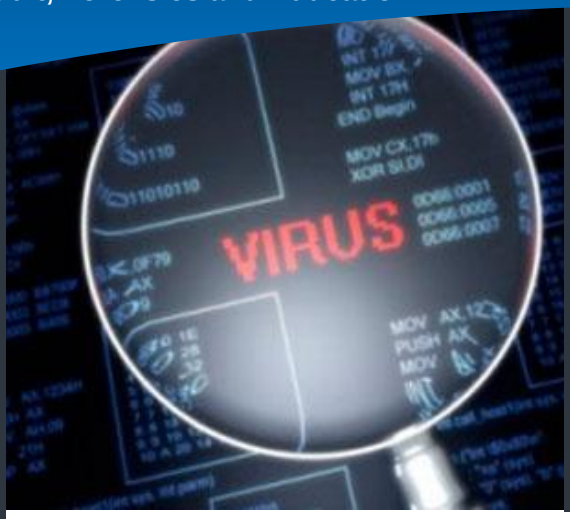
Centre for Cyber Security, Audit, Forensics and Education

School of Computing & Mathematical Sciences
UNIVERSITY of GREENWICH

Visit: http://cms1.gre.ac.uk/research/csafe



Friday, March 02, 2012 issue #1

This issue:

CSAFE News

Register for InfoSec 24-26 Aprl 2012 Earls Court, London UK

Infosecurity Europe provides free access to an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise.

Register Here for Free

CSAFE Short Courses

- Computer Forensic Evidence and the Law (Legal Aspects)
- Computer Forensics for Lawyers
- EnCase Computer Forensics 1 and 2 Certification (EnCE©)
- Introduction to Computer Forensics
- Introduction to Computer Forensics
- Penetration Testing and Vulnerability Assessment

Duqu son of Stuxnet: A new breed of Malware?

By Ryan Heartfield, CSAFE contributing writer

On October 14 2011, a research lab with strong international connections alerted Symantec to a sample malware discovered to be extremely similar to the infamous Stuxnet – named Duqu

Analysis of Duqu's code showed parts were nearly identical to Stuxnet, but with a very different purpose all together. The malware was written by the same authors or those who had access to the Stuxnet source (it was widely assumed after the discovery of Stuxnet the source code would be sold on the black market), and therefore showed that people were actively working on adapting Stuxnet for a new, sophisticated purpose identified as targeted information gathering; inconsequently Symantec personified Duqu as "essentially the precursor to a future Stuxnet-like attack".

What is "Duqu" and how does it work?

Unlike Stuxnet, Duqu contains no code related to industrial control systems and can be defined primarily as a RAT (Remote Access Trojan). The malware has no self replication capabilities and according to Symantec, the threat was highly specific – targeting a limited number of organisations for their specific assets. The details of the targeted organisations have not been disclosed.

So how does Duqu work?

The attackers used Duqu as a remote access tool to download and install an infostealer that could record keystrokes and gain other system information – further proving the attackers were searching for assets possibly to use in a future attack.

Duqu employs HTTP and HTTPS to communicate with a C&C server (command and control); from this the attackers were able to download additional executables used for information gathering and recognisance i.e. enumerating the network, keystroke logging and gathering system information. Interestingly this information is logged to a "lightly" encrypted and compressed local file which is then attempted to be "exfiltrated" out of the system.

The C&C server communication uses a custom built protocol which primarily downloads/uploads dummy JPG files; in addition data for "exfiltration" such as the encrypted log files are sent and received. Perhaps what is most interesting and important is the threats configuration to run for 36 days specifically, and then perform automatic removal from the infected system after this time. This highlights the underlying industrial espionage behind Duqu – the attackers are not simply searching for data indiscriminately... which poses the question what are they looking for?

