AHOJ, ASI SA TERAZ ČUDUJEŠ, ČO SA VLASTNE STALO.

Náplň projektu

Môj projekt je zameraný na útok škodlivým software-om, a ako jeho súčasť som zapracoval simuláciu útoku na seba, kedy sa útočník dostal k mojim Facebook údajom, a mohol rozšíriť tento malware cez Messenger správy. Konkrétne som sa zameral na ransomware, alebo škodlivý kód, ktorý vám zablokuje údaje na počítači, a potom si žiada výkupné za ich navrátenie do pôvodného stavu.

Hrozba

Keď ste aplikáciu spustili sami od seba, bez toho, aby ste vedeli, že vás sem zavedie, tak ste sa vystavili hrozbe útoku. V tomto okamihu by ste už mali zašifrované dôležité údaje na počítači (fotky, osobné súbory, dokumenty ...), a na obrazovke by vám svietilo upozornenie, že ste boli napadnutí, a máte určitý čas na zaplatenie výkupného, alebo svoje dáta už neuvidíte (a/alebo budú predané tretej strane). Takto spustený program má prístup ku všetkým dátam a údajom, ako aktuálne prihlásený používateľ, ale ak si pri spustení alebo inštalácii vyžiada administrátorské práva (a obeť to schváli), získava prístup ku celému obsahu vášho počítača.

Ak ste aplikáciu sami nespustili, chcel by som vás aj tak poprosiť o vyplnenie dotazníku: https://forms.gle/Tm2e2KPPNwGtcz1C9

AKO SA VYHNÚŤ ÚTOKOM A INÉMU ŠKODLIVÉMU OBSAHU

Opatrnosť

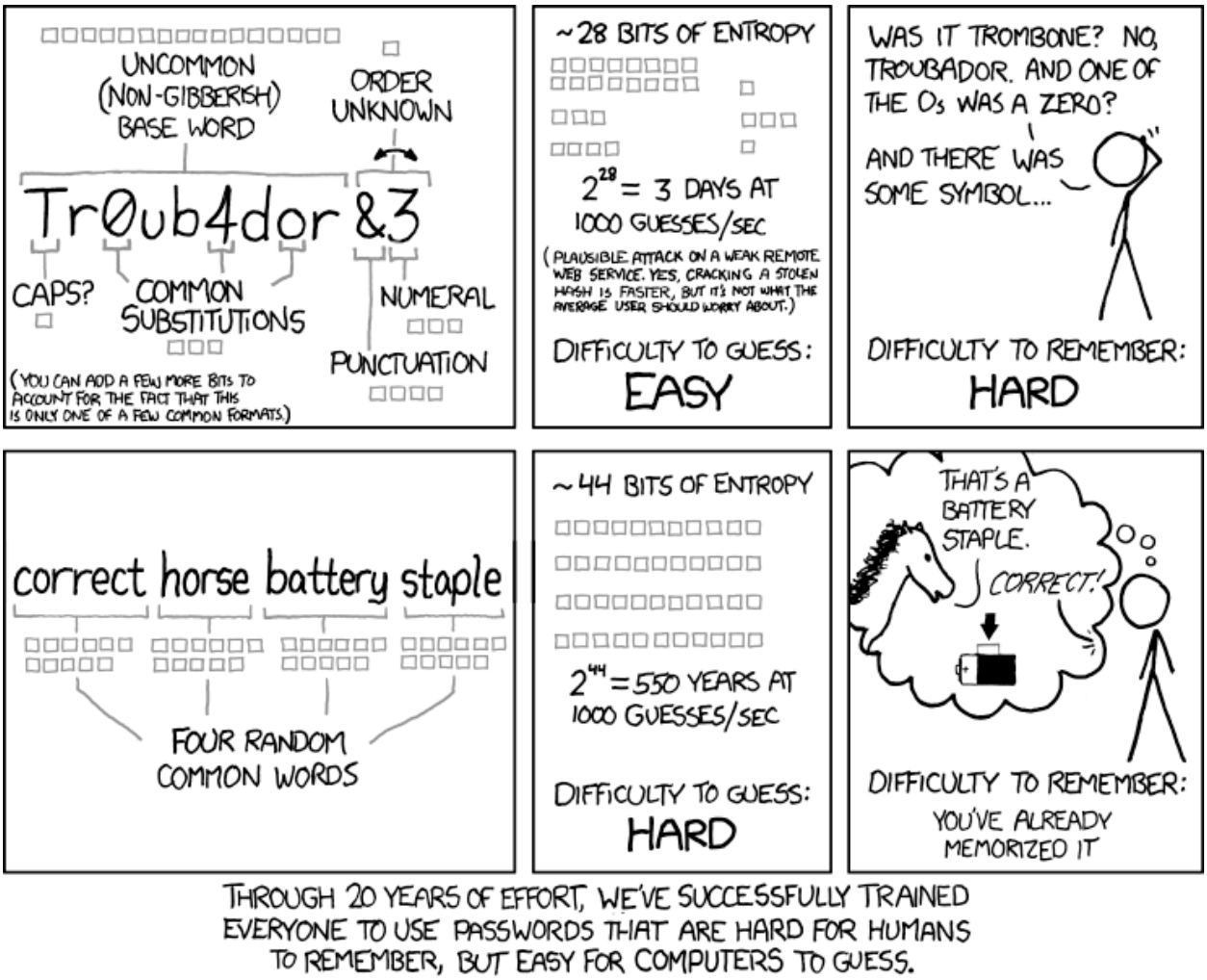
Najjednoduchší, a najdôležitejší spôsob, ako sa dá škodlivému software-u vyhnúť je: dávať si pozor pri otváraní neznámych link-ov a pri sťahovaní súborov z neznámych stránok. Ak vám príde správa, ktorá nevyzerá veľmi legitímne, skúste si najskôr overiť, či sa nejedná o podobný útok, ako bol simulovaný v tomto projekte.

