REN-ISAC

Ransomware Best Practices (TLP:WHITE)

The Colonial Pipeline attack—including its implications for critical infrastructure—only further highlights the growing ransomware problem. According to the FBI, ransomware attacks have dramatically increased over the past few years (37% from 2018 to 2019; 20% from 2019 to 2020). The pandemic led to the number of attacks more than doubling year-over-year, with a particularly large surge in the education and healthcare sectors.

Vectors of Initial Access

According to REN-ISAC analysis of the most prevalent ransomware targeting EDUs and teaching hospitals (which aligns with the latest Mandiant M-Trends Report), these groups predominantly rely on the same initial access vectors including

- Phishing (T1566, such as malspam)
- External Remote Services (T1133, such as VPNs/RDP)
- Valid Accounts (T1078, such as credential stuffing and brute-forcing)
- Exploit Public Facing Apps (T1190, such as ERPs and Firewalls)

Mitigate and strengthen these access points by

- Ensuring public apps are protected from OWASP Top 10
- Locking down/disabling Office macros
- Changing the default file handlers to Notepad for file extensions **.hta, .js, .jse, .vbs, .vbscript, .wsf, .wsh**
- Pushing security patches fast and frequently
- Having a process for identifying/changing compromised credentials
- Implementing multi-factor authentication

2021 Blended Threat Workshops Insights

With its ransomware-based scenario, the 2021 Blended Threat Workshop offers a unique enterprise approach to risk management. In our sessions, experts from a variety of functional offices in the higher education community responded to an on-campus ransomware threat with physical repercussions.

To help you and your organization mitigate the threat of a ransomware attack, REN-ISAC has compiled a short list of actionable prevention and response tactics discovered during our 2021 Blended Threat Workshop ransomware-based scenario.

If you would like to participate in one of this year's workshops, please visit our webpage to register for one of our upcoming sessions.

Prevention Best Practices

- Segment networks to limit the spread of ransomware. A single compromise does not trigger the same level of response as one that reaches the departmental or organizational level, so keeping networks separated can turn a would-be major event into something a small IT team can handle.
- Conduct drills regularly to practice responding to a ransomware event. Critical stakeholders from leadership, emergency management, IT, legal, communications, third party cyber vendors, and facilities should be involved in these events to create a practiced, unified organizational response.
- Build (or update) a product inventory of all assets within the institution. The inventory will help gauge the potential impact of a threat, as well as keep cybersecurity professionals informed on who to alert about specific threats to expedite corrective actions.
- Get involved in information sharing and peer networks. Valuable information—such as IoCs or mitigation practice—can be found on both formal and informal information sharing networks, especially during fast-paced incidents. Getting involved in these networks ahead of time can pay dividends during events.

Response Best Practices

- Decide organizational thresholds for when to pay the ransom ahead of time, whether that is based on level of financial impact, organizational disruption, or a strict policy of non-payment. This is a difficult decision to make in the middle of an incident, so now is the best time to make these decisions.
- Prepare media templates ahead of time so that communications to stakeholders and users during an event is quick, relevant, and accurate. The messages should contain the legally established notification requirements for data breaches. In addition, create an actionable policy for what level of stakeholders need to be informed based on the level of infection discovered. Working with communications professionals ahead of time to create templates and determine the correct audience can greatly help save time during incident response.

For More Information

CISA: Ransomware Guidance and Resources

CISA & FBI Joint Advisory AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks