Ze zápisníku CSIRT.CZ

Zajímavé bezpečnostní incidenty zachycené českým týmem CSIRT

Michal Prokop, Pavel Bašta

Jednou z hlavních náplní činnosti národního CSIRT (Computer Security Incident Response Team) týmu České republiky je reakce na bezpečnostní incidenty. Protože jsme v první polovině tohoto roku zaznamenali v CSIRT.CZ několik velice zajímavých incidentů, rádi bychom s nimi čtenáře seznámili.

V první řadě je třeba říci, že v rámci řešení incidentů se podílíme také na proaktivních akcích, kdy nás buď přímo osloví jiná instituce či jednotlivec s informací o nalezených zranitelných strojích v rámci rozsahu IP adres delegovaných do České republiky, nebo sami proaktivně takovéto informace vyhledáváme. V textu bude zmíněno i několik příkladů vztahujících se k těmto aktivitám.

Volně dostupné databáze

V rámci proaktivní spolupráce jsme informovali držitele IP adres, na nichž byla detekována dostupná rozhraní databází umožňující přístup k datům v nich uloženým. Konkrétně byly za dané období na 614 IP adresách volně dostupné informace z cachovacích softwarových aplikacích Redis a Memcached a na 113 IP adresách v ČR byl také volně dostupný obsah Mongo databází. Je s podivem, kolik administrátorů zapomíná, jak důležité informace mohou databáze obsahovat. Nejen e-mailové adresy zákazníků, ale i například informace o platebních kartách nebo čísla bankovních účtů.

Malware Ferret a Madness

Jedná se v obou případech o malware určený pro operační systémy Windows XP a vyšší. Technicky se nakažené stroje stanou DDoS boty umožňujícími spustit útoky na různých vrstvách sítě. Je zajímavé, že oba tyto typy malwaru jsou známé už od roku 2013 a antivirové společnosti je mají také již delší dobu uložené ve svých databázích. I přesto bylo v České republice v roce 2015 napadeno tímto malware více než 80 strojů. Uživatelé těchto zařízení tak pravděpodobně nemají nainstalované antivirové programy.

Malware Geodo

Tento e-bankovní malware, který se původně jmenoval Feodo a nyní je známý také pod jménem Cridex nebo Bugat, se v roce 2014 šířil prostřednictvím e-mailu, který obsahoval falešné faktury za mobilní služby. Využíval tedy falešná loga i podpisy společností jako je například Deutsche Telekom, O2 nebo Vodafone. Naštěstí většina těchto falešných zpráv byla psána německy, a proto u nás nezaznamenal velký úspěch. Staronový malware Geodo má upravený kód, ale používá stejné šifrování a komunikuje se stejným C&C serverem. Zároveň ale také tento malware prostřednictvím napadeného stroje rozesílá spamové zprávy, ke kterým využívá více jak 50 000 SMTP serverů, k nimž zná přihlašovací údaje. V České republice bylo tímto malwarem napadeno více než 1900 unikátních IP adres.

DHL

Aby těch škodlivých spamů nebylo málo, tak koncem března tohoto roku, začaly chodit zprávy s informacemi o zásilce, které se tvářily, že jsou od společnosti DHL. Falešné

Na co se připravit v budoucnu?

- Sofistikovanější phishingové útoky – vzpomeňme například exekuční e-maily nebo falešné zásilky od České pošty z minulého roku. Domnívám se, že těchto útoků bude přibývat a budou se objevovat stále lepší způsoby jak uživatele zmást.
- SOHO routery a Internet věcí – sáhněme si na srdce a přiznejme, kdo z nás kontroluje, s kým si náš kávovar na internetu povídá. Určitě stojí za to zvážit, která zařízení skutečně potřebují připojení k Internetu.
- Podvody na sociálních sítích – v dnešní době má Facebook už většina uživatelů Internetu, ale hesla, která ke svým účtům používají, nejsou zrovna moc silná. Žebříček nejpoužívanějších hesel vedlo i v minulém roce heslo „123456“.
- Útoky na CMS - velká část webových stránek používá open source CMS, jako jsou Joomla, WordPress, či Drupal. Útočníkovi pak stačí počkat na objevení chyby třeba v nějakém doplňku pro Joomlu a využít jej k plošnému napadení mnoha webových stránek během relativně krátké doby.

e-maily však příjemce obdržel od „DHL Logistik-Team“, která samozřejmě nemá s touto společností nic společného. V těle zprávy byly informace o převzetí zásilky spolu s číslem objednávky, které odkazovalo na různé domény. Na těchto URL se nacházel .ZIP soubor, který obsahoval trojského koně. CSIRT.CZ obdržel od jednoho českého uživatele seznam 395 takovýchto URL z více jak 17 zemí. Kontaktovali jsme proto všechny vládní nebo národní bezpečnostní týmy za účelem odstavení těchto nebezpečných stránek.

