Analysis of Sasser Malware:
A Case Study of Destructive Complications
From a Virtual World

for
Professor Janece Glauser
School of Arts and Humanities
The University of Texas at Dallas
Dallas, Texas

by
Zen Park
ECS 3390.016 Student

October 25, 2020

Table of Contents

Figures and Tables

Abstract

It did not take even 20 minutes for Sasser to infect the world, just right after its illegal release on May 1, 2004. By scanning every IP address publicly available across the globe at the time, Sasser sent packets which caused each infected computer to constantly shut down without any way to cancel it. Internet speeds have significantly dropped. Important financial institutions, government organizations, universities [7], hospitals are just a few of the infected names where disasters have occurred. The release of Sasser was a crime, which gave many blessings and detriments towards the world's stance on cybersecurity, which will be covered throughout this paper.

Introduction

1.1 What is Malware?

Malware is a general term for the universal set of viruses, trojans, rootkits, worms, and the like. In other words, a virus would be a very specific type of malware. Malware is often designed with a certain goal in mind. These programs are often made to generate data, which often leads to big influxes of money laundering [3]. Ever since Sasser, which was said to be one of the state-of-the-art malwares of its age, criminals learned from this malware to create even much more sophisticated malware.

1.2 History of Malware

Malware started off as simple coding pranks. These were often created to demonstrate the ability of a coder. As more and more people started learning about malware, more and more coders have started to appear. Eventually, some people saw opportunities to make money by creating such software. These led to criminal activity, and very sophisticated organizations which focused on illegal activity [2]. Sasser was eventually developed by 18-year-old Sven Jaschan from Germany, who developed this malware as a prank.

1.3 Significance of Sasser

Stuxnet is notorious for the damage it caused in 2010. It is very possible that Stuxnet was inspired from Sasser, which caused the largest international disaster caused by malware by the time. During Sasser's domination in 2003, the world was at Sasser's mercy as majority of computers used Windows at the time [3]. Sasser also showed many people how one person can significantly impact the world, and many criminals learned from this situation [5].

Discussion

2.1 Details of Sasser Malware

2.1.1 What Sasser Accomplished

Sasser accomplished exactly what it wanted. Although Sasser was developed as a malicious prank, the implications it caused were enormous. By targeting a computer's LSASS (Local Security Authority Subsystem Service) executable, Windows operating system would panic, causing a force shutdown [1]. The computer's CPU would easily reach max speeds, which greatly slowed down every process inside the computer; thus, rendering the computer unusable.

2.1.2 Where Sasser Targeted

Sasser was meant to be a minor prank. It was never supposed to affect the entire world – yet it did. By scanning for vulnerable IP addresses, Sasser would split into A, B, C, or D parts to increase efficiency [1]. Afterwards, Sasser would leave a text document containing the IP addresses of nearby vulnerable computers. Just like a domino effect, once a computer gets

infected, more computers get infected as well. Those infected computers would eventually infect even more computers furthermore. The process continued infinitely, until the entire globe was infected.

