MVP

Computer worms

Contents

Introduction 3
Overview of the malware 3
History 3
Technical 4
Summary 4
References 5

Introduction

A computer worm is a malware program which has the defining feature of self-replication, it can use its host to replicate itself, spread to, and infect, other machines. It also does not require user interaction and functions as an independent program, without need of a host [2]. This makes the worm a highly insidious actor, whose impact can rise exponentially [1].

Overview of the malware

- Rarity:
  Worms remain actively developed and deployed; users are at risk.

- Risk:
  A worm can be stopped by a competent anti-virus, anti-malware software. However, zero-day exploits are still possible as in all cases. Worms are also increasingly malicious, early experimental worms spread over machines and potentially performed some operations on the host OS. Now, worms are likely contain a payload of malware .

  Malicious emails or texts, network vulnerabilities and file-sharing all present vectors for the transmission of a worm. And these are the general categories the worm can be grouped under: Email, IM/ IRC, Network and P2P worms [7].

- Impact:
  Worms may or may not contain a payload, even without one, they almost invariably cause harm to a network by consuming bandwidth and resources. A primary use of worms is the creation of botnets for other malicious purposes such as DDoSing.

History

The first worm was developed in in 1971 and was dubbed ‘Creeper’, and propagated across ARPANET, an early computer network ancestor of the modern internet, which was operated by the U.S Department of Defence. It was a proof of concept for a program which self-replicated and spread to other computers. It contained no malicious software, but printed out the message ‘I'M THE CREEPER : CATCH ME IF YOU CAN’ on teletype machines [3].

The second worm, ‘Reaper’, developed the following year, is considered the first anti-virus software as it was propagated across ARPANET to erase the original Creeper program [3].

The Morris worm is a famous early example, originating from Robert Tappan Morris, a computer science student. His worm infected approximately 10% of all computers connected to the internet at that time, and he became the first person charged with the 1986 Computer Fraud and Abuse Act. [4] The damages incurred from this incident may reach into the millions of USD [4].

A significant example from 2000 illustrating the harm of worms is ILOVEYOU. Written in VBScript and spread via malicious emails, it first copied itself to the Windows system directory, then added itself

to the registry, and altered the homepage of the Internet Explorer browser to link to a binary, if this is run, it established persistence upon restart. The program is a Trojan and begins scanning the IE instance for cached passwords to phone home with. It then attempted to spread itself via IRC and Outlook [5].

It was found to have originated in the Philippines and believed to have infected approximately 10% of internet connected computers, estimated to have caused ~10Bn USD in damages [6].

The 2017 extremely damaging WannaCry ransomware was spread via worm [8].

Stuxnet was spread via a highly intricate computer worm [9].

Technical

TBC

Summary

TBC

References

[1]

J.-Y. Marion, “From Turing machines to computer viruses,” Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 370, no. 1971, pp. 3319–3339, Jul. 2012, doi: https://doi.org/10.1098/rsta.2011.0332

[2]

C. Zhang, S. Zhou, and B. M. Chain, “Hybrid Epidemics—A Case Study on Computer Worm Conficker,” PLOS ONE, vol. 10, no. 5, p. e0127478, May 2015, doi: https://doi.org/10.1371/journal.pone.0127478.

[3]

T. Chen and J.-M. Robert, “The Evolution of Viruses and Worms.” Available: https://ivanlef0u.fr/repo/madchat/vxdevl/papers/avers/statmethods2004.pdf

[4]

Federal Bureau of Investigation, “Morris Worm,” Federal Bureau of Investigation. https://www.fbi.gov/history/famous-cases/morris-worm

[5]

“What is the ILOVEYOU worm, what does it do, and how do I detect and remove it?,” kb.iu.edu. https://kb.iu.edu/d/aioe

[6]

E. Root, “ILOVEYOU: the virus that loved everyone,” www.kaspersky.com, Aug. 08, 2022. https://www.kaspersky.com/blog/cybersecurity-history-iloveyou/45001/

[7]

“Kaspersky Threats — Worm,” threats.kaspersky.com. https://threats.kaspersky.com/en/class/Worm/

[8]

Microsoft Corporation, “Ransom:Win32/WannaCrypt threat description - Microsoft Security Intelligence,” Microsoft.com, 2017. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom%3AWin32%2FWannaCrypt (accessed Aug. 13, 2023).

[9]

“Stuxnet explained: What it is, who created it and how it works,” www.kaspersky.com, Apr. 19, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet