BCYB 2019L

ANALIZA RAPORTU „HAMMERTOSS” GRUPY FIRE EYE

Artur M. Brodzki

12 marca 2019

1 WSTĘP

W niniejszym dokumencie przeanalizowano raport grupy FireEye dot. złośliwego oprogramowania typu APT, tzw. „Hammertoss”, wykorzystującego zaawansowane metody steganografii i unikania wykrycia. Analizę przeprowadzono z punktu widzenia koncepcji Intrusion Kill Chain oraz matrycy MITRE Attack. Rozważono również potencjalne sposoby obrony przed tego rodzaju zagrożeniami.

2 ANALIZA IKC

Według koncepcji IKC (ang. *Intrusion Kill Chain*), atak sieciowy sklada się z 7 podstawowych faz:

1. Rekonesans,
2. Uzbrajanie,
3. Dostarczenie,
4. Eksploitacja,
5. Instalacja,
6. Command and Control,
7. Akcje atakujących.

Przedmiotowy raport nie skupia się na pierwszych pięciu fazach ataku sieciowego, począwszy od rekonesansu do instalacji; zamiast tego, otrzymujemy szczegółowey opis działania backdoora już po jego pomyślnym dostarczeniu i zainstalowaniu na maszynie ofiary. „Hammertoss” stosuje zaawansowane techniki steganograficzne, wykorzystując media społecznościowe do ukrytego przekazywania komend od operatora backdoora – jest to faza Command and Control. Dodatkowo, backdoor posiada możliwość wykradania danych z zainfekowanej maszyny i przekazywania ich na zdalny serwer atakującego. Odbywa się to poprzez upload danych na konto w chmurze, którego dane zostały przekazane w kanale C&C. Jest to faza akcji atakujących.

3 MITRE ATTACK

Matryca MITRE Attack stanowi metodę klasyfikacji ataków sieciowych w sposób dwupoziomowy, z podziałem na taktyki – działania służące do osiągnięcia określonego celu oraz techniki – w ramach zadanej taktyki, konkretny sposób (zachowanie) pozwalające na osiągnięcie zadanego celu.

W przedmiotowym raporcie zawarto opisy trzech głównych taktyk realizowanych przez programowanie „Hammertoss": *defense evasion* (unikanie obrony), *exfiltration* (infiltracja[1]) oraz *command and control*:

1. *Defense evasion*: „Hammertoss" wykorzystuje technikę *Deobfuscate/Decode Files or Information*, a mianowicie ukrywanie danych w plikach obrazkowych, zamieszczanych na generowanych pseudolosowo kontach twitterowych sprawiających wrażenie kont zwyczajnych użytkowników;

2. *Exfiltration*: „Hammertoss" oprócz tego, że ukrywa dane (steganografia) to stosuje jeszcze szyfrowanie (*Data encryption*), wyprowadzając dane poprzez upload na zadane konto w chmurze; dane tego konta przekazywane sa w kanale C&C, jest to technika *Exfiltration Over Alternative Protocol*;

3. *Command and control*: do komunikacji z operatorem stworzono autorski protokół komunikacji (*Custom Command and Control Protocol*), którzy wykorzystuje Twittera jako warstwę pośrednią (*Connection Proxy*), ukrywający komendy do przekazania w plikach obrazkowych (*Data Obfuscation*).

Techniki te połączone razem tworzą narzędzie, które jest szczególnie trudne do wykrycia.

4 TECHNIKI OBRONY

„Hammertoss" stosuje znany algorytm ukrywania danych w pliku obrazkowym, możliwe jest więc stosowanie narzędzi przeznaczonych do wykrywania tego rodzaju ukrytej transmisji za pomocą sygnatur. Wydaje się jednak, że w wypadku nieznanego zagrożenia realizującego działania steganograficzne, główną linią obrony powinna być analiza ruchu przez systemy typu IDS/IPS. Wykrycie anomalii w ruchu sieciowym, np. ponadprzeciętnie częstych zapytań do Twittera, powinno zwrócić uwagę administratorów na możliwość zainfekowania sieci przez nieznany malware, wykorzystujący Twittera jako medium komunikacji.

5 PODSUMOWANIE

Raport FireEye stanowi interesującą analizę niebezpiecznego oprogramowania, które dzięki połączeniu wielu różnych technik w jednym narzędziu stanowi duże wyzwanie dla cyberbezpieczeństwa.

[1] W języku angielskim występują osobne określenia *exfiltration* oznaczające ukryte wynoszenie danych oraz *infiltration* posiadające głównie znaczenie hydrologiczne, ale też oznaczające uzyskanie nieautoryzowanego dostępu do miejsca lub zasobów. W języku polskim słowo „eksfiltracja" nie występuje i jako takie stanowi niepoprawną kalkę językową, a zarówno nieautoryzowany dostęp do danych jak i ich wynoszenie na zewnątrz mieszczą się w zakresie słowa „infiltracja", używanego głównie w żargonie wojskowym.