Notes from the field

George Balafoutis
Cybersecurity Architect
Microsoft

MALTA INFORMATION TECHNOLOGY AGENCY

CYBER SECURITY MALTA
Digital Security Your Priority

What we will cover

- Quick Refresher
- What sensors are seeing
- What cybersecurity consultants are seeing (Redacted)
- Take-home lessons
- Where to start

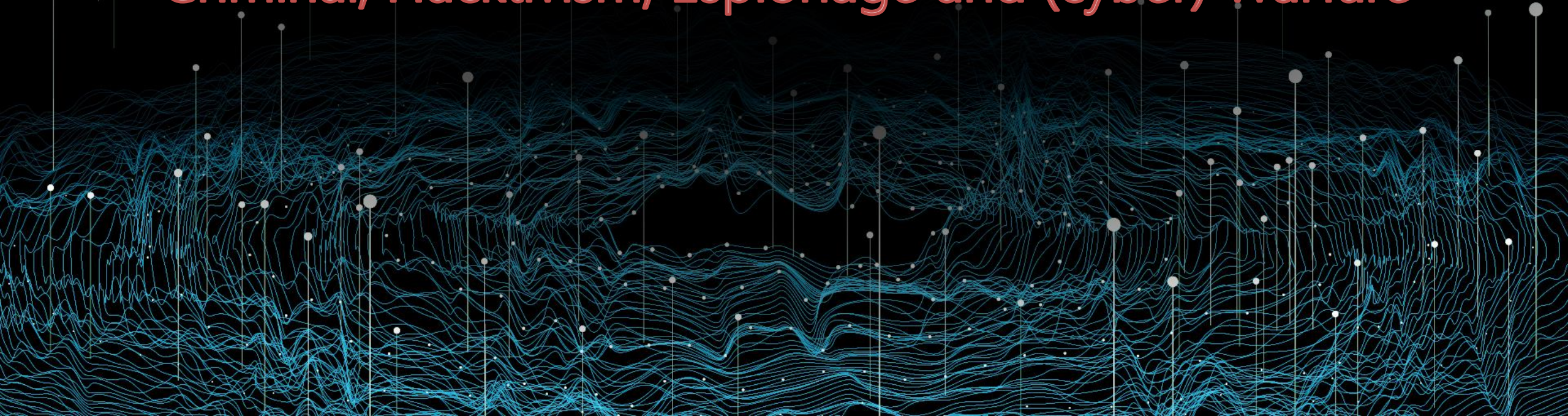
QUICK REFRESHERS

Microsoft

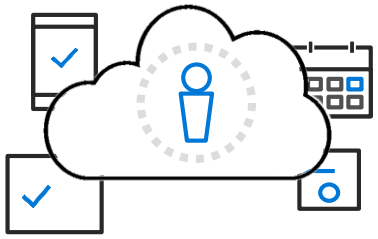
The world is changing…are you prepared?

CHEW

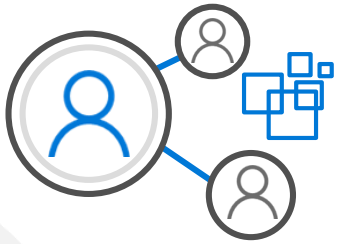
Criminal, Hacktivism, Espionage and (cyber) Warfare



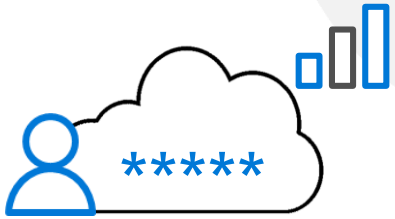
Identity is central to digital transformation – and it's where attackers focus



Seamless access across apps, groups, and devices across the organization



Collaboration and data sharing with teams and partners



IT efficiency with self-service management for passwords and access

Enhanced security and compliance with access policies

100 million
user identities attacked every month

Source: GCI blog, 4 October 2017

300% increase
in identity-based attacks reported in the last year

Source: Microsoft Security Intelligence Report, vol 22

$15 million
average cost of breach and associated business impact (plus loss of partner and customer trust, damage to reputation)

