RANSOMWARE
PROTECTION PLAYBOOK

ROGER A. GRIMES

WILEY

Table of Contents

List of Tables

List of Illustrations

Ransomware Protection Playbook

Roger A. Grimes

WILEY

Introduction

I've been doing computer security since 1987, for more than 34 years now. I remember the first ransomware program I, or anyone else alive at the time, saw. It arrived in December 1989 on a 5-1/4″ floppy disk and quickly became known as the *AIDS PC Cyborg Trojan*.

Wess didn't call it ransomware then. You don't make up entirely new classification names until you get more than one of something, and at the time it was the first and only. It remained that way for years. Little did we know that it would be the beginning of a gigantic digital crime industry and a huge blight of digital evil across the world in the decades ahead.

It was fairly simple as compared to today's ransomware programs, but it still had enough code to thoroughly obfuscate data, and its creator had enough moxie to ask for $189 ransom in order to restore the data. The story of the first ransomware program and its creator still seems too strange and unlikely even today. If someone tried to duplicate the truth in a Hollywood hacker movie, you wouldn't believe it. Today's ransomware creators and gangs are far more believable.

Dr. Joseph L. Popp, Jr., the creator of the first ransomware program, was a Harvard-educated evolutionary biologist turned anthropologist. He had become interested in AIDS research and was actively involved in the AIDS research community at the time of his arrest. How he got interested in AIDS research isn't documented, but perhaps it was his 15 years in Africa documenting hamadryas baboons. Dr. Popp had co-authored a book on the Kenya Masai Mari Nature reserve in 1978 (https://www.amazon.com/Mara-Field-

Guide-Masai-Reserve/dp/B000715Z0C) and published a scientific paper on his baboon studies in April 1983 (https://link.springer.com/article/10.1007/BF02381082). AIDS is thought to have originated from nonhuman primates in Africa, and those theories were starting to be explored more around the same timeframe as people searched for “patient zero.” Dr. Popp was in the right place at the right time. His study of one could have led to the other.

Back in the late 1980s, AIDS research and understanding was fairly new and very rudimentary. There was still a widespread fear of the relatively new disease and how it was transmitted. Unlike with today's treatments and antivirals, early on, getting HIV/AIDS was a death sentence. At the time, many people were afraid of kissing or even hugging people who might have AIDS or were in high-risk groups. There was great interest for the latest information and learnings, inside and out of the medical community.

No one besides Dr. Popp knows why he decided to write the world's first ransomware program. Some have speculated he was disgruntled at not getting a much-desired job in the AIDS research industry and wanted to strike back, but it can just as easily be stated that he just wanted to make sure he got paid for his work. Still, there are definite signs of hiding and malevolent intent from a man who knew his creation would not be taken well. It's hard to say you didn't know something was illegal when you try to hide your involvement.

Dr. Popp purchased a mailing list of attendees from a recently held October 1988 AIDS conference in Stockholm put on by the World Health Organization and purportedly also used the subscriber lists of a UK computer magazine called *PC Business World* and other business magazines.

Dr. Popp created the trojan horse program using the QuickBasic 3.0 programming language. It must have taken him months of code writing and testing. When he was finished, he copied it onto more than 20,000 disks, applied labels, printed accompanying usage instructions, applied postage manually, and then mailed them to unsuspecting recipients in the United States, United Kingdom, Africa, Australia, and other countries. Dr. Popp must have had help doing all of this, because creating 20,000 software packages and manually applying postage would likely have taken weeks and weeks of work by one person. But no other person's involvement was ever declared in court documents or volunteered by Dr. Popp.

The trojan floppy disk was labeled “AIDS Information Introductory Diskette” (see Figure I.1).

