



**CHECK POINT
INCIDENT RESPONSE TEAM**

TALES FROM THE TRENCHES

RAYMOND SCHIPPERS - LEAD ANALYST - AMA

TLP: GREEN

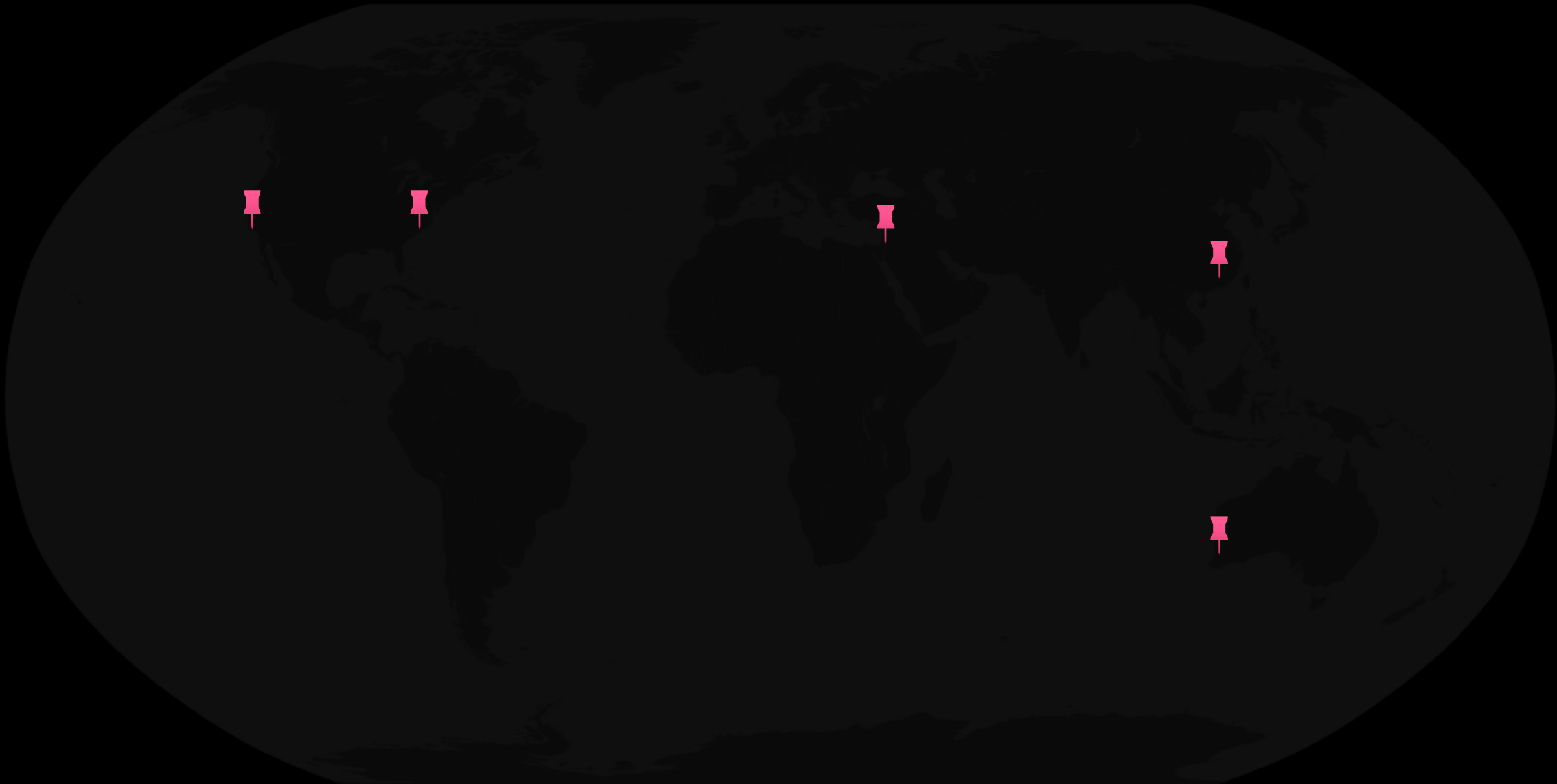
RAYMOND SCHIPPERS



- Lead Analyst AMA (Asia, Middle East, Africa)\
- Leading outreach
- Previously SecOps lead, gambling company
- Enjoy hunting bad guys

- No photos please

WHO AM I?



