CSI: Internet

4. část

Mobil místo hasáku

V nejnovějším případě detektivů Chipu jde o tvrdou průmyslovou špionáž. Na zcizení utajované konstrukční dokumentace tentokrát zlodějům stačil trojský kůň vyvolaný SMS zprávou.

Valentin Pletzer, autor@chip.cz

Pan M. vede malý podnik, který se specializuje na výrobu příslušenství k autorádiím. Pirátské kopírování cizích výrobků není bohužel nijak vzácné. Až dosud však bylo zboží většinou v asijských továrnách kopírováno až poté, co se objevilo na trhu – a ne už předem. Choulostivý případ se proto stal velkou výzvou pro speciální jednotku Chipu, která se ihned pustila do zajišťování stop na síti a v počítačích. Stejně jako v seriálu CSI si vyšetřovatelé nejprve musí udělat úplný obraz o situaci a potom z něj vyvodit správné závěry. Při pátrání po skulině, kterou konstrukční výkresy adaptéru unikly, je důležitý každý, i sebemenší detail.

Jako první krok tedy náš tým provádí důkladnou inventuru počítačů a příslušenství. A už při ní zaznamenáváme první objev: jedno péčéčko je přes ISDN připojeno k telefonnímu zařízení. „To je náš přenosový server pro posílání dat," vysvětluje nám pan M. „Na zdejším pracovišti jenom vyvíjíme prototypy a vzory. Vlastní výroba přístrojů probíhá v zahraničí." Zbystřujeme pozornost a necháváme si zaběhaný postup vysvětlit. „Každý vývojář má svou vlastní pracovní stanici. Aby přitom každý z nich pracoval s aktuální verzí podkladů, je výrobní dokumentace centrálně uložena na serveru."

Hledání slabin

Plni zvědavosti si podrobněji bereme pod lupu zmíněný server. Tento počítač se nám totiž zdá ideálním sídlem pro trojské koně nebo spyware, neboť poskytuje všechna důležitá data a ve zdejší malé firemní síti zároveň představuje vstupní bránu pro vpád zvenčí. Naše snaha však úspěch nepřináší, a zdá se tedy, že server žádný malware neobsahuje. Protokoly o příchozích ani odchozích spojeních neexistují – což je ovšem hrubá nedbalost!

Rozšiřujeme pátrání i na ostatní počítače. I tady však bezvýsledně – na žádném PC nepozorujeme nic neobvyklého. Měníme proto taktiku a žádáme pana M. o zcela přesné vysvětlení návrhářských a výrobních postupů. Doufáme totiž, že bychom si přitom mohli povšimnout potenciálních záchytných bodů pro datové lupiče.

I nadále se nám jako jediná možnost napadení jeví průnik přes server připojený k internetu. Poněvadž je však přístupové heslo každý den měněno a partnerům sdělováno po telefonu, stále nechápeme, jak by k tomu mohlo docházet. Chystáme se tedy podívat se důkladněji na telefonní zařízení – když vtom zaslechneme jen tak mimochodem pronesenou poznámku sekretářky: „Na telefon se vůbec dívat nemusíte. Šéf stejně telefonuje jenom přes mobil."

Necháváme si tedy ukázat ředitelův mobilní telefon – a opravdu narážíme na první horkou stopu. V přístroji je aktivován konferenční hovor. To však znamená, že při každém telefonátu je – aniž by to držitel mobilu zpozoroval – kromě partnera v rozhovoru připojen ještě další účastník. Pan M. je očividně překvapen. „Vůbec jsem nevěděl, že můj mobil něco takového umí," říká. Ale nelze se mu příliš divit. Konferenční hovor se totiž zřizuje prostřednictvím operátora. Tuto funkci tedy může využívat v podstatě každé spojení – ale aktivovat konferenční hovor musí uživatel sám. Poněvadž pan M. samozřejmě nic takového neudělal, padá naše podezření na trojského koně v jeho Nokii N90 a vydáváme se po této stopě. I tato ulička je

Použitá zbraň: mobil

BEZBRANNÁ TELEFONIE: **Proti SMS šířícím trojské koně není momentálně chráněn prakticky žádný mobilní telefon. Chyba v systému GSM sítí tak hackerům jejich nekalé řemeslo hodně usnadňuje.**

Nový seriál Chipu

V americkém kriminálním seriálu o CSI objasňují vyšetřovatelé zločiny pomocí vědeckých metod. Chip si vzal „Kriminálku Las Vegas" za vzor pro novou řadu článků, která ukáže, jak profesionální vyšetřovatelé a specialisté bojují proti strmě narůstající počítačové kriminalitě.

však slepá: v mobilu nenalézáme ani nová loga, ani vyzváněcí tóny. Pan M. používá přístroj skutečně jen k telefonování.