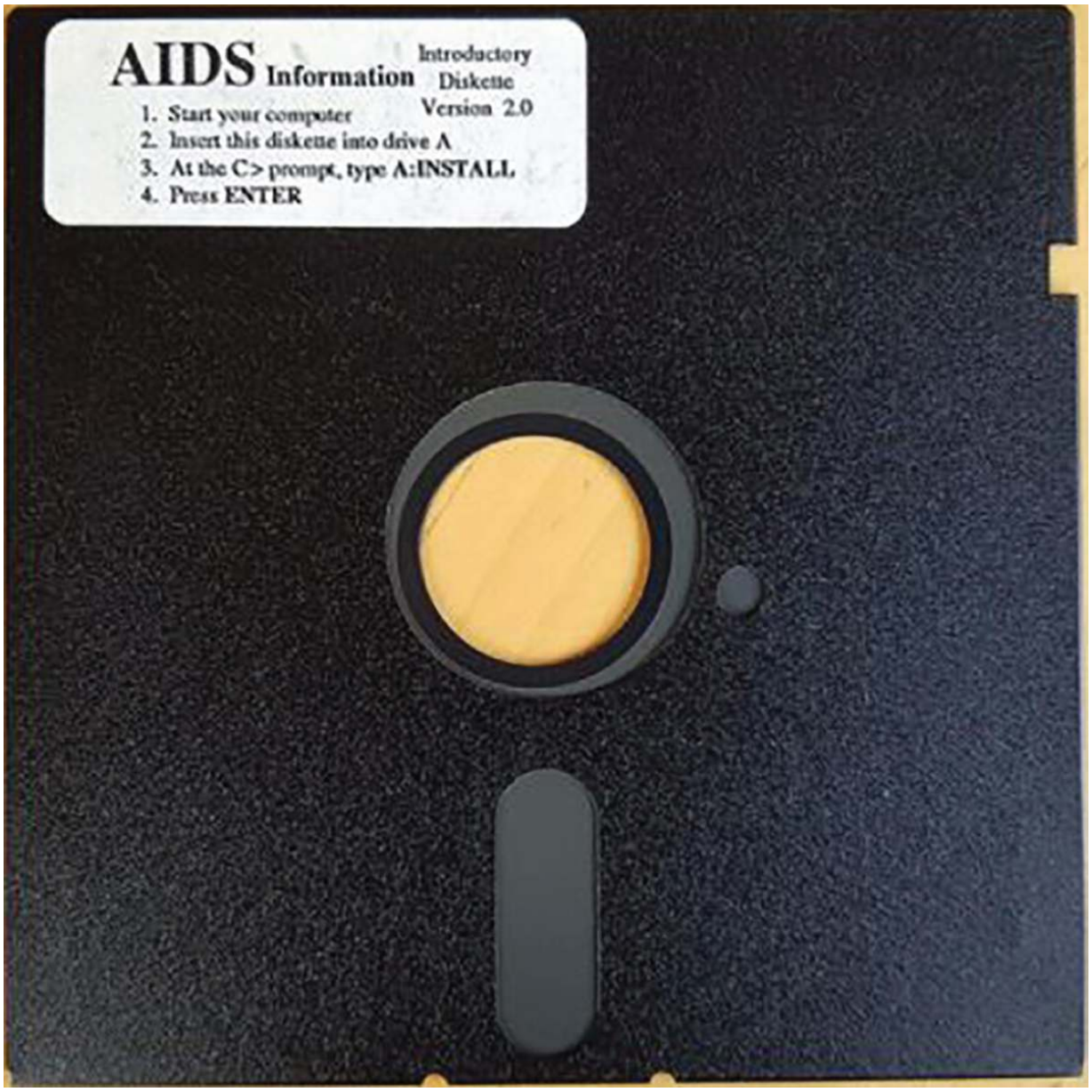


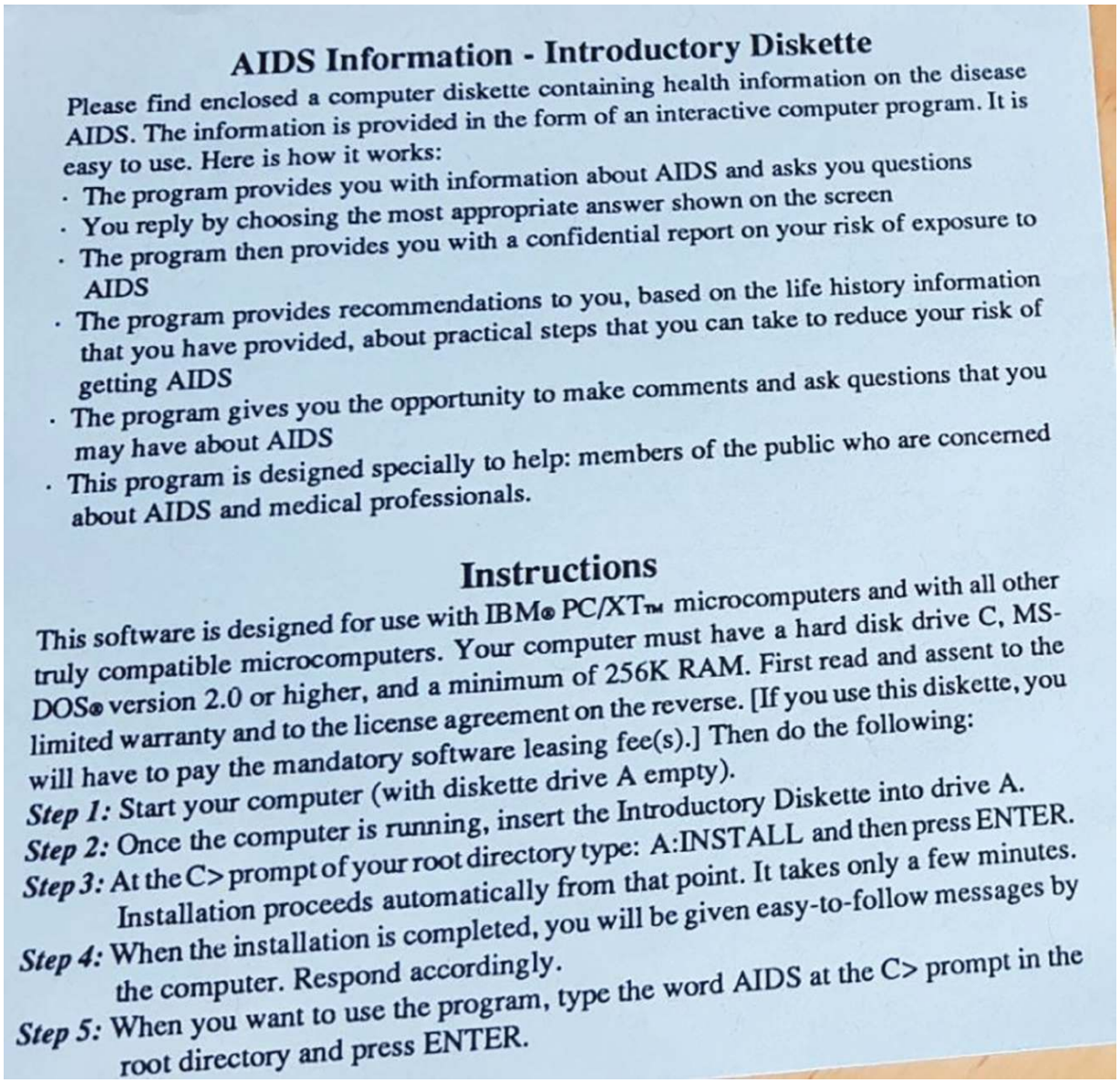
Figure I.1 Picture of disk that AIDS PC Cyborg trojan arrived on

Courtesy Eddy Willems

The floppy disk instructions introduced the disk as purporting to be a program with information about AIDS. After viewing, the user would be asked a series of personal behavior questions. The answer to those questions would be used to give the user a report on their personal risk of

getting AIDS along with recommendations on how to avoid getting it.

The instructions included the warning, “If you use this diskette, you will have to pay the mandatory software licensing fee(s).” This latter warning would later be used by Dr. Popp in his defense as to why his program should not be considered illegal extortion. You can see the instructions and ominous warning in Figure I.2.



AIDS Information - Introductory Diskette

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

Step 1: Start your computer (with diskette drive A empty).

Step 2: Once the computer is running, insert the Introductory Diskette into drive A.

Step 3: At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.

Step 4: When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.