24/7/365

GLOBAL COVERAGE

Report

Summary: Last 7 days

HOST STATUS

Compromised



48

COMPROMISED

58

HOSTS

Top Compromised Objects

665

[12839384.exe](#)

[12903696.exe](#)

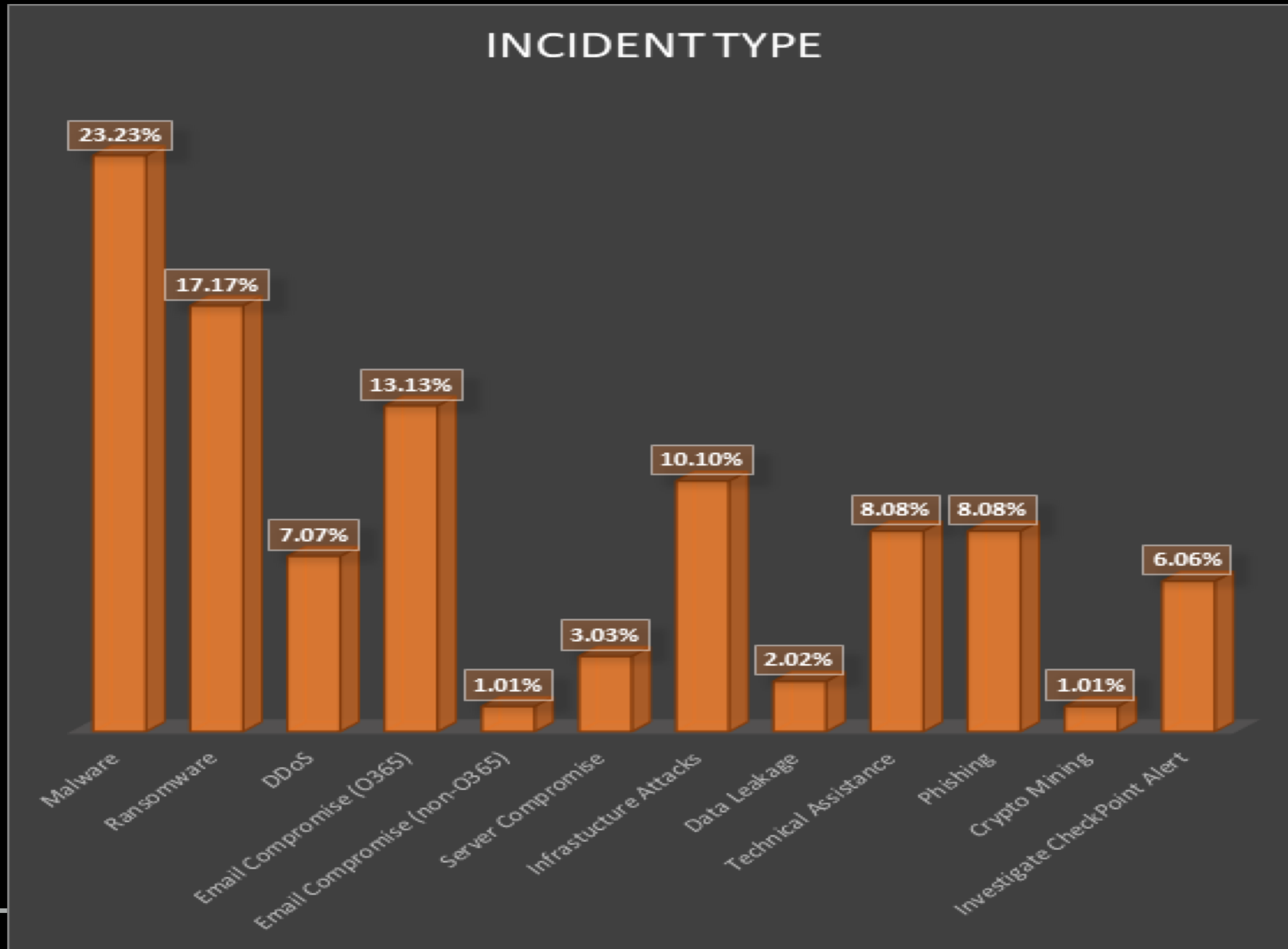
[14412248.exe](#)

WE INVESTIGATE

WHAT DO WE DO?

