CYBER SECURITY ADVISORY – COVID-19 PHISHING

March 28, 2020

EXECUTIVE SUMMARY

You are receiving this advisory to make you aware of increased Phishing and malicious activity using the COVID-19 pandemic as a lure. A prominent security organization has observed a 667% increase in COVID-19 related phishing activity since the end of February.

An Ontario organization in the Public Sector was recently impacted, and a compromised account was used to distribute phishing messages with the subject line, “Re: COVID-19 (Payroll Adjustment)".

It is strongly recommended that organizations exercise a heightened level of awareness around emails related to COVID-19/Coronavirus and that they follow email hygiene/ phishing best practices to defend against the increased threat.

HOW DOES THIS INCIDENT AFFECT MY ORGANIZATION?

Phishing and fraudulent emails remain a prominent way in which attackers can gain access and compromise security; malicious parties can try to steal credentials and make victims think the emails come from a trusted party and attempt to convince them to click on malicious links or malicious attachments.

The Government of Ontario Cyber Security Division is aware of phishing scams using the COVID-19 pandemic as a lure. Sophisticated threat actors (including multiple nation-state backed groups) are often behind the scams.

The phishing emails sent by the impacted Public Sector organization contained a link that led to a fraudulent site which attempted to convince users to enter their email credentials.

WHAT SHOULD I DO?

As soon as possible, forward this notification to your IT support partners for immediate action.

If you have received any emails with the subject line, “Re: COVID-19 (Payroll Adjustment)” delete them.

TECHNICAL DETAILS:

COVID-19 related phishing attacks have increased 667% since the end of February. The four main types of COVID-19 phishing attacks are scamming, brand impersonation, blackmail and phishing messages distributed from compromised email accounts. Goals of the phishing attacks include malware distribution, credential theft and financial gain.

Threat actors are known to be sending alerts that appear to be from the World Health Organization, pose as official communications from University personnel, purport to have information on the spread of Coronavirus, as well as emails that target personnel who are working from home.

In addition to this, we are also aware of recently registered domains "selling" masks and sanitizer, and scams featuring “doctors” pretending to work for the Centers for Disease Control and Prevention (CDC) asking people to download attachments for more information or to donate bitcoin. Other topics include emails from companies on their preparations for COVID-19 (which often include malicious attachments) and blackmail themed emails threatening people with COVID-19 infection if they don’t pay a ransom.

The Canadian Anti-Fraud Centre reports that other phishing scams include private companies offering fast COVID-19 tests for a price, or fraudsters urging investment in “hot new stocks” related to the COVID-19 pandemic.

The Government of Ontario Cyber Security Division also expects to see threat actors leverage the Government’s recent announcement on Ontario's Action Plan: Responding to COVID-19 (March 2020 Economic and Fiscal Update) for more phishing themes. Phishing themes will likely be related to child care subsidies, utilities and tax rebates or deferrals, OSAP loan relief, mortgage payment deferrals and the emergency assistance program.

The Government of Ontario Cyber Security Division has indicators of compromise related to this threat. You can receive these by emailing cyberadvice@ontario.ca, with the subject line “corona ioc”

RECOMMENDED ACTION:

Be wary of COVID-19 related emails asking you to open attachments or click on links. Especially from sources that you would not normally receive emails from, or from sources that would not expect would be providing information on COVID-19.

Exercise caution when opening emails related to COVID-19 even from organizations you do expect to receive communication from. Threat actors will attempt to disguise their emails so that they appear to come from trusted organizations. See the links below for more tips.

The Canadian Anti Fraud Centre provides educational material and guidance on various fraudulent activities including phishing and related scams, more information can be found at the following site: http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/phishing-hameconnage/index-eng.htm

The Canadian Centre for Cyber Security has resources on how to spot phishing messages and a webpage on COVID-19 related phishing.

https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100

https://cyber.gc.ca/en/guidance/cyber-hygiene-covid-19

FOR FURTHER INFORMATION

If you find any of the indicators of compromise (IOCs) on your networks, have related information or any questions, please contact cyberadvice@ontario.ca.

NO WARRANTY

This Cyber Advisory contains third party content and links. CS CoE does not control or maintain third party links and makes no representation or warranty that the link will still work when you click on it or the service or content is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether you want to follow any link or agree to receive or rely on any service or content that is made available to you.

Cyber Security CoE is providing information about a known threat for potential use at the sole discretion of recipients to protect against cyber threats. This notification is provided to help health care organizations enable cyber preparedness and resilience.

DEFINITIONS:

Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security THREAT Advice is issued when NO ACTIVE EXPLOITS are observed. Purpose of the advice: to enable organizations to prepare for and mitigate cyber threats.

- Cyber Security INCIDENT Advice is issued when an ACTIVE EXPLOIT is observed. Incident advice is time sensitive to inform partner organizations of an ongoing cyber incident for a timely response and remediation.