Digital Forensics

2021SM_CS_6419_FRE1A

Final Project:
Background Research

Prepared by:
Mohammadali Rahnama

Student number:
3709515

EST. 1785
UNB
UNIVERSITY OF NEW BRUNSWICK

TABLE OF CONTENTS

INTRODUCTION

Zusy malware is a banking Trojan that uses man-in-the-middle attacks to steal bank information. It is a spin-off of the well-known Zeus banking Trojan and is where Zusy takes its name. Zusy (also known as TinyBanker, Tinba, and Zegost) is a malicious piece of malware that is used to steal not only money but also personal information. Regardless of its name or size, it packs a powerful punch. It is critical to have a dependable endpoint anti-malware solution in place to protect your computer from infections like Zusy.

Zusy malware variants have been around for a long time. Zusy's early incarnations were in the form of adware. According to researchers, later versions of Zusy have been updated with a spyware component used to steal information from businesses.

The original version of Zusy works by injecting itself into Windows processes such as.explorer.exe and winver.exe, so that when victims of the malware visit a financial services website, a bogus form appears, tricking them into submitting personal information. The newer Zusy variant, on the other hand, can infect a user's device simply by hovering over a hyperlink in an infected PowerPoint document. The user does not even need to click on the link for the malware to execute – a simple mouse hover over it will suffice. The PowerPoint attachment is frequently distributed via spam emails with subject lines such as "Order Confirmation" or "Purchase Order Number."

In addition, newer versions of Zusy can steal information by spying on webcams and turn your computer into a zombie machine controlled by the cybercriminal. Furthermore, when compared to other malware, Zusy malware is quite small, making it difficult to detect once it has infected a device. However, Zusy's small size has no bearing on the amount of damage it is capable of inflicting.

Office Macros are small pieces of code written in Visual Basic (VBA) that allow you to perform specific repetitive tasks. They are useful in and of themselves, but malware writers frequently exploit this functionality to introduce malware into your computer system.

A Macro virus is a virus that exploits Macros that run in Microsoft Office applications such as Word, PowerPoint, and Excel. Cybercriminals send you a macro-infested payload or a file that will later download a malicious script via email, with a subject line that entices or provokes you to open the document. When you open the document, a macro is launched to carry out whatever task the criminal has set for himself.

SUMMARY OF THE FIRST PAPER

Paper title: “From ZeuS to Zitmo: Trends in Banking Malware” [1].

The ZeuS botnet has moved from PCs to mobile devices, focusing on online banking. DroidDream is a mobile botnet-based malware that debuted in 2011. IKee.B is a malicious programme that infects jailbroken iPhones. AnserverBot is a sophisticated new Android malware that goes by the name AnserverBot. Malware attaches itself to common applications, sends bogus SMS messages, and engages in social engineering. The only defence is to completely reset the iPhone and restore all settings to factory defaults.

ZitMo is a cutting-edge example of mobile malware. The ZeuS botnet has moved from PCs to mobile devices, focusing on online banking. It is designed to steal mobile transaction authorization numbers (mTAN) sent by banks using social engineering techniques.

Bmaster infects mobile phones using a variety of exploits and Trojan applications. The only defence is to completely reset the iPhone and restore all settings to factory defaults.

AnserverBot installs a backdoor in order to infect mobile phones and steal sensitive data. The malware attaches itself to standard applications, sends bogus SMS messages, and employs social engineering techniques.

SUMMARY OF THE SECOND PAPER

Paper title: “Highly resilient peer-to-peer botnets are here: An analysis of Gameover Zeus” [2]

Gameover ZeuS (GOZ) is a variant of the ZeuS Trojan. It is based on a peer-to-peer botnet infrastructure that is more difficult to detect and neutralise. The Zbot variant includes a new C&C server that cybercriminals can use. In the underground market, centralised ZeuS variants are available as builder kits. SpyEye, Ice IX, and Gameover ZeUS are among those that can be easily removed from a user's device. These tools can be used by cybercriminals to target specific institutions or businesses.

The primary functions of the Zeus P2P network are to facilitate the exchange of binary and configuration updates among bots and to propagate lists of proxy bots. Zeus prefers to push peer list updates; when a bot receives a message from another bot, it adds that other bot to its local peer list if it has fewer than 50 peers. The Zeus P2P network is not a Distributed hash table and has nothing in common with Kademlia.

If a Zeus bot discovers that all of its neighbors are unresponsive, it attempts to reconnect to the network by contacting the peers on its hardcoded peer list. If this also fails, the bot switches to a backup channel, from which it can retrieve a new peer list if necessary.