Naše podezření je však posléze potvrzeno účtem za telefon. Konferenční hovor není levná záležitost a na faktuře také zanechal hodně drahou stopu: každý hovor byl zároveň předáván na jisté telefonní číslo v zahraničí. Poněvadž jsme nenašli ani software, ani malware, zbývá jen jediné hodnověrné vysvětlení: trojský kůň vniknuvší do počítače pomocí SMS.

Žádný mobil není bezpečný

Přivoláváme na pomoc specialistu. W. Hafner, bezpečnostní expert firmy Securstar, zná „SMS trojské koně" velmi důvěrně. „S pouhými 130 znaky se nabouráte do každého mobilu," říká. „Umožňuje to servisní SMS." A dodává: „Tak málo znaků samozřejmě trojského koně obsahovat nemůže. Ale dá se v nich vyslat příkaz k jeho stažení. Anebo jen prostě aktivujete existující funkci – jako zde konferenční hovor. To má navíc další výhodu: nemusíte znát operační systém mobilního telefonu své oběti." Pro každého útočníka právě operační systém mobilu představuje největší problém. Skoro každý výrobce totiž používá vlastní systém. A aby útočník dokázal do mobilu své oběti propašovat trojského koně, musel by vědět, jaký systém v přístroji pracuje.

Technika, kterou hacker nejspíše použil, nese název „OTA programování" (over the air programming). Tento postup měl vlastně majitele mobilů zbavit práce s konfigurováním služeb jako WAP – stačí jediná SMS od operátora, a všechna nastavení proběhnou automaticky. Jenomže takovou OTA-SMS může poslat nejen provozovatel mobilní sítě. Smí tak učinit kdokoliv – a s libovolným obsahem. To by ještě nebylo tak hrozné, kdyby si mobil každou změnu konfigurace nechal potvrdit. Avšak i tuto ochranu lze malým trikem prolomit. Software pro generování OTA-SMS je k dispozici na webu.

Jelikož nyní víme, že klíčem k datové loupeži byl mobilní telefon pana M., dokážeme si dobře představit, jak se hacker dostal k výrobní dokumentaci: útočník nejprve prostřednictvím OTA-SMS mobil překonfiguroval a pak přes konferenční hovor prostě odposlechl, jaké heslo pro server pan M. telefonicky sděloval svým partnerům. S touto znalostí si už hacker dokázal ze serveru stáhnout výrobní dokumentaci.

EXPERT

Wilfried Hafner je obchodním ředitelem a bezpečnostním specialistou firmy Securstar. Uživatele varuje před bezpečnostní mezerou v mobilních telefonech.

Ochrana šifrováním

Kdyby byl server nakonfigurován tak, aby zaprotokoloval všechna spojení, byli bychom se přinejmenším dozvěděli, kam byla data odesílána. Ale ani pak bychom se pravděpodobně dál nedostali. Pokud vede stopa například do Číny, prakticky nemáme – a dokonce ani úřady – žádnou možnost, jak hackera vypátrat.

Pan M. si tedy z celé akce odnese alespoň ponaučení, že své duševní vlastnictví musí lépe chránit. Hesla bude napříště předávat osobně nebo je bude posílat po zašifrovaném spoji. Kromě toho bude přístup na server povolen jen z určitých IP adres. To je sice jen malá překážka, ale může získat čas až do dalšího útoku průmyslových špionů.

U nás bezpečněji?

Pokud vás náš případ vyděsil a honem hledáte své nastavení mobilního telefonu, pak vás můžeme uklidnit. Žádný z českých mobilních operátorů nic podobného nenabízí a vaše telefonáty tak zůstávají v relativním bezpečí. Někteří operátoři sice nabízejí možnost konfigurace telefonu pomocí SMS (například nastavení internetu), ovšem tato nastavení je ještě nutné potvrdit nebo aktivovat přes webové rozhraní služby.

Valentin Pletzer

VÍCE INFORMACÍ

www.securstar.com: Na webové stránce bezpečnostní firmy najdete v současnosti jediný nástroj na ochranu proti SMS trojským koňům.

Zrádná stopa


Rechnung

Kopie

e-plus

Kundennummer
Rechnungsdatum 11.01.2007
Erstellt am 10.02.2007
Rechnungsnummer
Kontakt bei Rückfragen
www.eplus.de/ks

Summe in €

1,9900
2,3749
7,3679
0,3900
0,6200
5,3749

Rechnungsbetrag / zu zahlender Betrag

733,37

Vielen Dank für die Nutzung unserer Serviceleistungen.

VYSOKÝ ÚČET: **Faktura za telefon ukazuje, že něco není v pořádku. Vysoké poplatky za nikdy neobjednané telefonní konference přivedly vyšetřovatele na správnou stopu.**