



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Cyber Alert

TLP:GREEN

Product No. 2020-04-035

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 28, 2020

NTIC CYBER CENTER ALERT

Phishing Campaign Masquerades as HR-Initiated Video Conference Invitations to Target Zoom Users

NTIC Cyber Center members,

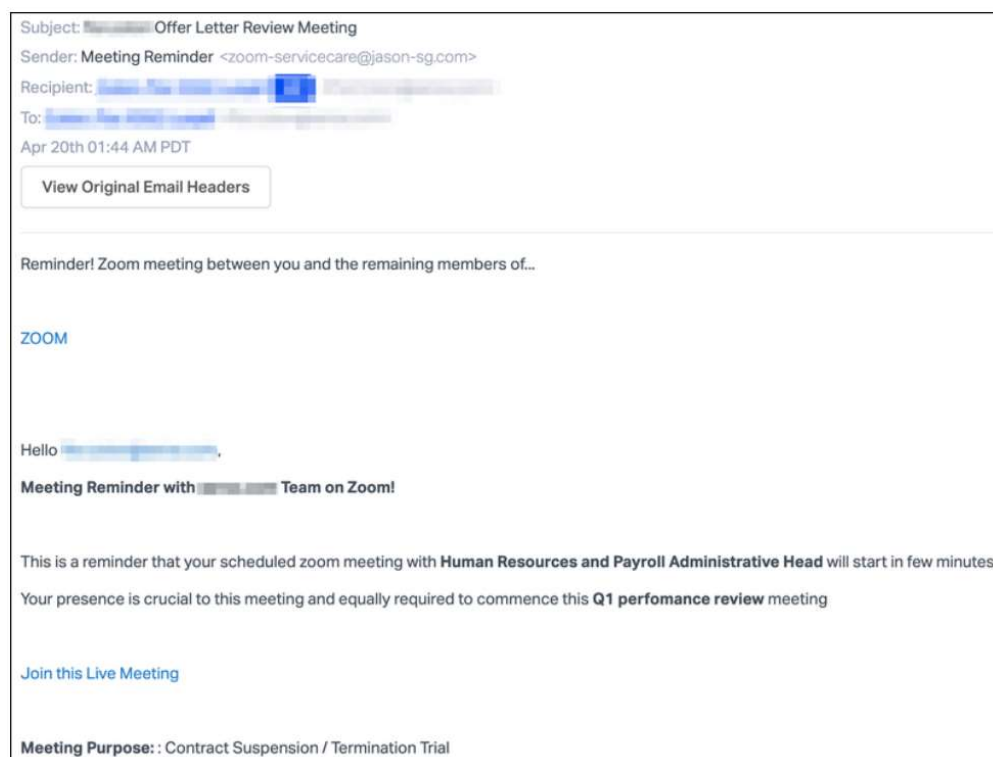
This alert is being provided for informational purposes and for potential use to protect systems, networks, and data against this cyber threat at the sole discretion of recipients. As the cyber threat landscape is ever-evolving and attribution can be difficult, the NTIC Cyber Center makes no guarantees 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

