

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.

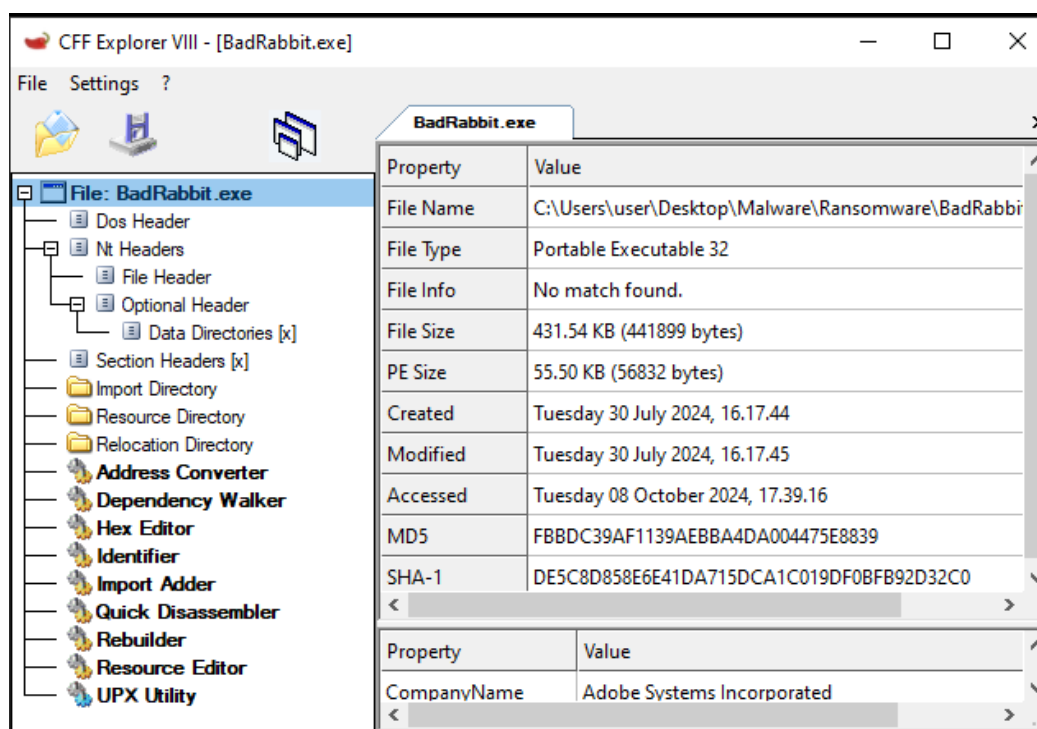
Ransomware come Bad Rabbit possono attaccare la rete in due modi: crittografando i file oppure bloccando lo schermo. Nel primo caso i dati presenti nel sistema colpito vengono cifrati e resi inaccessibili senza la rispettiva chiave di decifratura. Gli screen locker, invece, si limitano a bloccare l'accesso 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:



CFF Explorer VIII - [BadRabbit.exe]

