



Threat **STOP**

The Ultimate Ransomware Guide

for Higher Education Institutions



TABLE OF CONTENTS

03	Introduction to Ransomware
04	Infection Vectors
05	Extortion and Payment Methods
06	Evolution: Before CryptoLocker
07	CryptoLocker - The Game Changer
08	Evolution: After CryptoLocker
09	Then and Now: Ransomware Trends
10	Famous Attacks
11	The Price of Ransomware
12	Prevention and Protection
13	Blocking Ransomware
14	About ThreatSTOP

What Is Ransomware?

Ransomware is a type of malware that prevents victims from accessing their data, and then threatens to publish or perpetually block access to it unless a ransom is paid. The first ransomware attack occurred in 1989, though the malware type became a threat to look out for only in the mid 2000's. Today, ransomware is one of the most prominent, dangerous cyber threats. What started out as a simple malware that locks up a few folders on the victim's computer has evolved into a cyber beast that is being used to handicap enterprises, shut down global production lines, halt IoT and medical devices, and extort enormous sums of money. In this whitepaper, we will review the evolution of this widely successful threat, and explain how to prevent ransomware infections.

Crypto vs. Locker

Crypto Ransomware

Cryptographic ransomware encrypts files on the victim's device, blocking them from accessing the files and demanding a ransom in order to decrypt them.



Locker Ransomware

Locker ransomware locks the victim out of their device, and then demands a ransom in order to restore access to the device and data.



INFECTION VECTORS



EMAIL

Ransomware is spread via email in two main ways: emails with malicious links that redirect the victim to a ransomware download, or emails containing malicious attachments, whether it be executables that download the malware, or Office files with macro exploits that ignite the ransomware download.



PROGRAMS

Some seemingly-legitimate programs are later revealed to be malicious applications, whose sole purpose is to download ransomware. In other cases, legitimate programs may be exploited and bundled together with ransomware.



COMPROMISED WEBSITES

Websites that have been hacked by cyber attackers can be laced with ransomware. The attackers implant ransomware on the compromised web page, causing visitors to unknowingly download the ransomware.



MALICIOUS ADVERTISEMENTS

Third party ads are a common sight on most websites, making it easy for attackers to insert malicious advertisements that redirect victims to ransomware downloads.



EXPLOIT KITS

Used in drive-by-downloads, EKs are a collection of known vulnerabilities packed together to exploit the victim's machine and serve malware. Today, EK's are used to serve many strains of ransomware.



RDP ACCESS

Hackers exploit the Remote Desktop Protocol (RDP) by brute-forcing credentials through relevant ports, purchasing credentials from breach sites or phishing for them through target victims. After hacking the target network, attackers will install ransomware.

EXTORTION & PAYMENT

Extortion Methods

After ransomware has compromised a victim's machine, and locked or encrypted their data, it's time for the attackers to ask for money. Over time, ransomware threat actors have used the following extortion tactics:



Ransom Note

Pay up or else!



Law Enforcement Notice

Pay up or face charges!



Decryption Tool

Buy our decryption tool!

Payment Options

The form through which attackers ask for payment has varied greatly over time and between different ransomware variants. In their ransom note, attackers would give victims one or more of the following options:

1

Calling or Texting

Attackers ask victims to call or text a "free" number regarding the problem that caused their data to be blocked, while the number is actually a premium rate number. This method is no longer in use today.

3

Prepaid cards and vouchers

Another uncommon method today, ransom notes would demand victims to buy prepaid cards such as gift cards, and send the codes to the attackers.

2

Wire Transfer

An old method that is no longer in use, attackers would ask for a wire transfer, or sometimes even a credit card payment.

4

Cryptocurrency

By far the most popular method today. These payments can reach over a million dollars.

EVOLUTION - B.C.

(BEFORE CRYPTOLOCKER)

The first ransomware variant was spotted in 1989, and ever since, this notorious threat has become drastically more sophisticated and prevalent. Our Ransomware Evolution Timeline examines important ransomware variants of the last 30 years, from before the infamous CryptoLocker ransomware unleashed its wrath in 2013, to where it is today, and the evolution between.

AIDS Trojan

1989

The first ransomware was handed out on floppy disks at an AIDS conference. The ransomware hid directories and encrypted the names of all files on drive C, then asked for \$189.



2006

MayArchive

Archived certain file types and deleted the original copy. As payment, MayArchive forced victims to buy products from "recommended" websites.

TROJ.RANSOM.A

This ransomware boasted a "gangster" ransom note, showing pornographic images and threatening to delete files every 30 minutes if the ransom is not paid.

Archiveus

Archiveus locked up everything in the My Documents folder with a 30-digit password. To obtain the password, victims needed to complete a purchase at an online pharmacy.

2011

Unnamed Locker

This locker displayed a warning for a fraudulent Windows license, telling victims to call a "free" number which was actually premium.