Step 5: When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

Figure I.2 Picture of AIDS PC Cyborg Trojan disk program instructions

Courtesy Eddy Willems

Further, when the trojan program was first run, it printed a license and invoice to the screen and to the printer if the PC was connected to a local printer. The license told users they must pay the software license and even included another ominous warning that you are unlikely to see on any legitimate software program:

> “If you install [this] on a microcomputer…
>
> then under terms of this license you agree to pay PC Cyborg Corporation in full for the cost of leasing these programs…
>
> In the case of your breach of this license agreement, PC Cyborg reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use…
>
> These program mechanisms will adversely affect other program applications…
>
> You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life…
>
> and your [PC] will stop functioning normally…
>
> You are strictly prohibited from sharing [this product] with others…”

Just like today, most people didn't read software license agreements. Normally it's not a problem, but in this case not reading the license agreement with its unusual dire warning would take on special importance. In the late 1980's, a large percentage of users also didn't pay for any commercial software they were not forced to pay for. Software was routinely illegally copied and traded. It was incredibly common for people to copy disks for their friends or even sell (even if they hadn't paid the original developer). Local computer clubs held monthly disk swaps. If you didn't have to pay for software, you didn't. In response, some developers created “copy protection” routines that prevented easy, standard disk copying.

> The author has seen other malicious programs and sites include similar “fair warnings” in their licensing information. It never hurts to read your end-user license agreements instead of simply trying your best to ignore and quickly get by them.

Dr. Popp either didn't know how to do legitimate copy protection or he counted singularly on his peculiar ransom enforcement for people who ignored his licensing instructions. Maybe he got the idea from an earlier malware program. In 1986, the first IBM PC-compatible computer virus, Pakistani Brain (https://en.wikipedia.org/wiki/Brain_(computer_virus)), was created as a copy prevention mechanism. Its Pakistani creators were tired of people illegally copying without paying for disks they had themselves often illegally copied. You can't make this stuff up. It caused boot problems and indirectly might have caused some people to pay money to the inventors to resolve. The malware, however, did not encrypt anything nor directly ask for a ransom.

There is a chance that Dr. Popp saw his ransomware program as simply a way to legally enforce his copyright and software license. There were warnings in at least two places clearly visible to users who used his software. In comparison, today's ransomware programs never give any warning. So perhaps, in only that way, Dr. Popp's creation was a slight bit more ethical than today's ransomware programs. But being a slight bit more ethical criminal among more unethical criminals is not a particularly high standard that anyone should want to be measured against.

Either way, the first time Dr. Popp's program was run by a user, it would install itself on the local hard drive (C:) and modify the `autoexec.bat` file to use as a boot counter. After

the involved PC was booted 90 or so times, the program would encrypt/obfuscate the user's files and folders. It would then display the message shown in Figure I.3.

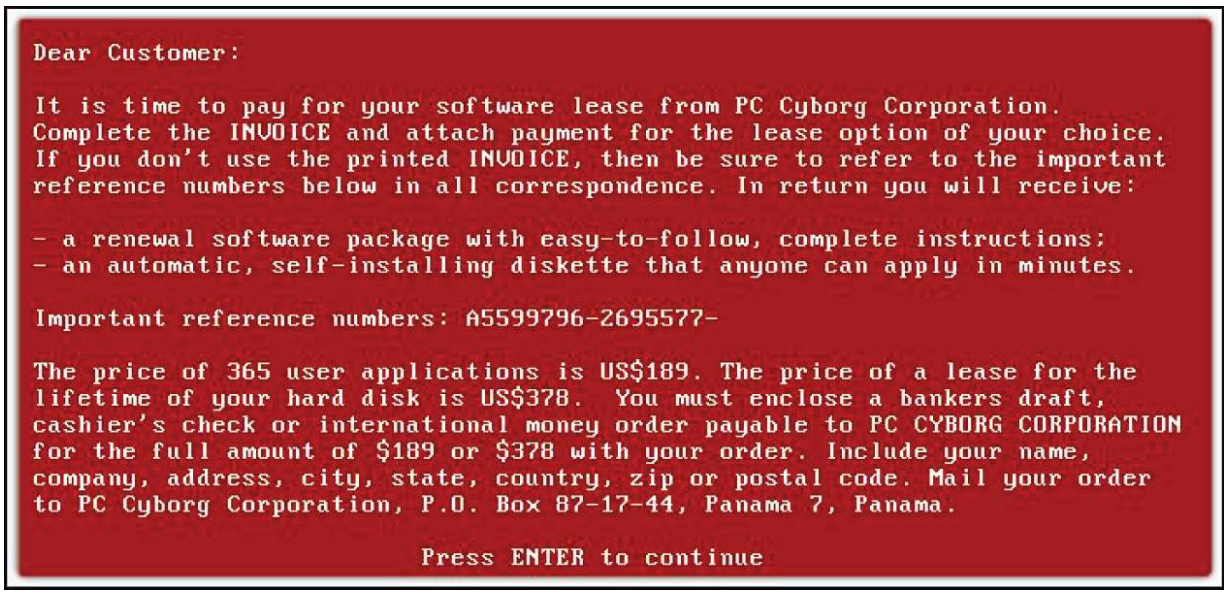


Figure I.3 Picture of AIDS PC Cyborg Trojan ransomware screen instructions

Courtesy Wikipedia

> No one knows why Dr. Popp put his trigger counter at 90. Perhaps he estimated that most people booted their PCs about once a day during the work week, and 90 workdays was more than enough time for someone to send payment for their program and for him to return a "block the lock" executable disk.

Dr. Popp had created a company with the name of PC Cyborg, which would lead to the naming of the virus. The name was shown in the original license and in the after-the-fact ransomware warning, along with asking for $189 for an annual "license" or $389 for a "lifetime license" to be sent to a Panama post-office box. It was this information that led to his quick identification and arrest. Today's

ransomware purveyors use hard-to-identify-true-ownership cryptocurrencies to avoid the same easy identification and detection by authorities.

Dr. Popp had clearly tried to hide his identity and original involvement with his creation. As is still true today, it is common for unethical people trying to hide their identity and financial gains to use offshore corporations and accounts. At that time, Panama was popularly used as a financial and tax avoidance safe haven much as the Cayman Islands and other offshore islands are used today.

When the trojan's program payload ran, before the ransom instructions were shown, it did some rudimentary symmetric encryption to the files and folders. It would move all the existing files and subdirectories into a new set of subdirectories under the root directory, rename them, and enable DOS' “hidden” attribute features on each file and folder, which made them seem to disappear. All the files and folders would also be renamed using “high-order” extended ASCII control characters, which made everything appear as being invisible. Even if the DOS hidden attribute was discovered and turned off, the file and folder names looked corrupted. If the impacted user tried to do some common exploratory commands to see what happened, the malicious code brought back a fake DOS screen with fake results to confuse the user.

The main set of malicious subdirectories were created using extended ASCII character 255, which is a control code that looks like a space even though it is not. But like a space, it would not display on the screen or when printed. For all intents and purposes, all the files and folders appeared, to most users, to have disappeared or at least badly corrupted. But, importantly, none of the files were actually encrypted (unlike today's ransomware programs).

The names of the files and folders were just renamed and moved.

The ransomware program created a conversion table that could be used to reverse the moving and renaming. If you found the table and understood what the trojan program did, you could convert everything back to the original file and folder names and locations. Several individuals figured this out and wrote “fix-it” programs, including early computer virus expert Jim Bates.

Bates created a free 40-page analysis report of the trojan that he would send to anyone who requested it, and he published a shorter, but still great, analysis in the premier antivirus journal Virus Bulletin (https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf.) in January 1990. Bates revealed the many dubious routines of the program including the multiple steps it took to fake what the user saw when investigating. It was a great example of the antivirus and online community coming together to defeat a common foe without thinking about profit.

> The PC Cyborg ransomware encryption routine used what cryptographers called *simple character substitution* for the encryption component. This is the absolute simplest type of encryption possible, and because of that, it's probably more accurate to call Dr. Popp's encryption routine obfuscation instead. It certainly wasn't anything close to as secure as how most digital encryption had been accomplished on computers for at least a decade before Dr. Popp's program, and much less sophisticated compared to encryption in today's ransomware variants. But the point is mostly semantic. To most victims, their data was gone and their computers were unusable.

Along with his detailed analysis, Bates created a free trojan removal program called AIDSOUT and a free AIDSCLEAR program that would restore any renamed and moved files to their original locations and names. The late John McAfee, of McAfee Antivirus fame, gained some early national media attention in the United States by talking about the ransomware program and by saying he went around rescuing people's locked-up PCs.

> It was the publicity surrounding John McAfee's computer virus recoveries during that time that led this author to disassembling DOS computer viruses for John McAfee later that year and largely led to the author's lifetime career in cybersecurity.

After the antivirus industry and law enforcement determined that Dr. Popp was involved, he was arrested on a warrant while at Amsterdam's Schiphol Airport and eventually imprisoned in London. During the arrest it was immediately noted that he was having some mental health

issues. Even before the arrest, he had apparently scribbled strange messages on another passenger's luggage, indicating that he, Dr. Popp, was in the luggage. He did many other unusual antics during this period of time, including wearing a condom on his nose and wearing curlers in his beard “to ward off radiation.” To this day no one knows if he was really having mental health issues or just faking being insane to avoid being found guilty. Either way, he was originally arrested or detained in the Netherlands and sent back to his parents in Ohio in the United States at some point. He was then re-arrested on many crimes including blackmail and extradited back to the United Kingdom for trial.

> Where the various arrests happened are swapped in some news stories, but it appears he was arrested or detained in two or three different countries at some point and faced some sort of adjudication in at least two of those countries. His final release came from a UK court.

Dr. Popp's original defense was to claim that everything he did was legal because he warned users, and they were the ones not paying for what they were legally obligated to pay. Some lawyers thought he may have a valid legal point even though it was unusual and unethical. Part of Dr. Popp's original defense fell apart because his program would also state that if users took his ransom program to another computer and allowed it to lock up that computer, that the program would then unlock the original computer so it could be used. This part of the program did not work, either intentionally or unintentionally, and both the original and additional PC would not be operational.

It's unclear if Dr. Popp ever got paid or sent a single unlock disk or if that unlock disk worked. I don't know of anyone who paid the ransom, and none of the victims in the dozens of old news stories claim to have paid the ransom or received an unlock disk from Dr. Popp. I think Dr. Popp was quickly on the run to avoid being arrested when his program started to make the news worldwide. It is doubtful that he had time to pick up his payments in Panama and send out unlock disks, and it is certainly true that he did not do this at scale. Every news story surrounding the PC Cyborg trojan starred victims whose PCs were locked up.

Dr. Popp claimed in court proceedings and to investigators that he planned to donate all the ransom money to AIDS research. That claim would be unlikely to persuade any court and would not result in the dismissal of any pending charges. Although it must be noted that Dr. Popp really did belong to several AIDS research groups that were raising money for research, and he was involved in several AIDS educational conferences and programs. In any case, one or more judges ruled that he was unfit to stand trial, and by November 1991 he was released back to his parents a free man by UK Judge Geoffrey Rivlin.

He faded back into relative obscurity and turned his interest back toward human anthropology. His infamous actions, which had both directly attacked and unfairly maligned AIDS researchers around the world, precluded his continued involvement in that field.

A decade later, in September 2001, he released a fairly controversial book called *Popular Evolution Life Lessons* (https://www.amazon.com/Popular-Evolution-Life-Lessons-Joseph-Popp/dp/0970125577), which contained many unconventional recommendations, including an aggressive focus on procreation, even by young females who had just obtained puberty. He strongly promoted “scientific ethics,” which

stand diametrically opposed to by most moral codes and ethics that the rest of us follow. Perhaps his belief in his own form of unconventional ethics played a part in his creating the first ransomware program. He was also for eugenics and euthanasia. He didn't believe in anyone having a pet. He pretty much offended almost anyone who lived a conventional life. Suffice to say, his book of recommendations was not a best seller and did nothing to diminish how strange he was seen by others even as he was pursuing other careers.

Sometimes even an eccentric man can be a gentle man and beloved by others. Just before he died in 2007, “Dr. Joe” funded The Joseph L. Popp, Jr. Butterfly Conservatory in upstate Oneonta, New York. They have their own Facebook page (https://www.facebook.com/Joseph-L-Popp-Jr-Butterfly-Conservatory-119385884741701/). The butterfly operation was still in business at least until the 2020 COVID-19 shutdowns, but the main website domain is now up for sale and there aren't any Trip Advisor reviews after early January 2020 (https://www.tripadvisor.com/Attraction_Review-g48333-d1755655-Reviews-Joseph_L_Popp_Jr_Butterfly_Conservatory-Oneonta_New_York.html). Some of the early reviews indicated things were looking a bit rundown and ragged before the COVID crunch, so maybe it has had its final opening.

In his life, Dr. Popp had a few different careers, including evolutionary biologist, author, anthropologist, and butterfly lover. But his likely biggest unwanted claim to fame, something he could not escape the rest of his life, was as the father of ransomware. There are still nearly as many stories on him today as the creator of ransomware, in 2021, as there were back in 1990 when his creation was creating digital havoc. His place in history far outlived his own life.

