Phishing Defense
The Art of Human Intuitive Repulsion

Jason Meurer
Researcher, Cofense
Fishing? Phishing? 1995
…24 Years ago: AOHell 95 v3.0 BEta 5
WHY ARE MAIL GATEWAYS FAILING TO PROTECT US?
These babies can stop so much phishing
.... trust me!
TESTING AND THIRD PARTY VERIFICATION

22 Firewalls tested and accredited
✓ Latest being 17-4-2019

2 Email gateways
✓ Latest being 31-12-2016
ALL NETS HAVE HOLES

90% OF VERIFIED PHISHING EMAILS WERE FOUND IN ENVIRONMENTS USING SECURE EMAIL GATEWAYS (SEGS)

This key finding in the Cofense™ Phishing Threat & Malware Review 2019 is based on research by the Cofense Phishing Defense Center™. From October 2018 to March 2019, our team verified over 31,000 malicious emails reported by customers’ users. This data is augmented below by findings from the Cofense Research and Cofense Intelligence™ teams.
Security Technology Bypass – Credential Phish

CREDENTIAL PHISH

The onslaught of credential phishing shows no signs of letting up. Threat actors are seeking network credentials, the keys to the enterprise kingdom.

- Nearly 75% of verified phish were credential phish.
- 91.2% of credential phishing attacks were found in environments with one or more SEGs.
- Almost 300,000 distinct credential phishing URLs have been identified in the wild since Q1 2018.

Source: Cofense Research
Security Technology Bypass – Malware

MALWARE DELIVERY

The game of Whack-A-Mole continues. As soon as anti-malware defenses evolve, threat actors turn on the creativity. New tactics and techniques ensure that malware payloads still reach their targets.

Over 4,800 Verified phishing emails that delivered malware

89.6% Of phishing attacks delivering malware were found in environments with one or more SEGs
Traditionally a wire transfer scam aimed at CFOs and CEOs, Business Email Compromise has shifted to targeting payroll administrators to reroute direct deposits. BEC occurs less frequently than other attacks, but inflicts billions of dollars in losses.

**Statistics:**
- **2,681** Verified BEC attacks
- **$12.5B** In global business losses due to BEC attacks
- **88.1%** Of BEC attacks were found in environments with one or more SEGs

*Source: FBI, May 2018*
Man Vs. Machine
Innovation from the attacker occurs when they become sufficiently frustrated.

**Higbee’s Law of Phishing Innovation**
Real Phish: Credential

Membership Problem - Order #1178-11382-099211 cancelled and scheduled for return

Amazon Prime <bonnie@bonnielowkramen.ccsend.com> on behalf of Amazon Prime <bonnielowkramen@gmail.com>  
Friday, September 13, 2019 at 5:58 PM

We cancelled your order(s) and your package is scheduled for return due to "membership" problem, please take a moment to review your membership status now.

MEMBERSHIP STATUS

It will only take few minutes to fix this

Sincerely,
The Customer Service (Ex. AMAZON)

Unsubscribe redacted@retail
Update Profile | About Constant Contact
Sent by bonnielowkramen@gmail.com in collaboration with

Constant Contact
Try email marketing for free today!
REAL PHISH: ATTACHED MALWARE

Exe in an ISO file with an IMG extension

BYPASSED GATEWAY ✅
Dear UPS customer - redirect you

order@iwriteessays.com  
redacted@healthcare
Tuesday, September 17, 2019 at 12:16 PM

You have a package coming to you.
This letter was delivered to notify you that your shipment is transferred to our allocation storage.
To validate the actual status of a parcel, please open the document attached to the receipt.

We're right here for you! Thank you for choosing our company. We look forward to providing you the best possible service and quick at the best price. Questions?
REAL PHISH: Sextortion

Dear [Victim],

Your account is now infected. It will be good idea to change the password right now.

You may be thinking about the alert that you received. We are not sure what you are getting this alert about, but you may be the victim of a malware infection.

Here's how we can help you:

1. Close all browser windows.
2. Remove any malware found on your device.
3. Update your security software.
4. Change your password.

We have received reports that your account may have been compromised, and we are here to help you.

Thank you for your time.

