

Файл лога: Logfile_4.PML

Цель: Найти вредоносный процесс, исследовать его вредоносную активность и разработать систему его обнаружения.

Инструменты: procmom, python (для дампа путей и сетевых адресов)

Результаты анализа

Имя вредоносного ПО: %USERPROFILE%\Desktop\keygen.exe

Назначение вредоносного ПО: программа-вымогатель, которая шифрует пользовательские данные и отключает восстановление

Тип вредоносного ПО: Ransomware

PID вредоносного процесса в файле лога: 2312

Механизм обеспечения поддержания заражения: программное поддержание отсутствует

Предполагаемая схема работы вредоносного ПО:

Этап 0: Социальная инженерия: имя файла указывает на то, что файл нужен, например, для обхода лицензионной защиты. Пользователь, влекомый выгодой, мог сознательно отключить антивирусное ПО и запустить программу от имени администратора. Таким образом у системы не осталось средств защиты.

Запуск ПО (keygen.exe)

cmd.exe

vssadmin.exe Delete Shadows /All /Quiet (Удаление теневых копий Windows)

bcdedit /set {default} recoveryenabled No (Отключение среды восстановления)

RegSetValue (Запись рабочих данных в реестр)

Путь: HKCU\Software\recfg

Данные: Криптографические ключи (pk_key, sk_key), уникальное расширение для шифрования (.1c67b99), статистика.

ReadFile (Активное рекурсивное сканирование файловой системы)

Поиск пользовательских данных для дальнейшего шифрования

WriteFile (шифрование пользовательских данных)

SetRenameInformationFile (добавление расширения .1c67b99)

Создание файлов 1c67b99-readme.txt с требованием выкупа

Создание oe05b91h5s.bmp в AppData\Local\Temp\

Предположительно изображение с требованием выкупа

Изменяет ключ реестра HKCU\Control Panel\Desktop\Wallpaper, устанавливая созданное изображение как обои рабочего стола

Устанавливает свой корневой сертификат в HKCU\Software\Microsoft\SystemCertificates\CA\Certificates\ компрометируя будущие HTTPS-соединения.

Устанавливает сотни TCP Connect-соединений с десятками серверов по всему миру (использует порт 443 для маскировки под HTTPS).

TCP Send (Отправляет небольшие пакеты данных на сервер, к которому удалось подключиться)

Предположительно передача ID жертвы и уникального приватного ключа.

Обоснование вредоносности: отключение неизвестным приложением среды восстановления и удаление теневых бэкапов само по себе вредоносно. Более того установка корневого сертификата для распространения по сети довольно опасна. Легитимная программа не будет массово переименовывать пользовательские файлы абсолютно разных расширений. Также установка изображения без осмысленного названия из %Temp% в качестве обоев является вишенкой на торте.

Объяснения механизма самозащиты после перезагрузки: шифровальщики шифруют данные асимметричным шифрованием за счет чего расшифровка и поиск ключа в файлах становится практически невозможным. Зашифрованные данные не расшифровываются после перезагрузки. Программа-вымогатель создает в папках с зашифрованными данными файлы readme, которые напоминают о том, где и как получить ключ расшифровки. Помимо этого обои, установленные вымогателем, скорее всего также содержат напоминание о том, что была атака и о том, что требуется заплатить. Таким образом ransomware не нужно оставаться запущенным после перезагрузки.

Рекорда 1:

MNA – Malware network activity

MCA – Malware cmd activity

EUF – Encrypting user files

RUF – Renaming user files

MRV – Malware Regedit Values

WUI – Writing user instructions

Если (TCP Connect или TCP Send или TCP Receive хотя бы по 3 адресам из примечания 1), то MNA = True

Если (запуск cmd с аргументами vssadmin.exe Delete Shadows /All /Quiet или bcdedit /set {default} recoveryenabled) MCA = True

Если (WriteFile с именем 1c67b99-readme.txt), то WUI = True

Если (SetRegValue с путем, содержащим HKCU\Software\recfg), то MRV = True

Если (SetRenameInformationFile на файлы с пользовательским расширением), то RUF = True

Если (WriteFile к файлам с пользовательским расширением), то EUF = True

Если (MNA или (MCA и (EUF или RUF или MRV или WUI)) или (EUF и MRV и WUI) или (MCA и RUF)) Детект()

Если ((EUF и RUF) или WUI или (MRV и (EUF или RUF))) Подозрение() //Отправка отчета SOC

Семейство вредоноса: Деструктивный (агрессивно удаляющий записи для восстановления) шифровальщик без механизма персистентности с сетевой коммуникацией.

