Muninn

A Brief History of Cyber Security

1960s

Image: nasa.com

It was during the 1960s when organisations first started to become more protective of their computers. During this time, there was no internet or network to worry about, so security was largely focused on more physical measures, and preventing access to people with enough knowledge about how to work a computer.

In order to do this, passwords and multiple layers of protection were added to devices, such as routines and logbooks to track access.

1970s

Image: clickamericana.com

In the 1971, researcher Bob Thomas created a computer programme called **Creeper** - a program which would become the first ever computer worm.

Ray Tomlinson, the inventor of email, wrote the programme **Reaper**, which chased and deleted Creeper. Tomlinson's invention was the very first example of antivirus software.

During the 1970s, threats to computer security were clear and visible. Often these threats were in the form of malicious insiders reading documents they shouldn't. The practice of computer security revolving around governance risk and compliance (GRC) therefore evolved separately from the history of computer security software.

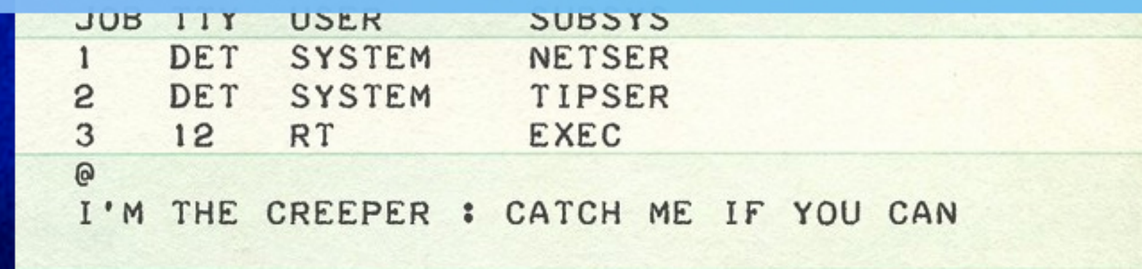


Image: IEEE Spectra

1980s

The "Elk Cloner" for the Apple II Systems was created by Richard Skrenta. It infected the Apple DOS 3.3 and spread to other computers by floppy disk transfer. The "Elk Virus" was responsible for being the first computer virus to cause a massive outbreak ever in history.

In 1983, while completing his dissertation, Frederick Cohen used the term **virus** in order to explain when a particular computer program is able to infect additional computer programs because it was capable of replicating itself.

Early spring 1988, the Ping-Pong virus was discovered at the University of Turin in Italy, a novel type of boot sector virus. The first ARPANET worm then saw daylight for the first time and disabled over 6,000 computers.

Tim Berners-Lee proposed an information management system on 12 March 1989, then implemented the first successful communication between a Hypertext Transfer Protocol (HTTP) client and server via the Internet in mid-November. Then, over the next decade, internet became mainstream.

The first polymorphic virus called the Chameleon was developed in 1991, it was released and also become known as Tequila. With its ever-changing nature , it became wide spread and difficult to detect.

Organised crime entities saw this as a new potential source of revenue and started to steal data from people and governments via the web. This issue prompted the emergence of anti-virus companies such as Kaspersky, McAfee and Symantec. It is estimated that there were over 1300 viruses in existence in 1992.

The late 90s saw an emergence of macro viruses attacking Excel and other consumer software, and virus via mail became a problem for internet users.

1990s

2000s

The first virus to infect one million computers was released on May 5th, 2000 - It was ILOVEYOU a.k.a. Lovebug. It was a Windows system file (vbs), and shortly thereafter malicious programmers figured out how to embed viruses in PDF documents, images and spreadsheets.

Organised crime start to heavily fund professional cyberattacks and governments begin to clamp down on cyber-criminality, giving much more serious sentences to those culpable.

