Stack Group

Autumn NEWSLETTER 2016

WRITTEN BY

Steve Cobham
Managing Director

WWW.STACK.CO.UK

Introduction

AUTUMN NEWSLETTER
2016

Welcome to the Stack Group Autumn 2016 Newsletter

Hello, and welcome to our Autumn Newsletter. Over the next few months we have got some exciting events planned. On 22nd November 2016 we will be holding a Business Continuity Brief at Old Trafford in Manchester. During this event we will be explaining how new technologies can help you to improve and future proof your business continuity plan.

We are also pleased to be continuing with our tradition of hosting clients at The Liverpool Philharmonic Spirit of Christmas Concert. You are invited to attend this event, which takes place on 20th December 2016. If you would like to attend, please RSVP by email to levans@stack.co.uk, or read more below.

Finally, we would like to draw your attention to our Industry Insights article, where Group Chairman, Jeff Orr, talks about the threat of Ransomware, and how hackers use social engineering techniques to manipulate people in to activating ransomware on their own device.

We hope you have a beautiful autumn

Best wishes,

Steve Cobham
Managing Director

Industry Insight

1/4

AUTUMN NEWSLETTER
2016

How Do They Hack Your Head? Social Engineering and its Role in Ransomware.

Ransomware is a type of malware used to attack individuals or organisations by encrypting valuable files, before demanding a ransom to decrypt them. It represents a growing problem all over the world with there being a 550% increase in the number of attacks in 2015-2016, compared to the previous 12 months. The reason for this rise is because it is simple to launch an attack and common for victims to pay the ransom, meaning that criminals can make huge amounts of money – quickly.

In order to enhance their success, hackers are increasingly using social engineering to exploit the weakest point in your security – people. Psychological techniques can be used to manipulate individuals to carry out actions which result in malware being activated. Cyber-criminals frequently play on feelings such as fear, urgency and curiosity.

Social engineering techniques have been commonly used against home computer users for a number of years, with banking link scams and tax refund cons being commonplace. However, there are now certain techniques which specifically target people in the workplace.

(CONTINUED)

Industry Insight

2/4

AUTUMN NEWSLETTER
2016

How Do They Hack Your Head? Social Engineering and its Role in Ransomware.

Before looking at these techniques, it is worth thinking about the aim of the criminals in the first place; to persuade the user to open a Trojan attachment which automatically installs ransomware; or to lead users to visit websites which are deliberately infected with malware.

One common technique used to meet these aims is spear phishing. Prior to an email being sent, the cybercriminal will identify and research the target organisation, in order to understand what the company does, who the key personnel are, who the customers are, what email domains are used – even going so far as to find out which forums and social media sites staff contribute too.

Emails are then crafted to make you believe that they are from someone you know - such as a customer - and an attachment is included. Document titles such as “Purchase Order” or “Payment Confirmation” are cleverly used to increase the chances of you opening the attachment thus preying on feelings or urgency or curiosity. It looks valid, but once opened, ransomware is installed.

(CONTINUED)

Industry Insight

3/4

AUTUMN NEWSLETTER
2016

Another example may be an email which looks like it has been sent from someone internal to your business – perhaps a Manager or Director – who is asking for feedback on an urgent report within a tight deadline. You open the attachment, which then invites you to enable macros in order to view the content. Because of the deadline, you do this and, once again, ransomware installs.

On other occasions, rather than encourage users to open attachments, cyber-criminals may manipulate users to visit websites which look both legitimate and relevant to their job role. By clicking on a link within an email, the user inadvertently visits a website already infected with malware. In the example below, the sender poses as an internal staff member. The criminal has clearly done research beforehand in order to know that the target contributes to the “Spiceworks” forum. By stating that confidential company data may have been divulged and that negative comments about the company are available online, the attacker capitalises on feelings of fear and urgency to encourage the recipient to act quickly. Finally, the web link included looks realistic, which further increases the likelihood of the target opening the website. In an example like this, we feel that a vast majority of people would fall victim to the attack.

(CONTINUED)

Industry Insight

4/4

AUTUMN NEWSLETTER
2016

Example Email

Hi Stu, I noticed that a user named securitybull72(claiming to be an employee) in a security forum posted some negative comments about the company in general and you in specific. He gave detailed instances on his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

The post generated quite a few replies, most of them agreeing with negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through appropriate channels before making this post. The link to the post is located here (it is the second one in the thread):

www.spiceworks.com/forums/security/234664/2345466.

Could you please talk to him?

Thanks,
Ste

Whilst ensuring that you have an adequate security solution in place is a sensible first step, it is important to understand that in some cases, ransomware can and does get through. Educating staff about the techniques used by hackers will help you to enhance your security even further, whilst we also recommend that you use a robust backup and recovery solution, to quickly get back on track in the event of an attack.

If you would like any help or advice about ransomware, please do not hesitate to contact an IT security expert such as Stack Group.

Next Generation Business Continuity

1/2

AUTUMN NEWSLETTER
2016

TECHNOLOGY FROM DELL EMC DELIVERED BY THE EXPERTS AT STACK GROUP

ABOUT THE EVENT

Information and data is at the heart of most businesses, with customer records, invoices, banking details and much more being critical to success. If this information was lost - be it through cyber-attack, human error, or natural disaster – could you continue to trade and how long would it take your business to get back on track? During this business event, Steve Cobham - Managing Director of Stack Group - will be discussing the importance of having a business continuity plan, and how new cloud technologies can help you to recover from disaster within minutes. Following on from this, Spencer Ralph from Dell EMC will provide the latest update on VxRail. Finally, Adam Lawton will introduce Unity – the newest midrange storage solution from Dell EMC. This will be a fantastic opportunity for you to be one of the first people to learn more about this new product. Lunch will then be served and our experts will be on hand to discuss any questions you have.

Date

22nd November 2016

(CONTINUED)

Next Generation Business Continuity

2/2

AUTUMN NEWSLETTER
2016

Speakers

Steve Cobham
Managing Director, Stack Group

A highly respected professional within the IT services industry, Steve is a Chartered Engineer with over 20 years' experience of advising on and building robust IT solutions for businesses across the UK.

Spencer Ralph
Senior Architect, Dell EMC

As a senior VARchitect at EMC, Spencer has been working in the Virtualisation space for the last 12 years, gaining his VCP in 2003. He began his IT career in 1988 and says he has touched almost every type of technology in the industry.

Adam Lawton
Senior Partner Systems Engineer, Dell EMC

Adam is an expert in the area's of cloud services, business continuity and software defined storage. An experienced and talented communicator, Adam has worked with organisations across a broad range of market sectors.