dms

The Evolution of Business Ransomware Attacks

www.dmstechnology.com

The Evolution of Business Ransomware Attacks

Ransomware can have a negative – even crippling – impact on businesses. This type of attack is becoming increasingly common and is constantly evolving into new, more advanced strains. Many companies are unaware of the threat it poses; however, it is important to protect your organization, and your data, against ransomware.

What is Ransomware?

Ransomware is a form of malware that holds your information hostage. Companies are often unaware that an attack has occurred until after a hacker has located and encrypted their data. While DMS Technology can help to recover data in some instances, the best strategy is to prepare in advance.

The History of Ransomware

The first ransomware attack was the AIDS Trojan, disseminated via floppy disk in 1989. This attack affected many people involved in the fields of science but wasn't widespread.

By 2005, ransomware became commonplace, affecting personal users and businesses across all industries. Apps that looked identical to spyware removal tools or other helpful programs spread misinformation, duping users into buying programs that did nothing.

> "2016 FBI estimates show cyber criminals' collective payout easily broke $1 billion for the year."

Crypto-ransomware followed soon after, sequestering personal and business data into password protected files while deleting the originals. The attacks evolved, allowing cyber criminals to disable access and control of computers, requiring a ransom to restore user control.

Users no longer have to download malicious programs for ransomware to take over — it can be installed without any input from the user, so long as their computer is left unprotected.

In previous years, users could wipe their business computers of ransomware using traditional security software to restore their access. However, as security measures tightened, cyber criminals found new ways to hit companies with ransomware.

Now, ransomware usually takes the form of crypto-attacks, outright demanding payment in exchange for restored data. Regular users lack the ability to remove the ransomware on their own, creating an unfortunate dilemma: lose important business data, some of which may even be confidential customer information or trade secrets, or face paying a ransom.

> "
>
> The cost to U.S. victim organizations and businesses is conservatively estimated to be more than $200 million, putting ransomware on pace to be a $1 billion crime.
>
> "

Using History to Inform the Future

Companies like DMS Technology have created plans to fight back against ransomware by looking at what happened in the past to learn how to avoid these problems now and in the future. We aim to be several steps ahead of cyber criminals, aware of what tactics they are currently using and anticipating what malicious technology they may soon introduce.

With a focus on business security and disaster recovery planning, security consultants can preemptively protect your company from ransomware attempts and other malicious attacks.

THE RISE OF RANSOMWARE

1989

AIDS MALWARE
First Known Ransomware

2005

GPCODDER
The Return of file-encrypting malware

2012

REVETON
Appears to be a fine from law enforcement

2013

THE REVOLUTION
Anonymous online payments with Bitcoin

CRYPTOWALL
First demanding Bitcoin for payment

ANDROIDDEFENDER
Fake antivirus + Lockscreen

2014

TORRENTLOCKER

CTB-LOCKER
Uses Tor for command-and-control

SIMPLOCKER
Targeting Android devices

2015

PCLOCK
Copycat ransomware, pretending to be CryptoLocker

TESLACRYPT
Goes after online gaming save files

2016

KERANGER
First targeting OS X

LOCKY
Delivered via Microsoft Word documents

> "
>
> 2.9 percent of compromised victims in a ransomware attack will pay the ransom.
>
> "

The High Cost of Ransomware

Historically, ransomware has cost companies billions, and the problem is projected only to get worse. Statistics show corporate attacks are on the rise, as malicious people know that businesses can afford higher ransoms than personal users. The cost of ransoms has increased too — 2016 FBI estimates show cyber criminals' collective payout easily broke $1 billion for the year.

A recent survey shows only 42% of surveyed IT professionals had adequate backups to recover from a ransomware attack. Unsecured business systems are wide open, leaving you paying high ransoms, losing important data, or both. Investing in a custom security solution is well worth it, given the increasing risk of your company suffering a ransomware attack of its own.

You can — and should — protect your business from ransomware attacks with robust security measures. DMS Technology is pleased to work with you to provide custom-designed solutions that will ensure your business information is safe.

Customers expect you to honor their trust by keeping their data safe, and you owe it to yourself to protect your company and help it thrive. Contact DMS Technology today for more information, and secure your vital business information.

"

The average cost of a data breach for targeted organizations is approximately $6.5 million.

"

New York Office

780 Third Ave, 15th Fl
New York, NY 10017
United States

P: 212-561-5222
www.dmstechnology.com

London Office

Berkeley Square House, 2nd Floor
Berkeley Square, London W1J 6BD
United Kingdom

P: 0207-084-7155
www.dmstechnology.com