Ejercicio de análisis malware

Datos generales:

Filename ***8cc84c910910535990b7.exe***

File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	212480 bytes
MD5	a57745a30d63f511d28aa43e4b710e1c
SHA1	5985e7d1831784fd15de2cc62451deb16b65b046
SHA256	8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3
SHA3-384	a4d474c03a27132484c5ebda6e12715cef86624e72c9a8ff44ec98ed828f9039e15988a6af16efdb311223d77125829f
CRC32	FDD14294
TLSH	T14324BF02F2D0C473D5DA20F252155FF6EEFAE83204769D87C3581AA54E686D2E71A2CF
Ssdeep	6144:634cRT8CJLtVXW+BPGaDEoi/Siazel15:s4OT8CJpVm+BuaDm/Sps

Análisis estático

Reglas Yara:

Vemos que durante el análisis estático realizado con CAPE ninguna regla YARA detecta el ejecutable, por lo que no obtenemos información sobre que realiza el malware desde este punto.

Estructura del PE:

Vemos las siguientes secciones:

.text

.rdata

.data

.cdata

.CRT

De esto deducimos que no existe packer en el PE, ya que vemos que la entropía mas alta es de 6,9, lejos del umbral de 7,5 que se espera cuando existe algún packer.

Strings:

Vemos indicativos de métodos antisandbox, como retrasar el análisis mediante un sleep o la comprobación de existencia de conexión:

Sleep
InternetConnectA
InternetReadFile
HttpOpenRequestA
HttpSendRequestA
InternetOpenA
InternetCloseHandle

Vemos que usa funciones especificas de servicios criptográficos, lo que nos indica que puede tratarse de un ransomware:

CryptAcquireContextW
CryptGetKeyParam
CryptReleaseContext
CryptGenRandom
CryptStringToBinaryA
CryptBinaryToStringA

Mitre:

A continuación, enumeramos los diferentes códigos de mitre se identifican del análisis estratico:

T1033 - System Owner/User Discovery

user_enum

T1083 - File and Directory Discovery

antiav_detectfile

T1518 - Software Discovery

antiav_detectfile

T1055 - Process Injection

injection_inter_process

T1070 - Indicator Removal on Host

deletes_executed_files

T1112 - Modify Registry

modify_proxy

stealth_hiddenreg

creates_largekey

persistence_autorun

T1202 - Indirect Command Execution

suspicious_command_tools

uses_windows_utilities

T1562 - Impair Defenses

stealth_hiddenreg

antisandbox_unhook

T1564 - Hide Artifacts

stealth_window

stealth_hiddenreg

T1546 - Event Triggered Execution

persistence_shim_database

T1547 - Boot or Logon Autostart Execution

persistence_autorun

T1071 - Application Layer Protocol

network_multiple_direct_ip_connections

network_http

procmem_yara

network_cnc_http

http_request

powershell_request

suspicious_ping_use

recon_checkip

T1095 - Non-Application Layer Protocol

network_excessive_udp

T1106 - Native API

process_creation_suspicious_location

antidebug_guardpages

T1203 - Exploitation for Client Execution

stack_pivot

exploit_heapspray

T1185 - Browser Session Hijacking

cape_extracted_content

T1485 - Data Destruction

anomalous_deletefile

T1539 - Steal Web Session Cookie

infostealer_cookies

Viendo estos códigos nos permite observar el funcionamiento el malware: vemos que busca usuarios en el sistema (T1033), busca bloquear los posibles antivirus (T1083 y T1518), usa inyección de código (T1055), elimina procesos ejecutándose (T1070), crea persistencia mediante registro, base de datos y inicio automático (T1112, T1546 y T1547), crea procesos en 2º plano (T1564), elimina archivos (T1485), robo de cookies (T1539) y emplea conexiones a internet (T1095 y T1071)

Análisis dinámico

Firmas:

- Conexiones con IP's caídas:

  IP: 34.107.221.82:80 **(United States)**
  IP: 127.0.0.1:49310
  IP: 127.0.0.1:49350

- Enumeración de usuarios del sistema
- Regla Yara detecta un indicador de ransomwere genérico en el dropper
- Se detectan métodos antisandbox

  Guard pages use detected - possible anti-debugging

  A process attempted to delay the analysis task
- Se envían datos a host remoto desde consola
- Se general ventanas ocultas

- Se detectan conexiones a mas de 512 IP's únicas, mayoritariamente de Rusia y Montenegro
- Se detectan comportamientos del ransomware tipo Cerber
- Ejecuta fichero desde carpeta con sin necesidad de permisos