Q3 2018

TRENDS

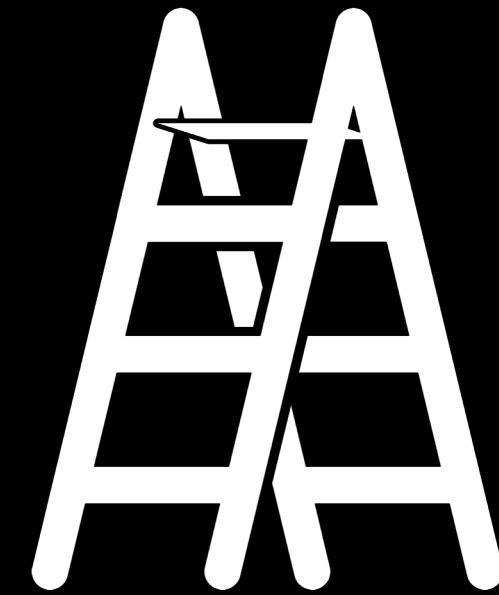
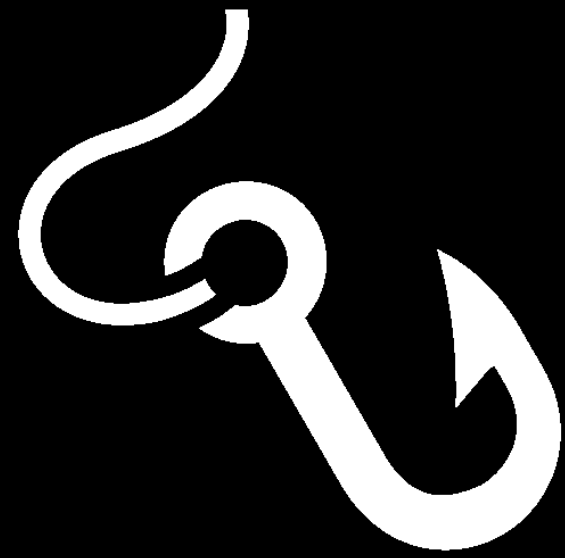




