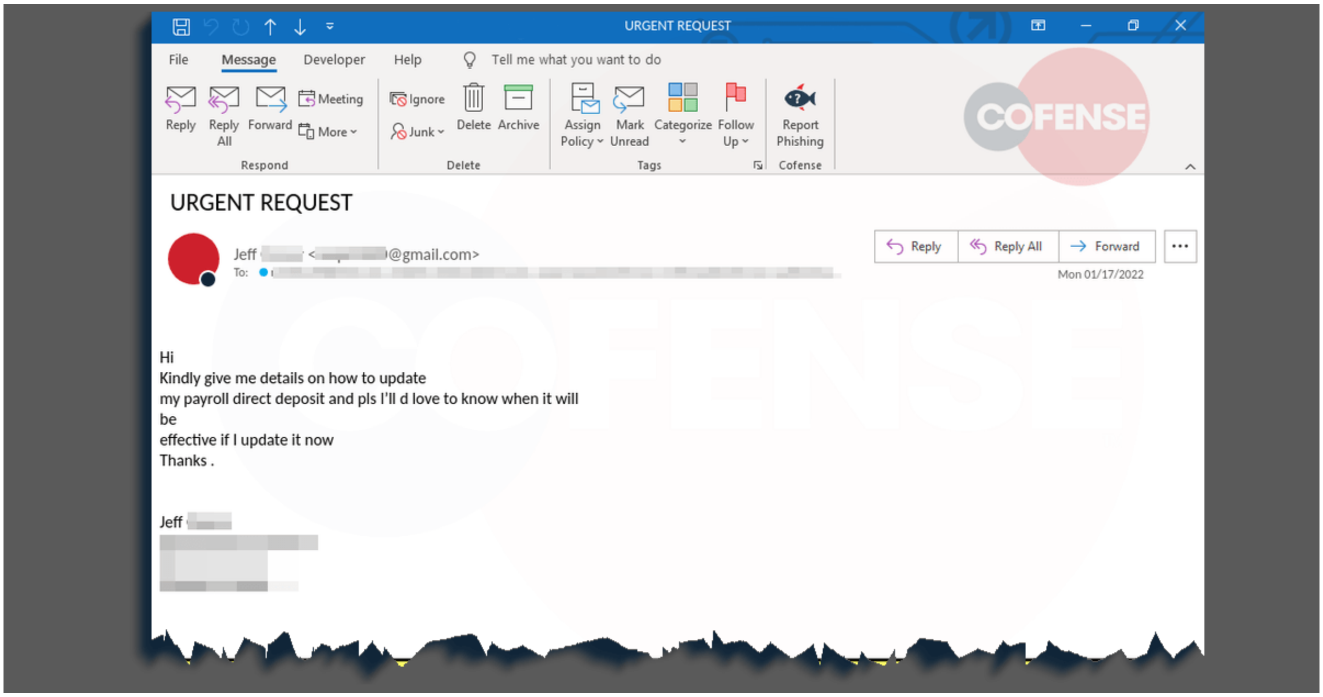
Phishers Spoof Power BI to Visualize Your Credential Data

cofense.com/blog/phishers-spoof-power-bi-to-visualize-your-credential-data

Cofense

February 17, 2022



URGENT REQUEST

Jeff [redacted] <[redacted]@gmail.com>
To: [redacted]

Mon 01/17/2022

Hi
Kindly give me details on how to update
my payroll direct deposit and pls I'll d love to know when it will
be
effective if I update it now
Thanks .

Jeff [redacted]
[redacted]