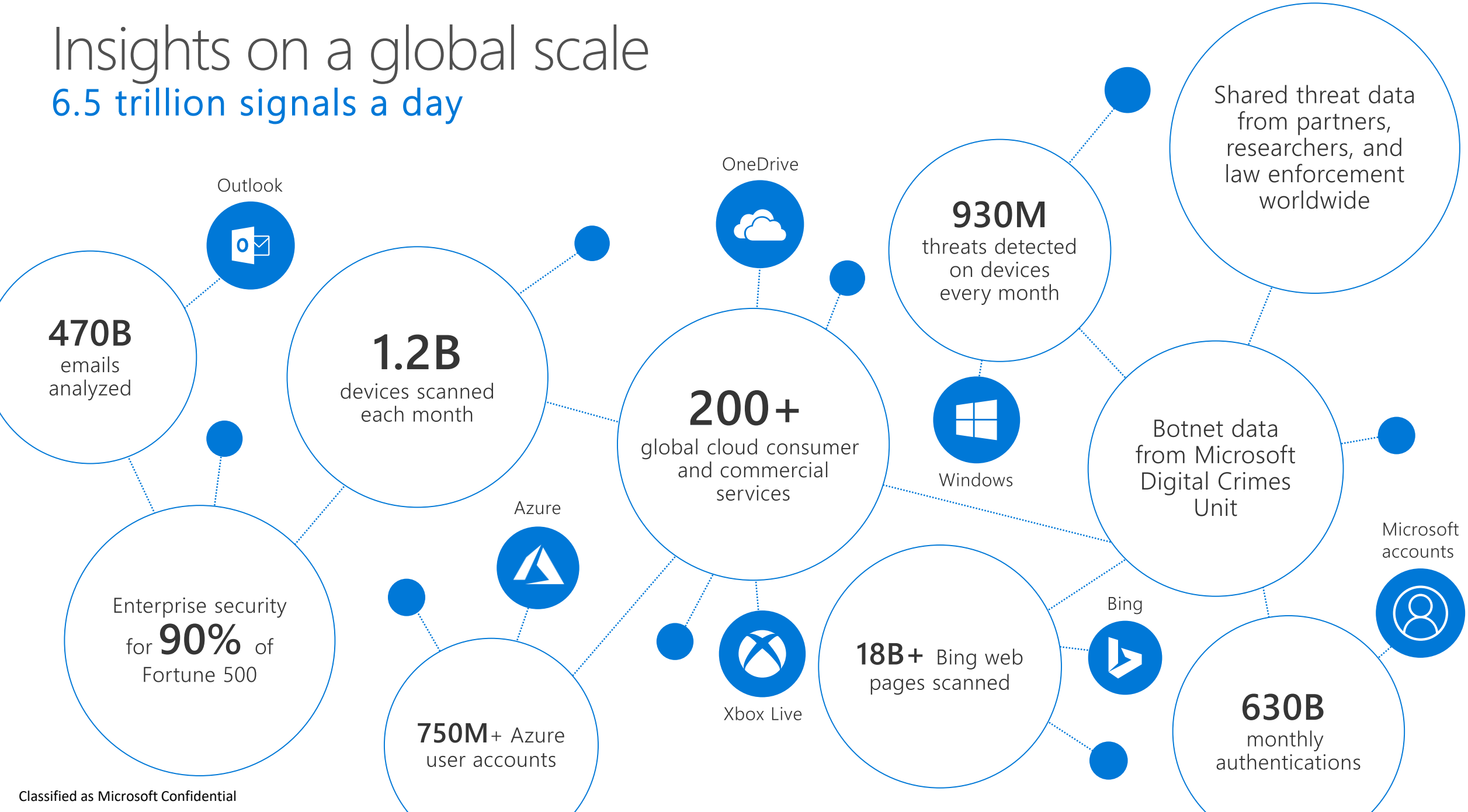
Source: GCI blog, 4 October 2017

WHAT SENSORS ARE SEEING

Microsoft

Insights on a global scale

6.5 trillion signals a day



What Sensors Are Seeing

SIR v24 identified 3 main topics

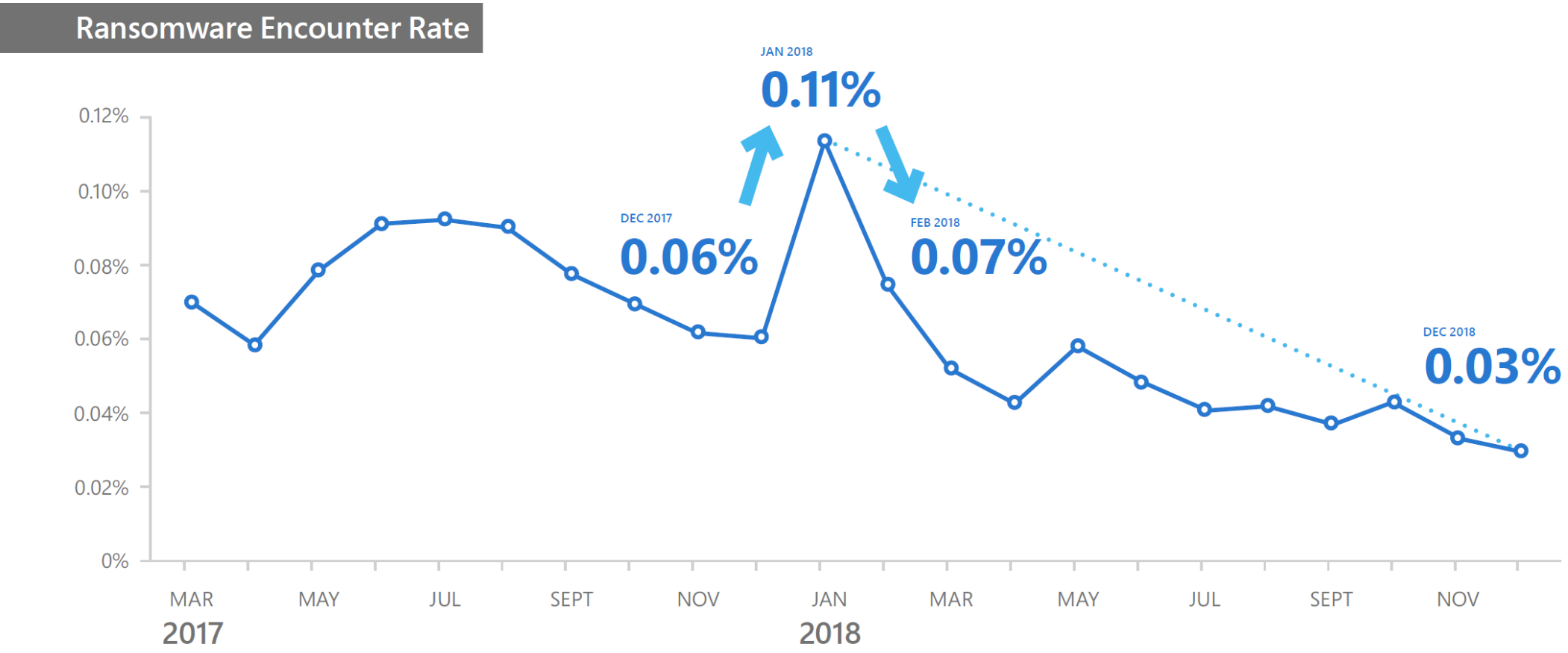
1. Ransomware vs. crypto-currency mining

2. Easy mark attack methods

3. Supply chain compromises

1. Ransomware vs. crypto-currency mining

Ransomware encounter rates **declined approximately 60%** between March 2017 and December 2018

