**MALWARE ANALYSIS**

**BadRabbit**

**Analisi statica:**

Il Bad Rabbit Virus è un tipo di ransomware apparso per la prima volta nel 2017 e prese di mira aziende del settore dei media in Russia e Ucraina. Presenta alcune caratteristiche comuni ad altri ransomware come WannaCry e Petya.

Ransomware come Bad Rabbit possono attaccare la rete in due modi: crittografando i file oppure bloccando lo schermo. Nel primo caso i dati presenti nel sistema colpito vengono cifrati e resi inaccessibili senza la rispettiva chiave di decifratura. Gli screen locker, invece, si limitano a bloccare l'accesso al sistema, attraverso una schermata di blocco, che avvisa la vittima del fatto che il sistema è stato crittografato.

Camuffato come un aggiornamento di Adobe Flash player, il Bad Rabbit si diffonde attraverso download nascosti, drive-by downloads, da siti web compromessi. Le vittime possono infettarsi semplicemente visitando un sito web malevolo o compromesso. Il malware viene incorporato nei siti web, utilizzando codice JavaScript iniettato nel codice HTML dei siti.

Se una persona clicca sul file di installazione, il ransomware Bad Rabbit crittografa tutti i file e mostra all'utente uno scarno messaggio in rosso e nero con le seguenti parole: “Se state leggendo questo messaggio, i vostri file non sono più accessibili. Magari state pensando di poter trovare un modo per recuperare i vostri file. Non perdeteci neppure il tempo”.

Il messaggio richiede il pagamento di circa 280$ in Bitcoin entro 40 ore. Alcune vittime, hanno riportato che, il pagamento del riscatto, ha consentito di rientrare in possesso dei file.

Possiamo oltremodo analizzare il malware attraverso CFF Explorer:

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

**Analisi dinamica:**

Per questo tipo di analisi utilizziamo il sandbox Cuckoo:

Immagine che contiene testo, software, Pagina Web, Icona del computer

Descrizione generata automaticamente

Al termine dell’analisi ci fornisce un report dettagliato:

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, linea, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Ho poi avviato il malware e al fine di vederne il funzionamento ho avviato il tool ProcessMonitor:

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Immagine che contiene testo, software, computer, Icona del computer

Descrizione generata automaticamente