Hopkinton Police Department

LAW ENFORCEMENT BULLETIN

Detective Bureau
74 Main St.
Hopkinton, MA 01748
508-497-3401
508-497-9785 (Tip Line)
detective@hopkintonpd.org

The Hopkinton Police Department wants to ensure the public is aware of potential scams being perpetrated across the state and the country during this unprecedented time.

Social Engineering: a psychological technique used by cyber threat actors to trick victims into performing actions against their best interest, or the interest of their organization. The most common forms of social engineering include phishing, spear phishing, whaling, vishing (voice phishing), and domain name and email spoofing. These methods are used to steal login credentials, obtain financial and other sensitive data, and infect victims with malware.

- A cyber security company observed several COVID-19-related email phishing campaigns spoofing official correspondence from known entities. These campaigns featured messaging advertising a secret cure for the virus, masquerading as an internal email from a business organization's president, and impersonating health authorities such as the World Health Organization. Many of these emails included links to spoofed websites designed to trick email recipients into surrendering user credentials for services by DocuSign, Microsoft Office 365, and Adobe. Other emails contained malicious

attachments that, when opened, install the NanoCore remote access Trojan to grant an attacker full control over a compromised system or the AgentTesla keylogger to record keystrokes and steal banking and financial information from victims.[1]

- An antivirus company observed COVID-19-related phishing emails disguised as correspondence from the Centers for Disease Control, advice from medical experts on how to protect against the virus, and human resources policies outlining organizational procedures for workplaces.[2]
- Security researchers discovered malicious code embedded in a website hosting a fraudulent copy of Johns Hopkins University's interactive COVID-19 heatmap. The website, registered in February 2020, hid a variant of AzorUlt spyware that was capable of skimming visitors' passwords and payment card details as well as deploying other malware. The website has not been observed in any known malicious email campaigns; however, it is believed that the threat actors have relied on organic visitor traffic to the website to propagate the information-stealing malware contained on the webpage.[3]

What can you do to protect yourself?:

Network Management

• Set a network performance baseline for network monitoring prior to an infection to improve your ability to detect anomalies and malicious activity.
• Ensure your firewall is enabled and properly configured.
• Close and monitor unused ports.
• Disable SMBv1 on firewall and all systems on the network.
• Block inbound traffic to TCP/UDP ports 139 and TCP port 445.

---

[1] (U); Sherrod DeGrippo; Proofpoint; "Attackers Expand Coronavirus-Themed Attacks and Prey on Conspiracy Theories"; 13 FEB 2020; https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracy-theories; accessed on 13 MAR 2020.
[2] (U); Steve Symanovich; Norton; "Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams"; published date unknown; https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html; accessed on 13 MAR 2020.
[3] (U); David Ruiz; Malwarebytes Labs; "Battling Online Coronavirus Scams with Facts"; 10 MAR 2020; https://blog.malwarebytes.com/socialengineering/2020/02/battling-online-coronavirus-scams-with-facts/; accessed on 13 MAR 2020

• Block known malicious Tor IP addresses.
• Perform vulnerability scans against your IP address range(s) regularly to identify poorly configured and vulnerable internet-facing systems and take the appropriate corrective actions as needed.

Mobile Device Management

• For Apple iOS devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media and apps from the official App Store, and avoid “jailbreaking” the device.
• For Android devices: disable the “unknown sources” option in the Android security settings menu, install apps only from the official Google Play store after carefully reading the associated ratings and reviews, and avoid "rooting" the device.

Legitimate Websites for COVID-19 Information

- Centers for Disease Control and Prevention (CDC): https://www.cdc.gov/
- Massachusetts Department of Public Health (MDPH): https://www.mass.gov/orgs/department-of-public-health
- Massachusetts State website: https://www.mass.gov/
- World Health Organization (WHO): https://www.who.int/
- American Red Cross: https://www.redcross.org/
- Massachusetts Emergency Management Association (MEMA): https://www.mass.gov/orgs/massachusetts-emergency-management-agency
- GIS Mapping: https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

As always if you are unsure or have questions regarding a potential scam please call the police department and speak with an officer 508-497-3401.