SUTHERLAND SHIRE BUSINESS CHAMBER

Detective Senior Constable Glen Spooner
Cybercrime Squad
State Crime Command

29th May 2019

TOPICS

- Business Email Compromise (BEC)
- Safety Practices
- Ransomware
- Crypto Currencies
- “Dark Net”

BUSINESS EMAIL COMPROMISE

According to the Federal Bureau of Investigation (FBI), this scheme has already caused US$12.5 billion losses to companies as of 2018.

This shows that BEC scams, while usually technically simple, are highly effective. We actively track BEC attempts and recorded 9,291 BEC attempts in 2018 Q1-Q3, a 46-percent increase from last year's 6,342 in the same period.

In our data, the U.S., Australia, and the U.K emerged as the top three countries most targeted by scammers.

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-end-review-business-email-compromise-in-2018

BUSINESS EMAIL COMPROMISE

- A Business Email Compromise (BEC) is a form of spear (targeted) phishing that aims to trick employees (mostly in finance) into transferring funds into a ‘new’ business bank account (belonging to the cyber criminal) or sharing sensitive information at the request of a cybercriminal impersonating a senior executive.
- Because these scams don't often use malicious links or attachments, they can get past **anti-virus** programs and **spam filters**. These emails also bypass **firewall** settings – what you thought as being your protection systems.
- Maybe plain text but usually include Word or PDF attachments (requests).
- Can come from actual known accounts or ones that appear to be real accounts you have dealt with in the past.
- Glen.brown@AustralianSandAndSoil.com.au
- Stuart.littlemore@bec.com.au
- **Can be internal mail requesting payment or external requesting payment**

HOW?

- **Internal account take over with credentials obtained from social media accounts or other publicly available private information – Spear fishing attack**
  - Now that control has been compromised – email sent with request for payment
  - Email deleted
  - Deleted mailbox removed
  - Mail rule setup to receive reply mail and forward to secondary mailbox account
  - Mail rule to delete incoming mail.
- **External - Registering of a Domain Name Server (DNS) (business name) similar to the real DNS.**
  - **Glen.brown@AustralianSandAndSoi1.com.au**
- Compromised internal or external system, to create similar account names within registered a DNS (Most spoofed positions are the CEO or Managing Director, targeting the CFO and Finance Director.) Alteration (spoofing) of an email sender address so that the message appears to have originated from a trusted source other than the actual source.
  - **Stuart.litt1emore@bec.com.au**

WARNING SIGNS

- Transfer requests sent when requester is travelling or otherwise unavailable.
- Transfer requests are sent near COB hours.
- Urgent/confidential transfer requests.
- Unknown persons

  Glen.brown@Austra1ianSandAndSoi1.com.au

  Stuart.littlenore@bec.com.au
- Poor use of English language.
- Vague accounting information
- **Generally if an account update is requested, or new payee – alarm bells should be ringing**

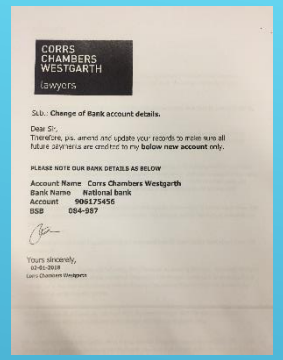
PREVENTION & TRAINING

- Employees receive latest phishing prevention/awareness training.
- Penetration Testing including simulated real time situation training.
- Encourage staff to ask questions and engage with their IT staff if they find something suspicious.
- **Check with the sender either face to face or by phone and use company directory not phone number provided in the email. (2FA)**
- **Not open any attachments or links. (System breach – escalation of privileges / ransomware)**
- Limit social media and casual browsing at work.
- Limit the use of unsecured Wi-Fi networks with business based devices.
- Multi purpose approval process for transactions over a certain threshold.

TYPICAL SETUP

FROM: CFO(Glen.brown@AustralianSandAndSoi1.com.au)

TO: ACCOUNTS(Stuart.1ittlemore@bec.com.au)



INTER NATIONAL BANK

UNCLASSIFIED

NEW SOUTH WALES POLICE FORCE
CULPAM POENA PREMIT COMES

RANSOMWARE

- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them
- Typical payments are made through virtual currencies, most notably Bitcoin
- The infection of ransomware is usually done by the person themselves by
  - **Clicking a link within an email (hover over the link, what does the URL look like)**
  - **Opening a document attached within an email (macro driven / self executing)**
  - **Visiting Internet sites that contain harmful content**

REAL COST OF RANSOMWARE

- In 2015 the cost of ransomware was an estimated **$24 million**
- In 2016 the cost of ransomware was around $1 billion dollars.
- In 2017 the cost of ransomware was around $2 billion dollars.
- In 2018 it was estimated that ransomware drained an estimated **$5 billion** from the global economy last year and has retained its position at the top of the malware threat list in 2018

- https://www.comparitech.com/antivirus/ransomware-statistics/

RANSOMWARE - 2019

File-encrypting ransomware has gone through significant ups and dramatic downs over the past few years.

Overshadowed by the influx of malicious cryptocurrency mining applications in late 2017, this area of cybercrime took a nosedive only the most durable strains could survive.

A sample called GandCrab made its debut in the midst of this hiatus and became a game changer.

In the first quarter of the year, the average daily ransom being paid to attackers rose to $12,762 from $6,733 in Q4 2018.

RANSOMWARE - 2019

GandCrab v5 ransomware is back with new features

By **Giedrius Majauskas** March 1, 2019 00:43 4

This fall has not only brought us rain, cold and colorful leaves, but also the notorious GandCrab ransomware back, this time even more improved and vicious. GandCrab v5 just showed up on September 24, 2018, roaming around and encrypting precious personal files all around the globe, but mainly Central Europe. After getting rather upset about the Pre-infection vaccine for the 4th GandCrab, developers had to take some time and figure how to improve the maliciousness and increase the chances of getting ransom from the victims. Therefore after a couple of months now we see the fifth and the latest GandCrab ransomware variant.

Latest infections

BabyNameReady Extension

1 Click PDF Malware

Webload.world pop-up virus

"Your PayPal Account Is On Temporary Hold" phishing scam

"Windows Detected Alureon Attack" warning

MaxWebSearch

Wal ransomware

Totmania.net pop-up virus

Aurora Cheat Tool

DriverHub PUP

Security Guides

Google redirect virus guide

Ransomware By extension

Stay connected

UNCLASSIFIED

RANSOMWARE - EFFECT

UNCLASSIFIED

CRYPTO / VIRTUAL CURRENCIES

UNCLASSIFIED

RANSOMWARE - PAYMENTS

Current price: $2,400.00. As payment, you need cryptocurrency DASH or Bitcoin

UNCLASSIFIED

HOW MANY CRYPTO / VIRTUAL CURRENCIES EXIST

Approximately 2,112

APPROXIMATE VALUE?

Approximately $350 Billion

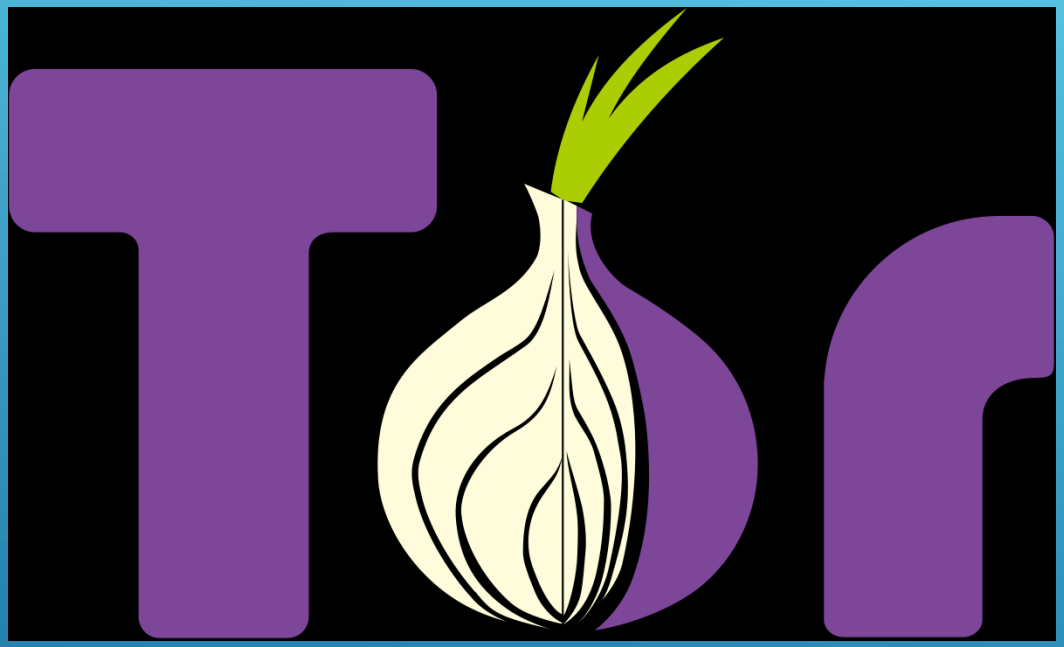
WHAT IS A CRYPTO / VIRTUAL CURRENCY ?

