McAfee Labs
Consolidated Threat Report:
Duqu

(MTIDs: M66234, M65791, M65790, M65789, M66239, M68971)

v2.2

By McAfee Labs

Version History

Date	Version	Author	Comments
11/1/2011	1.0	Jim Walter	Initial Draft
11/2/2011	1.1	Jim Walter	Update: References, Appendix modifications, style changes. Network/Protocol detail update
1/3/2011	1.2	Jim Walter	Update to HLO & Duqu/Stuxnet code comparisons. Network/Protocol details update.
11/3/2011	1.3	Jim Walter	Network / Protocol updates
11/3.2011	1.4	Dan Sommer	Style and Formatting Review
11/4/2011	1.5	Jim Walter	Public Release
11/4/2011	1.6	Jim Walter	Format Adjustment / Industry Refs
11/5/2011	1.7	Jim Walter	Sample Data update / Information update
11/7/2011	1.8	Jim Walter	Format and branding updates, citation updates.
11/8/2011	1.9	Jim Walter	AV Coverage detail update (Exploit-CVE2011-3402)
11/14/2011	2.0	Jim Walter, Dan Sommer	Countermeasure details (Stinger), SMB clarification, “Dexter”-related font data, additional review
12/13/2011	2.1	Jim Walter	Updated to include references to MS11-087
3/20/2012	2.2	Jim Walter	Updated to include new Sample Data - bca394d73015153cc18e315c0d705301

Introduction: The Consolidated Threat Report

McAfee Labs Consolidated Threat Reports bring together all the verified and corroborated intelligence on highly relevant and publically critical threats and events. Our researchers and engineers continually monitor the global threat landscape and provide relevant data to both our direct customers and to the public at large. We do this to assist in risk assessment and mitigation, as well as to “serve the greater good” as we cooperate and conduct research with other agencies and communities. Our Consolidated Threat Reports combine all the up-to-the-minute information from various sources (Global Threat Intelligence, blog entries, podcasts, whitepapers, presentations, and more.)

Introduction to Duqu

Beginning in mid-October 2011, McAfee Labs, along with a number of other vendors, were alerted to and began actively monitoring and acting upon reports of an emerging threat known as Duqu. It appears that the primary attack (the seeding and distribution of the malware) occurred in September and October. Much of the initial intelligence came courtesy of CrySyS (Laboratory of Cryptographic and System Security) in Budapest, Hungary. CrySyS is responsible for naming this threat, based on a prefix used in some of its associated files. There are many reasons for the escalated concern and reaction to this particular threat. We will attempt to highlight those reasons in this document. In particular, the threat’s apparent relationship to the highly sophisticated Stuxnet attacks are reason enough to dig deeper and attempt to uncover the motivation, behavior, and overall effects of this threat. For some background perspective, Stuxnet is a highly sophisticated malware threat targeted at specific Siemens SCADA systems. The associated attack took place between 2009 and 2010 and is considered to be one of the most sophisticated, targeted, attacks in recent history. Stuxnet primarily targeted facilities in Iran, India, and Indonesia.

High-Level Overview

- Targeted attacks have been reported in Iran, England, and the United States
    - Limited reports also indicate attacks in Austria, Hungary, and Indonesia
- The executables share injection code with the Stuxnet worm and were compiled after the last Stuxnet sample was recovered
- The structure of Duqu is very similar to that of Stuxnet (using Portable Executable (PE) format resources)
- There is no industrial control system–specific attack code in Duqu.
- The primary infection vector is a malicious Microsoft Word document, which exploits a zero-day vulnerability in Microsoft Windows (CVE-2011-3402)
    - On November 3, 2011, Microsoft posted an associated Security Advisory addressing the vulnerability, as well as documenting a workaround.
        - **Microsoft Security Advisory (2639658) - Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege**
        - https://technet.microsoft.com/en-us/security/advisory/2639658
    - As of November 2, 2011,the only related public disclosure was BID 50462
        - http://www.securityfocus.com/bid/50462
    - On December 13, 2011, Microsoft released an update to address the associated vunerability (referenced in 2639658).
        - MS11-087 - https://technet.microsoft.com/en-us/security/bulletin/ms11-087
- The infected organizations appear to be limited
- There is no known targeting of energy-sector companies
- The malware employed a valid digital certificate (revoked as of October 14, 2011)
- The malware is designed to remove itself
    - We have observed two such mechanisms: one set to 30 days and one to 36 days
- The known control servers were hosted in India and Belgium

