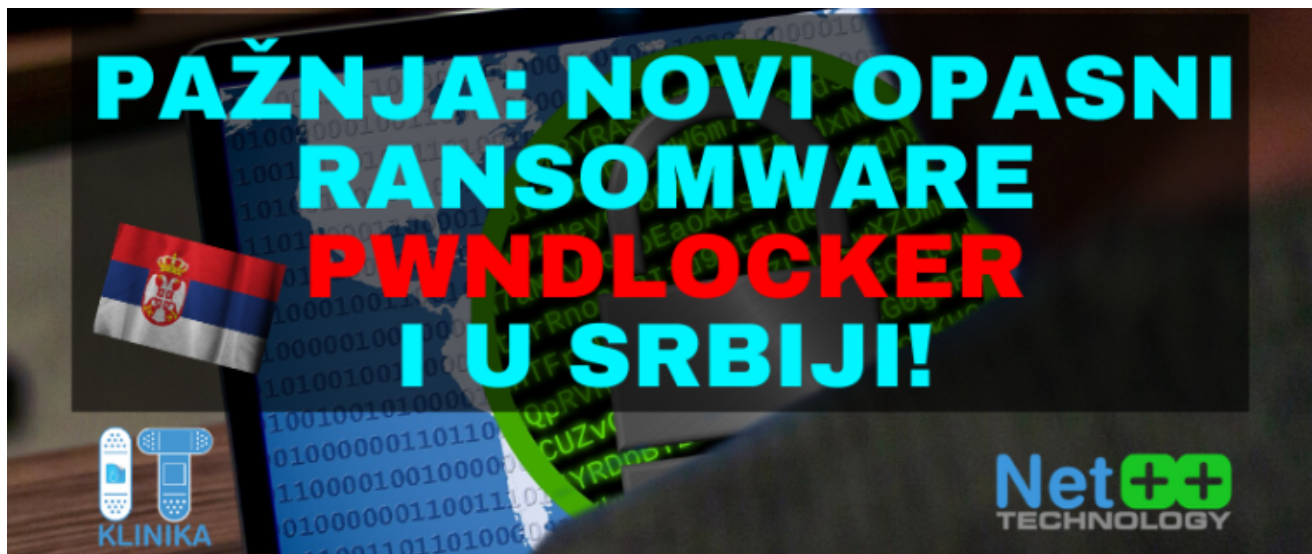


Pažnja: Novi opasni ransomware pwndLocker i u Srbiji, napadnut Novi Sad!

it-klinika.rs/blog/paznja-novi-opasni-ransomware-pwndlocker-i-u-srbiji



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!

```
Your network have been penetrated and encrypted with a strong alorythm  
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.
```

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:004032BB      push    edx
.Flat:004032BC      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      loc_4032E1:  cmp    dword ptr [esi+12F0h], byte_402ACD
.Flat:004032E1      jnz    short loc_4032E8
.Flat:004032E8      lea    eax, byte_402ACD
.Flat:004032F0      loc_4032F0:  cmp    dword ptr [esi+12F0h], aRecycle_bin
.Flat:004032F0      jnz    short loc_4032F7
.Flat:004032F7      lea    eax, dword_402B13
.Flat:004032FF      loc_4032FF:  cmp    dword ptr [esi+12F0h], aWindows
.Flat:00403306      jnz    short loc_40330E
.Flat:00403308      lea    eax, byte_402ACD
.Flat:0040330E      loc_40330E:  sub    eax, [esi+1034h]
.Flat:00403314      add    eax, [esi+1034h]
.Flat:0040331A      add    eax, edi
.Flat:0040331C      cmp    dword ptr [esi+1034h], aMicrosoft
.Flat:0040331F      jz     short loc_403326
.Flat:00403321      jmp    loc_4031FA
.Flat:00403326      ; aKasperskyLab
.Flat:00403326      loc_403326:  push  dword ptr [esi+1034h]
.Flat:0040332C      add    dword ptr [esi+1034h], aWindows
.Flat:00403333      push  ebx
.Flat:00403334      call  sub_402A60
.Flat:00403339      pop   ebx
.Flat:0040333A      sub   dword ptr [esi+1034h], aAllUsers
.Flat:00403341      jmp   loc_40355A
```

aRecycle_bin	db	'Recycle.Bin',0
aWindows	db	00h,'Windows',0
aSystemVolumeIn	db	00h,'System Volume Information',0
aPerflogs	db	00h,'PerfLogs',0
byte_402B13	db	0
aCommonFiles	db	00h,'Common Files',0
aDvdMaker	db	00h,'DVD Maker',0
aInternetExplor	db	00h,'Internet Explorer',0
aKasperskyLab	db	00h,'Kaspersky Lab',0
aKasperskyLabSe	db	00h,'Kaspersky Lab Setup Files',0
aWindowspowersh	db	00h,'WindowsPowerShell',0
aMicrosoft	db	00h,'Microsoft',0
aMicrosoft_net	db	00h,'Microsoft.NET',0
aMozillaFireFox	db	00h,'Mozilla Firefox',0
aMSBuild	db	00h,'MSBuild',0
aWindowsDefende	db	00h,'Windows Defender',0
aWindowsMail	db	00h,'Windows Mail',0
aWindowsMediaPl	db	00h,'Windows Media Player',0
aWindowsNt	db	00h,'Windows NT',0
aWindowsPhotoVi	db	00h,'Windows Photo Viewer',0
aWindowsPortabl	db	00h,'Windows Portable Devices',0
aWindowsSidebar	db	00h,'Windows Sidebar',0
aWindowsapps	db	00h,'WindowsApps',0
aUninstallInfor	db	00h,'Uninstall Information',0

2020-02-21: PwndLocker Ransomware | Whitelist Logic

```

.flat:00401806 aAgntsvcntaosdb db 'agntsvcntaosdbeng5dbsnmpencsvexcel.firefoinfopaisqlplmbamtrmsacc'
.flat:00401806 db 'emsfteemspub.mydeskmysqldntrtsccocautocomm.occsd.onenotoracleoutl'
.flat:00401806 db 'oopccntmpowerpsqbcorsqlagesqlbrosqlsersqlwrsteam.synctitbirdcthe'
.flat:00401806 db 'batthundetmlistvisio.winworwordpaxfssvczoolz.',0
.flat:004018F7 align 4
.flat:004018F8 db 0
.flat:004018F9 align 2
.flat:004018FA aAcronisUssProv db '"Acronis USS Provider"',0
.flat:00401C11 aEnterpriseClie db '"Enterprise Client Service"',0
.flat:00401C2D aLanmanserver db '"LanmanServer"',0
.flat:00401C3C aLanmanworkstat db '"LanmanWorkstation"',0
.flat:00401C50 aSqlmcollectio db '"SQLdmCollectionService$Default"',0
.flat:00401C71 aSqlmmanagemen db '"SQLdmManagementService$Default"',0
.flat:00401C92 aSqlmpredictiv db '"SQLdmPredictiveAnalyticsService$Default"',0
.flat:00401C8C 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 aAup db 'AUP',0
.flat:00401D78 aBackupexecagen db 'BackupExecAgentAccelerator',0
.flat:00401D93 aBackupexecag_0 db 'BackupExecAgentBrowser',0
.flat:00401DA0 aBackupexecdevi db 'BackupExecDeviceMediaService',0
.flat:00401DC7 aBackupexecjobe db 'BackupExecJobEngine',0
.flat:00401DD8 aBackupexecmana db 'BackupExecManagementService',0
.flat:00401DF7 aBackupexecrpcs db 'BackupExecRPCService',0
.flat:00401E0C aBackupexecvssp db 'BackupExecUSSProvider',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 aEpscurityserv db 'EPSecurityService',0
.flat:00401E50 aEpuupdateservic 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

```

2020-02-21: PwndLocker Ransomware | Process Killer (Partial)

```

mov     dword ptr [esi+143Ah], 0
push   0
push   80h
push   2
push   0
push   0
push   40000000h
lea    edx, [esi+1442h]
push   edx
call   dword ptr [esi+1054h]
mov    [esi+143Ah], eax
lea    edi, aYourFilesAreEn ; "Your files are encrypted!\r\n\r\nAll yo"...
sub    edi, [esi+1014h]
add    edi, [esi+1010h]
push   0
lea    edx, [esi+143Eh]
push   edx
push   2D4h
push   edi
push   dword ptr [esi+143Ah]
call   dword ptr [esi+1058h]
push   dword ptr [esi+143Ah]
call   dword ptr [esi+1044h]

```

```

loc_403094:
lea    edx, [esi+10h]
push   edx
call   dword ptr [esi+1028h]
add    eax, eax
mov    duord ptr [esi+eax+10h], 2A005Ch
add    eax, 4
mov    duord ptr [esi+eax+10h], 0
lea    edx, [esi+12FCh]
push   edx
lea    edx, [esi+10h]
push   edx
call   dword ptr [esi+101Ch]
cmp    eax, 0FFFFFFFh
jz     locret_40356F

```

