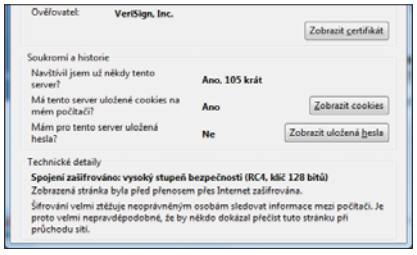
Internetové šifrování hacknuto

Vědci vyvinuli teorie, které by mohly přečíst šifrovaný internetový provoz po celém světě.

Není to tak dávno, co média po celém světě propírala rozsáhlé špehování ze strany NSA. Celá řada firem na to reagovala zavedením šifrovaného provozu (nebo prohlášením, že již šifrování používají). Některé německé freemaily dokonce rozhodly o implicitním šifrování všech e-mailů. To by mělo teoreticky znemožnit jejich přečtení ze strany tajných služeb. Jak se ale zdá, důvěra v techniku zvanou TLS (Transport Layer Security) nemusí být oprávněná. Na nedávné hackerské konferenci Black Hat se totiž ukázalo, že může být zranitelná. Několik výzkumníků zde představilo teoretické způsoby, jak by TLS mohlo být prolomeno. Například Florent Daignière, známý bezpečnostní odborník z Anglie, identifikoval slabé místo v TLS session tiketech.

Ty mimo jiné obsahují klíče, které server i klient používají pro šifrování procesu. Aby byl útočník schopen hacknout proces, potřebuje získat přístup k cache serveru. Podle Daignièra může hacker tento přístup získat například z chyb vznikajících při práci aplikace s pamětí, které lze v programech najít poměrně často. Nicméně i když v současnosti nikdo nedokáže přečíst klíče přímo, experti odhadují, že ve střednědobém horizontu bude bezpečnost TLS komunikace ohrožena.



SOUČASNÉ ŠIFROVÁNÍ ZŮSTANE BEZPEČNÉ UŽ JEN NĚKOLIK LET

Podle Javeda Samuela, kryptografického experta pracujícího pro poradenskou firmu ISEC, bude během několika let možné přečíst data, která byla zakódována pomocí RSA a Diffie-Hellman procesu. To je důvod, proč již některé země pracují na jejich nástupci, označovaném jako ECC (kryptografie eliptických křivek).

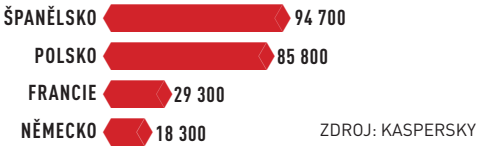
Nová varianta je považována za velmi bezpečnou, přesto v nás ale může vyvolávat určitou pachuť, když si uvědomíme, že tuto techniku již vyvinula NSA v roce 2005 pod krycím jménem „Suite B". Otázkou tedy zůstává, jak moc velký je náskok, který před námi tajné služby mají.

Konec bezpečí?

Možnost snadného prolomení šifrování by pro surfaře znamenalo problém.

TITO HRÁČI BÝVAJÍ NEJČASTĚJI TERČEM HACKERŮ

S téměř 95 tisíci útoky se stávají španělští hráči nejčastějším terčem internetových podvodníků.



ZDROJ: KASPERSKY

DATOVÉ ÚNIKY MĚSÍCE

US-AIRWAYS: KRÁDEŽ BONUSOVÝCH MÍLÍ

Do serverů americké letecké společnosti US Airways pronikli hackeři a získali kombinace uživatelského jména a hesla zákazníků. Hackeři pak z hacknutých účtů prodali bonusové míle na internetu. Jedna z obětí se zmínila o 400 000 ukradených mílích. Společnost US Airways ale odmítá přesně určit, kolik zákaznických účtů bylo hacknutím ovlivněno.

APPLE: CÍLEM ÚTOKŮ VÝVOJÁŘI

Apple na několik týdnů stáhl z internetu stránku pro vývojáře, aniž by firma sdělila jakékoliv důvody. Podle expertů prý neznámí hackeři zkoušeli získat přístup k vývojářským serverům s cílem dostat se k detailním informacím o účtech registrovaných vývojářů. Na přímý dotaz Apple připustil, že některý z těchto pokusů byl úspěšný. Podle něj prý došlo k odcizení některých datových souborů obsahujících jména, e-mailové adresy a poštovní adresy některých uživatelů. Proto Apple věnoval celý týden re-instalaci a zabezpečení stránky pro vývojáře.