History and Relationship to Stuxnet

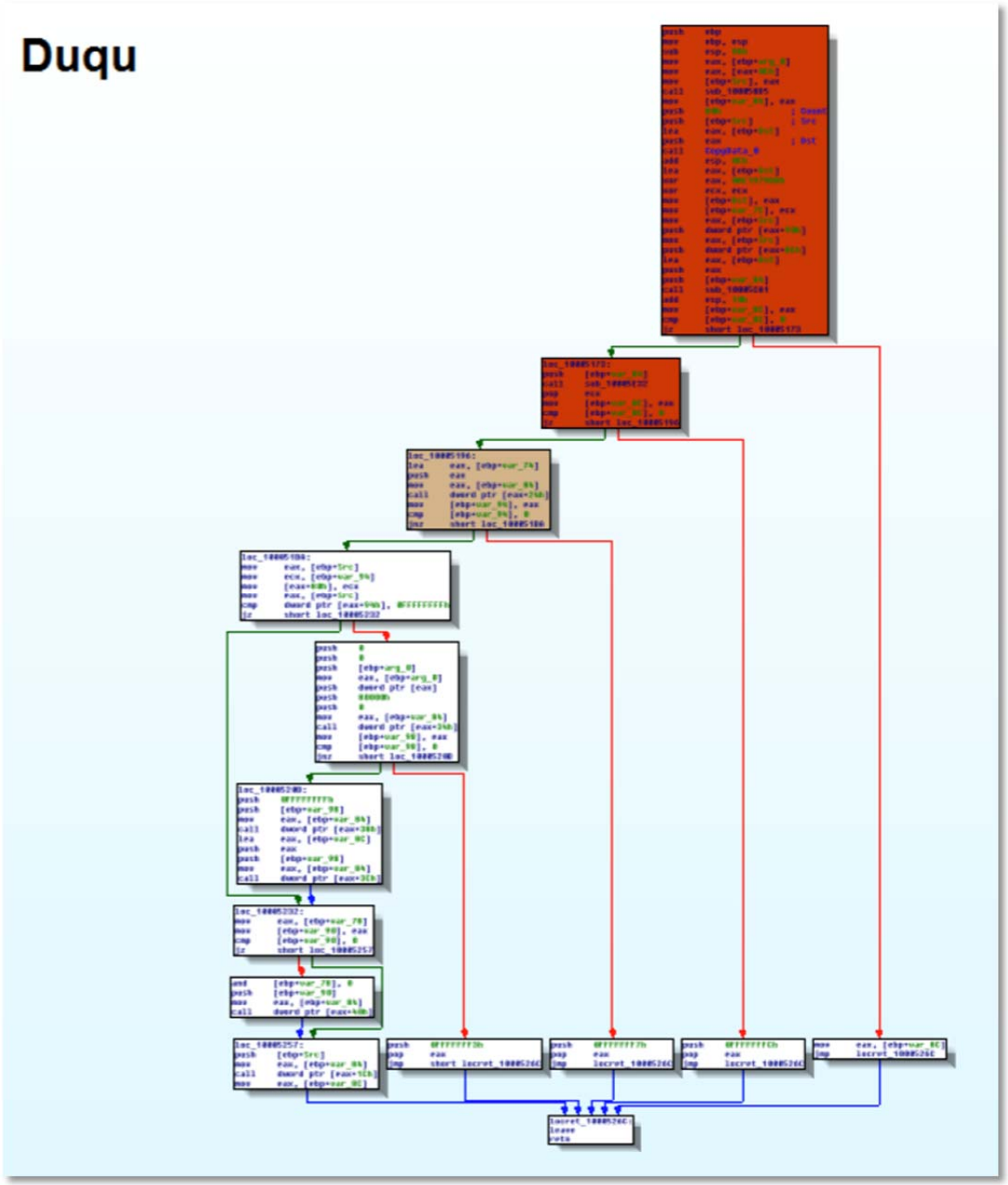
The Duqu threat family has many monikers, ranging from “Mother of Stuxnet,” “Son of Stuxnet,” “Stuxnet’s third cousin,” and more. As of this writing, the general consensus is that Duqu, in concept and execution, is a framework component for a Stuxnet-like attack. To continue the family-tree analogy, Duqu should be though of as an ancestor of future Stuxnet-like attacks.

There are a number of dead-on similarities in the code and functionality of Duqu and Stuxnet. A breakdown of these similarities can be seen in the following table:

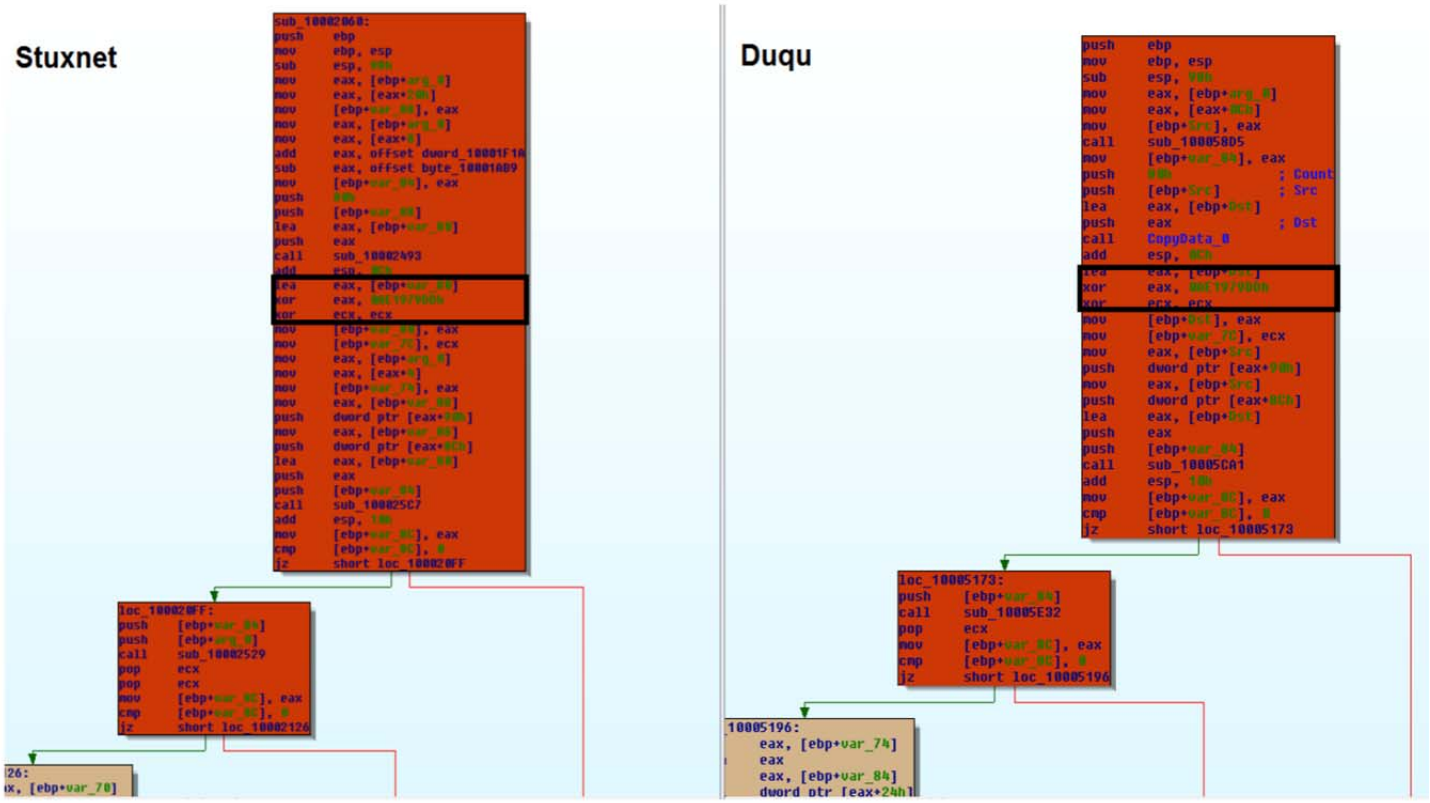
Feature	Duqu	Stuxnet
Composed of multiple modules	Yes	Yes
Rootkit to hide its activities	Yes	Yes
System driver is digitally signed	Yes (C-Media)	Yes (Realtek, JMicron)
System driver decrypts secondary modules in PNF files	Yes	Yes
Decrypted DLLs are directly injected into system processes instead of dropped to disk	Yes	Yes
Date sensitive: functionality is controlled via complex, encrypted configuration file	Yes (30 or 36 days)	Yes
Uses XOR-based encryption for strings	Yes (key: 0xAE1979DD)	Yes (key: 0xAE1979DD)
References 05.09.1979 in configuration file (http://en.wikipedia.org/wiki/Habib_Elghanian)	Yes (0xAE790509)	Yes (0xAE790509)
New update modules via control server	Yes (keylogger)	Yes
Known module to control PLC/SCADA systems	No	Yes

Duqu and Stuxnet Code Comparisons: DLL Injection Code

Continuing with the code-based similarities, we outline the DLL injection code below:



DLL Injection code



Primary Functionality Within the Main Module(s)

Before diving too deeply into Duqu's core functionality, we need to make a few key points.

- As of November 1, 2011, the exact nature of the distribution of the initial malware "dropper" is unknown. New reports from CrySyS say that the first phase of the infection occurred via a malicious Microsoft Word document. This document used currently undisclosed methods (exploits) to drop additional components. The malicious .doc file appears to load a kernel driver, which in turn injects a DLL into services.exe, thus starting the installation.
- All malware associated with Duqu are Trojans. They do not self-replicate. They require additional interaction (either directly by an acting adversary, or through programmatic methods via other malware components).
- The dropped malware components, which persist on an infected host, are basic backdoor Trojans, keyloggers, and a (user-mode) rootkit component.
- Duqu appears to have been written in a C-based object-oriented language and compiled in Microsoft Visual C 2008.

