14.12.2018, 16:53, "Matthew Adams" <adamsmatthew@mail-xen.com>

Dear Ariana,
Thank you for your responding. I apologize for the late reply. Too many things to do at the same time. I think you understand me like no other. I am very glad that your restaurant will serve my son's holiday.
In the file above, I prepared a complete list, time and date. Please feel free to ask me any questions. As soon as I need to pay for all the services, let me know your bank details here. I look forward to hearing from you.
King Regards,
Matthew

14.12.2018, 16:16, "237 Travel Center" <travelcenter.237@pilottravelcenters.com>

Good Morning Matthew,

We are ready to take your order when you have it ready. Please include the date and time.

Thank You,
Ariana

---

From: Matthew Adams [mailto:adamsmatthew@mail-xen.com]
Sent: Thursday, December 13, 2018 3:22 AM
To: 237 Travel Center
<TravelCenter.237@pilottravelcenters.com>
Subject: Re: Cinnabon
Dear Araina,
Thank you for responding. I will try to make every effort not to spoil the birthday of my son. You are very sweet and attentive. I wish you a great vacation. Can I write Maria to your email or will you give me her personal one?
Regards,
Matthew

---

19.12.2018, 18:58, "237 Travel Center" <travelcenter.237@pilottravelcenters.com>:

Can you try faxing to us? Our fax number is 831-775-0360. As long as we are given a day notice we should be fine. I am going on vacation tomorrow, Maria is my Co manager and she is aware of the situation. She will respond on emails for me.

Thanks,
Ariana

---

From: Matthew Adams <adamsmatthew@mail-xen.com>
Sent: Wednesday, December 19, 2018 8:51 AM
To: 237 Travel Center <TravelCenter.237@pilottravelcenters.com>
Subject: Re: Cinnabon

Dear Ariana,
Thank you for your efforts. I do not understand why my list does not reach you. I will try to find the old one for you. I will be back in town on Thursday.

Matthew Adams
Threat Landscape:
Nearly 100% of Attacks are Human Activated
Threat Landscape:
The Attacker’s View: Global Advertising

OVER 99% OF TARGETED ATTACKS EXPLOIT HUMAN VULNERABILITY, NOT TECHNICAL VULNERABILITY
Malware Needs End Users to Click

Hello,

Even for those of us who’ve followed the Snowden revelations closely, Permanent Record is full of surprises.

Scan book below.

---

TOTAL
$375.00

DUE DATE
13/09/2019

Thank you for your business. Full details, including payment terms, are included. If you have any questions, please don’t hesitate to contact us. Kind regards,

TALK TALK TELECOM GROUP PLC

POWERED BY

© 2019 Proofpoint. All rights reserved
Email Credentials: Key to Your Cloud Identity
Threat Landscape:
What About the Lowest Tech Threat of All... BEC

1. Impersonate corporate identities
2. Highly-targeted, low volume attacks
3. Aim to solicit:
   - Fraudulent wire transfers
   - Steal company data
   - Steal credentials and other confidential information

Employee Name <employee@company.com>
CEO Name <CEO@company.com>
CEO Name <mu.constructionptltd@gmail.com>

I need you to instruct our Chief Financial Officer to initiate a wire transfer of £150,000 to the account details that follows, file for auditing.

It is consequential it is done today. It’s for an urgent acquisition. I have a deadline to deal with, which may be passed.

BANK NAME: Barclays Bank Plc
ACCOUNT NAME: E grand logistics.
ACCOUNT NUMBER: 13396770
SORT CODE: 20 29 81
IBAN: GB94BARC20298113396770
BIC: BARCGB22
Threat Landscape:
Defenders Don’t Focus on People, Attackers Do…

- Threats use social engineering, not vulnerabilities
- Shift to cloud creates new threat vectors, data exposure
- BEC/impostor email fraud becomes board-level issue

99%+ rely on users to run malicious code.
45% of companies breached via cloud apps.
$26.2B losses from BEC/EAC since 2016.
$12.5B 2013 - 2016.
...And Email is Still the Preferred Channel

Source: Verizon DBIR

Source: Gartner Information Security Market* WW End-User spending 2018
Threat Landscape:
More Attacks are Conducted by Humans
Protect Your Human Attack Surface…

Who Gets Targeted by Serious Threats?
Receive highly targeted, very sophisticated, or high volumes of attacks

Who Is Likely To Fall For Those Threats?
Clicks on malicious content, fails awareness training, or uses risky devices or cloud services

Who Represents Risk to the Organisation?
Can access critical systems or sensitive data, or can be a vector for lateral movement

proofpoint
...With Adaptive Controls

- Protect Information with DLP
- Block Threats & Protect Access Zero Trust + Isolation
- Orchestrate + Automate Response
- Customise Training
- Prevent Impersonation Attacks
- Integrate with Ecosystem Controls

Network
SIEM
PAM
Identity
Endpoint

© 2019 Proofpoint. All rights reserved
PEOPLE-CENTRIC ATTACK VECTORS: INITIAL COMPROMISE

Deliver protection and automated response across the key people-centric threat vectors

Make users more resilient against threats

Minimise the damage from compromises that do occur

Stop people-centric attacks across the broader ecosystem

PROOFPOINT
© 2019 Proofpoint. All rights reserved
Threat Landscape: The Attacker’s View: Global Advertising

- PR MANAGER (APAC)
- MD, GOVERNMENT COMMUNICATIONS (APAC)
- PR DIRECTOR (APAC)
- GENERIC INFO@ EMAIL (ME)
- MD (U.S.)
- DEPUTY-CHAIR (EMEA)
- CEO
- COMMUNICATIONS OFFICER

- Stealer
- Keylogger
- Unknown Malware
- Consumer Credential Phishing
- Unknown Credential Phishing
- RAT
- Corporate Credential Phishing
- Banking
- Ransomware
- Downloader
- MalSpam
- Unknown
LEARN MORE

@proofpoint

Proofpoint Human Factor Report 2019
https://www.proofpoint.com/uk/resources/threat-reports/human-factor