STM JOURNALS

Journal of
Telecommunication, Switching Systems and Networks

ISSN: 2454-6372
Volume 11, Issue 3, 2024
September–December
DOI (Journal): 10.37591/JoTSSN

https://journals.stmjournals.com/jotssn

Review JoTSSN

Exploring the Connection: Analyzing the Relationship Between Duqu and Stuxnet

Rushikesh Ravindra Adsule[1,*], Asra Sadaf[2]

Abstract

Malware computer worms like Stuxnet and Duqu have the ability to take down any computer system in the globe. Although they are extremely similar to one another, Duqu is superior to Stuxnet. Because it comes in two versions, Duqu 1.0 and 2.0, it is also more harmful and dangerous than Stuxnet. The first malware attack to garner international attention was Stuxnet, which was designed to physically harm industrial infrastructure that seemed to be cut off from the internet. The malware known as Stuxnet was discovered in 2010 by the Belarusian antivirus company VirusBlokAda. This discovery marked the first time that a cyber weapon had ever been reported globally. Duqu and Stuxnet are two of the most sophisticated and notorious pieces of malware to have emerged in recent years. Both are believed to be state-sponsored cyber weapons made for some specific purposes, with Stuxnet designed mainly to target Iran's nuclear program and Duqu being associated with espionage activities in different countries. This paper is used to provide a comparative analysis of Stuxnet and Duqu and examining their origins, functionalities, propagation method, and impacts on cybersecurity. These two malwares not only impacted some computer network but also caused huge losses to many industries in different countries. This paper examines the lessons learned from analyzing these sophisticated threats and the measures taken by organizations and governments to defend against similar cyber weapons in the future.

Keywords: Duqu, Stuxnet, espionage, zero-day vulnerabilities, cybersecurity

INTRODUCTION

In June 2010, the Stuxnet malware marked the beginning of a new era in the cybersecurity arms race. For the first time in history, a targeted cyberattack designed to physically damage parts of the nation's critical infrastructure had been discovered. The most intriguing malware in recent memory is Stuxnet, which has been the subject of analysis by hundreds of security specialists and coverage by thousands of media. The primary reason for the high visibility is targeted attacks against known, real-world industrial targets, which were previously considered a thought experiment. Although experts discussed the potential for such a sophisticated attack, Stuxnet made the effects of cyberattacks on vital infrastructure more widely known [1]. It turns out that there are other viruses of this kind than Stuxnet.

The malware research community's continued efforts, combined with increased awareness and understanding, have led to the discovery of several new targeted attacks that are somehow connected to Stuxnet. In October 2011, The CrySyS Labs in Budapest, Hungary discovered Duqu, a malware very similar to Stuxnet, but with clearly different targets.

***Author for Correspondence**
Rushikesh Ravindra Adsule
E-mail: rushikeshadsule2016@gmail.com

[1]Student, Jawahar Education Society A.C. Patil College of Engineering, Department of Computer Science Engineering (IOT and Cybersecurity including Blockchain), University of Mumbai, Kharghar, Maharashtra, India
[2]Professor, Jawahar Education Society A.C. Patil College of Engineering, Department of Computer Science Engineering (IOT and Cybersecurity including Blockchain), University of Mumbai, Kharghar, Maharashtra, India

Received Date: August 05, 2024
Accepted Date: August 12, 2024
Published Date: September 05, 2024

Citation: Rushikesh Ravindra Adsule, Asra Sadaf. Exploring the Connection: Analyzing the Relationship Between Duqu and Stuxnet. Journal of Telecommunication, Switching Systems and Networks. 2024; 11(3): 11–17p.

Incidentally, Stuxnet and Duqu are part of the same family of malware, but Duqu itself has two versions: Duqu 1.0 and 2.0.

- *Duqu 1.0:* It is a highly modular and stealthy malware platform capable of stealing sensitive information, including intellectual property and confidential documents.
- *Duqu 2.0:* It had advanced espionage capabilities, including the ability to monitor and exfiltrate sensitive data from compromised systems, as well as to conduct remote surveillance and reconnaissance.

There are many other types of malware like Flame and Gauss, which were also created to do cyber espionage attacks [2]. Flame is also one of the destructive malware similar to Stuxnet and Duqu which also had a zero-day vulnerabilities that is a threat to cyber security and can be responsible to cyber war in the future also. Most people agree that the United States and Israel worked together to create Stuxnet, primarily with the intention of undermining Iran's nuclear program. While some people think that Unit 8200 of the Israel Defense Forces' Israeli Intelligence Corps, which is in charge of covert operations, gathering signal intelligence (SIGINT) and code decryption, intelligence and cryptography, counterintelligence, cyberwarfare weaponry, military intelligence, and surveillance, is the group that created Duqu. Due to the many similarities between Stuxnet and Duqu, it is believed that the creator of both malware is the same person [3]. Working of Stuxnet is shown in Figure 1.

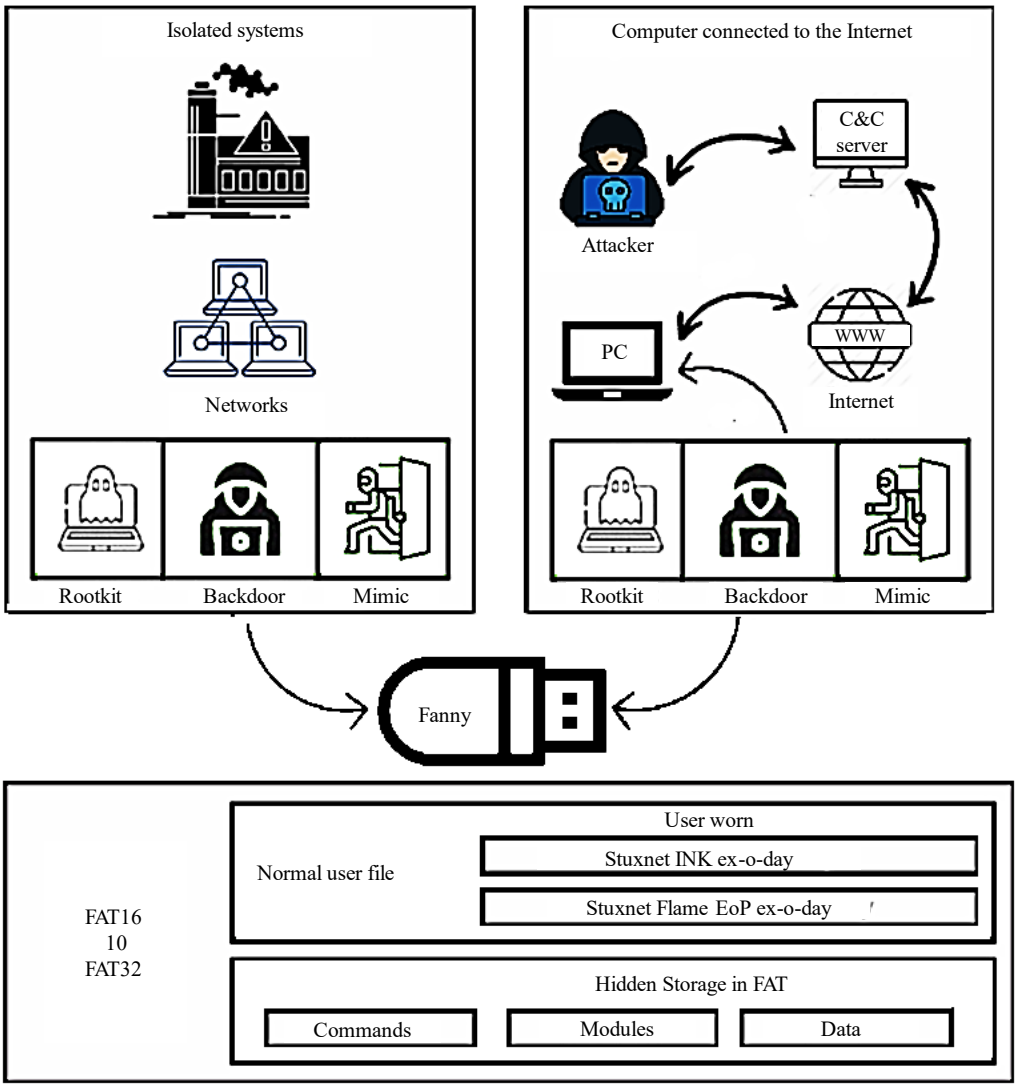

Figure 1. Working of Stuxnet [4].