Reveton

Reveton informed users that their machine had been used to download copyright material or child pornography and demanded a payment of a "fine".

WinLock

2010

This ransomware spammed victims with pornography and asked them to send a \$10 premium-rate SMS. The WinLock attackers made \$16 million in one year, but then got caught and sent to jail.



CRYPTOLOCKER: THE GAME CHANGER

In 2013, a ransomware variant named **CryptoLocker emerged** in the wild. This variant was so much stronger than its predecessors, that it completely changed the ransomware realm and the cybersecurity industry's conception of ransomware as a threat.

CryptoLocker was the first ransomware to make big news outside the cyber realm. It had stronger encryption, using a RSA 2048-bit key, and much better file encryption coverage - it encrypted locally connected, network-attached, or cloud-based storage, a wider variety of file extensions, as well as mapped drives, DropBox files and more. CryptoLocker also used Domain Generated Algorithms (DGAs) to dynamically and randomly assign domains to their Command and Control (C&C) servers. Since the control domains were constantly changing, it became difficult to take the operation down. To assure steady profits, the ransomware even had a customer support service, making sure that every victim received the help needed in carrying out the ransom payment.

After CryptoLocker, a wave of advanced, evasive and effective ransomware variants hit the cyber threat landscape. Evolving from simple Locker malware asking for a couple hundred dollars, ransomware has become one of the biggest (and most expensive) threats to watch out for.

CryptoLocker's Fate: Operation Tovar

In 2014, a joint operation by the FBI, Interpol, and various security companies succeeded in taking down the Gameover Zeus botnet and seizing CryptoLocker's C&C servers. The FBI has been on the search for the man behind the ransomware, Evgeniy Bogachev, for years, and they are offering \$3 million as a reward for information on his whereabouts. At its peak, the reward stood at a whopping \$4.6 million.

EVOLUTION - A.C. (AFTER CRYPTOLOCKER)

TeslaCrypt

2015

A famous CryptoLocker copycat, the threat actors made a small fortune before surprisingly publicly releasing the ransomware's public key.

SamSam

This ransomware specializes in targeted attacks, hitting large entities from hospitals to city municipalities, and more.



WannaCry

2017

This high-class ransomware cryptoworm used the famous EternalBlue exploit to propagate in victim networks. The WannaCry attacks in 2017 caused havoc around the world, spreading to over 150 countries and causing worldwide financial losses of over \$4 billion.

NetWalker

2019

NetWalker is tailored for targeted attacks, and has compromised organizations in various industries, including government, healthcare and higher education.

Sodinokibi

This ransomware is famous for its advanced evasion capabilities, and an affiliate program that allows the ransomware to spread widely and efficiently.

2016

Locky

This sophisticated variant created a vast public fear of ransomware in 2016, infecting victims in both mass campaigns and successful targeted attacks.

Jigsaw

Jigsaw ransomware, which boasted one of the creepiest ransom notes, was the first variant to gradually delete the victim's files until they paid the ransom.

Petya

Instead of encrypting specific files, Petya would encrypt the victim's Master File Table, blocking them from their entire hard drive.

NotPetya

NotPetya may show some similarities to Petya, but this destructive variant created much more havoc, deploying a ransomware attack that cost billions of dollars in damages.

2018

Ryuk

One of the most expensive ransoms in history, Ryuk targets state, local, tribal, and territorial government entities, and then asks for huge sums of money to release victim data.

GandCrab

The GandCrab gang were extremely successful in 2018, providing it as a Ransomware as a Service (RaaS) and making it one of the most prevalent variants of the year.

RANSOMWARE: THEN AND NOW

Ransomware has changed drastically over time. Attackers have become quicker and more strategic, and ransomware has become more sophisticated and evasive. In other words - ransomware has become extremely powerful, enough to halt an organization's business, freeze production lines, and disrupt healthcare services. Ransomware's capabilities and targeted industries grow every day.

Over the last 30 years, the ransomware threat landscape has seen some drastic changes and trends:

Payment Options

Ransom payments went from a mere couple hundred dollars via simple, easier to track payment methods, to thousands and even millions via cryptocurrency.

Today, almost all ransomware payments are made through the TOR network, so that threat actors can stay anonymous while cashing in on their attacks.

TOR Usage

No More Police Ransomware

At its beginning, many ransomware variants used law enforcement warnings as ransom notes. Today, they explicitly state the attack and demand payment.

While many early ransomware variants were simple Locker ransomware, today almost all are classified as crypto ransomware, encrypting victim data.

Mostly Crypto

Extortion Tactics

Up until recent years, ransomware's digital damage mostly ended in encrypted files, but variants today will also threaten to publish or delete victim data.

With ransomware's growing popularity, attackers started supplying ransomware as a service to any hacker who wants to join in on the fun (and the profits).

