2021 REN-ISAC Blended Threat Workshop Series

Final Findings Report

October 27, 2021

FOREWORD

On behalf of the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), thank you for taking the time to read this report. More importantly, thanks to everyone who contributed to the success of the 2021 REN-ISAC Blended Threat Resilience Workshop Series, including our hosts, our planning teams, our REN-ISAC staff, our colleagues at Gate 15, and our participants.

The 2021 Blended Threat Workshop Final Findings Report is full of actionable information that you can apply at your organization. The report is also evidence of how the REN-ISAC community can continue to learn from each other and how to turn our collectively generated ideas into innovative ways to protect, defend, and respond efficiently and effectively.

This year's workshop series was different from previous years. As with all other aspects of our lives, the COVID-19 pandemic impacted the workshops. We took a long pause during the early planning to confirm the educational necessity the workshops provide and to evaluate, with our Gate 15 partners, virtual delivery options. The virtual offerings allowed us to blast out the traditional borders of space and region, making the workshops available to many more participants.

We decided on the topic of ransomware early and never varied from it. By the time we started planning, it was clear that ransomware was a beast (and not in a good way) that wasn't going away. That certainly played out in 2021 as we saw institution after institution victimized. Some news media are now declaring ransomware attacks as inevitable. Discussions on how to lessen the impact and what to do during a ransomware attack are necessary. I was inspired to see the workshop participants take full advantage of the workshop opportunity to ask hard questions and learn from each other. Allowing individuals and organizations to deeply analyze and discuss a significant, stress-inducing—sometimes even catastrophic—ransomware event helped to prioritize guiding principles, articulate processes, and even develop preventative controls.

As we continue to offer education and workshops to and with the REN-ISAC community, we take the information articulated in this report as opportunities for change, inspiration for additional offerings, and suggestions for improving services. The REN-ISAC staff (including me) get so motivated when we hear participants say "Couldn't the REN-ISAC…" or "What if the REN-ISAC…" during workshops and educational events. It inspires us to try new things and to keep our service mission close to our hearts.

Best regards,

Kim Milford, Executive Director

REN-ISAC

Executive Summary

This Final Findings Report compiles observations from all seven workshops of the multi-national 2021 REN-ISAC Blended Threat Workshop Series. Representatives from approximately 322 higher education institutions and 39 other organizations attended the workshop.

We would like to thank the institutions that hosted individual workshops. The following report provides an overview of the series' discussion. The scenario was developed over the course of four modules, each providing situation updates that led to a facilitated discussion. This report presents participants' observations from these discussions as Best Practices, Areas of Improvement, and Challenges. All participant comments have been anonymized.

Appendices provide the 2021 workshop schedule, acronyms, the full text of the scenario's modules and questions, Core Capabilities linked to each observation, and references and resources.

Hosts

REN-ISAC would like to thank the following organizations that generously volunteered to host the 2021 Blended Threat Workshop Series. REN-ISAC would like to especially acknowledge Jon Garvin, Jill Kowalchuk, Rich Nagle, Dave Robinson, Greg Sawyer, Theresa Semmens, and Lisa Zerkle for the effort they put into making these events as successful as they were. Without their help, this report would not have been possible.

CAUDIT
Council of Australasian University Directors of Information Technology

JOHNS HOPKINS UNIVERSITY

CANSSOC

Grinnell College

THE OHIO STATE UNIVERSITY

PURDUE UNIVERSITY FORT WAYNE

NEVADA SYSTEM OF HIGHER EDUCATION

CANADA'S National Research & Education Network

BLENDED THREAT WORKSHOP SERIES OVERVIEW

Series Background

Definition: Workshop

The HSEEP definition is an informal discussion "employed to build specific products, such as a draft plan or policy."

The REN-ISAC Blended Threat Workshop Series began in 2018 out of a desire to improve the Education Facilities Critical Infrastructure (CI) Subsector's[1] capability to respond to threats with both cyber and physical components. These threats, whether they are labeled blended, complex, or some variation, are increasing in number and scope as network devices continue to be integrated into the life of the everyday citizen. REN-ISAC established the Blended Threat Workshop Series to create opportunities for ISAC members and other higher education professionals across a wide range of disciplines to confront threat-informed, risk-based scenarios in order to improve their institutions' security posture before any major incidents occur.

Definition: Blended Threat

The Wikipedia definition is a natural, accidental, or purposeful physical or cyber danger that has or indicates the potential for crossover implications to harm life, information, operations, the environment, and/or property.

Following the format of prior years' series, the 2021 Blended Threat Workshop Series presented seven workshops containing a scenario with a ransomware-based threat to Internet of Things (IOT) devices commonly used on college campuses. Due to the complexities created by the COVID-19 pandemic, all 2021 workshops were virtual, a first for the series. At each event, participants interacted with each other through plenary sessions and breakout rooms. The sessions were organized into four modules that helped focus discussion, while still allowing attendees to speak to the broader topic of cyber and physical threats. REN-ISAC collected data from these events to produce two types of reports: seven **TLP:AMBER** individual reports summarizing the conversation for each workshop and this final **TLP:WHITE** comprehensive report that looks across all seven workshops to pull out actionable strategies and tactics.

Definition: Complex Threat

Two or more separate attacks aimed at the same general or specific target or objective

The observations from this workshop are divided into three categories:

- **Best Practices** – Processes, procedures, or other observations identified as valuable or effective.
- **Areas of Improvement** – Opportunities for the sector to enhance its security posture.
- **Challenges** – Inherent issues that, in today's threat environment, are unable to be eliminated but may be mitigated.

