Berbew Backdoor Spotted In The Wild

Published: 2023-02-03 · Archived: 2026-04-05 22:45:39 UTC

This week, the Sonicwall Capture Labs Research team analyzed a sample of Berbew, a trojan that has been seen used in connection with Download.Ject and FormBook to steal user passwords for banking and other financial institutions. Berbew acts as both an infostealer and proxy to allow for command and control (C2) activities or routing of additional malware.

Analysis

Berbew has previously been reported as being a second-stage payload once the first stage has infiltrated a target and used an exploit; Download.Ject targeted Microsoft IIS services, FormBook is transmitted via phishing email attachments. Static analysis shows that the file is 56kb in size with a timestamp set in the year 2036.

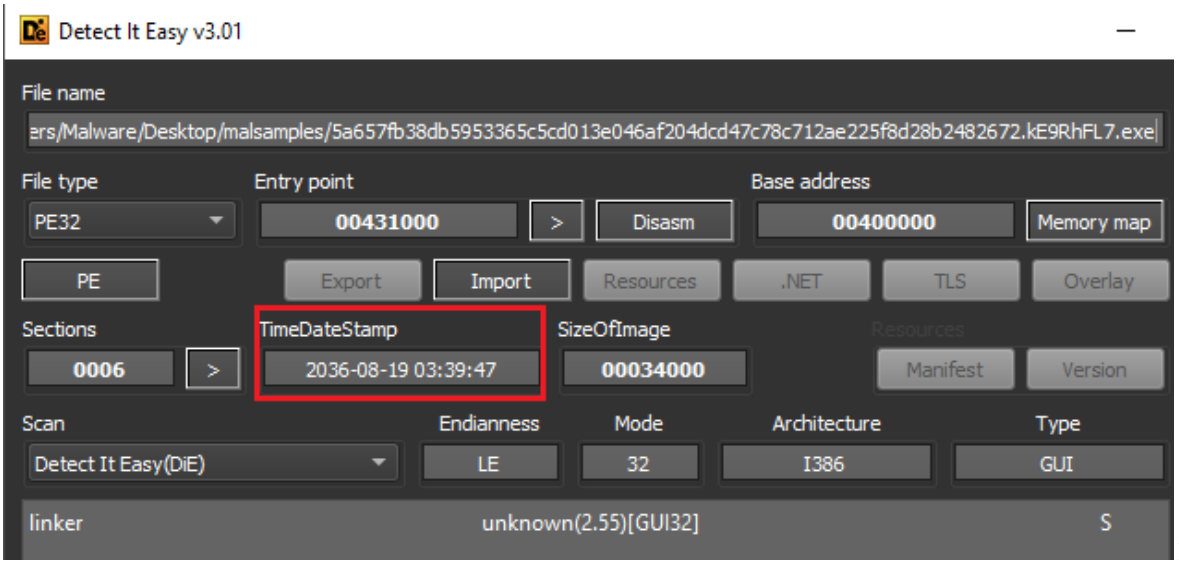

Figure 1: Future creation date

There are a variety of additional red flags in the form of file sections, in which each is a random alphanumeric string. Two of these are also self-modifying, a method that malware can use to change its own code. The second section (.E9Mdns0) is also making use of virtualized code which is a protective measure against analysis, but it's empty before runtime meaning that data will be inserted during runtime. The last item to note is that the entry-point is set within section '.neYm'; this is atypical because the entry-point is generally in the first section of any program.

Figure 2: Items to note, 1) section names, 2) self-modifying sections, 3) virtualized code, 4) entry-point address

The strings show some additional context as to what the program can do. WININET.DLL is a networking library which appears will read from URL entries. It has the ability to read, write and search through registry entries using the 'Reg' values, as well as obtaining security settings on the system.

flag (28)	label (20)	group (13)	value (3416)
-	-	synchronization	WaitForSingleObject
x	-	security	GetSecurityInfo
x	-	security	SetSecurityInfo
x	-	security	SetEntriesInAcl
-	-	resource	LoadCursor
-	-	resource	LoadIcon
x	-	registry	RegCreateKeyEx
-	-	registry	RegCloseKey
-	-	registry	RegOpenKeyEx
-	-	registry	RegQueryValueEx
x	-	registry	RegSetValueEx
-	-	reconnaissance	GetComputerName
x	-	reconnaissance	GetCurrentProcessId
-	-	reconnaissance	GetSystemDirectory
-	-	reconnaissance	GetTickCount
-	-	reconnaissance	GetVersionEx
-	-	reconnaissance	GetWindowsDirectory
-	-	reconnaissance	GetUserName
-	file	network	WININET.DLL
x	-	network	DeleteUrlCacheEntry
x	-	network	FindFirstUrlCacheEntry
x	-	network	FindNextUrlCacheEntry
x	-	memory	GlobalMemoryStatus

