Nové lákavé cíle pro

Průmyslové viry pro osobní počítače, hacky přes cloud a útoky na chytré sítě – organizovaná počítačová kriminalita roste rychle a agresivně.

CLAUDIO MÜLLER

Krysa – krysy. S těmito slovy zničil vynálezce Nevil Maskelyne v červnu roku 1903 iluzi o bezpečné bezdrátové komunikaci. Vynálezce Marconi a jeho kolega Fleming chtěli všem ukázat, že lze bez problémů poslat zprávu morseovkou i na vzdálenost téměř 500 kilometrů. Maskelyne přenos očekával a pomocí jednoduchého vysílače se do komunikace naboural. Mělo jít o pomstu Marconimu, který získal patenty pro radiokomunikaci.

V současné době se změnila technologie, motivy zločinců však zůstávají podobné. Hackeři se snaží proniknout do systémů uživatelů a firem, kde hledají citlivé informace, které by mohli zpeněžit. Mezi atraktivní cíle patří velké kanceláře, banky, vládní organizace. Ty jsou ale samozřejmě chráněny, nejlépe pomocí bývalých hackerů.

V ohrožení tak zůstávají především menší firmy a běžní uživatelé. Jejich bezpečnostní programy sice některé hrozby odstraní, proti útokům profesionálních hackerů jsou ale bezbranné. Hackeři navíc začínají při útocích na tyto cíle používat nástroje získané z profesionálních hrozeb – například z trojského koně Stuxnet. V nejbližší budoucnosti se tedy máme na co těšit.

S armádou PC proti velkým firmám

Po složitých exploit kitech (jako Blackhole) a trojských koních zaměřených na data z bankovnictví (jako Citadela) nyní odborníci očekávají další vývojové stadium malwaru. První náznaky ukazují, že trendem bude využití technologií (nebo přímo součástí) průmyslových trojských koní Stuxnet a Flame. To potvrzuje i Stefan Wesche ze společnosti Symantec: zranitelnosti, které využíval Stuxnet, se velmi rychle objevily ve výzbroji klasického malwaru. Tyto exploity využívaly mezery ve Windows nebo v Javě a umožňovaly propašování škodlivého kódu do počítače.

Dalším zajímavým trendem je změna způsobu zneužívání počítačů ovládaných hackery. Zatímco dříve bylo obvyklé jejich využití k rozesílání spamu, v současnosti roste počet počítačů zapoje-

HACKERY

PC A BOTNETY

ných do DDoS útoků. V rámci nich je na cílové servery posíláno obrovské množství požadavků, které jsou tímto náporem zahlceny, nebo se dokonce zhroutí.

Samotné DDoS útoky nejsou na internetu nic nového – znají je politicky motivované skupiny, před časem je použila skupina Anonymous jako nástroj pomsty proti německému autorskému svazu GEMA.

Nedávno ale hackeři předvedli tento útok na zcela nové úrovni. V březnu letošního roku proběhl útok na servery organizace Spamhaus, která oficiálně vytváří seznamy společností, jež poskytují připojení spammerům – a tyto seznamy používá celá řada firem k blokování jejich stránek. To se ale celé řadě lidí a organizací nelíbí: například podle vyjádření nizozemské společnosti CyberBunker prý Spamhaus dělá samozvaného cenzora a rozhoduje, co na webu bude a co ne. A právě to bylo pravděpodobně příčinou největšího DDoS útoku v historii – nejmenovaný poskytovatel potvrdil, že v souvislosti s tímto útokem zaznamenal tok přesahující 300 Gb/s.

Experti odhadují, že v budoucnu bude podobných útoků přibývat – význam spamu totiž neustále klesá a hackeři hledají vhodné využití zombie počítačů v botnetech. Dá se tedy očekávat, že se autoři malwaru zaměří tímto směrem a místo občasného rozesílání nabídek s viagrou se z ovládnutých počítačů stanou nástroje masových útoků.

Botnety pro smartphony a další hrozby

V tomto roce už byla prodána přibližně miliarda chytrých telefonů a tři čtvrtiny z nich pracují s operačním systémem Android. Přestože má tento systém celou řadu výhod, nelze zatajit ani jeho zásadní slabiny. Experti mu vytýkají především pochybnou aktualizační politiku (více v Chipu 9 na straně 38) a velké množství neoficiálních obchodů s aplikacemi bez jakékoliv kontroly na malware. Není tedy divu, že počty malwaru pro tuto platformu rostou raketovou rychlostí.

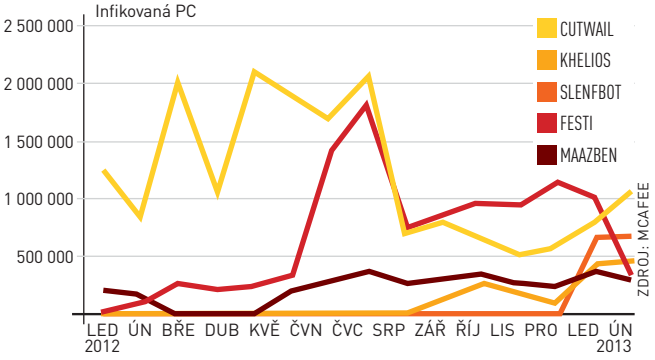
Jedničkou na žebříčku hrozeb stále zůstává SMS trojský kůň. Jeho princip je jednoduchý, ale mimořádně výnosný: do smartphonu je propašován trojský kůň, který odesílá drahé prémiové SMS, ze kterých dostanou autoři virů svůj podíl. Pokud není majitel telefonu obezřetný, všimne si ukradené částky až při měsíčním vyúčtování, nebo i později. Že jde opravdu o lukrativní záležitost, to nedávno potvrdila i společnost Symantec. Odhalila totiž mobilní botnet (pomocí malwaru více propojených smartphonů do sítě) označovaný jako Bmaster, který ovládal téměř 30 tisíc telefonů a denně vydělával 6 700 eur – ročně tedy téměř 2,5 milionu eur.

Dalším nebezpečným trendem je hloubka infiltrace do systému. Až doposud se malware obvykle skrýval v neškodné aplikaci. Pokud jste ji odinstalovali, eliminovali jste i malware. Nejnovější hrozba označovaná jako Obad jde ale dále. Při prvním spuštění zavirované aplikace požádá o administrátorská práva, a pokud je dostane, integruje se hluboko do systému. Když poté zavirovanou aplikaci z telefonu odstraníte, Obad v zařízení i nadále zůstane. Řídicímu serveru pošle telefonní číslo, MAC adresu zařízení a číslo přístroje (IMEI), a na oplátku od něj získá nový seznam prémiových SMS čísel. Obad jde ale ještě dál – pokud je aktivní, pokouší se napadat a infikovat jiná zařízení přes Bluetooth a vytváří komplexní botnet.

Christian Funk, virový analytik firmy Kaspersky, říká, že Obad obsahuje nejrozsáhlejší komplex škodlivých funkcí ze všech doposud testovaných hrozeb pro platformu Android. Tento sofistikovaný malware lze v současnosti odstranit pouze tak, že telefon vrátíte do továrního nastavení.

BOJ PROTI BOTNETŮM

Pokud jsou řídicí servery odhaleny a odstaveny (jak se to například stalo v srpnu 2012), pak počet počítačů ovládaných botnety klesá. Bohužel ale ne na dlouho.



ZDROJ: MCAFEE

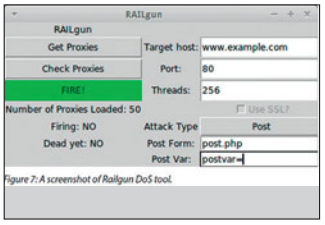
POČÍTAČE V SÍTÍCH AKTIVNÍCH BOTNETŮ

Počet počítačů infikovaných malwarem a zařazených do aktivních botnetů po eliminaci sítě Bredolab na konci roku 2010 poklesl, nyní ale znovu pomalu začíná růst.