JAVA FORUM: HESLA NA WEBU

Části uživatelské databáze jednoho z největších diskusních fór zaměřených na Javu na adrese **java-forum.org** se objevily volně dostupné na internetu. Podle některých uživatelů se ve zveřejněných informacích nachází uživatelská jména a hesla. Toto fórum bylo v srpnu 2013 prodáno subjektu specializujícímu se na marketing.

Odhalení Kaspersky Lab: Kybernetická špionáž „Icefog“

Společnost Kaspersky Lab zveřejnila zprávu o objevu „Icefog“ (**www.securelist.com/en/downloads/vlpdfs/icefog.pdf**), skupině APT (Advanced Persistant Threat, vyspělá přetrvávající hrozba), která se soustředila na cíle zejména v Jižní Koreji a v Japonsku a zasáhla dodavatelské řetězce západních firem. Operace začala v roce 2011 a v posledních letech se rozšířila a zintenzivnila.

„Za poslední roky jsme viděli nespočet útoků APT na prakticky všechny typy obětí a odvětví. Ve většině případů útočníci působili v podnikových a vládních sítích po celé roky a dolovali z nich terabajty citlivých informací,“ řekl Costin Raiu, ředitel výzkumného týmu Kaspersky Lab. „Ukazuje se nový trend – malé gangy jdou po informacích s chirurgickou přesností. Útok obvykle trvá několik dnů nebo týdnů a po získání toho, po čem jdou, útočníci zametou stopy a zmizí.“

Analytici Kaspersky Lab očekávají v blízké budoucnosti nárůst množství přesně zacílených skupin APT, které budou své služby nabízet za úplatu a budou se specializovat na rychlé operace. „Stávají se z nich takoví ‚kybernetičtí žoldáci‘ v moderním světě“.

NEJDŮLEŽITĚJŠÍ ZJIŠTĚNÍ KASPERSKY LAB:

- Útočníci měli zájem o cíle zejména v těchto odvětvích: armáda, stavba lodí a námořní operace, vývoj počítačů a softwaru, výzkumné společnosti, telekomunikační operátoři a média.
- Útočníci odcizili citlivé dokumenty a plány společností, detaily o e-mailových účtech a hesla k různým zdrojům uvnitř i vně napadené sítě.
- Během akce útočníci využili backdoor sadu „Icefog“. Kaspersky Lab identifikovala jejich verze pro Microsoft Windows i OS X.
- Zatímco u jiných APT kampaní byly všechny oběti infikovány měsíce či roky, Icefog zpracovával oběti jednu po druhé, nalézal a kopíroval jen určité informace. Po jejich obdržení útočníci zmizeli.
- Lidé stojící za útokem Icefog zřejmě dobře věděli, co od obětí potřebují. Hledali specifická jména souborů a složek, rychle je identifikovali a převáděli na C&C servery.

ÚTOK A JEHO TECHNOLOGIE

Experti Kaspersky Lab prozkoumali třináct z více než sedmdesáti domén, které útočníci využili. Poskytlo jim to přehled o počtu obětí po celém světě. C&C servery útoku Icefog obsahovaly zašifrované údaje o obětech spolu s operacemi na nich provedenými. V některých případech to pomohlo oběti či cíle odhalit. Kromě Jižní Koreje a Japonska experti odhalili spojení s dalšími zeměmi, včetně Tchaj-wanu, Hongkongu, Číny, USA, Austrálie, Kanady, Velké Británie, Itálie, Německa, Rakouska, Singapuru, Běloruska a Malajsie. Celkem to bylo 4 000 IP adres a několik set obětí (desítky z nich užívaly Windows a více než 350 jich užívalo OS X). Na základě analýzy IP adres využívaných ke sledování a ovládání infrastruktury analytici Kaspersky Lab předpokládají, že hlavní hráči stojící za útokem pocházejí z Číny, Jižní Koreje a Japonska. Celou zprávu Kaspersky Lab o útoku Icefog si můžete přečíst na webu **www.securelist.com**.

