MVP

Computer worms

Contents

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 (Zhang, Zhou and Chain, 2015). This makes the worm a highly insidious actor, with an impact that can rise exponentially (Marion, 2012).

Overview of the malware

- Rarity:
  Worms are a broad category of malware, and their rarity is difficult to establish.

- 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 (Pratama and Rafrastara, 2012). 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, which conducts identity theft, extort victims for ransom, compromises their credentials etc. Malicious emails or texts, network vulnerabilities and file-sharing all present vectors for the transmission of a worm. And these are the categories the worm can be grouped under in terms of dissemination method: Email, IM (instant message), Network and P2P worms (Kaspersky, n.d.).

- 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 (Pratama and Rafrastara, 2012). Worms are deployed primarily due to their capability to infect high volumes of vulnerable hosts. The worm concept also obfuscates the origin of the attack, making backtrack challenging due to the indirect nature of the release. These factors combined contribute to the hazard of the worm as malware, it is able to infect vast amounts of hosts quickly, act independently and carry extremely harmful payload (Pratama and Rafrastara, 2012).

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 connected teletype machines (Chen and Robert, n.d.).

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 (Chen and Robert, n.d.).

The Morris worm is a famous early example, originating from Robert Tappan Morris, a computer science student at Cornell University. 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 (Federal Bureau of Investigation, n.d.). The damages incurred from this incident may have reached into the millions of USD (Federal Bureau of Investigation, n.d.).

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 (kb.iu.edu, n.d.). 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 (Root, 2022). This demonstrates the potential scope of successful attacks.

The 2017, extremely damaging WannaCry ransomware was spread via worm. It infected upwards of 300,000 hosts worldwide, across 150 countries and resulted in significant damage to sectors across the global economy including manufacturing, healthcare, telecommunications and public services. It was spread after confidential NSA backdoors(EternalBlue and DoublePulsar) were leaked by hackers (Akbanov, Vassilakis and Logothetis, 2019).

The infamous Stuxnet was a highly intricate computer worm developed by Israel and the USA (Kaspersky, 2023). This worm was mostly harmless, but targeted specific programmable logic controllers used to automate industrial processes. It was employed as a cyberweapon against Iran which resulted in the destruction of ~1000 centrifuges in the Natanz nuclear facility, part of Iran's nuclear energy program. It did so by fluctuating the operating speed of the machines to induce vibration and failure. It was also able to cross 'air gaps' by infecting removable storage devices, enabling it to hop from the public internet to disconnected systems (Kelley, 2013).

Technical

Worms are a broad family of malware, therefore a specific technical analysis is not possible, but general characteristics of worms do exist. A worm can be comprised of up to five components, with the 1st being the only critical. Others extend the functionality of the malware and allow it to exploit a system further, phone-home and establish persistence (Pratama and Rafrastara, 2012).

1) Infection propagation

This is a critical task which involves the distribution of the worm to vulnerable hosts. This enables the following four to take effect.

2) Remote control and update interface

This may or may not be present, but some worms exhibit the ability to be remotely controlled and updated. Some worms may attempt to reach a server, whose response or lack thereof can act as a killswitch.

3) Life-cycle manager

Here, the control over the worms existence is defined, some are pre-programmed to self terminate after fulfilling certain objectives, others attempt to prolong their existence by exploiting further vulnerabilities and others exhibit a static runtime.

4) Payload

This is component does not relate to the function of propagation. Rather it is the contents, possibly other malware, the worm delivers to the infected host.

5) Self-tracking

Worms may 'phone-home' with updates on their progress, sending information via the internet back to their developers with telemetry.

Again, the worm is a generic malware template, and thus, many techniques and exploits exist to fulfil its objectives. However, four key stages of its life cycle can be identified as common to all (Pratama and Rafrastara, 2012).

A) Target acquisition, which can be accomplished by scanning the internet, this can be done in a random or targeted fashion. Random searches may try known IP addresses or attempt to generate their own.

   Other worms may have a pre-ordained target list baked in, or the program may generate one for itself unique to each instance of the worm.

   Yet other worms may wait for a user to connect to a compromised host, at this point the malware infects the user. This approach is favourable as contrasted with other techniques it does not present active signals in attempting to infect victims. No unusual activity will be registered by an ID+PS.

B) Target space, this was touched on in Overview: Risk. This defines the scope of how a worm propagates, via the internet is a given, most make direct connects over TCP/IP in an attempt to propogate but others attempt to spread by email, P2P services or IM.

C) Propagation method, the worm's mechanism for carrying itself to hosts is defined. It may send itself as a part of the infection process, or it may send a component of itself which allows for further exploitation by opening more channels of communication with the system targeting the victim.

D) Activation method, effectively, this is the technique the worm takes advantage of to turn itself from passive to active. This may be caused by human interaction, such as executing the local instance of the program, possibly influenced by social engineering. It may also trigger when a user performs some action unrelated, but it used as a signal for activation nonetheless. The worm may also automatically through scheduled processes.

Summary

Worms are a broad category, often contrasted with computer viruses and Trojans as distinct family of malware with a variety genera and species beneath this classification. They are the template for perhaps the most sophisticated single artefact of software known to exist, Stuxnet. The historical examples provided illustrate the potential impact of a competent worm being deployed via the internet, how it can damage individuals, organisations and countries.

The basic concept of a worm as malware is one of the earliest and most prolific examples of a malware family, which has had wide ranging impacts on culture, the economy and computer security. Their extremely desirable and powerful properties mean that they are likely to remain relevant, studied and actively developed by hackers for the foreseeable future.

References

Marion, J.-Y. (2012). From Turing machines to computer viruses. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 370(1971), pp.3319–3339. doi:https://doi.org/10.1098/rsta.2011.0332.

(Marion, 2012)

Zhang, C., Zhou, S. and Chain, B.M. (2015). Hybrid Epidemics—A Case Study on Computer Worm Conficker. PLOS ONE, 10(5), p.e0127478. doi:https://doi.org/10.1371/journal.pone.0127478.

(Zhang, Zhou and Chain, 2015)

Chen, T. and Robert, J.-M. (n.d.). The Evolution of Viruses and Worms.

(Chen and Robert, n.d.)

Federal Bureau of Investigation. (n.d.) Morris Worm. fbi.gov/history

(Federal Bureau of Investigation, n.d.)

kb.iu.edu. (n.d.). What is the ILOVEYOU worm, what does it do, and how do I detect and remove it?

(kb.iu.edu, n.d.)

Root, E. (2022). ILOVEYOU: the virus that loved everyone.

(Root, 2022)

Kaspersky. (n.d.). Kaspersky Threats — Worm.

(Kaspersky, n.d.)

“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

Kaspersky. (2023). Stuxnet explained: What it is, who created it and how it works.

(Kaspersky, 2023)

Pratama, A. and Rafrastara, F.A. (2012). Computer Worm Classification. (IJCSIS) International Journal of Computer Science and Information Security, 10(4).

(Pratama and Rafrastara, 2012)

Kelley, M.B. (2013). The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought.

(Kelley, 2013)

Akbanov, M., Vassilakis, V.G. and Logothetis, M.D. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journal of Telecommunications and Information Technology, 1(1), pp.113–124. doi:https://doi.org/10.26636/jtit.2019.130218.

(Akbanov, Vassilakis and Logothetis, 2019)