ZDROJ: SYMANTEC

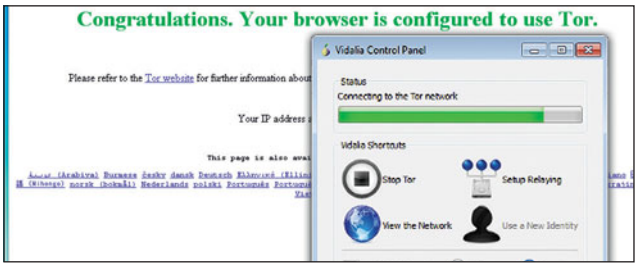
JEDNODUCHÉ NÁSTROJE PRO MASIVNÍ ÚTOKY

Útočníci mohou na vybrané servery generovat velký počet dotazů například i pomocí jednoduchého nástroje s označením RAILgun. Tento typ útoku (označovaný jako DDoS) server přetíží a vyřadí z provozu.



ANONYMNÍ SURFOVÁNÍ PŘES SÍŤ TOR

Pomocí speciálního prohlížeče můžete na internetu surfovat anonymně a především bezpečněji.



PŘEDPOVĚĎ PRO ROK 2014

V příštím roce očekávají experti nárůst lokálně kontrolovaných botnetů a agresivního vyděračského malwaru. Také přibude útoků na cloud.

Jak se chránit: Používejte kvalitní bezpečnostní nástroje a pravidelně aktualizujte svůj software. Velkou pozornost věnujte svému prohlížeči a jeho slabinám. Na rizikových webech doporučujeme deaktivovat potenciálně rizikové technologie (JavaScript, Javu, Flash a nebezpečná rozšíření).

Další oblastí zájmu hackerů v mobilních zařízeních je určení přesné polohy pomocí GPS a Wi-Fi triangulace. Vzhledem k nejčastějšímu umístění zařízení lze takto například zjistit bydliště majitele. Tuto detekci polohy zvládají určit i aktuální hrozby a v budoucnu lze očekávat zisk ještě detailnějších informací. Experti například varují před spojením Google Maps a navigační služby Waze. Tobias Jeske z univerzity v Hamburku obě služby prověřil a výsledek jeho analýzy příliš lichotivý není. Požadavky na ověření byly provedeny nedostatečně, a to jak v případě Googlu, tak i u protokolu Waze. Na hackerské konferenci Black Hat Europe navíc Jeske ukázal, jak by se dal využít Google a Waze při plánování trasy tak, aby bylo možné s GPS daty manipulovat v reálném čase přímo z telefonu (Floating Car data). Jeske používal Android 4.0.4 a ukázal, že nesprávné informace o dopravě mohly zobrazit dopravní zácpy, které ve skutečnosti neexistovaly. Hackeři tímto způsobem mohou dokonce za velmi nízkou cenu vytvořit dopravní chaos na objízdných trasách.

Pro počítačové zločince je vždy klíčová otázka, zda pomocí těchto triků mohou získat přístup do zařízení a snadno vydělat peníze. U klasických počítačů zní odpověď jednoznačně ano a při použití metody „drive-by-download", při které je do počítače stažen libovolný malware, si zloději jen mohou diktovat požadavky. U chytrých telefonů ale není zatím odpověď jednoznačná – zde hackeři budou ještě pravděpodobně nějakou dobu spoléhat na klasickou infiltraci malwaru do aplikací v neoficiálních obchodech.

Hackeři a chytré televizory

V dalších připojených zařízení – chytrých televizích a v systémech inteligentní domácnosti – se scénář útoků a hrozeb poněkud liší. Zde platí, že rapidně roste výbava televizorů, ale jen u minima z nich najdete zabudované účinné bezpečnostní funkce. A často i ty bývají plné chyb a zranitelností. Jens Heider, vedoucí bezpečnostní testovací laboratoře Fraunhoferova institutu, říká, že některé chyby poměrně překvapí: „Nejnebezpečnějším problémem, na který jsme narazili, byla nedostatečná kontrola certifikátu SSL pro přenos dat."

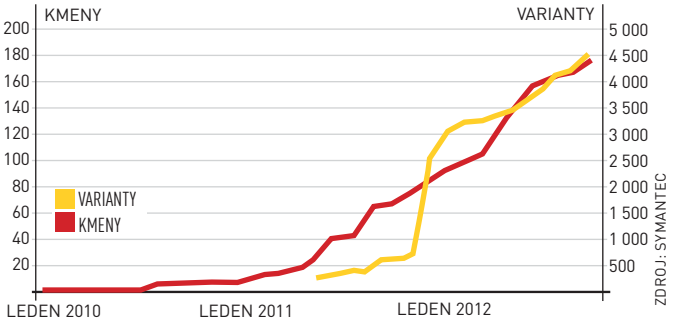
Bezpečnostní konzultant Martin Herfurt nám ukázal, jak snadno lze takové zařízení vyřadit z provozu. Pro svůj útok použil rozhraní HbbTV, které zobrazuje informace ohledně posledního přenášeného programu. TV signál vysílá URL, které si prostřednictvím stávajícího připojení k internetu vyžádá data ze serveru, a to v momentě, kdy člověk mění kanál. Technicky tyto zobrazené informace pocházejí z webu, který exportuje HTML a JavaScript. Hacker by mohl na webových stránkách dokonce i skrýt skript, který by z jiného webu stáhl malware. Ten by poté bez jakýchkoliv omezení mohl slídit v zařízení připojeném do domácí sítě.

Martin Herfurt uvádí, že žádný ze zkoumaných televizních „odesílatelů" nepoužíval pro HbbTV SSL chráněná připojení. Útočníci tak mohli získat přímý přístup k přenášeným datům (pomocí útoku Man-in-the-Middle) a změnit ho. V podstatě jde o stejný útok, jako byl ten, který asi před 110 lety předvedl Nevil Maskelyne.

Možná vás napadne, proč by někdo něco takového dělal. Stačí si ale uvědomit, že ti, kdo dokážou zmanipulovat požadovanou webovou stránku u HbbTV, mohou nahradit televizní data jinými a tak šířit nepravdivé informace. A pravda je, že tato informační válka už vypukla – zpravodajství Associated Press přineslo na Twitteru 23. dubna závažnou informaci: „Aktuálně: Dva výbuchy v Bílém domě a Barack Obama je zraněn." Ačkoliv byla zpráva poměrně rychle odhalena jako nepravdivá, stačil během několika málo minut Dow Jonesův index (jeden z nejznámějších ukazatelů vývoje

VÝVOJ MALWARU PRO ANDROID

Počet variant virů se zvyšuje, pravděpodobně proto, že útočníci investovali více času a peněz do vývoje.



ZDROJ: SYMANTEC

VERZE ANDROIDU A JEJICH SLABINY

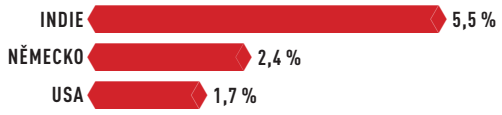
Nepovedený proces aktualizace OS Android znamená, že miliony uživatelů používají zastaralé systémy, které mají nezazáplatované bezpečnostní mezery.

JMÉNO/VERZE	ZRANITELNOSTÍ	UŽIVATELŮ
GINGERBREAD 2.3	11	288 Mil.
ICE CREAM SANDWICH 4.0	6	206 Mil.
JELLY BEAN 4.1	3	196 Mil.
JELLY BEAN 4.2	3	17 Mil.

ZDROJ: TREND MICRO

KDE VÁM HROZÍ NÁKAZA?

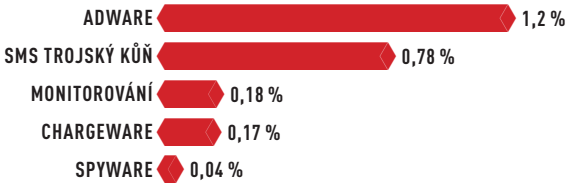
Pravděpodobnost, že běžný uživatel narazí na malware, je vyšší především tam, kde se častěji používají jiné než oficiální obchody s aplikacemi. Tedy například v Indii.



