COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

IN THE MATTER OF:

ELECTRONICAPPLICATION OF ROWAN WATER,	**)**	
INC. FOR AN ALTERNATIVE RATE ADJUSTMENT	**)**	
AND AN INVESTIGATION INTO ROWAN WATER	**)**	**CASE NO.**
INC. AND ITS INDIVIDUAL DIRECTORS, LARRY	**)**	**2022-00252**
JOHNSON, DANNY STEVENS, DANNY COX,	**)**	
MIKE COLLINS, ENOCH BLAIR, AND ITS	**)**	
MANAGER, JERRY PATRICK, FOR ALLEGEDLY	**)**	
FAILING TO COMPLY WITH KRS 278.300 AND	**)**	
A COMMISSION ORDER	**)**	

NOTICE OF ATTENDING WATER TRAINING

Comes now Rowan Water, Inc. ("Rowan Water"), by and through counsel, and notifies the Commission that Rowan Water's general manager and each of board members attended the Commission approved training on August 14, 2025 for a total of 1 hour. A filing was made in Case No. 2025-00133 for proof of attendance on August 30, 2025, and is attached as Exhibit 1 to this notice. This training is required by the Commission's Ordering paragraph 8 of the Commission's October 17, 2023 Order in this proceeding. This additional hour was approved and was attended by each of the board members and the general manager.

Dated this 30th day of August 2025.

Respectfully submitted,

L. Allyson Honaker
Heather S. Temple
Meredith L. Cave
HONAKER LAW OFFICE, PLLC
1795 Alysheba Way, Suite 1203
Lexington, Kentucky 40509
(859) 368-8803
allyson@hloky.com
heather@hloky.com
meredith@hloky.com

Counsel for Rowan Water, Inc.

CERTIFICATE OF SERVICE

This is to certify that foregoing was submitted electronically to the Commission on August 30, 2025 and that there are no parties that have been excused from electronic filing. Pursuant to prior Commission orders, no paper copies of this filing will be submitted.

Counsel for Rowan Water, Inc.

EXHIBIT 1

COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

IN THE MATTER OF:

ELECTRONICAPPLICATION OF ROWAN WATER, INC. FOR APPROVAL OF WATER TRAINING	**)** **)**	**CASE NO. 2025-00133**

NOTICE OF FILING

Comes now Rowan Water, Inc., its individual directors and its general manager (collectively, "Rowan Water"), and Honaker Law Office, PLLC ("Joint Applicants") to give notice of the filing of the following documents:

1. A sworn statement attending that the second and final installment of the accredited instruction entitled "**Rowan Water 2025 Training"** was performed on August 14, 2025 (Exhibit 1).
2. A copy of the presentation on cyber securiy provided to the attendees is attached as Exhibit 2.
3. The name of each attending water utility Commissioner, Director, and Manager and the number of hours that they attended is attached as Exhibit 3.
4. Attendees appeared in person.
5. The only written materials provided to the attendees were copies of the agenda.

Dated this 30th day of August, 2025.

Respectfully submitted,

Meredith Cave

L. Allyson Honaker
Heather S. Temple
Meredith L. Cave
HONAKER LAW OFFICE, PLLC
1795 Alysheba Way, Suite 1203
Lexington, Kentucky 40509
(859) 368-8803
allyson@hloky.com
heather@hloky.com
meredith@hloky.com

Counsel for Rowan Water, Inc.

CERTIFICATE OF SERVICE

This is to certify that foregoing was submitted electronically to the Commission on August 30, 2025 and that there are no parties that have been excused from electronic filing. Pursuant prior Commission orders, no paper copies of this filing will be submitted.

Counsel for Rowan Water, Inc.

Exhibit 1

COMMONWEALTH OF KENTUCKY)
)
COUNTY OF FAYETTE)

AFFIDAVIT

L. Allyson Honaker of Honaker Law Office, PLLC, Counsel for Rowan Water, Inc., being duly sworn, states that:

1. She has served as organizer and presenter of the water training program entitled "**Rowan Water 2025 Training"** in the above-referenced case.

2. The second and final installment of "**Rowan Water 2025 Training"** was held on August 14, 2025, at the offices of Rowan County Water Association, 1765 Christy Creek Road, Morehead, Kentucky 40351.

3. The presentation on cyber security listed in the proposed agenda submitted to the Kentucky Public Service Commission in this matter was conducted for the length of time specified, a total of 1 hour of instruction.

4. Each attendee was provided in paper medium a copy of the agenda and the presentation was provided in electronic form.

L. Allyson Honker
HONAKER LAW OFFICE, PLLC
1795 Alysheba Way, Suite 1203
Lexington, Kentucky 40509
(859) 489-4667
allyson@hloky.com

The foregoing Verification was signed, acknowledged and sworn to before me this 20th day of August 2025, by L. Allyson Honaker of Honaker Law Office, PLLC, Counsel for Rowan Water, Inc..

Heather S. Temple

Notary Commission No. KYNP98715

Commission expiration: April 9 20229

Exhibit 2

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Critical Infrastructure Protection

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CISA Regions

I	Boston, MA
II	New York, NY
III	Philadelphia, PA
IV	Atlanta, GA
V	Chicago, IL
VI	Irving, TX
VII	Kansas City, MO
VIII	Lakewood, CO
IX	Oakland, CA
X	Seattle, WA
CS	Pensacola, FL

Joe Parker
October 22, 2024

Protective Security Advisors

- Protective Security Advisors have five mission areas that directly support the protection of critical infrastructure:
  - Plan, coordinate, and conduct security surveys and assessments
  - Plan and conduct outreach activities
  - Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
    - World Games, 60th Anniversary of “Bloody Sunday”, Mardi Gras, Rock the South, NASCAR 500
  - Respond to incidents, provide a vital link for information sharing in steady state and incident response
  - Coordinate and support improvised explosive device awareness and risk mitigation training

