WINSTON & STRAWN LLP

BLOG

Healthcare Organizations and Essential Services Increasingly Targeted as Pandemic-Related Malicious Online Activities Persist

MAY 11, 2020

On May 5, 2020, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert, warning of the continued attacks by malicious cyber actors seeking to capitalize on the COVID-19 pandemic. This is an update to a previous alert issued by these organizations to provide additional guidance on safeguards that organizations can implement to best protect themselves against these attacks.

CISA and NSCS announced that they continue to see bad actors using COVID-19-related targeting efforts, and noted that they are seeing a growing number of incidents in which these attempts are targeting organizations specifically involved in national and/or international pandemic responses, including:

- Pharmaceutical companies
- Healthcare organizations and bodies
- Medical research organizations
- Local governments
- Academia, including universities

These efforts are likely driven by attempts to steal sensitive research data and intellectual property related to COVID-19, intelligence on national and/or international health care policy, and bulk personal information. Companies with global reach and international supply chains may be particularly attractive targets; cyber actors view supply chains as a "weak link" that they can exploit to obtain access to better-protected targets. These potential vulnerabilities may be exacerbated by the shift to increased remote working and related technologies like VPNs.

In particular, "password spraying" is one commonly used style of attack that is on the uptick; cyber actors enter commonly used passwords in numerous organizational email accounts, hoping to successfully reach a targeted organization's network. These attacks can be successful because, in a large set of users, there will likely be some number of them that have common passwords—and if even a single account is compromised, the bad actors can use the successful password to then access other accounts and information.

To mitigate against this sort of brute-force attack and other malicious cyber action, CISA and NCSC have provided a set of recommendations that includes the following:

- **Ensure secure passwords are in place.** Review your organization's password policies and encourage all users to frequently update and maintain secure passwords. This includes avoiding frequently used phrases and words such as the month or the year, seasons, and the name of the company or organization. Also consider implementing multi-factor authentication if it is not already in place.
- **Keep all software, systems, and devices as up-to-date as possible.** Apply software patches and security updates as soon as they are available. This includes updates to VPNs, network infrastructure devices, and other devices being used to facilitate remote-work environments. In addition, use modern systems and software whenever possible, as they have stronger security built into them than older models do.
- **Safeguard the management interfaces used to oversee your infrastructure.** It is crucial to protect the management interfaces for different technologies implemented within your organization. This includes remote-access tools, browser-based administration interfaces to configure infrastructure, and web-based interfaces that can be used to configure cloud services. Applying appropriate safeguards can help prevent outsiders gaining privileged access to your vital assets.
- **If your organization does not yet have security-monitoring capabilities, implement them now.** These logging processes will allow your organization to collect the data that will be needed to analyze network intrusions, should they occur; to recover from an incident; and to develop a defense.
- **Review and, as needed, update your organization's incident-management processes.** Have a plan in place before an attack occurs. This should include the type and nature of incidents, and determining what steps your organization will take—and which individuals will take them—when a cyber-attack or other security incident occurs. As a practical matter, these risk-based plans should account for any remote-work environments and proactively address any challenges that may be encountered from activating the response procedures from multiple locations.
- **Consider investing in antivirus software, anti-spyware tools, and/or firewalls.** This is especially critical if the organization is using older devices or cannot implement other information security measures. Once these tools are implemented, ensure that alerts are enabled so any threat can be identified and isolated or otherwise addressed in a timely manner.

View all of our COVID-19 perspectives here. Contact a member of our COVID-19 Legal Task Force here.
3 Min Read

Authors

Sara Susnjar

Alessandra Swanson

Related Locations

Chicago | London | Paris

Related Topics

COVID-19 | Health Care Privacy

Related Capabilities

Privacy & Data Security | Health Care

Related Regions

Europe | North America

Related Professionals

Sara Susnjar

Alessandra Swanson

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.