More information and stories on Dr. Popp and his PC Cyborg program can be found at the following resources:

- https://en.wikipedia.org/wiki/AIDS_%28Trojan_horse%29
- https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html
- https://www.vice.com/en/article/nzpwe7/the-worlds-first-ransomware-came-on-a-floppy-disk-in-1989
- https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/
- https://www.thepitchkc.com/dr-popp-the-first-computer-virus-and-the-purpose-of-human-life-studies-in-crap-gapes-at-popular-evolution/
- https://blog.emsisoft.com/en/34742/history-of-ransomware-a-supervillain-30-years-in-the-making/
- https://www.villagevoice.com/2009/04/16/dr-popp-the-first-computer-virus-and-the-purpose-of-human-life-studies-in-crap-gapes-at-popular-evolution/
- https://www.gwinnettdailypost.com/news/business/the-bizarre-story-of-the-inventor-of-ransomware/article_bed2be94-129c-5d5a-a973-2112d99556a6.html
- https://www.knowbe4.com/aids-trojan

The PC Cyborg ransomware trojan was a startling wake-up. The lesson learned was that there are people in this world who have no ethical qualms with encrypting your hard drive and asking for a ransom to be paid to unlock it. They were willing to risk going to jail to do it.

Surprisingly, after Dr. Popp's trojan, there wasn't a lot of imitation as antivirus fighters had feared. Perhaps it was

because Dr. Popp had not been successful. He didn't get rich. He ended up in jail. Lesson learned. Other criminals learned that it was hard to do digital extortion and get away with it, at least at the time. But in another decade or so, other advances in technology would give them the means to get away with the crime almost every time.

Dr. Popp's encryption wasn't very good either. But around the same time period, other types of malware, especially computer viruses, were starting to experiment with better encryption. But encryption was used only to hide and protect the malware program itself from quick antivirus detection and not to encrypt data files and ask for ransom.

Slowly a few slightly “better” ransomware programs started to appear. Most of them made up their own encryption routines, which is to say almost always resulted in very bad, easily-breakable, encryption. These early “cryptoviruses” or “cryptotrojans,” as they were known then, rarely required a decryption key to unlock the data. Hobbyist cryptographers often figured how to decrypt the locked files without having to pay the ransom. Good encryption is hard to make. By 2006, a second class of crypto-malware started to show up, this time using known and proven cryptographic routines that were not so easy to break. By 2013, ransomware programs using encryption that was really hard to impossible to break were fairly common.

As the encryption issue was being fixed, the far bigger problem for criminals was how a ransomware creator could get paid without getting caught and sent to jail. Two things happened. First, Bitcoin was invented in 2009. It took a few years, but by 2014, the ransomware programs made the link to Bitcoin, and the whole ransomware industry exploded. Now, criminals could get paid without getting caught.

Second, some major countries, like Russia, became cyber safe havens for ransomware criminals. Today, many ransomware gangs are located in or around Russia and operate with near impunity. Many pay bribes to local and country law enforcement as a part of doing business, and their revenue streams are seen as a net positive in their host countries. As long as they don't encrypt computers in their host or friendly ally countries, they are free to do business with few exceptions.

With these two new developments in place, sophisticated ransomware programs started to take out entire businesses, hospitals, police stations, and even entire cities. Today, ransomware is so prolific that entire companies being taken down, and ransoms paid in the multi-million-dollar range don't even raise an eyebrow. Ransomware attacks are taking down oil pipelines, food production plants, corporate mega-conglomerates, closing schools, delaying healthcare, and pretty much exploiting everything they can with near impunity. As I write this, ransomware gangs are likely in their “golden years,” causing more disruption and making more money, than ever before. At this moment, we aren't doing a very good job at stopping it.

But we can. That's what this book is about. It's about preventing ransomware from happening in the first place, as your number-one objective, and minimizing damage if your organization gets hit. Turns out there are many things any organization can do to avoid being hit by ransomware or to at least significantly minimize the odds. Fighting ransomware is more than having a good, solid backup and up-to-date antivirus program.

This book will tell you the best things you can do to prevent a ransomware attack from happening in the first place, better than any other source you can find. It will tell you

the details of what you need to do before you are possibly hit by ransomware and what to do, step-by-step if you are exploited. You don't have to be a victim. You can fight back.

