RANSOMWARE
PROTECTION PLAYBOOK

ROGER A. GRIMES

WILEY

Ransomware Protection Playbook

Ransomware Protection Playbook

Roger A. Grimes

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

ISBN: 978-1-119-84912-4
ISBN: 978-1-119-85001-4 (ebk)
ISBN: 978-1-119-84913-1 (ebk)

Library of Congress Control Number: 2021945410

Cover Image: © Just_Super/Getty Images
Cover Design: Wiley

This book is dedicated to my wife, Tricia. She is always the brightest light in any room, blotting out the sun with her smile, beauty, kindness, brilliance, and laughter. People like me better after meeting her.

About the Author

Roger A. Grimes is a 34-year computer security consultant, instructor, holder of dozens of computer certifications, and author of 12 previous books and more than 1,100 magazine articles on computer security. He has spoken at many of the world's biggest computer security conferences (e.g., Black Hat, RSA, etc.), been in *Newsweek*™ magazine, appeared on television, been interviewed for NPR's *All Things Considered*™ and the Wall Street Journal, and been a guest on dozens of radio shows and podcasts. He has worked at some of the world's largest computer security companies, including Foundstone, McAfee, and Microsoft. He has consulted for hundreds of companies, from the largest to the smallest, around the world. He specializes in host and network security, ransomware, multifactor authentication, quantum security, identity management, anti-malware, hackers, honeypots, public key infrastructure, cloud security, cryptography, policy, and technical writing. His certifications have included CPA, CISSP, CISA, CISM, CEH, MSCE: Security, Security+, and yada-yada others, and he has been an instructor for many of them. His writings and presentations are

often known for their real-world, contrarian views. He was the weekly security columnist for *InfoWorld* and *CSO* magazines between 2005–2019.

You can contact the author at:

Email: roger@banneretcs.com

LinkedIn: https://www.linkedin.com/in/rogeragrimes/

Twitter: @rogeragrimes

CSOOnline: https://www.csoonline.com/author/Roger-A.-Grimes/

About the Technical Editor

Aaron Kraus, CCSP, CISSP, is an information security professional with more than 15 years of experience in security risk management, auditing, and teaching information security topics. He has worked in security and compliance roles across industries including US Federal Government civilian agencies, financial services, and technology startups. Aaron is a course author, instructor, and cybersecurity curriculum dean with more than 13 years of experience at Learning Tree International, and most recently taught the (ISC)^2 CISSP exam prep. He has served as an author and technical editor for numerous Wiley publications including *The Official (ISC)^2 CISSP CBK Reference*; *The Official (ISC)^2 CCSP CBK Reference*; *(ISC)^2 CCSP Certified Cloud Security Professional Official Study Guide, 2nd Edition*; *CCSP Official (ISC)^2 Practice Tests*; *The Official (ISC)^2 Guide to the CISSP CBK Reference, 5th Edition*; and *(ISC)^2 CISSP Certified Information Systems Security Professional Official Practice Tests, 2nd Edition*.

Acknowledgments

I want to start by thanking Jim Minatel, my Wiley acquisitions editor. We've been together for at least four books now. Jim always figures out the right book for us to write at the right moment and brings together the rest of the talented team to make it happen. I want to thank the rest of my production team, including project manager Brad Jones, managing editor Pete Gaughan, Sacha Lowenthal, Saravanan Dakshinamurthy, Kim Wimpsett, and tech editor Aaron Kraus. I didn't know Aaron before this project, but I now know he's a rock star. He's one of the best tech editors I've ever had. Brad was just perfect in tempo and responsiveness.

Special thanks to Anjali Camara, M.S., M.A., partner, and cyber practice leader for Connected Risk Solutions. She took time out from her PhD work to educate me on cybersecurity insurance issues and the big changes in the industry that ended up becoming a whole chapter. Special thanks for my multidecade friend, Gladys Rodriguez, Microsoft principal cybersecurity consultant for the information she gave me on recovering Microsoft environments

and is usually the smartest person in the room on any Microsoft technology subject she's interested in.

I have to thank my KnowBe4 co-workers, starting with Erich Kron. It was his early ransomware slide decks I viewed when first learning about newer breeds of ransomware many years ago. I stand on his shoulders. My friend and co-worker, James McQuiggan, was my constant sounding board, and is great for turning my 30-minute rants into more memorable 30-second quips that people will actually listen to and read more often. Fellow author Perry Carpenter has forgotten more about social engineering than I'll ever learn. My awesome co-workers, Javvad Malik (check out his YouTube videos and his and Erich's Jerich Show podcasts), Jacqueline Jayne (she puts the Human in Human Firewall), Anna Collard (South African rock star!), and Jelle Wieringa (he knows how to read, write, and talk in 5 languages, including C-Level Boardroom). All taught me about how ransomware impacts their countries and regions.

A big thanks is owed to my CEO, Stu Sjouwerman; direct leader Kathy Wattman (I have never had a bigger supporter); SVP Michael Williams; our excellent marketing team, including Mandi Nulph, Mary Owens, and Kendra Irimie; our PR team, including Amanda Tarantino, Megan Stultz, and Reilly Mortimer, for either letting or forcing me to speak about ransomware hundreds of times over the last few years. Nothing fine-tunes your understanding of subject matter more than speaking about it hundreds of times and using the resulting comments to get it right. Thanks to co-worker Ryan Meyers for helping me to look for the right phishing clues that are or might be used by ransomware gangs.

Lastly, thanks to the hundreds of existing ransomware resources—articles, presentations, whitepapers, and surveys—that provided much of the education that I tried to consolidate into this book. Defeating ransomware is going to take everyone. I hope I've added some value to the path of defeating ransomware.

Contents

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).

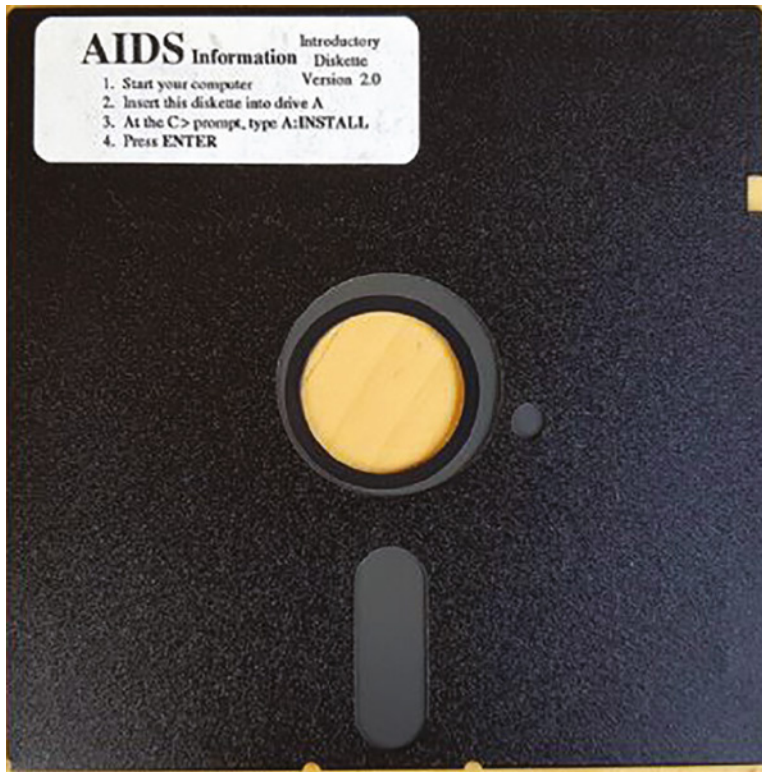
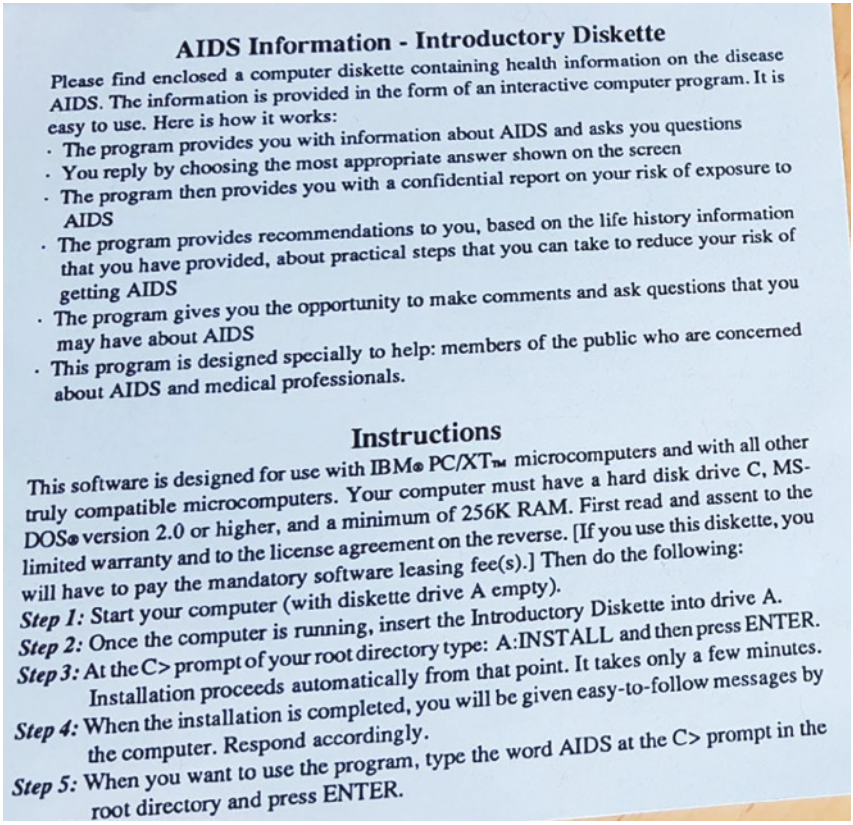


Figure I.1 Picture of disk that AIDS PC Cyborg trojan arrived on
Courtesy Eddy Willems

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.

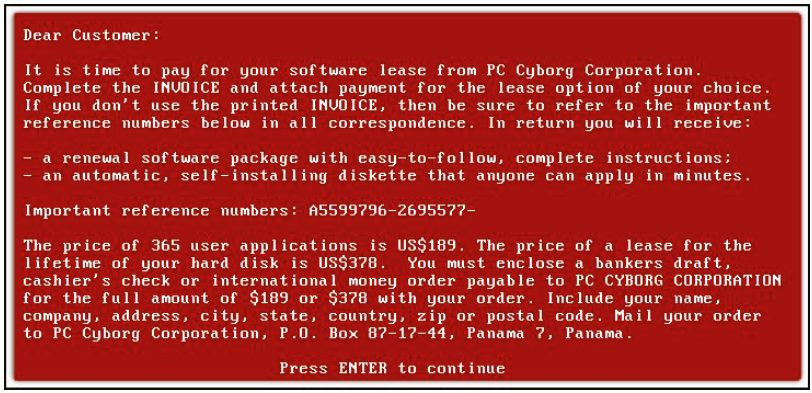


Figure I.3 Picture of AIDS PC Cyborg Trojan ransomware screen instructions
Courtesy Wikipedia

> 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