ZDROJ: LOOKOUT

NEJČASTĚJŠÍ RIZIKA PRO UŽIVATELE ANDROIDU

Největšími hrozbami jsou v současnosti reklamní adware a trojský kůň odesílající prémiové SMS.



ZDROJ: LOOKOUT

PŘEDPOVĚĎ PRO ROK 2014

Výkonné a velmi nebezpečné trojské koně jako Obad jsou sice stále spíše výjimkou, ale trend je jasný: komplexnější schopnosti malwaru znamenají větší zisky pro jejich tvůrce. Jediným problémem tak zůstává šíření: útočníci jsou nuceni škůdce integrovat do normálního softwaru.

Jak se bránit: Konzervativním a nenáročným uživatelům stačí instalovat pouze známé aplikace z oficiálních obchodů, náročnější uživatelé by měli přemýšlet o mobilním antiviru.

CHYTRÉ TV A INTELIGENTNÍ DOMY

na americkém akciovém trhu) poklesnout o jedno procento. Ti, kdo o akci věděli, mohli během chvilky vydělat miliony dolarů.

Cílem hackerů ale brzy nebudou jenom televizory, ale také váš dům či byt. Nejnovější trend označovaný jako „Smart Home", tedy inteligentní domácnost, by se ale ve skutečnosti měl nazývat „Dangerous Home" – nebezpečná domácnost. Smutným faktem totiž je, že použité technologie v celé řadě případů nesplňují dokonce ani ty nejjednodušší bezpečnostní normy. Typickým příkladem potenciálně rizikových oblastí mohou být tzv. inteligentní elektroměry, které přenáší data o spotřebě energie provozovateli sítě, a ten zase naopak pomocí těchto údajů řídí svou síť. Tyto tzv. Smart Grids propojují elektrárny, rozvodné stanice a spotřebitele. Ten by měl ve finále profitovat z vyšší transparentnosti vyúčtování odebrané elektřiny a ušetřit peníze (což však může být sporné, vzhledem k nákladům na zařízení). Důležité ale je, že v budoucnu ani jiná volba nebude – rozhodnutí o postupné celoevropské implementaci bylo přijato na úrovni EU. A jak může chytré zařízení vadit?

Riziko výpadku proudu kvůli chytrému elektroměru?

Zásadním problémem je, že „zařízení první a druhé generace byla vyvinuta, aniž by se přihlíželo k bezpečnostnímu hledisku", jak říká Dr. Frank Umbach z Centra pro evropské bezpečnostní strategie. Tyto přístroje byly například nainstalovány v masovém měřítku v Itálii, Španělsku a Portugalsku.

Chytré elektroměry (označované také jako Smart Grids) používají pro komunikaci se sítí systémy SCADA, jejichž slabé zabezpečení zneužíval už například známý červ Stuxnet. Díky bezpečnostním rizikům může vzniknout nebezpečná situace: elektroměr přímo komunikuje se systémy poskytovatele sítě, přičemž i samotný systém je přístupný přes elektroměr.

Útok na systém by mohl být – za předpokladu, že by byl důkladný a zdařilý – naprosto katastrofální. Zkuste si představit, jak hackeři ovládají nejkritičtější a nejzranitelnější oblasti: dopravní systémy, logistiku, dodávky potravin, lékařskou podporu nebo komunikační sítě. V zásadě by byly ovlivněny všechny sféry života.

Dalším rizikem je to, že tato chytrá zařízení nemusí komunikovat jen přes napájecí síť, ale v některých případech i bezdrátově – zde totiž SCADA často využívá zranitelných bezdrátových standardů. Pokud jsou data a řídicí příkazy předávány bezdrátově, může je hacker pomocí příslušného vybavení zaznamenat a také zmanipulovat. I díky tomu experti očekávají, že se brzy objeví útoky na kritické infrastruktury přes bezdrátové připojení.

