**City of Coral Gables**
**Information Technology Department**

**Case Study: Email Phishing Attacks to Local Municipalities on the Rise during the Covid-19 Pandemic**

**Prepared by:** Raimundo Rodulfo, P.E., SMIEEE - CIO / Director of Information Technology | May 2020

## Abstract

During the Covid-19 pandemic, local municipalities in the U.S. have been dealing with waves of email phishing attacks that have significantly increased in frequency, force, and complexity from March to May 2020. Recent advisories from DHS-CISA and international cybersecurity agencies confirm what many local government entities have already experienced: that hackers are increasingly targeting organizations with phishing scams to steal usernames and passwords, and that as organizations depend more on the internet and teleworking during the pandemic, cybercrime has significantly gone up.

This case study documents one of the recent attacks that targeted multiple local municipalities in the U.S. This kind of attacks are on the rise during the Covid-19 pandemic and have similarities with other coordinated phishing campaigns that have targeted organizations in several countries in recent months, exploiting the current crisis and the accelerated digital transformation it has triggered worldwide.

## Objective

The objective of this paper is to raise awareness on the risks that local municipalities face from this kind of phishing attacks and the growing threats associated with them, and to propose solutions and best practices to mitigate those risks.

## Identify

The MO and the symptoms of these attacks are, with case-to-case variations:

1. Phishing emails sent to employees with a faux electronic document form/link (e.g.: fake DocuSign, Box, Dropbox, FTP sites, Covid-19 related sites, job sites, ticketing portals, etc.) impersonating/spoofing a real official or provider of the organization ->
2. Users affected by the scam are asked to provide their email credentials to "log in", review "documents" or "data reports", "register" on a site, "open a ticket", etc. ->
3. The scammer (or malicious AI bot) fraudulently obtains the user's cloud email credentials (e.g.: Office 365, Gmail, etc.) and uses them to obtain access to the employee's email account ->
4. The scammer (often using malicious AI bots) starts impersonating the targeted employee from their compromised account to scam other employees and propagate the phishing attack to other organizations (e.g.: other municipalities in their region) from the compromised email account, sometimes collecting the users contact list and sending emails from an outside open relay ->
5. Other organizations may receive the attack from a "real/trusted account" (compromised by the attacker) impersonating an employee from the first municipality, which now unwillingly acts as proxy helping propagate the attack to other organizations.

Content examples of the phishing emails, signaling with a label the fake sources used in the scam:

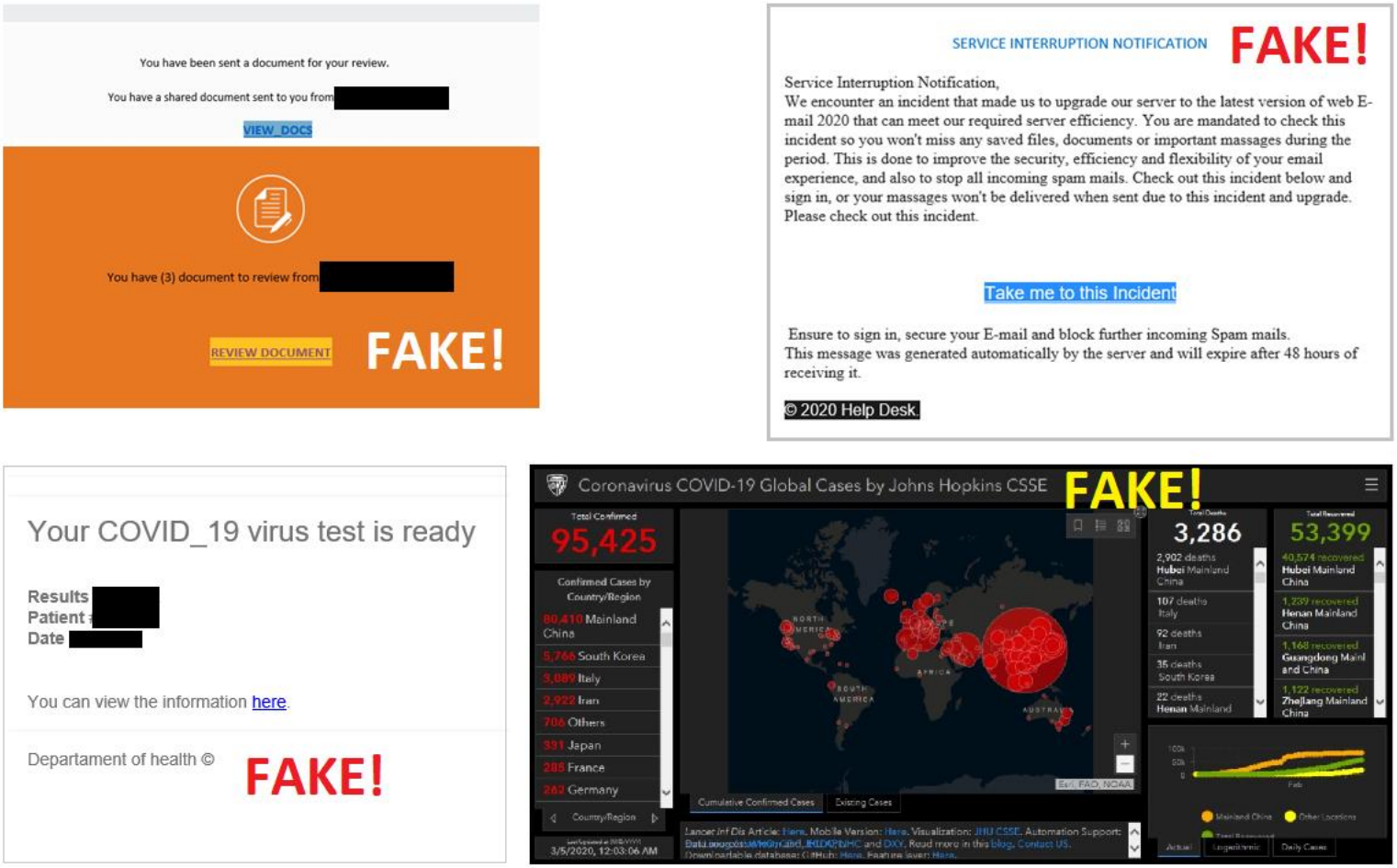


**Figure 1 -** Phishing email scams associated with these attacks: fake documents/tickets/notifications/reports

**Detect**

When an attack like this is happening, it is critical to quickly determine which email accounts and internal users and systems have been affected or are at risk to be affected in the organization. A combination of user awareness and enterprise security systems, including content filters, advanced threat detection and log/event management systems, allows a prompt detection of this kind of phishing attacks. For example:

- Various enterprise email management platforms in the cloud are capable of quickly pointing to all accounts at risk, which allows the response team to contain/isolate them, scan them, remediate them, and eventually reset them to normal status with new credentials and controls.
- For example, these platforms can generate alerts triggered by unusual behavior, or user login attempts and password resets coming from suspicious/unusual domains.
- Since the initial phishing emails of this kind of attacks may come from trusted organizations and real user accounts, the effectiveness of the first line of defense relies on the detection capabilities of the systems that handle the email process chain, and the ability of the end users to identify the risks and follow avoidance and reporting protocols.
- Prompt notifications coming from users to administrators of any suspicious email as soon as they see it and the immediate activation of internal response mechanisms can quickly stop the attack.

**Respond**

It is critical at the beginning of the incident response to prevent these attacks from propagating to other users and from further compromising enterprise networks, systems, applications, or data through the execution of malware. Some of the measures that can help to achieve that objective are:

- Conduct an initial impact and risk assessment of the phishing attack by building on the detection capabilities described above, and adding these steps (as applicable to each case scenario): i. Determine all internal users that received and resent the malicious messages, all external sources of the malicious emails, and all external high-risk links and files that are part of the attack. ii. Review systems and security logs, including all enterprise and cloud-based security defenses, to quickly detect all high-risk or malicious sign-ins and suspicious activity such as password resets, to mitigate and remediate accordingly. iii. Examine the header of the NDRs received by the user via the malicious messages. iv. Determine the originating IP and return path, to shape the appropriate filtering measures.
- Immediate containment and remediation actions are executed after the first detection and initial impact assessment, and include reactive measures to stop the attack, such as: i. Temporarily disable compromised accounts. ii. Reset passwords of all affected and at-risk email users. iii. Scan the users' computer and mobile devices for malware. iv. Block the originating IP address and source Internet service provider of the attack (if feasible, based on live/production constraints).
- Send an advisory to all users in the organization, through the appropriate and most effective dissemination channels, warning them of the phishing attack and the characteristics of the malicious emails, links and attachments, and asking them to follow the established protocols for reporting and risk avoidance. Also, reach out to the official points of contact and email administrators of the other agencies and third parties affected by this attack, to collaborate on a coordinated response and joint action plan, and quickly alert and educate all their users at risk.
- Run IP tracing and other network and data flow forensics analyses to determine where the attacks originate from, understand their behavior, and take the appropriate filtering actions.
- Use an isolated testing environment to analyze the traffic associated with the malicious URLs and identify users and client computers at risk to perform immediate scans and remediation steps.
- Analyze potentially malicious URLs with the use of trusted online cybersecurity intelligence tools and set up web filtering on blocks of malicious URLs to mitigate the risk of users clicking on risky links and engaging with the hackers.
- Run frequent scans on all backend, frontend, and client systems after the incident, to make sure they return clean and clear of malware traces. Perform a full antimalware scan on physical computers and virtual environments of all users, including those where no threats were initially found. Continue monitoring on a continuous basis.

