější potřebě analyzovat systémy, které jsou v chodu (tzv. živé systémy). Je zřejmé, že digitální stopy získávané z takových systémů jsou velmi náchylné ke kontaminaci. Je tedy velmi důležité, aby měli forenzní pracovníci k dispozici vhodné alternativní postupy, které mohou v těchto případech použít a které budou akceptovány v případném soudním řízení.

Tento příspěvek se soustředí na analýzu digitálních stop, které jsou obsaženy ve volatilní paměti, a na postupy, kterými lze tyto stopy analyzovat tak, aby nebyla znemožněna následná tradiční forenzní analýza systému.

Volatilní paměti

Vnitřní paměti moderních počítačů bývají realizovány téměř výhradně pomocí pamětí s libovolným přístupem (RAM). Jedná se buď o statické (SRAM), které se používají pro paměti typu cache, nebo dynamické (DRAM), ty se používají k výrobě operačních pamětí. Obsah obou těchto pamětí se ztrácí krátce po odpojení zdroje napětí. Takovým pamětem říkáme volatilní neboli závislé na napájecím napětí.

V současné době mají i osobní a přenosné počítače od 512 MB paměti výše. Windows 7 např. potřebují pro správné fungování alespoň 1 GB paměti pro 32bitový systém a 2 GB paměti pro 64bitový systém. Takové paměti už mohou obsahovat velké množství forenzně relevantních dat.

Specifické problémy forenzní analýzy živých systémů

Forenzní analýza živých systémů musí řešit minimálně dva zásadní problémy. Prvním je skutečnost, že data na běžícím počítači se neustále mění. Tato skutečnost sama o sobě digitální stopy

[1] V praxi jde o kopírování celého obsahu pevného disku (případně jiných úložišť dat) metodou bit-by-bit. Tato metoda kopíruje přesně celý harddisk bez ohledu na adresářovou strukturu. Zkopíruje tedy také např. vymazané nebo porušené soubory.

získané z živých systémů neznehodnocuje. Je však třeba počítat s tím, že získané digitální stopy jsou odrazem stavu systému v konkrétním okamžiku a že v budoucnu nebude možné stejným postupem naprosto identické stopy získat. Přesto mohou tyto stopy obsahovat velmi cenné informace.

Druhým problémem je schopnost dokumentace změn, které nastaly v důsledku forenzní analýzy živého systému tak, aby mohly být vzaty v úvahu při pozdější tradiční forenzní analýze. Jedním ze základních principů tradiční forenzní analýzy je, že žádná aktivita nesmí měnit data uchovávaná v informačních systémech nebo médiích pro ukládání dat, která budou později prezentována jako digitální důkazy. Forenzní analýza živého systému zanechá v systému digitální stopy stejně jako každá aktivita. Je třeba vědět, které stopy to jsou, a umět je identifikovat při případné pozdější tradiční forenzní analýze.

Současné metody forenzní analýzy živých systémů se v některých případech spoléhají na funkčnost operačního systému. Pokud by byl tento operační systém jakýmkoli způsobem narušen, nelze se na jeho funkčnost spoléhat a je třeba přejít přímo k tradiční forenzní analýze. Moderní postupy by tedy měly používat takové nástroje, které operační systém zkoumaného systému či jakékoli jeho aplikace ke své práci nepotřebují.

Principy forenzní analýzy živých systémů

V praxi je třeba při forenzní analýze dodržovat několik základních principů (viz [3]), které zajistí maximální kvalitu a objem získaných digitálních stop a minimalizují dopad na případné další zkoumání informačního systému. Mezi nejdůležitější principy patří používání pouze známých programů, hashování všech získaných digitálních stop a získávání dat v pořadí jejich volatility.

Používání pouze známých a prověřených programů

Při forenzní analýze není možné se spoléhat na spustitelné programy, které jsou k dispozici ve zkoumaném informačním systému. Je třeba používat vyzkoušené a prověřené vlastní spustitelné programy. Tyto programy by měly být spouštěny z média, na které nelze zapisovat (např. CD ROM). Zároveň by na něm měly být umístěny všechny knihovny, které příslušný program potřebuje.

Spustitelné programy by pokud možno neměly být kopírovány na disk, protože by mohly přepsat digitální stopy, které na tomto disku jsou, např. vymazané soubory. Pokud však bez kopírování na disk není možné digitální důkazy z živého systému získat, je třeba učinit informované rozhodnutí o tom, jak dále postupovat a který postup přinese větší informační hodnotu. Je třeba vzít v úvahu, že škody způsobené kopírováním spustitelných programů na disk obvykle nejsou zásadní a neohrozí významným způsobem případné tradiční forenzní šetření.

Hashování všech získaných digitálních stop

Všechny získané digitální stopy musí být uchovávány takovým způsobem, aby mohl forenzní expert později prokázat, že v průběhu zkoumání nedošlo k jejich změně. V praxi se akceptuje metoda výpočtu kryptograficky bezpečného digitálního otisku (hash). Typicky se používají algoritmy MD5 nebo SHA-1. Hash má 16–20 bytů a jeho opětovným výpočtem lze prokázat shodu původních a analyzovaných stop. Digitální stopy i hash je třeba uchovávat v bezpečí a zacházet s nimi jako s jiným důkazním materiálem.

Získávání dat v pořadí jejich volatility

Různá data na počítačích jsou různě trvanlivá. Otevřená síťová připojení se mění obvykle rychleji než uživatelé přihlášení k systému. Některé aktivity mohou ovlivňovat jiné. Přihlášení nového uživatele vytvoří nové zápisy v tzv. log souborech. Je třeba si tyto možné závislosti uvědomovat a při analýze systému s nimi počítat. Lze uvést následující příklady různých typů digitálních stop:

- obsah paměti;
- odkládací soubor (swap file);
- systémové datum a čas;
- běžící procesy;
- síťová připojení, otevřené TCP a UDP porty včetně jejich příslušnosti k procesům, NetBIOS;
- informace o souborovém systému;
- přihlášení uživatelé;
- naplánované úlohy;
- historie užití internetu v internetovém prohlížeči;
- proměnné prostředí;
- registry Windows;
- logy;
- moduly jádra.

Postupy získávání dat

Pro získávání dat z živého systému existují podle [2] dva základní postupy. Prvním je přímý přenos dat z živého systému. Druhý postup se soustřeďuje na analýzu paměti. V obou případech je prvním krokem k vytvoření důvěryhodného prostředí pro spouštění příkazů (trusted command shell). Poté se již oba postupy liší.

Příkaz	Zjišťované údaje
date	systémové datum
time	systémový čas
ipconfig	konfigurace TCP/IP
netstat	síťová připojení a porty
psinfo	informace o příslušném systému (hardware, software, verze, záplaty apod.)
pslist	běžící procesy
at	plánované úlohy
psloggedon	přihlášení uživatelé a časy přihlášení
psloglist	záznamy o událostech
psservice	systémové služby
listdlls	používané dynamické knihovny

Tabulka 1: Příklady příkazů spouštěných k získání dat z živého systému.

Přenos dat z živého systému

Přenos dat z živého systému spočívá v přesměrování výstupu systému buď na jiný (vzdálený) systém (např. pomocí utility netcat), nebo např. na připojené USB zařízení. Na analyzovaném systému pak můžeme spouštět různé příkazy, kterými získáváme požadované informace. Výstupy těchto příkazů jsou přesměrovány na námi zvolený systém, kde je pak můžeme analyzovat. Příklady spouštěných příkazů jsou uvedeny v Tabulce 1. S takto získanými daty pracujeme podobně jako při tradiční forenzní analýze – vytvoříme hash, bezpečně uložíme kopii nezpracovaných dat a provádíme analýzu.

Všechny příkazy spouštěné na analyzovaném systému je třeba dokumentovat a být si vědom veškerých změn, které tyto příkazy v analyzovaném systému způsobí. Změny je pak třeba vzít v úvahu při případné tradiční analýze systému po jeho odpojení/vypnutí (viz předchozí strana Tabulka 1).

Analýza paměti

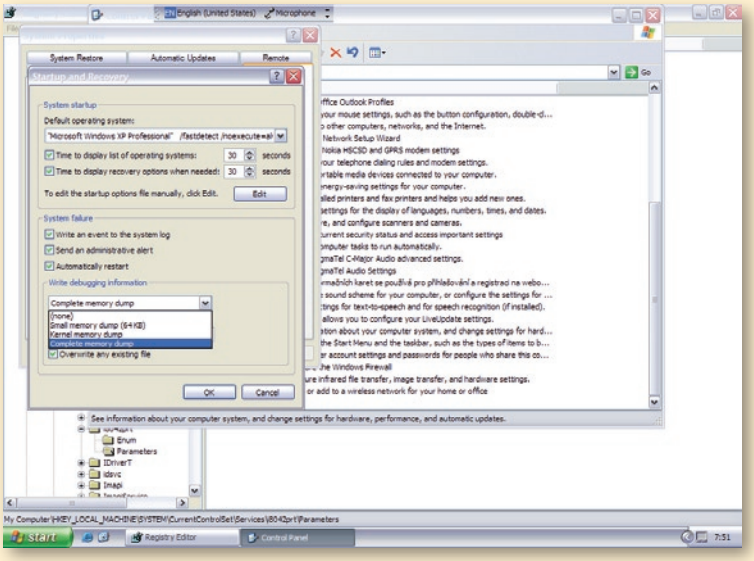
Druhý postup spočívá v analýze paměti. Na rozdíl od prvního postupu, při kterém se získávají veškerá data, jsou v tomto případě získány pouze tzv. memory dumps (zkrácené výpisy stavu paměti viz box 1). S těmito daty se pak pracuje podobně jako s daty získanými při tradiční forenzní analýze. Výpisy je možné prohlížet pomocí nástrojů dumpchk.exe (součást nástrojů odborné pomoci), WinDbg nebo KD.exe (součást balíčku Debugging Tools pro Windows).

Analýza získaných digitálních stop

Tradiční forenzní postupy zahajují analýzu digitálních stop až po získání všech dat. V případě forenzní analýzy živých systémů to není vždy optimální přístup.

Nastavení výpisů paměti — BOX 1

Jako příklad lze uvést analýzu paměti operačního systému Windows. Většinu verzí systému Windows je možné nakonfigurovat tak, aby při neočekávaném zastavení počítače vytvořily záznam, který obsahuje buď úplný, anebo zkrácený výpis paměti (viz obr. 1). Název souboru obsahuje datum a pořadové číslo souboru daného dne a je typicky uložen v adresáři %SystemRoor%\Minidump.



Obr. 1: Příklad výpisu paměti operačních systémů Windows.

V praxi se obvykle provádí alespoň hrubá analýza každé části dat ihned po jejich získání. Podle jejich obsahu se mění priority dalšího postupu. Zejména při velkých objemech dat umožňuje tento přístup účinněji zaměřit analýzu a rychleji dospět k požadovaným výsledkům, případně získat digitální důkazy, které by pozdější analýzou získaných dat nebylo vůbec možné získat.

Závěr

Forenzní analýza živých systémů je relativně mladá a v praxi zatím málo používaná metoda získávání dat pro forenzní účely. S narůstajícími objemy dat se však budou stále více ukazovat její přednosti. Forenzní experti se musí připravit na to, jak při analýze živých systémů postupovat a jak data získaná těmito postupy prezentovat tak, aby mohla být akceptována v případném soudním řízení. V této souvislosti bude třeba vyvinout postupy, které umožní získávání dat z různých typů operačních systémů i aplikací metodami, které minimálně kontaminují analyzovaný systém a budou dostatečně průkazné. Tato oblast se v současné době velmi rychle rozvíjí a postupy či nástroje pro tyto analýzy přibývají rychlým tempem.

Eva Racková
evarackova@kpmg.cz

RNDr. Eva Racková, ACCA, CISA

Absolvovala Přírodovědeckou fakultu Univerzity Karlovy v Praze. Od roku 1993 pracuje v KPMG Česká republika. Je partnerkou zodpovědnou za oddělení Performance & Technology, pro společnost KPMG Česká republika působí rovněž ve funkci CIO.

POUŽITÉ ZDROJE

[1] ADELSTEIN, F. *Live Forensics: Diagnosing Your System Without Killing It First*. Communications of the ACM, Vol. 49, No. 2, February 2006.
[2] WAITS, C., AKINYELE, J. A., NOLAN, R., ROGERS, L. *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis*. Technical Note CMU/SEI-2008-TN-017, August 2008.
[3] LAW, F. Y. W., CHOW, K. P., KWAN, M. Y. K., LAI, P. K. Y. *Consistency Issues on Live Systems Forensics*. Vol. 2, pp. 136–140, Future Generation Communication and Networking (FGCN 2007) – Volume 1, 2007. www.microsoft.com.