[1] DHS CISA: The Education Facilities Subsector covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. The subsector includes facilities that are owned by both government and private sector entities.

In order to inform future emergency preparedness efforts stemming from this report, each observation is tied to the appropriate Core Capabilities, as identified in the Federal Emergency Management Agency's (FEMA's) National Preparedness Goal. Core Capabilities for each observation can be found in Appendix D.

Purpose and Design

Scope

The following is the scope of the 2021 Blended Threat Workshop Series as approved by the 2021 Blended Threat Workshop Series planning team:

- *In CY2020/2021, REN-ISAC will lead the development and conduct seven security-focused discussion-based exercises, anticipated to be workshop events. These exercises are anticipated to be conducted virtually between Sep 2020 – June 2021 and to be approximately six-hours each. Exercise participants are expected to include institutions' leadership personnel, physical and cybersecurity, emergency management, information technology (IT), administration, student affairs, and other key personnel, leaders and / or staff from REN-ISAC and other higher education institutions, as well as other partners and subject matter experts, as may be appropriate.*

Objectives

The following are the objectives of the 2021 Blended Threat Workshop Series as approved by the 2021 Blended Threat Workshop Series planning team:

1. *Provide a forum for Higher Education organizations to use a complex or blended ransomware threat scenario to prompt discussion and share approaches from leaders in the community regarding physical and cybersecurity preparedness, coordination, and response (these exercises will not focus on recovery) to help inform organizational preparedness.*
2. *Provide participants an opportunity to interact with one another and discuss issues, concerns, best practices, and other salient points to help inform organizational preparedness.*
3. *Provide feedback to members and the broader higher education community on best practices, preparedness gaps, and opportunities for improvement identified through the exercise series to help inform organizational and community security preparedness.*
4. *REN-ISAC will provide participants and their organizations a summary of the discussion within 90 days of exercise completion to help inform organizational preparedness.*
5. *REN-ISAC will provide participants and their organizations a roll-up summary of the complete 2021 exercise series no later than 90 days after completion of the exercise series in order to help inform organizational preparedness.*

Scenario

In 2020, the 2021 Blended Threat Workshop Series planning team was formed from the following REN-ISAC stakeholders: Kim Milford, Todd Herring, Andy Jabbour, Joe Potchanant, Amy Starzynski Coddens, Damian Wilk, Sarah Bigham, Brett Zupan, Al Arboleda, Keith Barros,

Jon Garvin, Donald King, Tim Krabec, Rich Nagle, James Offer, Dave Robinson, Theresa Semmens, and Lisa Zerkle.

This team developed a four module scenario focused on a ransomware threat to a generic university with a subsequent IOT-based threat to campus devices. At the beginning of each module, a situation update from "Gotham University" was presented to participants. Facilitator-led discussion in a plenary session guided attendees through questions established by the planning team, as well as any comments, concerns, or other issues raised during the natural flow of conversation. Module Three contained additional breakout discussions that were reported back out to the plenary session. Module Four had three variants, each representing different IOT threats the planning team felt were plausible and topical. Each host chose one variant from the list to present at their event. The following are summaries of the four modules exercised during the 2021 Blended Threat Workshop Series. The full text of the 2021 modules can be found in Appendix C.

Module One: Secret Origin

During this module, participants were informed that a new strain of malware, PuRevil, had been discovered and was targeting non-education sectors. The infection rate of this particular ransomware strain saw significant growth over multiple weeks.

Module Two: Confidential

During this module, participants were informed that PuRevil infections have begun to appear across the higher education community. Institutions that do not pay the ransom would have their data sold online. A subset of institutions was infected with a PuRevil variant that targeted on-campus IOT devices.

Module Three: Speeding Bullets

During this module, participants were informed their institution had been compromised by PuRevil and that the threat actor behind it had already delivered a ransom threat.

Module Four: The Dark Side (Facilities/Housing Variant)

During this module, participants were informed their institution declined to pay the ransom. Because of this, the threat actor behind PuRevil used the malware's capability to compromise IOT devices. The HVAC, lighting systems, and access control systems within student residences are being manipulated to create an uncomfortable living environment.

Module Four: The Dark Side (Remote Learning Variant)

During this module, participants were informed that their institution decided to not pay the ransom. Because of this, the threat actor behind PuRevil used the malware's capability to compromise IOT devices. Faculty, staff, and students connected to the institution's remote learning systems have had devices on their home network infected with PuRevil.

Module Four: The Dark Side (Research Variant)

During this module, participants were informed that their institution decided to not pay the ransom. Because of this, the threat actor behind PuRevil used the malware's capability to compromise IOT devices. Vulnerable devices within research labs are being manipulated to damage equipment and sabotage research data.

OBSERVATIONS

Best Practices

Definition

Procedures, processes, or other observations identified as valuable or effective.

Observations

1. Utilizing REN-ISAC as a Cyber Information Broker During Incidents

During the workshops, REN-ISAC observed that there was an opportunity for institutions who are being consumed by incident response activity to use the ISAC as an information broker. When initially responding to an incident, many institutions do not think about dedicating resources towards information sharing, as those resources are prioritized towards putting out the biggest fires; however, timely information sharing is the most powerful way to help other members in information sharing communities. One participant noted the benefit of being able to offload information sharing onto REN-ISAC; the institution can save time and focus on direct incident response while knowing the information is being shared and used to assist other organizations.

