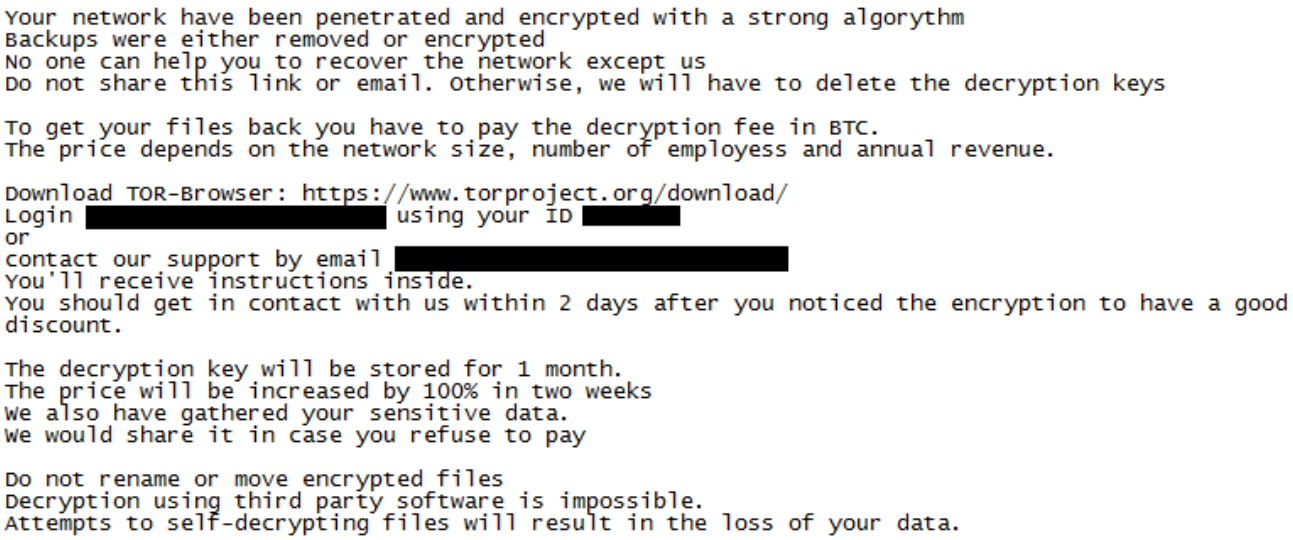
Pažnja: Novi opasni ransomware pwndLocker i u Srbiji, napadnut Novi Sad!

Published: 2020-03-02 · Archived: 2026-04-05 12:54:03 UTC

Otkriven je novi ransomware koji je mesecima delovao daleko od javnosti. Pretnja je globalna, napadnute su organizacije širom sveta, tako da treba biti oprezan i ažurirati definicije AV rešenja. Napadači određuju cenu otkupnine u zavisnosti od veličine mreže, broja zaposlenih i godišnjih prihoda. Posle napada na gradove u SAD-u, saznajemo da je napadnut i jedan grad u Srbiji!