Рекорда 2:

DB – Destroying backups = False

DRM – Disabling recovery mode = False

File_encryption_counter = 0

File_renaming_counter = 0

Readme_counter = 0

Unknown_cmd_runner = 0

Проверка_дерева() { //0, если безвредно, 1 опасно

 Если (процесс неизвестен <MD5 и SHA-256 нет в базе> и родителя нет)
 вернуть 1 //Значит пустили как exe

 Если (процесс неизвестен и есть родитель) Проверка_дерева(родитель)

 Если (процесс известен)

 Если совпали хэши – вернуть 0

 Не совпал хоть один – вернуть 1

}

Если (запуск cmd) Проверка_дерева(процесс)

 Если (опасно) Unknown_cmd_runner = 1

Если (запуск cmd с аргументом "vssadmin" и "Delete Shadows"), то DB = True

Если (запуск cmd с аргументом "bcdedit" и "recoveryenabled No"), то DRM = True

Если (WriteFile к файлам с пользовательским расширением), то
File_encryption_counter += 1

Если (SetRenameInformationFile на файлы с пользовательским расширением), то
File_renaming_counter += 1

Если (WriteFile с именем, похожим шаблон из Примечания 2), то Readme_counter
+= 1

Malware_points = 0

Если (Unknown_cmd_runner), то Malware_points + 49

Если (DB == True), то Malware_points += 50

Если (DRM == True), то Malware_points += 30

Если (File_encryption_counter > 20), то Malware_points += 25

Если (File_renaming_counter > 20), то Malware_points += 20

Если (Readme_counter > 0), то Malware_points += 40

Если (Malware_points >= 90), то

 Детект() // Высокая уверенность

Иначе Если (Malware_points >= 50), то

 Подозрение() // Средняя уверенность, отчет в SOC

Примечание 1: (список адресов сетевого подключения нашего ransomware)

95-165-137-165.static.spd-mgts.ru:https
s007.cyon.net:https
192.237.192.175:https
ing.r1.websupport.sk:https
webhosting-cluster.transip.nl:https
11.56.157.185.anleggsregister.agnitio.no:https
158.25.214.35.bc.googleusercontent.com:https
82.94.246.8:https
ec2-52-11-37-152.us-west-2.compute.amazonaws.com:https
104.24.103.93:https
cl01.hiperactive.net:https
vh33.sweb.ru:https
104.247.81.13:https
163-172-24-64.rev.poneytelecom.eu:https
192-254-186-190.unifiedlayer.com:https
server.publiccompserver.de:https
217-160-0-208.elastic-ssl.ui-r.com:https
ip-160-153-131-189.ip.secureserver.net:https
ti-01.overtheweb.nl:https
51-15-159-75.rev.poneytelecom.eu:https
217-160-0-18.elastic-ssl.ui-r.com:https
box2262.bluehost.com:https
www4.servers58.com:https
104.18.60.24:https
s23.internetwerk.de:https
s9.gestiondeservidor.com:https
domainparking.ru:https
a64c2b794233c60a6.awsglobalaccelerator.com:https
chah.savviihq.com:https
217-160-0-84.elastic-ssl.ui-r.com:https
64.70.194.103:https
ns2.hostdown.es:https
67.227.226.240:https
172.67.138.91:https
host5.server.ae:https
103-23-22-248.isi.cloud.id:https
2040.wp.34sp.com:https
hm8202.locaweb.com.br:https
37.202.7.169:https