- There is no agreed world wide definition !!!
- Crypto / virtual currency can best be described as digital money / tokens / property/ shares but they all hold some type of value and it can be exchanged / converted for either real money or other crypto / virtual currencies.
- In contrast, a digital currency is a currency that is non convertible !!!
- It is purchased in one system and it must be used inside the same system. Eg: Inside a video game you buy your digital currency and it is exchanged for some item within that game system but you can not exchange or convert it back to a digital currency

DARK WEB

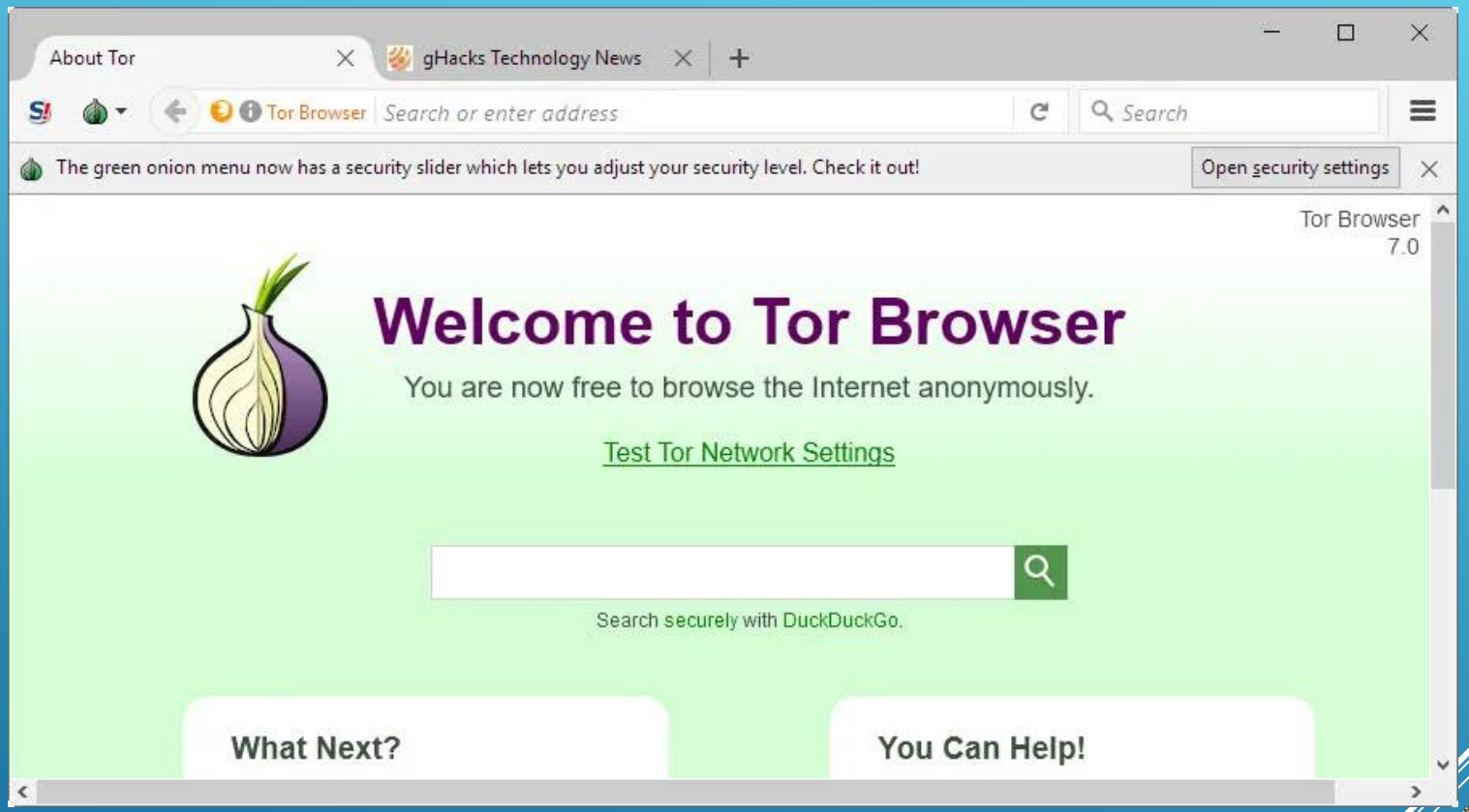
UNCLASSIFIED

TOR – THE ONION ROUTER



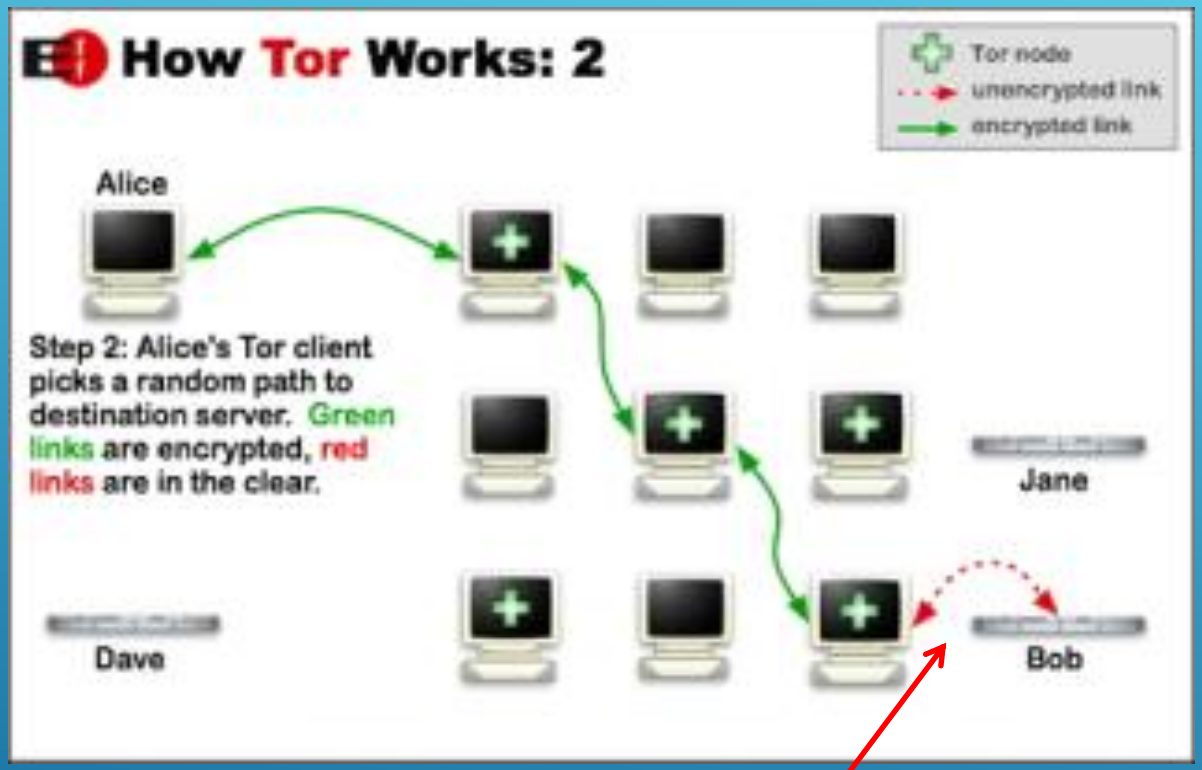
UNCLASSIFIED

DARK WEB



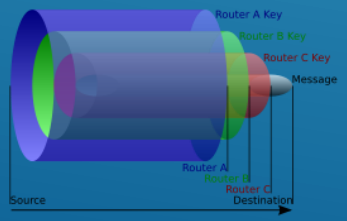
UNCLASSIFIED

HOW DOES TOR WORK?



Any message sent by the Tor network only knows where it is going, it does not know where it has come from.

Each message is encrypted by each node for the journey between nodes. At each node the message is decrypted and re-encrypted for the next travel to the next node



The message at all points in the chain is encrypted except when it exits the last node.

UNCLASSIFIED

REMEMBER THE TWO EMAIL ADDRESSES?

Varying Domain Name

- Glen.brown@AustralianSandAndSoi1.com.au
- Glen.brown@Austra1ianSandAndSoil.com.au
- Glen.brown@AustralianSandAndSoi1.com.au
- Glen.brown@Austra1ianSandAndSoi1.com.au

Varying Account Name

- Stuart.littlemore@bec.com.au,
- Stuart.litt1emore@bec.com.au,
- Stuart.1ittlemore@bec.com.au,
- Stuart.littlenore@bec.com.au,

UNCLASSIFIED