Main Module Functionality Breakdown

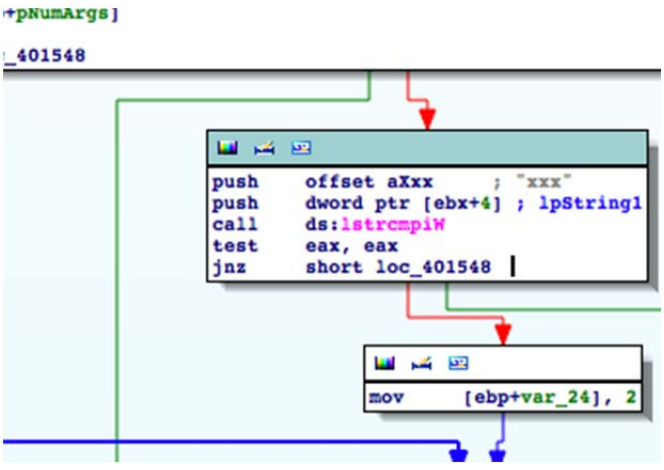
In this section we will focus on the two initial variants of the driver components (.sys).

- The two variants of .sys files are responsible for restarting the malware
    - The .sys filenames mimic JMicron and C-Media driver filenames (cmi4432.sys and jminet7.sys)
    - The JMicron mimic file is not signed, and is the earlier variant
- Drivers are loaded according to Network Group
- The .sys drivers decrypt the associated PNF files and inject the resulting DLL file into services.exe
    - This functionality is part of the malware's anti-firewall and anti-BB features
- The decrypted and injected DLL is responsible for decrypting the payload module from its resource section. The resource ID (302) is the same for all modules.
- The payload module is directly injected into running processes using the same methods as Stuxnet
- The DLL implements the rootkit component/functionality to hide the payload from the user's view

Keylogger Module

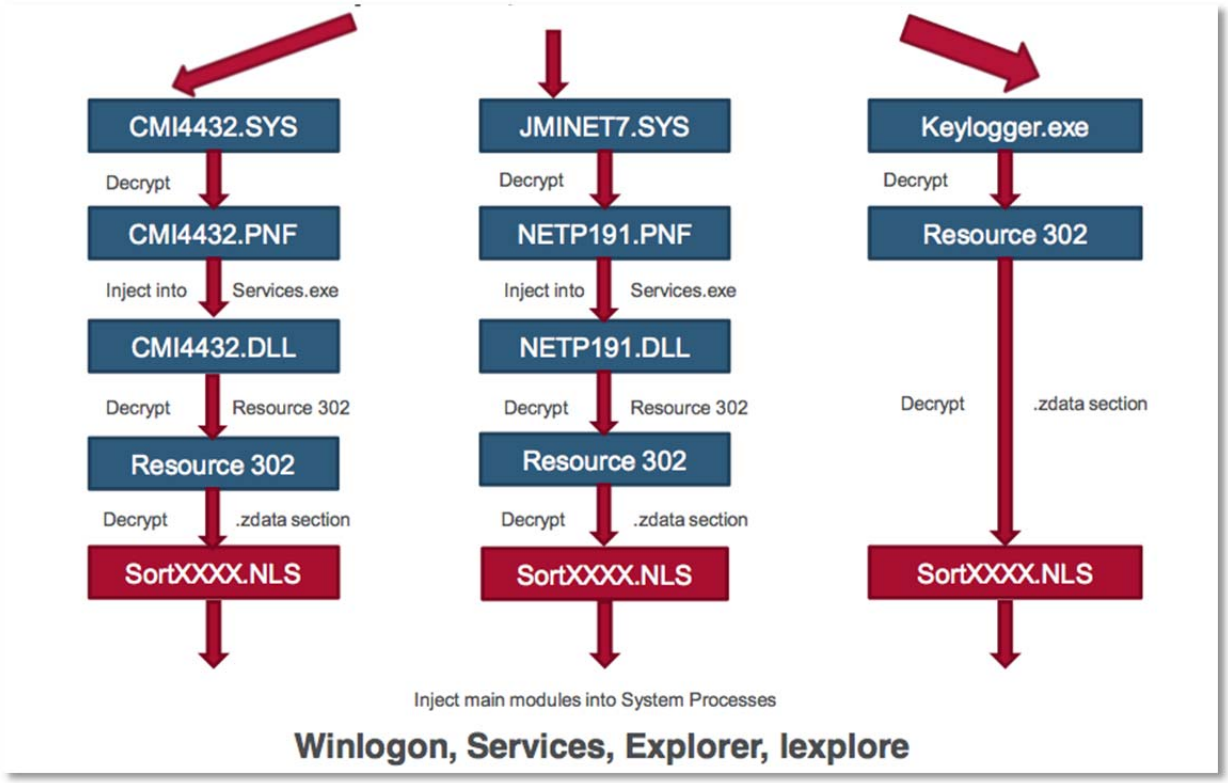
The keylogger component is a standalone module. It is delivered via a control server to the target after the initial infection.

