



**NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**

Cyber Alert

TLP:WHITE

Product No. 2020-08-010

HSEC-1 | NTIC SIN No. 2.5

August 7, 2020

NTIC CYBER CENTER ALERT

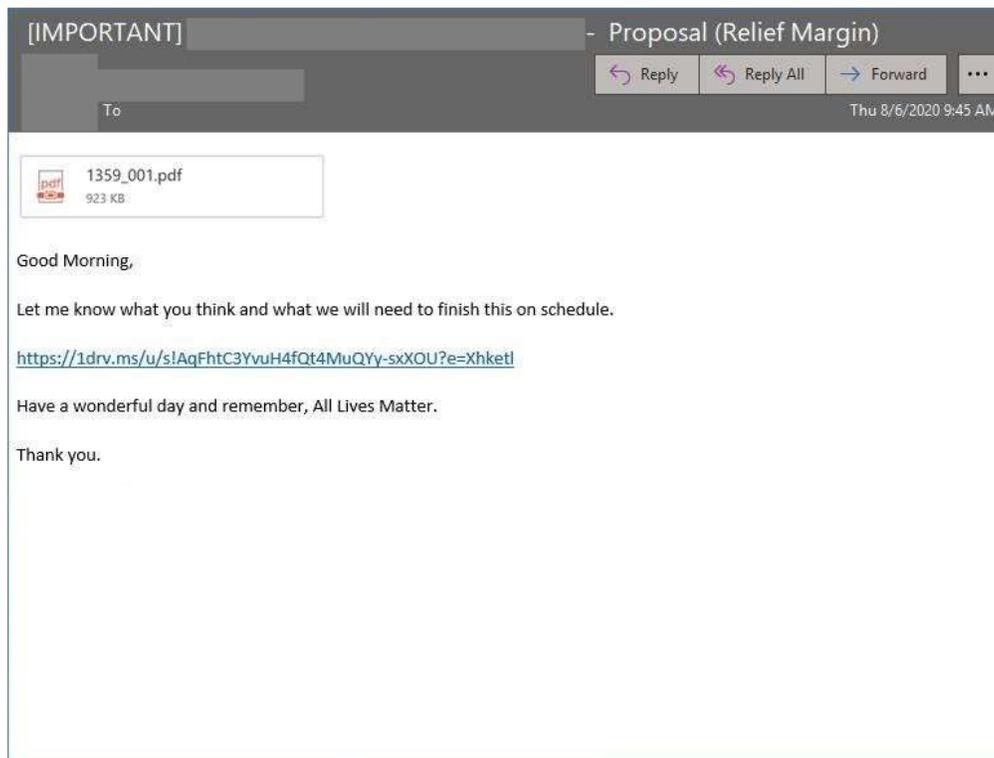
**Two Active Phishing Campaigns Using Compromised
Enterprise Accounts to Steal Microsoft Office 365 Login
Credentials**

NTIC Cyber Center members,

This alert is being provided for informational purposes and for potential use to protect systems, networks, and data against this cyber threat at the sole discretion of recipients. As the cyber threat landscape is ever-evolving and attribution can be difficult, the NTIC Cyber Center makes no guarantees of the accuracy of this information during and after the dissemination of this alert as indicators of compromise (IoCs) and adversary tactics, techniques, and procedures (TTPs) may change. Recipients are urged to use caution before implementing any changes to systems, software, and procedures.

SUMMARY

The NTIC Cyber Center is aware of two currently active phishing campaigns that attempt to steal Microsoft Office 365 login credentials from unsuspecting victims. These campaigns use previously compromised enterprise email accounts to send fraudulent emails to addresses in the accounts' contact lists. Both campaigns include the words "proposal" and "relief margin" in either the subject or body of the emails. In one campaign that we observed, the phishing emails contained a malicious link in both the body of the email and in a PDF attachment that, if opened, redirects to a fraudulent website prompting victims to enter their Microsoft Office 365 login credentials.

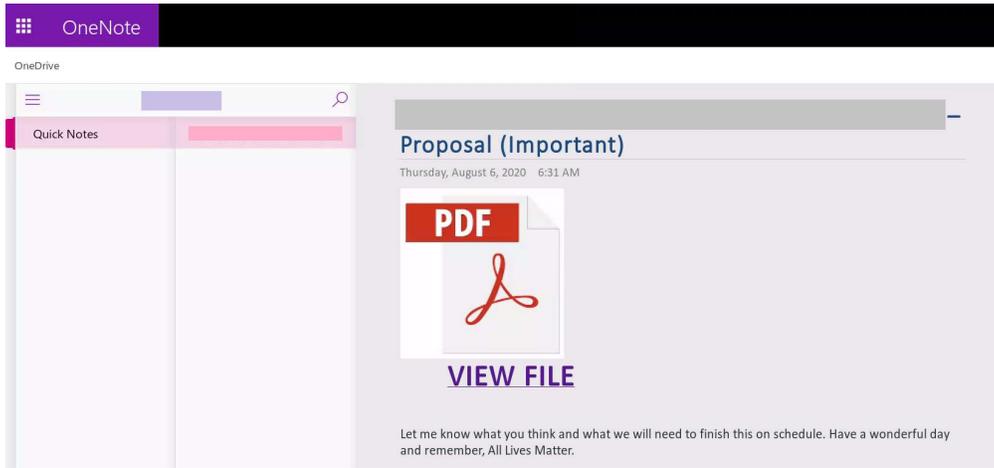


(Example of Email from First Phishing Campaign)

In the second campaign, the subject line of the email contained the words "new message received" and the body of the email contained a link that, if clicked, accessed and opened a page on the Microsoft OneNote web application associated with the compromised sender account. This OneNote page displayed an icon for a PDF file with a link that, if clicked, redirects victims to a phishing page hosted via Google Docs that prompts victims to enter their email address and password. It also requests that victims verify ownership of a web-based email account.



(Example of Email from Second Phishing Campaign)



(Screenshot of Compromised OneNote Page in Second Phishing Campaign)



Microsoft Office365 Secured Online Document© 2020

Sign in with your valid email account to view document.

* Required

Email address *

Your email

***** *

Enter password

Your answer

Sign in with (Office365, Hotmail, Outlook, Yahoo, AOL, Webmail, Others) Simply login with your valid email and password to download file. *



Verify Ownership.

Submit

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

(Screenshot of Google Docs Landing Page in Second Phishing Campaign)

The NTIC Cyber Center assesses with high confidence that these two email campaigns originated from the same cyber threat actor or group as both campaigns were sent to end users at the same organization at approximately the same time and both include legitimate Microsoft OneDrive shortened URLs to bypass email security gateways. Additionally, both campaigns include the following verbiage: *Let me know what you think and what we all will need to finish this on schedule. Have a wonderful day and remember, All Lives Matter.*

RECOMMENDATIONS

The NTIC Cyber Center has reported the phishing page to Google for removal and notified affected parties; however, we recommend all organizations continuously educate their end users about this and other phishing threats. We also recommend remaining vigilant for phishing campaigns that originate from inside an organization. Always verify the legitimacy of an unexpected email from a known sender that contains links or attachments by contacting the sender directly through another means, such as a phone call or text message. As always, avoid opening unexpected emails and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Enable multifactor authentication on every online account that offers it to reduce your risk of account compromise due to credential theft. If you believe you have been targeted by this or any other malicious email campaign, please notify your organization's IT department immediately.

The information contained in this alert is designated TLP:WHITE, subject to standard copyright rules, and may be distributed without restriction.

We welcome your feedback.

Please click [here](#) to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: This NTIC Cyber Center Cyber Alert is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