Best regards,

[Redacted]
SEXTORTION PHISHING PAYS

<table>
<thead>
<tr>
<th>BTC Address</th>
<th>1GoWv5yjz3XXB1YxLU9tXCBMgibpzn4sQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wallet Name</td>
<td>03e0071e5615e8db</td>
</tr>
<tr>
<td>Current Balance</td>
<td>0.00000000</td>
</tr>
<tr>
<td># Transactions</td>
<td>33</td>
</tr>
<tr>
<td>First Transaction</td>
<td>26 Feb 19</td>
</tr>
<tr>
<td>Last Known Input</td>
<td>1CG9EC7U6...</td>
</tr>
<tr>
<td>Repeated Inputs From (50 most recent transactions)</td>
<td>None</td>
</tr>
</tbody>
</table>

**Total Received:** 1.31587581  
**Total Sent:** 0.00000000  
**Final Balance:** 1.31587581  
**Total transactions:** 10

**Recent transactions:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-04-10 21:06:17</td>
<td>0.13297806</td>
<td>1.31587581</td>
</tr>
<tr>
<td>2019-04-10 13:14:01</td>
<td>0.12966500</td>
<td>1.18289775</td>
</tr>
<tr>
<td>2019-04-09 21:23:03</td>
<td>0.01012720</td>
<td>1.05323275</td>
</tr>
<tr>
<td>2019-04-09 19:50:08</td>
<td>0.13863366</td>
<td>1.04310555</td>
</tr>
<tr>
<td>2019-04-09 18:41:11</td>
<td>0.14846624</td>
<td>0.90447189</td>
</tr>
<tr>
<td>2019-04-09 17:46:19</td>
<td>0.16162063</td>
<td>0.75600565</td>
</tr>
<tr>
<td>2019-04-09 06:30:15</td>
<td>0.16433371</td>
<td>0.59438502</td>
</tr>
<tr>
<td>2019-04-08 17:42:31</td>
<td>0.14055864</td>
<td>0.43005131</td>
</tr>
<tr>
<td>2019-04-08 06:33:23</td>
<td>0.15209267</td>
<td>0.28949267</td>
</tr>
<tr>
<td>2019-04-07 13:26:01</td>
<td>0.13740000</td>
<td>0.13740000</td>
</tr>
</tbody>
</table>
RE: RE: Preschool for our daughter.

REDACTED CONTACT LIST INDIVIDUAL <REDACTED@transrod.cl>
REDACTED.GOV
Friday, October 4, 2019 at 5:57 PM

File: 100520194085-1
0 KB

Download All  Preview All

Good afternoon All,

I also attached your file in DOC format as looks much more professional.

Kindly assist, please.

Kindest Regards

LastName, FirstName <redacted@redacted>

Sent from my Samsung Galaxy smartphone.

Message protected by MailGuard: e-mail anti-virus, anti-spy and content filtering.

Hi FirstName,

I just created an account and provided my credit card information.

We can take a morning spot pretty much anywhere in the REDACTED district if it is available. If nothing is available anywhere, can you please waitlist us where you think there will be a better chance to get a spot.

Thanks,
FirstName LastName

555 555-5555 (cell)

From: LastName, FirstName [mailto:redacted@redacted.org]
Sent: Thursday, August 02, 2018 1:24 PM
To: LastName, FirstName <REDACTED@REDACTED.gov>
Subject: RE: Preschool for our daughter.

I do not have a spot open there right now. And most sites only have afternoon. You could check back with us to see if anything opens up. If you want to create an account I put you on a waitlist.
What you actually want your user base clicking....
Man AND Machine
1 in 7

USER-REPORTED EMAILS WITH MALICIOUS CONTENT
WHAT IS YOUR RESILIENCY?

All Industries - Resiliency Analysis of Last 12 Months

Technologies ratio is **1.12**
Better than your peers?

18.36 Tech employees would click on a GRU phish... and **20.63** would REPORT it

Energy sector ratio is **5.29**

7.68 Energy employees would click on a GRU phish... and **40.55** would REPORT it

APT28/29 sent 120 emails to Florida workers in one campaign
Email Gateway

Is this guacamole?

Phishing Email
KEY TAKEAWAYS

• Attackers are constantly evolving their tactics in response to technology
• Gateways are definitely needed, but can’t be relied on as your only defense
• People can be trained to identify bad
• Creating an environment that encourages reporting can save you
Visit Our Website to Learn More!

- https://cofense.com/
- https://cofenselabs.com/