protiviti®
Face the Future with Confidence

FBI Warns of Ransomware Assault on the Healthcare and Public Health Sector

October 30, 2020

On October 28, 2020, the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and the Cybersecurity and Infrastructure Security Agency (CISA) issued a Joint Cybersecurity Advisory regarding credible information of imminent cyber attacks to infect systems in the Healthcare and Public Health (HPH) sector with Ryuk ransomware.

Ransomware campaigns using the combination of tools described in the advisory include 'dwell time' for the attacker ranging from four to six weeks. Dwell time is the amount of time an attacker spends undetected in a victim's network environment. The damage associated with previous campaigns includes:

- Encryption and ransom of vulnerable systems including medical equipment that may have a significant impact on patient safety
- Disruption of care through denial of access to medical systems and records
- Exfiltration and extortion threats made around releasing electronic protected health information (ePHI) and personally identifiable information (PII)
- Secondary costs of regulatory reporting, investigation, remediation, notifications and litigation

The Joint Advisory issued the following key findings:

- CISA, FBI and HHS assess malicious cyber actors are targeting the healthcare sector with Trickbot malware, often leading to ransomware attacks, data theft and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

Protiviti is providing guidance on this issue via this Flash Report. Such guidance is not guaranteed to prevent any attack but may impede potential vectors the campaign may utilize or allow identification of an attack underway before it is completed. Protiviti's Cyber Threat Intelligence Lab is gathering indicators of attack (IoAs) and issuing specific guidance to clients via their engagement teams. If IoAs are found, organizations should investigate or contain immediately.

General Guidance With Ransomware

Organizations should consider the following common observations related to ransomware threats that are provided with both long-term improvements to mitigate the threat and specific advice to react to an attack underway or an early detection of an IoA.

- **Observation:** Almost all attacks are facilitated by exploitation of identity. While some services and processes can be exploited, the most immediate goal of most attackers is to obtain a privileged identity (user's account) with which to explore the environment and launch further tools.

  Mitigation: Follow a three-tiered identity architecture recommended by Microsoft. Never allow domain administrators to use their domain credentials unless they are absolutely needed for the task at hand.

  React: Change privileged account passwords using a script provided by Microsoft to change the Kerberos Ticket Granting Ticket twice rapidly to lock out possibly compromised domain credentials.

- **Observation:** The damage from ransomware is maximized in an environment without backups.

  Mitigation: Store three copies of your critical data on at least two different forms of media with at least one offsite. Test your backups in a full restoration at least yearly and then readjust when they fail. Plan your full operational resilience lifecycle from business impact analysis, business continuity planning, cyber crisis management and disaster recovery.

  React: Take the backup system offline and test as soon as possible. Preserve the most recent backup possible.

- **Observation:** Traditional security tools like anti-virus scanners and lesser EDR (endpoint detect and response) tools may not be sufficient to alert and block evolving ransomware campaigns.

Mitigation: Protect your endpoints (servers and workstations) with EDR tools that monitor active processes and memory threads.

React: Consider deployment of an EDR with fresh threat intelligence. Market-leading EDR tools (e.g., Carbon Black) bring this capability. You can contact Protiviti for additional insights regarding other tools in this space. If you already have an EDR tool, deploy it more broadly and use fresh indicators of attack for scanning and monitoring.

- **Observation:** Effective monitoring and alerting are critical to stop or limit ransomware campaigns from achieving their desired impact.

  Mitigation: Assess your own security operations center (SOC) maturity and supplement needs to meet demand. Engage with a managed security service provider (MSSP) or, if possible, engage a full-service managed detection and response (MDR) provider. Work with them throughout the onboarding process. Fully understand the limitations of MSSP visibility and service provisioning as part of a holistic security approach. Work to improve the gaps observed and ensure your organization's strategy to respond to alerts is current.

  React: Alert your MSSP or MDR provider to the indicators you have seen and/or notify your internal SOC.

- **Observation:** Attacks adapt to defenses, and successful mitigation requires the ability to diagnose and respond effectively. No static plan will be sufficient.

  Mitigation: Incident response plans should be updated and implemented soon, including critical components such as crisis communications plans, engagement of counsel, public relations and surge support for technical staff.

  React: Establish a trusted channel (mobile phones or a conference bridge service) for use if attackers are already inside your mail system.

- **Observation:** Extortion attempts may follow ransom attempts. Preserve your ability to assess exfiltrated data rapidly to make rational judgments on extortion, regulatory compliance and public confidence.

  Mitigation: Recognize that the response to a ransomware attack includes more than just technical resources. Investigation and internal context for implicated systems are needed to assess risk of disclosure.

React: Review this issue with counsel and start an investigation immediately to determine the scope of the compromise. Attempt to preserve logs to enable investigation after the event.

- **Observation:** Many technical teams rely on live tools to run their networks; these systems may be the victims of the ransomware. File shares containing critical information technology team data and planning may be unavailable.

  Mitigation: Preserve regular backups of these key systems or tools offline. Preserve network and data maps in offline systems.

  React: Attempt to collect file inventories and preserve them in offline storage. Also, preserve your latest backup of critical databases offline.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Protiviti can assist companies with preparing to respond to the evolving threats posed by ransomware and other cyber attacks. Our professionals can:

- Be available in a critical situation to help you respond quickly. Contact Protiviti's Incident Response Team at IR@protiviti.com for technical, crisis management and investigative support or for any other questions/needs related to this announcement.
- Leverage our knowledge of best practices to help your organization refine its incident response plan. We can accomplish this via a dynamic range of methods including:
    - **Assessing** program strategy and process
    - **Developing** necessary **governance** and incident response structure
    - Partnering with you to identify, select and **implement key technologies** to improve response capabilities
    - Facilitating simulated exercises that **test your response readiness** and highlight key improvement opportunities
- Help you evaluate enterprise cybersecurity capabilities guided by Protiviti's expertise in dealing with healthcare organizations nationwide. We can help refine your existing strategy to ensure it incorporates not only the appropriate elements to detect and respond to threats, but also to enable more proactive protection and optimize security investments.

protiviti®