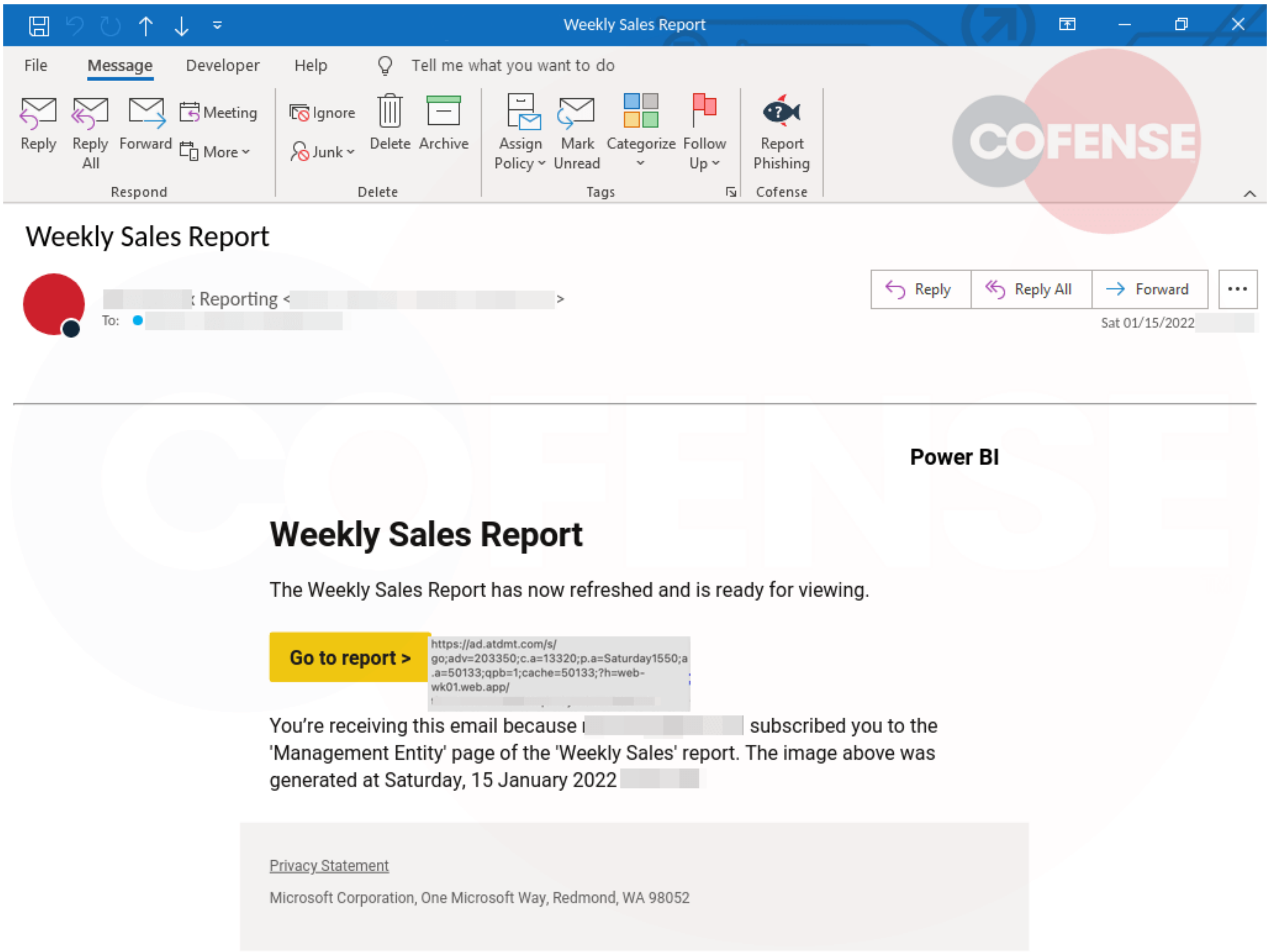
Email Gateways Bypassed

Cisco IronPort | Mimecast | Symantec

By Jake Longden, Cofense Phishing Defense Center

Microsoft Power BI, a popular data-visualization tool, is designed to help users wrangle their data in multiple and more human-friendly formats. As a recognizable application from a commonly used and trusted vendor, Power BI is also a prime target for threat actors to spoof and abuse it for phishing attacks.

The Cofense Phishing Defense Center (PDC) has observed a new phishing campaign that harvests Microsoft credentials by impersonating Power BI emails.



Weekly Sales Report

[redacted] Reporting <[redacted]>

To: [redacted]

Sat 01/15/2022 [redacted]

Power BI

Weekly Sales Report

The Weekly Sales Report has now refreshed and is ready for viewing.

Go to report >

https://ad.atdmt.com/s/go;adv=203350;c.a=13320;p.a=Saturday1550;a.a=50133;qpb=1;cache=50133;?h=web-wk01.web.app/ [redacted]

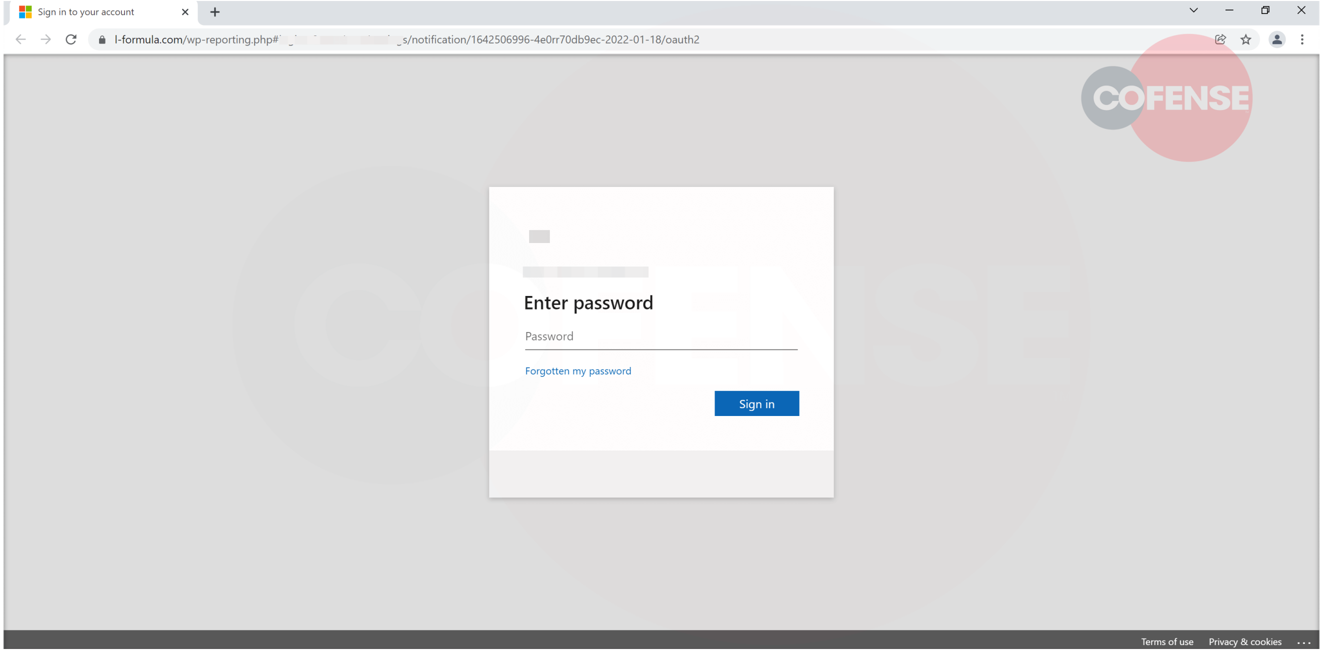
You're receiving this email because [redacted] subscribed you to the 'Management Entity' page of the 'Weekly Sales' report. The image above was generated at Saturday, 15 January 2022 [redacted]

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Figure 1: Email Body

As seen in Figure 1, the email resembles a legitimate Microsoft notification. There are a couple of reasons how this happens. Threat actors have become comfortable adapting legitimate MS notifications in their phishing templates. We also observe them leveraging stolen credentials to create a legitimate looking notification from a legitimate MS instance. We see that the threat actor in this email used a common theme to try to get the recipient to interact with the links – Weekly Sales Report.



Sign in to your account

l-formula.com/wp-reporting.php#[redacted]s/notification/1642506996-4e0rr70db9ec-2022-01-18/oauth2

[redacted]

Enter password

Password

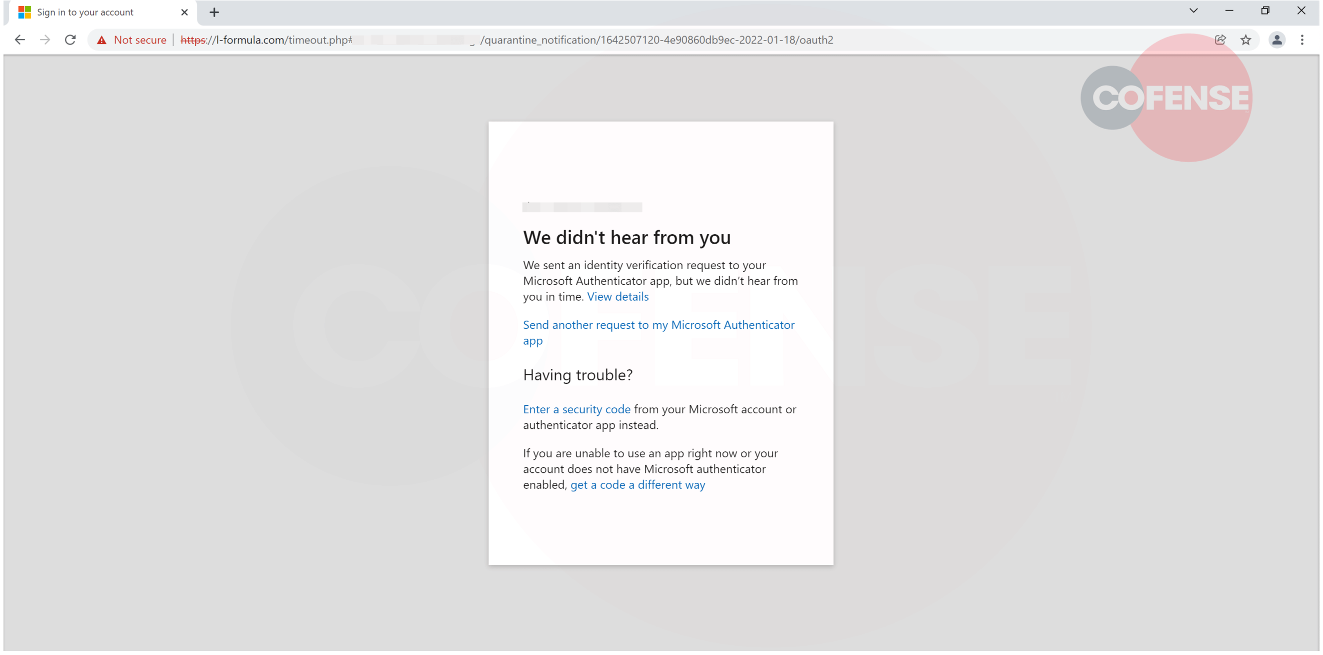
Forgotten my password

Sign in

Terms of use Privacy & cookies ...

Figure 2: Phishing Page

Once the user has clicked the link in the email, they are presented with a page seen in Figure 2, designed to look like a legitimate Microsoft log-in page. The first indicator that something's not right with the page, beyond the missing standard imagery, is that the URL doesn't look anything close to what's indicated in the email or associated with Microsoft services.



Sign in to your account

Not secure | ~~https~~://l-formula.com/timeout.php#[redacted]/quarantine_notification/1642507120-4e90860db9ec-2022-01-18/oauth2

[redacted]

We didn't hear from you

We sent an identity verification request to your Microsoft Authenticator app, but we didn't hear from you in time. View details

Send another request to my Microsoft Authenticator app

Having trouble?

Enter a security code from your Microsoft account or authenticator app instead.

If you are unable to use an app right now or your account does not have Microsoft authenticator enabled, get a code a different way

Figure 3: Phishing Final Page

Subsequent to the recipient providing their credentials, the final step of the attack is an error message indicating that there was an issue with the account verification. This is another Microsoft spoof the threat actor employed to distract the recipient from the fact that they have not been redirected to the Power BI report they expected to see. This discourages the recipient from suspecting that they have just given away their credentials.

Cofense continues to observe credential phishing as a major threat to organizations. This is why it’s critical to condition users to identify and report suspicious messages to the security operations team. This recipient was well-conditioned to identify something wasn’t adding up with this email and landing page, and used Cofense Reporter to send this off to the Cofense Phishing Defense Center. Cofense can help you, too. Attacks such as this one are effective at eluding common email security controls, and are – by design — overlooked by end users. Cofense can help. Ask us how we can help your teams spot phishing email that turns up in environments protected by “secure” email gateways.

Network IOC	IP
hXXps://ad[.]atdmt[.]com/s/go;adv=203350;c.a=13320;p.a=Saturday1550;a.a=50133;qpb=1;cache=50133;?h=web-wk01[.]web[.]app	
hXXps://web-wk01[.]web[.]app	
hXXps://l-formula[.]com/wp-reporting.php	202.254.234.76

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats. Past performance is not indicative of future results.

Don't miss out on any of our phishing updates! Subscribe to our blog.