Toto zahŕňa hlavne email-ové prílohy a linky, chat-ovacie služby (aj sms-ky), ale hlavne okná, ktoré sa samé otvárajú pri navštívení niektorých stránok (pop-up windows).

Pri sťahovaní obsahu (hlavne torrentov, alebo nelegálne šírených kópii hier, filmov) si treba tiež dávať pozor, nakoľko tieto súbory môžu slúžiť ako trójsky kôň pre malware, a tak namiesto novej hry sa vám na počítači zobrazí chybová hláška.

Heslá

Používanie silného hesla. Heslo, ktoré sa môže zdať človeku náročné môže byť v skutočnosti veľmi jednoduché na prelomenie strojom. (Neodporúča sa ale ani použiť nižšie spomínané “correcthorsebatterystaple”, nakoľko to je svetovo známe).



Antivírus

Využitie anitivírusového programu. Tieto programy sú priamo určené na kontrolovanie stiahnutých súborov, zaznamenávanie nezvyčajnej aktivity, a iné. Vďaka použitiu antivírusového programu sa môžete kompletne vyhnúť vírusom, alebo aj opraviť niektoré napáchané škody. Vedia odhaliť, ak sa na vašom počítači už nachádza nejaký malware, ktorý napríklad zbiera údaje o vašej aktivite, alebo využíva váš hardware (grafickú kartu, procesor) keď ich vy nepoužívate.

Aktualizácie

Aktualizovanie systémových aplikácii. Windows 10 dostáva nové bezpečnostné aktualizácie pomerne často (aj viackrát do mesiaca), preto je dobré ich inštalovať, nie len odkladať čím neskôr, pretože sa tak vystavujete riziku útoku kvôli nejakej chybe, ktorá už môže byť v ďalšej verzií programu ošetrená.

Admin

Odporúča sa, nepoužívať administrátorského používateľa na bežné aktivity. Je to z dôvodu, že administrátorské konto má všetky možné získateľné práva, preto je aj pre škodlivý software jednoduchšie cez neho napádať počítač (automaticky má viac práv, môže otvárať viacero priečinkov, pristupovať k viacerým súborom ...).