REN-ISAC already consistently monitors threats to the Education Facilities CI Subsector in coordination with multiple public and private security partners. This puts REN-ISAC in a unique position where they can take on the burden of distributing IOCs and other critical threat intelligence from institutions suffering severe impacts to these partners. Anyone intending to use REN-ISAC in this manner will be in full control of their information. This includes the Traffic Light Protocol (TLP) level at which the information is shared, which partners (government, private sector, other ISACs) the information is allowed to be shared, whether or not the contributing organization is anonymous, and any other requirement the information provider wants to set. Once those decisions have been made, REN-ISAC staff can take on the burden of coordinating with those partners to get the information out to other organizations that could use it to proactively defend their own networks.

2. Preserving Secure, Reliable Backups

Backups are commonly cited as a mitigation against ransomware infections, but multiple participants discussed that it is necessary to establish a truly effective backup process. The first set of variables involves the backup process itself. Security leaders should be able to identify where backups are stored, how often those backups are executed, and the methods used to protect backups from intrusion or infection. Backups do not work if, in the process of infiltrating the network to plant ransomware, the threat actors are present long enough to also compromise the backup system.

The second set of variables involves educating and informing stakeholders, especially leaders, about the backup process. With the current international focus on ransomware, institutional leaders should be fully educated on the elements of the organization’s backup policies and the implications they pose on recovering from an incident. This not only helps decision making

during an incident but also, as one participant noted, creates an opportunity for the IT team to receive resources to help fill any gaps. Another piece of information critical for ransomware response is knowing the average time it takes to recover from backups or to rebuild compromised systems. This metric is critical when determining the impact of a successful ransomware attack and whether or not the institution should pay.

3. Taking Advantage of Templates

REN-ISAC observed that multiple workshop participants utilized the events as a way to jumpstart the creation of their institutions' Incident Response Plan (IRP) or ransomware-specific plan. It can be a difficult task to build a comprehensive IRP from start to finish with no assistance, and those participants found the workshops to be a source of inspiration and ideas that could serve as a potential foundation. Many participants shared existing templates they had discovered (see Appendix D) while researching the creation of a departmental or institutional plan.

Discussed at multiple workshops, a critical piece of advice for these participants was that institutions without an IRP should consider duplicating a template from another source to use as their initial policy. To that end, a number of useful resources were shared by participants of the workshops. This document, whether from a peer institution providing a copy of their plan or a sample document created by experts, can be tweaked to fit the details of any organization and rapidly enshrined as policy. As the institution becomes used to the plan through exercises or incidents, it can become more customized to the needs of all stakeholders. The benefit of this approach is that there is no delay; the institution has an existing document and can begin working on continually updating the plan based on resource availability and real-world needs. This is in contrast to an institution that spends a lot of resources to make an initial plan from scratch in hopes it will perfectly fit the institution but, in reality, will still require continuous updates based on the lessons learned from exercises and actual incidents.

4. Preplanning the Decision of Paying the Ransom

Workshop participants were at different stages of the policy conversation when it came to deciding whether to pay and, if so, how to pay or not pay the ransom when their institution was eventually infected with ransomware. Some institutions had no guidelines, some institutions had set guidelines, and some institutions were in the process of building guidelines. Setting a policy for when to pay a ransom is a difficult topic, especially since there is the potential for damage if criminal actors or the media are able to access that policy. However, it is important for institutional stakeholders, especially leaders, to have put effort into planning if and how to pay a ransom when an incident occurs. It is not a decision any leadership team wants to be suddenly confronted with during an incident event.

One participant offered a best practice at their institution: establishing a clearly defined group of roles that have the responsibility to decide whether or not to pay the ransom for any piece of malware on the university's network, whether it is a single professor's computer or large numbers of machines. The participant's institution chose the CISO, CIO, CFO, Provost, and Chief Legal Officer as the stakeholders for their group; however, the makeup of this group could vary. The key consideration here is to include the leaders who understand the current impact of any ransomware infection and possess the capability to facilitate a payment if necessary. A side

benefit of creating this decision-making body is that it does not commit the institution to either paying or not paying, while still proactively assigning responsibility for how to handle that aspect of a ransomware incident.

5. Using the Incident Command System

The use of the National Incident Management System (NIMS) Incident Command System (ICS) was a topic at multiple workshops. Multiple participating organizations used it as the framework to organize their incident response activities. The NIMS ICS is a nationally recognized process developed by FEMA and utilized by law enforcement, paramedics, fire fighters, and other first responders that have to confront complex natural disasters or incidents. It is designed with interoperability in mind, so that all responders are working off a common language. Other public and private sector organizations have adopted it as their own incident management processes for that reason.

There are many free resources available for individuals and organizations who want to become certified with NIMS ICS. FEMA offers a suite of online classes that can help professionals get up to speed on the foundational concepts of the ICS process. Institutions should consider identifying critical incident response decision makers and make the training mandatory for those roles, though any stakeholder involved would find the information useful. Furthermore, current plans and processes should be examined for their compatibility with NIMS ICS and, if it makes sense, aligned to better fit with the system. 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.

6. Maintaining an Exercise Program

Across all workshops, it was agreed: the act of training and exercising existing plans and procedures is the only way to truly be ready for an event. Having a plan on file does not confer experience on how to execute it or familiarity with how it works under real world conditions. An organization will gain a benefit from their plans only through dedicating resources, time, and the attention of its leaders. Institutional muscle memory for incident response is built through practice and multiple participants noted that this muscle memory can be more important than the plan itself, as it allows staff to be flexible and know their role even if a situation does not fit the plan or becomes unpredictable.