  C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\LocationNotifications.exe
- Pone puerto en escucha de conexiones entrantes
- Inyecta código en un proceso abierto

  injection: LocationNotifications.exe(2552) -> explorer.exe(2452)
- Crea persistencia mediante registro

  regkey:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\LocationNotifications
  data:"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\LocationNotifications.exe"
  regkey:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\LocationNotifications
  data:"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\LocationNotifications.exe"
  regkey: HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
  data:"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\LocationNotifications.exe"

Análisis de red:

DNS:

Name	***Response***	***Post-Analysis Lookup***
ip-api.com	A 208.95.112.1	208.95.112.1
detectportal.firefox.com	A 34.107.221.82 CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudops.mozgcp.net	34.107.221.82
prod.detectportal.prod.cloudops.mozgcp.net		34.107.221.82
prod.detectportal.prod.cloudops.mozgcp.net	AAAA 2600:1901:0:38d7::	34.107.221.82
example.org	A 93.184.216.34	93.184.216.34
ipv4only.arpa	A 192.0.0.171 A 192.0.0.170	192.0.0.170

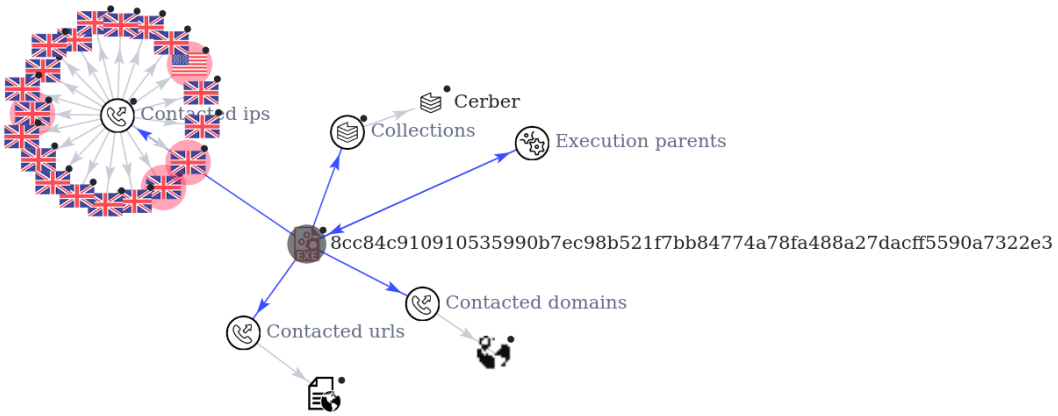
Árbol de proceso:

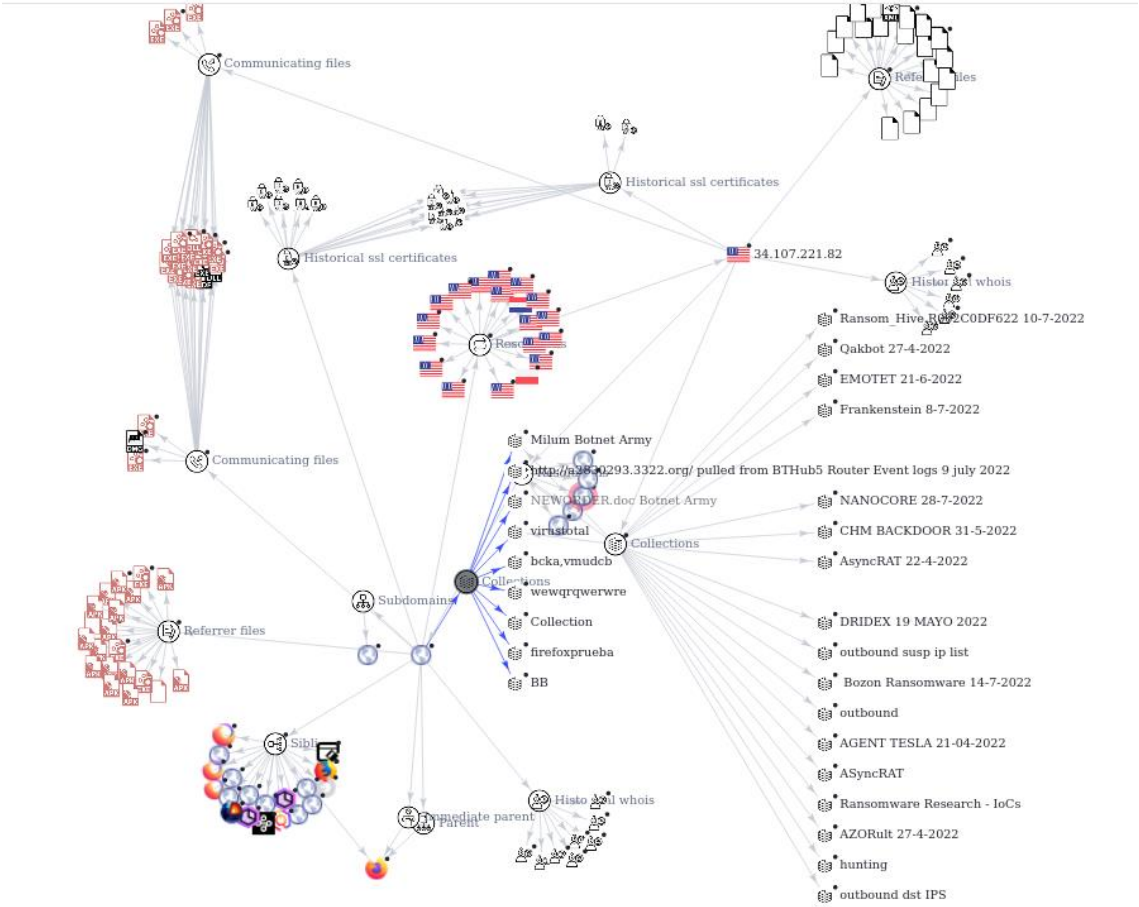
- **8cc84c910910535990b7.exe** 1512
    - **LocationNotifications.exe** 2552
        - **explorer.exe** 2452
        - **explorer.exe** 2892
        - **explorer.exe** 3028
        - **explorer.exe** 2776
        - **explorer.exe** 2448
        - **explorer.exe** 1460
        - **explorer.exe** 980
        - **explorer.exe** 2152
        - **explorer.exe** 1200
        - **explorer.exe** 2024
        - **explorer.exe** 2064
        - **explorer.exe** 2736
    - **cmd.exe** 172 */d /c taskkill /f /im "8cc84c910910535990b7.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7.exe" > NUL*
        - **taskkill.exe** 752 *taskkill /f /im "8cc84c910910535990b7.exe"*
        - **PING.EXE** 2156 *ping -n 1 127.0.0.1*
- **explorer.exe** 2216
    - **firefox.exe** 3904 *-url "C:\Users\ama\Desktop\# DECRYPT MY FILES #.html"*
        - **firefox.exe** 2408 *-url "C:\Users\ama\Desktop\# DECRYPT MY FILES #.html"*
            - **firefox.exe** 228 *-contentproc --channel="2408.0.1968025190\366901585" -parentBuildID 20210310152336 -prefsHandle 1200 -prefMapHandle 1188 -prefsLen 1 -prefMapSize 226965 -appdir "C:\Program Files\Mozilla Firefox\brows ...(truncated)*
    - **firefox.exe** 3780 *-url http://bqyjebfh25oellur.onion.to/F77C-E225-F332-0046-1C91?auto*
        - **firefox.exe** 1860 *-contentproc --channel="3780.0.1140559337\1453368696" -parentBuildID 20210310152336 -prefsHandle 1244 -prefMapHandle 1236 -prefsLen 1 -prefMapSize 236852 -appdir "C:\Program Files\Mozilla Firefox\brow ...(truncated)*

Herramientas online

VirusTotal:

- https://www.virustotal.com/gui/file/8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3/
- Detecciones: 55
- Investigación:





- Vemos conexiones con otros malwares como: AsyncRAT, Emotet, Hive, Bozon y Frankenstein entre otros.
- También vemos conexiones con 2 botnets, Milum y NewOrder, lo que concuerda con las IP's de Rusia y Montenegro.

Polyswarm:

- https://polyswarm.network/scan/results/file/8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3
- No facilita información nueva

Any.run:

- https://app.any.run/tasks/124345c9-f1c7-48fd-80c9-24c5530af909
- Localizamos que conecta con el dominio bqyjebfh25oellur.onion.to

Comportamiento:

Tras el análisis realizado vemos que el malware funciona de la siguiente manera:

- Se trata de un ransomware de la familia Cerber.
- Crea persistencia mediante registros de Windows para arrancar al inicio de sesión.
- Contine varios métodos anti-sandbox
- Roba información del usuario y del sistema
- Crea conexiones con diferentes botnets
- Contacta con una URL .onion
- Encripta los ficheros
- Crea fichero con instrucciones para recuperar los ficheros encriptados

Mitigación

- Borrar registro de persistencia
- Borrar el fichero C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\LocationNotifications.exe
- Recuperar sistema desde un backup

Recomendaciones

- Gestionar permisos para que solo el root pueda crear registros
- Trabajar sin usar usuario root
- Incluir hashes en herramientas de detección