THE HISTORY OF **CYBERTHREATS**

History is a good teacher. Knowing the history of cyberthreats provides a better understanding of how we got here— and helps us prepare the resources we'll need to battle them in the future better.

PRE-CYBER ERA
THE RISE OF THE WORM

1940s The possibility of replicating computer programs is floated.

1950s Core Wars, a game that vies for control of the computer, launches.

1960s *Game of Life,* a life-emulating program, comes to life.

1970s The first true self-replicating programs launch.

1971 "I'm the creeper, catch me if you can" scrolls across computer screens.

THE CONTAGION ERA
THE RISE OF VIRAL ATTACKS

Worms evolve, the law catches up.

1983 Patent for a "cryptographic communications system and method" is granted.

1983 The term "computer virus" is born.

1986 The "Pakistani Brain" virus becomes the first to cause serious damage.

1986 The U.S. passes the Computer Fraud and Abuse Act (CFAA).

1988 Robert T. Morris releases the Morris Worm and is convicted under CFAA.

THE LONE WOLF ERA
THE RISE OF ME-TOO ATTACKS

"Lone wolf" hackers launch attention-grabbing viruses and anti-virus software emerges. The media takes notice.

1993 DEF CON Conference launches with 100 attendees.

1995 Secure Sockets Layer (SSL) becomes online purchasing standard.

2000 Mafiaboy brings down major websites, causing an estimated $7.5 million in damages.

2000 ILOVEYOU virus attacks tens of millions of Windows PCs, causing email systems to crash.

THE CROWDSOURCING ERA
THE RISE OF TARGETED ATTACKS

Groups use technology for financial gain and political/social change. Organizations respond.

2003 Anonymous launches a DDoS attacks on the Church of Scientology.

2006 More than 45.7 million customer records stolen in TJX Companies attack.

THE CYBERWAR ERA
THE RISE OF NATION-STATE ATTACKS

The technologies, attack vectors, and goals continue to advance.

2010 Google announces an attack on its infrastructure in China.

2017 Linked to Russian intelligence, APT28 (Fancy Bear), launches a cyberespionage campaign against the Montenegrin government.

2018 U.S. intelligence reveals a U.S. military program aimed at gleaning information from terrorists' computers.

2018 China-linked hackers target U.S. and Southeast Asian firms to intercept their military and civilian communications.

2018 China breaches the computers of U.S. government agencies and major corporations, ending a 12-year cyberespionage campaign that was later found to affect as many as 12 other countries.

THE FUTURE
THE RISE OF THE CYBERSECURITY LABOR SHORTAGE

Even as cyberthreats become more routine, they're becoming more sophisticated. **Yet the biggest threat may be the lack of skilled professionals to deal with the onslaught of attacks.**

AS ONE EXPERT SAYS:

"The greatest virtual threat today is not state sponsored cyber-attacks; newfangled clandestine malware; or a hacker culture run amok. The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage..."

WHICH BEGS THE QUESTION:

HOW CAN THE CYBERWAR BE WON WITH FEW RESOURCES ON THE BATTLEFIELD?

Sources: "A Brief and Incomplete History of Cybersecurity," U.S. Cybersecurity Magazine; "A Brief History of Cybersecurity," Cybersecurity-Insiders.com, 2019; "The History of Cybersecurity," Colorado Technical University; "9 Latest Cyber-Espionage Affairs," EC-Council.org, 03/2019.