Cybersecurity at Fermilab: Past, Present, and Future

Jessie Pudelek
jpudelek@fnal.gov

54th Annual Users Meeting
5 August 2021

Fermilab’s history in computing

- Fermilab was actively involved in the growth of the Internet, in particular the world wide web (www) by hosting the second web server in North America
- Tim Burners-Lee, responsible for creating the first website at CERN in 1991, even visited Fermilab in the early 90s as part of this new endeavor
- This long history means the laboratory has a lot of technical debt and a unique intertwining of public and private information

2021: Cybersecurity is more important than ever

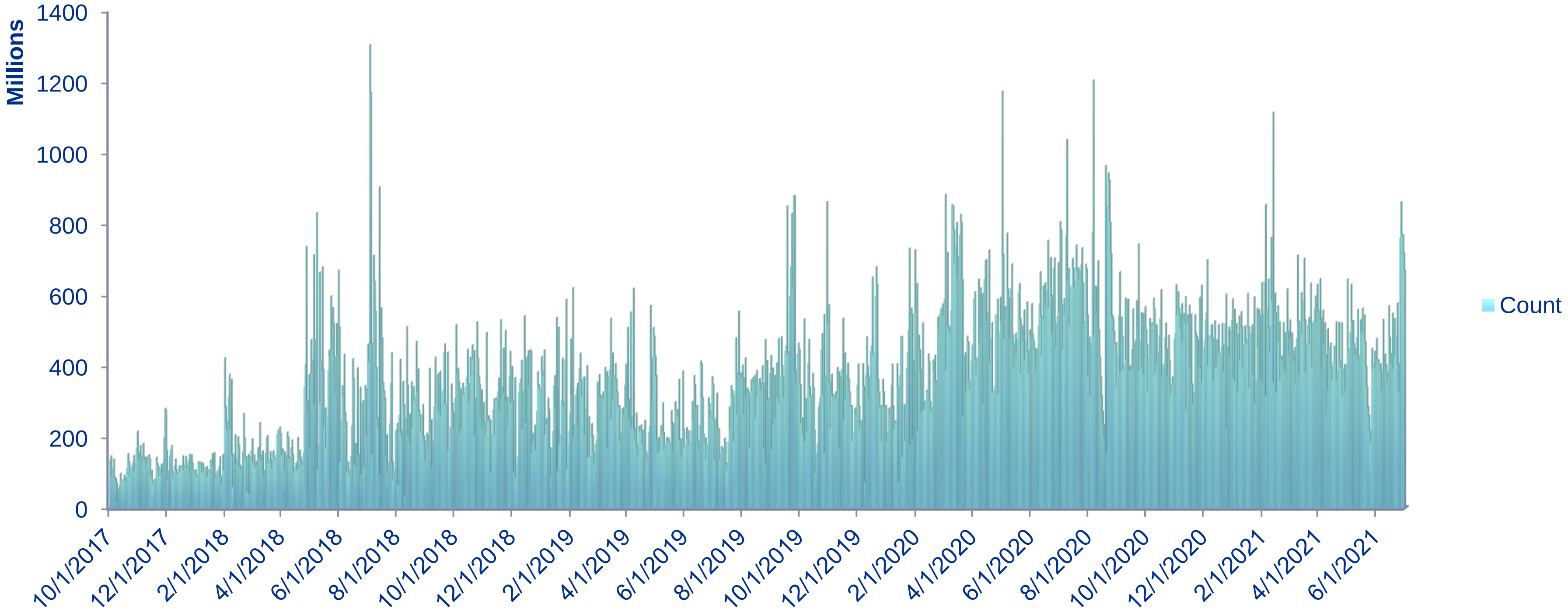
- **Increased cyber criminal activity, including ransomware being a notable threat**
  - 102% increase in ransomware attacks in the first half of 2021 compared to the same time last year
  - Meat and gas supply companies hit with ransomware effects society at large
  - Phishing is the starting point for these kinds of attacks

- Telecommuting risks that became commonplace in 2020 are still present in 2021

- **Threat actors will always seek new ways to damage organizations, such as recent supply chain attacks**
  - These cyber attacks target less-secure elements in the supply chain by installing malicious code or hardware-based spying components
  - Ex: SolarWinds attack

- Increased activity from threat actors probing Fermilab for open ports and vulnerabilities than ever before

Scan Volume to Unallocated Subnets (Oct 01 2017 to Jun 30 2021)



Fermilab deploys defense in depth: Continuous scanning

- Fermilab uses a combination of homegrown and commercial products to scan for vulnerabilities in systems and active threats

- **Scanner farm**
  - Homegrown tool that performs a series of scanning operations on nodes connected to the network
  - Nodes will be scanned upon connection to Fermi network
  - Persistent nodes will be rescanned every 2 days

- Logging of network activity via syslog and Splunk

- **Weekly vulnerability scans performed via Nessus**
  - Vulnerability scanning tool searches for out-of-date software packages and holes that attackers can exploit
  - Tickets are opened with system owners to address issues that come up in these scans

- Packet capture and analysis via Sourcefire IDS

Fermilab addresses weakest link: Social engineering

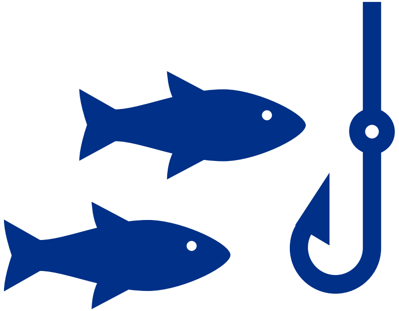
- **Social engineering** is a tactic used by attackers to manipulate victims into clicking on malicious links in emails

- Phishing is a major threat for not just Fermilab but all organizations

- **91% of cyber attacks start with a phishing email**

- Anti-phishing program at Fermilab seeks to educate user community on current threats by sending simulated phishing emails that replicate real phishing attempts

- **Vigilance and cooperation essential to spotting these threats. Report phishing to cybersecurity@fnal.gov**



New cybersecurity initiatives to be aware of

- Updates to current policies will be coming soon, including new initiatives that may be mandated by DOE, as well as additional efforts to increase the laboratory's security posture

- Creation of highly protected data areas for mission needs (quantum technology)

- Investigating options for greater network segmentation
  - Goal to separate networks based on business and experiment requirements
  - Address future DOE initiatives as necessary

New initiatives: Your help is essential!

- The Laboratory is in the process of separating public and private information that is hosted for its collaborations
  - Ex: In depth review of content hosted on public websites at Fermilab

- **Goal:** Maintain a middle ground for High Energy Physics (and its related fields) between open access to the world (including the criminals) and Fermilab via SSO
  - Establish trust by authenticating people via federated identity
  - Creates the effect of a ‘gated community’ with a safe computing environment

- Your cooperation and assistance in this process of weeding out personal from public information will help everything run smoothly

Summary

- Fermilab has a rich history in High Energy Physics and computing
- Cybersecurity threats are getting more dangerous and damaging as time goes on
- Current defense-in-depth strategies work together to protect the laboratory’s data and resources
- New initiatives will increase Fermilab’s security posture and address DOE initiatives
- Your cooperation and vigilance is essential to maintaining a secure computing environment
- Cybersecurity Awareness Week 2021 coming this October – please see Fermi News for a save the date

Cybersecurity is everyone’s responsibility!

References

- https://en.wikipedia.org/wiki/List_of_websites_founded_before_1995
- https://www.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html
- https://en.wikipedia.org/wiki/Supply_chain_attack
- https://www.cisecurity.org/solarwinds/