SECURITY BULLETIN

Týždeň 30. 08. 2017 – 05. 09. 2017

No: B20170905-01V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Google Chrome Extension Banker Malware

Popis

V tomto týždni sa objavila cielená phishingová kampaň, ktorá bola šírená prostredníctvom podozrivých e-mailov s prílohami. Prílohy obsahovali súbory, ktoré slúžili na inštaláciu rozšírení prehliadača Google Chrome, ktorých účelom bolo sledovať a následne odcudziť prihlasovacie údaje do bankových kont, údaje z kreditných kariet a zneužitie ďalších spôsobov platby cez internet. Takisto sa zameriava aj na spôsob platby „boleto“, ktorá je obľúbená najmä v Brazílii.

Útočníci použili ukradnutý firemný e-mailový účet, aby zvýšili mieru úspešnosti a dôveryhodnosti u obete. Príloha e-mailu mala evokovať dokument o prepustených zamestnancoch v súbore s koncovkou .zip.

Technická analýza

- Súbor s koncovkou .zip prílohy e-mailu obsahuje skrytý skript s koncovkou .vbs, ktorý po vykonaní zhromažďuje informácie o systéme a posiela ich na Control & Command server (C & C)
- Na základe získaných informácií C & C server rozhodne, či je infikované zariadenie virtuálne (VM). Ak áno, vráti URL adresu do súboru JPEG, ktorý nie je škodlivý. V opačnom prípade sa vráti URL, cez ktorú stiahne druhú časť škodlivého softvéru, ktorý sa javí ako .zip súbor, no v skutočnosti ide o obfuskovaný VBE skript – tento následne spustí
- VBE skript vykoná ďalšie kontroly systému a následne stiahne ďalší .zip súbor, ktorý obsahujú adresár "Chrome" a DLL knižnicu
- DLL knižnica je nainštalovaná a nakonfigurovaná tak, aby sa načítala vtedy, ak sa používateľ prihlási do systému
- Rozšírenie Google Chrome je programovo načítané do prehliadača Google Chrome pomocou parametra "--load-extension"
- Škodlivé rozšírenie s názvom IDKEY STOR začne monitorovať všetky navštevované webové lokality a identifikuje v nich citlivé informácie. Keď sa zhodujú s konkrétnym reťazcom, rozšírenie zaznamená tieto informácie a posiela ich na C & C server
- Pri „boleto“ transakciách je škodlivý kód zameraný na to, keď obeť generuje čiarový kód transakcie. Pri generovaní tohto čiarového kódu malvér zachytáva komunikáciu, komunikuje s C & C serverom a žiada od neho náhradný, podvodný čiarový kód. Následne komunikuje s API rozhraním v inej finančnej inštitúcii, generuje obrázok čiarového kódu a nahradí ten, ktorý sa mal pôvodne vygenerovať. Obeť teda obdrží podvodný čiarový kód a po jeho zobrazení a použití vykoná platbu na účet útočníka.

Zasiahnuté systémy

Google Chrome – pri inštalácii z nedôveryhodných zdrojov alebo inštalácii nedôveryhodných rozšírení

Následky

Strata citlivých údajov, neoprávnené vykonanie škodlivého kódu

IOC (Indicators of Compromise)

MD5 hashe Google Chrome rozšírenia:

MD5 (1.js) = 1d91e021e5989029ff0ad6dd595c7eb1
MD5 (2.js) = d996bdc411c936ac5581386506e79ff4
MD5 (3.js) = 59352276c38d85835b61e933da8de17b
MD5 (manifest.json) = c6157953f44bba6907f4827a1b3b4d0a

MD5 hashe iných súborov:

MD5 (myinside.dll) = 574322a51aee572f60f2d87722d75056
MD5 (uia.zip) = bae703565b4274ca507e81d3b623c808

URL odkazy:

hxxp://cdn.ahnegao.com.br/2017/07/casa.jpg?1491404962
hxxp://storage.googleapis.com/fogoreal/uia.zip
hxxp://storate.googleapis.com/fogoreal/top019.zip
hxxps://tofindanotherrace.com/
hxxp://insidevx.net/log5.php?logins=did&s=ch
hxxp://insidevx.net/log5.php?logins=did&s=b

Súbory detekované v systéme:

%userprofile%\appdata\roaming\microsoft\windows\start menu\programs\startup\<randomname>.vbs
%userprofile%\myinside.dll
%userprofile%\ext\[Chrome|1.9.6]

Odporúčania

V záujme ochrany vašich citlivých údajov a informácií vám odporúčame dodržiavať nasledujúce opatrenia:

- Inštalujte softvér a rozšírenia softvéru len z overených a dôveryhodných zdrojov.
- Neotvárajte prílohy podozrivých e-mailov. V prípade, ak si nie ste istí, či sa jedná o podozrivú prílohu, kontaktujte odosielateľa (ak je vám známy) iným spôsobom ako e-mailom a overte, či vám skutočne zaslal e-mail s prílohou. Ak však máte akékoľvek pochybnosti o pôvode e-mailu, kontaktujte IT oddelenie vašej organizácie a požiadajte ich o pomoc.
- Používajte aktualizované antivírové a antimalvérové programy, ktoré dokážu detekovať škodlivý softvér.

