Uncovering Duqu
The Stuxnet Attackers Return

Nicolas Falliere

4/24/2012
Agenda

1. Revisiting Stuxnet
2. Discovering Duqu
3. Inside Duqu
4. Weird, Wacky, and Unknown
5. Summary
Revisiting Stuxnet
Key Facts

- Windows worm discovered in July 2010
- Uses 7 different self-propagation methods
- Uses 4 Microsoft 0-day exploits + 1 known vulnerability
- Leverages 2 Siemens security issues
- Contains a Windows rootkit
- Used 2 stolen digital certificates
- Modified code on Programmable Logic Controllers (PLCs)
- First known PLC rootkit
Cyber Sabotage
Discovering Duqu
Boldi Bencsath (CrySyS) emails: “important malware Duqu”

Hours later the C&C is wiped

Boldi emails: “DUQU DROPPER FOUND MSWORD 0DAY INSIDE”

Announce discovery and publish 25 page paper on Duqu
Inside Duqu
Key Facts

- Duqu uses the same code as Stuxnet except payload is different
- Payload isn’t sabotage, but espionage
- Highly targeted
- Used to distribute infostealer components
- Dropper used a 0-day (Word DOC w/ TTF kernel exploit)
- Driver uses a stolen digital certificate (C-Media)
- No self-replication, but can be instructed to copy itself to remote machines
- Multiple command and control servers that are simply proxies
- Infections can serve as peers in a peer-to-peer C&C system
Countries Infected

Six organizations, in 8 countries confirmed infected
Architecture

- Main component
  - A large DLL with 8 or 6 exports and 1 main resource block
  - Resource = Command & Control module
- Copies itself as %WINDIR%\inf\xxx.pnf
- Injected into several processes
- Controlled by a Configuration Data file
- Lots of similarities with Stuxnet
  - Organization
  - Code
- Usual lifespan: **30 days**
  - Can be extended
Installation

1. Document Opened Triggers Exploit
2. Exploit Loads Shellcode
3. Shellcode decrypts driver and Installer
4. Shellcode executes driver
5. Driver injects Installer into services.exe
6. Installer decrypts 3 files and passes execution to the main component
Signed Drivers

- Some signed (C-Media certificate)
- Revoked on October 14
Command & Control Module

- Communication over TCP/80 and TCP/443
  - Embeds protocol under HTTP, but not HTTPS
  - Includes small blank JPEG in all communications
  - Basic proxy support

- Complex protocol
  - TCP-like with fragments, sequence and ack. numbers, etc.
  - Encryption AES-CBC with fixed Key
  - Compression LZO
  - Extra custom compression layer

- Infections can serve as proxies to enable a peer-to-peer C&C system
Payloads

- C&C sends modules to the infected systems
  - Executed directly in memory
  - Saved to disk encrypted

- Modules seen
  - Infostealer
  - Reconnaissance module
  - “Lifespan expansion” module
Weird, Wacky, and Unknown
TTF 0-Day Exploit

- Vulnerability in GDI in Win32k.sys processing a TTF object
- Able to modify 1 byte

```assembly
jbe short loc_BF989EA6
movzx edi, ax
mov edi, edi

loc_BF989EA6:
    mov dl, [ecx] ; CODE XREF: sfac_GetSbitBitmap(x
    or [esi], dl ; overwrite here
    inc ecx
    inc esi
    dec edi
    jnz short loc_BF989EA6

loc_BF989EAF: ; CODE XREF: sfac_GetSbitBitmap(x
    movzx edx, [ebp+arg_28]
    add ebx, edx
    dec [ebp+arg_24]
    jnz 18 FreeBSD
```
TTF 0-Day Exploit

- Font file claims to be "Dexter Regular" by "Showtime Inc."
- Dexter is a television series about Dexter Morgan, a blood pattern analyst for the Miami Metro Police Department
- He moonlights as a serial killer, but only kills other murderers

- The font file only has two characters defined

: )
Link with “Stars” Virus

- In April 2011 Iranian officials stated they were hit by a virus named “Stars”
- Inside one of the keylogger components is a partial image
  - Used before an embedded MZ file
  - Perhaps used to obfuscate the embedded MZ file
Link with “Stars” Virus
Odd Code

- Duqu is almost entirely C++
- The C&C module is not C++, but very much like it
  - Object oriented
  - Function table is directly in the class instance and can be modified after the constructor is called
  - Objects communicate using method calls, queues, and event callbacks
  - Constructors and destructors
  - Function table locations are not fixed (some at offset 0, some not)
  - Member functions can be called directly or via the object function table
  - The ‘this’ pointer can be in any register or stack
- Most likely C, with custom C++ features added
Conclusion

- Stuxnet was the first publicly known malware designed to cause “real” real-world damage
- Duqu shares many similarities but is used for espionage
- Both required resources at the level of a nation-state
- Raises attribution issues
- Created by the same organization
- Level of sophistication is singular
- Attackers have not gone away
  - New Duqu binary compiled in Feb 2012
More information

- Check out Symantec’s papers and blogs

W32.Stuxnet Dossier
Version 1.4 (February 2010)

Nicolas Falliere, Liam O Murchu, and Eric Chien

W32.Duqu
The precursor to the next Stuxnet
Version 1.3 (November 2011)

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors reserve the right to make revisions to this document shortly after release as new information is unraveled or as they may be publicly disclosed. This paper is the work of numerous individuals at the Symantec Security Response team over the past three months and beyond the cited authors. Without their assistance, this paper would not be possible.

Introduction
W32.Stuxnet has garnered a great deal of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our blog series on the topic. While some of the information from these blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code or reprogrammable logic controllers (PLC) to make them work in a manner the attacker intended and to hide these changes from the operator of the equipment. In order to achieve this goal the creators wanted to set a large array of components to increase their chances of success. This includes zero-day exploits, a Win32 backdoor, the first-ever PLC exploit, and virus variants.
Questions?

Thank you!