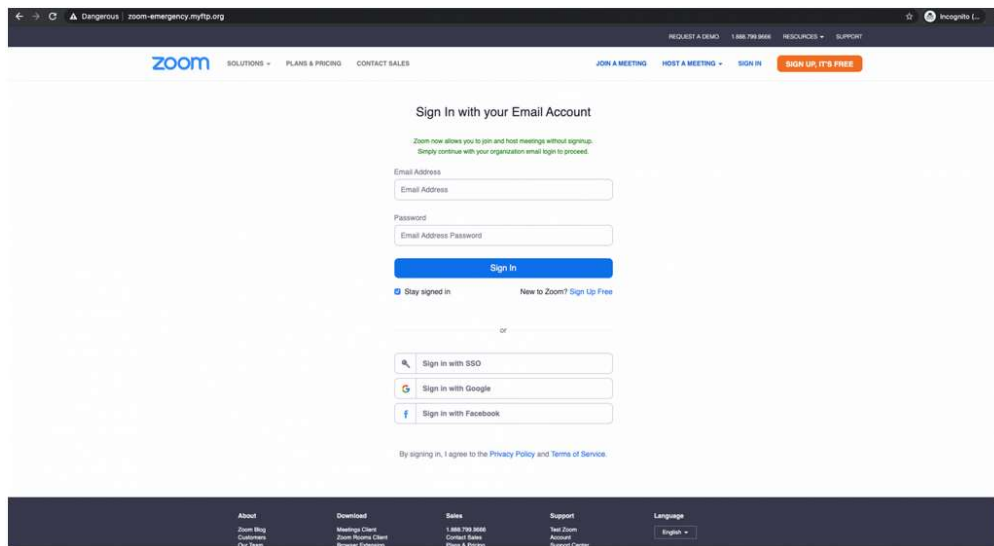
On Friday, April 24, cybersecurity website BleepingComputer [reported](#) that a newly discovered phishing campaign was targeting users of video conferencing software Zoom. The emails in this phishing campaign masquerade as urgent Zoom conferencing requests from the recipient's human resources department and suggest that the virtual meeting is needed to discuss the recipient's potential layoff or employment termination. The fraudulent emails contain an embedded link that, if clicked, redirects recipients to a phishing page that prompts them to sign in using their email account credentials. This campaign can be particularly effective because the cyber threat actors attempt to exploit recipients' fears of job and income loss, a common concern during the COVID-19 pandemic.

Cybersecurity firm Abnormal Security [analyzed](#) this campaign and determined that at least 50,000 Office 365 end users have been targeted in this attack. Additionally, they determined that the embedded link within these phishing emails resolved to the domain zoom-emergency[.]myftp[.]org. However, the NTIC Cyber Center has determined that this domain currently does not resolve to an active website. Our additional analysis revealed that the base domain myftp[.]org redirects to freeddns[.]noip[.]com, a subdomain belonging to No-IP, a legitimate DNS and domain name registration service provider. According to the company's website, No-IP offers both paid and free services that allow users to map static and dynamic IP addresses or long URLs to a customizable No-IP-owned domain. The free dynamic DNS service provides users the ability to create up to three hostnames, automate dynamic DNS updates, and configure URL and port 80 redirects for the purpose of establishing remote connections to home security cameras, home-based gaming servers, and other internet-connected devices.

Based on this phishing campaign, the NTIC Cyber Center assesses with medium confidence that cyber threat actors will likely continue to leverage and exploit No-IP free dynamic DNS services to attempt to trick victims into visiting malicious websites.



(screenshot of Zoom phishing email courtesy of BleepingComputer)



(screenshot of associated phishing landing page courtesy of BleepingComputer)

RECOMMENDATIONS

The NTIC Cyber Center recommends network administrators of organizations whose employees do not currently have a legitimate business need for No-IP dynamic DNS services on an enterprise network proactively block all outbound traffic to the following associated base domains:

noip[.]com
myftp[.]org
myftp[.]biz
hopto[.]org
ddns[.]net
ddnsking[.]com
3utilities[.]com
bounceme[.]net
freedynamicdns[.]net
freedynamicdns[.]org
gotdns[.]ch
myddns[.]me
myvnc[.]com
onthewifi[.]com
redirectme[.]net
servebeer[.]com
serveblog[.]net
servecounterstrike[.]com
serveftp[.]com
servegame[.]com
servehalflife[.]com

servehttp[.]com
serveirc[.]com
serveminecraft[.]net
servemp3[.]com
servepics[.]com
servequake[.]com
sytes[.]net
viewdns[.]net
webhop[.]me
zpto[.]org

We also recommend blocking the following email sender domain as it was associated with this phishing campaign and currently promotes a bulk emailing service:
jason-sg[.]com

The information contained in this alert is designated TLP:GREEN. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

We welcome your feedback.

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

TLP:GREEN

Disclaimer: NTIC Cyber Center Cyber Alerts are 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, signing up via our website, 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.