Zahraniční spolupráce

Vzhledem k tomu, že je CSIRT.CZ národním bezpečnostním týmem České Republiky, obracíse na nás také zahraniční, národní nebo vládní CSIRT/CERT týmy s prosbami o pomoc při řešení incidentů v sítích provozovaných v České republice. Zde jsou příklady zahraničních týmů, které nás informovaly o incidentech na IP adresách delegovaných do České republiky.

Taiwan → poskytnutí seznamu IP adres, které komunikují s botnetem

Kanada → poskytnutí seznamu IP adres, které byly infikovány malwarem Sakula

Cert-RO → poskytnutí seznamu IP adres routerů, které měly nastavené jednoduché nebo žádné heslo pro konfiguraci

CERT-FR → poskytnutí seznamu volně dostupných ICS/SCADA systémů

Abuse.ch → poskytnutí seznamu 1200 IP adres, které byly infikovány dosud neznámým trojským koněm

TI (Trusted Introducer) → v tomto případě jsme obdrželi informaci ohledně DDoS útoků na banku v Gruzii. Následující den přibyly informace ohledně DDoS útoku na vládní internetové stránky a nové banky v Gruzii. Tento případ připomínal DoS útoky z roku 2013.

Případ Sony Pictures

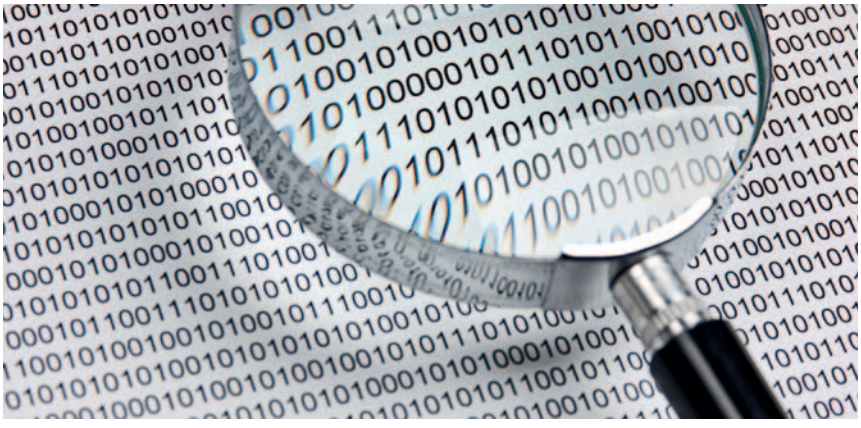
Vzhledem k tomu, že útok na společnost Sony Pictures byl probírán i v mainstreamových médiích, zmínil bych naši spolupráci s korejským národním CERT týmem. Jeho pracovníci nám zaslali seznam IP adres, kde stroje na těchto IP adresách vykazovaly známky napadení malwarem volgmer, který pomocí těchto „zombie PC“ útočil na vybrané cíle. Cílem číslo jedna byly servery společnosti Sony Pictures. V tomto případě byla za původce útoků označena Severní Korea, která údajně neměla zájem na zveřejnění filmu Interview. Napadené stroje však útočily i na další cíle. Aktivity, na nichž se podílely, zahrnovaly například DDoS útoky, kradení čísel kreditních karet nebo přihlašovacích údajů. Objevily se také zprávy, že tyto stroje stály za napadením sítě PlayStation Network. V tomto případě byl útok směřován přímo na pevné disky připojené k herní konzoli.

Spolupráce s Policií ČR

S Policií ČR spolupracujeme na řešení incidentů jak v rámci České republiky, tak i mimo ni. V průběhu tohoto roku jsme obdrželi několik požadavků spojených s odstraněním malwaru na zařízeních mimo ČR. Šlo například o URL, která vybízela ke stažení falešných aplikací pro Android (např. Seznam.cz, Facebook). Asi největší akce, na níž jsme se společně podíleli, souvisela s on-line obchody. V tomto případě byla na 28 doménách umístěných v sedmi zemích prodávána čísla kreditních karet s jejich CVC. Díky našemu zásahu byla většina těchto domén v krátké době zablokována.

Honeypoty

Kromě uvedených incidentů stojí za zmínku ještě statistika ze zpracování incidentů zaznamenaných v prostředí honeypotů provozovaných naším týmem. V dubnu 2015 jsme začali aktivně upozorňovat odpovědné administrátory, respektive bezpečnostní týmy v zemích, kde se útočící IP adresa nachází, na nahrání malwaru na naše honeypoty. Za první tři měsíce provozu bylo zaznamenáno více než 4258 unikátních IP adres (IP adresa, která se pokoušela uploadovat vícekrát, ale počítána je pouze jednou) a kontaktováni správci z více jak 49 zemí. Nové vzorky malware získané z honeypotů také poskytujeme k analýze antivirovým společnostem. ■



Michal Prokop a Pavel Bašta

Autoři článku jsou bezpečnostní analytici sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