# SPAM—Malware's Super Highway

*How To Protect Yourself Against Malicious Emails*

# What The Good Guys Are Up Against

| According to Kaspersky Lab: |
| --- |
| • The decline in SPAM emails over the past few years has reversed |
| • March 2016 statistics show that malicious SPAM emails are 4 times the level they were in 2015 |
| • SPAM emails have risen to 61% of all email traffic |
| • Over 50% of email phishing attacks are directed against banks, online stores and payment systems |

**Statista reports that in 2014, global spam volume reached 28 billion per day**

# What Spammers Do

Send thousands of emails daily infecting as many PCs as possible

**The math is simple:**

If a hacker sends 50,000 infected emails and just 1% take action, 500 computers get infected

If done on a daily basis, each hacker can steal data from millions of systems

Many compromised computers are commercial machines allowing entry into highly-prized business networks

Stolen data is sold to the criminal underground for lucrative paydays with little effort

# How They Do It

Large criminal enterprises sell Crime as a Service (CaaS) system packages to newbie cyber-thieves making barrier to entry extremely low

- Wannabe thieves get comprehensive crime systems plus technical support
- They're shown how to send malicious emails, infect PCs, recruit bots, and track results

They also use the Internet of Things (IoT) to spread SPAM

- Hackers easily compromise internet-enabled household appliances, TVs, baby monitors, home smart sensors, medical devices, etc.
- Criminals use them to spy on people and steal their data
- They draft them into bot armies to send infected SPAM emails

The problem is fueled by millions of people freely giving their information on the internet so hackers don't have to work very hard to harvest email addresses

# What Happens When You Click On An Infected Link Or Open An Attachment?

## At first, nothing may appear to be happening at all, however…

- Malware is downloaded, undetected in the background
- Or you are redirected to an infected site where malware is downloaded automatically
- Passwords, financial data, personal and client information are all targeted and sent to criminal servers—your system and/or network may also be encrypted and held for ransom

## **Fact:** Current anti-virus programs can't detect all malware, especially new ones

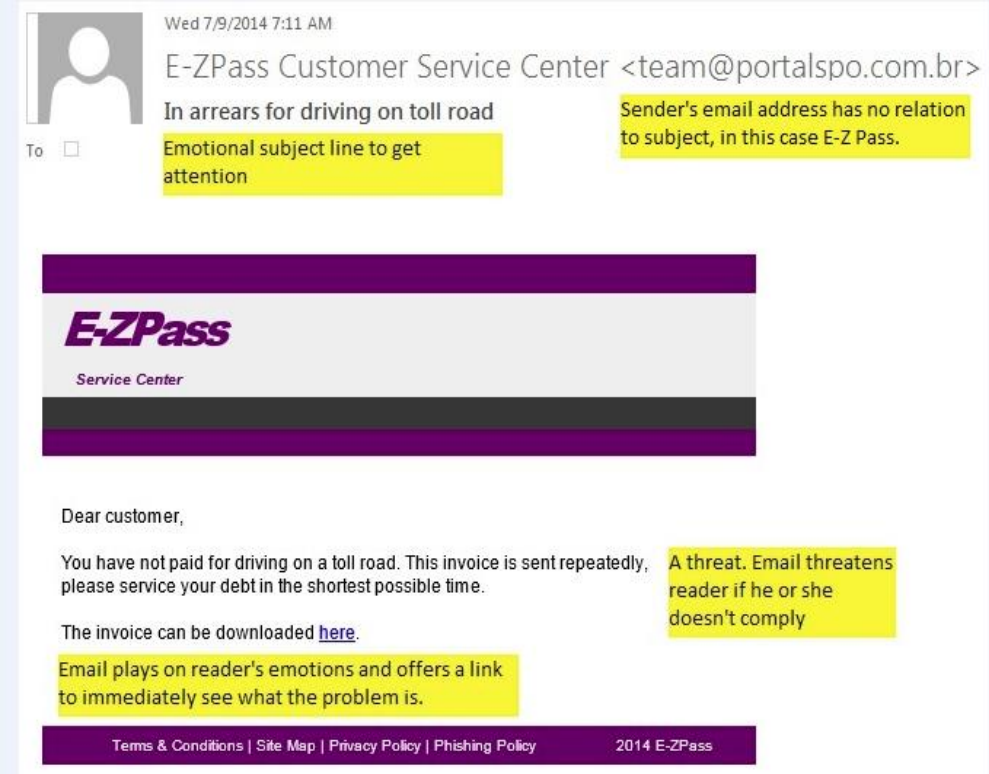
- Security companies must see the strain first before creating methods to detect it
- Some viruses even change their behavior to bypass anti-virus programs
- Newer strains have the ability to wait undetected, activating at a later time
- Encrypting ransomware has become cyber-crime's number one cash cow
- It's been estimated that over 250,000 new malware strains are produced each day