**Risk Mitigation and Prevention**

If a phishing attack like this has been able to reach the organization's email users and put them at risk, an immediate analysis of gaps and lessons learned should be performed in parallel, in an agile manner, to implement timely reinforcing and remediation action plans and appropriate incident response steps to mitigate the risk of subsequent similar attacks. This analysis should include in-detail network and cloud cybersecurity scans to make sure no backend or client systems have been affected beyond the user email accounts. It is also important to share in a compliant way the lessons learned with the other organizations affected by the attack and update the organization's Incident Response Plan (IRP) accordingly. Effective mitigation strategies to prevent future attacks and block attempts like these should include:

- Review current configuration and setup of networks, email platforms and enterprise systems, strengthen cloud security infrastructure, and improve remediation plans based on best practices.
- Create conditional access policies for logging in to the email cloud platforms. These policies monitor all login attempts and block any attempts to the system from outside the trusted domains. Set up log analysis services to collect all user logins to look for common threats, unusual login attempts (e.g.: time, device, geolocation, activity), and provide insight on executed action plans and policies.
- Reinforcing cybersecurity systems with tools to fight adversarial AI like phishing bots and other advanced threats. Deploy AI-based anti-malware alert and monitoring security engines to further protect cloud and enterprise-based digital assets.
- Communicate and collaborate with trusted/partnering official security expert entities and auditors, to discuss best practices and increase awareness of known threats, cases, trends, and solutions.
- Continuously harden the organization's cloud and on-prem assets with advanced security tools offered by trusted partnering expert organizations, hosting providers and enterprise security solutions in place. Check with your cloud and email providers what enterprise security tools they offer in their platforms, and what security hardening configuration they recommend for high-risk environments; for example: anti-phishing/anti-spam, DLP, intrusion detection, antimalware, encryption, identity management, PoLP, auditing, monitoring, and other tools and controls.
- Enable multi-factor authentication in your cloud/email environment, and deploy it to users, where appropriate. Disable legacy protocols and authentication, and deprecated tools/configurations.
- Continue running daily malware detection scans in all enterprise systems and keep all security systems up to date with latest versions, patches, and definitions.
- Information security policies should be periodically reviewed and validated for best practices on data classification, email retention, and mobile device management.
- Maintain a cybersecurity awareness and education program on cyber-hygiene that covers how to deal with phishing scams and follow email best practices. One of the most effective lines of defense is a well-informed and aware user community which reduces the risk of access, redirection, account compromise and system penetration by malicious actors.
- Education and awareness campaigns aimed to all employees and stakeholders in the organization, and multi-layered advanced threat detection, content filtering, intrusion prevention and other cybersecurity systems and controls -when properly designed, implemented, configured and maintained-, have proven to be effective preventing, detecting, and responding to this kind of attacks.

**Conclusion**

Email phishing attacks is just one of many risks and threats impacting local municipalities and other government organizations. Many other threats such as ransomware, credit card and e-commerce fraud, hacking of web and social media sites, DDoS, and others, are also on the rise. Now more than ever, organizations need to properly plan and carefully execute a comprehensive information security strategy that covers all necessary aspects of risk management, detection, protection, response, cyberinfrastructure and asset management, and compliance. Protecting the organization's information assets is a team effort where all members of the organization and its stakeholders are key participants in a first line of prevention, detection, and defense. As the risks rapidly grow and evolve during the Covid-19 pandemic, the organization's cybersecurity strategy, awareness, and controls must be continuously reviewed and improved.