```

.flat:00401875 aDeleteShadowsA db 'delete shadows /all /quiet',0
.flat:00401890 aResizeShadowst db 'resize shadowstorage /for=c: /on=c: /maxsize=401MB',0
.flat:004018C3 aResizeShadow_0 db 'resize shadowstorage /for=c: /on=c: /maxsize=unbounded',0
.flat:004018FA aP db 'p',0
.flat:004018FC aAth_txt: unicode 0, <ath.txt>,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 Illinois, 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

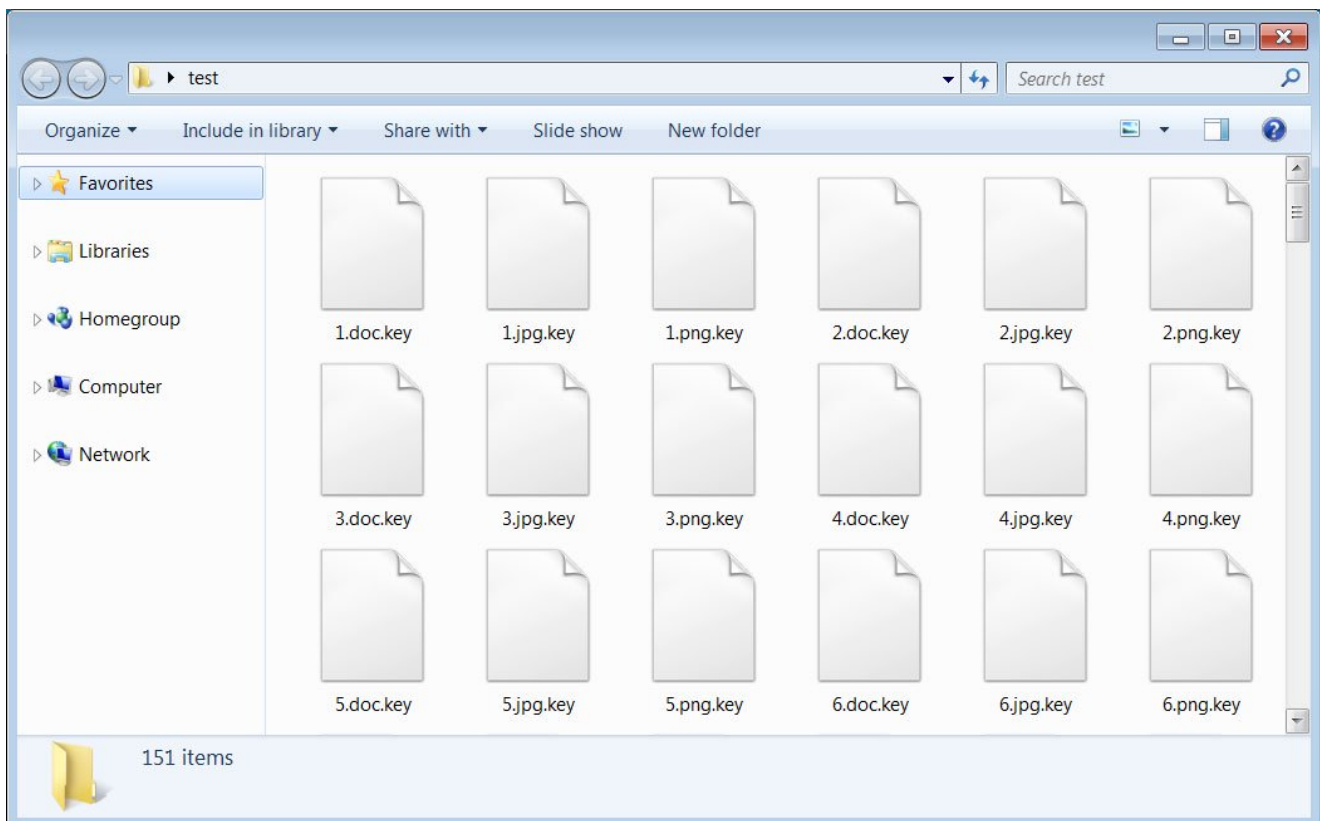
All Users

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 **How_T0_Rec0very_Files.txt**, a kao dokaz da će dekriptor raditi, nude da besplatno otključaju do 2 fajla.

© 2022 IT klinika & Net++ technology. All Rights Reserved.