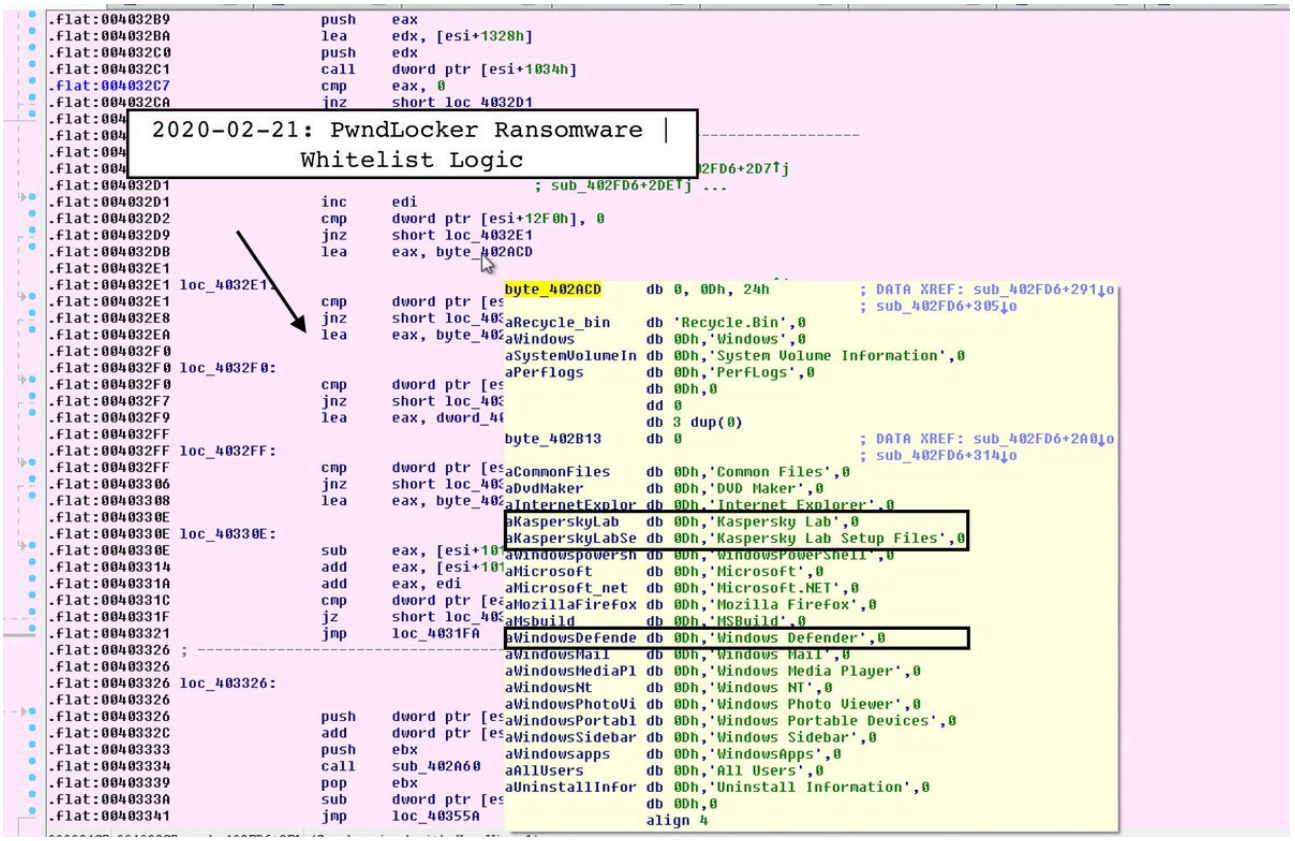


Slika 1. Poruka o otkupnini, pwndLocker. Izvor slike: MalwareHunterTeam.

U poruci o otkupnini, napadači navode da će dekriptor čuvati mesec dana i apeluju na žrtve da im se jave u roku od dva dana kako bi dobili "popust". Takođe, posle 2 nedelje cena se duplira. Još jedna pretnja žrtvama je da će osetljive informacije koje su prikupili iz mreže organizacije pustiti u javnost.