BUSINESS EMAIL COMPROMISE IN THE CLOUD

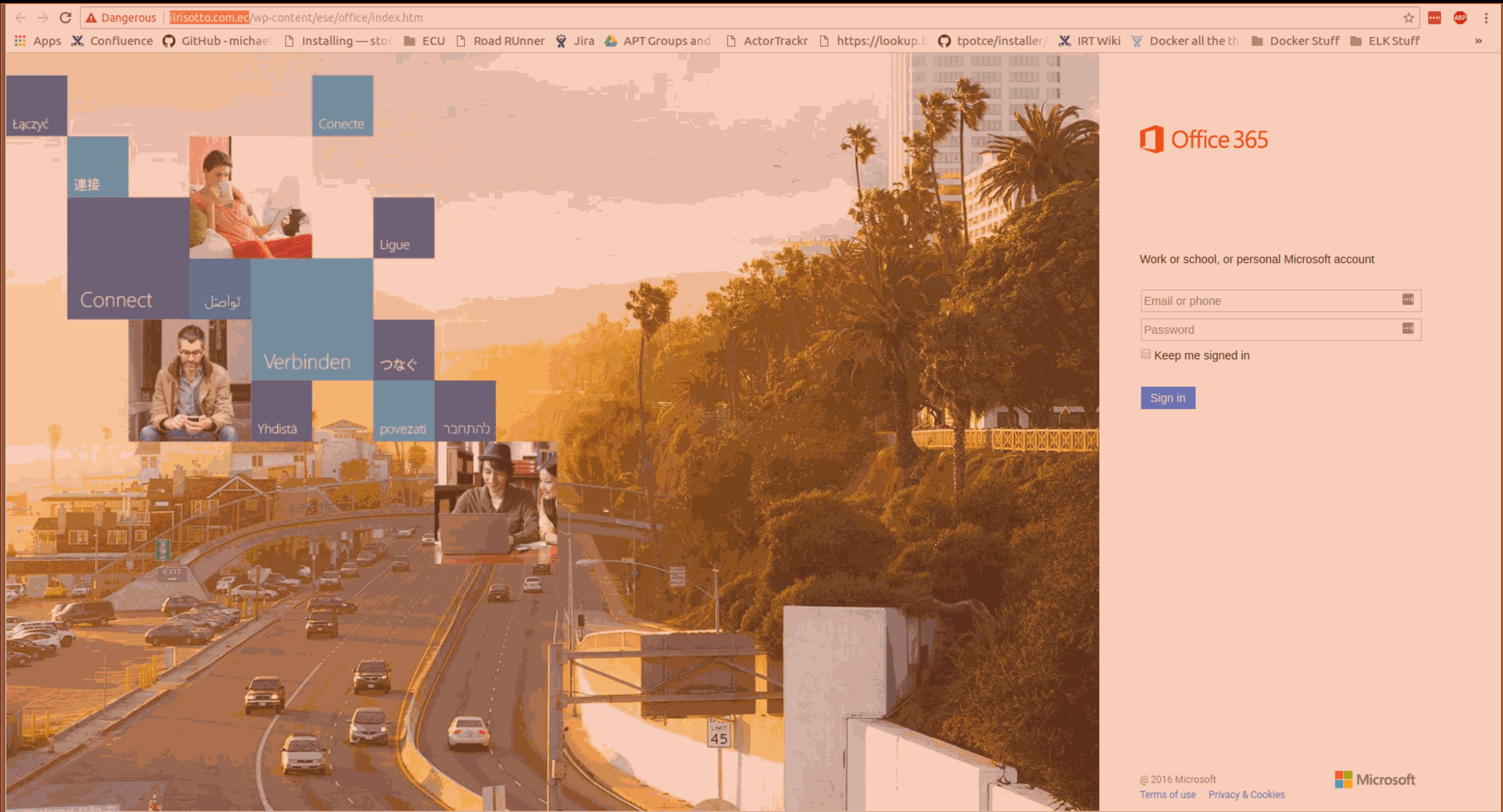
TLP: GREEN

COMMON BEC CASE



← → ↻ ⚠ Dangerous | irisotto.com.ec/wp-content/ese/office/index.htm ☆ 🔴 🔴 🔴

Apps Confluence GitHub - michael Installing — sto ECU Road RUNner Jira APT Groups and ActorTrackr https://lookup.b tpotce/installer/ IRT Wiki Docker all the th Docker Stuff ELK Stuff »



Łączyć Conecte

連接 Ligue

Connect تواصل

Verbinden つなぐ

Yhdistä povezati להתחבר

Office 365

Work or school, or personal Microsoft account


Email or phone

Password

Keep me signed in

Sign in

@ 2016 Microsoft
[Terms of use](#) [Privacy & Cookies](#)



TLP: GREEN

500 compromised users

Full AD password reset

9,500 spam sent per account

\$0 lost

UNIVERSITY CASE

THE STATS

TLP: GREEN

4 account compromised

Dwell time ~ 1 week

1 email

USD \$ 2.5 million lost

SMALL BUSINESS CASE


THE STATS

Filter by title

- > Get started
- > Protect access to data and services
- > Prevent data loss (DLP)
- > Manage data governance
- > Protect against threats
- > Search for content
- > Manage legal investigations
- > Search the audit log
- > Monitor security and compliance
- > Security solutions
- > Compliance solutions
- > Security incident management
- > Service assurance
- > Exchange Online Protection
- Office 365 Enterprise

↓ Download PDF

Security best practices for Office 365

📅 05/21/2018 • ⌚ 4 minutes to read • Contributors 

Minimize the potential of a data breach or a compromised account by following these recommended best practices.

This article contains a quick list of best practices. For more in-depth analysis and information on setting up security, see [Office 365 security roadmap: Top priorities for the first 30 days, 90 days, and beyond](#). In that article, you'll find information based on investigations of real-world attacks, where our top Microsoft Office 365 cybersecurity experts provide coaching on how to assess risk and implement the most critical security, compliance, and information protection controls to protect your Office 365 tenant. You'll learn how to prioritize threats, translate threats into technical strategy, and then take a systematic approach to implementing features and controls.

