a window into cyber

November 2020

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

Ransomware features large in this month's newsletter. We've mentioned it before, but I make no apology for keeping it in the spotlight. In September, an attack on Universal Health Services, a hospital and healthcare network with 400 facilities, crippled the company's computers. There's also been a dramatic recent rise in Emotet attacks, with cyber security agencies in France, the Netherlands, Italy, Japan and New Zealand publishing new warnings about this highly dangerous malware.

As I write, the NCAS has just issued an alert about the imminent risk of cyber attacks on US healthcare providers. In this new era of increased remote and mobile working, the criminals have never been more active – and organisations have never been more vulnerable.

This month's author Éireann Leverett gives us his unique perspective on ransomware – and our Datasafe page highlights the recent 'If You Connect It, Protect It' campaign. Ransomware is huge – and it's growing fast. But at Brit, we're with you every step of the way.

Once again, stay safe – and get in touch if you need us.

this month's author: **Éireann Leverett**

Co-founder, Concinnity Risks. Co-author: 'Solving Cyber Risk'

Éireann works on various research departments and loves quantifying cyber risks and studying cyber crime. He co-chairs the Cyber Insurance Special Interest Group at FIRST.org and speaks publicly at both hacker and insurance conferences regularly. He likes writing essays and exploits, and sitting in gardens and libraries of Cambridge learning.

Dissecting ransomware
(it's not Bitcoin's fault)

Éireann Leverett | Co-founder, Concinnity Risks
Co-author: 'Solving Cyber Risk'

Ransom and Extortion is the last refuge of the terminally incompetent. It's a thug's approach to making money through hacking. Other hackers find subtler and more interesting ways to make money like Fin5[1], or Magecart[2]. Personally, I think hacking for money is gauche, which is why I prefer to do it out of curiosity and for my own understanding.

The desire to get paid for it only surfaced when I realised I had to feed a family... though I confess I do spend a little money on Patxaran, too. I digress though, because I am here to tell you things you might not expect about ransomware. Firstly, some fools will no doubt try to tell you that ransomware is caused by Bitcoin. I can assure you the phenomenon predates Bitcoin[3], and extortion has been around since long before hacking or the US dollar. Secondly, people will try to blame the victim for lack of security or a failure to backup, but this is ridiculous too. We shouldn't accuse those targeted by abuse for deserving it. These criminal enterprises really are out to make money without regard to the impact on human life[4].

Now getting to the intersection of ransomware and insurance, it is clear that negotiating is now a full blown industry[5]. Clearly the ransoms get paid because the losses are assumed to be larger, but how big can the ransoms get?

It is clear that negotiating is now a full blown industry.

I decided to find out by gathering as much data as I could over the last few years. I wrote a dry academic paper with a few talented friends that will get published at eCrime2020 this year[6], covering the economics behind what I learned. If that sort of thing interests you, then do get in touch for the full copy.

Now, what makes a ransom large? Most people assume it is the virus itself; how destructive it is, how widely it spreads, how well constructed. Let's try a thought experiment though: what would happen if you were an elite cyber criminal and deployed ransomware in Cuba. The ransom can't be more than anyone earns, and while there might be some variance within those earnings, it's likely to be a pretty flat distribution. If your ransomware were to sample from a normally distributed range of incomes, you would certainly see more variance. Ideally though, you'd want to deploy your ransomware on companies with heavy tailed distributions of wealth. In other words, in a society like ours, where the distribution of wealth can be characterised by powerlaws, one really big score might be more than all the little ones combined!

Now we believe that ransoms alone are heavy tailed, and while there's more research to be done to confirm distributions, the averages of ransoms fluctuate wildly. So in a nutshell, ransoms ALONE have heavy tails, and if you're a bigger organisation, you'll get asked for a bigger ransom. Just because you don't know who they are doesn't mean they don't read your accounts. After all, they already hacked you, you can't be sure you've got any secrets left.

continued on next page

Just because you don't know who they are doesn't mean they don't read your accounts.

One thing we can be sure of is that the losses are usually bigger than the ransoms. Otherwise it would be mathematically irrational to pay them! The real problem is figuring out the risk and return on investment before you get hit with the ransomware. For that, you'll have to read our academic papers. Thank you for reading to the end, but it is time for me to get back to Bacalao and backgammon and next time we can discuss all the covers and triggers of ransomware.

Click for links:
1 Finn5
2 Magecart
3 Bitcoin
4 Hackney hacked
5 UCSF ransom
6 eCrime 2020

Adelle Gruber

Senior Underwriter, Global Cyber, Privacy & Technology

An underwriter's outlook

Ransomware: removing the fear factor through better preparation

The Covid-19 pandemic has presented the insurance industry with multiple changes. High on the list is the greater reliance on IT systems. A scattered workforce inevitably means a loss of oversight and control, with many employees working on home computers. The challenge for businesses and their IT departments lies in ensuring that their remote operations remain smooth, whilst preventing unauthorised access.

Against this backdrop, we have seen a marked increase in the frequency and scale of ransomware events. There is a theory that the willingness of companies with cyber insurance to pay ransoms has contributed to this. There is also anecdotal evidence that payment of ransoms, (which some companies believe to be the most economical way of getting back online rather than restoring from back-ups) actually makes them more likely to be targeted again.

The better prepared a business is to recover from a cyber incident, the lower the risk they'll have to contemplate paying a ransom to continue trading. Brit's range of services, from cyber fitness checks and incident response planning to our virtual CISO and panel of experts help our clients stay ahead of the hackers.

Adelle recently contributed to Cyber Security: getting ahead of the hackers for *Insider Engage*. Read the whole article here.

highlights from datasafe

BRIT

Datasafe provides the latest risk management resources, enabling Brit's clients to proactively manage their data protection and privacy risks.

Current hot topics for Brit policyholders

top training courses completed:

Ransomware

Spear-Phishing

Malware

Public Wi-Fi

Phishing

Password Best Practices

Employee Mistakes

Privacy Basics 2

top resources accessed:

- Cybersecurity Fitness Check
- Classifying Your Data
- HIPAA Risk Assessment Workbook
- How to Securely Work from Home
- Information Security Incident Response Plan
- Methodologies for Risk Assessment
- NIST Risk Assessment Workbook
- Personal Mobile Device Security Policy

One of our recent campaign topics was:

If You Connect it, Protect it

Connected devices make businesses more productive. But there are many security trade-offs. Here are some best practices for using connected devices.

Brit Cybersecurity Byte

- Research the security reputation of a connected device before purchasing.
- Change all default passwords to strong ones (many characters, uppercase, lowercase, numbers, and symbols).
- Use multi-factor authentication.
- Keep software up to date.
- Disable unneeded features.
- Turn off the device when not using it.
- Erase all sensitive data when decommissioning it.

Online Training for Data Security Basics

Understanding how to keep your devices secure can give you and your organisation a leg up when it comes to preventing a data breach. This mini-series explains the basics when it comes to data security best practices.

- Malware
- Password Best Practices
- Public Wi-Fi

stop press urgent cybersecurity alert

On 28 October the US Government's National Cyber Awareness System (NCAS) issued an advisory note. It warns of specific ransomware actively targeting US hospitals and healthcare providers.

Be vigilant – Businesses should look for precursor Ryuk malware such as Trickbot and/or Emotet. Trickbot may appear as an executable file with a 12-character (includes .exe), randomly generated file name
(eg mtjdieks.exe) found in one of the following directories.
C:\Windows\
C:\Windows\SysWOW64\
C:\Users\[Username]\AppData\Roaming\

Act fast – If you suspect you have this malware on your system, call 855-440-3400 immediately, and:

- Back up critical data (including EHR) and isolate or air gap those backups
- Alert your internal Incident Response Team and IT department
- Keep and review hard copies of your incident response/business continuity plans (including out of band communications and key contact information)
- Ensure proper staffing and check systems are patched and up to date

Although this alert is specific to healthcare organisations, ALL businesses should remain vigilant. For details click here.

britinsurance.com/cyber