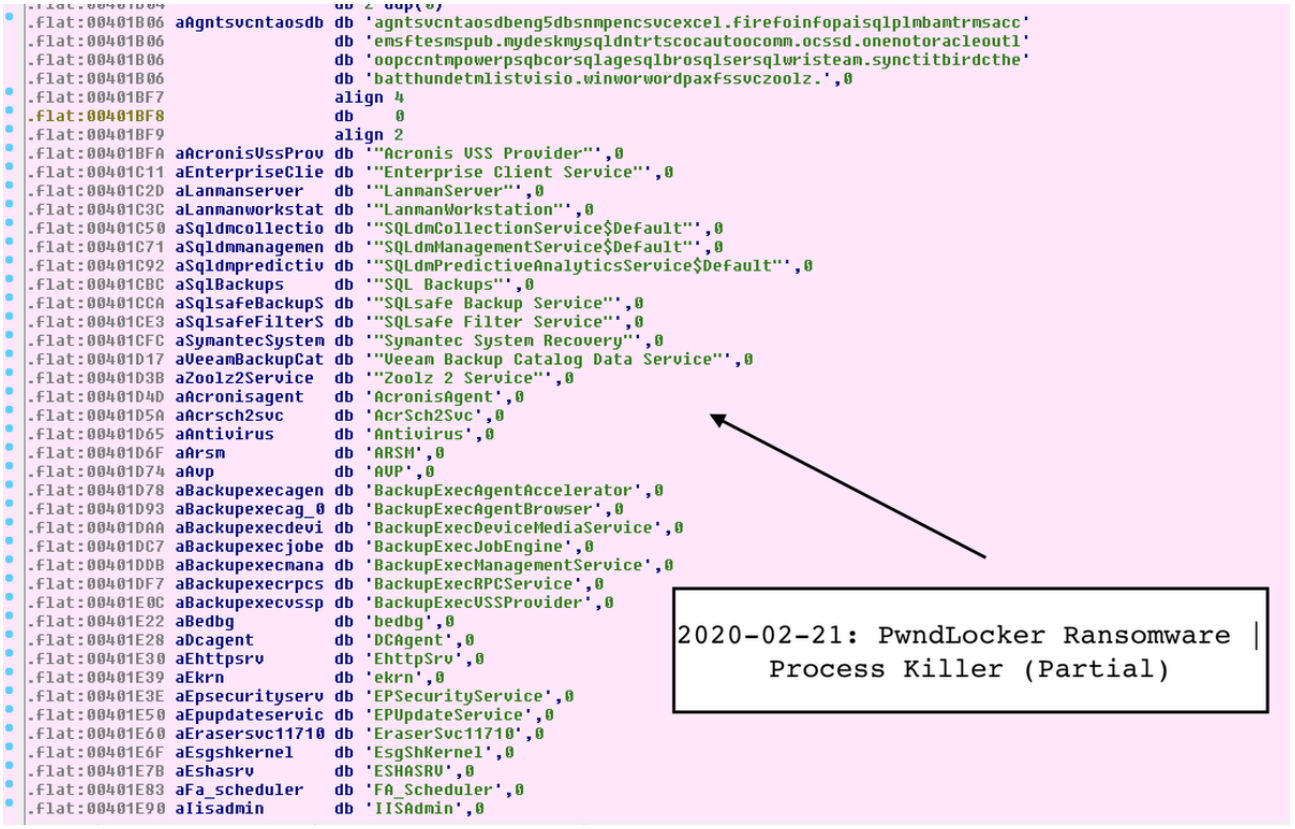
Ovaj ransomware, pored toga što zaključava podatke, pokušava da obriše i Shadow kopije i da "ubije" procese i servise AV rešenja. Prema prvim informacijama, najverovatnije se radi o ciljanom ransomwaru koji napada tzv. "high-value" mete.

Tehničke detalje možete videti na slikama ispod, autor je Vitali Kremez:

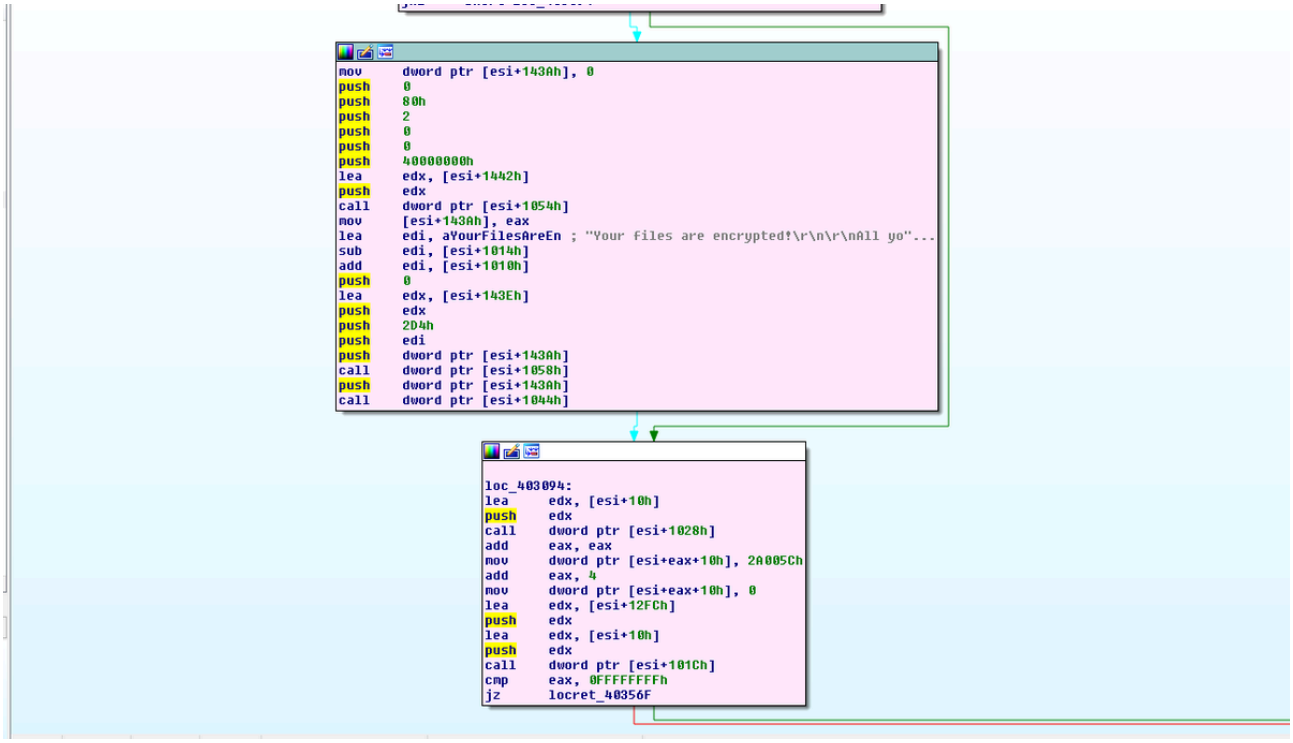


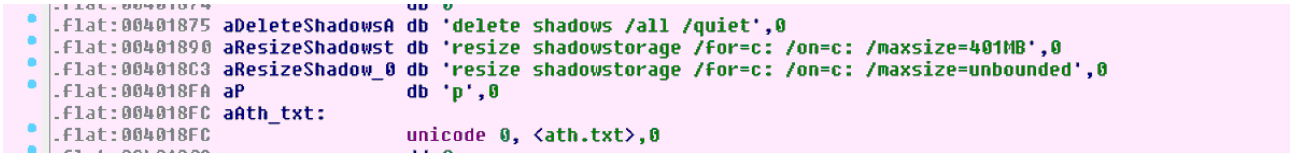

```
.flat:004032B9                push    eax
.flat:004032BA                lea     edx, [esi+1328h]
.flat:004032C0                push    edx
.flat:004032C1                call    dword ptr [esi+1034h]
.flat:004032C7                cmp     eax, 0
.flat:004032CA                jnz     short loc_4032D1
.flat:004032D1                inc     edi
.flat:004032D2                cmp     dword ptr [esi+12F0h], 0
.flat:004032D9                jnz     short loc_4032E1
.flat:004032DB                lea     eax, byte_402ACD
.flat:004032E1
.flat:004032E1 loc_4032E1:
.flat:004032E1                cmp     dword ptr [es
.flat:004032E8                jnz     short loc_40
.flat:004032EA                lea     eax, byte_40
.flat:004032F0
.flat:004032F0 loc_4032F0:
.flat:004032F0                cmp     dword ptr [es
.flat:004032F7                jnz     short loc_40
.flat:004032F9                lea     eax, dword_4
.flat:004032FF
.flat:004032FF loc_4032FF:
.flat:004032FF                cmp     dword ptr [es
.flat:00403306                jnz     short loc_40
.flat:00403308                lea     eax, byte_40
.flat:0040330E
.flat:0040330E loc_40330E:
.flat:0040330E                sub     eax, [esi+10
.flat:00403314                add     eax, [esi+10
.flat:0040331A                add     eax, edi
.flat:0040331C                cmp     dword ptr [es
.flat:0040331F                jz      short loc_40
.flat:00403321                jmp     loc_4031FA
.flat:00403326 ; ---------------------------------------
.flat:00403326
.flat:00403326 loc_403326:
.flat:00403326
.flat:00403326                push    dword ptr [es
.flat:0040332C                add     dword ptr [es
.flat:00403333                push    ebx
.flat:00403334                call    sub_402A60
.flat:00403339                pop     ebx
.flat:0040333A                sub     dword ptr [es
.flat:00403341                jmp     loc_40355A
```

```
                                ; sub_402FD6+2D7↑j
                                ; sub_402FD6+2DE↑j ...
byte_402ACD     db 0, 0Dh, 24h          ; DATA XREF: sub_402FD6+291↓o
                                        ; sub_402FD6+305↓o
aRecycle_bin    db 'Recycle.Bin',0
aWindows        db 0Dh,'Windows',0
aSystemVolumeIn db 0Dh,'System Volume Information',0
aPerflogs       db 0Dh,'PerfLogs',0
                db 0Dh,0
                dd 0
                db 3 dup(0)
byte_402B13     db 0                    ; DATA XREF: sub_402FD6+2A0↓o
                                        ; sub_402FD6+314↓o
aCommonFiles    db 0Dh,'Common Files',0
aDvdMaker       db 0Dh,'DVD Maker',0
aInternetExplor db 0Dh,'Internet Explorer',0
aKasperskyLab   db 0Dh,'Kaspersky Lab',0
aKasperskyLabSe db 0Dh,'Kaspersky Lab Setup Files',0
aWindowspowersh db 0Dh,'WindowsPowerShell',0
aMicrosoft      db 0Dh,'Microsoft',0
aMicrosoft_net  db 0Dh,'Microsoft.NET',0
aMozillaFirefox db 0Dh,'Mozilla Firefox',0
aMsbuild        db 0Dh,'MSBuild',0
aWindowsDefende db 0Dh,'Windows Defender',0