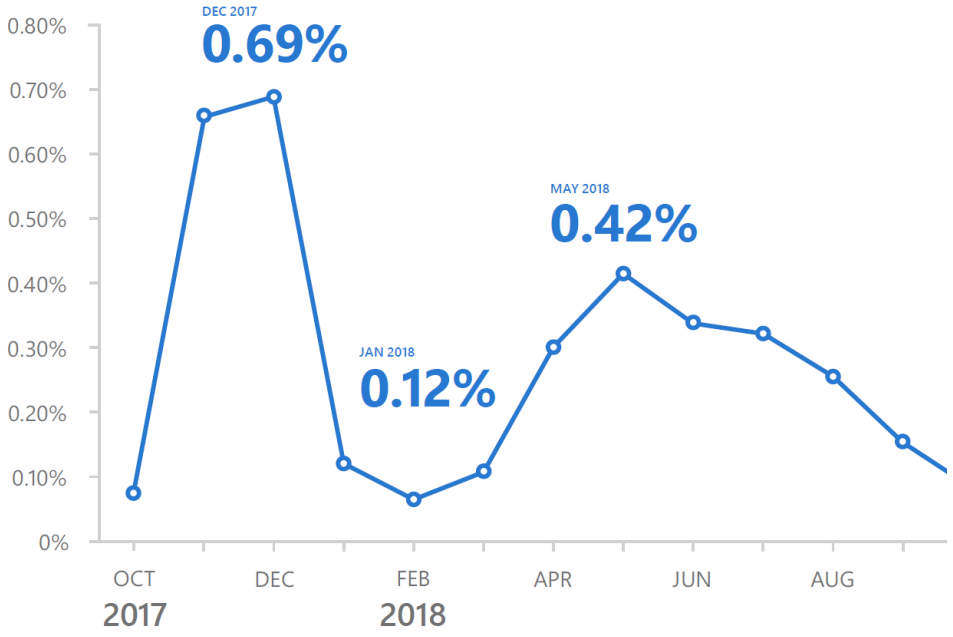


1. Ransomware vs. crypto-currency mining

Mining coins continues to be **lucrative**

Encounter **trends shift with crypto-currency prices**

Brocoiner Encounter Rate



Bitcoin prices

2. Easy mark attack methods

Phishing

Broad-based phishing and spear phishing both rely on what's most often cited as security's weakest link: people. Phishing can take many shapes, including:

Email links and attachments

Domain spoofs

User impersonation

Domain impersonation

Links to fake SaaS apps

180,000,000–200,000,000

Approximate number of phishing emails Microsoft detected each month, over three months (November 2017 - January 2018).