# 12 Critical things You Can Do To Protect Yourself From Malicious Emails

- Use a disposable email address for public use
- Keep your antivirus software up-to-date and  scan suspect emails
- Strengthen your email client's SPAM filter to send suspicious emails to your Junk Folder
- Use an Advanced SPAM Filter as an additional layer of protection
- Delete suspicious emails and don't click on any links—not even the "Unsubscribe" link—since they may also infected
- Clean out your Junk folder and also delete suspect emails from your Deleted folder
- Read everything before agreeing to terms and make sure vendor's aren't selling your information to third parties
- For added protection, set your email to plain text rendering links inactive
- If you receive an email from the U.S. Post Office, FedEx, etc.—do not click on the tracking link—instead, manually enter it into the search box on the official website
- Don't operate your PC with Administrator privileges—that's how ransomware propagates through business networks
- Disable macros on Microsoft applications to prevent their automatic execution when opening infected attachments
- Learn how to identify bogus links (next slide)

# How To Identify Bogus Emails

Below is an example of a bogus email, annotated to show what to looked for:




*If you hover your mouse over the link [DO NOT CLICK!], you can see where it leads to.*

*In this case, the Top Level Domain (TLD) of .ir shows that it's from Iran!*

# People Are The Weakest Link In Security

- No matter how cautious you are, others can break your security by the actions they take or fail to take
- One click on an infected link by a staff member can trigger a ransomware attack on the entire organization
- The simple fact is that a magic bullet to save us from malware and ransomware simply doesn't exist
- To give yourself and your company a fighting chance, institute the steps outlined earlier and …

## Make sure you have a viable backup of your data!

# There Are Mainly 3 Types Of Backup To Choose From

## Data Backup

- Only backs up data
- Is slow since it backs up 1 file at a time
- Doesn't guarantee a quick recovery
- It's not easy to check if backups are viable

## Image-based Backup

- Takes a complete picture or image of a server or PC allowing for quicker restorations
- Is better than data backup because it snapshots the entire system
- Does not provide instant failover should a server fail, get damaged or destroyed

**Best Option**

## Hybrid-cloud / Instant Failover Solution

- Takes images of systems and saves them to an onsite device and two cloud locations
- Provides alternate server functionality both onsite and from the cloud
- Daily Screenshots of boot-up screens for virtualized servers verifies viability of backups
- Full Management: installation, monitoring, troubleshooting and assisting in recovery

# BUSINESSES SHOULD INCLUDE THE DATTO SIRIS SOLUTION AS PART OF THEIR DISASTER RECOVERY ARSENAL

*The Datto SIRIS Is The Ultimate Protection Against Data Loss*


| What It Is | What It Does | What To Expect |
|---|---|---|
| ✓ A Hybrid-cloud Backup Solution | ✓ Instant onsite fail-over | ✓ **NO** data loss |
| ✓ Snapshots of your entire server | ✓ Cloud Continuity for maximum protection | ✓ **NO** costly downtime |
| ✓ Infinite data retention | ✓ Image Capture for super fast restores | ✓ **FULL** Business Continuity |
| ✓ Automatic onsite & offsite protection | ✓ Bare Metal Restore (BMR) capability | ✓ **FULL** Management & Support |

# XSolutions And Datto—An Unbeatable Combination!

XSolutions is an Elite Partner of Datto, the world leader in Hybrid-cloud Business Continuity solutions whose systems protect 180+ Petabytes of data with over 700 employees around the globe.

We are experts in the configuration, installation and management of Datto Business Continuity and Backup systems.

We'll manage, monitor and maintain your backup systems, making sure that they're working properly and that they'll be ready when needed.

**With XSolutions, you're NEVER alone**. We'll be there to help you whenever you need it, from restoring individual files to full server restorations.

In addition to automated alerts, we physically check backups throughout the day making sure they're viable and taking place on schedule. If an issue arises, we'll resolve it immediately or work with Datto's award-winning support team until the problem is solved.

**Contact us to schedule a FREE demo!**

Call: (845) 362-9675

Email: contactus@xsolutions.com

Web: www.xsolutions.com