



CERT



NASSAU COUNTY



Main Office:

516-573-9600

Email:

oemcert@nassaucountyny.gov

**CERT IS
WHAT
YOU
MAKE IT**



**COUNTY,
STATE,
&
FEDERAL
ONE TEAM**

CERT Monthly Newsletter

OCTOBER 2021

Dear Members,

Our thoughts and prayers go out to all the victims, whose lives have been devastated by recent weather events and wildland fires. Also to the first responders, military and volunteers who have been actively assisting in operations.

October is Fire Prevention Month! The goal of Fire Prevention Month is to raise awareness about fire safety and help ensure your home and family is prepared in the event of an emergency. Today, we celebrate Fire Prevention Week and Month by raising fire safety awareness and educating families, students and communities across the United States. During this month, fire departments educate their communities, and encourage parents and loved ones to practice fire safety and whole home safety. The NFPA's 2021 campaign for Fire Safety Month is "Learn The Sounds of Fire Safety." Help protect and keep your home safe today by installing smoke and carbon monoxide alarms, as well as having fire extinguishers at home.

Thank you to all the CERT members who assisted OEM with phone calls from residents reporting damage to their residents from Hurricane Ida. Also, those that assisted with the Long Island Marathon .

*Have a Great October
Stay Safe and Stay Healthy
Bob, Rick & Paul*



October is Fire Prevention Month! The goal of Fire Prevention Month (and week October 3rd – 9th) is to raise fire safety awareness and help ensure your home and family is protected. In 1922, the National Fire Protection Association (NFPA) named the second week of October Fire Prevention Week in commemoration of the Great Chicago Fire in 1871. Today, we celebrate Fire Prevention Week and Month by raising fire safety awareness and educating families, students and communities across the United States. During this month, fire departments provide education to their communities, and encourage parents and loved ones to practice fire prevention and whole home safety.

Did You Know?

Fire Prevention week is the perfect time to educate and talk with your whole family about fire safety – include testing alarms, changing the batteries or upgrading to 10-year sealed battery alarms, how to use a fire extinguisher and escape route planning.

- ◆ 3 of every 5 home fire deaths resulted from fires in homes with no working smoke alarms
- ◆ Less than 50% of homeowners have an escape plan
- ◆ Carbon monoxide (CO) is the #1 cause of accidental poisoning in the US
- ◆ 60% of consumers do not test their smoke and CO alarms monthly*
- ◆ Only 47% of people report having CO alarms in their home
- ◆ Just 43% of homeowners have an escape plan*
- ◆ Unattended cooking is the #1 cause of home fires

Help Protect Your Whole Home

We urge you to practice whole home safety, so you and your family are prepared not only during Fire Prevention Week and Month, but throughout the entire year. Having functioning alarms installed throughout your home is the first line of defense for fire prevention. They work around the clock to provide your family an early alert in the event of an emergency, providing you time to safely escape. Smoke and CO alarms should be placed on every level of the home, including the basement, as well as inside and outside each bedroom to keep your home and family safe. Fire extinguishers should also be placed on every level of the home, especially in the kitchen and garage.

Placement of Fire Extinguishers, Smoke Alarms and CO Detectors



Smoke Alarm

One on every level and in every bedroom



Carbon Monoxide Alarm

One on every level and in every bedroom



Fire Extinguisher

One on every level, plus kitchen and garage

Being proficient, familiar and comfortable with fire extinguisher use is important as they are used in times of high stress. Getting together as a family and learning how to use your fire extinguishers correctly can save both lives and property.

Here is a super-easy way to remember how to use a fire extinguisher with the acronym P.A.S.S.

P - Pull the pin

A- Aim the nozzle at the base of the fire

S- Squeeze the trigger

S- Sweep from side to size

Fire Prevention & Safety Checklist

The most effective way to protect yourself and your home from fire is to identify and remove fire hazards. Sixty-five percent of home fire deaths occur in homes with no working smoke alarms. During a home fire, working smoke alarms and a fire escape plan that has been practiced regularly can save lives.

- If a fire occurs in your home, **GET OUT, STAY OUT** and **CALL** for help.
- Install smoke alarms on every level of your home, inside bedrooms and outside sleeping areas. Test them every month and replace the batteries at least once a year.
- Talk with all household members about a fire escape plan and practice the plan twice a year.



Steps You Can Take Now

- Keep items that can catch on fire at least three feet away from anything that gets hot, such as space heaters.
- Never smoke in bed.
- Talk to children regularly about the dangers of fire, matches and lighters and keep them out of reach.
- Turn portable heaters off when you leave the room or go to sleep.

Cooking Safely

- Stay in the kitchen when frying, grilling or broiling food. If you leave the kitchen for even a short period of time, turn off the stove.
- Stay in the home while simmering, baking, roasting or boiling food. Check it regularly and use a timer to remind you that food is cooking.
- Keep anything that can catch fire—like pot holders, towels, plastic and clothing—a way from the stove.
- Keep pets off cooking surfaces and countertops to prevent them from knocking things onto the burner.

Caution: Carbon Monoxide Kills

- Install carbon monoxide alarms in central locations on every level of your home and outside sleeping areas.
- If the carbon monoxide alarm sounds, move quickly to a fresh air location outdoors or by an open window or door.
- Never use a generator, grill, camp stove or other gasoline, propane, natural gas or charcoal-burning devices inside a home, garage, basement, crawlspace or any partially enclosed area.



Smoke Alarms

- Install smoke alarms on every level of your home, inside bedrooms and outside sleeping areas.
- Teach children what smoke alarms sound like and what to do when they hear one.
- Once a month check whether each alarm in the home is working properly by pushing the test button.
- Replace batteries in smoke alarms at least once a year. Immediately install a new battery if an alarm chirps, warning the battery is low.
- Smoke alarms should be replaced every 10 years. Never disable smoke or carbon monoxide alarms.
- Carbon monoxide alarms are not substitutes for smoke alarms. Know the difference between the sound of smoke alarms and carbon monoxide alarms.

Fire Escape Planning

- Ensure that all household members know two ways to escape from every room of your home.
- Make sure everyone knows where to meet outside in case of fire.
- Practice escaping from your home at least twice a year and at different times of the day. Practice waking up to smoke alarms, low crawling and meeting outside. Make sure everyone knows how to call 9-1-1.
- Teach household members to **STOP, DROP** and **ROLL** if their clothes should catch on fire.



Follow Your Escape Plan!

Remember to **GET OUT, STAY OUT** and **CALL 9-1-1** or your local emergency phone number.

- If closed doors or handles are warm, use your second way out. Never open doors that are warm to the touch.
- Crawl low under smoke.
- Go to your outside meeting place and then call for help.
- If smoke, heat or flames block your exit routes, stay in the room with doors closed. Place a wet towel under the door and call the fire department or 9-1-1. Open a window and wave a brightly colored cloth or flashlight to signal for help.

Use Caution with Fire Extinguishers

- Use a portable fire extinguisher **ONLY** if you have been trained by the fire department and in the following conditions:
 - The fire is confined to a small area, and is not growing.
 - The room is not filled with smoke.
 - Everyone has exited the building.
 - The fire department has been called.
- Remember the word **PASS** when using a fire extinguisher.
 - **P**ull the pin and hold the extinguisher with the nozzle pointing a way from you.
 - **A**im low. Point the extinguisher at the base of the fire.
 - **S**queeze the lever slowly and evenly.
 - **S**weep the nozzle from side to side.



For more information on disaster and emergency preparedness, visit RedCross.org.



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



Alert (AA21-243A)

Ransomware Awareness for Holidays and Weekends

Summary

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

Threat Overview

RECENT HOLIDAY TARGETING

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of ransomware, as network defenders and IT support of victim organizations are at limited capacity for an extended time.

- In May 2021, leading into Mother's Day weekend, malicious cyber actors deployed DarkSide ransomware against the IT network of a U.S.-based critical infrastructure entity in the Energy Sector, resulting in a week-long suspension of operations. After DarkSide actors gained access to the victim's network, they deployed ransomware to encrypt victim data and—as a secondary form of extortion—exfiltrated the data before threatening to publish it to further pressure victims into paying the ransom demand.
- In May 2021, over the Memorial Day weekend, a critical infrastructure entity in the Food and Agricultural Sector suffered a Sodinokibi/REvil ransomware attack affecting U.S. and Australian meat production facilities, resulting in a complete production stoppage.
- In July 2021, during the Fourth of July holiday weekend, Sodinokibi/REvil ransomware actors attacked a U.S.-based critical infrastructure entity in the IT Sector and implementations of their remote monitoring and management tool, affecting hundreds of organizations—including multiple managed service providers and their customers.

RANSOMWARE TRENDS

The FBI's Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for reporting information on cyber incidents, received 791,790 complaints for all types of internet crime—a record number—from the American public in 2020, with reported losses exceeding \$4.1 billion. This represents a 69 percent increase in total complaints from 2019. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020, representing a 20 percent increase in the number of incidents, and a 225 percent increase in ransom demands. From January to July 31, 2021, the IC3 has received 2,084 ransomware complaints with over \$16.8M in losses, a 62 percent increase in reporting and 20 percent increase in reported losses compared to the same time frame in 2020.¹ The following ransomware variants have been the most frequently reported to FBI in attacks over the last month.

- Conti
- PYSA
- LockBit
- RansomEXX/Defray777
- Zeppelin
- Crysis/Dharma/Phobos

The destructive impact of ransomware continues to evolve beyond encryption of IT assets. Cyber criminals have increasingly targeted large, lucrative organizations and providers of critical services with the expectation of higher value ransoms and increased likelihood of payments. Cyber criminals have also increasingly coupled initial encryption of data with a secondary form of extortion, in which they threaten to publicly name affected victims and release sensitive or proprietary data exfiltrated before encryption, to further encourage payment of ransom. (See CISA's Fact Sheet: [Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches](#).) Malicious actors have also added tactics, such as encrypting or deleting system backups—making restoration and recovery more difficult or infeasible for impacted organizations.

Although cyber criminals use a variety of techniques to infect victims with ransomware, the two most prevalent initial access vectors are phishing and brute forcing unsecured remote desktop protocol (RDP) endpoints. Additional common means of initial infection include deployment of precursor or dropper malware; exploitation of software or operating system vulnerabilities; exploitation of managed service providers with access to customer networks; and the use of valid, stolen credentials, such as those purchased on the dark web. Precursor malware enables cyber actors to conduct reconnaissance on victim networks, steal credentials, escalate privileges, exfiltrate information, move laterally on the victim network, and obfuscate command-and-control communications. Cyber actors use this access to:

- Evaluate a victim's ability to pay a ransom.
- Evaluate a victim's incentive to pay a ransom to:
 - Regain access to their data and/or
 - Avoid having their sensitive or proprietary data publicly leaked.
 - Gather information for follow-on attacks before deploying ransomware on the victim network.

Threat Hunting

The FBI and CISA suggest organizations engage in preemptive threat hunting on their networks. Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack. Threat actors can be present on a victim network long before they lock down a system, alerting the victim of the ransomware attack. Threat actors often search through a network to find and compromise the most critical or lucrative assets. Many will exfiltrate large amounts of data. Threat hunting encompasses the following elements of understanding the environment by developing a baseline through a behavior-based analytics approach, evaluating data logs, and installing automated alerting systems.

- **Understand the IT environment’s routine activity and architecture by establishing a baseline.** By implementing a behavior-based analytics approach, an organization can better assess user, endpoint, and network activity patterns. This can help an organization remain alert on deviations from normal activity and detect anomalies. Understanding who logs in to the network—and from what location—can assist in identifying anomalies. Understanding the baseline environment—including the normal internal and external traffic—can also help in detecting anomalies. Suspicious traffic is usually the first indicators of a network incident but cannot be detected without establishing a baseline for the environment.
 - **Review data logs.** Understand what standard performance looks like in comparison to suspicious or anomalous activity. Things to look for include:
 - Numerous failed file modifications,
 - Increased CPU and disk activity,
 - Inability to access certain files, and
 - Unusual network communications.
 - **Employ intrusion prevention systems and automated security alerting systems**—such as security information and event management software, intrusion detection systems, and endpoint detection and response.
 - **Deploy honeypots** and alert on their usage to detect lateral movement.

Indicators of suspicious activity that threat hunters should look for include:

- Unusual inbound and outbound network traffic,
- Compromise of administrator privileges or escalation of the permissions on an account,
- Theft of login and password credentials,
- Substantial increase in database read volume,
- Geographical irregularities in access and log in patterns,
- Attempted user activity during anomalous logon times,
- Attempts to access folders on a server that are not linked to the HTML within the pages of the web server, and
- Baseline deviations in the type of outbound encrypted traffic since advanced persistent threat actors frequently use encryption for communication.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on [Technical Guidance to Uncovering and Remediating Malicious Activity](#) for additional guidance on hunting or investigating a network, and common mistakes in incident handling. Also review the Ransomware Response Checklist in the CISA-MS-ISAC [Joint Ransomware Response Guide](#).

CYBER HYGIENE SERVICES

CISA offers a range of no-cost [cyber hygiene services](#)—including vulnerability scanning and ransomware readiness assessments—to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attacks.

Ransomware Best Practices

The FBI and CISA strongly discourage paying a ransom to criminal actors. Payment does not guarantee files will be recovered, nor does it ensure protection from future breaches. Payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of malware, and/or fund illicit activities. Regardless of whether you or your organization decide to pay the ransom, the FBI and CISA urge you to report ransomware incidents to [CISA](#), a [local FBI field office](#), or by [filing a report with IC3](#) at [IC3.gov](#). Doing so provides the U.S. Government with critical information needed to help victims, track ransomware attackers, hold attackers accountable under U.S. law, and share information to prevent future attacks.

INFORMATION REQUESTED

Upon receiving an incident report, the FBI or CISA may seek forensic artifacts, to the extent that affected entities determine such information can be legally shared, including:

- Recovered executable file(s),
- Live memory (RAM) capture,
- Images of infected systems,
- Malware samples, and
- Ransom note.

Recommended Mitigations

The FBI and CISA highly recommend organizations continuously and actively monitor for ransomware threats over the network. Additionally, the FBI and CISA recommend identifying IT security employees to be available and "on call" in the event of a ransomware attack. The FBI and CISA also suggest applying the following network best practices to help reduce the risk of compromise.

MAKE AN OFFLINE BACKUP OF YOUR DATA.

- Make and maintain offline, encrypted backups of data and regularly test your backups. Backup procedures should be performed on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find accessible backups.

REVIEW YOUR ORGANIZATION'S BACKUP SCHEDULE TO TAKE INTO ACCOUNT THE RISK OF DATA LOSS AND DISRUPTION TO BACKUP PROCESSES DURING WEEKENDS OR HOLIDAYS.

DO NOT CLICK ON SUSPICIOUS LINKS.

IMPLEMENT A USER TRAINING PROGRAM AND PHISHING EXERCISES TO RAISE AWARENESS OF THE RISKS INVOLVED IN VISITING MALICIOUS WEBSITES OR OPENING MALICIOUS ATTACHMENTS AND TO REINFORCE THE APPROPRIATE USER RESPONSE TO PHISHING AND SPEARPHISHING.

IF YOU USE RDP—OR OTHER POTENTIALLY RISKY SERVICES—SECURE AND MONITOR ACCESS.

- Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA. If RDP must be used, it should be authenticated via VPN.
- Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts, log RDP login attempts, and disable unused remote access/RDP ports.
- Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB to prevent propagation of malware across organizations.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement listing policies for applications and remote access that only allow systems to execute known and approved applications under an established security policy.
- Open document readers in protected viewing modes to help prevent active content from running.

UPDATE YOUR OS AND SOFTWARE; SCAN FOR VULNERABILITIES.

- Upgrade software and operating systems that are no longer supported by vendors to currently supported versions. Regularly patch and update software to the latest available versions. Prioritize timely patching of internet-facing devices—as well as software processing internet data, such as web browsers, browser plugins, and document readers—known vulnerabilities. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which network assets and zones should participate in the patch management program.

- Automatically update antivirus and anti-malware solutions and conduct regular virus and malware scans.

CONDUCT REGULAR VULNERABILITY SCANNING TO IDENTIFY AND ADDRESS VULNERABILITIES, ESPECIALLY THOSE ON INTERNET-FACING DEVICES. (SEE THE CYBER HYGIENE SERVICES SECTION ABOVE FOR MORE INFORMATION ON CISA'S FREE SERVICES.)

USE STRONG PASSWORDS.

ENSURE STRONG PASSWORDS AND CHALLENGE RESPONSES. PASSWORDS SHOULD NOT BE REUSED ACROSS MULTIPLE ACCOUNTS OR STORED ON THE SYSTEM WHERE AN ADVERSARY MAY HAVE ACCESS.

USE MULTI-FACTOR AUTHENTICATION.

REQUIRE MULTI-FACTOR AUTHENTICATION (MFA) FOR ALL SERVICES TO THE EXTENT POSSIBLE, PARTICULARLY FOR REMOTE ACCESS, VIRTUAL PRIVATE NETWORKS, AND ACCOUNTS THAT ACCESS CRITICAL SYSTEMS.

SECURE YOUR NETWORK(S): IMPLEMENT SEGMENTATION, FILTER TRAFFIC, AND SCAN PORTS.

- Implement network segmentation with multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL blocklists and/or allowlists.
- Scan network for open and listening ports and close those that are unnecessary.

FOR COMPANIES WITH EMPLOYEES WORKING REMOTELY, SECURE HOME NETWORKS—INCLUDING COMPUTING, ENTERTAINMENT, AND INTERNET OF THINGS DEVICES—TO PREVENT A CYBERATTACK; USE SEPARATE DEVICES FOR SEPARATE ACTIVITIES; AND DO NOT EXCHANGE HOME AND WORK CONTENT.

HAVE AN INCIDENT RESPONSE PLAN.

- Create, maintain, and exercise a basic cyber incident response plan that:
 - Includes procedures for response and notification in a ransomware incident and
 - Plans for the possibility of critical systems being inaccessible for a period of time.
 -



Radio Amateur Civil Emergency Services

(RACES)

RACES / CERT Comms Group SITREP

October 2021



RACES is now holding meetings on the first Thursday of the month.

The next meeting is Thursday, October 7.

This will also be a Zoom meeting for all those who do not feel comfortable attending an in person meeting



Anyone wishing to attend can Join from any computer, tablet, or smartphone by entering:

<https://zoom.us/j/95928146234> in your browser.

Or, for audio only, you may dial by phone: 646-876-9923 and enter Meeting ID: 959 2814 6234 #

Any questions you can contact us at nassaucountyny.races@gmail.com

October 2021





Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4	5	6	7 RACES Meeting 7:30pm	8	9
10		12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
						

Important CERT Dates

RACES Meeting

October 7
Time: 7:30 pm
TBD

November 2021

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1		3	4 RACES Meeting 7:30pm	5	6
	8	9	10		12	13
14	15	16	17	18	19	20
21	22	23	24		26	27
	29	30				

Important CERT Dates

RACES Meeting

November 4
 Time: 7:30 pm
 TBD



Nassau County CERT Coordinator

Bob Chiz & Rick Delucia

oemcert@nassaucountyny.gov

Division 1

Division Supervisor

Bill Pavone

nassaucertdiv1@yahoo.com

CERT Deputy Director

Paul Shapiro

pshapiro@nassaucountyny.gov

Division 2

Division Supervisor

Marvin Stein

certdiv2nassau@gmail.com

