ATTORNEYS AT LAW

BULKLEY
RICHARDSON

BETTER REPRESENTATION

RANSOMWARE ASSAULTS THREATEN HEALTH CARE PROVIDERS

Three federal agencies, including the Federal Bureau of Investigation, have “credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers.” The threat, described in more detail in a **Joint Cybersecurity Advisory**, is of the installation of ransomware and other malicious code.

This malicious code makes its way onto a company’s network through a three-step process:

- Step one is typically an email phishing campaign, during which an employee clicks on a link that downloads malware.
- Step two is typically that a loader, like TrickBot or BazarLoader, discussed below, distributes the “payload” and uses a back door to install the malware on an end-user’s machine.
- Step three is whatever is of most value to the attackers—data exfiltration, the encryption of data accompanied by a demand for ransom, or monitoring of network communications to prepare more targeted, high-value schemes, such as business email compromise.

The Joint Cybersecurity Advisory gives information about the hallmarks of the TrickBot and BazarLoader “loaders” that install malware on servers and user’s machines, and Ryuk Ransomware, which is deployed to encrypt data (and, if they choose, for the attackers to demand ransom for the decryption of data). The Advisory includes a link to an **open source tracker** for TrickBot C2 servers, **a list of indicators of compromise** by the BazarLoader and several tips for mitigating a ransomware attack.

If you are a health care provider, please consider taking the following steps immediately to protect your data and networks:

- Provide a copy of the **Joint Cybersecurity Advisory**, which includes the technical details of the attack, to the manager of your business’s technology. They may be able to use that information to scan for the malware and improve your existing defenses.
- Tell your employees—all of your employees, including C-suite executives, who are frequent targets of phishing campaigns—that phishing emails are the entry method for this very serious threat to your business’s systems. In many cases, such emails appear to be routine, legitimate business correspondence. Employees should be instructed to refrain from clicking links or downloading attached files if the email address of the sender, the language in the attached email or any other element of the correspondence **appears suspicious**.
- Identify critical assets such as patient database servers, medical records and telehealth and telework infrastructure. Create backups of these systems and house the backups offline from the network and under password protection.
- Develop or update existing business continuity and recovery plans to account for this threat.

> If you experience a ransomware or other cyberattack, would like to update your existing WISP to account for this threat or have any further questions, please contact Bulkley Richardson’s Cybersecurity Practice Group.

Lauren Ostberg

✉ lostberg@bulkley.com
☎ 413-272-6282

Jim Duda

✉ jduda@bulkley.com
☎ 413-272-6284

Scott Foster

✉ sfoster@bulkley.com
☎ 413-272-6258