NOVINKY OD ESETU

NOD32 Antivirus 7 a Smart Security 7

Antivirová společnost Eset vydala nové verze svých vlajkových produktů určených pro domácnosti – NOD32 Antivirus 7 a Smart Security 7. Ty nabízejí zcela nové funkce, mezi které patří blokování zranitelností, pokročilá kontrola paměti a ochrana na sociálních sítích.

Kyberzločinci v poslední době často vytvářejí složitě zašifrovaný, a tím pádem těžko odhalitelný malware, čímž zvyšují pravděpodobnost infekce a případných škod. Eset proto vylepšil svou technologii detekce právě za účelem odhalování těchto zákeřných hrozeb. Exploit Blocker je novinková funkce verze 7, která sleduje pokusy o útok na aplikace, jako jsou webové prohlížeče nebo PDF čtečky. Funkce Advanced Memory Scanner (pokročilá kontrola paměti) naopak zasahuje zpětně a snaží se vyhledávat malware, který jiné technologie dosud nezachytily. Tento skener pomáhá chránit zejména před škodlivými kódy, které se snaží aktivně obejít detekci různými maskovacími metodami.

„Nové technologie v sedmé verzi našich vlajkových produktů mohou pracovat současně a jsou schopny proaktivně detekovat a blokovat zranitelnosti, jako je PDF exploit CVE-2013-0641, který je označován jako exploit roku vzhledem k jeho vysoké popularitě a častému začlenění do exploit kitů," říká Juraj Malcho, ředitel výzkumu společnosti Eset. „Tato technologie by také měla pomoci řešit problematiku cílených útoků, které získaly na síle až v poslední době. Příkladem může být i neslavný případ útoků na bezpečnostní firmu RSA v roce 2011."

Klíčová vylepšení obou produktů pomáhají uživatelům při odhalování šifrovaného malwaru, který se může pokusit infiltrovat jejich zařízení. Mají také vestavěný čisticí modul, jenž odstraňuje nutnost používat speciální čisticí nástroje a další doplňky.

Hlavní technologické funkce produktů Eset NOD32 Antivirus a Eset Smart Security verze 7 nabízejí vylepšenou detekci a ochranu před novým a dosud neobjeveným malwarem, jako jsou zranitelnosti „zero day" a dosud neznámé hrozby:

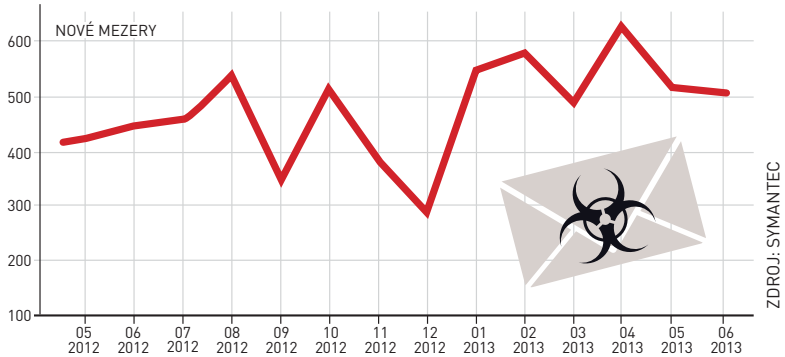
- Exploit Blocker – chrání uživatele před vyspělými, cílenými, negenerickými webovými útoky malwaru, eliminuje zamykání obrazovky, GPcode a ransomware. Blokování se zaměřuje na nejčastější typy útoků na internetové prohlížeče, PDF čtečky, e-mailové klienty nebo MS Office.

- Eset Advanced Memory Scanner a Vulnerability Shield zastavuje silně šifrované hrozby, jejichž cílem je vyhnout se odhalení. Advanced Memory Scanner představuje další úroveň bezpečnosti. Jde o rozšíření technologie Host-based Intrusion-Prevention System (HIPS), která provádí hloubkové skenování paměti počítače v reálném čase. Tím zlepšuje detekci malwaru a umožňuje efektivní prevenci před infekcí i v případech, v nichž se malware snaží skrývat šifrováním. Díky schopnosti analyzovat zašifrované soubory přímo v paměti počítače mohou nové produkty účinně chránit před neznámými útoky škodlivého softwaru. Funkce Vulnerability Shield funguje na úrovni sítě a chrání před zneužitím známých zranitelností v síťových protokolech.