SUMMARY OF THE THIRD PAPER

Paper title: “On the analysis of the Zeus botnet crimeware toolkit” [3]

Many banks in many countries now allow customers to access their accounts via the Internet. Mobile platforms have provided an additional channel for online banking, but with these advancements, financial services have become vulnerable to new types of online attack. ZeuS botnets have been found to be responsible for 44% of online malware infections during financial transactions and approximately 90% of global banking fraud.

During the years 2009 and 2010, approximately 3.6 million computers in the United States were infected with ZeuS.

ZeuS is the most significant financial malware created so far and there is little evidence that its impact is fading. Attacks are still occurring and may increase as cybercriminals develop more sophisticated concealment and evasion techniques. The scope of threat from ZeuS and its derivatives has been growing.

In the underground community, Zeus crimeware toolkit v. is regarded as the most recent stable publicly available version. The Zeus botnet aims to make machines act as spying agents in order to gain financial benefits. Email addresses, passwords, online banking accounts, credit card numbers, and transaction authentication numbers can all be found in stolen data. This section describes the network communication that takes place between the C&C server and an infected machine. IDS rules and anti-virus detection routines can be written using network analysis.

SUMMARY OF THE FOURTH PAPER

Paper title: “Titans’ revenge: Detecting Zeus via its own flaws” [4]

The monetary loss caused by cybercrime has recently been estimated to be more than one hundred billion dollars. Computer virus/malware incidents have been linked to 54% of these crimes. Because of its sophisticated methods of stealing banking credentials, the Zeus malware has been dubbed the world's most notorious banking malware.

This paper provides a thorough overview of the Zeus malware family. They propose a method for obtaining the keystream used by a specific malware (Zeus) to encrypt its payload. This enables further identification of Zeus malicious traffic within a computer network. The keystream extraction technique does not rely on static analysis to find the encryption key (which is usually obfuscated in the executable), but instead analyses network traffic generated by the infected computer. They also present Cronus, an intrusion detection system (IDS) capable of detecting the malicious botnet, i.e. both the C&C and its bots, using only a few bytes of the previously discovered key.

The Dorothy Framework is designed to analyse, track, and visualise a botnet in a highly automated manner. Holz et al. developed a method for tracking and observing botnets using honeypot technologies. Caballero et al. proposed a tool that uses the binary code reuse technique to extract code fragments from malware encryption/decryption routines and then uses them to decrypt malicious communication traffic. They focused on defaming botnet toolkits with the goal of discouraging or prosecuting botnets.

SUMMARY OF THE FIFTH PAPER

Paper title: “Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware” [5]

Malware is used to commit online payment fraud, which costs millions of Euros each year. Around 15% of domains attract 90% of attacks, but domain size does not predict attack intensity. The code similarity between attacks is well over 90%, implying code sharing, selling, or stealing among attackers.

As web-based online banking platforms have grown in popularity over the last few decades, so has online banking fraud. The European Central Bank recently published fraud statistics for the Single European Payment Area, which totaled approximately €800 million (roughly $1.1 billion). In 2012, the United Kingdom reported a total loss of approximately €299 million due to CNP--fraud (FFA UK, 2013) This paper's main contribution is to improve our understanding of the underground economy surrounding malware--based financial fraud. It also lays the groundwork for future research into the interactions between financial service providers' and attackers' security tradeoffs.

Every year, financial malware on home computers and mobile devices causes millions of Euros in losses. Why are some financial service providers more frequently targeted than others? There has been very little comparative empirical research across providers and countries to identify the factors that influence the choice of financial services as targets. Regardless of the length of the attack code, code attacks to the same URL are more than 90% similar. Code is re--used to an astonishing degree: only 1% of the inject code is never repeated, and 226 different inject codes are repeated over 1000 times.

REFERENCES

[1] N. Etaher, G. R. S. Weir, and M. Alazab, “From ZeuS to Zitmo: Trends in Banking Malware,” in 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, vol. 1, pp. 1386–1391, doi: 10.1109/Trustcom.2015.535.

[2] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, “Highly resilient peer-to-peer botnets are here: An analysis of Gameover Zeus,” 2013, pp. 116–123, doi: 10.1109/MALWARE.2013.6703693.

[3] H. Binsalleeh et al., “On the analysis of the Zeus botnet crimeware toolkit,” in 2010 Eighth International Conference on Privacy, Security and Trust, 2010, pp. 31–38, doi: 10.1109/PST.2010.5593240.

[4] M. Riccardi, R. Di Pietro, M. Palanques, and J. A. Vila, “Titans’ revenge: Detecting Zeus via its own flaws,” Comput. Networks, vol. 57, no. 2, pp. 422–435, 2013, doi: https://doi.org/10.1016/j.comnet.2012.06.023.

[5] S. T. Tajalizadehkhoob, H. Asghari, C. Gañán, and M. J. G. Van Eeten, “Why them? Extracting intelligence about target selection from Zeus financial malware,” 2014.