Making Sense of Office 365 Email (In)Security

13-14 November 2018

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd
ABN 14 098 237 908

Sydney
Level 8, 59 Goulburn Street
Sydney NSW 2000

Melbourne
Level 15, 401 Docklands Drive
Docklands VIC 3008

Tel. 1300 922 923
Intl. +61 2 9290 4444
www.senseofsecurity.com.au

@ITSecurityAU

1. Why Mail is a Good Target and O365 Context
2. Anatomy of Typical O365 Hack
3. Indicators of Compromise
4. Regulatory Impact and Countermeasures

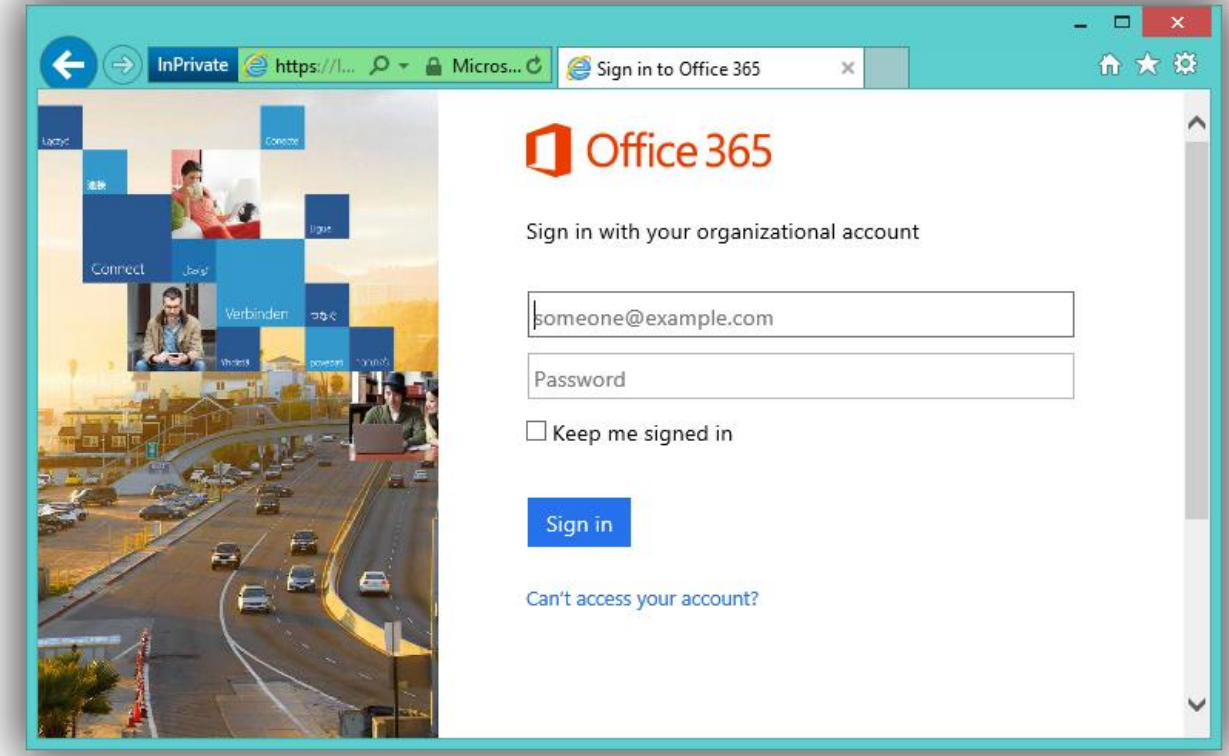
Why Mail is a Good Target

- Inbox has become the “document management system” of choice
- Trusted communication by many
- Accepted way of transacting
- Data can be easily monetised
- Launchpad for further attacks

O365 Context

- Cloud-based SaaS business system
- Over 120M business users
- Strong investment in data security
- Many independent certifications
- No breaches of the platform have ever been publicised
- Many **configurable** security controls

