BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

June 2017 | Briefing 31

RANSOMWARE PREVENTION BEST PRACTICES

Ransomware is now the #1 security concern for organizations

Ransomware is a cyber epidemic that continues to evolve, targeting home users, businesses, and government networks globally. This type of cyberattack blocks access to your computer or network, and holds the information "hostage" until ransom is paid by virtual currency (typically Bitcoins). Ransomware infection methods are no different than "typical" malware - opening email attachments (even from known-senders), or visiting a webpage that surreptitiously installs the code.

The latest cyberattack in history, named "WannaCry", recently affected more than 400,000 systems in 150 countries including United States, Canada and China (with the largest concentration of computers infected due to unlicensed or outdated versions of Windows), and approximately 4,000 other ransomware attacks have occurred daily since January 2016.

Protecting your personal or corporate data will cost you less than the impact of losing it, which may risk your organization's reputation, or incur financial problems as a result.

What protective measures do you need to make? Are you fully protected?

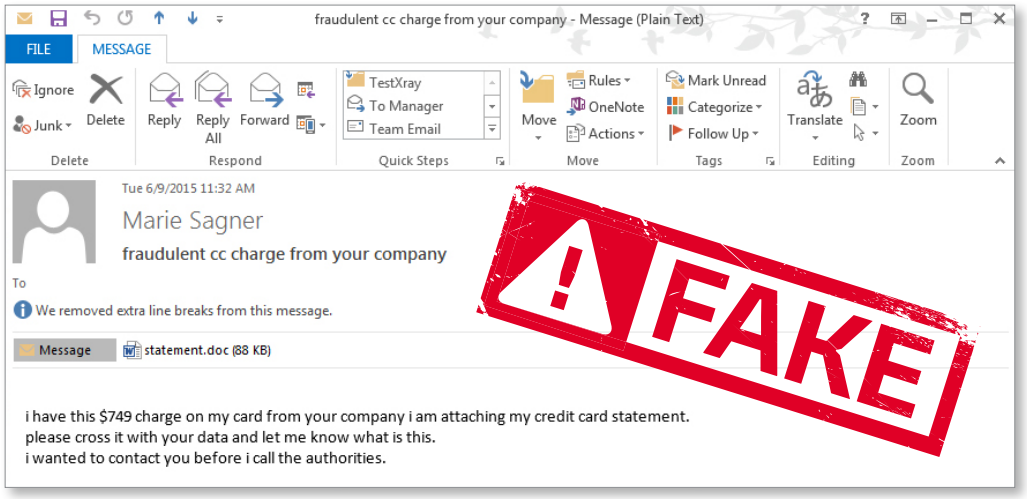
METHODS OF ATTACKS:

- **Phishing**
- **Whaling**
- **Water Holing**
- **DDoS Attacks**
- **Malware**
- **Malvertising**

PROTECT YOUR DATA

HOME USERS, mitigate risk by:

- **Practicing safe browsing.** Use a browser that provides extensions or add-ons which prevent malicious code from running, such as uBlock Origin, or NoScript.
- **Be suspicious of emails, especially those with attachments.** If you're not expecting an email from someone, ASK the person if they have sent you anything recently.
- **Never clicking on suspicious links on e-mails, social media or messenger chats.** Only open links from senders addresses you trust, and you are familiar with the site.



KEEP AN EYE for fake e-mails and webpages. Malicious websites will often have bad spelling, utilize symbols or spell company names differently.

ENTERPRISES, mitigate risk by:

- **Developing workforce cyber awareness training.** Train your employees to detect suspicious e-mails or websites. Create an internal cyber protection policy that will keep employees vigilant and report any unusual activities.
- **Installing & keeping anti-virus software and firewalls up to date.** Make sure your anti-virus solutions are set to automatically update their definitions and conduct scans.
- **Backing up valuable information often:** Categorize your information and keep a separate backup for sensitive data.
- **Conducting an annual penetration test and vulnerability assessment:** Stay informed of emerging threats and make sure you have a good incident response plan for when an attack is detected.

"Businesses, as well as home users, have become victims, and relying on backups is often the last line of defense when cybersecurity should be first"

– Symantec

THE LAST FIVE YEARS HAVE SHOWN A STEADY INCREASE IN ATTACKS TARGETING BUSINESSES WITH LESS THAN 250 EMPLOYEES.

MOBILE DEVICES = SMALL COMPUTERS

As technologies advance, ransomware becomes more powerful and will even find new targets beyond PCs to your smartphone. Protect your mobile device by creating automatic backup, refraining from downloading suspicious apps and only install apps from trusted sources.

Mobile attacks: While the majority of mobile malware infections are due to user error – installing malicious apps – much like with PC's, mobile devices are able to be infected by opening attachments or visiting sites with underlying malicious code. According to a report released by Kaspersky Lab, mobile ransomware attacks increased by 250% in Q1 2017.

RECOVERING FROM INFECTION

It is recommended to not pay the requested ransom, as payment does not guarantee you will regain access to your data. Instead you should:

1. **Isolate the infected computer immediately** (disconnect from your network, either Ethernet or WiFi).
2. **Secure backup data** or systems by taking them offline.
3. **Contact law enforcement and provide all information** gathered: date, time, location, number of infected users and type of equipment used.

Cybersecurity is not only about employing the right technology but requires a team effort from everyone; both at home, and in the office. **Cyber awareness and education are the greatest tools to prevent, mitigate and recognize possible attacks before they put your data, and your customer's information at risk.**

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.