aWindowsMail    db 0Dh,'Windows Mail',0
aWindowsMediaPl db 0Dh,'Windows Media Player',0
aWindowsNt      db 0Dh,'Windows NT',0
aWindowsPhotoVi db 0Dh,'Windows Photo Viewer',0
aWindowsPortabl db 0Dh,'Windows Portable Devices',0
aWindowsSidebar db 0Dh,'Windows Sidebar',0
aWindowsapps    db 0Dh,'WindowsApps',0
aAllUsers       db 0Dh,'All Users',0
aUninstallInfor db 0Dh,'Uninstall Information',0
                db 0Dh,0
                align 4
```




```
.flat:00401B06 aAgntsvcntaosdb db 'agntsvcntaosdbeng5dbsnmpencsvcexcel.firefoinfopaisqlplmbamtrmsacc'
.flat:00401B06                 db 'emsftesmspub.mydeskmysqldntrtscocautoocomm.ocssd.onenotoracleout1'
.flat:00401B06                 db 'oopccntmpowerpsqbcorsqlagesqlbrosqlsersqlwristeam.synctitbirdcthe'
.flat:00401B06                 db 'batthundetmlistvisio.winworwordpaxfssvczoolz.',0
.flat:00401BF7                 align 4
.flat:00401BF8                 db    0
.flat:00401BF9                 align 2
.flat:00401BFA aAcronisVssProv db '"Acronis VSS Provider"',0
.flat:00401C11 aEnterpriseClie db '"Enterprise Client Service"',0
.flat:00401C2D aLanmanserver   db '"LanmanServer"',0
.flat:00401C3C aLanmanworkstat db '"LanmanWorkstation"',0
.flat:00401C50 aSqldmcollectio db '"SQLdmCollectionService$Default"',0
.flat:00401C71 aSqldmmanagemen db '"SQLdmManagementService$Default"',0
.flat:00401C92 aSqldmpredictiv db '"SQLdmPredictiveAnalyticsService$Default"',0
.flat:00401CBC aSqlBackups     db '"SQL Backups"',0
.flat:00401CCA aSqlsafeBackupS db '"SQLsafe Backup Service"',0
.flat:00401CE3 aSqlsafeFilterS db '"SQLsafe Filter Service"',0
.flat:00401CFC aSymantecSystem db '"Symantec System Recovery"',0
.flat:00401D17 aVeeamBackupCat db '"Veeam Backup Catalog Data Service"',0
.flat:00401D3B aZoolz2Service  db '"Zoolz 2 Service"',0
.flat:00401D4D aAcronisagent   db 'AcronisAgent',0
.flat:00401D5A aAcrsch2svc     db 'AcrSch2Svc',0
.flat:00401D65 aAntivirus      db 'Antivirus',0
.flat:00401D6F aArsm           db 'ARSM',0
.flat:00401D74 aAvp            db 'AVP',0
.flat:00401D78 aBackupexecagen db 'BackupExecAgentAccelerator',0
.flat:00401D93 aBackupexecag_0 db 'BackupExecAgentBrowser',0
.flat:00401DAA aBackupexecdevi db 'BackupExecDeviceMediaService',0
.flat:00401DC7 aBackupexecjobe db 'BackupExecJobEngine',0
.flat:00401DDB aBackupexecmana db 'BackupExecManagementService',0
.flat:00401DF7 aBackupexecrpcs db 'BackupExecRPCService',0
.flat:00401E0C aBackupexecvssp db 'BackupExecVSSProvider',0
.flat:00401E22 aBedbg          db 'bedbg',0
.flat:00401E28 aDcagent        db 'DCAgent',0
.flat:00401E30 aEhttpsrv       db 'EhttpSrv',0
.flat:00401E39 aEkrn           db 'ekrn',0
.flat:00401E3E aEpsecurityserv db 'EPSecurityService',0
.flat:00401E50 aEpupdateservic db 'EPUpdateService',0
.flat:00401E60 aEraserSvc11710 db 'EraserSvc11710',0
.flat:00401E6F aEsgshkernel    db 'EsgShKernel',0
.flat:00401E7B aEshasrv        db 'ESHASRV',0
.flat:00401E83 aFa_scheduler   db 'FA_Scheduler',0
.flat:00401E90 aIisadmin       db 'IISAdmin',0
```