Anyone can be a victim of ransomware. Ransomware is difficult to defeat currently. The aim of this book is not to say that you can 100 percent defeat ransomware. You can't. No one can make that claim. Cybersecurity defense is about risk minimization, not elimination. My goal is to help you minimize the risk as much as possible. If you follow the ideas and steps in this book, you will minimize your risk of a successful ransomware exploit as best you can given the current state of what we can do until we get new defenses that work better for us all (covered in Chapter 2, “Preventing Ransomware”).

Fight the good fight!

Who This Book Is For

This book is primarily aimed at anyone who is in charge of managing their organization's computer security, from the front-line defender to the top computer security executive. It is for anyone who is considering reviewing, buying, or implementing computer security defenses for the first or the tenth time.

What it will take to prevent and mitigate ransomware is what it will take to prevent and mitigate all malicious hackers and malware. The lessons taught in this book, if followed, will significantly reduce risk of all malicious hackers and malware attacks. Even if one day ransomware goes away, the lessons learned here will readily apply to the next “big” attack. Ransomware is not your real problem; it's an outcome of your real problem.

What Is Covered in This Book?

Ransomware Protection Playbook contains 12 chapters separated into 2 distinct parts.

Part I: Introduction

Part I summarizes what ransomware does, how sophisticated it is, and how to prevent it from exploiting your organization and devices. Many people don't understand how mature ransomware is and even more don't concentrate enough on stopping it before it attacks.

> **Chapter 1, “Introduction to Ransomware”** Chapter 1 covers ransomware starting with a little bit of history of the significant milestones and then discusses the very sophisticated and mature versions used today. The ransomware industry is run much more like a multilevel marketing firm/ecosystem than anything else. Chapter

1 will cover the common pieces and parts. As an encompassing introduction, it is also the longest chapter in the book.

Chapter 2, "Preventing Ransomware" Preventing ransomware is something that isn't talked about enough. The most recommended "prevention" control, a good backup, is not prevention at all. Chapter 2 will talk about the things every person and organization should be doing to prevent ransomware to the best of their ability. And in the process of discussing how to defeat ransomware, it will discuss how to best defeat all malicious hackers and malware.

Chapter 3, "Cybersecurity Insurance" The decision to purchase cyber insurance is a big dilemma for organizations facing the threat of ransomware. Cyber insurance is complex. Chapter 3 gives readers a basic understanding of cyber insurance, including the things that should be avoided when considering a policy. It ends with a frank discussion of the massive changes happening in the cybersecurity industry right now and where it's headed.

Chapter 4, "Legal Considerations" Chapter 4 covers the legal considerations involved with dealing with a successful ransomware attack, not only in the decision of whether to pay or not pay the ransom, although that is a big part of this chapter, but also how to use legal help to your benefit during an attack. Chapter 4 will contain tips and recommendations that every organization should utilize in their planning and responses to ransomware.

Part II: Detection and Recovery

Part II will help you plan for and respond to a successful ransomware attack.

Chapter 5, "Ransomware Response Plan" Every organization should have a detailed ransomware response plan created and practiced ahead of an actual ransomware event. Chapter 5 will cover what your ransomware response plan should contain.

Chapter 6, "Detecting Ransomware" If you can't stop a cybersecurity exploit from happening, the next best thing is early warning and detection. Chapter 6 covers the best ways to detect ransomware and gives you the best chance to stop it before it begins to do real damage.

Chapter 7, "Minimizing Damage" Chapter 7 assumes ransomware has been able to successfully compromise an environment and has encrypted files and exfiltrated data. How do you minimize the spread of ransomware and its damage during the first hours of the first day? Chapter 7 tells you how.

Chapter 8, "Early Responses" After the initial damage has been prevented from spreading further, now comes the initial cleanup, better assessment, and additional responses, beyond just preventing further spread. Chapter 8 is what you need to be doing after the first day or two. How well you perform this part of the response often determines how long it will take to fully recover.

Chapter 9, "Environment Recovery" Chapter 9 covers what you need to be doing after the first few days. You've stopped the spread, minimized the damage, and started to get some initial systems back up and working. Chapter 9 is what you need to be doing after the initial worst is over. It covers the longer-term items, the ones that often take days to weeks, or even months, to recover or rebuild.