1. CONTEXTO DEL RANSOMWARE AS A SERVICE

Según la pagina oficial de Malwarebytes, definen ransomware “como un tipo de malware que impide a los usuarios accedes a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder a ellos.”

En 1989, fue reconocido el primer ransomware, “AISD (Aids Info Desk)” o “PC CyborgTrojan”, escrito por el Dr. Joseph Popp. El funcionamiento de este software malicioso se trataba de un contador que enumeraba el numero de veces que se había encendido el dispositivo, cuando este contador llega a 90, se cifraban y ocultaban todos los archivos y directorios que se encontraran en la unidad C:, dejando inutilizable el sistema. Para obtener el acceso al dispositivo, el usuario tendría que para 189 dólares a PC Cyborg Corp., en un apartado de Correos en Panamá Popp.

Con la expansión del uso de Internet en los últimos 20 años y la necesidad del teletrabajar que surgió durante la época de pandemia del COVID-19, los grupos de ciberdelincuentes están constantemente creando nuevas variantes de malware.

a. QUE ES EL RAAS

La forma de distribuir malware conocida como “Ransomware as a Service (RaaS) se trata de una variación del modelo de negocio “Software as a Service (SaaS)”. Este plan ofrece a sus clientes, un conjunto de herramientas y servicios desarrollados por los grupos ransomware, con las cuales se pueden llevar a cabo una campaña de ataque sobre un objetivo. Son útiles para clientes que no tienen los conocimientos necesarios o no disponen del tiempo suficiente para desarrollar su programa.

Esta forma de distribuir software permite a los grupos ransomware centrarse especialmente en la terea de desarrollo, ya que los clientes son los que mayormente llevan a cabo los ataques.

b. CUALES SON LOS PRINCIPALES GRUPOS

Los principales grupos de RaaS se pueden definir como las bandas ciberdelincuentes con un mayor número de incidencias o mayor número de beneficios obtenidos gracias a los delitos cometidos.

Observando los principales ataques llevados a cabo entorno a los últimos 10 años, podemos decir que los grupos con mayor importancia respecto a los ataques ransomware son:

LAZARUS GROUP

Grupo de amenazas cibernéticas patrocinado por el estado de Corea del Norte que se ha a la Oficina General de Reconocimiento. Según estudios, ha sido el responsable del ataque realizado en noviembre de 2014 contra la empresa Sony Pictures Entertainment como parte de una campaña denominada “Operation Blockbuster de Novetta”.

WIZARD SPYDER

Grupo de amenazas con sede y patrocinado financieramente en Rusia. Esta agrupación ha desarrollado numerosas herramientas y ha llevado campañas de ataques contra gran variedad de organizaciones.

c. CUALES SON SUS HIDEN SITES EN TOR
d. COMO ACTUAN ESTOS GRUPOS
e. QUÉ HERRAMIENTAS DE CIFRADO USAN Y COMO SON DE EFECTIVAS

LAZARUS GROUP

WannaCry se trata de un ransomware creado por el grupo “Lazarus Group” detectado por primera vez en mayo de 2017 en un ataque global que afecto a más de 150 países.

