INFORMAČNÍ ZPRÁVA

160323MIN01 5/4/2016

VÝZNAM			
		ZÁVAŽNÝ	

Název informační zprávy:

Analýza vektoru útoku vedeného z infikované domény škodlivým javascriptem.

Úvodní informace:

Centrum CIRC detekovalo a analyzovalo vektor útoku vedeného z infikované webové stránky např. **http://www.autadomazlice.cz**. Po navštívení této webové stránky dojde ke stažení skriptu „**myzones.xyz/chrome.js?i=0.85451231534534**“, který rozesílá zprávy a status pomocí stánek „**facebook.com**“. Tyto zprávy nabádají uživatele ke stažení skriptu „**video.jse**“. Po kliknutí na video dojde ke stažení skriptu „**autoit**“, který infikuje a přenastaví webový prohlížeč, zablokuje přístupy na stránky antivirových společností. Dále rozesílá odkazy na infikované webové stránky jiným přihlášeným uživatelům na „facebook.com“.

Podrobný technický popis:

Centrum CIRC rozdělilo vektor útoku do čtyř fází, popis jednotlivých fází je uveden níže a grafické znázornění v příloze:

Fáze 1

V první fázi uživatel přistupuje na infikované stránky (viz seznam níže), které mají v kódu webové stránky vložen odkaz na obfuskovaný skript „chrome.js?i=číslo“ (main.js, post.js).

Infikované webové stránky jsou:

- http://www.autadomazlice.cz
- http://kladno.volejbal.cz/cz/a-tym/utkani-turnaje/kdy-po-vanocich-na-extraligu-377.html
- http://mojedilo.ireceptar.cz/navody/konopna-mast-recept-a-vyroba/
- http://www.nabo-rajec.cz/Chia-seminka-1000-g-d777.htm

Po přístupu na infikované stránky dojde k automatickému spuštění skriptu. Útočník vložil odkaz na obfuskovaný skript s různými doménami (viz seznam níže), aby si zabezpečil jeho funkčnost z více cest. Tento skript se během prováděné analýzy měnil, což ukazuje na jeho automatizaci nebo neustálou aktivitu útočníka. V době analýzy byly funkční pouze některé ze škodlivých domén:

- myzones.xyz/chrome.js - funguje
- fsafakfskane.net/chrome.js - nefunguje
- kejumayu.com/main.js - nefunguje
- ue4free.xyz/post.js - nefunguje

Analýzou obfuskovaného skriptu „chrome.js“ bylo zjištěno:

- skript detekuje, zda má uživatel v prohlížeči otevřenou záložku s přihlášeným účtem na „facebook.com“,
- vytvoří status s obrázkem, který vypadá jako spustitelné video s textem „oh my god“,

který po kliknutí odkazuje na infikovanou stránku, ze které se uživateli stáhne do počítače obfuskovaný skript „video.jse“,

- tento status rozešle zprávu desítkám jiných uživatelů, kteří jsou přihlášení na stránky facebook.com,
- funkce get_d() - Generování škodlivých odkazů se skriptem video.jse je prováděno na https://myzones.xyz/goop/get_d.php (Výsledek: https://www.bit.ly/1S3TJO8)
- funkce get_r() - provádí generování spustitelných obrázků, které jsou využity k nalákání uživatelů. Toto se provádí na webových stránkách „https://myzones.xyz/goop/get_r.php“ (Výsledek: https://c2.staticflickr.com/2/1613/25206950673_86387a065e.jpg)
- skript má i další funkce, které dosud nebyly použity. Ty jsme zatím ještě nebyli schopni analyzovat.

2. Fáze

Pokud uživatel klikne na škodlivý odkaz (vytvořený status nebo obrázek na facebook.com - viz 1. fáze), stáhne si skript „video.jse“ do svého počítače v domnění, že se jedná o video.

Analýzou obfuskovaného skriptu „video.jse“ bylo zjištěno:

- po spuštění skriptu se stáhne infikovaný soubory do složky ../AppData/Mozila/
- tyto soubory jsou stahovány z webových stránek „http://neampol.xyz/lom/ekl.jpg “ a jsou uloženy s příponou .jpg
- konkrétně se stáhnou programy autoit.exe, ekl.au3, force.au3, sabit.au3, up.au3, manifest.json, bg.html, ff.zip (soubory profilu programu firefox) a „run.bat“
- po stažení dojde ke spuštění „run.bat“, který spustí „autoit“ a jeho skripty.

3. Fáze

Stažený soubor „run.bat“ spustí „autoit“ s jeho skripty. Analýzou obfuskovaného skriptu „ekl.au3“ bylo zjištěno, že skript:

- manipuluje s verzemi nainstalovaných webových prohlížečů, zaměřuje se na nejpoužívanější prohlížeče chrome.exe, firefox.exe, browser.exe, iexplorer.exe a opera.exe
- smaže ikony prohlížečů z plochy a z panelu start a nahradí je novými s přidaným parametrem a cestou ke škodlivým souborům (appData/Mozila/) --load-and-launch-app="C:\Users\REM\AppData\Roaming\Mozila“
- manipuluje se záznamy prohlížečů v registrech
- rozbalí „ff.zip“ a nakopíruje je do složky \Program Files\Mozilla Firefox, pokud je nainstalována - přidá uživatelský profil
- vypne běžící procesy prohlížečů a po změnách je znovu spustí.

4. Fáze

Pokud uživatel spustí prohlížeč přes ikonu na ploše, nebo v panelu start:

- v případě prohlížeče Firefox Mozilla dojde při každém spuštění k otevření stránky www.youtube.com/watch?v=_rmQN5ghZCY – toto video je již odstraněno z důvodu spamu, klamavých praktik a podvodů

- v případě prohlížeče Google Chrome dojde k přístupu na webové stránky „https://goo.gl/qivXOo“, které odkazují na facebook.com/??. Dojde k otevření staženého souboru bg.html, který spustí skript bg.js na https://lokteamry.xyz/bg.js - tento skript blokuje přístup na stránky antivirových programů a znemožňuje otevřít nastavení v prohlížeči Google Chrome (možná vypíná některé ochrany prohlížeče – nepodařilo se prozatím zanalyzovat)
- skript bg.js spustí skript br.js, který je uložený na webových stránkách https://lokteamry.xyz/br.js - tento skript odkazuje na „facebook.com/hashtag/_profile“ a nejspíše provádí „lajkování“ pomocí „//goo.gl/EUDs6o“ - plugin like.php facebooku, dále spustí br.php, který je na myzones.xyz/br.php?skript
- skript „br.php? “ je totožný se skriptem „chrome.js“ a způsobuje další šíření odkazů přes facebookové statusy a zprávy

Závěr a nutná opatření:

Centrem CIRC byly vytvořeny signatury detekující přístupy na škodlivé skripty. Infikované domény byly přidány do blacklistu.

Dále Centrum CIRC cestou KC CIRC žádá o předání informace na NCKB, které by mělo upozornit uživatele a poskytovatele těchto služeb na výskyt infikovaných stránek.