The keylogger component (and other Duqu payloads) does not specifically contain code to "spread' or otherwise self-replicate (via SMB shares, for example). Its ability to spread relies on communication with, and instructions received from, the control server. The keylogger uses the same decryption routines as the other modules. It can collect different types of information from the target machine:



- Keystroke data
- Machine information (OS version, patches, machine name, users, etc.)
- Process list
- Network information
- List of shared folders
- List of machines on the same network
- Screen shots

The Keylogger also accepts command-line parameter instructions, and works only if “xxx” is the first parameter passed. The following images offer a graphical view:



Network Activity

Information around Duqu's control server activity has remained largely static. However, new variants were discovered on November 1, 2011, that behave the same as earlier versions but use a different control server. A quick breakdown of the network information follows:

Variants observed prior to November 1:

- Control server: 206.183.111.97
- DNS: canoyragomez.rapidns.com
- Protocol: HTTP and HTTPS
- Ports: 80 and 443
- WHOIS
- Web Werks WEBWRKS-PHLA1 (NET-206-183-104-0-1) 206.183.104.0–206.183.111.255
- Web Werks India Pvt. Ltd. WEBWERKSIND00001 (NET-206-183-111-0-1) 206.183.111.0–206.183.111.255
- ASN - AS33480 ASN-WEBWERKS Web Werks
- Geography: India

Variants observed on November 1:

- Control server: 77.241.93.160
- DNS: N/A (no A records)
- Protocol: HTTP and HTTPS
- Ports: 80 and 443
- WHOIS
- COMBELL
- 77.241.93.0–77.241.93.255
- AS34762
- Geography: Brussels, Belgium

Network Protocol Details

Once the DLL module is started, the known variants try to contact the control server at the address below on TCP Ports 80 and 443 (via HTTP or HTTPS).

The malware first tries to reach the control server on Port 443. The traffic appears to be an invalid SSL flow. After two failed attempts on port 443, Duqu tries Port 80 and makes a GET request, demonstrated below:

- GET / HTTP/1.1
- Cookie: PHPSESSID=o5ukre1ul0q6i2il1ij3ghi0j1
- Cache-Control: no-cache
- Pragma: no-cache
- User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9 (.NET CLR 3.5.30729) Host: x.x.x.x

The PHPSESSID is an encrypted message sent to the control server.

The User-Agent is most likely copied and pasted from the current browser.

The host header contains the actual IP address of the control server. At certain intervals (in our tests we have observed 90 seconds), Duqu will send an HTTP POST request to the control server, with the post content embedded in a .jpg file with MIME encoding.

POST / HTTP/1.1

Cookie: PHPSESSID=0h04dt1bds86iigl012g0g3131

Cache-Control: no-cache

Pragma: no-cache

Content-Type: multipart/form-data; boundary=----------9fafb3fc325e16

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9 (.NET CLR 3.5.30729)

Host: x.x.x.

Content-Length: 1280

Connection: Keep-Alive

Attack-Specific Network Details

One specific address has revealed itself as an “Address of Interest” tied to two specific campaigns against targets in Iran. The campaigns took place within a 12-day period. Associated IP and host details follow:

IP Address: 68.132.129.18

- Geo = United States (Virginia)
- UUNET Technologies, Inc
- 22001 Loudoun County Parkway, Ashburn, VA 20147

The IP address 68.132.129.18 originally resolved to kasperskychk.dydns.org. Querying this address allows the Trojan to confirm an Internet connection. It also queries microsoft.com.

Multiple .jpg images are used, but one appears to have gotten the most attention. One image is of NGC 6745, an irregular galaxy that some think resembles the head of a bird. There has been much speculation about the significance of this image, and of anything it might resemble. For now, it remains speculation, and may be nothing more than an interesting “Easter egg” created by the author. Claims that the image is anything otherwise are uncorroborated.

Notes on the Control Servers

- The original control server was removed on October 14, 2011
- On October 19, 2011, canoyragomez.rapidns.com began to resolve to 207.106.22.3. At this point the host/DNS name is no longer related to Duqu. However, this (still active) IP appears to redirect to various survey scams and spam sites. It is also under the Web Werks registrar.

Who is Actually Affected/Infected?

At this time, we are aware of at least 12 confirmed infected environments, with as many as 16 infections possible. As details emerge around the November 1, 2011, samples, this number may change. This count is based on the number of attack-specific Duqu-drivers we have observed. Each targeted environment received a unique variant of the Duqu driver(s).