There is no secret to consistent training and improvement; it is simply a function of what is invested into the exercise program. Effort has to be spent to create useful training scenarios, time has to be set aside to get key stakeholders together for long discussions, and a champion is needed to keep the process moving between exercises. Thankfully, exercise programs are something that easily scale and an institution can start small before expanding outwards. Regular workshops are an easy beginning goal since they use short, informal discussions to brainstorm approaches to different types of incidents that could target an institution. From there, an organization can work up to more formal workshops and, eventually, to a tabletop exercise where a fully developed plan is tested against a rigorous scenario. When ready, organizations can move from discussion-based exercises towards more challenging operational testing, including drills, functional and full-scale exercises.

7. Preparing to Determine the Value of Compromised Devices

When looking at the question of paying the ransom from an economic perspective, it is a comparison of the cost of the ransom versus the cost of downtime for all infected devices. However, multiple workshop participants noted that accurately calculating the cost and providing that to leaders in a timely manner requires resources. This capability should be prepared and practiced ahead of an incident, so organizations can avoid the pitfall of improvising such critical numbers while also battling the pressure tactics of the criminal actors who have their data.

Determining an accurate cost of ransomware-related downtime requires understanding what data the ransomers have in their possession, the relative value and priority of all assets within the organization, and the amount of time it would take for the IT team to restore the network. Generating these numbers is difficult and requires investing in initiatives (such as business impact studies focused on network infrastructure and system owners) or internal drills to determine the average time it takes to restore from backups. These are resource-intensive and take time to integrate, but leaders will benefit from a much deeper understanding of their organization's networks and the consequences of any incidents targeting it.

8. Controlling IOT Proactively

One best practice offered by cybersecurity leaders focusing on IOT device management within their organization was to engage in proactive IOT control through asset inventories and creating and maintaining relationships with other IOT-related teams in the institution. IOT devices are particularly insecure. Not knowing what is being connected to the network or who is doing it creates multiple points of vulnerability a network defender has to manage. The best way to gain this awareness is to coordinate with all IOT stakeholders.

Creating and maintaining proactive IOT control requires a multi-pronged approach. Multiple IT participants cultivated a relationship with other teams in charge of deploying or maintaining IOT devices, especially with facilities management personnel. Many of these participants had regular meetings with their counterparts, some even attending the other team's weekly meetings. This allowed for the informal flow of information, which helped to provide context or alert managers of potential incidents before they became an issue. These relationships assisted with maintaining more robust asset inventories. While cataloging all devices connected to the network is an eternal challenge, building relationships and educating peers helped IT leaders get support from other teams for processes that recorded when new IOT devices were procured and added to the network.

9. Prioritizing Threats

Many participants shared the methods they utilized to prioritize threats to their institution's networks on a daily basis, and there were a few common themes that were observed across all workshops. Smaller IT shops, due to a lack of resources, tended to use third parties to signpost pressing issues. Alerts from government organizations like CISA, information sharing organizations like REN-ISAC, and similar partners were triggers for those teams to abandon steady state operations to examine the potential threat. Larger shops were able to handle the vulnerability management side of operations, but only the largest were able to dedicate full-time

resources to threat hunting. Teams of every size utilized personal connections built with peers at other institutions to further prioritize the multitude of threats faced by cyber defenders every day.

Another consideration when it came to threat prioritization is redundancy. For most teams, threat hunting, if done at all, is only one component of team members' daily duties. Participants discussed the different methods they used to share that burden. In terms of redundancy, the best results were noted to come from assigning multiple staff members to the job part time, each using a personalized collection of intelligence sources. In terms of uniformity, the best results were noted to come from assigning one or two staff members to the job in a more permanent role, producing a regular threat intelligence product. Either way, IT leaders noted the importance of staff members being able to communicate and coordinate with each other horizontally in order to quickly disseminate threats and their priority.

Areas of Improvement

Definition

Opportunities for the sector to enhance its security posture.

Observations

1. Confronting the Difficulty of Timely Emergency Procurement

As one participant noted after their institution underwent a major internal exercise, an organization could potentially ad hoc every other aspect of their incident response process except for procurements. Responding to an incident might require sudden and unusual purchases of specialized equipment and steady state procurement processes are often not capable of achieving this expectation. One participant reported that all emergency procurement requests had to go through their institution's board of trustees, which could be a challenge in the middle of an incident. Emergency procurement is an especially important topic in relation to ransomware attacks, as the best way to ensure the network is free from infections is to replace compromised machines.

Security leaders should think about testing their institution's procurement policies against its incident response policies to see if they are capable of working in tandem. If they are not, then it is critical to bring together the appropriate stakeholders to discuss how procurement should work during emergencies. Consider running a conversational drill to expose areas of concern, such as discussing how to recover from a theoretical ransomware incident that involved a large number of infected devices on the network. Once discovered, these concerns can then be addressed by the group as a whole. This is not a conversation that can be had in the middle of an incident, which makes it a major priority for organizations trying to proactively strengthen their security posture.

2. Misinterpreting Cyber Insurance Requirements

One theme repeated throughout all the workshops was the lack of detail participants had about key elements of their insurance policies' requirements. Many were unaware of when and how their organization's policy would be activated or did not know what the threshold was before leaders would consider involving insurance in an incident. This was largely because insurance policies can be confusing and translating a policy's minutiae into actionable incident response processes is an intensive task. However, not knowing these thresholds can have serious consequences for security practitioners, as the activation of an insurance policy creates significant limitations on the actions incident responders can take during major incidents or otherwise their organization could lose valuable coverage.

