CSI: Internet

1. část

Nebezpečné odkazy

Hackeři se pomocí jednoduchých triků snaží okrádat on-line banky. Na úvod nové série „CSI" vás seznámíme s prací profesionálů, kteří takovéto útoky dokáží vystopovat. *Valentin Pletzer, autor@chip.cz*

Michal M. se stal obětí útoku hackera. Dokázat to však nemůže. Nemá žádný jednoznačný důkaz: v protokolu serveru jeho banky je uvedena pouze jeho IP adresa, jeho počítač je bez virů, spywaru a trojských koní. Škoda však přesto vznikla: účet na více než 2000 eur za nákup elektroniky v ruském on-line internetovém obchodě je toho důkazem.

„PIN k mému on-line kontu znám pouze já a TAN jsou bezpečně uschovány," říká pan M. a ujišťuje: „Na žádný phishing-mail jsem neskočil. Vím přece, že mě banka nebude žádat mailem o zaslání mého PIN a TAN ve formě formuláře."

Případy, jako je tento, již však patří k denní rutině profesionálů, kteří se zabývají stopováním podvodníků. Extrémní množství webových stránek totiž vykazuje nebezpečné mezery v zabezpečení, které kreativním hackerům umožňují spouštět Cross-Site-Scripting útoky. K postiženým patří řada známých bankovních institucí – na jejichž stránkách se teoreticky každý může stát obětí hackerů. Naši kolegové vyzkoušeli například „hack" webové stránky TÜV, nejen německého synonyma pro bezpečí.

Ale zpátky k našemu případu. V naději, že se přece jenom podaří „ztracené" peníze vypátrat, nás pan M. poprosil, zda bychom se na jeho problém nemohli podívat. Dobré je, že za celou dobu od tohoto incidentu se svého počítače ani nedotkl. Stejně jako soudní znalci z kriminálního seriálu „CSI" („Crime Scene Investigation") zdokumentuje speciální jednotka Chipu pro zajištění stop nejprve místo činu – tedy počítač a jeho obsah. Jako první věc můžeme potvrdit výpověď pana M.: Počítač je čistý. Manipulaci pomocí trojského koně nebo keyloggeru můžeme tedy vyloučit. Případ zůstává i nadále záhadou. Kdo si obstaral přístup ke kontu pana M.? A hlavně jak?

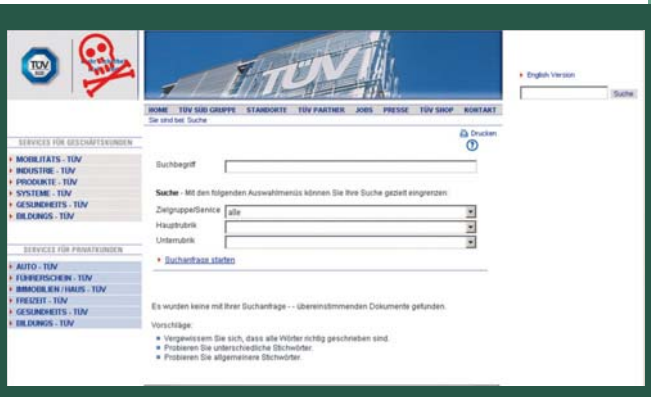
Zajištění stop na místě činu

První stopu jsme objevili na mailovém účtu Michala M. – zprávu s vyhlídkami na lákavé zisky. „Klikněte sem a dostanete se na výherní hru". Na první pohled je zpráva podezřelá, protože na rozdíl od klasického phishingového mailu odkazuje link skutečně na server banky. Ale stopa je to horká: webová stránka, která se otevře, pochází sice z domény bankovního ústavu, ale tam neexistuje. Obsah této stránky neviděl nikdy nikdo jiný než pan M. Vpašoval nějaký hacker tento obsah do spojení pomocí Man-in-the-Middle útoku? To je nemožné: HTTPS, tedy SSL-šifrování na straně banky, takovéto útoky znemožňuje.

Hledáme proto dále a narážíme v mailu na další stopu. URL odkazuje na stránku vyhledávání banky, a tam, kde by měl být zadán hledaný výraz, se nachází nezvykle dlouhý řetězec znaků. Analýza ukazuje jasný výsledek: Jde o hexkód, který se při dešifrování změní na JavaScript, a to na takový skript, který obvykle nebývá uložen na serverech bank. Naše podezření: Pan M. se stal obětí Cross-Site-Scripting útoku (XSS).

Tajemství JavaScriptu: Abychom zjistili, jak útok proběhl, analyzovali jsme link JavaScriptu v laboratoři. Nejdříve jsme otevřeli odkaz tak, jak to udělal i pan M. Na první pohled se nestane nic neobvyklého. Otevře se webová stránka, na níž se prezentuje údajná výherní hra. Bližší zkoumání zdrojového kódu webové stránky však prozradí mnohem více. Tam se totiž objevuje znovu JavaScript kód, který známe z dešifrovaného linku. Kód je přesně na tom místě, kdy by měl být za normálních okolností obsah masky vyhledávání – klasický Cross-Site-Scripting trik.

Teď je nám to již jasné. Programátoři webové stránky pozapomněli filtrovat zadání uživatelů. Hacker proto mohl zadat do formuláře JavaScript tag a čekal již pouze na stisknutí tlačítka „Hledat", aby se skript poté mohl integrovat do stránky. Na stránce



SNADNÁ KOŘIST? Mnoho stránek není vůči Cross-Site scriptingu vůbec chráněno. Některé, jako např. stránky TÜV Süd, byly zabezpečeny až po našem upozornění. Nyní již opět platí slogan, který byl překryt nálepkou hackera: „Více bezpečí, větší hodnota."