WannaCry file system activity

STEP	OPERATION	PURPOSE
1	SetSecurityFile	Modify discretionary access control list (DACL) of original document to Full for group Everyone, via the Windows application ICACLS.EXE.
2	CreateFile	Check if encrypted document with ‘.WNCRY’ file extension exists.
3	CreateFile (Generic Read)	Open original document for read only.
4	QueryBasicInformationFile	Record timestamps on original document.
5	ReadFile	Read first 8 bytes of original document.
6	CreateFile (Generic Write)	Create encrypted file with ‘.WNCRYT’ file extension, for write only.
7	WriteFile	Write ‘WANACRY!’ string (8 bytes) in encrypted file.
8	WriteFile	Write 4 bytes, at offset 8 bytes, in encrypted file.
9	WriteFile	Write 256 bytes, at offset 12 bytes, in encrypted file.
10	WriteFile	Write 4 bytes, at offset 268 bytes, in encrypted file.
11	WriteFile	Write 8 bytes, at offset 272 bytes, in encrypted file.
12	ReadFile	Read original document, entirely (0 bytes to EndOfFile).
13	WriteFile	Write encrypted file, entirely, at offset 280 bytes.
14	SetBasicInformationFile	Give encrypted file same timestamps as original document.
15	CloseFile	Close original document.
16	CloseFile	Close encrypted file.
17	SetRenameInformationFile	Change file extension of encrypted file from ‘.WNCRYT’ to ‘.WNCRY’.
18	CreateFile (Generic Write)	Open original document for write only.
20	WriteFile	Write 1,024 bytes (1 KB) in original document. **At offset EndOfFile -1,024 bytes.**
21	FlushBuffersFile	Commit all buffered data to be written to disk.
21	WriteFile (Non-cached)	Write 4,096 bytes (4 KB) in original document, at offset AllocationSize on disk -4,096 bytes.
22	WriteFile	Write in chunks of 262,144 bytes (256 KB) in original document.
23	CloseFile	Close original document, now encrypted file.
24	OpenFile (Read Attributes)	Open encrypted file.
25	SetRenameInformationFile	Rename file to %temp%\<num>.WNCRYT. ReplaceIfExists: True.
26	CloseFile	Close encrypted file.
#	SetDispositionInformationFile	Once all documents on the disk are encrypted, a separate application TASKDL. EXE is run to delete %temp%*.WNCRYT (i.e. all ‘.WNCRYT’ files).

WIZARD SPYDER

Sodinokibi o Conti se trata de un Ransomware-as-a-Service que se detecto por primera vez en diciembre de 2019. Esta implementado a través de TrickBot y se utilizó principalmente contra las principales agencias gubernamentales de América del Norte.

Sodinokibi file system activity

STEP	OPERATION	PURPOSE
1	CreateFile (Generic Read/Write)	Open document for reading and writing.
2	ReadFile	Read data from document.
4	WriteFile	Write encrypted data into document.
5	WriteFile	Add key blob to encrypted document at end of file.
6	CloseFile	Close now encrypted document.
7	CreateFile (Read Attributes)	Open encrypted document.
8	SetRenameInformationFile	Rename document: add '4pqrk340' file extension.
9	CloseFile	Close encrypted document.

f. SISTEMAS DE AFILIADOS

La gran mayoría de grupos Ransomware as a Service proporcionan sus servicios en sus sitios web oficiales, ubicados en Dark Web, un lugar oculto en Internet al cual solo se puede acceder mediante un navegador web especializado (TOR Browser). Dependiendo de la organización, los requisitos para registrarse en el sistema de afiliados son diferentes, algunas solo permiten el acceso a usuarios con habilidades determinadas, en cambio, otras buscan distribuir el malware de forma rápida.

Cabe destacar que cualquier transacción que se realice para obtener un servicio o una comisión, se realizará en criptomonedas disminuyendo la posibilidad de ser detectados.

Estas comunidades proporcionan a sus usuarios escoger 4 formas de suscripción:

- Suscripción mensual a cambio de utilizar el ransomware proporcionado.
- Perteneciendo al sistema de afiliados, en el que además de pagar una suscripción mensual deben aportar una comisión del rescate.
- Suscripción de un ransomware con un solo uso.
- Los usuarios no deben pagar ninguna suscripción, pero deben de aportar una comisión de cada ataque realizado con éxito.

Además, los afiliados tendrán disponible una documentación de incorporación que incluye un tutorial de cómo llevar a cabo un ataque.

g. PUBLICACION DE RANSOMWARE LEAKS

Cada compañía tiene disponible en su Hiden Site un apartado denominado “Ransomware Leaks”, un lugar en el cual se publican todos los ataques que se están llevando a cabo, el porcentaje actual para ser completado, fechas de inicio, archivos que son publicados, ataques exitosos, beneficios obtenidos, rescates pagados…

Se trata de un tablón informativo en el que el grupo hace un resumen para que los afiliados puedan observar de manera rápida el estado de los ataques realizados.