Use Office 365 Secure Score

Secure Score is a security analytics tool that recommends what you can do to further reduce risk. Secure Score looks at your Office 365 settings and activities and compares them to a baseline established by Microsoft. You'll get a score based on how aligned you are with best security practices. For more information about how to get Secure Score and use it to increase the security of your Office 365 organization, see [Introducing the Office 365 Secure Score](#).

Want to try out Secure Score?

In this article

Use Office 365 Secure Score

Use multi-factor authentication (MFA)

Use Office 365 Cloud App Security

Secure mail flow

Enable mailbox audit logging

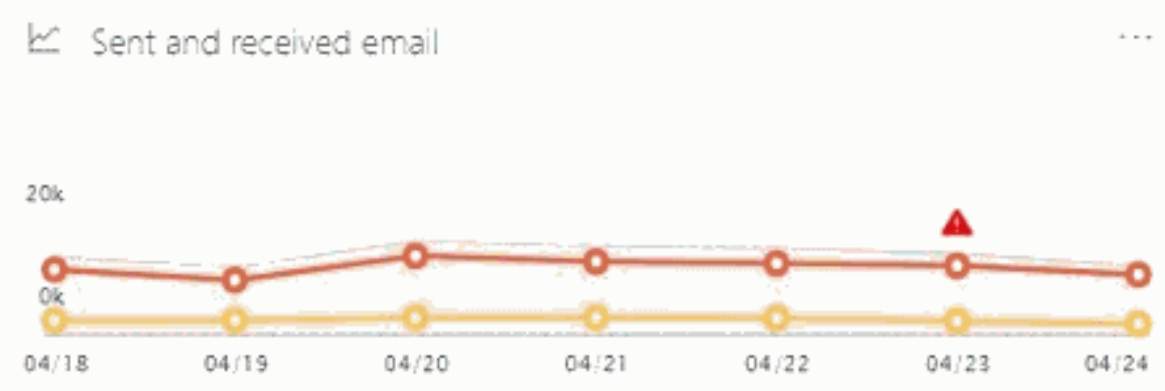
Configure Data Loss Prevention (DLP)

Use Customer Lockbox

Try it yourself

- Home
- Alerts
- Permissions
- Classifications
- Data loss prevention
- Data governance
- Threat management
- Mail flow
- Dashboard
- Message trace
- Data privacy
- Search & investigation
- Reports
- Service assurance

Mail flow [Customize](#)



Recommended for you

Fix possible mail loop

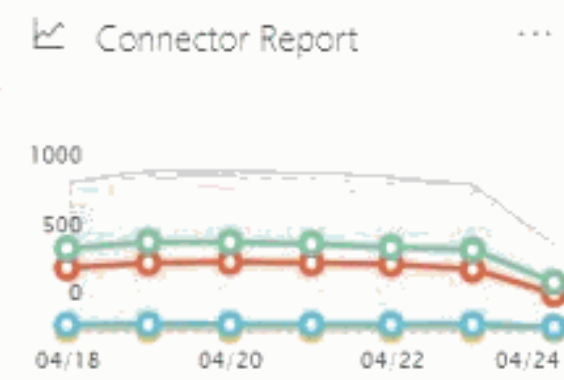
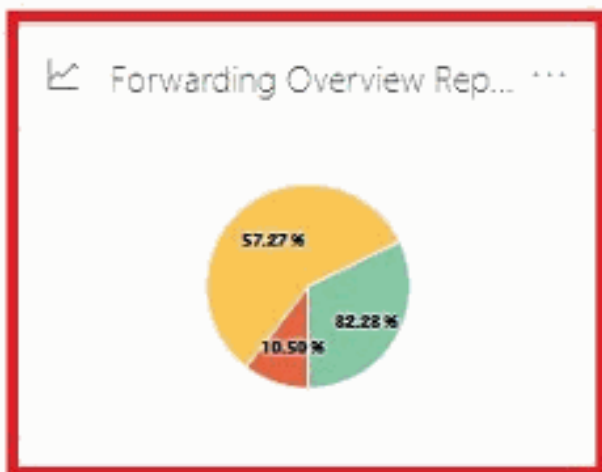
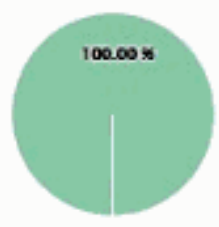
Yesterday, one or more recipients were in an email loop.