Signed Driver Examples

MD5	Data
BDB562994724A35A1EC5B9E85B8E054F	Verified: Unsigned File date: 9:59 AM 10/25/2011 Publisher: Intel Corporation Description: Intel Matrix Storage SCSI driver Product: Intel Matrix Storage SCSI driver Version: 6.2.0.1354 File version: 6.2.0.1354
0EECD17C6C215B358B7B872B74BFD800	Verified: Unsigned File date: 9:58 AM 10/25/2011 Publisher: JMicron Technology Corporation Description: JMicron Volume Snapshot Driver Product:JMicron Volume Snapshot Version:2.1.0.14 File version: 2.1.0.14
3D83B077D32C422D6C7016B5083B9FC2	Verified: Unsigned File date: 9:58 AM 10/25/2011 Publisher: Adaptec, Inc. Description: Adaptec StorPort Ultra321 SCSI Driver Product:Adaptec Windows 321 Family Driver Version:2.1.0.14 File version: 2.1.0.14
4541E850A228EB69FD0F0E924624B245	Verified: Revoked Signing date: 9:57 AM 10/25/2011 Publisher: C-Media Electronics Incorporation Description: Onboard Sound Driver Product:C-Media Electronics Incorporation Version:2.1.0.14 File version: 4.2.0.15

C9A31EA148232B201FE7CB7DB5C75F5E	Verified: Unsigned File date: 9:58 AM 10/25/2011 Publisher: IBM Corporation Description: IBM ServeRAID Controller Driver Product:IBM ServeRAID Contoller Version:4.33.0.12 File version: 4.33.0.12
BCA394D73015153CC18E315C0D705301	Verified: Unsigned File date: 1:30 AM 12/9/2011 Publisher: Microsoft Corporation Description: High changer class Driver Product: High changer class Driver Version: 2.1.0.14 File version: 2.1.0.14

Motivation and Targets

The motivation behind Duqu can be viewed from a couple of angles. At a high level, we see Duqu as a Trojan module framework. It can be tailored to each attack, similar to Stuxnet. The sequence of spearphishing document to Trojan dropper to remote administration tool/backdoor method is very common. What sets this threat apart is its complexity, and its ability to potentially be very direct in its use and effect. Again, Stuxnet is a prime example of a derivative threat.

Specific to the September-October attacks, the most likely purpose was information theft and industrial espionage. In at least one case, we also believe that a specific Certificate Authority was targeted by generating rogue certificates. Doing so allowed the malware to act freely in the targeted environment, at least until the rogue certificate was revoked.

Targeting a Certificate Authority is one method of attack. Theft, transmission of sensitive information, and espionage are compelling motives. The Duqu attacks appear to be highly targeted attempts to gather sensitive data and environmental information (a form of reconnaissance) that could be used in future attacks.

Finding the Forest Among the Trees

The Duqu attacks serve as a prime example of malware evolution. For years we have observed targeted attacks, exponential growth in static malware types and propagation, and the growing "malware as a service" market. Attacks such as Duqu and Stuxnet give us a glimpse of a certain level of convergence. We do not yet know who is behind Duqu, nor do we know why its creator chose certain targets. However, we do know that this attack was carefully planned, with a great deal of diligence. Even though the security industry had many of the malware samples months prior to the attack, it was only by chance that CrySyS and a few other parties saw the connection. Once they did, we uncovered a much greater event. Just as we have learned with similar events—Stuxnet, Night Dragon, Aurora—our industry must continually watch for connections that could reveal major threats.

Shared Research Leads to Effective Defense

We have had confirmation (since November 3, 2011) that the main Duqu dropper is a malicious Microsoft Word document that exploits an unpatched vulnerability in Microsoft Windows (CVE-2011-3402). Unfortunately, we know little more. In a surprising reversal of the usual extensive cooperation

and sharing of files and other information among security vendors, the three entities that are known to have samples of the malicious Word document have yet to share those with others in the industry. Other potentially helpful pieces of information, such as file hashes, file attributes, or even a neutered, yet functional live exploit, have also not been shared. McAfee Labs and other leading security vendors believe in and support the established culture of information exchange within our industry.

Manual Mitigation and Forensics

As we have detailed, these attacks were highly targeted and only specific environments have actually experienced a live infection. If there is concern that a specific organization or environment has been targeted, there are specific steps that can be taken to confirm this. It is to our advantage that there are a very limited number of C&C servers associated with this threat. We also have specific timelines for the confirmed attacks. Some simple methods for verifying attack components are below:

- Search or mine logs for ingress and egress points for associated hostnames, IP addresses or filenames during the defined time period.
- Query for the existence of associated files on hosts.
- Simple, built-in, tools can be used to gather network-related information from hosts.
    - Netstat – monitor and collect information on active data connections
    - Ipconfig /displaydns – display and gather the DNS cache on a host.