Stuxnet can be spread on the system connected to the internet or also an isolated system can be attacked by using some external storage devices like pen drives, etc. In the Iran nuclear program cyberattack, Stuxnet was uploaded in the system from a pen drive by some person.

The computer worm Stuxnet propagates using detachable storage devices, like USB memory sticks and computers. The worm automatically copies itself to any USB drive connected to an infected computer, then infects any other computers to which the USB drive is subsequently connected. The worm exploits a previously unknown zero-day vulnerability in the Windows operating system to jump between computers. The spreading of Stuxnet is shown in Figure 2.

The term "zero day" refers to when the vendor or developer has just learned about the bug, which means they have a "zero day" to fix it. When a hacker takes advantage of a vulnerability before a developer has a chance to address it, it is known as a zero-day assault. Zero-day vulnerability is shown in Figure 3.

REVIEW OF LITERATURE

Cyberattacks are studied within the theoretical framework of Marie Kaldor's Old and New Wars, and cases are analyzed from the perspective of conventional and modern warfare. Stuxnet was the first cyberattack to be conducted with complete secrecy for an extended period of time, physically destroying targets while hiding any evidence that could lead to the malware. Stuxnet's importance lies not only in its sophisticated capabilities but also in its chosen target, Iran's nuclear enrichment program.

The cyberattack makes one wonder how vulnerable and unsecure the world is in these kinds of circumstances. However, if we do not comprehend the nature of such attacks, it is challenging to both anticipate and defend against them. Judging from Stuxnet's goals, participants, and methods, cyberattacks clearly contain characteristics of old and new wars [4].

Over the past year, Duqu's propagation strategies and payload have been thoroughly examined, and it has been claimed that Duqu and Stuxnet share some functions. We concentrate on the drivers Duqu employs when an infection occurs. We recreate the driver's source code and examine the techniques it employs to carry out the payload covertly as part of our reverse engineering effort. The driver was then changed to a protective version that could recognize injections in Windows binaries, stopping additional attacks. We specifically show how Duqu's modified driver would have detected Duqu [5].

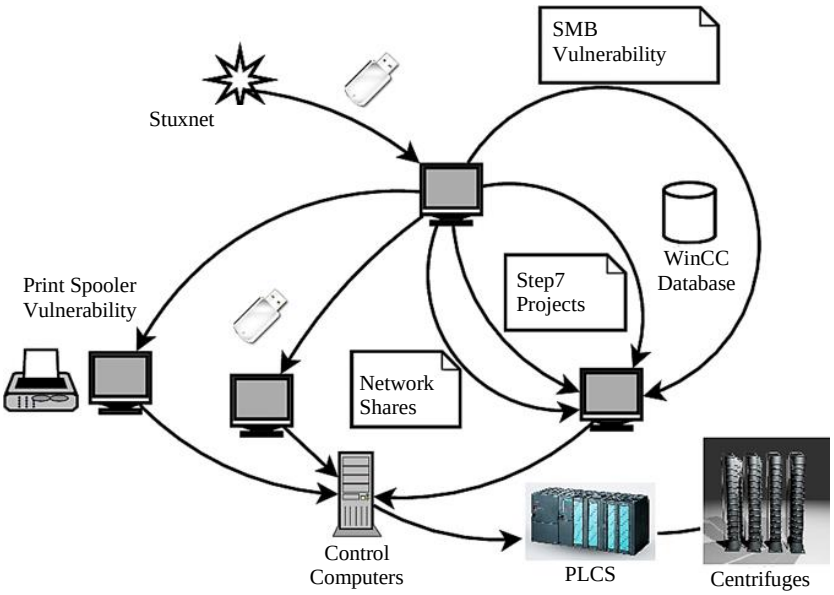

Figure 2. Spreading of Stuxnet [6].

