


## Chapter 13

# Evolution of Malware in the Digital Transformation Age

Shahid Alam

 <https://orcid.org/0000-0002-4080-8042>

Adana Alparsalan Turkes Science and Technology University, Turkey

### ABSTRACT

*As corporations are stepping into the new digital transformation age and adopting leading-edge technologies such as cloud, mobile, and big data, it becomes crucial for them to contemplate the risks and rewards of this adoption. At the same time, the new wave of malware attacks is posing a severe impediment in implementing these technologies. This chapter discusses some of the complications, challenges, and issues plaguing current malware analysis and detection techniques. Some of the key challenges discussed are automation, native code, obfuscations, morphing, and anti-reverse engineering. Solutions and recommendations are provided to solve some of these challenges. To stimulate further research in this thriving area, the authors highlight some promising future research directions. The authors believe that this chapter provides an auspicious basis for future researchers who intend to know more about the evolution of malware and will act as a motivation for enhancing the current and developing the new techniques for malware analysis and detection.*

### INTRODUCTION

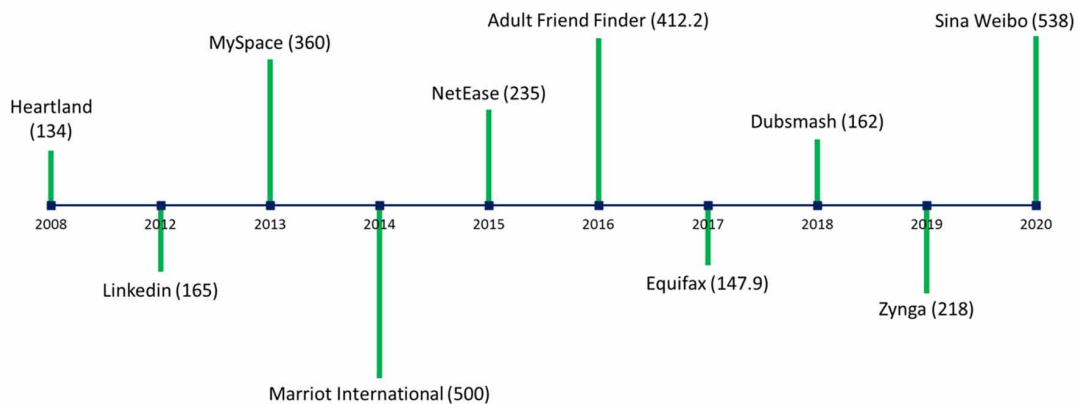
As we are advancing into the new digital transformation age, most of the enterprises have been adapting to this new pace of technology by adopting leading-edge technologies like cloud, mobile, big data, and the Internet of things. At the same time, organizations are facing a new wave of security attacks, which are posing a severe impediment in implementing these technologies. WannaCry ransomware attack in 2017 affected many leading organizations around the globe. The ransomware was a CryptoWorm (used cryptography to design the malicious software) (Zouave et al., 2020) and targeted Microsoft Windows operating system by encrypting the data and demanding ransom payments in the CryptoCurrency (Narayanan et al., 2016). Within a day the ransomware infected more than 230,000 computers in over 150 countries. Stuxnet, malware (malicious software), was used to cause substantial damage to supervisory

DOI: 10.4018/978-1-7998-6975-7.ch013

## Evolution of Malware in the Digital Transformation Age

control and data acquisition systems. Targeting industrial control systems, the malware infected over 200,000 computers. Shamoon, another similar malware, was used for cyber warfare against some of the national oil companies in the middle east. Recently, Twitter got hacked where hackers were able to steal US high profile accounts, and Magellan Health, a Fortune 500 company, faced a sophisticated ransomware attack that affected thousands of patients. Cyberattacks are on the rise and pose a serious threat to a company's financial and other resources. A chronological timeline of such and other high-profile cybersecurity attacks on different companies is shown in Figure 1. As we can see from Figure 1 the number of breaches (break into an account to steal information, including passwords, banking, etc.) of user accounts of a company range from 134 million accounts in the year 2008 – 538 million accounts in the year 2020. The average cost of a malware attack on a company is 2.4 million USD. These attacks highlight the vulnerabilities of the current cyberinfrastructure. They also emphasize the importance of the integration of cybersecurity as part of the new scenario for digital transformation.

*Figure 1. A chronological timeline of high-profile cybersecurity attacks from 2008 to 2020 with affected accounts in millions*



Most of the cyberattacks are executed by installing malware that carries out different malicious activities. According to a recent report by AV-TEST, an independent IT security institute, the total number of new malicious programs are on the rise. The malware growth reported by AV-TEST is shown in Figure 2. As we can see from Figure 2, the number of malware programs grew from 65.26 million in the year 2011 – 1101.88 million in the year 2020. This shows a significant growth (almost 16 times) in the number of malware programs in these ten years. The numbers can be explained by the fact, that initially, malware writers were hobbyists but now the professionals have become part of this group because of the incentives attached to it, such as financial gains, intelligence gathering, and cyber warfare, etc. Moreover, the malware writers are adopting reusable software development methodologies, and also using obfuscation (Linn & Debray, 2003) to create new malware that is a copy (variant) of the original malware. Malware has also grown in sophistication, from a simple file infection virus to programs that can propagate through networks, can change their shape and structure (polymorphic and metamorphic malware) with a variety of complex modules to execute malicious activities. Malware writers have also adapted to new platforms, such as smartphones and IoTs, etc. The research in the defense and analysis

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/evolution-of-malware-in-the-digital-transformation-age/284155](http://www.igi-global.com/chapter/evolution-of-malware-in-the-digital-transformation-age/284155)

## Related Content

---

### Achieving a Security Culture

Adéle Da Veiga (2022). *Research Anthology on Business Aspects of Cybersecurity* (pp. 233-261).

[www.irma-international.org/chapter/achieving-a-security-culture/288681](http://www.irma-international.org/chapter/achieving-a-security-culture/288681)

### Contemporary Financial Risk Management Perceptions and Practices of Small-Sized Chinese Businesses

Simon S. Gao, Serge Orealand Jane Zhang (2014). *International Journal of Risk and Contingency Management* (pp. 31-42).

[www.irma-international.org/article/contemporary-financial-risk-management-perceptions-and-practices-of-small-sized-chinese-businesses/115817](http://www.irma-international.org/article/contemporary-financial-risk-management-perceptions-and-practices-of-small-sized-chinese-businesses/115817)

### Emerging Technologies in a Modern Competitive Scenario: Understanding the Panorama for Security and Privacy Requirements

George Leal Jamiland Alexis Rocha da Silva (2021). *Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy* (pp. 1-16).

[www.irma-international.org/chapter/emerging-technologies-in-a-modern-competitive-scenario/271768](http://www.irma-international.org/chapter/emerging-technologies-in-a-modern-competitive-scenario/271768)

### A Decision Support System for Privacy Compliance

Siani Pearsonand Tomas Sander (2012). *Threats, Countermeasures, and Advances in Applied Information Security* (pp. 158-180).

[www.irma-international.org/chapter/decision-support-system-privacy-compliance/65767](http://www.irma-international.org/chapter/decision-support-system-privacy-compliance/65767)

### Open Project Planner

Kenneth David Strang (2012). *International Journal of Risk and Contingency Management* (pp. 58-61).

[www.irma-international.org/article/open-project-planner/67376](http://www.irma-international.org/article/open-project-planner/67376)