Cyber Security Update

Simon Bulleyment

Director





www.sibrossa.com









Topics

- Ransomware
- Targeted phishing attacks
- What you can do and where you can get help
- Cyber Essentials





Ransomware - what's changed?

- How it was
 - WannaCry (2017)
- 'Professionalisation' of ransomware organisations
- Ransomware as a Service
 - Shift from sophisticated to the less sophisticated
- Double extortion tactics
 - Data exfiltration
- Multi extortion tactics
 - Denial of Service (DoS) attacks





Ransomware in 2022



66%

hit by ransomware in the last year



65%

72%

attacks resulted in data encryption



experienced an increase in volume/ complexity/impact of cyber attacks



\$812,360

average ransom payment (excluding outliers)



86%

ransomware attack caused loss of business/revenue

SOPHOS Cybersecurity delivered.

The State of Ransomware 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries.



98%

pay-out rate on ransomware claims





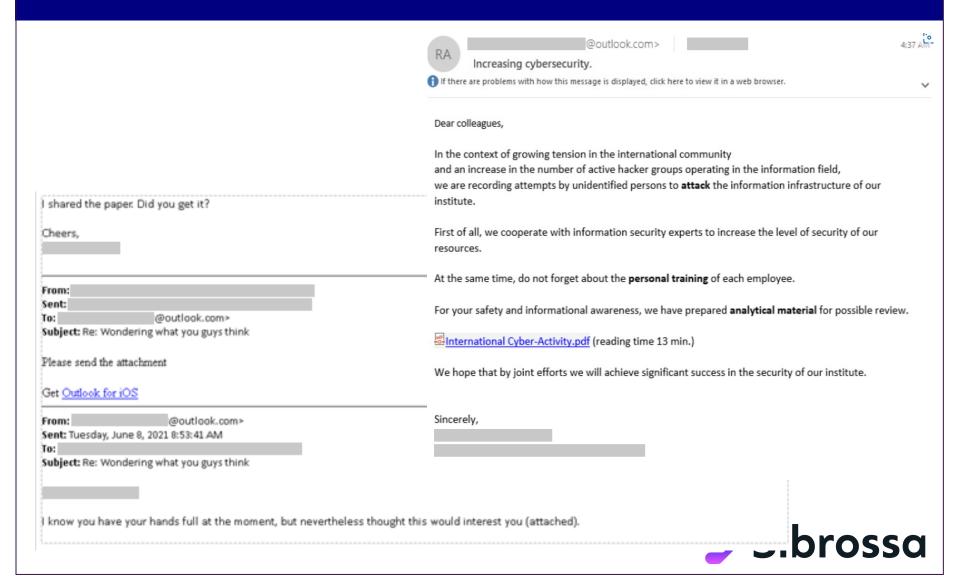
Phishing attacks

- Phishing/spear phishing
- The rise of smishing attacks
- Microsoft Threat Intelligence Center
 - SEABORGIUM
 - Primarily targets NATO countries, particularly US/UK
 - No prizes for guessing origin of attacks!
 - Use of social media, LinkedIn, general open-source intelligence
 - Attacks on Microsoft 365 (email: attachments/URLs, OneDrive)
- What can you do?
 - Review email security controls
 - User awareness and processes
 - Implement multi-factor authentication (MFA)





SEABORGIUM





Where can you get help?

- National Cyber Security Centre
- Cyber Security: Small Charity Guide
 - https://www.ncsc.gov.uk/collection/charity/cyber-security-smallcharity-guide-pdf-download
- For larger charities, the cyber security Board Toolkit
 - https://www.ncsc.gov.uk/collection/board-toolkit
- For medium and larger charities (can be used in tandem with the Board Toolkit), 10 Steps to Cyber Security
 - https://www.ncsc.gov.uk/news/large-uk-organisation-10-steps-stayahead





What can you do?

- Updated risk assessments
- Cyber improvement plan/strategy
- Implement controls, review effectiveness, test
- Obtain cyber security insurance
- Create a cyber incident response plan
 - Consider a third-party service
 - Table-top exercises
 - Red Team testing
- NCSC Early Warning Service
 - https://www.ncsc.gov.uk/information/early-warning-service





Cyber Essentials

- Government backed
 - Aim
- Value to organisations
- What is is
 - Self assessment
 - Covers five areas
 - Annual renewal
 - Fixed fee
 - Prescriptive controls
- It's difficult to achieve ... and that's a good thing!
- Cyber Essentials Plus



Micro organisations (0-9 employees)	£300 +VAT
Small organisations (10-49 employees)	£400 +VAT
Medium organisations (50-249 employees)	£450 +VAT
Large organisations (250+ employees)	£500 +VAT