h. QUE TIPO (TAMAÑO, PAÍS, SECTOR) DE EMPRESAS ATACAN

Normalmente los ataques que se realizan a cargo de estas compañías suelen ser a víctimas con cierto prestigio e importancia, consiguiendo gran repercusión a nivel mundial y pidiendo un significativo rescate. Dependiendo del grupo que ejerza la opresión, los objetivos serán diferentes, pero haciendo un resumen se observa que hay ciertos patrones que son comunes.

i. TRIPLE EXTORSIÓN

Las técnicas de extorsión que son utilizadas por estas bandas criminales han ido evolucionando a lo largo del tiempo, mejorando las formas de actuación y los métodos para obtener la mayor cantidad de recursos posible.

Inicialmente, únicamente cifraban los archivos y pedían un pago a cambio de la clave de descifrado. A posteriori de la gran popularización de este modelo de negocio, dependiendo de las filtraciones o las interrupciones que se lleven a cabo se puede hablar de diferentes modelos de extorsión:

- Extorsión única: Se trata de la técnica más antigua de extorsión, en el que las víctimas tienen que pagar una recompensa a cambio de descifrar los archivos.
- Doble extorsión: Como las empresas aumentaron su seguridad y perfeccionaron sus copias de seguridad, podían establecer cualquier sistema y tenerlo operativo en cuestión de tiempo, por lo que los grupos criminales empezaron a amenazar con difundir o divulgar cualquier información obtenida.
- Triple extorsión: Si las empresas no tienen ninguna preocupación sobre la filtración de sus datos, los grupos ransomware utilizan negación de servicios para sobrecargar un servidor o red con tráfico y dejarlo inoperativo.
- Cuádruple extorsión: Una vez comenzado un ataque ransomware, las bandas se ponen en contacto con los usuarios más influyentes en la empresa o principales clientes, creando una gran situación de estrés y presión.
- Extorsión quíntuple: Intimidan y presionan a las empresas con vender información confidencial a competidores o usuarios interesados en la víctima.

2. INVESTIGACION
    a. ENTORNO CONTROLADO DE TRABAJO

Antes de ejecutar cualquier tipo de análisis a una muestra malware, es necesario un entorno de trabajo seguro y controlado. Se utilizará la ayuda de maquinas virtualizadas en un dispositivo anfitrión que será configurada de una manera determinada dependiendo del análisis que se quiera realizar en cada momento.

La virtualización se llevará a cabo con el software “VirtualBox”, “una potente herramienta de uso empresarial y doméstico, rico en funciones y de alto rendimiento para clientes empresariales. Además, se trata de la única solución profesional que está disponible de manera gratuita como software de código abierto bajo los términos de la licencia publica general GNU (GLP) versión 2”. E in

https://www.virtualbox.org/

El sistema operativo que utilizado para montar la máquina virtual será “IE11 on Windows7 (x86)”, obtenido de la pagina oficial de desarrollo de Microsoft, que software gratuito con un limite de uso de 90 días.

https://developer.microsoft.com/es-es/microsoft-edge/tools/vms/

Una vez creado correctamente el servicio virtualizado, se debe configurar la maquina con las herramientas para llevar a cabo los análisis estáticos y dinámicos de ejemplares ransomware.

Primero será necesario instalar un navegador web actualizado, Mozilla Firefox o Google Chrome. Un navegador que define Google, la empresa creadora, como “sencillo, seguro y rápido”.

Por otra parte, instalaremos el navegador TOR Browser, un navegador que protege la privacidad de los usuarios y mejora la seguridad online.

b. MUESTRAS: PLATAFORMAS VIRUSTOTAL, ANYRUN

https://es.malwarebytes.com/ransomware/

https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

https://asianssr.org/index.php/ajct/article/view/55/37

https://attack.mitre.org/groups/

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sophos.com/de-de/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcyber.mitre.org/wp-content/uploads/2021/08/Ransomware-Paper-V2.pdf

https://asianssr.org/index.php/ajct/article/view/55/37

https://medium.com/picus-security/three-key-ransomware-trends-in-2022-raas-multiple-extortion-and-iabs-340953f7bca9