Figure 3: Berbew program strings

At runtime, the executable drops 934 files within 'C:\Windows\SYSWOW64' and executes between 23-25 in sequence. Of the files dropped, 467 are duplicates of the main executable, with the other half being DLL files. They have a naming scheme of six alphabetic characters and 32.exe, or eight alphabetic characters (this applies to both the .EXE and .DLL files). A hook is set up for capturing data using 'DirectDrawCreateEx', which allows for saving keyboard, mouse, clipboard, and screen activity.

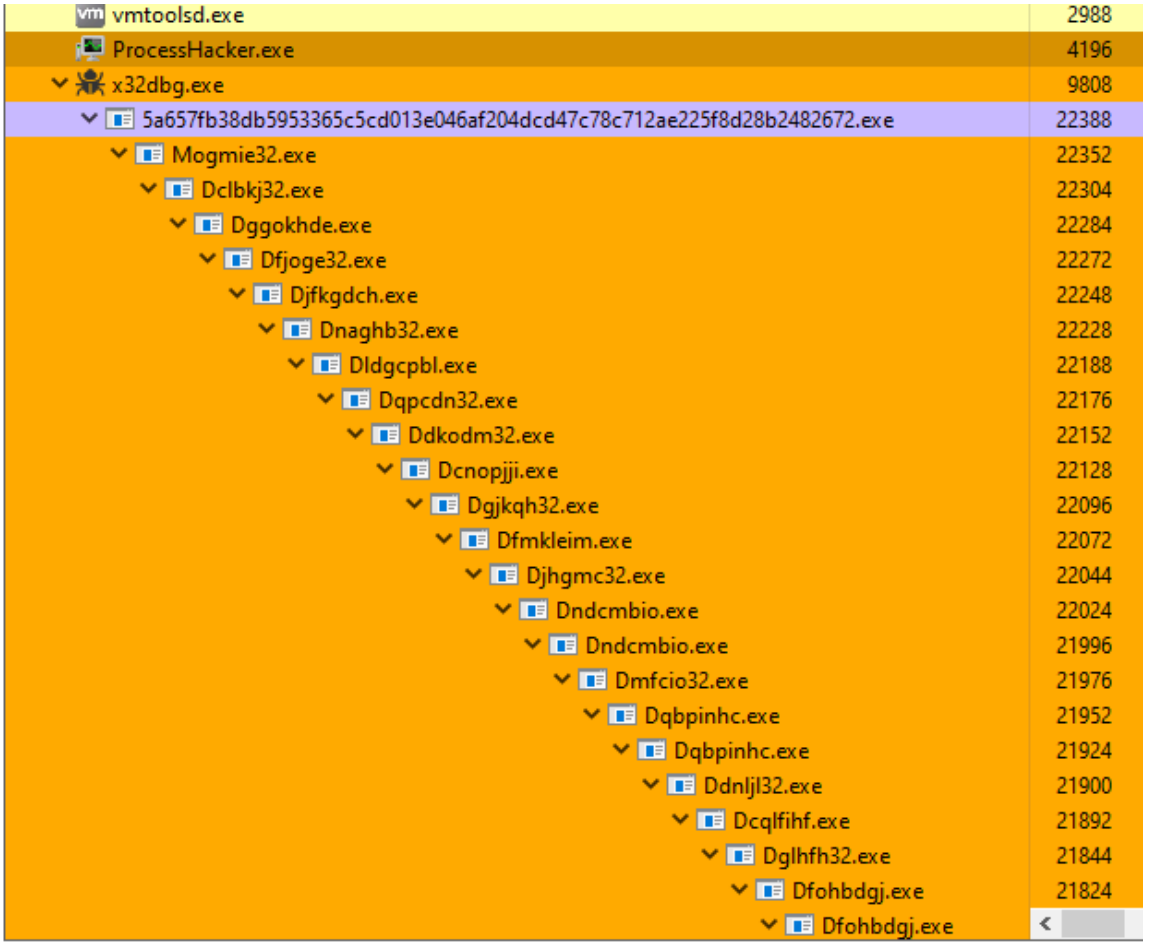

Figure 4: Runtime sequence of dropped executables

In addition, there are also registry keys written for persistence:

-
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
Web Event Logger
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{79FEACFF-FFCE-815E-A900-316290B5B738}\InProcServer32
-
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

These will be triggered on restart to load one of the dropped DLL files and restart the program. The dropped DLL files are all identical to each other and only 7kb in size.