Appendix A: Sample List

MD5	Filename	Detection	Detection Added
4541E850A228EB69FD0F0E924624B245	cmi4432.sys	PWS-Duqu!rootkit	10/16/2011
F60968908F03372D586E71D87FE795CD	nred961.sys	PWS-Duqu!rootkit	10/16/2011
0EECD17C6C215B358B7B872B74BFD800	jminet7.sys	PWS-Duqu!rootkit	10/18/2011
B4AC366E24204D821376653279CBAD86	netp191.PNF	PWS-Duqu!rootkit	10/18/2011
9749D38AE9B9DDD81B50AAD679EE87EC	keylogger.exe	PWS-Duqu.dr	9/14/2011
0A566B1616C8AFEEF214372B1A0580C7	cmi4432.pnf	PWS-Duqu!dat	10/20/2011
92AA68425401FFEDCFBA4235584AD487		PWS-Duqu	10/26/2011
C9A31EA148232B201FE7CB7DB5C75F5E	nfred965.sys	PWS-Duqu!rootkit	10/19/2011
3D83B077D32C422D6C7016B5083B9FC2	adpu321.sys	PWS-Duqu!rootkit	10/19/2011
4C804EF67168E90DA2C3DA58B60C3D16		PWS-Duqu	10/24/2011
856A13FCAE0407D83499FC9C3DD791BA		PWS-Duqu	10/26/2011
94C4EF91DFCD0C53A96FDC387F9F9C35	netp192.pnf	PWS-Duqu!dat	10/18/2011
E8D6B4DADB96DDB58775E6C85B10B6CC	cmi4464.PNF	PWS-Duqu!dat	10/18/2011
BDB562994724A35A1EC5B9E85B8E054F	iaStor451.sys	PWS-Duqu!rootkit	10/22/2011
7A331793E65863EFA5B5DA4FD5023695	iddr021.pnf	PWS-Duqu!dat	11/1/2011
9E4FBEBCC458C9C29D3D2BC8272B5B32		PWS-Duqu	11/1/2011
D101E7156C08F24AD5A2427C17EC4A03		PWS-Duqu!dat	11/1/2011
EEDCA45BD613E0D9A9E5C69122007F17		PWS-Duqu!rootkit	11/1/2011
BCA394D73015153CC18E315C0D705301	mcd9x86.sys	PWS-Duqu!rootkit	3/21/2012

Proof-of-Concept Microsoft Word documents containing exploit code that attacks CVE-2011-3402 contain strings associated with the Showtime series “Dexter.” The name of the font used in these examples is “Dexter” or “DexterRegular.” Further strings, internal to the TrueType font file, include other references to the show.

Notes on the 3/20/2012 Sample

It is important to note that the basic file data/attributes are not impervious to spoofing and other forms of obfuscation. Attributes like the compilation date, Publisher, Version, the file date can all be set and reset.

The 3/20/2012 sample (BCA394D73015153CC18E315C0D705301) was observed w/ the following attributes:

Verified: Unsigned
File date: 1:30 AM 12/9/2011
Publisher: Microsoft Corporation
Description: High changer class Driver
Product: High changer class Driver
Version: 2.1.0.14
File version: 2.1.0.14
Compilation Date: 2/23/2012

Appendix B: McAfee Countermeasures and Product Coverage

Product/Technology	Coverage	Details
AV (DAT Files)	Yes	Coverage for known, dropped, malware components is provided as PWS-Duqu, PWS-Duqu!dat, and PWS-Duqu!rootkit. Updated coverage provided for new samples in the 6656 DAT release (March 21). Coverage for malicious documents, targeting CVE-2011-3402 is provided as “Exploit-CVE2011-3402” in the 6524 DATs, released November 8, 2011.
AV (McAfee Labs Stinger Tool)	Yes	Detection for the PWS-Duqu family is available in McAfee Labs Stinger Tool - Build 20111111 or later.
HIPS/VSE (Generic Buffer Overflow Protection)	N/A	Out of scope
NIPS (McAfee Network Security Platform)	Yes	Coverage for control server–related traffic is provided via existing signature Attack ID 0x45c02300, "Invalid SSL Flow Detected.", released June 2010. Coverage for associated domains, IPs, and URLs is provided via GTI (Global Threat Intelligence). The UDS Release of November 4 provides coverage for HTTP Transmission of the malicious .DOC file.
McAfee Vulnerability Manager	Yes	The MVM release of November 2 includes a vulnerability check to determine if your systems are at risk.
McAfee Web Gateway	Yes	Coverage for known malware components is provided in the current Gateway Anti-Malware Database Update.
McAfee Remediation Manager	N/A	Out of Scope
McAfee Policy Auditor/MNAC (SCAP)	N/A	Out of Scope
McAfee Firewall Enterprise	Partial	Partial coverage for associated domains/IPs is provided in deployments running the GTI component
McAfee Application Control	Yes (malware-specific)	Runtime control of applications using Execution Control (only authorized programs can run) and Memory Protection (against remote code execution) help in protecting against this attack. The kernel-based exploitation attempt, via malicious Word Document, is out-of-scope.

McAfee Security Updates and Information Locations

- AV/DAT Files: http://mcaf.ee/df784
- Non-AV product release details: http://mcaf.ee/eab06
- McAfee Threat Intelligence Service (MTIS) Advisories: http://mcaf.ee/
- McAfee Labs – Attack: Duqu - http://mcaf.ee/6bxgh
- McAfee Labs Stinger Tool - http://mcaf.ee/0b81d

Appendix C: Industry References

McAfee	M66239
BID	50462
Microsoft	2639658
Microsoft	MS11-087
CVE	CVE-2011-3402
Secunia	SA46724
TELUS	TSL20111103-05
OSVDB	76843
US-CERT	ICS-ALERT-11-291-01E
ICS-CERT/US-CERT	JSAR-11-312-01
IBM XFDB	71073
OVAL	oval:org.mitre.oval:def:13998
Metasploit Framework	duqu_check.rb
VUPEN	2261

Appendix D: McAfee Labs Information Resources

- McAfee Labs – Attack: Duqu - http://mcaf.ee/6bxgh
- McAfee Labs Blog. http://blogs.mcafee.com/mcafee-labs
- McAfee Labs. “The Day of the Golden Jackal—The Next Tale in the Stuxnet Files: Duqu Updated” (original post). http://mcaf.ee/4fspu
- McAfee Labs. “Kernel Vulnerabilities and Zero Days: a Duqu Update.” http://mcaf.ee/cjs7x
- Podcast. McAfee’s 2-Minute Warning, November 3, 2011. http://mcaf.ee/9bjal
- McAfee Labs. “Duqu: Threat Research and Analysis” (PDF). http://mcaf.ee/orcm9
- McAfee Labs. PWS-Duqu, updated March 20, 2012. http://mcaf.ee/as304
- McAfee Labs. PWS-Duqu!dat. http://mcaf.ee/t97by
- McAfee Labs. PWS-Duqu!rootkit. http://mcaf.ee/mcrxj
- McAfee Communities. Security Awareness. http://mcaf.ee/ayjr2
- McAfee Corporate Knowledgebase. http://mcaf.ee/cgafk
- McAfee Labs Threat Intelligence. http://mcaf.ee/tc
- McAfee Trusted Source. http://www.trustedsource.org/
- Intel Security Center. http://security-center.intel.com/
- @McAfee (Twitter). https://twitter.com/#!/mcafee
- McAfee (Facebook). https://www.facebook.com/McAfee
- Podcast. McAfee AudioParasitics. http://podcasts.mcafee.com/audioparasitics/
- Podcast. McAfee’s 2-Minute Warning. http://podcasts.mcafee.com/
- Press. “McAfee: Why Duqu is a big deal.” http://mcaf.ee/xmtn1
- Press. “What Is McAfee Up To?” http://mcaf.ee/52i0o
- Press. “Duqu May Have Targeted Certificate Authorities for Encryption Keys.” http://mcaf.ee/wiqk6
- Press. “Focus 2011: McAfee and Intel Offer Defense in Depth.” http://mcaf.ee/6uzy9
- Press. “McAfee Says Duqu No Threat to Utilities.” http://mcaf.ee/nlqvu

Appendix E: Duqu Information Resources (non-McAfee)

- Microsoft. Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417). https://technet.microsoft.com/en-us/security/bulletin/ms11-087
- Microsoft Security Advisory (2639658). Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege. https://technet.microsoft.com/en-us/security/advisory/2639658
- Microsoft Knowledgebase: Microsoft Security Advisory. Vulnerability in TrueType font parsing could allow elevation of privileges. http://support.microsoft.com/kb/2639658
- CrySyS. “Duqu Dropper Discovered!” http://crysys.hu/
- Symantec. “W32.Duqu: The Precursor to Stuxnet.” http://mcaf.ee/8h71i
- Cisco. “Duqu: The Next Stuxnet?” http://mcaf.ee/ld1tw
- Microsoft. @msftsecresponse (Twitter). http://mcaf.ee/skam0
- SecurityFocus. “Microsoft Windows Kernel Word File Handling Remote Code Execution Vulnerability.” http://www.securityfocus.com/bid/50462

Acknowledgements

Special thanks to Zheng Bu, Paula Greve, Venere Guilherme, Vinay Mahadik, Stuart McClure, Peter Szor, and multiple anonymous information donors for their insight and research within this report.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors-malware, web, email, network, and vulnerabilities-McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence™. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com