A Cyber Campaign Stealing Payroll Information Is Affecting Local Governments in New York State

The Cyber Analysis Unit of the New York State Intelligence Center (NYSIC) has recently issued a report on a cyber campaign that has affected several local governments in New York. This campaign involves customized and convincing-looking phishing emails that were used to capture user login names and passwords. These credentials were then used by cyber criminals to redirect payroll deposits to bank accounts controlled by the malicious actor(s). Municipal employees and officials should be instructed to call the local government’s information technology support line if they have any questions about a suspicious email before clicking on any link.

While there is no indication that the people responsible for these campaigns are specifically targeting New York’s local governments, these examples are yet another indication of the sophistication and pervasiveness of cyber criminals. Together with the multiple incidents of ransomware in local governments that have been publicized in the open press, these cases remind us of the need to be ever vigilant and careful in the use of email and social media.

NYSIC encourages you to make sure everyone who has email accounts on your systems is aware of this campaign and advise them to be extra careful in their use of email. In particular, never to give their account credentials to anyone, even the IT professionals in your organization.

The specific emails in question appeared to come from the local governments’ “Help Desk” and requested employees click on a link to update email account information. When individuals clicked on the link and provided their information, the malicious actor used the credentials to take control of victims’ payroll accounts, diverting payroll deposits to the hacker’s bank accounts.

The emails appeared to be from an official source and contained the subject lines, “Important update – Action required” or “Important update for [employee/victim email address]”. In addition, the emails explained (1) that a supposed system upgrade required the recipient to login utilizing the a link in a large box colored blue with white letters and spelling out the word “HERE” and (2) that a non-response would result in the account being deactivated. Finally, the emails are signed by the government entity’s help desk using appropriate agency branding, and the bottom of the email body contains official instructions detailing proper usage and handling.
The following elements of an email are indicators of a possible phishing campaign:

- The “From:” line of the email appears to be from a different state than the recipient yet claims to be from a local municipality.

- The “From:” line of the email is from a domain indicative of a school district while claiming to be from a local municipality.

- The “To:” line shows the recipient’s full email address rather than name which indicates the email may be from outside the network.

- The email’s date and time stamp are outside of typical business hours.

- The email is addressed “Dear (entire email address of recipient)”.

- When the recipient hovers the mouse over the link in the email (without clicking the link) shows a website link to Outlook Web Access (OWA) which is a remote way to access email outside a network.

If someone in your municipality receives such an email, we encourage you to alert Federal authorities by forwarding the email to the Federal Trade Commission at spam@uce.gov and to the FTC’s Anti-Phishing Working Group at reportphishing@apwg.org, and by reporting the phishing attack at ftc.gov/complaint. New York State has also asked that you report any emails similar to one described in this message to them by notifying the NYS Division of Homeland Security and Emergency Services at (866) OCT-CIRT. Of course, if you fall victim to this campaign, we encourage you to contact law enforcement immediately.

More specific advice about phishing may be found at the New York Department of State’s website at: https://www.dos.ny.gov/consumerprotection/identity_theft/protect_yourself_from_identity_theft/phishing.html and from the FTC at https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.