S ohledem na nárůst spamu a malwaru zaměřeného na sociální sítě obsahuje sedmá verze produktů Eset pro domácnosti vylepšenou funkci Social Media Scanner. Ta monitoruje a udržuje v bezpečí na sociálních sítích nejen účet samotného uživatele, ale i jeho přátel. Uživateli umožňuje automatické nebo jednorázové skenování určené k odhalení případných hrozeb. Kromě lepší kontroly Facebooku je ochrana nově rozšířena i na Twitter. Součástí tohoto nástroje je Centrum zabezpečení, které zobrazuje aktuální úroveň ochrany osobních údajů na Facebooku a Twitteru, případně navrhuje změny v nastavení soukromí. Všechna vylepšení jsou součástí účtu na **my.eset.com**. Více informací o nových technologiích a vylepšení základních funkcí a také možnost stáhnout si sedmou verzi produktů naleznete na produktových stránkách na webu **www.eset.com/cz**.

NOVÉ BEZPEČNOSTNÍ MEZERY

Ve srovnání s loňským rokem se počet zjištěných chyb v zabezpečení zvýšil přibližně o 16 procent. Každý měsíc přibývá v průměru asi 450 nových zranitelností.



Bitcoin: Krádež prostřednictvím mobilního telefonu

Vývojáři projektu Bitcoin varují před chybou v zabezpečení telefonů s OS Android, při které může být hackery odcizen soukromý klíč pro aplikaci Bitcoin. Útočníci tak získají přístup k Bitcoin peněžence. Chyba je již aktivně zneužívána útočníky. Škodlivý software zneužívající chybu často pochází z napadených aplikací, které nejsou staženy z oficiálních obchodů s aplikacemi.

NOVÁ HROZBA:

Masivní nárůst trojanů požadujících výkupné

Laboratoř pro výzkum malwaru společnosti Eset zkoumá neobvyklý nárůst výskytu malwaru Filecoder – trojského koně, který šifruje uživatelské soubory a následně po uživatelích požaduje výkupné za jejich opětovné dešifrování.

Eset od července zaznamenal nárůst detekcí hrozby Win32/Filecoder oproti průměrnému výskytu v období od ledna do června téměř o 200 %. Obzvlášť vysoký podíl detekcí (44 %) pochází z Ruska, nezanedbatelné počty výskytu tohoto škodlivého kódu byly ale zaznamenány i ve střední a východní Evropě (Německo, Česko, Polsko, Rumunsko a Ukrajina), jižní Evropě (Itálie, Španělsko) a USA. K infikování počítače využívají kyberzločinci různé druhy infiltračních metod – stažení hrozby do počítače z nakažených internetových stránek, e-mailové přílohy, instalaci prostřednictvím jiného trojanu nebo backdooru, případně manuální instalaci provedenou přímo útočníkem.

„Rodina hrozeb Win32/Filecoder je nebezpečnější než ostatní typy tzv. ransomwaru, protože dokáže zašifrovat obrázky, dokumenty, hudbu a archivy. V průběhu času jsme pozorovali širokou škálu technik a úrovní sofistikovanosti v nejrůznějších variantách," říká Róbert Lipovský, výzkumník malwaru společnosti Eset. „Tato hrozba se navíc může velmi prodražit. Jednotlivé varianty požadují od uživatelů sumy okolo 100 až 200 eur, objevily se ale i pokusy vymáhající od lidí 3 000 eur. Vydírání vysokými částkami se objevuje v případě, kdy se útočníci zaměřují na firmy a organizace, které si mohou dovolit zaplatit více peněz než jednotlivci," dodává Lipovský. Jedna z aktuálních variant dostává oběti pod tlak odpočtem, který zobrazuje čas zbývající do definitivního smazání šifrovacího klíče, čímž by byl jakýkoli pokus o obnovu dat v počítači uživatele téměř nemožný.

Detailní analýzu malwaru si přečtěte v příspěvku na adrese **bit.ly/19zXulH** na serveru WeLiveSecurity.com.