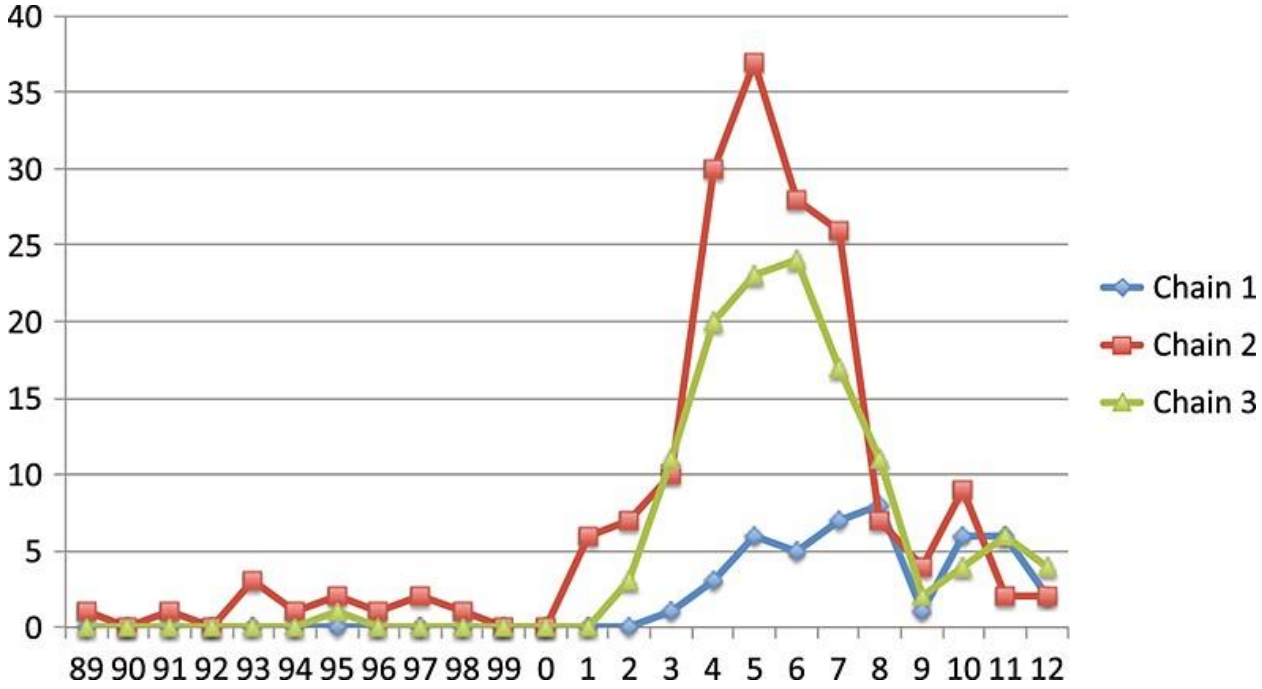

Table 1 shows different versions of Sasser can quickly infect many computers in a very short time. After reaching its peak, solutions to protect computers against Sasser started to increase, which explains the decrease. [9]

2.1.3 Who Sasser Hurt the Most

As the globe was infected, Sasser was the pandemic of the computing world. Police stations, hospital equipment, government computers, servers, and many more were all affected by Sasser. Because Sasser was very quick, there was virtually no one who could escape the grasps of the malware. In 2004, many parts of the world used computers in one way or another.

2.1.4 Methods Sasser Uses to Infiltrate Systems

As stated above, Sasser attacks the Windows process called LSASS. In fact, Sasser was named after this process. Because majority of computers in 2004 did not have firewall nor any antivirus installed, Sasser very easily targeted and attacked these computers [2]. To give a comparison, it would be the same as a person leaving his house's door open in a busy city such as Los Angeles, which some people may take gladly take advantage of this situation.

Figure 1 above shows what a typical computer looked like after recovering from Sasser's attacks. [10]

2.1.5 Dangers of Weak Security

In 2004, cybersecurity was not taken seriously at all. Many businesses had their ports open, which allowed virtually everybody to connect to gain access to their confidential information. Having information leaked through a computer was virtually unheard of. This is the reason why many business computers did not have firewall protection, nor did they use any antivirus software [2]. Because of Sasser and similar malware, many important documents and files had been lost [5]. This caused a major setback for many businesses which relied on computers with weak security.

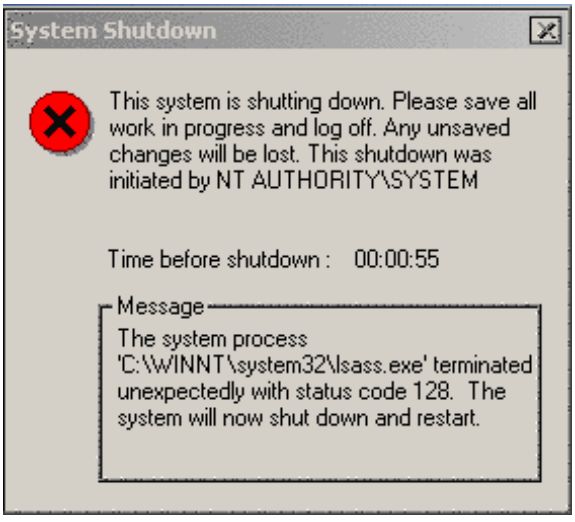

Figure 2 shows the error message caused when Sasser attacked the LSASS process. [11]

2.2 Studies from Sasser

2.2.1 How Sasser Could Have Been Prevented

Sasser could have been easily prevented if people took the threat of online security seriously. Because the internet was still a foreign concept for most computer owners in 2004, most users chose to be ignorant. A simple firewall or even an outdated antivirus would have protected computers from contracting with Sasser. The lack of proper communication also served an important role [4]. The government was slow to respond, and Sasser had done significant damage by the time the malware had achieved its goal.