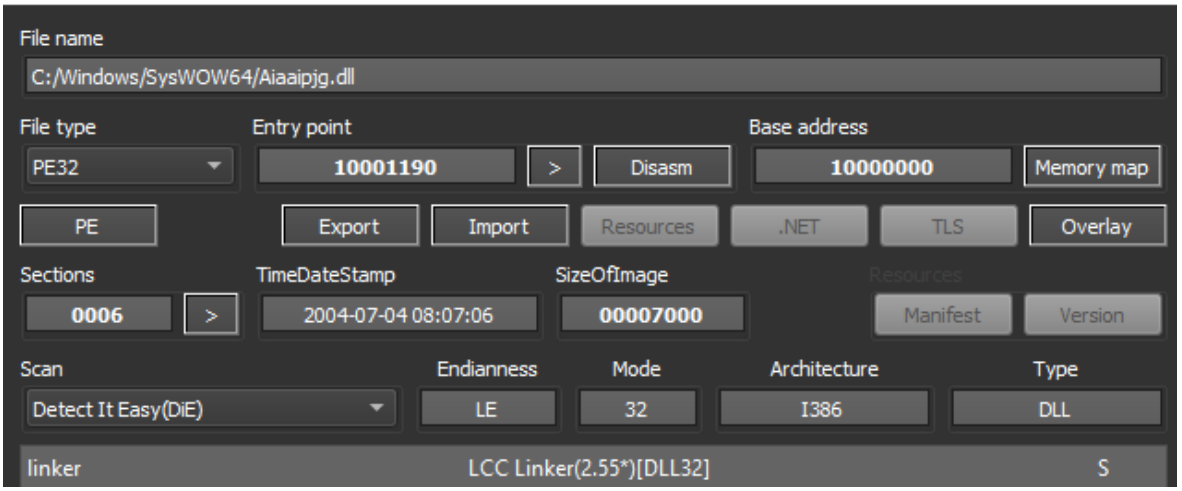

Figure 5: Detection of dropped DLL

When a financial website has been brought up, or during regular use, the system will bring up prompts to change passwords. This info is then relayed to one of the URLs in memory; however, no connections are made before data has been collected.

SonicWall Capture Labs provides protection against this threat via the following signature:

GAV: Berbew.F (Trojan)

This threat is also detected by SonicWALL Capture ATP w/RTDMI and the Capture Client endpoint solutions.

IOCs

Sample 1
MD5: 7350C5C9F3020FB201AD2184453DBBAC
SHA1: C68E9514A58D803C65647191153F35BD742A7463
SHA256: BCC12EEF62B196293032ECB05804510474A276B9A12DD70248F55EFFD405474C
Size: 56kb

Sample 2
MD5: FE1AE2707A3D86E7EF8B921A77D571EB
SHA1: 01F484BA1B4B28555FD8DD959A428C94A652443D
SHA256: 73AE10E87168EA0F543C0CFE23B1BA71726AC597E52F06075432EFE30FDED843
Size: 7kb

Registry Keys

-
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
Web Event Logger
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{79FEACFF-FFCE-815E-A900-316290B5B738}\InProcServer32
-
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

URLs

hxxp://adult-empire[.]com/index.php
hxxp://color-bank[.]ru/index.php
hxxp://crutop.nu
hxxp://crutop.nu/index.htm
hxxp://crutop.nu/index.php
hxxp://crutop.nuAWM
hxxp://crutop[.]ru/index.htm
hxxp://crutop[.]ru/index.php
hxxp://cvv[.]ru/index.htm
hxxp://cvv[.]ru/index.php
hxxp://devx.nm[.]ru/index.php
hxxp://fethard.biz/index.htm
hxxp://fethard.biz/index.php
hxxp://gaz-prom[.]ru/index.htm
hxxp://hackers.lv/index.php
hxxp://kadet[.]ru/index.htm
hxxp://kavkaz[.]ru/index.htm
hxxp://kidos-bank[.]ru/index.htm
hxxp://konfiskat.org/index.htm
hxxp://ldark.nm[.]ru/index.htm
hxxp://master-x
hxxp://parex-bank[.]ru/index.htm
hxxp://promo[.]ru/index.htm
hxxp://ros-neftbank[.]ru/index.php
hxxp://trojan[.]ru/index.php
hxxp://virus-list.com/index.php
hxxp://www.redline[.]ru/index.php