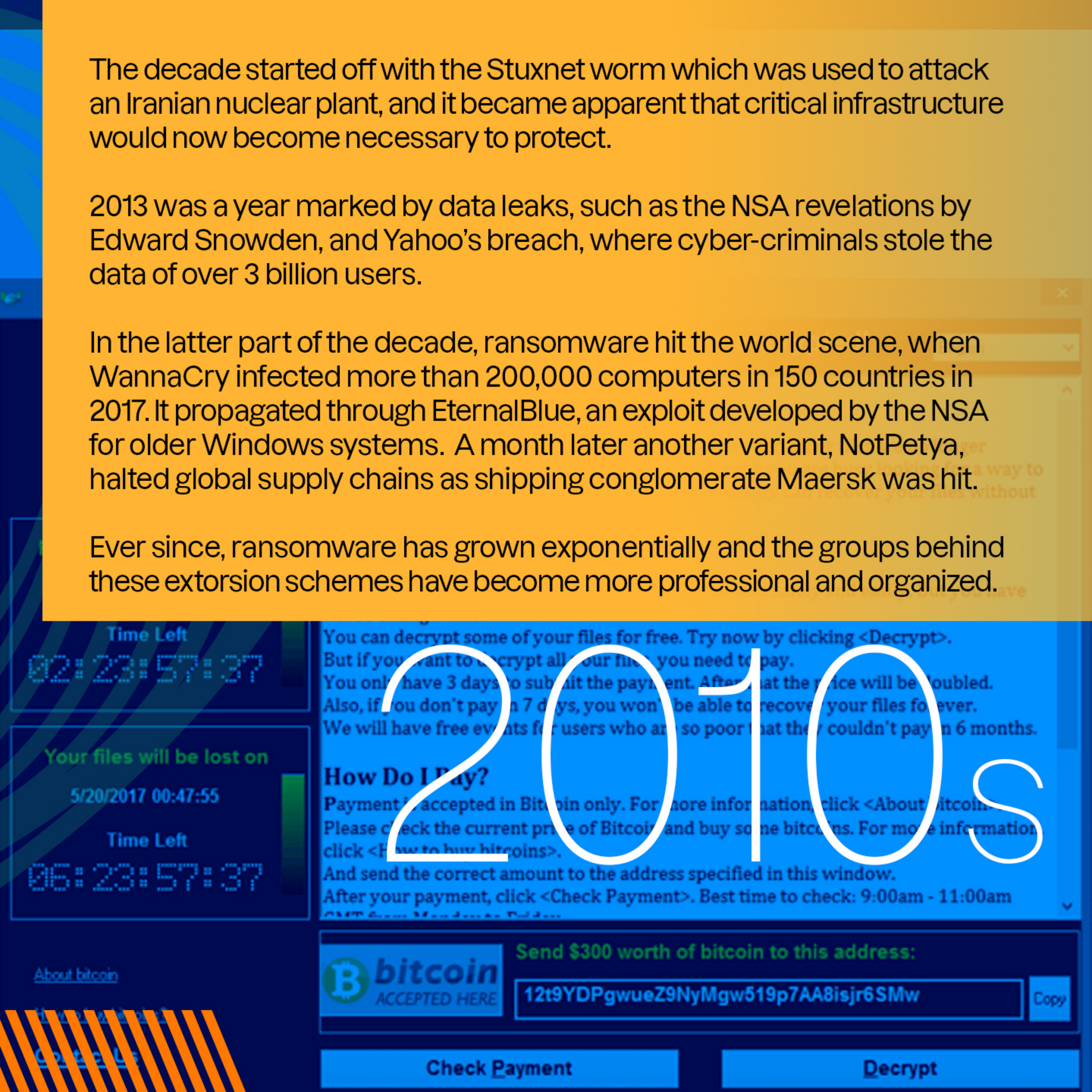
New digital markets such as gaming, social media, forums and entertainment opened new attack vectors to cyber-criminals, and viruses stealing banking details became a serious and lasting threat.

The decade started off with the Stuxnet worm which was used to attack an Iranian nuclear plant, and it became apparent that critical infrastructure would now become necessary to protect.

2013 was a year marked by data leaks, such as the NSA revelations by Edward Snowden, and Yahoo's breach, where cyber-criminals stole the data of over 3 billion users.

In the latter part of the decade, ransomware hit the world scene, when WannaCry infected more than 200,000 computers in 150 countries in 2017. It propagated through EternalBlue, an exploit developed by the NSA for older Windows systems. A month later another variant, NotPetya, halted global supply chains as shipping conglomerate Maersk was hit.

Ever since, ransomware has grown exponentially and the groups behind these extorsion schemes have become more professional and organized.



presented by

Muninn

CSH

muninn.ai