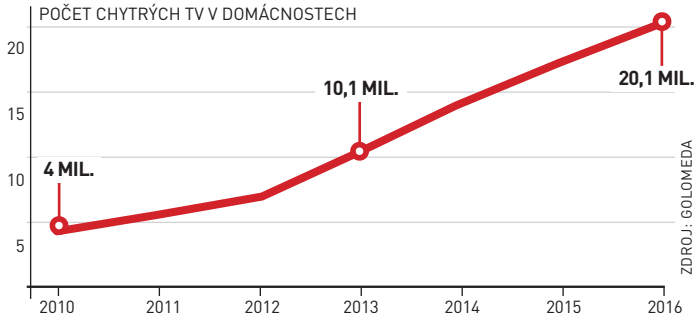
Některé firmy jsou ale na podobné útoky připraveny. Například v sousedním Německu je podle mluvčího RWE vše důkladně zajištěno: přenos přes elektrické vedení je chráněn šifrovaným heslem a při přenosu přes mobilní síť je použita síť VPN. Používané bezpečnostní standardy zde dosahují úrovně srovnatelné s těmi pro on-line bankovnictví.

Experti upozorňují, že i kdyby v některých oblastech existovaly bezpečné oblasti, riziko stále existuje. V síti pro dodávky elektřiny existuje po celé Evropě tolik bezpečnostních děr, že masivní útok by ovlivnil i dobře zabezpečené systémy. Je také důležité si uvědomit, že stávající systémy mohou být brzy překonány – a jen málokomu se bude chtít každé dva roky měnit inteligentní měřič.

Frank Ubach tvrdí, že spotřebitelé by měli být v blízké budoucnosti připraveni na případná selhání: ačkoliv prozatím

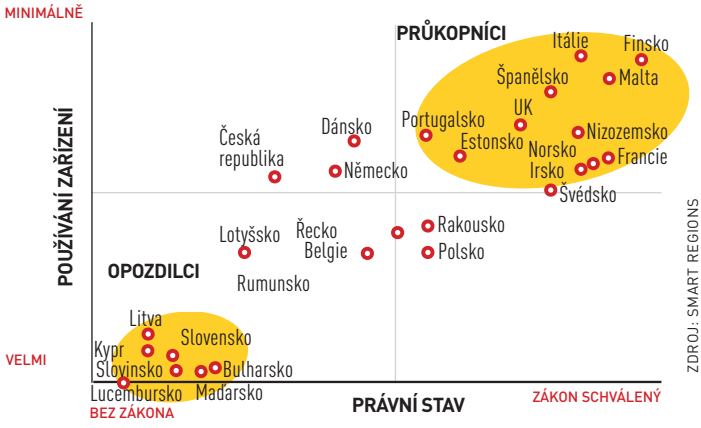
ROZŠÍŘENÍ CHYTRÝCH TELEVIZORŮ

Většina těchto k síti nově připojených zařízení je pro hackery velmi lákavým cílem.



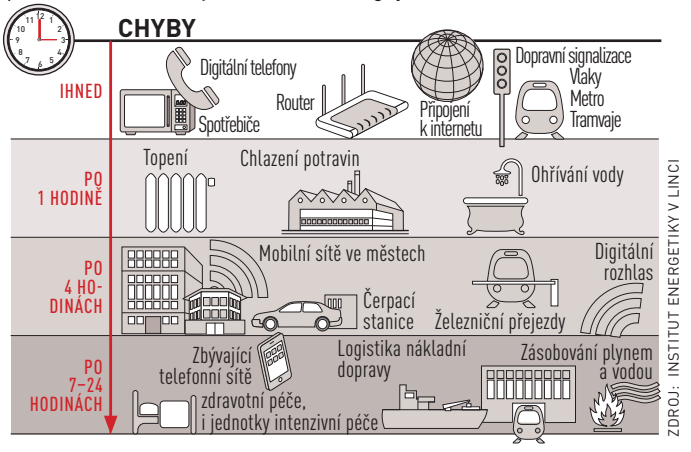
POUŽÍVÁNÍ INTELIGENTNÍCH ELEKTROMĚRŮ

Inteligentní elektroměry jsou v zemích, jako je Itálie, používány velmi intenzivně a mnoho z těchto zařízení je otevřeno pro útoky hackerů.