[+ View details](#)

Queues TLS overview report

Messages queued for more than an hour
(for messages leaving Office 365 via a connector)

2632
As of 4/24/18 12:17 PM

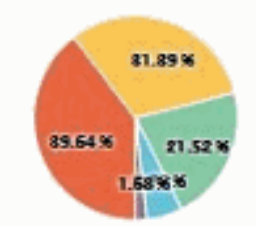


Recent alerts

Severity	Alert policy	Category	Time	Activities
High	Mails have been delay...	Mail flow	4/24/18 4:58 PM	2619
High	Mails have been delay...	Mail flow	4/24/18 3:59 PM	2637
High	Mails have been delay...	Mail flow	4/24/18 2:59 PM	2625
High	Mails have been delay...	Mail flow	4/24/18 1:57 PM	2626

[View all alerts](#)

Top Senders And Recipients





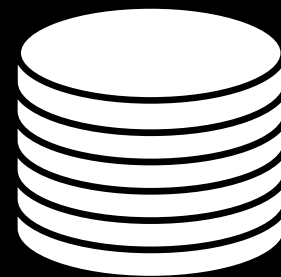
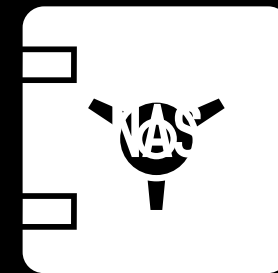
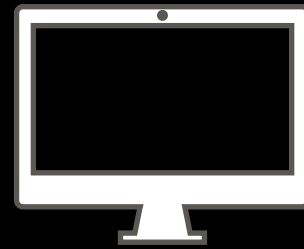
ADVANCED PERSISTENT RANSOMWARE

TRICKBOT ADAPTATIONS

Modular Design
Mimikatz Module



A TIME TO DWELL



ADVANCED RANSOMWARE



🔍 Search IPS Protections, Malware Families, Applications and more...

Ryuk Ransomware: A Targeted Campaign Break-Down

Over the past two weeks, Ryuk, a targeted and well-planned Ransomware, has attacked various organizations worldwide. So far the campaign has targeted several enterprises, while encrypting hundreds of PC, storage and data centers in each infected company.

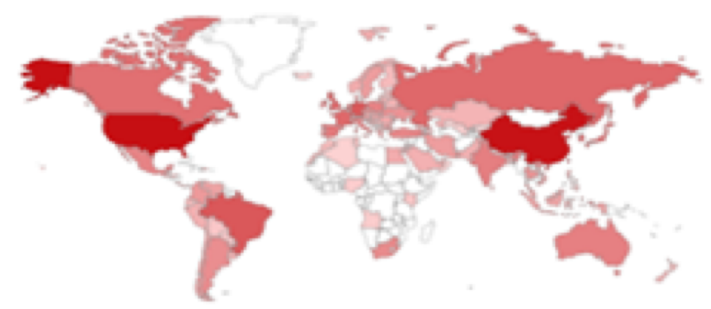
While the ransomware's technical capabilities are relatively low, at least three organizations in the US and worldwide were severely hit by the malware. Furthermore, some organizations paid an exceptionally large ransom in order to retrieve their files. Although the ransom amount itself varies among the victims (ranging between 15 BTC to 50 BTC) it has already netted the attackers over \$640,000.

Curiously, our research lead us to connect the nature of Ryuk's campaign and some of its inner-workings to the HERMES ransomware, a malware commonly attributed to the notorious North Korean APT Lazarus Group, which was also used in massive targeted attacks. This leads us to believe that the current wave of targeted attacks using Ryuk may

TOTAL RESULTS

2,362,154

TOP COUNTRIES



United States	544,926
China	518,202
Germany	108,455
Brazil	106,061
Korea, Republic of	68,119

TOP SERVICES

RDP	2,332,651
RDP (3388)	28,808
SMB	385
Citrix	208
HTTPS	23

TOP ORGANIZATIONS

Tencent cloud computing	162,470
Amazon.com	146,997
Korea Telecom	42,079
Vivo	33,292
China Telecom jiangsu	24,062

TOP OPERATING SYSTEMS

Windows XP	8,522
Windows 7 or 8	6,373
Windows 6.1	190
Unix TLP: GREEN	105
Linux 3.x	8