Addressing this issue requires integrating the third-party insurance company into internal plans and exercises. Having an insurance representative present while key incident response stakeholders discuss how to approach potential scenarios creates an educational opportunity for those stakeholders to learn how the policy applies to their work. Furthermore, the ability to ask

questions directly creates the opportunity to build a more comprehensive policy that includes expected actions from third parties that are critical to the institution's incident response plans.

Challenges

Definition

Inherent issues that, in today's threat environment, are unable to be eliminated but may be mitigated.

Observations

1. Handling the Limitations of Small IT Teams

While they found the discussion useful, participants from institutions with smaller IT teams noted multiple restraints their size imposed on their ability to protect the network. These limits hindered putting into place large-scale network changes, developing a formal and up-to-date incident response plan, and maintaining awareness of the network. The last item was especially difficult for smaller teams since, as one professional noted, they can be responsible for a number of endpoints on campuses the size of a medium city. The consequence of this is increased difficulty in maintaining advanced capabilities and in dedicating resources to longer term planning.

This is an inherent challenge that resource constrained organizations face across the country and the world. Deliberate and informed prioritization can help mitigate some of the downsides of a smaller team, but constraints still exist. When it comes to planning and preparation, it is important to inform institutional leadership of these constraints in order to create a more nuanced understanding of how the team can assist during incidents.

2. Resisting the Lack of IOT Controls

Many participants were concerned by the challenge the campus environment posed to their ability to maintain control over risk-prone IOT devices. Bring Your Own Device (BYOD) is a common policy across most universities and the default for any student who comes on campus. In addition, many departments have the tendency to contribute to shadow IT when they procure internet-connected equipment to supplement operations or research without notifying the main IT team. This leads to an environment where IOT enabled devices are connected to the network without the proper security controls being applied to them, and the IT team has no awareness of this state of affairs until those devices have been impacted. Furthermore, depending on organizational policies, IT or cybersecurity teams may not have the authority to secure IOT devices, making it difficult to apply security controls even if they are aware of the insecure devices.

Definition: Shadow IT

The CISCO definition is "the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization."

Lack of control over IOT devices isn't limited to higher education and is a common challenge across critical infrastructure, though the Education Facilities CI Subsector does face unique issues due to its campus environment. Educating staff and faculty can help them understand the importance of and their role in reducing the number of unknown devices on the network. Tracking student IOT devices will remain an inherent issue because many students both live and learn on

campus, inherent privacy concerns, and a general lack of responsibility as students learn to become more independent.

3. Facing Legal Hurdles to Sharing Information

When discussing why institutions may not be able to share threat intelligence in a timely manner, a common refrain was the existence of legal roadblocks. Multiple cybersecurity professionals cited concerns that their legal team would require a lengthy period to confirm the release of details that could be helpful for a sector-wide response due to the inherent sensitivity of significant cybersecurity incidents. Furthermore, at some institutions, there was widespread confusion as to the extent of the information sharing agreements signed with third parties like REN-ISAC. Due to this lack of understanding of the legal protection given to data shared with these partners, leaders would default to the least risky option.

This challenge is inherent to the role and function of the legal team. Their job is to protect the organization from legal risk, which mandates a cautious approach. However, security stakeholders should utilize existing resources (see Appendix D for relevant CISA and FS-ISAC reports) and focus on educating their coworkers about the risks and threats they face in an effort to build understanding about the critical importance of and legal protections surrounding information sharing. These efforts can help build partnerships that allow for the timely sharing of threat information with reduced legal risk to the institution.

4. Failing to Share Timely Post-Incident Information

Security professionals are always looking for new ways to improve their organization's security posture and one of the most useful sources of best practices and lessons learned are After Action Reports (AARs, sometimes referred to as post-mortems) and similar documents or presentations explaining how other organizations have handled prior real world incidents. However, the creation of AARs is not traditionally prioritized by institutions recovering from events and these products are often restricted for internal use only. The public sharing of AAR results is relatively rare. This hurts the Education Facilities CI Subsector's ability to improve itself through the use of collective experience.

The challenge is that many emergency management teams may not be thinking about AARs when responding to a major incident, and rightfully so. Their priority is to respond and remediate the issue. But when it comes time to consider recovery, the creation of an AAR should begin sooner than one would anticipate. Leaders should consider rapidly crafting an AAR for internal use and consider preparing a version that can be distributed either publicly or within large, trusted communities. It does require time for all departments to approve the product, and the danger of an extended AAR process is that some intelligence and mitigations have shelf lives. If it takes a year to produce a public AAR, that information could potentially be six or nine months out of date, and a window to help others avoid some of the same challenges – especially in fast moving cyberattacks – may be missed. If complete AARs are not feasible, preliminary reports, or partial reports, may provide some actionable lessons learned or key considerations, which can be of value to peer organizations while a more robust and approved AAR is developed. Workshop participants also noted that there are reputational benefits to engaging in publicly releasing timely AARs as an institution can gain a favorable reputation as an organization that publicly provides proven best practices to the higher education community as a whole.

CONCLUSION

The pandemic that developed in 2020 led to significant operational changes across higher education, as well as both new threats and new opportunities. The REN-ISAC Blended Threat Workshop Series was postponed as the situation developed, but with the valued partners listed in this report, planning continued with a renewed focus on exercises in 2021.

The Blended Threat Workshop Series successfully achieved its stated objectives in 2021 and promoted valuable dialogue among participants across seven workshops. The exercises highlighted a number of valuable findings, shared in both the individual event reports and this Final Findings Report that captures the Best Practices, Areas of Improvement, and Challenges identified throughout the entire series.