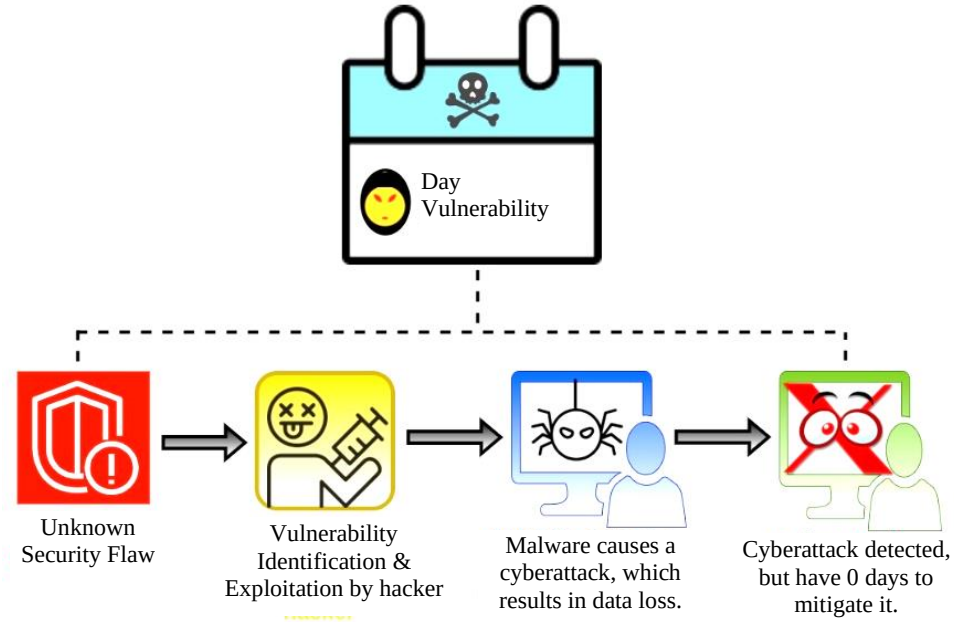

Figure 3. Zero-day vulnerability [7].

OBJECTIVE

The main aim of this paper is to present a comprehensive study on the architectural framework, propagation strategies, functionalities, and origins of the malware Stuxnet and Duqu. Additionally, it is vital to explore another important aspect related to these threats, which is the effect they can have on international and national institutions [8].

The virus, in the form of Stuxnet, moved from one USB to another and then infected the Microsoft Windows operating system that had been installed on personal computers. It inspected each of the computers that it had already infected to see if there was any sign of SIMATIC Step 7 software because it is this software that is used by industrial PCs serving as PLCs (programmable logic controllers) for automation and supervision purposes in electro-mechanical devices. After identifying the PLC computer, the worm updated its code via internet channels and started sending damage-inducing instructions to control electro-mechanical equipment through the PC while providing false feedback from the main controller at the same time. Monitoring the equipment from the beginning would not have identified any signs of a problem until the equipment itself was destroyed by its internal mechanism. Based on the Stuxnet code, Duqu was intended to record the keystrokes of users and harvest information from industrial facilities. This was supposed to serve as a later threat. A study from 2017 revealed that the invisible, fileless malware has become commonplace and is now present in 40 countries on at least 140 institutions, including banks, governmental organizations, and telecommunication companies. Once a computer with malware is rebooted, the malware will change its name, which will make it difficult for digital experts to find any remnants of the malware. The bank's security team did not identify it until they discovered a copy of Meterpreter in the actual memory of a Microsoft domain controller.

Researchers discovered that the Meterpreter code was loaded and inserted into memory via PowerShell statements [6]. One intriguing aspect of Duqu's C&C architecture was the utilization of a potential zero-day vulnerability associated with OpenSSH 4.3 that would have taken control of new servers. The research associated with the salvaged log files from the Duqu C&C servers that were deleted by their owners revealed that immediately following the hacking of each C&C server, the hacker would upgrade OpenSSH from version 4.3 to the current version (5.8). Some theorize that the practice of updating OpenSSH is intended to remediate the vulnerability that was used to hack the server in the first place in order to prevent someone else from taking over control of a hacked server. The presence

of this OpenSSH vulnerability has not been documented, so many scientists believe that the owners of Duqu simply forged the SSH accounts of the servers they accessed. Also, the owners of Duqu seemed to have a preference for the Linux distribution CentOS 5.x; this could have been accidental or they had a way to circumvent the security features of CentOS 5.x [9–11].