60.184.184.213

China Telecom Lishui
 Added on 2018-07-26 12:49:05 GMT
 China, Lishui
[Details](#)

self-signed

SSL Certificate

Issued By:
 Common Name: USER-5BI28MEV8H
 Issued To:
 Common Name: USER-5BI28MEV8H

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Supported SSL Versions

TLSv1

185.160.21.161

host161.kaora.cz
 Allstar Net s.r.o.
 Added on 2018-07-26 12:48:47 GMT
 Czech Republic, Stranice
[Details](#)

self-signed

SSL Certificate

Issued By:
 Common Name: WIN-J0BEB3M4FFP
 Issued To:
 Common Name: WIN-J0BEB3M4FFP

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group
 2

119.202.16.174

Korea Telecom
 Added on 2018-07-26 12:48:42 GMT
 Korea, Republic of, Gyeongju
[Details](#)

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

118.44.240.135

Korea Telecom
 Added on 2018-07-26 12:48:41 GMT
 Korea, Republic of, Cheongju
[Details](#)

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

115.47.141.52

Beijing Teletron Telecom Engineering Co.
 Added on 2018-07-26 12:48:41 GMT
 China, Beijing
[Details](#)

SSL Certificate

Issued By:
 Common Name:
 Issued To:

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

HARDEN

- Segment your network
- Use Microsoft LAPS to have different local admin crews
- Use protected users AD group for privileged
- Run BloodHound AD against your AD - then freak out
- Hold & Prevent all mails and files
- HTTPS Inspection

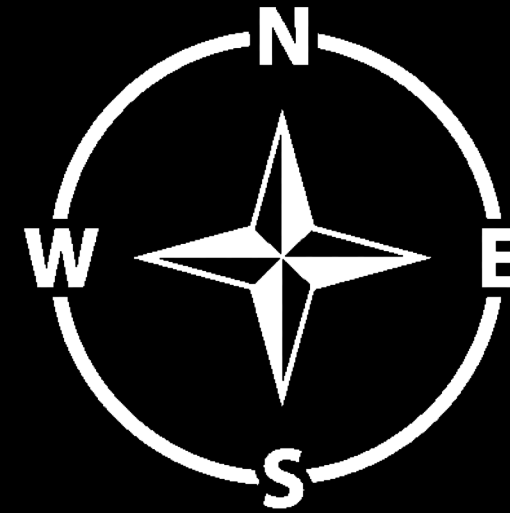
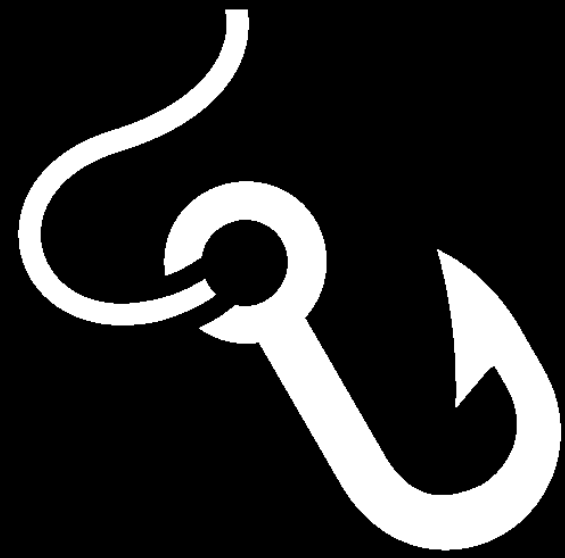


MITIGATION



TO THE CLOUD

AD DDOS



ATTACKING SALES

E-COMMERCE



Westpac Online Banking - verify your personal details

Step 1
Personal Identification

Step 2
Security information

Step 3
Successful



Need help?

Call us on 1300 655 505

8am-8pm, 7 days a week

verify your personal details

For your security, please provide the requested details below to seure your account.

verify your online banking details

Telephone Banking Pin

Telephone Banking Password

Email Addresss

Email Password

Date of birth

Westpac Protect™

Submit

COMPLEXITIES WE FACE

THE CHALLENGES

TLP: GREEN

INCIDENT RESPONSE TEAM



CHECK POINT

+1-866-923-0907

EMERGENCY-RESPONSE@CHECKPOINT.COM

TLP: GREEN