Zálohovanie

Zálohovanie je prospešné nielen pri útoku na počítač, ale aj pri fyzickej poruche niektorého z komponentov. Odporúča sa robiť si zálohy na externý disk (ktorý nie je pripojený k počítaču) aspoň raz za mesiac, ale aj raz za pol roka je lepšie, ako nič. Na zálohovanie sa dajú tiež využívať online úložiskové priestory (Google Drive, OneDrive ...). Tieto služby majú verziu zadarmo, a pri zaplatení (napríklad mesačnej platby) sa zväčší dostupné úložisko.

ČO ROBIŤ V PRÍPADE, ŽE STE NAPADNUTÍ

Antivírus

Pri bežných útokoch stačí pri podozrení na napadnutie stiahnuť niektorý z dostupných antivírusových programov, ktorý vykoná hlboký sken cez celý počítač, a ak sa tam nachádza nejaký malware, ktorý využíva vaše prostriedky, monitoruje aktivitu alebo iné, tak ich vie odhaliť a vymazať.

Ransomware

Pri ransomware útokoch je ale problém, že súbory už sú zašifrované, a ich odšifrovanie je prakticky nemožné bez kľúča na odšifrovanie. Preto aj keď antivírus odhalí nejaký škodlivý program (centrum útoku), súbory už vrátiť nevie.

Zaplatiť výkupné

Ak si obeť neudržiavala zálohy na nejakom externom úložisku, jediná možnosť je zaplatiť výkupné. Problém ale je, že takmer v tretine prípadoch útočník dáta ani po zaplatení výkupného neodblokoval.

Obnova systému

Obnovenie celého systému, alebo nová inštalácia systému je najbezpečnejší spôsob, ako svoj počítač zbaviť malware-u. Táto metóda vás ale zbaví aj všetkých dát, preto je potrebné si udržiavať zálohy na externom disku, ktoré môžu byť následne znovu stiahnuté a načítané.

ČO ROBIŤ, AK NEMÁM ZÁLOHY

Zašifrované údaje

V prípade, že nemáte žiadne dostupné zálohy, a váš počítač bol napadnutý nejakým škodlivým kódom, ktorý vám zašifroval dokumenty, zostáva už len obrátiť sa na profesionálov. Kontaktovať nejakú antivírusovú firmu, ktorá sa už mohla s takýmto útokom stretnúť, a teda môže vedieť pomôcť (napríklad ESET). Môžu za to ale požadovať pomerne vysoké poplatky, preto treba zvážiť, či sa to oplatí.

Vymazané dáta

Ak boli údaje vymazané, existuje množstvo programov, ktoré vedia takto odstránené súbory vrátiť naspäť. Najdôležitejšie je stiahnuť tento program na nový disk (aby sa predišlo prepísaniu existujúcich údajov), ak to nie je možné, tak pri stiahnutí na napadnutý disk hrozí, že niektoré z dokumentov nebudú obnovené. Ak škodlivý program len vymazal údaje, a neformátoval ich priestor, je možné, že takýto program na obnovu dát vymazané dokumenty objaví. Ak ale malware prepísal miesto, kde sa súbory nachádzali, už sú natrvalo vymazané, a nie je možné ich získať späť.

Disclaimer

Môj program, aj celá simulácia útoku je verejne dostupná na adrese nižšie, a nie je žiadnym spôsobom nebezpečný. Celá jeho činnosť je otvorenie dvoch link-ov v predvolenom prehliadači, jeden na dotazník, a jeden na GitHub repozitár, kde sa nachádzajú všetky súbory tejto simulácie útoku. Program nezhromaždil, neprečítal a ani nikam neposlal vaše údaje.

ZDROJE

1. Samuel Bubán: RansomwareAwareness 2.3.2021
   https://github.com/Mahrkeenerh/RansomwareAwareness

2. xkcd: Password Strength
   https://xkcd.com/936/

3. levinec, Dansimp, Alluthewriter, joinimran, martyav, imba-tjd, DaniHalfin, get-itips, nschonni, DuncammaMSFT: Prevent malware infection 1.22.2021
   https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection

4. Google Support: Protect yourself from malware
   https://support.google.com/google-ads/answer/2375413?hl=en

5. Amrit Singh: Ransomware: How to Prevent or Recover from an Attack 13.10.2020
   https://www.backblaze.com/blog/complete-guide-ransomware/