RaaS

Targeted Attacks

Attackers used to deploy wide hit-or-miss ransomware campaigns, but in recent years, there has been a jump in campaigns targeting specific industries and institutions.

FAMOUS ATTACKS

Too many higher education institutions have fallen victim to ransomware attacks over the last few years. In 2019 alone, 89 universities, colleges and school districts were hit with ransomware, potentially affecting operations at over 1,200 individual schools. These are some of the most famous attacks:



Monroe College

Year: 2019
Variant: Unknown
Ransom Price: 2M



University of California, San Francisco

Year: 2020
Variant: NetWalker
Ransom Price: 1.14M (paid)



University of Utah

Year: 2020
Variant: Unknown
Ransom Price: 457K (paid)



Michigan State University

Year: 2020
Variant: Unknown
Ransom Price: Unknown



Columbia College

Year: 2020
Variant: NetWalker
Ransom Price: Unknown



University College London

Year: 2017
Variant: WannaCry
Ransom Price: Unknown



University of Calgary

Year: 2016
Variant: Unknown
Ransom Price: 20K (paid)



Newcastle University

Year: 2020
Variant: DoppelPaymer
Ransom Price: Unknown

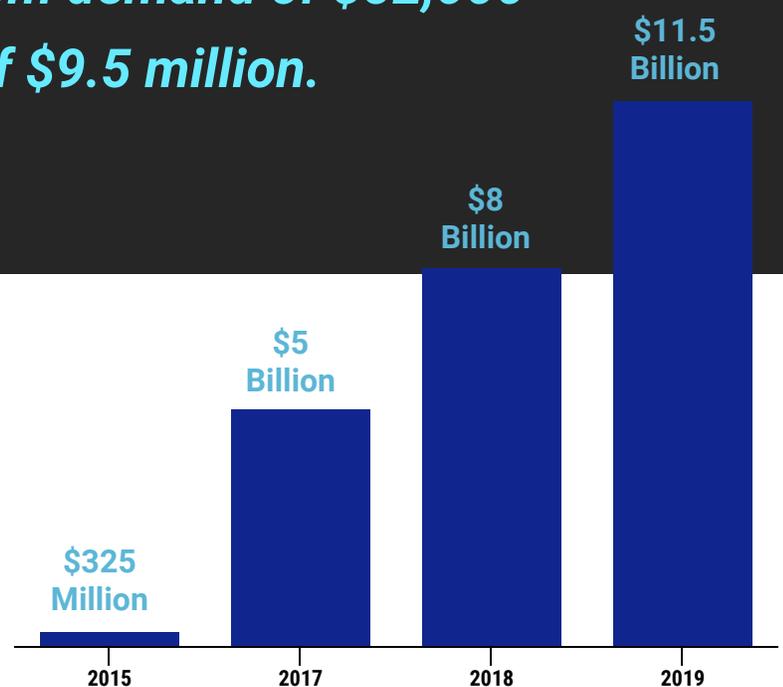
THE PRICE OF RANSOMWARE

So much has been discussed regarding "the cost of ransomware", but is the damage caused by this threat merely the cost of its ransom? The answer is a definite no, it's much much more. From the moment a ransomware infection begins, the price that the victim institution is set to pay is far higher than the price written on the ransom note. First of all, ransomware recovery takes time and effort, even if backups are present, and institutions may have to pay hardware replacement and repair costs. Major prices and burdens caused by a ransomware attack also originate from impaired operations such as lost classes and cancelled events, damage to the victim's brand, and hourly fees for extra IT support.

The City of Atlanta had a ransom demand of \$52,000 compared to a recovery cost of \$9.5 million.

Ransomware Damages by Year

As depicted in Cybersecurity Ventures' estimation of annual ransomware damage costs throughout the years, we may soon be facing over \$20 Billion in damages per year.



PREVENTION & PROTECTION

So how do you make sure that you're protected from ransomware? With next-generation capabilities and evasion techniques, effective infection methods, and targeted campaigns, ransomware is getting more advanced and harder to combat. In addition, **academic environments** are meant to be **publicly accessible, open networks by design**, greatly limiting their protection and prevention options in the face of ransomware. We've put together this list of recommendations, tips and processes for you to use to protect your higher education institution.

Scan and Filter Content

on your mail servers to block malicious incoming emails.

Update and Patch Often to minimize vulnerability exploitation.

Implement and Secure VPNs

for your students and staff, allowing secure from-home access to certain areas in your network.

Secure Remote Desktop Protocols with multi-factor authentication to prevent RDP abuse, a common infection method for ransomware.

Backup Backup Backup

your data as much as possible with minimize damage to your data if you do fall victim to a ransomware attack.