CISA Priorities- Target Rich/ Cyber Poor

Healthcare - K-12 Schools - Water/Wastewater

Water-Wastewater Sector Toolkit

- Water and Wastewater Cybersecurity | CISA
  - Specific Alerts and Advisories for Water/Wastewater Sector
  - EPA Resources
  - **Incident Response Guide**
  - Funding Resources
  - CISA Live Events on Water/Wastewater

CYBER THREATS

Cyber Threats of Today

Business Email Compromise

- 2 Billion in Loss
- Credential Stealing
- Phishing/ PopUps/ Poison Domains/ Onsite Exchange Vulnerabilities
- Steals Data
- Finance Diversions
- SupplyChain/External Dependencies Exploitation

Ransomware

- 700K per Victim
- Ransomware-As-A-Service Brokers – Gootloader
- Phishing-As-A-Service – Greatness (M365 exploitations)
- Lockbit, Blackcat, Blacksuit, AlphV, Conti, Darkside
- Russian and North Korea State Actors
- Steals and Encrypts Data
- Double Extortion
- Destructive Malware Trends- Russia
  - Hermeticwiper and Wispergate

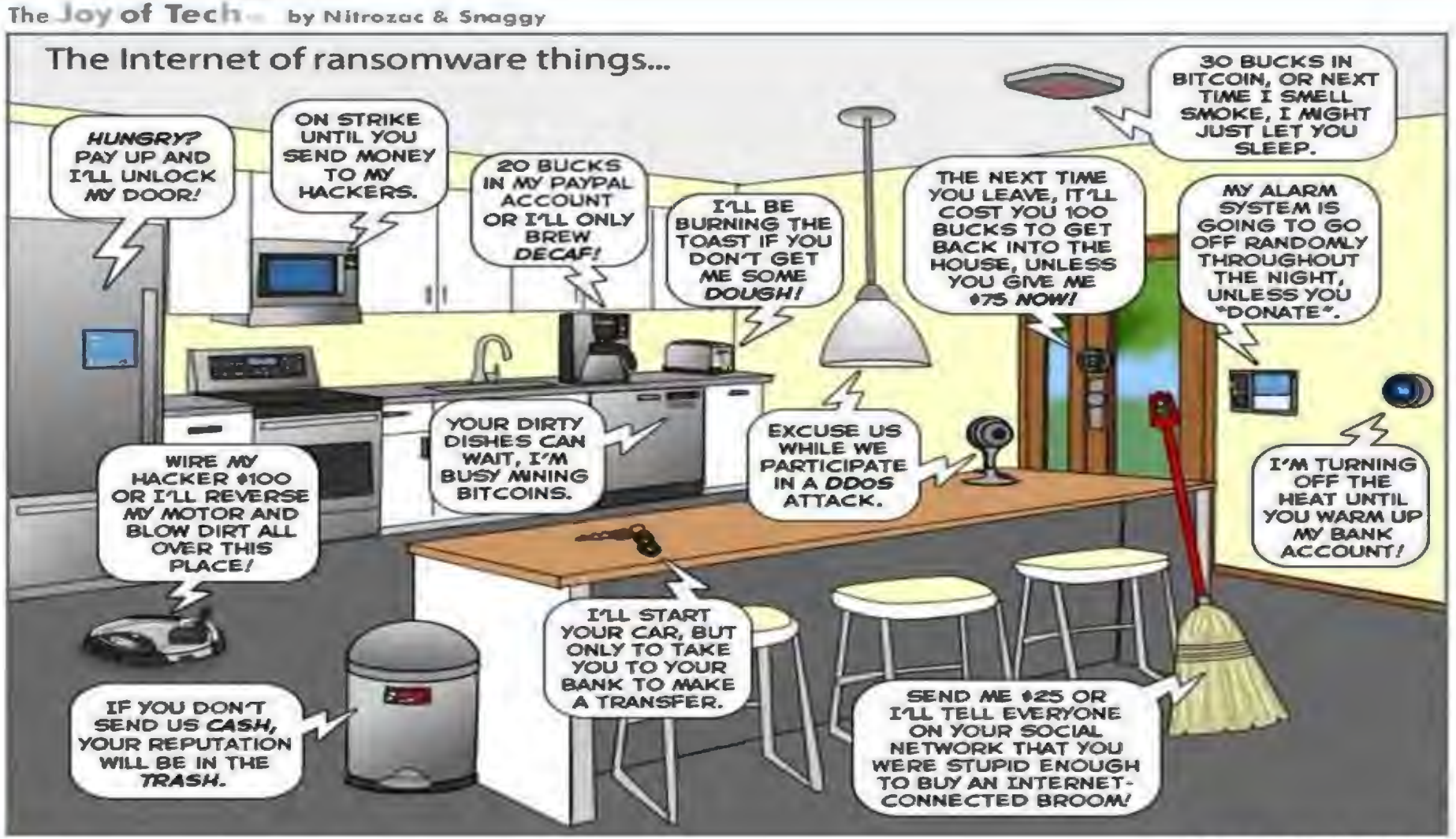
Denial of Service

- Russian-affiliated KILLNet Group
  - Feb 2023 Coordinated DDoS of Healthcare
- Dark Storm and Anonymous Sudan
  - Russian-Affiliated
  - Aug 2023 and March 2024 Threats to CI

Common Defensive Measures

- Multifactor Authentication (MFA)
- Backups- Off Network
- Vulnerability Management – Patching
- Configuration Management - RDP, SMB, etc
- Log Management and Review

Ransomware: Infects…Encrypts…Extorts



#Stop Ransomware - Resources

Stop Ransomware | CISA

Events of interest

- **Ransomware**
  - Social engineering- phishing and malware
    - Gootloader- asset management important
  - Ransomware notifications via phone calls and voicemails
  - Encrypted a network via an IP Camera
- **Hactivists**
  - Cyber Av3ngers targeting Unitronics PLCs and default passwords
  - Pro-Russian targeting HMIs via VNC protocol over default port 5900
- **Volt Typhoon**
  - People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

ICS/OT Threat – CyberAv3ngers

- IRGC-Affiliated Cyber Actor
- Exploited PLCs in Multiple U.S. Critical Infrastructure Sectors (Nov-Dec 2023)
  - Water/Wastewater, Health, Food, Energy, Manufacturing
  - **Water/Wastewater primary target with 60 percent of activity**
- Targeted Israeli-made Unitronics Vision Series PLCs/ Human-Machine-Interfaces (HMI)
  - However, likely pivot to other venders
- Most exploitations took advantage of ***"Default" passwords (1111)*** and direct
  - **exposure to the internet.**
- Group used destructive wiper malware in past

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities | CISA

Pro-Russian Hacktivist Targeting

- Defending OT Operations Against Ongoing Pro-Russian Threats
- Joint Advisory Published May 2024
- Pro-Russian hacktivist groups ongoing activity against US and Europe
- Targeting Operational Technology (OT)/ ICS in Critical Infrastructure
- Primary Targets: Water/Wastewater, Dams, Energy, Food and Agriculture
- **Exploitations of internet-exposed ICS through their software components, such as human machine interfaces (HMIs), virtual network computing (VNC) remote access software, and PLCs.**
- Leveraging default passwords; weak passwords; lack of multi-factor

Pro-Russian Hacktivist Targeting cont..

- **Physical disruptions** from attacker remotely manipulating HMIs.
- Caused water pumps and blower equipment to exceed their normal operating parameters.
- Maxed out set points, altered other settings (Ladder Diagram Logic), turned off alarm mechanisms, and changed administrative passwords to lock out the WWS operators.
- Some victims experienced minor tank overflow events; however, most victims **reverted to manual controls** in the immediate aftermath and quickly restored operations.

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Published 13 Dec 24

Threat actors can exploit exposed HMIs at WWS Sector utilities to view the contents of the HMI, make unauthorized changes, and potentially disrupt the facility's water and/or wastewater treatment process.

In the absence of cybersecurity controls, unauthorized users can exploit exposed HMIs in Water and Wastewater Systems to:

- **View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings) and**
- **Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process.**

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems | CISA

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

In 2024, pro-Russia hacktivists manipulated HMIs at Water and Wastewater Systems, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts at water systems and forced victims to revert to manual operations.

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Mitigations

- Conduct an inventory of all internet-exposed devices.
- If possible, disconnect HMIs and all other accessible and unprotected systems from the public-facing internet.
- If it is not possible to disconnect the device, secure it by creating a username and strong password to prevent a threat actor from easily viewing and accessing the devices. Change factory default passwords.
- Implement a strong password and multifactor authentication (MFA) for all access to the HMI and OT network.
- Implement network segmentation by enabling a demilitarized zone (DMZ) or a bastion host at the OT network boundary.
- Implement geo-fencing across the entire network and enforce network segmentation based on specific locations.

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Mitigations

- Keep all systems and software up to date with patches and necessary security updates.
- Establish an allowlist that permits only authorized IP addresses to access the devices.
- Log remote logins to HMIs; be aware of failed attempts and unusual times.
- Implement your vendor's recommendations for best securing your product.
- Sign up for CISA's free cybersecurity vulnerability scanning service to identify software vulnerabilities and confirm that patching is up to date and done correctly.

Volt Typhoon

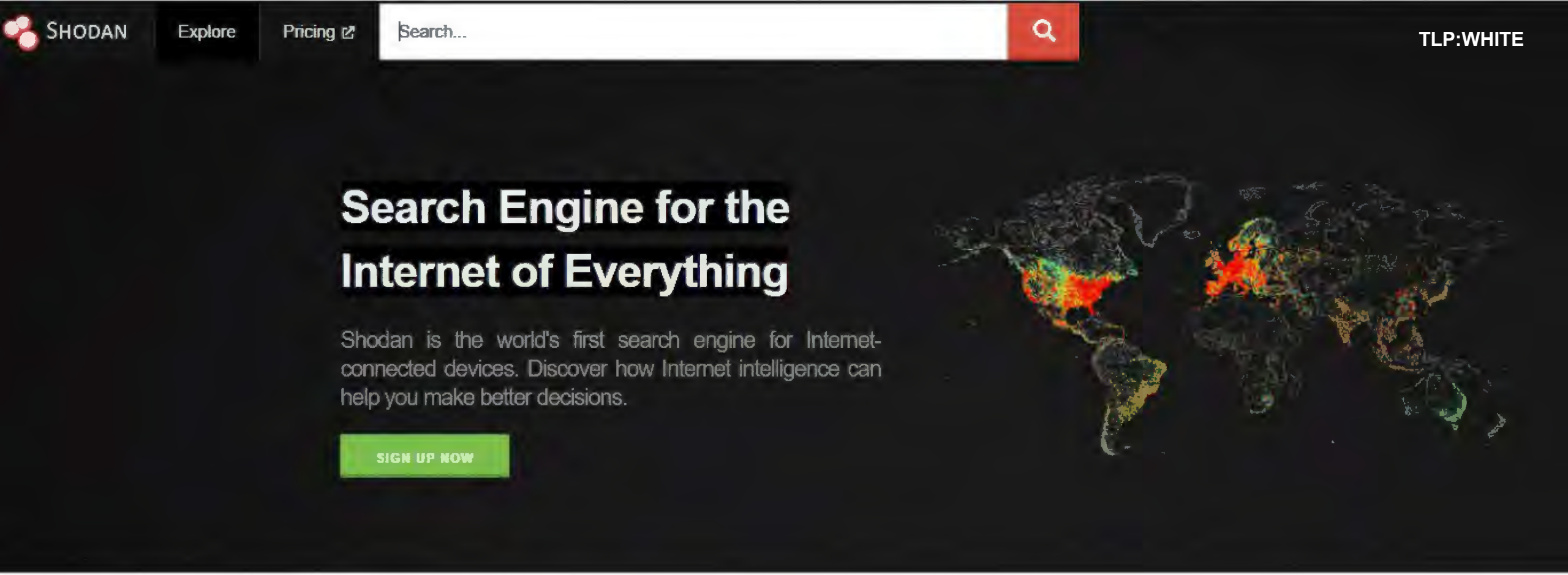
- Chinese state-sponsored threat actor using stealth techniques and targeted malicious activity aimed at critical infrastructure organizations in the United States
- Observed behavior suggests that the threat actor goal to maintain access without being detected for as long as possible
- Volt Typhoon pursues capabilities to **disrupt critical infrastructure during future crises**
- Affected Sectors Include:
  - Communications
  - Manufacturing
  - Utility
  - Construction
  - Maritime
  - Government
  - Education
  - Transportation
  - Information technology

CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance | CISA
Volt Typhoon: Hiding in Plain Sight - Critical Start
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

Living Off the Land (LOTL)

- Sophisticated cyberattack technique that leverages legitimate tools **already present within a victim's system** to execute and sustain an attack
  - Bypasses traditional signature-based defenses (Behavioral Vs. Signature Analysis is key)
  - Windows Management Instrumentation
  - **PowerShell**
  - **Scheduled Tasks Actions**
  - **C2- Home User Networks**
  - FTP, SMB, and SSH
  - Log Deletion (Event 1102)

Living Off the Land (LOTL): The Invisible Cyber Threat Lurking in Your System (socradar.io)



Shodan (www.shodan.io) is a web-based search platform for Internet connected devices. This tool can be used not only to identify Internet connected computers and Internet of Things/Industrial Internet of Things (IoT/IIoT), but also Internet connected Industrial Control Systems (ICS) and platforms.

RDP Search-KY

SHODAN Explore Downloads Pricing | state:ky port:3389

TOTAL RESULTS

512

TOP ORGANIZATIONS

Charter Communications Inc	170
AT&T Enterprises, LLC	47
CINCINNATI BELL	25
Private Customer - AT&T Internet S...	16
AT&T Services, Inc.	14

More...

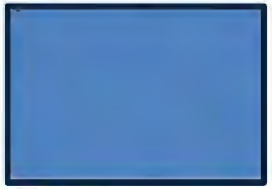
TOP OPERATING SYSTEMS

Windows (build 10.0.19041)	169
Windows 11 (build 10.0.26100)	70
Windows 11 (version 22H2) (build 1...	49
Windows (build 10.0.14393)	41
Windows Server 2022 (build 10.0.20...	41

More...

View Report | Download Results | Historical Trend | Browse Images | View on Map | A

Access Granted: Want to get more out of your existing Shodan account? Check out everything you ha



United States, Elizabethtown

self-signed

SSL Certificate

Issued By:
|- Common Name:
Server2019.monroepva.local

Issued To:
|- Common Name:
Server2019.monroepva.local

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1809)/Windows Server 2019 (version 1
  OS Build: 10.0.17763
  [redacted]
  NetBIOS [redacted]
  NetBIOS Comput...
```

United States, Bowling Green

self-signed

SSL Certificate

Issued By:
|- Common Name:
Igor-PC

Issued To:
|- Common Name:
Igor-PC

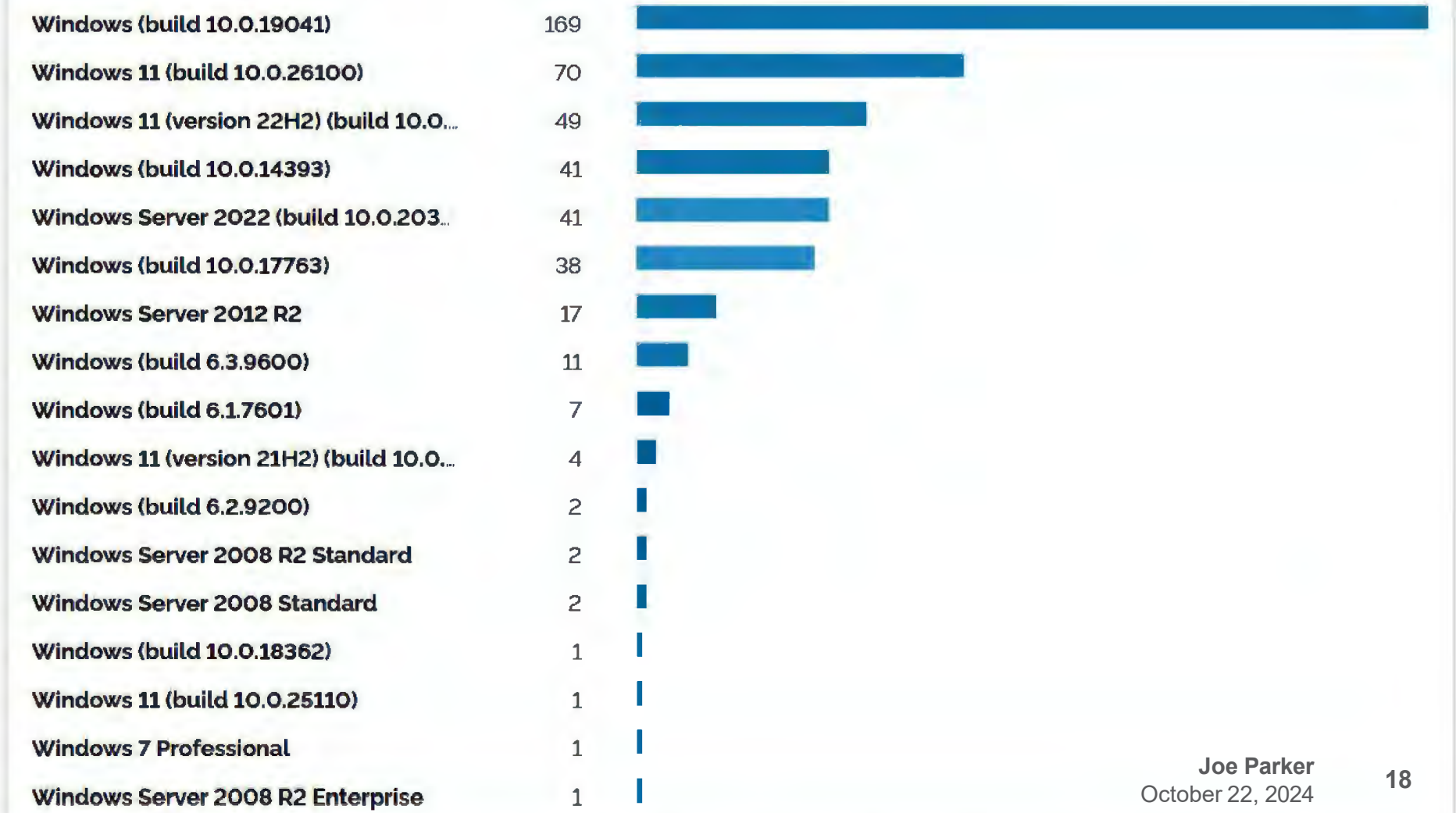
Supported SSL Versions:
TLSv1, TLSv1.1

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 2004)/Windows Server (version 2004)
  OS Build: 10.0.19041
  Target Name: IGOR-PC
  NetBIOS Domain Name: IGOR-PC
  NetBIOS Computer Name: ...
```

RDP Sear

st_te_ky port:3389 | os

// TOTAL: 512



ICS Screenshot Search - Worldwide

SHODAN | Explore | Downloads | Pricing | screenshot.label:ics | Accoun

TOTAL RESULTS

437

TOP COUNTRIES

United States	101
Germany	54
Italy	27
Poland	24
China	21

More...

TOP PORTS

5900	145
80	58
3389	42
5901	15
6590	15

More...

View Report | Download Results | Historical Trend | Browse Images | View on Map | Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

2025-03-06T19:57:48.042761

PLC Search: KY

SHODAN | Explore | Downloads | Pricing | state:ky "allen bradley"

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

TOTAL RESULTS

48

TOP PORTS

44818	46
161	1

TOP ORGANIZATIONS

Wireless Data Service Provider Corporat...	26
AT&T Mobility LLC	10
Charter Communications Inc	3
NORTH CENTRAL TELEPHONE COOPER...	3
Limestone Cable Vision, Inc.	1

More...

TOP PRODUCTS

Rockwell Automation/Allen-Bradley	31
Schweizerische Bankgesellschaft Zuerich	1

[redacted]
Mayfield Electric & Water Systems
United States, Mayfield

ics

```
Product name: 1766-L32BWAA B/15.04
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x4064ffba
Device type: Programmable Logic Controller
Device IP: 192.168.10.199
```

[redacted]
South Central Rural Telecommunications Cooperative Inc.
United States, Horse Cave

ics

```
Product name: 1766-L32AWAA B/13.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x4062325e
Device type: Programmable Logic Controller
Device IP: 192.168.100.50
```

[redacted]
United States, Murray

```
Product name: 1766-L32AWA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60e4d95f
Device type: Programmable Logic Controller
Device IP: 10.5.10.31
```

Specific SCADA Search: KY

TOTAL RESULTS

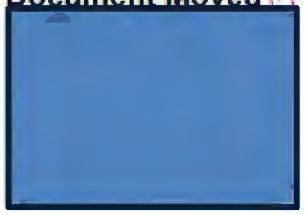
11

TOP ORGANIZATIONS

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

Document Moved



```
HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: [redacted]scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frames-Options: DENY
X-Content-...
```

Document Moved

```
HTTP/1.1 302 Redirect
Content-T[redacted]
Location: [redacted].scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frames-Op...
```

Document Moved

```
HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: [redacted]scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 1; mode=block
```

Open Vulnerabilities

// LAST SEEN: 2025-03-06

General Information

Hostnames	[redacted]
Domains	SPECTRUM.COM
Country	United States
City	Louisville
Organization	Charter Communications Inc
ISP	Charter Communications Inc
ASN	AS10796

Open Ports

22 8080

// 22 / TCP -1169060451 | 2025-03-05T03:10:02.484054

OpenSSH 7.3

```
SSH-2.0-OpenSSH_7.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCooUGO8gCEJ3USWDxpaa/jjEJwX/ayY3ShTvX7HgCodGAz
4n1nz+pdanKNfaDWKwmNDAnruHuyc7paJMCaHHGznxT25NwqJzWentm6+UZHOcdbamjaKn84I/40
EH+vCk4TVb8lIHKexNoY0LMlP7FialPkbh9EkxlKMdWP+r3oOpdQz+q2LIc9sYIBYyYag6f6wFZc
cncH76+HF1IVum0lLsn7G4++8swhVYkc4HwVO5ay4uInAyGLY3iukbjQ5YXdlsyrX7ZWlJiA5GZu
pukwTAs733HEYUH5Z+8A1dRAyuKRtU69niwrX1oKrNejlPtEIay0M7gDVcNpNJH5q+Fz
Fingerprint: 58:3e:96:30:e7:1d:a9:66:ba:f4:1d:d1:2a:19:1e:75

Kex Algorithms:
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
        diffie-hellman-group14-sha1

Server Host Key Algorithms:
        ssh-rsa
        rsa-sha2-512
        rsa-sha2-256
```

Vulnerabilities

Port 22 | CVSS

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

Critical (2)

CVE-2023-38408 — 9.8 The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not

Stuff Off Search

Shodan	Censys	Thingful
Shodan is a web-based search platform for internet connected devices. Key features: • Identify Internet connected devices, Internet of Things/Industrial Internet of Things (IoT/IIoT), and industrial control systems (ICS). • Potential exploits. • Default passwords. • Integrations with vulnerability tools, logging aggregators and ticketing systems allow Shodan to be seamlessly integrated into an enterprise. https://www.shodan.io	Censys is a web-based risk management tool that helps identify publicly accessible assets —even if they can't be scanned by a vulnerability management tool. Key features: • Home network risk identifier (HNRI), allowing employers to anonymously monitor staff's home network infrastructure for vulnerabilities that may pose a risk to the company. • Exposed routers. • Default credentials. • Popular vectors for ransomware. https://www.censys.io	Thingful is a search engine for the Internet of Things (IoT). Key features: • Searchable index of public and private connected objects and sensors around the world. • Monitors IoT networks and infrastructures including energy, radiation, weather, and air quality devices. • Reports seismographs, iBeacons, vehicles, ships, aircraft and animal trackers. The tool assists with response by enabling end users to create watchlists and publications on public/private IoT resources. https://www.thingful.net/

Joe Parker

Web: Stuff Off Search | CISA

Operational Technology (OT) Vulnerabilities

- Building Automation Systems (BAS) BACNet Field Panels (BFP)
  - HVAC Systems Control- elevators, lighting, emergency services, sensors, access control, etc.
- Utility PLCs (programable logic controllers) and Human Machine Interface (HMI)
- Camera Systems
- Specialty Equipment (Vender Maintained)
- Diagnostic Systems - CT, Ultrasound, MRI, Imaging etc.
  - Picture Archiving Communication System (PACS) network
  - Digital Imaging and Communications in Medicine (DICOM) format
- Medical Devices – Infusion pumps, patient monitors

Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA

CISA ICS No-Cost Virtual Training

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

https://www.cisa.gov/ics-training-available-through-cisa

Steps to take to be a bit more secure

SECURE OUR WORLD

Teach Employees to Avoid Phishing

Require Strong Passwords

Require Multifactor Authentication

Update Business Software

Secure Our World | CISA

Phishing

- Phishing - online messages designed to look like they're from a trusted source and/or hijack legitimate accounts intended to lure target to: click a **link**, open an **attachment**, or take an **action**.

- **Common Red Flags:**
  - Urgent/ Emotionally Charged
  - Requests to Send or Change Personal/ Finance Info
  - Unexpected/ Suspicious Attachments (uncommon naming/ file types)
  - Untrusted/Suspicious Links (URL mismatches)
  - Email Addresses Do Not Match Sender
  - Official Emails Originating from Outside Company
  - Too Good To Be True

- Mitigation:
  - Resist and Report
    - Spam – Organization
    - Blocks Current Sender
  - Delete
    - Avoid Unsubscribe Link
      - Could Be Malicious

Password Defense

1 Make them long

At least 16 characters—longer is stronger!

****

2 Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

cXmnZK65rf*&DaaD

Create a memorable passphrase of 5-7 unrelated words:

HorsPerpleHatRunBayconShoos

Get creative with spelling to make it even stronger.

3 Make them unique

Use a different password for each account:

k8dfh8c@Pfv0gB2

LmvF%swVR56s2mW

e246gs%mFs#3tv6

Tip! Use a password manager to remember them.

Multifactor Authentication (MFA)

- MFA (two-factor): Confirms Our Identities.
- Highly Impactful Defense Against Cyber Attacks.
- Enable on EVERY account and Device possible.

Multifactor Authentication

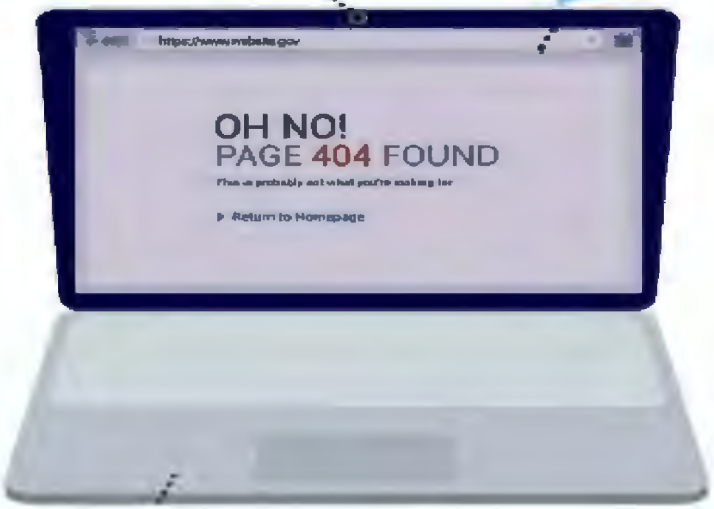
Software Updates

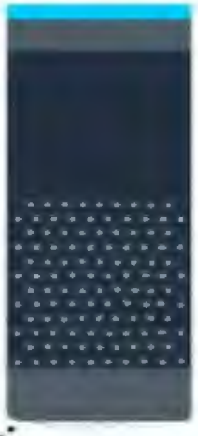
- Install Updates to fix Security Risks.
  - Mobile Phones, Computers/ Tablets, Operating Systems, Software, Web Browsers, Watches, Network and Security Equipment, IoT
- Time is Critical once Vulnerabilities are known.
- Turn on Automatic Updates
- Watch for Notifiers – Not every update can be automatically installed

Home Network Security

Webcam
- Cover cameras when not in use.

Web Browser
- Ensure transit security encryption, usually with a lock icon in the address bar.





External Storage
- Back up data on external drives or portable media.

ISP Router Management
- Change Default Password
- Enable Firewall
- Enable Network Address Translation (NAT

Home Assistance
- Limit nearby sensitive conversations.
- Mute microphones when not in use.

Laptop/Computer
- Utilize a non-privileged "user" account for everyday activities.
- Update with the latest patches, preferably through automatic updates.

Wireless Access Point/Router
- Use WPA3 or WPA2/3 with protected management frames.
- Update with the latest patches, preferably through automatic updates.
- Schedule weekly reboots.

NSA-Best Practices For Securing Your Home Network

Change Default Password - - - Restart Often

Mobile Device Security

- Enable User Authentication (Passcode)
- Install Updates
- Restart Phone Often (Memory Dump)
- Create backups
- Reinstall From backups Occasionally (After Foreign Travel or Loss of Control)
- Only Download Apps from Legitimate Sources
- Limit Remote Sharing
- Limit Public Exposure
  - Change Device Name

CISA Services

Cybersecurity Resources

Partnership Development

- Outreach Activities
- Informational Exchanges (individual, group, etc.)
- Committees and Working Groups support
- Symposiums/ Conferences/ Webinars/ Cyber Camps

Stakeholder Preparedness

- Cybersecurity Workshops
- Technical Exchange
- Introductory Visits and Cyber Protective Visits (CPVs)
- Cyber Exercises support/ *Tabletop Exercises*
- Awareness and Cyber Threat Training/ Briefings

Assessments

- Cybersecurity Performance Goals assessments (CPGs)
- Ransomware Readiness Assessments (RRAs)
- Cyber Resilience Reviews (CRRs)
- External Dependency Management Assessments (EDMs)

Vulnerability Scanning

- Cyber Hygiene Service (Public Attack Surface)
  - Known Exploitable Vulnerabilities (KEV)
- Web Application Scanning
- Penetration Testing

Ransomware Vulnerability Warning Pilot (RVWP)

A new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

- Leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.

  - CISA's Cyber Hygiene Vulnerability Scanning
  - Known threat vectors
  - Administrative Subpoena Authority
  - Homeland Security Act of 2002

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Vulnerability Scanning by CISA (Cyber Hygiene)

Known exploited vulnerabilities are easy access for attackers, with incidents averaging $100,000 in damages for small and medium businesses.

CISA's free vulnerability scanning service helps identify exposed assets and exploitable vulnerabilities and is proven to reduce risk for participating organizations.

Avoid costly disruptions with early detection and action. Through weekly reports and timely alerts, we will help you act before others take advantage.

Auto enrollment with CISA Ransomware Vulnerability Warning

BY THE NUMBERS

- 7,200+ current customers nationwide
- Over 3 Million vulnerabilities found and fixed
- On average a 40% reduction in risk and exposure by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first 90 days

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

Joe Parker
October 22, 2024

Vulnerability Scanning Report

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services

Dashboard Coming Soon

Cyber Performance Goals (CPG)

- A common baseline of cybersecurity practices that **all critical infrastructure entities** should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.
- IT and operational technology (OT) cybersecurity practices that meaningfully reduce the likelihood and impact of known risks and adversary techniques
- Informed by real-world threats and adversary tactics, techniques, and procedures (TTPs)
- Aids in identifying areas for potential future investment

1.A Asset Inventory	ID.AM-1	CURRENT ASSESSMENT

COST: $$$ IMPACT: HIGH COMPLEXITY: MEDIUM

☐ IMPLEMENTED
☐ IN PROGRESS
☐ SCOPED
☐ NOT STARTED

TTP or Risk Addressed

- Hardware Additions (T1200)
- Exploit Public-Facing Application (T0819, ICS T0819)
- Internet Accessible Device (ICS T0883)

Recommended Action

Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

CPG Effectiveness – Cyber Hygiene Service

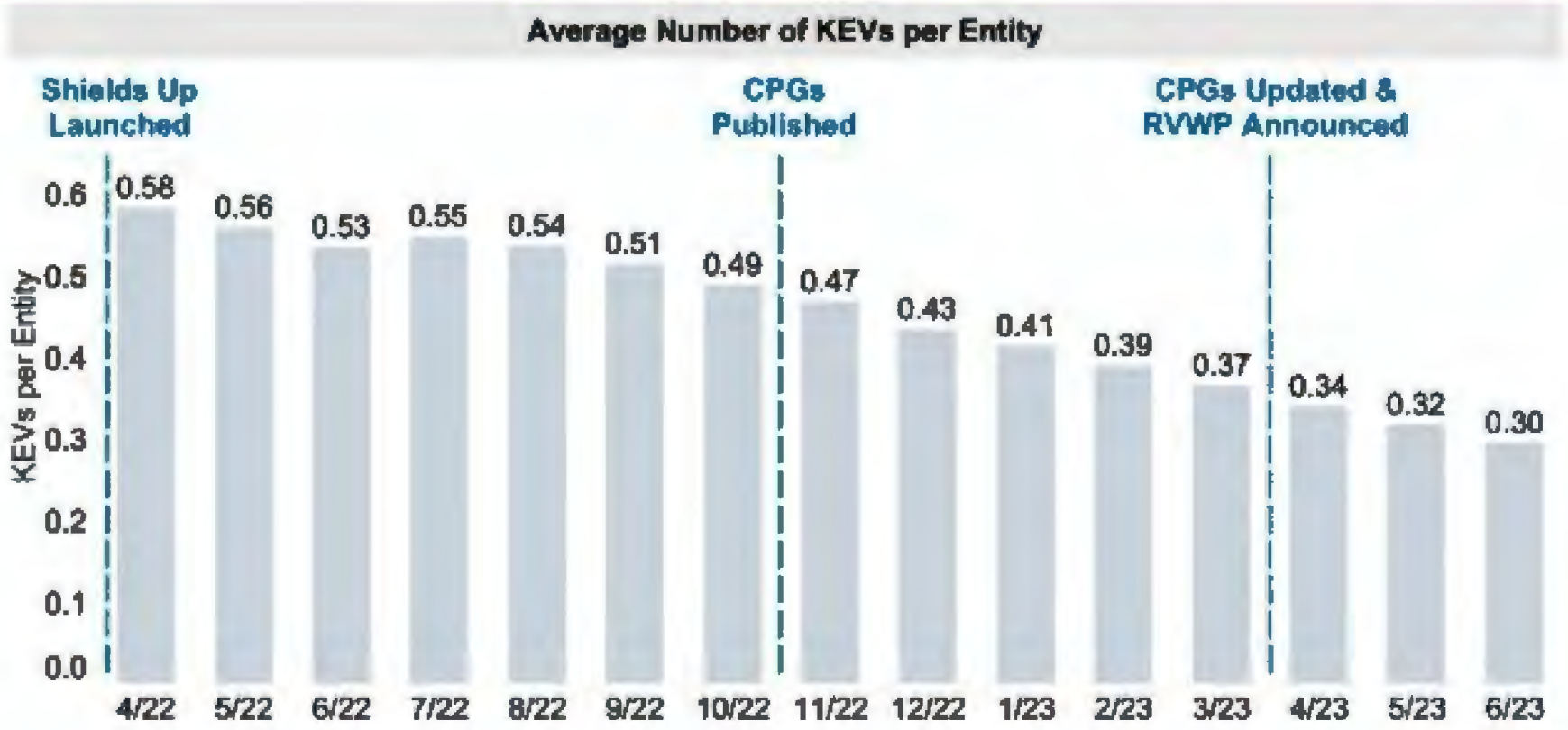
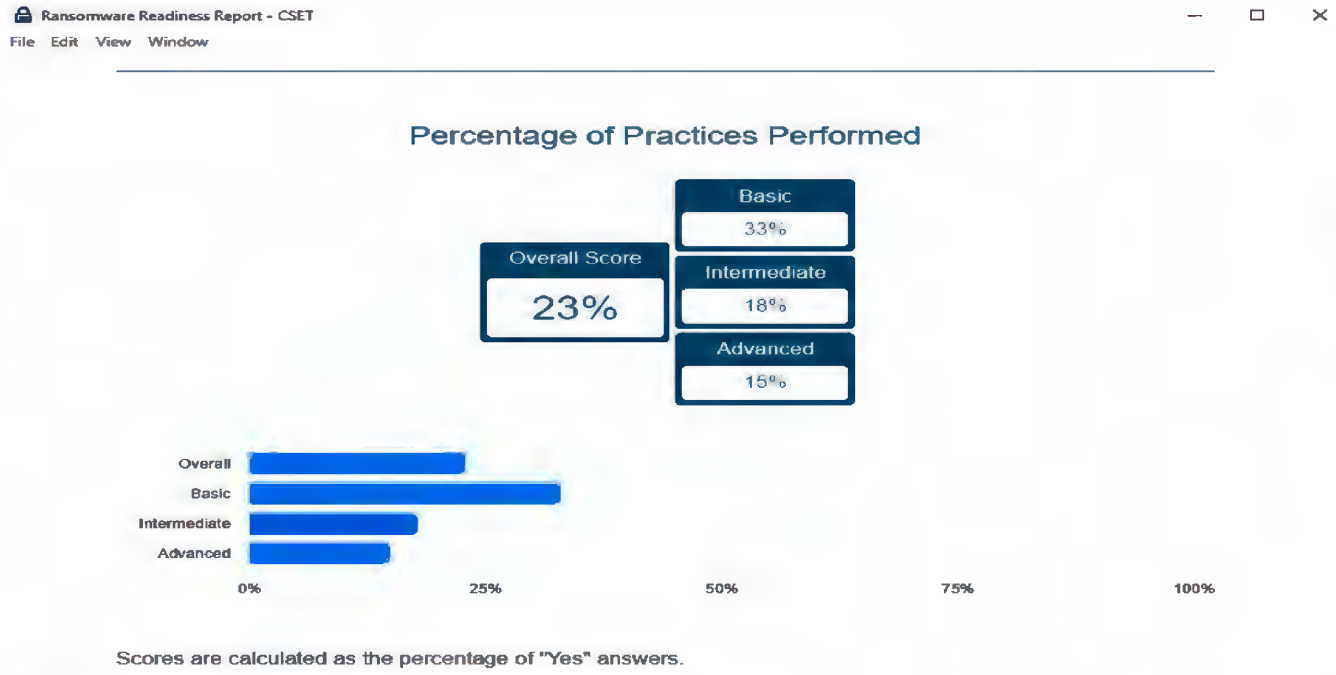


Figure 1: With publication of the CPGs, organizations enrolled in vulnerability scanning continued to demonstrate reductions in KEVs on their networks.

Ransomware Readiness Assessment

- To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA).



CISA No-Cost Cybersecurity Tools

Water and Wastewater Cybersecurity | CISA
Free Cybersecurity Services & Tools | CISA
Known Exploited Vulnerabilities Catalog | CISA
Cyber Hygiene Vulnerability Scanning| CISA
Ransomware Vulnerability Warning Pilot (RVWP) | CISA
Cross-Sector Cybersecurity Performance Goals | CISA
Downloading and Installing CSET | CISA
Logging Made Easy | CISA
Untitled Goose Tool
Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA
Secure Cloud Business Applications (SCuBA) Project | CISA
GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines
Hybrid Identity Solutions Guidance (HISG)
Subscribe to Updates and Alerts from CISA | CISA
https://www.cisa.gov/sites/default/files/publications/FINAL-CSSO-Protective_DNS-Fact_Sheet.pdf
CIS Critical Security Controls Version 8 (cisecurity.org)
Information Security Policy Templates | SANS Institute
Secure Our World | CISA – Home and Business Best Practices and Awareness Tools
Malware Next-Generation Analysis | CISA

Malcolm Components

Report an Incident

- CISA: **cisa.gov/report** ; report@cisa.gov, (888) 282-0870
- FBI/ Internet Crime Complaint Center (IC3): **ic3.gov**

Final Thoughts: Cyber Threat Mitigations

- Secure Access – Passwords and MFA for Remote Access
  - Change Default Passwords
- Reduce Attack Surface (Configuration Control)
  - Asset Identification – Vulnerability Patch Management
- Network Segmentation
- Aggressive Logging and Threat Hunting
- Firewall Whitelisting/ Allow List (IP and Apps) (Outbound and Inbound)
- Backups- 3-2-1 Method

No-Cost CISA Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing

- **Cybersecurity Advisors –** Regionally deployed advisors
  - Incident response coordination
  - Public Private Partnership Development
  - Advisory assistance and cybersecurity assessments

CISA Contact Information

Colin Glover **Ryan Lewis**	colin.glover@cisa.dhs.gov ryan.lewis@cisa.dhs.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	***Call 1-888-282-0870*** ***Email*** *CISAservicedesk@cisa.dhs.gov* ***visit*** *https://www.cisa.gov*

Exhibit 3

Attendance August 14, 2025	Rowan County Summer Training			
NAME	*Water Utility*	DW#/WW#	Signature	Hours
Jerry Patrick	Rowan Water Inc.			1
Larry Johnson	Rowan Water Inc.			1
Mike Collins	Rowan Water Inc.			1
Enoch Blair Randy	Rowan Water Inc.			1
Cox	Rowan Water Inc.			1
[redacted]	[redacted]			
Duane Dehart	Rowan Water Inc.			1