

# Win32/Duqu, injection de code intéressantes

Samuel Chevet

January 23, 2002

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

@cBekrar (VUPEN)

What is Duqu ?

Driver / Main DLL

Downloaded  
threat

Conclusion

*Duqu is in the wild since a year and the AntiVirus vendors are so proud to detect it 12 months late. Offensive security will always win!*

# What is Duqu ?

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

@cBekrar (VUPEN)

What is Duqu ?

Driver / Main DLL

Downloaded  
threat

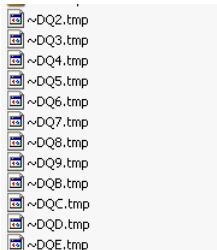
Conclusion

- October 14, 2011
- Backdoor
- CrySyS at Budapest University
- Limited number of organizations
- Limited number of countries

# Why is it called Duqu?

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet



~DQ2.tmp	62 Ko	Fichier TMP
~DQ3.tmp	53 Ko	Fichier TMP
~DQ4.tmp	24 Ko	Fichier TMP
~DQ5.tmp	41 Ko	Fichier TMP
~DQ6.tmp	33 Ko	Fichier TMP
~DQ7.tmp	30 Ko	Fichier TMP
~DQ8.tmp	15 Ko	Fichier TMP
~DQ9.tmp	31 Ko	Fichier TMP
~DQB.tmp	26 Ko	Fichier TMP
~DQC.tmp	24 Ko	Fichier TMP
~DQD.tmp	1 Ko	Fichier TMP
~DQE.tmp	118 Ko	Fichier TMP

- File name with prefix  
“~ DQ”

Duqu

@cBekrar (VUPEN)

What is Duqu ?

Driver / Main DLL

Downloaded  
threat

Conclusion

# What is Duqu ?

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

- Word document (CVE-2011-3402 True Type Font parsing)
- Network spreading
- JMINET7.SYS = MRXCLS.SYS (Stuxnet)
- Taiwanese company called C-Media Electronics Incorporation
- Creation date : November 2010

Duqu

@cBekrar (VUPEN)

What is Duqu ?

Driver / Main DLL

Downloaded  
threat

Conclusion

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

## Driver

- Activate the threat at system start
- HLM\SYSTEM\CurrentControlSet\Services\JmiNET3
- DriverReinitializationRoutine
- PsSetLoadImageNotifyRoutine()
- services.exe

## Main DLL

- RPC Component (Stuxnet ?)
- Command And Control functionality
- Scan Security Product

Duqu

@cBekrar (VUPEN)

What is Duqu ?

Driver / Main DLL

Downloaded  
threat

Conclusion

- Recovered on compromised computers
- Standalone
- InfoStealer

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

Downloaded  
threat

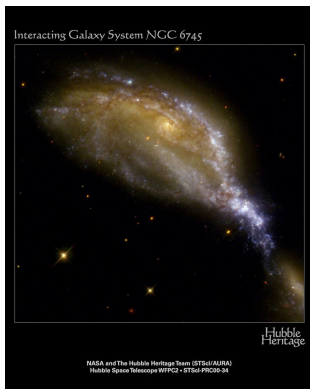
Downloaded threat

DLL

Injection method

Nine main routines

Conclusion



```
.text:004012EA loop_decrypt_dll
```

```
.text:004012EA          not     byte ptr [eax]
```

```
.text:004012EC          inc     eax
```

```
.text:004012ED          dec     ecx
```

```
.text:004012EE          jnz    short loop_decrypt_dll
```

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

Downloaded  
threat

Downloaded threat

DLL

Injection method

Nine main routines

Conclusion

- CreateProcess lsass.exe ( Suspended State )
- ZwQueryInformationProcess() for gathering PEB address
- ReadProcessMemory()

```
>dt nt!_PEB
+0x000 InheritedAddressSpace : UChar
+0x001 ReadImageFileExecOptions : UChar
+0x002 BeingDebugged : UChar
+0x003 SpareBool : UChar
+0x004 Mutant : Ptr32 Void
+0x008 ImageBaseAddress : Ptr32 Void
```

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

Downloaded  
threat

Downloaded threat  
DLL

Injection method  
Nine main routines

Conclusion

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

Downloaded  
threat

Downloaded threat  
DLL

Injection method  
Nine main routines

Conclusion

- ZwCreateSection()
- ZwMapViewOfSection( ..., VIEW\_SHARE, ..)
- STATUS\_CONFLICTING\_ADDRESSES
- ZwUnmapViewOfSection()
- Be able to change All PE File
- No SetThreadContext(), or CreateRemoteThread(),  
...

# Nine main routines

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

```
.data:1000E028      db  68h                ; Take Screenshot
.data:1000E029      db  0
.data:1000E02A      db  0
.data:1000E02B      db  0
.data:1000E02C      dd  offset nullsub_2
.data:1000E030      dd  offset wrapper_delete_BC
.data:1000E034      dd  offset take_screenshot
.data:1000E038      db  0
.data:1000E039      db  0
.data:1000E03A      db  0
.data:1000E03B      db  0
.data:1000E03C      db  69h ; i            ; NetWork Information
.data:1000E03D      db  0
.data:1000E03E      db  0
.data:1000E03F      db  0
.data:1000E040      dd  offset clean_network_info
.data:1000E044      dd  offset nullsub_1
.data:1000E048      dd  offset network_info
.data:1000E04C      align 10h
.data:1000E050      db  67h ; g            ; Keylogging
.data:1000E051      db  0
.data:1000E052      db  0
.data:1000E053      db  0
.data:1000E054      dd  offset loop_getmsg
.data:1000E058      dd  offset wrap_pthreadss
.data:1000E05C      dd  offset keylogging
```

Duqu

Downloaded  
threat

Downloaded threat

DLL

Injection method

Nine main routines

Conclusion

# Nine main routines

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

- 65h : List of running processes (CreateToolhelp32Snapshot())
- 66h: Drive names and information (GetLogicalDrives(), ...)
- 67h: Keylogger (SetWindowsHookExW(), WH\_KEYBOARD\_LL, ...)
- 68h: Take a screenshot (BitBlt(), ...)
- 69h: Network information (GetNetworkParams(), ...)
- 6Ah: Window enumeration (EnumWindows(), ...)
- 6Bh: Share enumeration (NetFileEnum(), ...)
- 6Dh: File exploration on all drives (FindFirstFileW(), ...)
- 6Eh: Enumerate computers on the domain (NetServerEnum(), ...)

Duqu

Downloaded  
threat

Downloaded threat

DLL

Injection method

Nine main routines

Conclusion

Win32/Duqu,  
injection de code  
intéressantes

Samuel Chevet

Duqu

Downloaded  
threat

Conclusion

- Always fun to study malware
- @w4kfu
- [blog.w4kfu.com](http://blog.w4kfu.com)