Additionally, the majority of the C&C communications software in Duqu was written in a previously unidentified programming language that was significantly different from the programming language used in other Duqu modules. Duqu's mystery language was finally identified after dedicated research efforts were crowd-sourced. Researchers had the assistance of various individuals. They concluded that Duqu's "mystery language" was a unique version of the C programming language called OO C (object-oriented C) that had custom additions and was compiled with the Microsoft Visual Studio Compiler. This anomalous utilization of OO C in comparison to a more common language like C++ to write parts of Duqu is another indication that suggests that the individuals who developed Duqu (and Stuxnet) have significant expertise, are funded, and are probably backed by a country. Both of these malwares have a zero-day vulnerability [7, 8].

Comparison Table: Comparison between Stuxnet and Duqu. is shown in Table 1.

RESEARCH METHODOLOGY

As our objective was to do research on Stuxnet and Duqu, we gathered data from various online sources like research papers, Wikipedia pages and also from some YouTube channels. We also mentioned some important points in the paper. There is also comparison between Stuxnet and Duqu also there are other versions of Duqu which are more dangerous than Stuxnet. And the important part of this research is to provide the detailed information on this malware.

DISCUSSION

Technical Capabilities

Different versions of Stuxnet employ different approaches to doing this: recent versions utilize a Windows LNK vulnerability, while older versions utilize an autorun.inf file vulnerability.

Table 1. Comparison between Stuxnet and Duqu.

Parameter	Stuxnet	Duqu
Purpose	Was designed to sabotage Iran’s nuclear program	Primarily a reconnaissance tool used for getting sensitive information from targeted system
Propagation	Spread through infected USB drives and network shares	Spread through targeted phishing emails and exploits
Modularity	Highly complex and self-contained	Modular design allowed for customization and adaptation to different environments
Detection	Stuxnet was discovered in June 2010 by VirusBlokAda, a security firm from Belarus, on systems in Iran	Duqu was discovered on September 1, 2011 by the Laboratory of Cryptography and System Security (CrySyS Lab) of Budapest University of Technology and Economics in Hungary
Stealth and persistence	It used valid digital certificates and rootkit functionalities to conceal its presence	It used advanced stealth mechanisms to evade detection, such as encryption and anti-analysis techniques
Codebase and development	Written in multiple programming languages, including C and C++	Shared some components and techniques with Stuxnet, but Duqu had a more modular and adaptable architecture
Attribution	Widely attributed to a joint effort by the United States and Israel, although neither government officially confirmed their involvement	While believed to be created by the same entities responsible for stuxnet, but with no official confirmation from any government
Impact	Caused significant damage to Iran’s nuclear program, delaying its progress	Primarily focused on information gathering and reconnaissance

LNK Weakness (CVE-2010-2568)

Stuxnet will code to an infected computer with Windows that, when inserted into it, will replicate Stuxnet to the drive. Interestingly, a previous copy of Stuxnet on the external drive will be erased if the drive has already infected three computers.

Autorun.inf file

An autorun.inf file is a file that causes Windows to automatically play a file on removable media when the media is inserted into the computer. Older versions of Stuxnet would place an autorun.inf file on flash drives that are inserted into a computer that is infected.

Stuxnet is able to self-update from infected Step7 project. If an infected Step7 project is opened and the Stuxnet version is newer than the version already on the machine, the version on the machine will be updated. A remote procedure call (RPC) server that is waiting for a connection powers each Stuxnet copy.

Using Zero-Day Vulnerability

Like Duqu, Stuxnet took advantage of several zero-day vulnerabilities that were previously unknown software flaws to infect systems.

Propagation: Stuxnet has the ability to spread through USB flash drives and local networks, as well as the internet.

Rootkit

Stuxnet uses rootkit techniques to hide itself on infected systems, which makes it hard to detect and remove.

Modular Design

Stuxnet was modular in design, consisting of multiple components that worked together to carry out its objectives. This modular architecture allowed it to be highly adaptable and capable of targeting specific systems.

Advanced Payloads

Stuxnet and Duqu contained highly advanced payloads designed to sabotage the targets. They employed sophisticated techniques to evade detection and cause physical damage to the targeted systems.