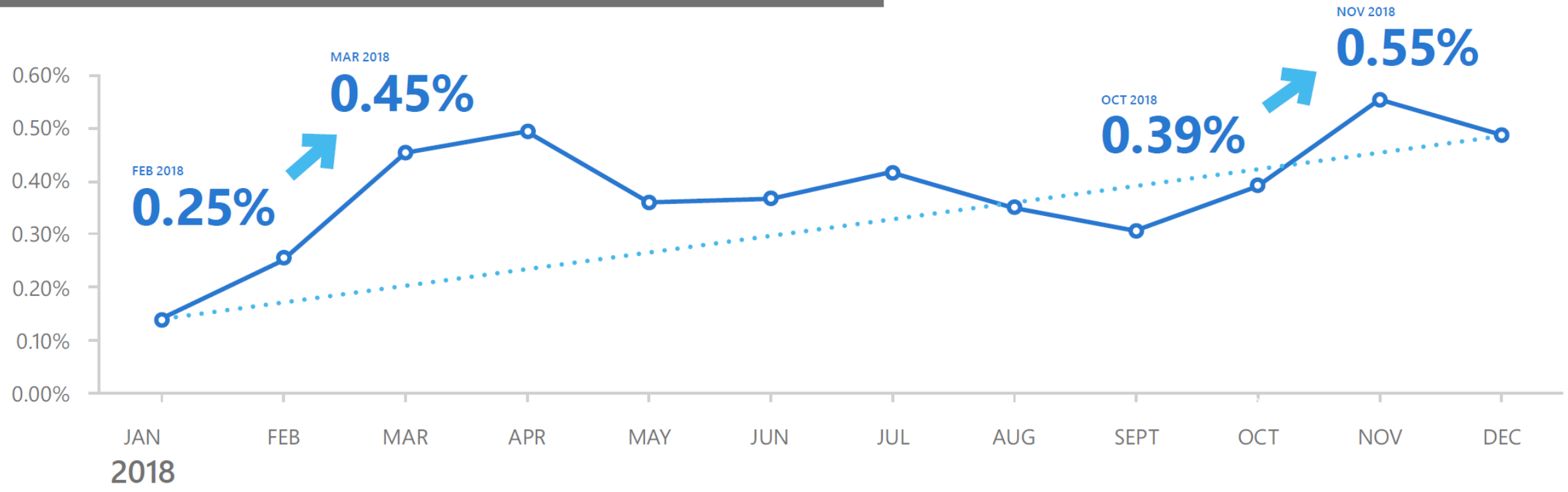
Microsoft

2. Easy mark attack methods

Inbound emails that were **phishing messages increased 250%** between January and December 2018

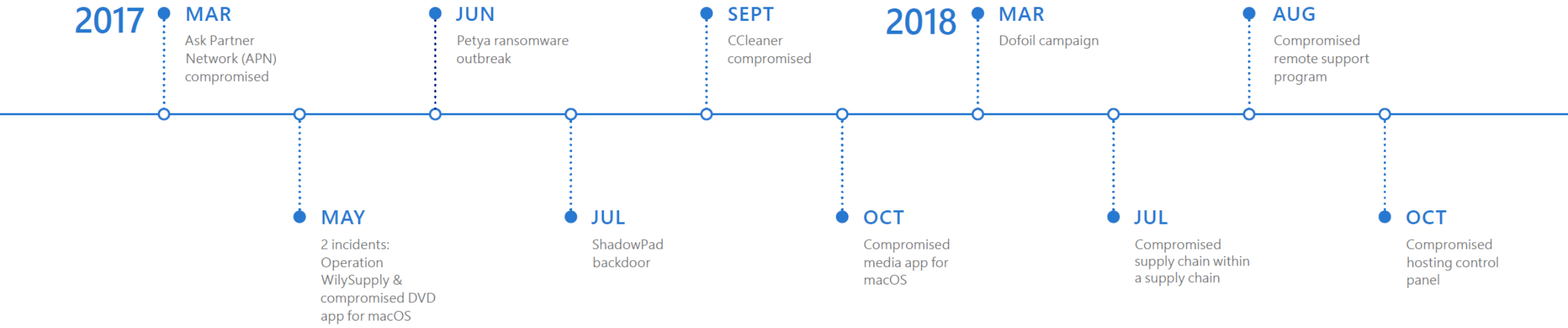
Phishing rates are still on the rise

Percentage of total inbound emails that are phishing emails



3. Supply Chain compromises

Software **supply chain attacks have been increasing** in the last few years



THIS SECTION IS REDACTED
FROM FINAL HANDOUT

WHAT CYBERSECURITY CONSULTANTS ARE SEEING

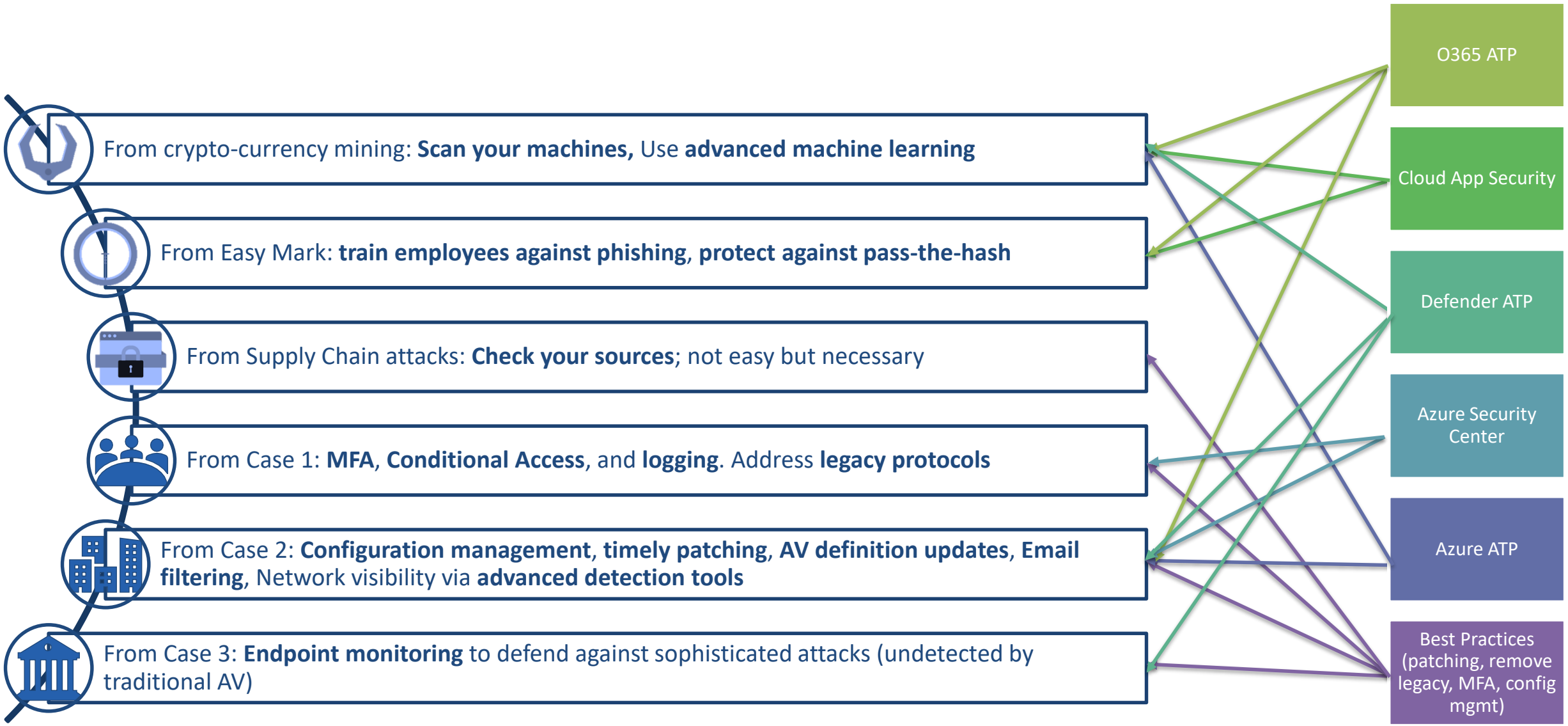
The examples used have modifications to obfuscate attacker methodology

Microsoft

LESSONS LEARNED

Microsoft

Lessons Learned (Partial list)



Basic Recommendations

- **Security hygiene is critical**
  remove legacy, perform patching, enable MFA & logging, etc.
- **Implement access controls**
  especially for sensitive/privileged roles; they have keys to the kingdom
- **Keep backups**
  warm and cold, to make ransomware irrelevant
- **Be aware and act**
  have an incident response plan in place; test it regularly
- **Stay up-to-date**
  www.microsoft.com/security/blog

Microsoft

mita
MALTA INFORMATION TECHNOLOGY AGENCY

THANK YOU

MALTA INFORMATION TECHNOLOGY AGENCY

Microsoft

CYBER SECURITY MALTA
Digital Security Your Priority