Educate

 staff and students

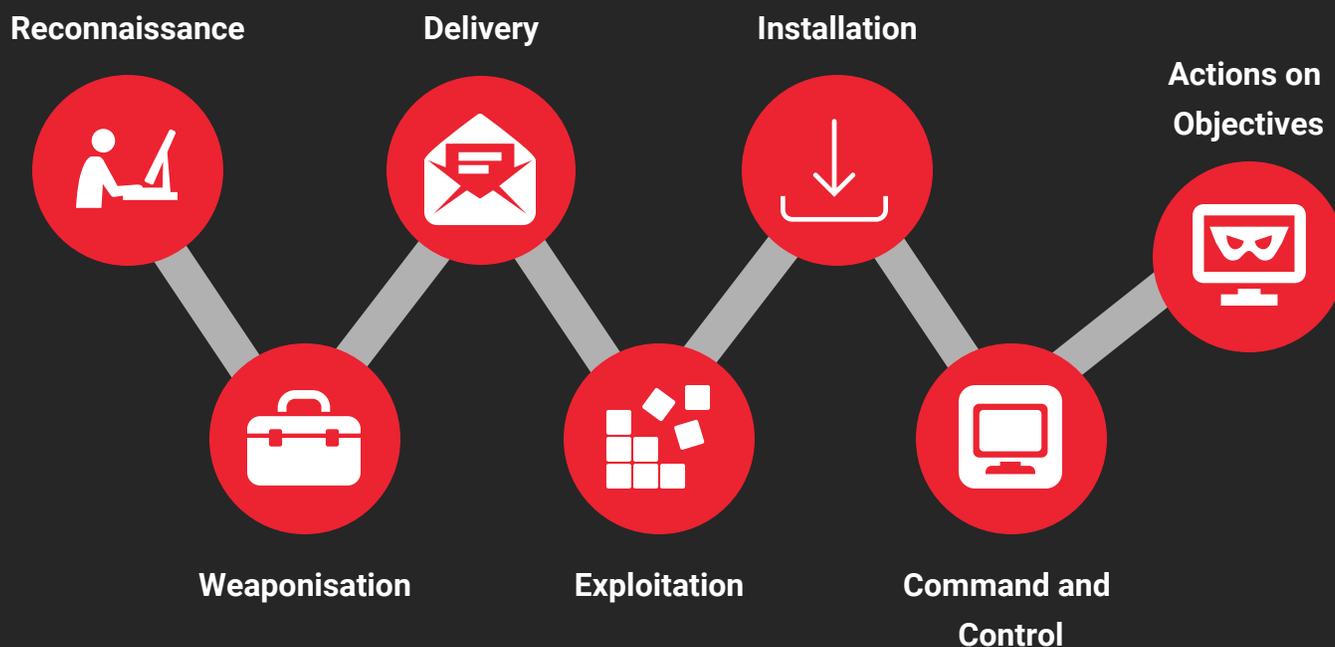
about cyber threats and ransomware, email and internet security - email caution, displaying file extensions, disabling automatic macro execution, secure downloading and more.

Use an Automated Security Solution with updated threat intelligence to block ransomware and threats and prevent the next breach before it happens.

BLOCKING RANSOMWARE THROUGHOUT THE KILL CHAIN

*Block inbound to terminate threats before they enter your network,
block outbound to add a second line of defense.*

A key to understanding inbound and outbound traffic filtering and blocking is understanding the cyber kill chain. The famous kill chain consists of seven steps, and while many security solutions focus on the middle steps by spending most or all of their effort on detecting malware behavior once it's on the machine, and trying to stop it at that level, a much simpler - and much more effective - approach combats malware and ransomware infections early on in the kill chain, so that infections are prevented in the first place.



Blocking suspicious **inbound** traffic creates protection all the way from step one. This allows devices to automatically block phishing and other reconnaissance attempts, barring attackers from gaining access to the machine or network. Inbound blocking will also prevent the ransomware delivery and installation, preventing the ransomware from downloading. If attackers have managed to pass filters and breach the system, blocking malicious **outbound** connections can also prevent the ransomware download in some cases, and will also block it from reaching its C&C servers, and thus from being unable to return data home.

About ThreatSTOP

ThreatSTOP proactively blocks threats - automatically, efficiently, and reliably.

The ThreatSTOP service delivers up-to-the-minute protection against malware, ransomware, DDoS and other advanced attacks, and enhances your existing security posture by improving the effectiveness of firewalls, IDS/IPS, routers, switches, endpoint and other security tools.

The service protects your network and devices by automatically delivering best-in-class threat intelligence to your perimeter security devices, including firewalls, routers and switches. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, the ThreatSTOP service provides immediate relief by deflecting attacks and unwanted or malicious traffic.

Connect with us today to learn more!

1-855-958-7867 (USA and Canada)

+1-760-542-1550 (international)

2720 Loker Avenue West, Carlsbad, California

Threat **STOP**