vh251.sweb.ru:https
102.122.185.35.bc.googleusercontent.com:https
server01.platzer-werbung.de:https
box5503.bluehost.com:https
vps228.keurigonline.nl:https
dedi3486.your-server.de:https
ec2-52-14-1-58.us-east-2.compute.amazonaws.com:https
82-214-136-24.itsa.net.pl:https
www.irizar.com:https
s215.webhostingserver.nl:https
box398.bluehost.com:https
csaballoons.com:https
172.67.129.195:https
ec2-3-125-197-172.eu-central-1.compute.amazonaws.com:https
web11.mydevil.net:https
indaix-poseidon.de:https
ns3146141.ip-51-89-7.eu:https
a23-37-124-8.deploy.static.akamaitechnologies.com:http
218.78.209.35.bc.googleusercontent.com:https
972953.vps-10.com:https
82.62.209.35.bc.googleusercontent.com:https
67.225.188.83:https
gators.ru:https
176.126.61.245.sky-net.com.ua:https
154.71.185.35.bc.googleusercontent.com:https
45.60.22.109:https
web2.atznet.dk:https
box5556.bluehost.com:https
trillian.ispgateway.de:https
srv1.ikmagazine.nl:https
ns527890.ip-192-99-7.net:https
premium76-1.web-hosting.com:https
ip-184-168-131-241.ip.secureserver.net:https
web-f588402d.lsh.hostnet.nl:https
53.151.233.35.bc.googleusercontent.com:https
ip-166-62-108-43.ip.secureserver.net:https
world-319.fr.planethoster.net:https
res5.mijnplesk.com:https
li1485-84.members.linode.com:https
revo2.w3b.it:https

104.27.187.170:https
ec2-100-21-184-71.us-west-2.compute.amazonaws.com:https
180.136.102.34.bc.googleusercontent.com:https
104.28.12.75:https
oliver.exonhost.com:https
172.67.142.212:https
ns.forextimes.ru:https
server18.hostwhitelabel.com:https
217-160-0-87.elastic-ssl.ui-r.com:https
titan.geekstorage.com:https
ip118.ip-54-36-201.eu:https
239.211.214.35.bc.googleusercontent.com:https
earth.verasoni.com:https
cluster028.hosting.ovh.net:https
134.119.88.129:https
104.27.173.109:https
s51-www.ogicom.net:https
hd1.sitew.com:https
167.99.54.169:https
eden6.ncsrv.de:https
linux57.unoeuro.com:https
199.16.172.213:https
5.180.185.169:https
80.240.20.142.vultr.com:https
ip-160-153-133-193.ip.secureserver.net:https
ec2-3-88-95-32.compute-1.amazonaws.com:https
217-160-0-92.elastic-ssl.ui-r.com:https
ip-166-62-110-213.ip.secureserver.net:https
inspot-srv1.oderland.com:https
dedi3093545.eu.raiolanetworks.com:https
chi108.greengeeks.net:https
217-160-0-237.elastic-ssl.ui-r.com:https
lrv1.globehosting.net:https
172.67.196.62:https
172.67.158.193:https
cyberfarm.dotserv.com:https
box5121.bluehost.com:https
vwp7696.webpack.hosteurope.de:https
172.67.207.210:https
101.99.77.144:https

dedi642.your-server.de:https
204.11.56.48:https
web410.default-host.net:https
67.225.161.117:https
static-148-95-24-46.ipcom.comunitel.net:https
server67.hosting.reg.ru:https
23.185.0.2:https
ec2-35-170-173-134.compute-1.amazonaws.com:https
serve.versacreative.com:https
92.204.68.14:https
wpiix5-2.rumahweb.com:https
154.86.216.242:https
crt.sectigo.com:http
linux33.unoeuro.com:https
2.103.209.35.bc.googleusercontent.com:https
soccmel.sgwebitaly.it:https
104.18.10.5:https
ec2-34-237-37-253.compute-1.amazonaws.com:https
tux419.loginserver.ch:https
104.31.76.205:https
box5551.bluehost.com:https

Примечание 2: (список шаблонов имен сообщений шантажиста)

readme.*
read_me.*
decrypt.*
recover.*
restore.*
unlock.*
help.*
instruction.*
info.*
note.*
message.*
locked.*
encrypted.*
crypted.*
_key.
*_id
_files.
how_to.*