Symantec ga detektuje kao **ML.Attribute.HighConfidence** Trojan Horse, a Fortinet kao **W32/AntiAV!tr**.

Update

Potvrđeno je da je u pitanju napad na **Novi Sad**, što je preneo i portal 021. Tokom vikenda kriptovani su serveri gradskih uprava i nekoliko drugih javnih službi preko JKP Informatika. Gradske kamere trenutno ne funkcionišu, a zaposlenima u gradskim službama rečeno je da ne mogu da pristupe svojim mejlovima.

Novi Sad odbio da plati napadačima - 04.03.2020.

Kako prenosi portal 021, gradska uprava Novog Sada neće platiti otkupninu. Napadači su prvobitno tražili 50 BTC (oko €400.000), a kasnije spustili cifru na 20 BTC. S obzirom na to da je i backup zaražen virusom, odnosno zaključan, Novi Sad će ostati bez svih kriptovanih podataka. Nije saopšteno šta je sve nestalo i koje su razmere napada. Gradonačelnik Novog Sada Miloš Vučević je izjavio da je upad u sistem izvršen preko emaila.

Napadi u SAD-u

Prema pisanju portala Bleeping Computer, pwndLocker targetira velike kompanije i lokalnu (javnu) upravu. Ovaj ransomware se pojavio u drugoj polovini 2019, a iznosi koje zahtevaju od svojih žrtava kreću se od $175.000 do $660.000 (isplata se vrši u Bitcoin kripto valuti). Još uvek nije poznato da li je neko od žrtava pristao da plati otkupninu.

Jedan od uspešnih napada ove grupe izvršen je na Lasalle County u državi Ilinois, a za dekriptor traže 50 BTC ($442.000). Tvrde i da su pre zaključavanja najpre izvukli sve podatke sa mreže, ali za to nisu pružili dokaz. Lasalle County ne planira da plati.

PwndLocker Ransomware

PwndLocker pokušava da isključi nekoliko Windows servisa preko 'net stop' komande kako bi mogao da kriptuje podatke. Neke od aplikacija čije servise "gađa" su: Veeam, Microsoft SQL Server, MySQL, Exchange, Acronis, Zoolz, Backup Exec, Oracle, Internet Information Server (IIS), ali i AV rešenja Kaspersky, Malwarebytes, Sophos i McAfee. Takođe, na meti su i različiti procesi koje pokušava da prekine - Firefox, Word, Excel, Access i druge procese vezane za bezbednosna rešenja, backup i database servere.

Zatim pomoću sledećih komandi "čisti" Shadow Volume kopije kako ne žrtva ne bi mogla da vrati fajlove:

> vssadmin.exe delete shadows /all /quiet
>
> vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB
>
> vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=unbounded

Kada izvrše sve pripreme, PwndLocker kreće da zaključava računare, ali preskače fajlove sa sledećim ekstenzijama:

