PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 17: SPAM AND MALWARE

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. PART 17 covers the effects of spam and malware on your business and identifies how to reduce the risk.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

If your website is subjected to cybercrime including using one of the methods outlined in this email campaign, then report it to **ACTION FRAUD**.
USE THE ONLINE REPORTING TOOL: https://reporting.actionfraud.police.uk/login
OR CALL ACTION FRAUD: 0300 123 2040 **(**helpline 24/7 for live attacks 8am till 8pm for others**)**

SPAM: WHAT IS IT, IS IT DANGEROUS AND HOW TO PREVENT IT

1.0 Spam is the term used for inappropriate or unsolicited email messages sent over the Internet, typically to many users, for the purposes of advertising, phishing money or data, or spreading malware. Most spam is irritating, but spam can be very dangerous as it hides malware and scams.

1.1 Because Symantec, an organisation that analyses internet activity globally, says that in the first quarter of 2019, 55% of global email traffic was spam, businesses should take all possible measures to reduce the threat of spam as it is a real and present danger to them. A common way to compromise business systems is through:

- **Phishing emails** which look like communications from legitimate sources such as well-known companies, people that the recipient knows, Google calendar updates, photos or similar items. With many phishing emails a link or picture within it is a package of malware which is launched when the user clicks on it.
- **Spear Phishing emails** are like phishing emails, but they are specifically aimed at causing the recipient to disclose confidential information which makes them vulnerable to identity theft or fraud.

1.2 Spam is a global problem and as we saw in the last issue of the email campaign much of it is driven by criminals and perhaps also by hostile foreign Governments. The actual origins of industrial scale spamming can be hard to determine as frequently professional spammers will go from server-to-server of multiple unsuspecting organisations in between in order to hide the true origin.

1.3 During 2017, the 'WannaCry' attack, which affected numerous institutions around the World, including the NHS in the UK was eventually attributed to North Korea as cyber experts managed to trace it back through various servers in between. The attack exploited a vulnerability in Microsoft Windows. The software tools to create the attack were identified by the National Security Agency, the national-level intelligence agency of the United States Department of Defence, and they formed part of the spying tools suite of that agency. These tools were either leaked or stolen by a hacking group called the Shadow Brokers, who are believed to be an off shoot of the Russian state, and

PROFIT

Shadow Brokers are then believed to have made the 'WannaCry' tool available to other malevolent operators.

1.4 Usually email scams are trying to get you to give up bank details so that the fraudsters can either withdraw money or steal your identity. Some spam contains more sinister malware which seeks to lock systems for ransom, spy on businesses, or steal data. According to the experts, the annual overall loss resulting from spam is estimated to be tens of billions of pounds. As a result, anti-spam protection is not only desirable, but an urgent necessity.

HOW TO STOP SPAM

1.5 Spam often originates from known malicious websites with IP addresses. PROFiT recommends that all organisations should protect themselves from spam by signing up to the free DNS service from the **Global Cyber Alliance**[1] (GCA) which is called **Quad9**.

1.6 **Quad9** protects users from accessing known malicious websites, leveraging threat intelligence from multiple industry leaders and currently blocks up to two million threats per day for users in 76 countries. It improves your system's performance, plus it preserves and protects your privacy. Quad9 is quick and easy to set up and can be obtained at: https://www.globalcyberalliance.org/quad9/.

1.7 Don't give your email address to companies that you don't trust. And when you do share it, make sure you are not opting into marketing emails, newsletters and other filler. Reputable companies should always provide a simple way to unsubscribe from their mailing lists, if you change your mind about receiving their updates.

1.8 Don't post your email address online where it can be harvested by would-be spammers. This includes using your email address on message boards or forums on the internet.

1.9 When you find spam in your inbox, don't just delete it. Select it and tell your mail client that this message is spam. How you do this depends on your client. You also need to train the mail client about your false positives. Once a day, go through your spam folder looking for messages that don't belong there. When you find one, select it and tell the client that it made a mistake.

1.10 If you recognize something as spam before you open it, don't open it. If you open it and then realize it's spam, close it. Do not click a link or a button, or download a file, from a message that you even *remotely* suspect is spam. If you opened a spam because it appeared to be coming from a friend or co-worker, contact them immediately and let them know that their account has been compromised.

1.11 Make sure that you have trusted email authentication to reduce the risks of having your emails spoofed or hacked. PROFiT recommends **GCA DMARC** which brings together email authentication protocols and adds reporting and compliance. Get your GCA DMARC at: https://dmarc.globalcyberalliance.org.

MALWARE

2.0 **Malware**, short for '***mal****icious* ***soft****ware*', is software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, compressed code in links, documents, or photographs and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. This type of software can be used to lock systems, steal data, or commit fraud on the victim. It is often deployed via spam emails.

2.1 **Malware** types include:

- **Adware** - a software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

[1] https://www.globalcyberalliance.org/who-we-are/

PROFIT

- **Backdoor** – a feature or defect of a computer system that allows covert unauthorized access to data.
- **Bots** – essentially Trojan/Worm combinations that attempt to exploit individual computers as part of a larger malicious network.
- **Cryptolocker** - a ransomware trojan which specifically targets computers running Microsoft Windows it is often hidden in a zip file attached to a spam email or through a link exploiting a legitimate organisations branding.
- **Keyloggers** - install themselves onto the computer and send back to the originator all keystrokes made by the user in order to steal information.
- **Logic Bomb** – is a set of instructions secretly incorporated into a program so that if particular conditions are satisfied, they will be carried out, usually with harmful effects.
- **Malvertising** - is the use of legitimate adverts or advert networks to covertly deliver malware to unsuspecting users' computers hidden in advertising.
- **Ransomware** – is software which damages or locks your system and offers to fix the problem if money is paid.
- **Rogue Security Software** - is malware that pretends to be a well-known security software update or warning which when opened by the user installs malicious software onto the computer and which might include ransomware.
- **Rootkits** - are a form of malware that hides from the user's anti-virus protection software.
- **Spyware** – is software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
- **Trojan Horses** - are malicious software, disguised as something innocent or desirable and so actively downloaded by the recipient.
- **Viruses** - infect programs onto your computer when they are opened.
- **Worms** - actively infect your systems and network without user action.

2.2 Malware is different from defective software, which is legitimate software but contains harmful bugs that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official looking company website in the form of a useful or attractive program which has the harmful malware hidden within it along with additional tracking.

2.3 Today, most malware is a combination of traditional malicious programs, often including parts of Trojans and worms and occasionally a virus. Usually the malware program appears to the end-user as a Trojan, but once executed, it attacks other victims over the network like a worm. Many of today's malware programs are considered rootkits or stealth programs. Essentially, malware programs attempt to modify the underlying operating system to take ultimate control and hide from anti-malware programs. To get rid of these types of programs, you must remove the controlling component from memory, beginning with the anti-malware scan.

2.4 Software such as anti-virus, anti-malware, and firewalls are relied upon by users at home, small and large organizations to safeguard against malware attacks which also help to identify and prevent the further spread of malware within the network.

AVOIDING PROBLEMS WITH MALWARE

2.5 Make sure that your computers and systems have good anti-virus and anti-malware software protection installed, kept it updated, and always activated. If possible, set the ant-virus and anti-malware software to update automatically so that you have the latest version of the protection offered.

2.6 Make sure that you are familiar with the different forms of malware attack that occur and ensure all staff within your organisation understand that they **should not open attachments or download software onto their computers or systems unless they can verify the source**, particularly if they are not expecting communication from that source.

2.7 Tell your staff that if they do receive an unexpected email from a source that they are aware of then they should talk to the IT team and take advice before attempting to open the email or any attachment or link within the email.

PROFIT

2.8 Make regular back-ups, storing them safely, preferably offline and increase the security settings on your browser. If you are unsure how to increase the security of your browser take advice from your IT team.

2.9 You should report attacks of these kinds upon your computer systems to the Police through Action Fraud as the assault may constitute a criminal offence under the Computer Misuse Act 1990 which recognises the following offences:

1. Unauthorised access to computer material,
2. Unauthorised access with intent to commit or facilitate a crime,
3. Unauthorised modification of computer material, and
4. Making, supplying or obtaining anything which can be used in computer misuse offences.

2.9 Although a Cryptolocker is readily removed, files remain encrypted in a way which some investigators consider impracticable to break. You may be tempted to pay the originator of a Cryptolocker due to the compelling offer that payment of the ransom will allow the user to download the decryption program, which is pre-loaded with the user's private key. The experts say that you should **not pay** the ransom as you cannot be sure that the files will be decrypted, or that the criminals won't come back for more money.

MISSED A PREVIOUS EDITION?

If you have missed a previous edition of the email campaign let us know and we can send you FREE a copy: contactus@profit.uk.com

1. Fraud Risks
2. Recruitment in Travel Fraud
3. Employee Fraud
4. Your Supply Fraud
5. Upon Discovering A Fraud
6. Investigating A Fraud
7. When Police Become Involved
8. Preparing For Court
9. Validating A Booking
10. Payment Fraud Issues
11. Challenging A Chargeback
12. Other Payment Fraud
13. Protecting Images
14. Protecting Websites
15. DDOS Attacks & Hacking
16. Know Your Enemies
17. Spam & Malware
18. Other Ways Data Is Lost

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com

Next Week: Part 18 Other Ways Data Is Lost

PROFIT