2021 Blended Threat Workshop Series
Final Findings Report Brief

Ransomware

About the Workshop Series

2020/2021 saw a dramatic increase in blended or complex threats, defined as combined physical and cyber danger that may harm life, information, operations, the environment, and/or property. For the third year, REN-ISAC executed the Blended Threat Workshop Series in accordance with our mission to strengthen the higher education community's ability to respond to these threats. The 2021 series consisted of seven interactive sessions in Australia, Canada, and across the U.S. that enabled security professionals from a multitude of disciplines to confront a hypothetical threat and brainstorm strategic, policy-oriented responses.

The 2021 program utilized a threat-informed and peer-approved scenario based on a hypothetical ransomware attack that caused follow-on physical impacts on campus facilities and services. By focusing on ransomware, participants gained proficiency in responding to blended threats while confronting a specific cyber threat that campuses have faced, are facing, or will soon face. Walking through this scenario allowed participants to experience the difference stages of a major ransomware incident and learn to effectively cooperate with peers across multiple security-related fields.

About this Document

To benefit the broader higher education community, REN-ISAC produced the 2021 REN-ISAC Blended Threat Workshop Series Final Report (read the full report), which contains a complete list of observations made over the course of the series. This document, the Final Findings Report Brief, is a high-level overview that provides the top five best practices revealed during the workshop series.

This document is **TLP:WHITE**, and we encourage you to share these findings with colleagues, supervisors, and administration at your institution.

Suggested Best Practices

1. **Utilizing REN-ISAC as a Cyber Information Broker During Incidents**
   Timely information sharing is the most powerful way to help other organizations; however, when currently responding to an incident, organizations usually do not have time to manage that and their incident response. They can save time and assist the higher ed sector by offloading this responsibility to the REN-ISAC, who will coordinate with public and private security partners in the Education and Facilities CI Subsector to distribute IOCs and other critical threat intelligence. Anyone intending to use REN-ISAC in this manner will be in full control of their information, including organizational anonymity, Traffic Light Protocol (TLP) level, the partners (government, private sector, other ISACs) the information is to be shared, and any other chosen requirements. Contact REN-ISAC Technical Operations for more information.

2. **Preserving Secure, Reliable Backups**
   Backups are one of the best mitigations against ransomware infections. An effective backup process enables security leaders to identify where backups are stored, how often those backups are executed, how they are protected from intrusion or infection, and how long it takes to recover from backups. Stakeholders, especially those in lead positions, should be fully educated on the organization's backup policies and their implications to incident recovery. This not only helps decision-making during an incident but also creates an opportunity for the IT team to receive necessary resources.

3. **Taking Advantage of Templates**
   Having an Incident Response Plan (IRP) is key to managing a ransomware (or other security) incident efficiently and effectively. Building a comprehensive IRP from scratch requires a lot of time and effort; however, using existing IRP templates can expedite this process. Organizations without an IRP should start with a pre-existing template as their initial policy. The template can then be tweaked to fit the details of any organization and rapidly made into policy. As it is used in exercises or incidents, the template-based IRP can easily be customized fit the needs of all stakeholders. See the full report for a list of possible templates.

4. **Using the Incident Command System**
   The National Incident Management System (NIMS) Incident Command System (ICS) (developed by FEMA) is a framework for incident response utilized by law enforcement, paramedics, fire fighters, and other first responders. Private and public sector organizations have adopted NIMS ICS because it creates a common language among responders. To align with the standard, organizations should have mandatory NIMS ICS training for incident response decision makers, and they should assess current plans and processes for NIMS ICS compatibility. Since NIMS ICS is a macro-scale methodology for responding to incidents, this alignment would be more beneficial for general plans, rather than incident-specific playbooks.

5. **Controlling IOT Proactively**
   Internet of Things (IOT) devices are known for lack of security, whether by design or by use. Proactive IOT control through asset inventories and collaborative relationships with other IOT-related teams helps mitigate the multiple points of vulnerability inherent in IOT devices. IT personnel should cultivate relationships with other teams that deploy or maintain IOT devices, especially facilities management. Regular meetings allow increased flow of information, help to provide context, maintain asset inventories, and alert managers of potential incidents.

Want More Information?

For a full list of best practices, as well as areas of improvement and challenges noted by workshop participants, consult the 2021 REN-ISAC Blended Threat Workshop Series Final Report.

Interested in hosting or participating in one of our future Blended Threat Workshops? Contact Sarah Bigham at sarah@ren-isac.net.