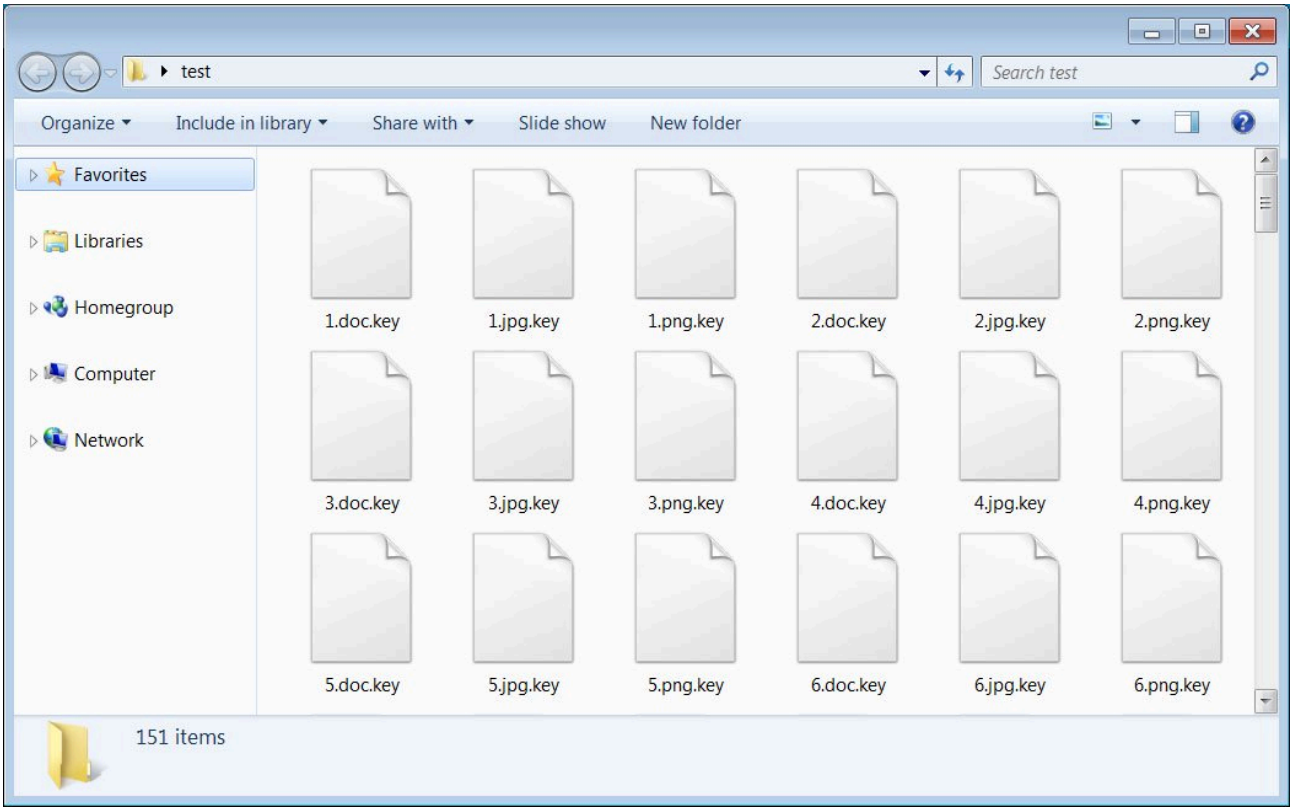
> .exe, .dll, .lnk, .ico, .ini, .msi, .chm, .sys, .hlf, .lng, .inf, .ttf, .cmd, .bat, .vhd, .bac, .bak, .wbc, .bkf, .set, .win, .dsk

Takođe, preskače i sve fajlove na sledećim lokacijama (folderima):

> $Recycle.Bin
>
> Windows
>
> System Volume Information
>
> PerfLogs
>
> Common Files
>
> DVD Maker
>
> Internet Explorer
>
> Kaspersky Lab
>
> Kaspersky Lab Setup Files
>
> WindowsPowerShell
>
> Microsoft

> Microsoft.NET
>
> Mozilla Firefox
>
> MSBuild
>
> Windows Defender
>
> Windows Mail
>
> Windows Media Player
>
> Windows NT
>
> Windows Photo Viewer
>
> Windows Portable Devices
>
> Windows Sidebar
>
> WindowsApps
>
> All Users
>
> Uninstall Information
>
> Microsoft
>
> Adobe
>
> Microsoft
>
> Microsoft_Corporation
>
> Packages
>
> Temp

MalwareHunterTeam je primetio da u zavisnosti od žrtve, zaključani fajlovi dobijaju ekstenzije **.key** ili **.pwnd**. Uzorak koji je Bleeping Computer analizirao ima .key ekstenziju, što se vidi na slici ispod:



Slika 6. Fajlovi koje je kriptovao pwndLocker. Izvor slike: Bleeping Computer.

Kada završe proces enkripcije podataka, na više lokacija (uključujući i desktop) ostavljaju tekstualni fajl, odnosno poruku o otkupnini sa nazivom **H0w_T0_Rec0very_Files.txt**, a kao dokaz da će dekriptor raditi, nude da besplatno otključaju do 2 fajla.
