Tema 8 Carbanak/Anunak

Raportul ce l-am ales este un raport de alerta de securitate de la Visa, in urma descoperirii facute de laboratoarele de la Kaspersky in februarie 2015 in legatura cu un APT stil de atac asupra institutiilor financiare, cu localizare in Ucrania, Rusia si Europa Centrala. Din 2013 grupul infractional cibernetic a folosit un malware identificat ca Carbanak cu o campanie sofisticata de a comite frauda financiara. Peste 100 de institutii financiare au fost afectate si se raporteaza daune in jurul sumei de 1 miliard de dolari.

Ca si descriere a atacului, este utilizata o metoda de spearphising ce e conceput a parea comunicare bancara legitima, folosind ca atasament un fisier Word si unul de tip Control Panel (.cpl). Odata ce atasamentele au fost deschise, este lansat un backdoor de exploatare numit Carbanak.

Odata ce backdoorul este realizat, atacatorii au acces remote asupra retelei tinte si pot face o scanare pentru a identifica sistemele si infrastructurile critice. Principalele tinte alte atacatorilor au fost bancomatele ATM si conturile financiare. S-a facut posibila modificarea bazelor de date a soldurilor conturilor, crearea de noi conturi bancare pentru a transfera banii si distrubuire de bani a divere bancomate unde atacatorii au fost pregatiti de recuperarea banilor.

In unele cazuri au fost capturate inregistrari video ale operatiunilor bancare, au fost inregistrate tastele (keystrokes), pentru a imita tranzactii legitime. Conturile ar fi fost marite la o anumita suma si apoi se retragea suma adaugata pentru a nu crea suspiciuni. De exemplu un cont cu 1000 de dolari ar fi fost crescut la 10000, iar atacatorul ar transfera diferenta de 9000 de dolari astfel incat titularul sa nu suspecteze nicio modificare in cont.

Tehnici, Tactici si Proceduri utilizate

**Spearphishing Attachment** (T1566.001):  
 Atacatorii au utilizat e-mailuri de tip spearphishing cu atasamente malitioase (.cpl sau .doc) care, odata deschise, declansau executarea malware-ului Carbanak.

**Remote Access Software** (T1219):  
 Dupa ce backdoor-ul era activ, atacatorii obtineau control de la distanta asupra retelelor vizate.

**Credential Dumping** (T1003):  
 Pentru a accesa conturi si a obtine privilegii mai mari, atacatorii extrageau acreditarile utilizatorilor.

**Manipulation of Financial Data** (T1565):

Modificarea soldurilor conturilor bancare.

Crearea de conturi fictive pentru transferuri financiare frauduloase.

**File and Directory Discovery** (T1083):  
 Cautarea fisierelor si directoarelor relevante, cum ar fi cele din "ProgramData" si alte locatii comune pentru stocarea datelor de utilizator.

**Indicator Removal on Host** (T1070):  
 Stergerea urmelor activitatilor, inclusiv fisierele binare malitioase si alte artefacte.

Lista completa a TTP-urilor este in link-urile din referinte a site-ului Mittre Att&ck.

Remediere, este recomandat ca institutiile financiare sa scaneze reteaua pentru urmatoarele IOCs

- Fisier Paexec

- Fisier cu extensie .bin (localizat in \All users\%AppData%\Mozilla\ sau c:\ProgramData\Mozilla\)

- Fisier Svchost.exe (localizat in Windows\System32\com\catalogue\)

- Serivicii rulate ce au ca terminatie sys

De asemenea pentru a preveni acest tip de atac este recomandata educarea angajatiilor asupra atacurilor de tip phishing si evitarea deschiderii atasamentelor, mentinerea la zi a actualizarilor de sistem si patchurilor software, utilizarea unui software de antivirus cu capacitatea de analiza comportamentala.

Referinte

<https://usa.visa.com/dam/VCOM/download/merchants/Alert-CARBANAK.pdf>

<https://attack.mitre.org/groups/G0008/>

<https://attack.mitre.org/software/S0030/>