Beginning with the kickoff workshop hosted by CAUDIT in February 2021 and concluding with the final workshop hosted by Grinnell College four months later, REN-ISAC, planning partners, hosts, and participants from around the world conducted meaningful discussions addressing an enduring threat: ransomware. Ransomware took on new levels of attention in 2021 as multiple incidents caused serious disruptions worldwide, including a number that impacted the Education Facilities CI Subsector.

REN-ISAC would like to thank all of our host organizations (See Appendix A) and all who participated in the workshops and shared their abundant experiences and valuable perspective. This international, crowdsourced report has been developed as a companion to the individual workshop reports which, taken together, are intended to inform and bolster the higher education community's collective security, preparedness, and resilience.

APPENDIX A: 2021 WORKSHOP SCHEDULE

Institution	Date	Module Four Variant
Council of Australasian University Directors of Information Technology (CAUDIT)	February 22nd & 23rd	Remote Learning
Johns Hopkins Bloomberg School of Public Health	April 20th	Facilities/Housing
Canadian Shared Security Operations Centre (CanSSOC)/Canada's NREN	Mary 3rd & 4th	Research
Ohio State University	May 18th & May 19th	Research
Purdue University Fort Wayne	June 9th & 10th	Research
Nevada System of Higher Education (NSHE)	June 16th & 17th	Research
Grinnell College	June 21st	Research

APPENDIX B: ACRONYMS

AAR	After Action Report
BYOD	Bring Your Own Device
CanSSOC	Canadian Shared Security Operations Centre
CAUDIT	Council of Australasian University Directors of Information Technology
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CI	Critical Infrastructure
CIO	Chief Information Officer
CISA	U.S. Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
FBI	U.S. Federal Bureau of Investigation
FEMA	U.S. Federal Emergency Management Agency
FS-ISAC	Financial Services ISAC
HHS	U.S. Department of Health and Human Services
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Incident Command System
IOC	Indicator of Compromise
IOT	Internet of Things
IRP	Incident Response Plan
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MS-ISAC	Multi-State ISAC
NIMS	National Incident Management System
NIST	U.S. National Institute of Standards and Technology
NREN	National Research and Education Network
NSHE	Nevada System of Higher Education
REN-ISAC	Research and Education Networks ISAC
TLP	Traffic Light Protocol

APPENDIX C: 2021 SCENARIO AND QUESTIONS

Note: [T] is used as a substitute value for the date the workshop occurred. All dates in each module are based around [T].

Note: This appendix contains the final version of the scenario, refined after execution at multiple workshops.

Module One: Secret Origin

Scenario

It is [T – 16 Weeks], and Gotham University staff have learned of a new piece of ransomware being used by criminal threat actors. Named PuRevil by the researchers who discovered it, the ransomware has garnered some media attention outlining the ransomware's capabilities. According to reports, the ransomware largely targets the Commercial Facilities Sector (buildings, venues, hotels, etc.). While it uses some novel code, it appears that PuRevil is only involved in a small percentage of infections compared to other well-known ransomware strains.

However, on [T – 12 Weeks], the coverage on PuRevil has changed as new infections are being observed at a significantly higher rate. The media is reporting that actors behind the ransomware seem to have expanded their targets across multiple communities, including large numbers of reported targets in the Critical Manufacturing and Healthcare and Public Health Sectors. One security company's blog notes that PuRevil has been modified to more easily contain and load modules that could give it new capabilities.

Questions

1. How does your organization's IT team learn about and keep track of threats on a daily basis? How do your organization's other teams learn about and keep track of threats?
2. How does your organization prioritize threats? Are there processes in place? Which departments are involved in those processes?
3. At this point, would the IT team anticipate taking any actions regarding this threat, and if so, what? At this point, would non-IT teams anticipate taking any actions?
4. What should members expect REN-ISAC's level of interest and reporting on this threat to be at this point?

Module Two: Confidential

Scenario

It is [T – 4 Weeks] and staff at Gotham University have learned there are multiple institutions in the higher education community that have been deliberately targeted by PuRevil. While details are still sparse, it appears some universities have paid the ransom. After initially being identified as victims by the PuRevil group, several institutions were subsequently removed from the victim list. The universities that chose not to pay saw their exfiltrated data offered on criminal markets.

Media coverage is largely focusing on a subset of institutions that were infected with a new PuRevil variant that could propagate to IOT devices. The actors behind the ransomware appear to have deliberately targeted on-campus IOT devices, specifically a dorm's HVAC system and the refrigeration and cooling systems in research buildings. No IOCs for PuRevil have been made available through open-source intelligence at this time.

Questions

1. Beyond the media, what other sources would your organization use to determine the scope and nature of this threat? How does your organization's IT and non-IT teams engage in information sharing communities, both formal and informal?
2. What actions would both IT and non-IT security personnel be taking at this time with regard to this threat? What actions would non-security personnel be taking at this time?
3. For cybersecurity professionals, if and when do you begin to reach out to non-cybersecurity peers within the organization about threats? Are there processes in place?
    a. What entities or individuals outside of IT/security would IT think to engage with?
    b. Who today, outside of IT/security thinks they should be contacted at this point, and what would you want to know?
4. Does your organization have policies and plans in place regarding ransomware? Which departments are involved in those plans? How often are those plans exercised during steady state operations?
5. What does REN-ISAC provide to members at this point in the threat's progression? As REN-ISAC members, what do you want from REN-ISAC at this point?

Module Three: Speeding Bullets

Scenario

It is [T] and staff at Gotham University have discovered that desktops and servers connected to their network have been compromised by PuRevil, which has significantly impacted operations at the university. The actors behind PuRevil have already contacted the university with their demands, including the ransom amount and a secure method of contacting them for further instructions. If the university does not pay within a day, they have promised to "use every tool at their disposal to destroy your institution, your students, and your reputation before the eyes of the nation."

Simultaneously, open-source intelligence is reporting commonalities among the higher education institutions suffering from attacks. The organizations were using network devices manufactured by Wayne Enterprises in conjunction with IOT devices manufactured by LexCorp, a combination that Gotham University is utilizing.

Questions

1. Who are the relevant stakeholders for a coordinated response? How would your organization bring them together to respond to this threat?
2. Who needs to be involved within the organization (leadership, student affairs, communications, legal, facilities, etc.) when faced with a ransomware threat?
3. What external entities may be engaged?
    a. Does your organization engage with REN-ISAC or other information sharing entities during this process? If so, when?
    b. Does your organization engage with law enforcement during this process? If so, when? Does that include federal law enforcement or local LE?
    c. When and how, based on your insurance policy, would you engage with your insurance provider?
    d. Are there are any vendors or suppliers that need to be involved in responding or informed of the incident?
4. Does your organization have any standard guidelines or criteria for deciding whether or not to pay a ransom? If possibly paying a ransom, does your organization have processes in place to handle the payment process?
5. How would the legal team be involved with ransom payment negotiation? Do you have any best practices for negotiating with criminals during a ransomware incident?

Module Four: The Dark Side

Scenario (Facilities/Housing Variant)

It is [T + 1 Day] and Gotham University has made the decision NOT to pay a ransom to the criminal actors behind PuRevil. After being informed of this decision, the actors behind the ransomware have moved beyond traditional network devices and activated the malware's capability to compromise IOT devices. The compromised devices appear to be clustered around a certain target, specifically on-campus housing, where HVAC, lighting, and access control systems have been infected. This escalated threat has caused immediate operational impacts, including making student residences uncomfortable to live in by manipulating the HVAC and lighting systems, making any doors installed with access control systems unusable, and even posting livestreams from dorm security cameras to a public site.

On [T + 2 Days], the university has demonstrated its continued unwillingness to pay the ransom; therefore, the ransomware's operators begin selling data from all compromised devices, including IOT devices, on their online portal.

Scenario (Remote Learning Variant)

It is [T + 1 Day] and Gotham University has made the decision NOT to pay a ransom to the criminal actors behind PuRevil. After being informed of this decision, the actors behind the ransomware have moved beyond traditional network devices and activated the malware's capability to compromise IOT devices. The compromised devices appear to be clustered around a certain target, specifically devices connected to students' and teachers' home networks, after the attackers hijacked remote learning platforms to further spread PuRevil. This escalated threat has caused immediate operational impacts, including students and teachers now refusing to participate in remote learning until Gotham University can guarantee the safety of their network and demanding assistance in fixing their own bricked IOT devices.

On [T + 2 Days], the university has demonstrated its continued unwillingness to pay the ransom; therefore, the ransomware's operators begin selling data from all compromised devices, including IOT devices, on their online portal.

Scenario (Research Variant)

It is [T + 1 Day] and Gotham University has made the decision NOT to pay a ransom to the criminal actors behind PuRevil. After being informed of this decision, the actors behind the ransomware have moved beyond traditional network devices and activated the malware's capability to compromise IOT devices. The compromised devices appear to be clustered around a certain target, specifically on-campus research labs where internet-connected laboratory equipment has been infected. This escalated threat has caused immediate operational impacts, including delays in time-sensitive research, the risk of damage to hazardous samples stored in freezers, and the potential compromise of research data.

On [T + 2 Days], the university has demonstrated its continued unwillingness to pay the ransom; therefore, the ransomware's operators begin selling data from all compromised devices, including IOT devices, on their online portal.

Questions (All Variants)

1. What are the immediate concerns of this IOT threat? What stakeholders are necessary to bring together to respond to this threat?
2. Does being informed of the public sale of data change your response?

APPENDIX D: CORE CAPABILITIES

In order to inform future emergency preparedness efforts stemming from this report, each observation is tied to the appropriate Core Capabilities, as identified in FEMA's National Preparedness Goal.

Best Practices

1. Utilizing REN-ISAC as a Cyber Information Broker During Incidents

Core Capabilities: Cybersecurity, Public Information and Warning, Intelligence and Information Sharing, Threats and Hazards Identification, and Situational Assessment

2. Preserving Secure, Reliable Backups

Core Capabilities: Cybersecurity, Planning, Long-term Vulnerability Reduction, and Infrastructure Systems

3. Taking Advantage of Templates

Core Capabilities: Cybersecurity, Planning, Operational Coordination, Operational Communications, and Risk Management for Protection Programs and Activities

4. Preplanning the Decision of Paying the Ransom

Core Capabilities: Cybersecurity, Planning, and Operational Coordination

5. Using the Incident Command System

Core Capabilities: Cybersecurity, Planning, Operational Coordination, and Operational Communications

6. Maintaining an Exercise Program

Core Capabilities: Cybersecurity, Planning, Operational Coordination, Operational Communications, and Risk Management for Protection Programs and Activities

7. Preparing to Determine the Value of Compromised Devices

Core Capabilities: Cybersecurity, Planning, and Risk and Disaster Resilience Assessment

8. Controlling IOT Proactively

Core Capabilities: Cybersecurity, Access Control and Identity Verification, Risk and Disaster Resilience Assessment, and Long-term Vulnerability Reduction,

9. Prioritizing Threats

Core Capabilities: Cybersecurity, Risk Management for Protection Programs and Activities, and Threats and Hazards Identification

Areas of Improvement

1. Confronting the Difficulty of Timely Emergency Procurement

Core Capabilities: Cybersecurity, Planning, and Operational Coordination

2. Misinterpreting Cyber Insurance Requirements

Core Capabilities: Cybersecurity, Operational Coordination, Situational Assessment, and Operational Communications

Challenges

1. Handling the Limitations of Small IT Teams

Core Capabilities: Cybersecurity, Risk Management for Protection Programs and Activities, Risk and Disaster Resilience Assessment, and Long-term Vulnerability Reduction

2. Resisting the Lack of IOT Controls

Core Capabilities: Cybersecurity, Access Control and Identity Verification, Risk and Disaster Resilience Assessment, and Long-term Vulnerability Reduction,

3. Facing Legal Hurdles to Sharing Information

Core Capabilities: Cybersecurity, Public Information and Warning, Intelligence and Information Sharing, Threats and Hazards Identification, and Situational Assessment

4. Failing to Share Timely Post-Incident Information

Core Capabilities: Cybersecurity, Planning, and Intelligence and Information Sharing

APPENDIX E: REFERENCES AND RESOURCES

Note: This Appendix is built from resources shared freely by participants in all seven workshops.

Information Sharing Standards

U.S. CISA – Traffic Light Protocol (TLP) Definitions and Usage

REN-ISAC – Information Sharing Policy

Resources – Public Sector

The White House - Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger, September 2, 2021

U.S. DHS – All Product Subscriptions

U.S. DHS – Fusion Center Locations and Contact Information

U.S. DHS – Campus Resilience Program (including Exercise Starter Kits)

U.S. FEMA – NIMS

U.S. FEMA – NIMS Training

U.S. CISA – National Cyber Awareness System Alerts

U.S. CISA – Automated Indicator Sharing (AIS) Documentation

U.S. CISA – Privacy and Civil Liberties Guidelines under the Cybersecurity Information Sharing Act of 2015

U.S. CISA – Business Case for Security

U.S. CISA – Stop Ransomware Resource Page

U.S. CISA – Rising Ransomware Threat to Operational Technology Assets Fact Sheet

U.S. CISA/MS-ISAC – Ransomware Guide

U.S. FBI – InfraGard

U.S. HHS Office for Civil Rights – Security Listserv

U.S. NIST – SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

U.S. Treasury - Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

Federal Asset Reporting Contacts

- U.S. CISA – Regional Protective Security Advisors
- U.S. CISA – Incident Reporting Forms

U.S. FBI – Field Offices

U.S. Secret Service – Field Offices

MS-ISAC Security Operations Center – soc@msisac.org

Australian Cyber Security Centre – Ransomware in Australia

CERT NZ – Ransomware

Quebec Secrétariat du Conseil du Trésor – Normative Framework for the Management of Information Resources (French)

U.K. National Cyber Security Centre - Ransomware: What board members should know and what they should be asking their technical experts

Resources – Private Sector – Templates, Playbooks, and Charts

EDUCAUSE/National Student Clearinghouse – Incident Response Playbooks

Counteractive Security – Incident Response Plan Templates and Playbooks

Adelia Risk – Ransomware Playbook: 31 Critical Questions to Build Your Own

EY – Ransomware: to pay or not to pay? Decision Chart

CERT NZ – How ransomware happens and how to stop it Attack Chart

Resources – Private Sector – Reports and Open Source Intelligence

FS-ISAC – Threat Information Sharing and GDPR: A Lawful Activity that protects Personal Data

Gate 15 – The White House Memo to Industry on Ransomware: Take Action (Now).

Martin Haller – What Does Ransom Negotiation Look Like

Cybereason – Ransomware: The True Cost to Business

DoublePulsar – The hard truth about ransomware: we aren't prepared, it's a battle with new rules, and it hasn't near reached peak impact.

SpecterOps – BloodHound versus Ransomware: A Defender's Guide

Reuters – Companies May Be Punished For Paying Ransoms to Sanctioned Hackers

VentureBeat – Cybereason: 80% of Orgs that Paid the Ransom Were Hit Again

Gartner Research – When OT Is Short for Overlooked Technology and Ransomware Becomes Siegeware

Insurance Journal – Insurer AXA to Stop Paying for Ransomware Crime Payments in France

ZDNet – Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again

Twitter Feeds

- Infosec Under 2.5k
- @Sean_Waite
- @Bad_Packets
- @InfoSecSherpa
- @Hacks4pancakes
- @tinkerSec

Security Podcasts

- Down the Security Rabbithole
- Paul's Security Weekly
- Defensive Security Podcast
- SANS Internet Stormcast

Media Sources

- Cyberwire Daily
- Threatpost
- The Hacker News
- Bleeping Computer
- Cyberscoop
- Hackbusters
- Infoblox
- The Intercept
- Krebs on Security
- Risky Business Podcast
- Sans Internet Storm Center Podcast
- Talos
- Wired

Resources – Private Sector – Software and Other

REN-ISAC – Emergency Operations Center listserv (Request access at support@ren-isac.net)

No More Ransom

Security Wizardry – Radar Console

Inverse Inc. – PacketFence

Telekom Security – T-Pot

Emergency Communications Platforms

- Everbridge
- Rave Mobile Safety
- Regroup

Black Hills Information Security/Active Countermeasures - Backdoors & Breaches, an Incident Response Card Game

- Backdoors & Breaches-Shuffle