Westlaw Today
powered by Reuters

Ransomware attacks target health care industry

By Desirée Moore, Esq., J.D. Koesters, Esq., and Gina Bertolini, Esq., K&L Gates

OCTOBER 31, 2022

Introduction

Ransomware hit the health care industry the hardest in second quarter of 2022, according to Kroll's Q2 2022 Threat Landscape Report.[1] During these months, threat actors rediscovered opportune ways to employ this devastating weapon. For health care entities confronting this concerning trend, the best defense is a good offense — including understanding the depth and breadth of today's digital-threat landscape and resulting legal liabilities.

Key takeaways

The key takeaways from Kroll's Second Quarter 2022 Threat Landscape Report and best practices for solutions to neutralize those threats include:

- The health care industry saw a 90% increase in ransomware attacks in the second quarter.
- Although phishing emails remain the top initial access point, threat actors' use of external remote services increased by 700%.
- Ransomware actors continue to use a dual-extortion approach, leaking sensitive data on the dark web if clients refuse to pay for the encryption keys.
- Multifactor authentication and updated password requirements are simple, standard solutions to help fortify networks from these threat actors.
- Ransomware attacks continue to increase. Knowing where your risks lie and how to respond if under attack are essential to recovering operations and navigating the growing regulatory oversight of digital infrastructure.

Planning for and responding to a ransomware attack

When the ransomware group Conti disbanded in May of 2022, the health care sector took a brief sigh of relief. Prior to that, for over a year, this Russia-based criminal organization wreaked havoc on hospitals and first responders. Unfortunately, the reprieve did not last long, as the health care industry saw a 90% increase in ransomware attacks in the aftermath of Conti disbanding, according to Kroll. Newcomers to the underworld, such as the Black Basta ransomware group, filled the void left by Conti.

Organizations' workforces continue to be a point of weakness, as phishing emails remain a top initial access method for ransomware. Spoofed emails[2] containing infected links or attached files allow attackers to infect entire systems in a matter of weeks. Once inside the systems, threat actors exfiltrate sensitive data and then deploy ransomware — encrypting entire systems.

Significant ransom demands attach to the restoration of these encrypted systems. If organizations do not engage in the ransom demand and do not pay for "keys" to decrypt their systems — for example, because they may be able to restore from back up — threat actors will threaten or begin to slowly leak sensitive data onto the dark web until they are paid (a two-fold threat, if you will).[3]

Ransomware actors continue to use a dual-extortion approach, leaking sensitive data on the dark web if clients refuse to pay for the encryption keys.

Although phishing remained the top initial access method, Kroll observed a 700% increase in the use of external remote services by threat actors. Platforms such as remote desktop protocols and virtual private networks, often used to support the hybrid- or remote-work models, served as the most used venue for ransomware. The last time Kroll saw this type of increase in leveraging remote services was at the height of the pandemic.

To combat these trends, Kroll recommends organizations proactively push defensive measures across their enterprises. This includes deploying updated password requirements and multifactor authentication, which goes a long way in preventing the exploitation of remote services.

Organizations should impress diligence on their employees in identifying fraudulent emails with suspicious links or attachments and follow up with internal test-phishing campaigns. Finally, employing screening and blocking tools for particular links or attachments in emails can be effective in mitigating phishing attacks.

The current threat landscape and its corresponding liability should serve as a reminder to health care organizations of the ongoing threat of ransomware and the need for self-assessment. The Health Insurance Portability and Accountability Act's (HIPAA) requirement

that risk assessments are conducted regularly and updates are made to an organization's risk management program[4] should be considered in light of the constantly changing tactics, techniques, and procedures of threat actors.

Health and Human Services' Office for Civil Rights Director Lisa Pino re-emphasized the importance of these assessments in her call for an increase in cybersecurity posture in February 2022.[5]

Each threat actor and regulatory body brings unique challenges to organizations when it comes to navigating the digital arena.

When (not if) a threat actor finds its way into an organization's networks, understanding how to respond to the attack and mitigate ensuing regulatory and other liability will save organizations time, money, and, for health care organizations, potentially lives.

Notes

[1] Kroll, Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit (Aug. 10, 2022), https://bit.ly/3SgvFvp.

[2] A spoofed email is an email that appears to be from a known or valid email address but actually comes from a fraudulent domain, which can only be seen in the details.

[3] Paying a threat actor is not an inevitability — and indeed, recent Office of Foreign Assets Control guidelines may prohibit such payment — but this narrative provides an overview of the typical threat actor process for information purposes.

[4] See 45 C.F.R. § 164.308.

[5] Pino, Lisa J., Improving the Cybersecurity Posture of Healthcare in 2022 | HHS.gov (February 28, 2022), https://bit.ly/3D8W3Ty.

About the authors



Desirée Moore (L) is a litigation partner and founding member and co-lead of **K&L Gates**' digital crisis planning and response client solution. Based in the firm's Chicago office, Moore counsels corporations, educational institutions, nonprofit organizations, national governing bodies, sports leagues, and high-profile individuals in proactively planning for and effectively managing crises of varying magnitudes, with a particular emphasis on data security incidents and data breaches. She can be reached at Desiree.Moore@klgates.com. **J.D. Koesters** (C), a certified information privacy professional, is counsel in the firm's Research Triangle Park office in Morrisville, North Carolina. With over a decade of experience in the departments of Justice and Defense, Koesters advises clients on data privacy and cybersecurity matters, including government enforcement actions, front-end compliance across various regimes and incident response matters. He can be reached at J.D.Koesters@klgates.com. **Gina Bertolini** (R) is a partner in the firm's Research Triangle Park office, where she concentrates exclusively on health care regulatory and transactional matters. Bertolini frequently advises clients on health care privacy and security, fraud and abuse, and digital health matters, providing guidance on the complex interplay between privacy, technology and health care. Bertolini has managed multiple health system data breaches, from initial mitigation and investigation to interfacing with government regulators and developing notice and response initiatives. She can be reached at Gina.Bertolini@klgates.com.

This article was first published on Westlaw Today on October 31, 2022.