2.2.2 Significant Advancement in Cybersecurity Because of Sasser

Today, cybersecurity is a well-respected field with appetizing offers for those who can choose its career. This field of computer science would not have been as appealing today if the world had not experienced past threats of computer security and malware. Whether it is a blessing or curse that security had to be amped to protect the world from online threats, this is a discussion for another topic. Sasser's imminent threat caused significant rise to the mentality of cybersecurity necessity.

2.2.3 The Benefit of Society from a Failure

Expanding from the previous point, Sasser benefited society in many ways. There was always the threat of even more dangerous malware aside from Sasser. Fortunately, Sasser was created as a prank. However, if an organized criminal organization took advantage of the world's online naivety, circumstances would have been far, far worse. Sasser helped prepare the world for the upcoming battle against destructive malware.

2.2.4 The Detriment of Society from a Failure

Some people view a water-filled cup as half-full. However, there are those who view that cup as half-empty. Just as a coin has two side, there are clear detriments as a result of Sasser, rather than just positive effects. Sasser had and has influenced many more criminal behaviors because of the ingenuity of its concept [5]. As we can see below in Table 1, there has been significant increase in the number of malwares after Sasser's career.

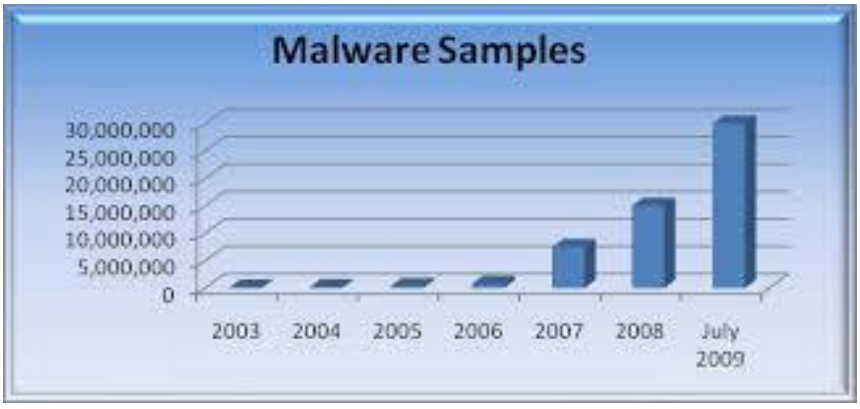

Table 2 shows the data of the amount of malware researched from Panda Antivirus. [12]

2.2.5 How Sasser Can Protect People (The World After Sasser)

The question about whether Sasser has helped the world or made it worse will always be up for debate amongst modern philosophers. However, there is no doubt that we can have confidence in many security solutions offered today, such as cloud security, mail encryption, voice call encryption – just to name a few. Time-to-time, there are instances of breaches where information is stolen. However, there are always active developers who work hard each day to protect our information and security [5]. Nearly every single business and organization today use some form of cybersecurity, completely different the world in 2004.

2.3 Modern Tips for Dealing with Modern Sassers

2.3.1 Effective Methods of Protecting Oneself

There is no shame in not being tech savvy, even in the modern age of technological advances. What matters most is the willingness to always learn. To protect oneself if Sasser were to reappear today, there are just two simple steps which must be followed. One is to activate the latest firewall, which Windows often comes preconfigured with. Never allow any software you do not know about to bypass firewall [8]. Two is to install an antivirus software you trust. The next section will discuss how to choose the best software.

2.3.2 Effective Cybersecurity Software Recommendations

One of the best and free antimalware software available for everyone is Malwarebytes.

