SecurElement White Paper

Protect Your Business from Ransomware and Other Threats

Kate Smith, Director, Sales & Marketing

SecurElement support has seen an influx of SMB organizations infected with email-based threats including types of ransomware such as CryptoLocker, CryptoWall and Lockey. Additionally, users are reporting seeing fraudulent emails consistent with wire transfer scams. It is vital to understand how these types of applications gain access into an infrastructure and how to prevent users from allowing access.

Ransomware (CryptoLocker) Type Threats – the most common email-based threat aimed at extorting money from users, Ransomware or CryptoLocker encrypts your files and require the user to pay a "fee" in order to unlock files. CryptoLocker is initiated when users open an infected email attachment (as a .zip, .JS, etc.) or click on a website link from an email directing you to an infected site (we've see this approach used to direct users to an infected Dropbox.com, Copy.com, or Google Drive account). CryptoLocker then systematically searches your PC for any local drives, mapped drives, external storage devices, etc. and encrypts everything.

The best defense is to be vigilant.

- Never open an email or attachment from a sender you do not know or are not expecting.
- Never click on a link in an email from a sender you do not know or are not expecting.
- Setup a policy that any email containing specific attachments be sent to IT for scanning of malicious content.
- Disable macros in Office applications to help prevent attacks as some ransomware applications require macros to be enabled.
- Have a sound, thoroughly tested backup policy so that if a ransomware type infection occurs, data can be restored from backup without paying a ransom.

Wire Transfer Email Scams - aiming to get employees working in the financial department of a company to transfer money for non-existent goods or services or for "admin expenses." Email requests usually appear to come from the company's CEO or some other executive-level employee complete with mimicked email signatures. Fake emails also use some version of the correct domain name with a slight difference; targeting @example.com but using @examplle.com in hopes that users won't notice the additional character in the email address.

Again, vigilance is key.

- Has the CEO or executive-level employee asked for wire transfers in the past?
- Is transferring funds in this method a normal or regular business practice?
- Can this request be confirmed by speaking with the requester directly?

484-323-1600 | www.securelement.com

SECURELEMENT
INFRASTRUCTURE SOLUTIONS

Employee education and a sound backup strategy are key to protecting your data and your assets. It is also wise to reach out to your trusted IT provider to assess your infrastructure vulnerabilities by conducting a security audit.

About the Author

Kate Smith, SecurElement's Director, Sales & Marketing is responsible for SecurElement's overall sales and marketing strategy as well as ongoing partner relationships with organizations such as Microsoft, Cisco, Barracuda, Dell and many others.