Self-Replication and Self-Propagation

Stuxnet and Duqu had the ability to self-replicate and spread autonomously, without requiring manual intervention. This allowed it to rapidly infect multiple systems within a network.

Stealthy Operation

Stuxnet was designed to operate stealthily, remaining undetected for an extended period to maximize its impact. To evade detection by analysis tools and security software, it used a variety of evasion strategies.

Advanced Code Injection Techniques

Duqu is capable of injecting its malicious code into legitimate processes to evade detection by antivirus software and other security measures.

Data exfiltration: Duqu is capable of stealing sensitive data from the compromised system, including documents, credentials, and other valuable information.

Persistence Mechanisms

Duqu employs various techniques to maintain persistence on the compromised system, including creating startup entries, installing rootkits, and using stealthy fileless malware techniques.

Encryption and Obfuscation

Duqu encrypts its communication with C&C servers and employs obfuscation techniques to make analysis and detection more difficult for security researchers.

CONCLUSION

Stuxnet, a highly sophisticated malware, is believed to have been developed by one or more nations, possibly Israel and/or the United States. Although it spread globally, its primary focus was Iran, particularly Natanz where it activated its payload. Had it not been detected by security researchers, Stuxnet could have caused even greater damage. It is estimated that around 1000 centrifuges were destroyed, causing a delay in Iran's nuclear weapon program. However, the impact may not have been as significant as its creators had anticipated. The emergence of Stuxnet has raised awareness about the vulnerability of industrial control systems, which have not been frequently targeted. As a result, efforts to strengthen these systems against attacks are expected to increase over time, although this must be weighed against the heightened risk of such attacks.

In this paper we have provided a concise analysis of Duqu. Our findings indicate a strong connection between Duqu and the notorious Stuxnet worm. Duqu was widely recognized as a highly sophisticated form of malware. Furthermore, our investigation demonstrates that the malware was meticulously crafted. Interestingly, it is commonly understood that intricate systems can be vulnerable. Typically, this observation is made from the defender's perspective, as complex infrastructures offer numerous entry points for malware. However, in this case, the argument is reversed: it was the malware itself that exhibited fragility, and we capitalized on this weakness to manipulate it for our own objectives.

REFERENCES

1. Denning DE. Stuxnet: what has changed? Future Internet. 2012; 4 (3): 672–687.
2. Maynard P, McLaughlin K, Sezer S. Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. J Cybersecurity. 2020; 6 (1): tyaa020.
3. Bencsáth B, Pék G, Buttyán L, Félegyházi M. The cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet. 2012; 4 (4): 971–1003.
4. Langner R. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. 1st Edition. Arlington, VA, USA: Langner Communications; 2013.
5. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. 1st Edition. New York, NY, USA: Crown Publishers; 2014.
6. Kushner D. The Real Story of Stuxnet: The Cyberweapons Program That Took Down Iran’s Nuclear Program. 1st Edition. San Francisco, CA, USA: New Press; 2013.
7. Bencsáth B, Pék G, Buttyán L, Félegyházi M. Duqu: analysis, detection, and lessons learned. In: Sadeghi A-R, editor. Proceedings of the ACM Conference on Computer and Communications Security (CCS 2012). October 16–18, 2012. Raleigh, NC, USA. ACM Press; 2012. pp. 749–762.
8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security. Plasil F, Stal M, editors. In: Proceedings of the 37th International Conference on Software Engineering (ICSE 2011), May 21–28, 2011, Honolulu, HI, USA. Berlin, Germany: Springer; 2011. pp. 149–152.
9. Falliere N, Murchu LO, Chien E. W32. Stuxnet dossier. In: Proceedings of the Virus Bulletin Conference. September 29–October 1, 2010. Vancouver, BC, Canada. Oxford, UK: Virus Bulletin Ltd.; 2010. pp. 7-22.
10. Lindsay JR. Stuxnet and the limits of cyber warfare. Security Stud. 2013; 22 (3): 365–404.
11. Sari A, Atasoy UC. Taxonomy of cyber attack weapons, defense strategies, and cyber war incidents. In: Sari A, editor. Applying Methods of Scientific Inquiry into Intelligence, Security, and Counterterrorism. Hershey, PA, USA: IGI Global; 2019.pp. 1–45.