There is joke which goes around the online community that the best and most effective antivirus software is common sense. However, many people have differing values, because not all common sense can be equal. Online common sense would be remaining vigilant, and not executing just any file that is found online [8]. By using personal and intelligent judgment, a person would be able to avoid finding themselves in bad situations.

2.3.3 Brief Overview of Protection in Progress

Malware often bypasses protection by obfuscating itself through various methods. One is to act like a trojan horse, which means to bundle itself with a regular software, then attack the computer once the user starts using the innocuous program [6]. Next is to delay the time when the malware activates to several hours or even days before attacking, so the malware does not get flagged from the antivirus software. To counteract these bypasses, antimalware software will often go through updates to help users defend themselves against loophole attacks.

Conclusion

3.1 Summary

In 2004 when Sasser spawned into this world, no one could have predicted how dangerous one single program could be. Ever since Sasser, the world started taking security much more seriously. Even if Sasser would not have existed, other malware very similar to Sasser or much

worse would have come as the harbinger of internet terror. Rather than lamenting over the pain and stress caused by Sasser, it is best that the world's community learn to protect themselves from such destructive malware.

3.2 Lessons Learned

Sasser hit when people's guards were down. Because security was taken very lightly, Sasser attacked using very simple yet clever methods. The lesson to learn here is to take basic precaution for any sort of computing activity, and to always protect oneself by turning on firewall and activating a trusted antimalware software. By following this advice, the prospect of getting attacked by Sasser in today's era would deem near impossible.

References

[1] M. Hyppönen, *The History and the Evolution of Computer Viruses*. Las Vegas, Nevada: DEF CON, 2011. Available: https://archive.org/details/DEFCON_19_The_History_and_the_Evolution_of_Computer_Viruses (Accessed: 11 September 2020).

[2] M. R. Faghani, *Effects of security solutions on worm propagation*. Isfahan University of Technology, Isfahan, Iran, 2008. Available: https://ieeexplore.ieee.org/abstract/document/4651266/authors#authors (Accessed: 14 October 2020).

[3] C. Zou, *Advanced Routing Worm and Its Security Challenges*. Orlando, Florida, 2006. Available https://doi.org/10.1177%2F0037549706065344 (Accessed: 14 October 2020).

[4] Microsoft, *Microsoft Security Bulletin MS04-011 – Critical Security Update for Microsoft Windows (835732)*. 2004. Available: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2004/ms04-011 (Accessed: 14 October 2020).

[5] National Vulnerability Database, *CVE-2003-0533 Detail*. MITRE, 2004. Available: https://nvd.nist.gov/vuln/detail/CVE-2003-0533 (Accessed: 14 October 2020).

[6] Common Vulnerabilities and Exposures, *CVE-2003-0533*. 2003. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533 (Accessed: 14 October 2020).

[7] Carnegie Mellon University, *The History and the Evolution of Computer Viruses*. Pittsburgh, Pennsylvania, 2004. Available: https://www.kb.cert.org/vuls/id/753212 (Accessed: 14 October 2020).

[8] G. Eschelbeck, *The Laws of Vulnerabilities: Which security vulnerabilities really matter?*. Information Security Technical Report, Volume 10, Issue 4, pp. 213-219, Elsevier, USA, 2005. Available: https://www.sciencedirect.com/science/article/abs/pii/S1363412705000646 (Accessed: 14 October 2020).

[9] A. Rey, *Mathematical modeling of the propagation of malware: a review*. 2015. Available: https://doi.org/10.1002/sec.1186 (Accessed: 25 October 2020).

[10] E. Bott, *Ten years of Windows malware and Microsoft's security response*. 2012. Available: https://www.zdnet.com/pictures/ten-years-of-windows-malware-and-microsofts-security-response/6/ (Accessed: 25 October 2020).

[11] F-Secure, *Net-Worm:W32/Sasser*. Available: https://www.f-secure.com/v-descs/sasser.shtml (Accessed: 25 October 2020).

[12] S. Correll, *The Business of Rogueware: Analysis of the New Style of Online Fraud*. 2009. Available:

https://www.pandasecurity.com/img/enc/The%20Business%20of%20Rogueware.pdf (Accessed: 25 October 2020).