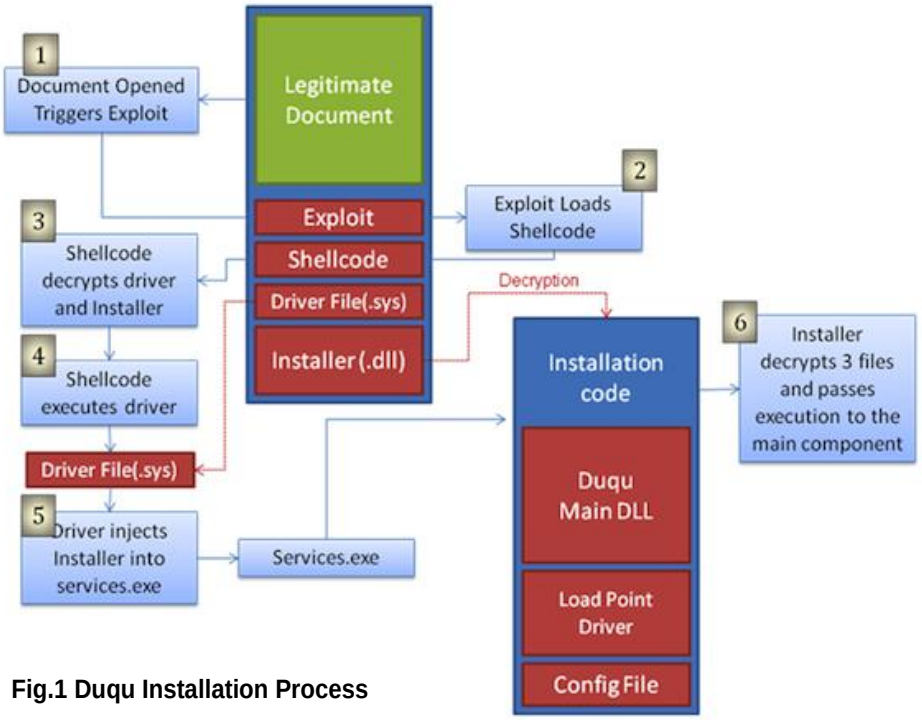


Fig.1 Duqu Installation Process

Duqu Install Process

One particular variant that Symantec were able to analyse found Duqu was delivered to the target using a specially crafted Microsoft Word document. This document contained a zero-day kernel exploit allowing execution of Duqu installation on the host computer, without user knowledge.

The word document itself arrives at the target as part of a phishing email attack; and such opening the word document attachment initiates the exploit. Duqu's installation process is highly involved and complex (see figure 1) and incorporates advanced programming techniques to minimize footprint on the target system, essentially installing drivers and injecting DLL installer processes into system services in order to load the threat on login and isolate operational footprint to running memory. For a detailed and in depth report on how the installation process works see Semantec's Duqu Whitepaper:

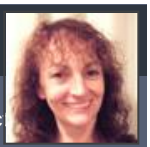
W32 Duqu: The Precursor to the next Stuxnet

What to EXPECT next?

With the arrival of Duqu in late 2011 and the relationship it holds with Stuxnet and or its original authors, it is safe to assume we have not seen that last of this threat.

Much like Conficker variants, Duqu may not be a direct strain of Stuxnet, but is definitely a recycled version of Stuxnet dedicated to a different purpose. Are Duqu's offspring around the corner and what will be their purpose? DoS, cyber warfare, industrial espionage? It would seem that Stuxnet is a landscape and a tool for which new threats are learning and adapting, whilst the security guys play catch up!"

Interview with a Security Expert – Dr Diane Gan



Q: Hi Diane, please tell us a little about yourself and your information security profile

A: I am a lecturer at the University of Greenwich and one of the founding members of C-SAFE. I teach networking, cyber security and forensics. My research interests at the moment are the threats from worms and botnets. There have been some very high profile attacks by these two types of malware in the last few years. The Stuxnet worm, which attacked nuclear power plants; the Zeus worm which targeted people's bank accounts; the Storm botnet which also gathered bank details, performed identity theft and sent out spam email; to name but a few. In the last few months Microsoft has successfully taken down Kelihos, a botnet which stole sensitive personal information and the Rustock botnet which generated mass spams. Good news.

Q: Does this mean that cyber security and forensics are good subjects to study?