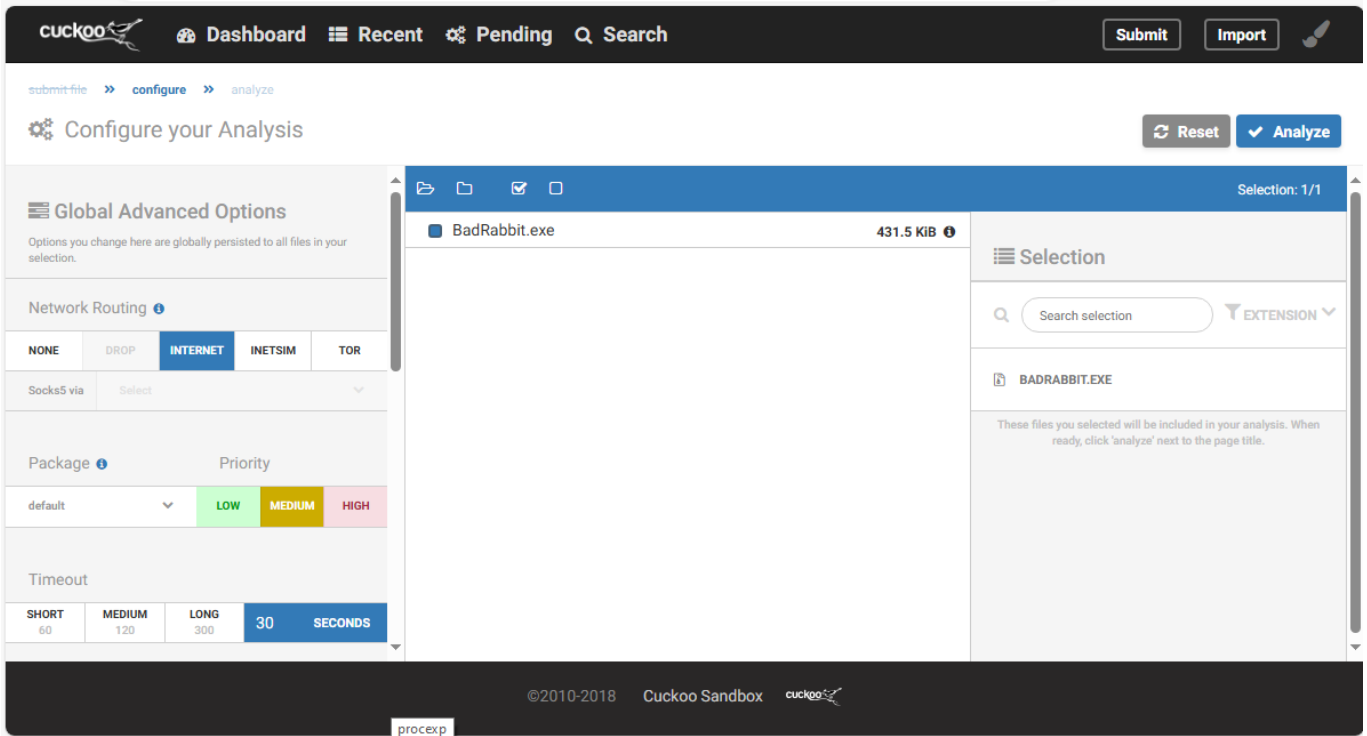
File Settings ?

BadRabbit.exe

Property	Value
File Name	C:\Users\user\Desktop\Malware\Ransomware\BadRabbit.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	431.54 KB (441899 bytes)
PE Size	55.50 KB (56832 bytes)
Created	Tuesday 30 July 2024, 16.17.44
Modified	Tuesday 30 July 2024, 16.17.45
Accessed	Tuesday 08 October 2024, 17.39.16
MD5	FBBDC39AF1139AEBBA4DA004475E8839
SHA-1	DE5C8D858E6E41DA715DCA1C019DF0BF892D32C0
Company Name	Adobe Systems Incorporated

Analisi dinamica:

Per questo tipo di analisi utilizziamo il sandbox Cuckoo:



Al termine dell'analisi ci fornisce un report dettagliato:

File *BadRabbit.exe*

Summary

Ultimo salvataggio del documento: Adesso

Download

Resubmit sample

Size	431.5KB
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	fbbdc39af1139aebba4da004475e8839
SHA1	de5cd858e6e41da715dca1c019df0bf92d32c0
SHA256	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da
SHA512	Show SHA512
CRC32	5FA1C9A5
ssdeep	None
Yara	<ul style="list-style-type: none">BadRabbit_Gen - Detects BadRabbit RansomwareCrowdStrike_CSIT_17183_01 - Detects BadRabbit Dropperwin_files_operation - Affect private profile

Score

This file is **very suspicious**, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Signatures

Yara rules detected for file (3 events)

>

Allocates read-write-execute memory (usually to unpack itself) (26 events)

>

Queries for the computename (2 events)

>

Checks if process is being debugged by a debugger (1 event)

>

Command line console output was observed (2 events)

>

Creates executable files on the filesystem (1 event)

>

Creates a suspicious process (3 events)

>

A process created a hidden window (1 event)

>

Searches running processes potentially to identify processes for sandbox evasion, code injection or memory dumping (1 event)

>

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

>

Checks for the Locally Unique Identifier on the system for a suspicious privilege (3 events)

>

Expresses interest in specific running processes (1 event)

>

Uses Windows utilities for basic Windows functionality (3 events)

>

❌ Installs itself for autorun at Windows startup (2 events)	>
❌ Created a service where a service was also not started (1 event)	>
❌ Uses Sysinternals tools in order to add additional command line functionality (1 event)	>
❌ File has been identified by 14 AntiVirus engine on IRMA as malicious (14 events)	>
❌ File has been identified by 65 AntiVirus engines on VirusTotal as malicious (50 out of 65 events)	>

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