Zdroje

https://isc.sans.edu/forums/diary/Second+Google+Chrome+Extension+Banker+Malware+in+Two+Weeks/22766/

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
06282/2017/SKB/OBPr-003

SECURITY BULLETIN

Týždeň 30. 08. 2017 – 05. 09. 2017

No: B20170905-02V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Spreading of Facebook malware

Popis

Spoločnosťou Kaspersky Lab a niekoľkými ďalšími cyber security odborníkmi bola zaznamenaná malvérová kampaň, cielená na používateľov sociálnej siete Facebook. Cieľom tejto kampane je masívne rozšírenie za účelom získania prístupových tokkenov používateľov, ktoré nemajú dátum expirácie.

Vektor infekcie a technická analýza

V prvotnej fáze sa malvér šíril pomocou Facebook Messengera, resp. cez správy vo webovom rozhraní. Obeť prijala správu od osoby vo svojom friendliste s videom, ktoré odkazovalo na falošnú stránku YouTube, kde sa spustilo sťahovanie škodlivého rozšírenia do prehliadača alebo sa spustila iná časť kódu podľa platformy, akú obeť používala (API, webové rozhranie, rôzne prehliadače a pod.). Škodlivý kód následne v komunikácii definoval prístupový tokken, ktorý odoslal na externý server, ovládaný útočníkom. Následne bolo vygenerované URL, ktoré bolo zaslané online priateľom obete.

Momentálne sa malvér šíri týmto spôsobom:

1. Načítava CSRF token a ID profilu (profile_id) od obete
2. Ak je vypnutá Facebook platforma na spúšťanie aplikácií tretích strán, malvér ju povolí
3. Načíta prístupový tokken pre aplikáciu „Pages Manager for iOS“ s app-id: 165907476854626
4. Z odpovede, ktorá prebieha medzi obeťou a aplikáciou, vyčíta prístupový tokken obete a tento zašle na server útočníka
5. Zbiera informácie obeti využitím Facebook Graph API s atribútom „name“
6. Vytvorí požiadavku na endpoint obete, čo spôsobí vytvorenie verejnej URL adresy na Google Drive s PDF súborom
7. Vytvorí pop-up okno pre link, ktoré je súčasťou Facebooku a vloží doň link s malvérom
8. Vytvorí post (status) a link je zdieľaný – je verejný a prístupný pre každého používateľa, nie len pre priateľov obete.
9. Využije friend list obete na získanie informácií a hľadá online a aj neaktívnych priateľov obete.
10. Označí všetkých priateľov z listu obete v poste (statuse), ktorý pred tým vytvoril použitím atribútu: comment_text: "@[1234:Test User] @[12345:Test User 2]"

Zasiahnuté systémy

Používateľské kontá sociálnej siete Facebook

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava
Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*
SK-CERT
Naša značka:
06282/2017/SKB/OBPr-003

Následky
S prístupovým tokkenom má útočník širokospektrálne možnosti, nakoľko vlastník tokkenu môže získať prístup k profilu obete (pôvodného majiteľa tokkenu), zmazať, upraviť, odcudziť alebo vytvárať veľké množstvo údajov a informácií o obeti, napríklad: - Prístup k friendlistu obete - Zverejňovanie obsahu na Facebooku v mene obete - Prístup k údajom služby Instagram, ak je táto pripojená k účtu na Facebooku obete - Odosielanie správ na Facebooku v mene obete - Prístup ku všetkým stránkam na Facebooku, ku ktorým má obeť prístup

Odporúčania
Na základe vektora infekcie a technickej analýzy malvéru odporúčame aplikovať nasledujúce odporúčania: - Na sociálnej sieti Facebook neotvárajte nedôveryhodné a neoverené externé URL odkazy od vašich priateľov alebo od cudzích používateľov - Po prijatí správy s podozrivým obsahom tento neotvárajte, ak je to možné, upozornite používateľa, od ktorého ste obdržali podozrivú správu, že vám takúto správu poslal, a to najlepšie iným spôsobom ako prostredníctvom správ na Facebooku (e-mailom, telefonicky, osobne) Čo je však najdôležitejšie pripomenúť – prístupový tokken, ktorý je odcudzený útočníkom, nemá dátum expirácie, čo znamená, že jeho platnosť je neobmedzená a tak môže na profil obete pristupovať bez časového obmedzenia. Taktiež to znamená, že nie je žiadny spôsob, ako zrušiť, zmazať alebo inak znefunkčniť prístupový tokken ak už ste boli infikovaný malvérom. Je preto nutné počakť na krok Facebooku, ako budú celú situáciu riešiť.

Zdroje
https://labs.detectify.com/2017/08/31/dissecting-the-chrome-extension-facebook-malware/