A. Absolutely. There is a huge shortage of computer security and forensics professionals in industry at the moment. This means that these are very good areas to study, with good job prospec when you graduate. Also both these areas are very interesting and fast moving fields with new threats emerging all the time. For example, cloud computing relies on virtualisation and this makes security and forensics investigations very challenging. Also Microsoft will shortly be releasing Windows 8 and this will be the next challenge for computer forensics, as we have not completely finished resolving Windows 7 issues. Cyber security and forensics are areas where your job can't be outsourced to another country. The number of cyber attacks grow each week and currently show no signs of slowing down. This may be where the next war between the super-powers takes place – in cyber space.

Q: In ONE word describe the biggest security threat facing the Cloud

A: Users (the weakest link in any security)

CSAFE SEES

Predicted 2012 Security Trends

Sans Institute Security Lab

- Security Grows Up - A Niche Industry No Longer
- More Targeted Custom Malware Attacks
- ARM Hacking
- What about Secure Hardware?
- Improved Social Engineering Attacks
- Social Media
- Wireless Security Issue
- More Cloud Computing Issues
- Smartphone's

SOFTWARE

Weekly Pick "KeePass"

KeePass is a freeware password management application that provides efficient and secure database storage for password credentials using enterprise – class encryption.

KeePass solves the password management headache by consolidating multiple system credentials in a secure database accessible under one master password. With an easy-to-use, intuitive interface usernames and passwords can be organised into labelled and managed groups based on their use. High grade encryption with AES 256 bit key cipher ensures database security (Used by the American Government for encrypting up to Top Secret class data).

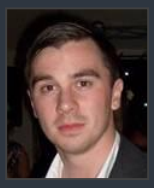
The password database files can stored anywhere such as in a portable storage i.e. USB flash drive, online storage (cloud) even within an email enabling access to the stored login credentials anywhere at any time. KeePass program is also available in a portable version for on the go access.

See: www.keepass.com for more info

About the Author

This week's author:

Ryan Heartfield



Ryan is a final year undergraduate at the University of Greenwich where he is actively involved in the collaboration of CSAFE magazine. Ryan conducts independent research in the field of information security with further potential for school sponsored projects in the near future.

Ryan also runs his own IT consultancy firm and blog providing IT solutions to small businesses.

Connect on LinkedIn:

Ryan Heartfield

CSAFE Collaborations

Why Social Networks compromise our security...

By Ryan Heartfield, CSAFE contributing writer

The inception of social networking technology has revolutionised the way we communicate and connect to each other through the internet. Social networks allow users to build their own public profiles based on their lives, interests, professions and activities which often tend to allow personal and sensitive data to be shared without adequate indication as to the security threats.

Facebook is estimated to have over 600 million user logins every day, 600 million people communicating and sharing information and data. So how did such popularity success manifest? Most of us have seen the film "The Social Network" – Facebook was not designed with security in mind but usability and essence of the "cool" fun factor it provided. In its inception Facebook was not concerned about security but rather attracting as many people as possible, which is probably true for its lesser counterparts such as Bebo and other social network giants like Twitter and LinkedIn. Therefore users where not warned of the risks of uploading personal information and data such as videos and pictures. However these are aspects of your life that are meaningful to you and could quite possibly be to someone else as well: criminals looking to take advantage of your or your information to their own end!

Is that picture of you and your dog "fluffy", publically available on Facebook making you vulnerable?

"Username: kate@hotmail.com
Password: ... fluffy? fluffy123, fluffy_123, fluffy345..."

It is important to consider how the information uploaded on a social network can be used against you for malicious purposes. Identity fraud is a big issue on the internet, by having details such as home address, contract number, email address and data of birth can pose a serious risk to your security. Coupled with a few good, full face profile pictures identity thieves have a pretty good profile of you to work with!

The most concerning issue? Social Networking sites encourage this type of information sharing to "Connect" with friends and for targeted advertising – always enforce the tightest security settings available on social network service you use; protect yourself and be cynical, or safe at least!