September 29, 2016

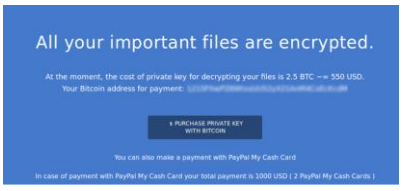
RANSOMWARE THREATENS HEALTH CARE INDUSTRIES

RECENT SPIKE OF INCIDENTS

Health care professionals and organizations are being targeted by cybercriminals on a regular and increasing basis. This disturbing trend in health care is not surprising when one considers that electronic medical records (EMRs) provide a treasure trove of both personal health information (PHI) and personal information (PI) that is extremely valuable on the black market. The personal information included in a typical medical record supports the creation of false identities to commit insurance fraud or enables the sending of malicious emails (phishing) to gain entry to IT systems. Health care has evolved to become "the most profitable malware victim in history". Hospital information systems and EMRs are extremely complex, multifaceted health systems in which critical, personal patient information contained in patient records can be distributed across multiple IT systems. These records include extensive personal histories, social insurance numbers, birth dates, names of relatives, addresses, government-issued health card numbers and other data valuable to cyberattackers. In addition, financial information is often collected. Together, these data sets are valuable to identity thieves and (especially in the U.S.) medical insurance scammers.

Cybercriminals are using an increasing set of aggressive tactics to either gain unauthorized access to third party personal information, or, as in the case of ransomware, to deny health care professionals EMR access by encrypting the data and withholding decryption tools until a ransom is paid. The fact that hackers are able to encrypt medical records doesn't necessarily mean they have gained access to those files, but the goal of this type of cyberattack is to make sure that the user cannot get access to their records. In health care, the consequences of any cyberattack are serious — personal health information can be lost, destroyed, or shared with malicious attackers, patient treatment can be delayed, and lives could even be lost as a result of systems being locked down by malicious attackers. There are a number of steps health care professionals can take to reduce their risk of a ransomware attack, as well as mitigate the potential harm.

WHAT IS RANSOMWARE?



Ransomware is a form of malware or malicious software distinct from other malware. Ransomware is initiated when someone unknowingly opens an email attachment containing a ransomware virus. Its defining characteristic is that it denies the user access to their data by encrypting the data with a key known only to the hacker who deployed the malware until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. More sophisticated ransomware may also encrypt back-up files and databases.

OntarioMD
Empowered Practices. Enhanced Care.

Indicators of a ransomware attack could include:

- A user's realization that a link that was clicked on, a file attachment opened, or a website visited, may have been malicious in nature;
- An increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- An inability to access certain files as the ransomware encrypts, deletes and renames and/or relocates data; and
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

HOW CAN PHYSICIANS PROTECT THEIR PATIENT DATA?

- Limit direct server access to system administrators. Users should only access workstations for daily use of their EMR.
- All workstations should have up-to-date anti-virus/anti-malware software, and operating system updates applied.
- Minimize the number of people with system administrative privileges. It is particularly damaging if this account information is stolen.
- Use strong alphanumeric passwords, and change them regularly (e.g., every 90 days).
- Ensure your Information Technology Provider has back-ups scheduled for your data with appropriate frequency, and that the back-ups are tested regularly for consistency.

WHAT TO DO IF YOU HAVE BEEN HIT WITH RANSOMWARE?

Once an attack has occurred, computers and networks should be shut down immediately. After containing the threat, staff should contact their EMR vendor's information technology department, their OntarioMD Practice Management Consultant, and the Ontario Medical Association.

Once your IT provider is engaged, they will help determine the extent of the impact. In most cases, the most complete way to remedy the situation is to restore data from back-ups prior to the ransomware attack. The appropriate local administrator should also convene an investigation team encompassing health IT professionals and clinicians to identify the root cause and establish processes for preventing and mitigating future incidents.

IS THIS A PRIVACY BREACH? CAN ATTACKERS ACTUALLY ACCESS YOUR PERSONAL HEALTH INFORMATION?

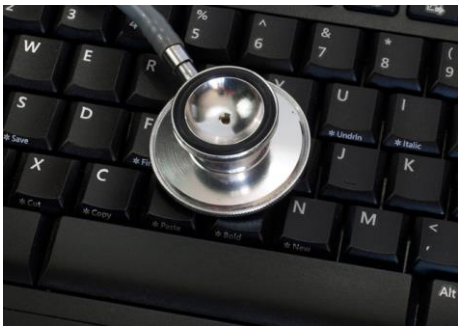
A ransomware attack is not usually a privacy breach. If EMR data is encrypted and cannot be accessed by a third party, there is no unauthorized access or disclosure of personal information. However, if an investigation shows that personal information was distributed to, or accessed by, an unauthorized third party, or, if a health care professional is locked out of their EMR and access cannot be restored through back-up, then notification to the appropriate regulatory entities and individuals should follow.

SOME SPECIFIC STEPS TO ADDRESS THE THREAT OF RANSOMWARE:

1. **Elevate awareness in your practice of potential threats.**
   - Cybersecurity must be considered as major a threat to patient safety as fires, hospital-acquired infections, or natural disasters.
   - Enhance employee awareness about malware threats and educate appropriate individuals on information security principles and techniques.
2. **Think like a hacker.**
   - Consider the following: How would you attack your own EMR system? What is the weakest link or the easiest back door? Ask your IT support to help identify this weak link.
3. **Make sure EMR back-ups are regular, secure and separate.**
   - In the case of a Local Client Server, a back-up restore of your EMR is only effective if the back-up itself is not encrypted, so it is important to keep multiple days' versions as opposed to over-writing the back-up file every night. Consider implementing a local and off-site back-up solution at the same time.
   - Verify the integrity of those back-ups.
   - Ensure back-ups are not connected to the computers and networks they are backing up.
   - Keep a recent back-up/recovery process copy — off site, with a well-defined frequency.
4. **Have up-to-date anti-virus and malware detection software installed on all computers and servers.**
   - Keep all software programs up-to-date with the latest patches, including operating systems, applications, browsers, plug-ins, firmware and anti-virus tools. All end-points should be patched as vulnerabilities are discovered.
   - Develop and maintain a whitelist of software programs that users are allowed to run and another list of those programs that are at risk of bearing malicious code. Only allow systems to execute programs known and permitted by security policy.
5. **Implement user-focused strategies to make defense systems more reliable.**
   - Health care providers and staff must operate applications and devices securely, and must be taught to spot email messages likely carrying malicious code.

- It is recommended to conduct simulating phishing attacks to educate employees, as well as routine risk and impact assessments, to prioritize applications that can experience downtime, and for how long, should an attack happen.

6. **Ask internal and external IT support to audit your disaster recovery and business continuity planning.**
7. **Limit use of privileged accounts.**
   - Minimizing the number of staff with administrative privileges. This information is very vulnerable.
8. **Beware of macro scripts.**
   - Do not enable macros in document attachments received via email.
   - Disable macro scripts from files transmitted via e-mail.
9. **Treat unsolicited attachments cautiously.**
10. **Prepare for a ransomware attack TODAY.**
    - Assume you will be targeted in a ransomware attack and prepare now. This includes developing specific plans on how you will continue to operate without access to your EMR, or other information systems, for an extended period of time.
11. **Review your EMR vendor's insurance.**
    - Check with your EMR vendor if their insurance covers cyber extortion demands, costs to restore compromised data, or loss of revenue from network downtime. Work with your vendor to address these gaps and others, such as breaches of protected health care information.
12. **Respond, recover, investigate and track lessons learned.**



FOR MORE INFORMATION:

If you have questions or comments not addressed in this bulletin, please contact your OntarioMD Practice Management Consultant or info@ontariomd.com. The Information and Privacy Commissioner of Ontario has also recently published a Fact Sheet on ransomware. If an infection of ransomware has occurred, the IPC has invited public institutions and healthcare organizations to contact them for advice. The IPC Fact sheet and contact information can be accessed here: https://www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=446.

OntarioMD
Empowered Practices. Enhanced Care.