DŮSLEDKY VÝPADKU PROUDU

Útok hackerů na napájecí síť může mít dalekosáhlé důsledky, protože bez elektřiny téměř nic nefunguje.



PŘEDPOVĚĎ PRO ROK 2014

Masivní útoky hackerů na chytré televizory se prozatím neočekávají, protože jejich penetrace je nízká a cena příliš vysoká. Terčem profesionálních útoků by ale mohla být energetická infrastruktura.

Jak se bránit: Vždy se ujistěte, že na zařízeních (routeru, TV, přehrávačích...) jsou nainstalovány nejnovější aktualizace firmwaru.

PLACENÁ INZERCE

k úspěšnému útoku (a masivnímu výpadku) nedošlo, provozovatelé energetických sítí jsou vydíráni už dnes. Celková částka takto získaná hackery v celém světě se prý pohybuje za hranicí stovek milionů dolarů.

Profesionální hackeři na špionážních misích

Speciální kategorií hrozeb jsou útoky na energetické sítě, průmyslové závody nebo na politické organizace. Ty totiž ve většině případů nejsou prací individuálního hackera. Za útoky obvykle stojí profesionální gangy, které pracují na zakázku. Jednou z nejaktivnějších skupin současnosti je sdružení Elderwood.

To se specializuje na využití „Zero-day" zranitelností – tedy chyb v programech, které ještě nejsou oficiálně známé a na které neexistuje záplata.

Stefan Wesche ze společnosti Symantec říká, že tato skupina má k dispozici celou sbírku neznámých mezer. Ke každému útoku používají jen jednu, pokud není mezera identifikována a opravena.

Celosvětová počítačová špionážní akce známá pod označením NetTraveler, kterou odhalila společnost Kaspersky, ukazuje, jak tyto útoky fungují. Skupina škodlivých programů infikovala 350 obětí, mezi nimi významné vládní a veřejné instituce ve 40 zemích světa. Cílem byly jak vládní úřady a ambasády, tak i o ropný průmysl, výzkumná centra, zbrojní firmy nebo i aktivistické organizace. Hlavním úkolem útoků bylo sledování činnosti obětí a také krádež dat. Operace byla provozována od roku 2004 a svého nejvyššího bodu dosáhla v letech 2010 a 2013.

Zajímavé bylo, že oběti útočníci napadli pomocí sofistikovaných phishingových e-mailů se škodlivými přílohami ve formátu Microsoft Office, které obsahovaly zranitelnosti, jež ale Microsoft už dávno opravil pomocí záplat. Cíle útoků naznačují i názvy phishingových dokumentů: Report - Asia Defense Spending Boom.doc (růst výdajů na obranu v Asii), Army Cyber Security Policy 2013.doc (armádní plán kybernetické bezpečnosti) nebo His Holiness the Dalai Lama's visit to Switzerland day 4 (návštěva Jeho Svatosti dalajlamy ve Švýcarsku, den čtvrtý).

Díky řízení na dálku a spojení s Command & Control servery zasílal malware všechna ukradená data na určená úložiště. Experti z firmy Kaspersky některé z nich prověřili a nalezli na nich 22 GB dat – a to lze předpokládat, že velkou část shromážděných údajů již provozovatelé malwaru stáhli a odstranili. V nalezených datech převažovaly záznamy z klávesnic, výkresy v digitální formě a také kancelářské dokumenty. To svědčí o tom, že útoky nebyly náhodné a oběti byly speciálně vybrány.

Stejně jako u většiny podobných útoků i zde zůstala identita útočníka neznámá. Podle některých odborníků šlo o útok vládou podporovaných čínských, ruských nebo íránských hackerů s cílem získat údaje o konkrétních společnostech nebo o zbraňových systémech v USA či Evropě.