Nový seriál Chipu

V americkém kriminálním seriálu CSI: Kriminálka Las Vegas objasňují soudní vyšetřovatelé zločiny pomocí vědeckých metod.

Chip použil CSI pro název nového seriálu a postupně vám odhalí metody, kterými IT profesionálové bojují s počítačovou kriminalitou.

výsledků vyhledávání se pak již neobjevilo „Výsledek hledání [termín]“, ale „Vaše hledání“. Java-Script byl automaticky zabudován na místě hledaného pojmu – a browser ho „spustil“. Pak musel hacker ještě zkopírovat link z adresního řádku do e-mailu panu M.

Abychom si tuto teorii potvrdili, zadáme do masky pro vyhledání bezpečný text

‘;-“<XSS>=&{()}

– trik, který jsme odkoukali od hackerů. A podívejme: Nezměněný sled znaků „<XSS“ ve zdrojovém textu webové stránky banky potvrdil XSS „zázrak“.

Ale co způsobuje JavaScript hackera? Abychom tuto otázku objasnili, otevřeli naši odborníci soubor a rozložili jeho funkce. Výsledek: JavaScript pracuje tak, že sleduje pohyby pana M. na stránce homebankingu. Při jeho pokusu zadat příkaz hacker udeřil. Zablokoval odeslání TAN a požádal pana M. o nové. Pomocí vymámeného čísla, PIN a TAN mohl jít hacker na nákupy. Útok je tedy jednoduchý a hacker měl štěstí – díky tomu, že se pan M. přihlásil na své konto ve správný okamžik, mohl zachytit bankovní data.

Jak ochránit svou webovou stránku

Aktuální phishing filtry jsou v boji proti Cross-Site-Scriptingu bezmocné. Je prostě příliš mnoho způsobů, jak zmanipulovat obsah webové stránky. Navíc k tomu přibývá skutečnost, že útoky neprobíhají na nějakém prolomeném webovém serveru, ale na jinak bezpečných stránkách banky, internetového obchodu nebo zpravodajského magazínu. Jediná rada tedy může znít: Neklikejte na podivné a především příliš dlouhé linky, a to ani v případě, že se jedná o HTTPS stránky. Ani známým internetovým stránkám banky byste neměli bezhlavě důvěřovat. Bezpečné surfování může zajistit v podstatě pouze jediná osoba: webmaster. Ten musí chránit formuláře pro zadávání na internetových stránkách proti manipulaci. V ideálním případě to znamená, že kromě písmen a čísel jsou všechny ostatní znaky ve formulářích tabu. Speciální znaky, jako např. špičaté závorky < >, interpretuje prohlížeč jako programový kód – a provede (spustí) potenciálně nebezpečný JavaScript.

Odvrácená strana prohlížečů

Jednoduché filtrování JavaScript kódu nestačí, což potvrzuje i náhled hackerům pod pokličku. JavaScript HTML příkaz „<script>“ totiž vůbec nepotřebuje. Skript je možno zavolat i jinak, např. přes „<img>“ tag, který za normálních okolností do internetových stránek integruje obrázky. Příkaz

<IMG SRC=jAVascriPt:alert(String.fromCharCode(88,83,83))

funguje v prohlížeči Opera 9.02 stejně jako v Internet Exploreru 6 a obchází řadu mechanismů filtrů. Ten totiž nepoužívá vůbec speciálních znaků, ale směsici velkých a malých písmen. Kromě toho chybí uzavírací závorky. Zda prohlížeče tento příkaz i přesto provedou, to závisí na jejich toleranci chyb. Protože mnoho webových stránek obsahuje špatné HTML tagy a bez korekce chyb by nefungovaly, uvolnili vývojáři (tvůrci) webových stránek trochu pravidla. Z výhody pro uživatele se tak stal zdroj potenciálního nebezpečí.

Chtěli jsme se dozvědět víc, a proto jsme oslovili uznávaného XSS experta. J. P. Hartmann je bezpečnostní expert a šéf firmy Mayflower, která na vyžádání kontroluje webové stránky a vyhledává mezery v zabezpečení. A Hartmann téměř vždy něco najde: „Člověk by nevěřil, kdo všechno je ohrožen.“ Pokud budete chtít prověřit zabezpečení svých webových stránek, můžete využít webový nástroj „Chorizo Security Scanner“, podmínkou je však bezplatná registrace u Mayflower. Po prověření zabezpečení nástroj zahlásí, kde přesně se nebezpečné skulinky nacházejí.

Hrátky se zabezpečením

Ohrožení XSS útoky se týká více webových stránek, než by si člověk uměl představit. Spousta webmasterů nemá o nebezpečných „dírách“ v zabezpečení svých webových stránek ani potuchy. Jiní úmyslně ignorují slabé místo XSS. Ten, kdo tyto vrátka pro hackery co nejrychleji neucpe, dává v sázku bezpečnost své webové stránky i bezpečnost svých návštěvníků. Zabezpečením stránek proti XSS však nejsou ani zdaleka všechna nebezpečí podchycena. Hackeři vymýšlejí stále nové metody útoků. „Jejich kreativita nezná hranic“, potvrzuje Hartmann. Více se dozvíte v dalším díle seriálu „CSI: Internet“.

Valentin Pletzer

VÍCE INFORMACÍ: Na adrese *https://chorizo-scanner.com* najdete webový nástroj firmy Mayflower, který testuje nedostatky v zabezpečení webových stránek.