Hospitals Targeted by Ransomware

Michael Torres
Sam Turner

What is **Ransomware?**

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.
Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. (CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY)

Notable Ransomware events in the past:

Reveton, 2012: claims the users computer was used for illegal activity, and a “fine” is requested.

CryptoLocker, 2013: Encrypted users files, threatening to delete encryption key if payment was not given.

CryptoLocker.F/TorrentLocker, 2014: Distributed by email with a CAPTCHA to prevent detection.

CryptoWall, 2014: Used website ads to redirect users to malicious websites that downloaded payload.

Fusob, 2015: Mobile Ransomware that claims to be organization of authority, locking device and demanding a fine.

WannaCry, 2017: Encrypted files and demanded payment via Bitcoin, 7 day deadline, large scale attack.

Petya, 2016: Locked the computer before booting into Windows, no way to unlock system.

Bad Rabbit, 2017: Encrypts users file, demanding Bitcoin as payment, distributed through false Adobe Flash update.

SamSam, 2016: Exploited vulnerabilities on weak servers, guess passwords, and attacked government/healthcare facilities.

Syskey: Windows tool used for encrypting account databases was modified to lock users out of their accounts. Was removed.

Increase in Ransomware Attacks on Hospitals

There has been an increase in ransomware attacks on US hospitals and healthcare providers. The COVID-19 pandemic has increased the amount hospitals and healthcare facilities are effected, since there is already added strain on these facilities. These ransomware attacks result in both data theft and a disruption of healthcare services (since patients have to be redirected to unaffected facilities).

- Since these are healthcare facilities the data theft not only carries the regular risks that are associated, but also results in HIPAA (Health Insurance Portability and Accountability Act of 1996) violations.
- A disruption of healthcare services can result in delayed care, which could ultimately lead to death, especially in a hospital system that is already strained under the weight of COVID-19 cases.

ACM Code of Ethics and Professional Conduct

1.2 Avoid harm

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified. In either case, ensure that all harm is minimized.

To minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. Additionally, the consequences of data aggregation and emergent properties of systems should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

ACM Code of Ethics and Professional Conduct

1.6 Respect privacy

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

ACM Code of Ethics and Professional Conduct

2.8 Access computing and communication resources only when authorized or when compelled by the public good

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code. Consequently, computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others.

Questions?

Thank you for your time.

Michael Torres
Sam Turner

References

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct.* ACM. Retrieved from: https://www.acm.org/code-of-ethics

BBC. (2017). 'Bad Rabbit' ransomware strikes Ukraine and Russia. BBC. Retrieved from: https://www.bbc.com/news/technology-41740768

BBC. (2017). Cyber-attack: Europol says it was unprecedented in scale. BBC. Retrieved from: https://www.bbc.com/news/world-europe-39907965

Constantin, Lucian. "Petya ransomware is now double the trouble". NetworkWorld. Retrieved from https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html

CyberSecurity & Infrastructure Security Agency. *Ransomware Activity Targeting the Healthcare and Public Health Sector.* CISA. Retrieved from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

CyberSecurity & Infrastructure Security Agency. *Ransomware Guidelines and Resources.* CISA. Retrieved from: https://www.cisa.gov/ransomware

Ferguson, Donna. (2013). CryptoLocker attacks that hold your computer to ransom. The Guardian. Retrieved from: https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware

Grubb, Ben (2014). Hackers lock up thousands of Australian computers, demand ransom. Sydney Morning Herald. Retrieved from: https://www.smh.com.au/technology/hackers-lock-up-thousands-of-australian-computers-demand-ransom-20140917-10hyyh.html

The Journal. (2012). Gardaí warn of 'Police Trojan' computer locking virus. The Journal. Retrieved from: https://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/

Rashid, Fahmida Y. (2016). Patch JBoss now to prevent SamSam ransomware attacks. InfoWorld. IDG. Retrieved from: https://www.infoworld.com/article/3058254/patch-jboss-now-to-prevent-samsam-ransomware-attacks.html

Petters, Jeff. (2020). The State of CryptoWall in 2018. Varonis. Retrieved from: https://www.varonis.com/blog/cryptowall/

Snow, John. (2016). Ransomware on mobile devices: knock-knock-block. Kaspersky Daily. Retrieved from: https://www.kaspersky.com/blog/mobile-ransomware-2016/12491/

Whittaker, Zack. (2017.) We talked to Windows tech support scammers. Here's why you shouldn't. ZDNet. Retrieved from https://www.zdnet.com/article/why-you-should-never-talk-to-windows-tech-support-scammers/

Photos by Taylor Vick