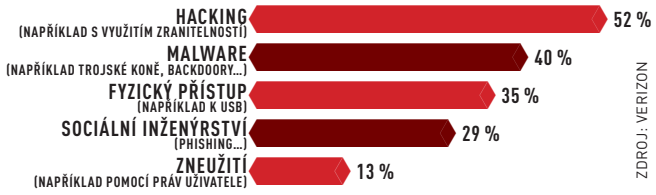
NATO na nedávné konferenci přiznalo, že jen za loňský rok zaznamenalo přibližně 2 500 útoků na své systémy, že každý měsíc bylo přibližně deset útoků závažných, nicméně žádný z nich nebyl úspěšný.

V této oblasti je tedy obecným trendem menší počet útoků, které jsou ale provedeny mnohem profesionálněji. Rostoucí počty profesionálních hackerských skupin (jako Elderwood) a národních kybernetických armád znamenají jediné: těžké časy pro systémové administrátory a IT specialisty, kteří mají chránit systémy svých zaměstnavatelů.

AUTOR@CHIP.CZ

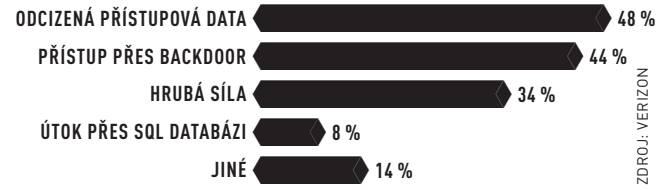
METODY POUŽÍVANÉ BĚHEM KYBERÚTOKŮ

Hackeři často během útoku používají více metod společně, což je důvod, proč součet jednotlivých metod v grafu přesahuje 100 procent.



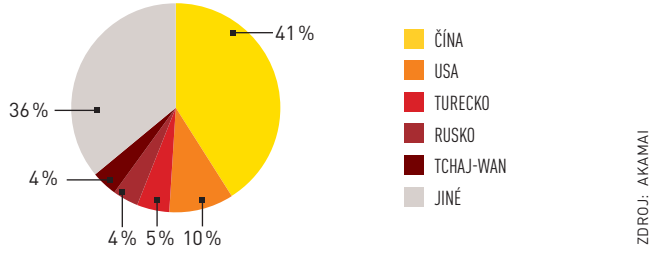
HACKERSKÉ ÚTOKY POD LUPOU

Preferovaná cesta hackerů vede přes krádež přístupových údajů zaměstnance a využití jeho účtu k vytvoření zadních vrátek v systému.



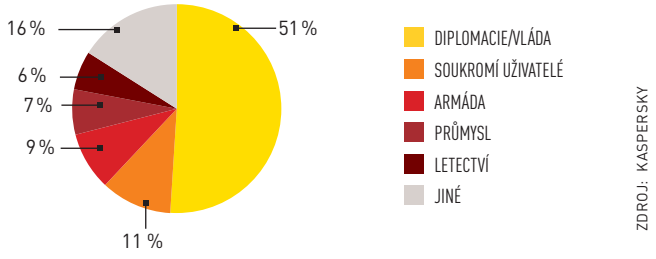
SVĚTOVÝ LEADER V KYBERZLOČINU

Více než polovina hlášených útoků hackerů na celém světě začíná podle záznamů datového provozu v Číně. Velmi aktivní jsou v této oblasti i USA.



CÍLE KYBERNETICKÉ ŠPIONÁŽE

Špionážní operace NetTraveler, objevená firmou Kaspersky, lovila data hlavně v politických institucích.



PŘEDPOVĚĎ PRO ROK 2014

Útoky na firmy a orgány státní správy mají většinou na svědomí organizovaní profesionálové a probíhají obvykle na zakázku. Tento trend bude i nadále sílit a pod palbou se bude ocitat i více menších a středních firem.

Jak se chránit: Dokonalá ochrana v tomto případě téměř neexistuje, ale pravidelná aktualizace počítačů, nasazení kvalitního bezpečnostního softwaru a proškolení pracovníků může míru rizika snížit na přijatelnou úroveň.