Anatomy of Typical O365 Attack



Anatomy of Typical O365 Attack

Step 1:
Usernames /
Email addresses

Buying lists

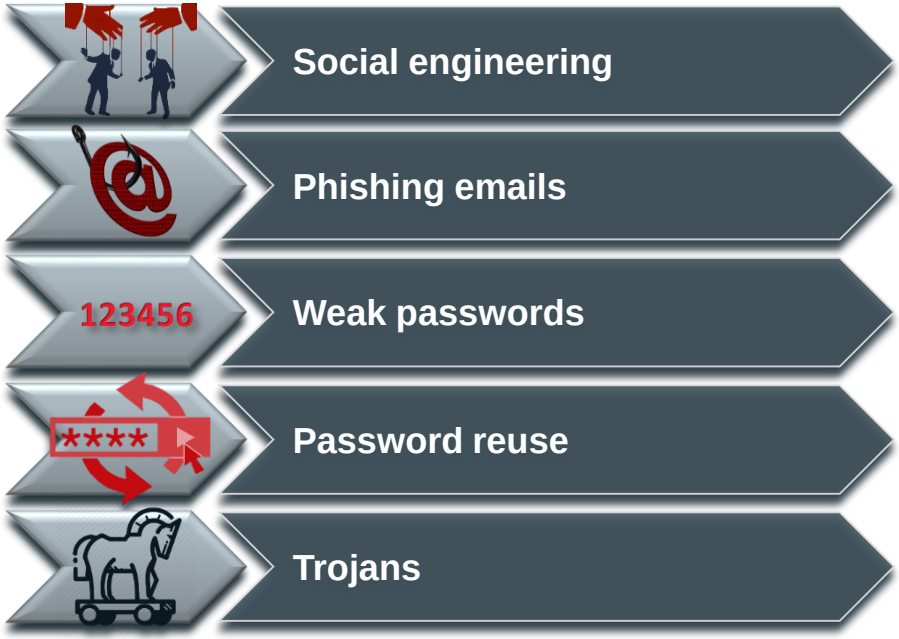
Public breach dumps

Services and Tools

Social media

Anatomy of Typical O365 Attack

Step 2: Password



Anatomy of Typical O365 Attack

Step 3:
Access is obtained

- Scour compromised in-box for confidential data, personal data, any transactional data
- Might email all your contacts (or a sample)
- Begin monitoring your email communications looking for something they can abuse
- Transact
- Abuse Skype and other O365 services to steal further data (OneDrive) or increase credibility with real-time chat
- Attacker can sit idle for extended periods and wait for the perfect moment to pounce

Indicators of Compromise

How individuals should know they've been p0wn3d:

- Sent or Deleted Items folders contain messages you did not write
- Identify unusual profile changes
- Unusual credential changes
- Mail forwarding was recently added
- Unusual email signature was recently added

Source: Microsoft

Impact of NDB

Australian Government
Office of the Australian Information Commissioner

- *Imposes data breach notification obligations on entities when a data breach is likely to result in serious harm to any individuals whose personal information is involved in a breach…*
- *Organisations that suspect an eligible data breach may have occurred must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected…*
- Email compromises are expensive breaches to investigate
- Years of emails need to reviewed to identify PII or PHI that may have been compromised

Countermeasures

1. Security awareness training and testing
2. Multi-Factor Authentication*
3. Improve internal control processes
4. O365 hardening, alerting, email security basics
5. Third-party mail gateway
6. Post-delivery protection
7. Immutable email archive
8. Well-defined incident response and escalation procedure
9. Detailed and thorough compliance policies and requirements

Thank You!

Questions?

Security, it's all we do. Knowledge, Experience & Trust.

Sense of Security Pty Ltd
ABN 14 098 237 908

Sydney
Level 8, 59 Goulburn Street
Sydney NSW 2000

Melbourne
Level 15, 401 Docklands Drive
Docklands VIC 3008

Tel. 1300 922 923
Intl. +61 2 9290 4444
www.senseofsecurity.com.au

@ITSecurityAU