



# WHAT IS

WHITEPAPER

# RANSOMWARE?



# *Table of Contents*

03

What is Ransomware?

---

04

History of Ransomware

---

05

Spread & Infection

---

06

Detection

---

07

Prevention

---

08

CITATIONS

---





# WHAT IS RANSOMWARE?

There are two types of ransomware. One is a form of malware that encrypts files and requires a ransom payment for decryption capabilities. The other is called a 'locker' that locks users out of their devices.



# HISTORY OF RANSOMWARE

The history of today's ransomware variants goes back to 1989, when individuals that attended the World Health Organization's AIDS conference were sent compromised diskettes containing a trojan that encrypted files and requested payment.<sup>3</sup> However, the use of ransomware only started to become mainstream in 2012. In September 2013, the identification of **CryptoLocker** re-introduced a far more dangerous encryption software used by adversaries.<sup>1</sup>

The use of CryptoLocker, and the many variants, have since extorted millions of dollars from organizations around the world.<sup>1</sup> 2017 was a pivotal year in ransomware. Threat actors used NSA tools to propagate **WannaCry**. It was estimated to have affected more than 200,000 computers across 150 countries.<sup>2</sup> Total damages from WannaCry ranged from hundreds of millions to billions of US dollars.<sup>3</sup>





# SPREAD & INFECTION

---

Infection is typically accomplished through exposed extraneous services that have weak or no credentials, successful email phishing campaigns against employees, and/or unpatched devices used to browse the internet.

The compromise of an initial device would lead to various malicious activity that could include additional phishing to internal targets, compromise of sensitive data (i.e. PHI, PII, etc.), or immediate spread and infection of the ransomware variant. Spreading throughout the environment may be performed by various means (including but not limited to): known user compromised accounts (administrative level permissions), cracked credential hashes of administrative users, network and operating system misconfigurations, open network shares, etc.

Once the adversary has identified means of lateral movement, they will install and prep the execution of ransomware on as many systems as possible. As variants have increased in capabilities and complexity, the installation process has moved from writing to disk to execution only in memory. The latest variants seek out backups and attempt to remove any chance of recovery short of paying the ransom.



# DETECTION

The use of end-point protection solutions, in conjunction with 24/7 monitoring, will provide organizations with an initial identification of ransomware.




Additional capabilities around identification of compromised devices or user accounts before ransomware is able to be installed, spread, and activated may be possible.



# PREVENTION

Many common security practices that can help with the protection against ransomware:

- 
- Patch management process with regular updates
  - (Air-gapped) Sensitive data backups
  - Multi-factor authentication for remote & externally facing applications
  - Regular reviews of firewalls and services
  - Not allowing RDP from the internet
  - End-point protection solution
  - 24/7 monitoring & alerting
  - Training end users on secure internet & email use
  - Removing local admin access to users
  - Using least privilege principles



# CITATIONS

---

- <https://www.malwarebytes.com/ransomware/><sup>1</sup>
- <https://www.us-cert.gov/ncas/alerts/TA13-309A><sup>2</sup>
- <https://blog.radware.com/security/2018/10/origin-of-ransomware/><sup>3</sup>



[tpx.com/cybersecurity](https://tpx.com/cybersecurity)

