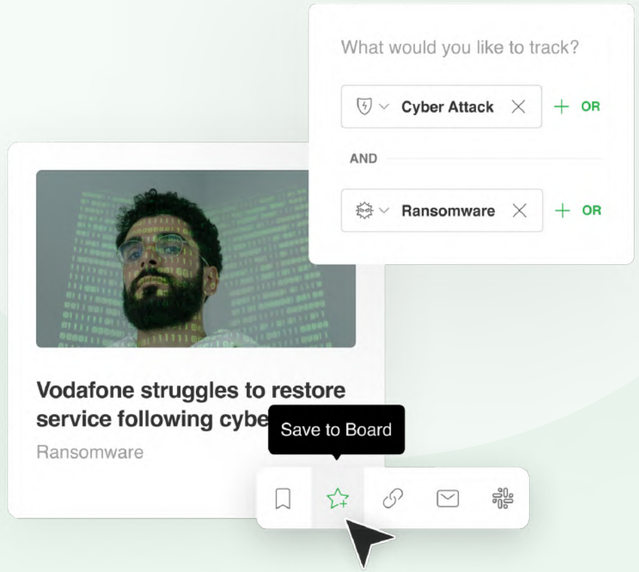
feedly



SANS OSINT Summit 2022 - Workshop

Expanding your intelligence capabilities when you can't expand your team

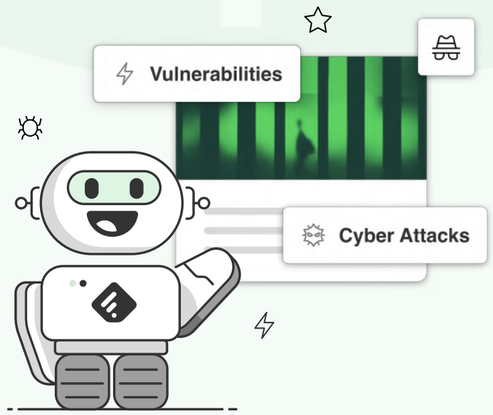
How to use threat-based prioritization to stay one step ahead of increasingly active adversaries

Chris Pickard

- 9 years working in Cybersecurity
- Defense, government, utilities, aerospace, and transport industries
- Joined Feedly in February to mentor Feedly for Threat Intelligence customers
- Avid gamer, and I also enjoy playing tennis, squash, badminton, or anything competitive!

Understaffed? Here are five tips on how to prioritize your open source threat intelligence

1. Prioritize your crown jewel assets
2. Prioritize trending vulnerabilities and emerging exploits
3. Prioritize your primary adversaries
4. Prioritize your defensive gaps
5. Monitor emerging threats proactively

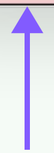


Thank you Michael Rossi, Gerald Lott, Valentina Costa-Gazcon, David Ortiz, Richard Stiennon, and Jim A. for helping shape these tips!

Prioritization Tip #1

Prioritize your crown jewel assets

Asset List Tracker						
Risk	Vendor	Product	Version	Install Date	Support Date End	Team
High	Cisco	ASA	9.14.1	01/03/2022	01/03/2024	Network Team
Medium	Adobe	Acrobat Reader	21.007.20099	22/10/2020	22/10/2023	Apps Team
Medium	Microsoft	Teams	4.11.17.0	10/01/2020	10/01/2023	Apps Team
High	Zoom		5.9.0	10/01/2020	10/01/2023	Apps Team
High	Fortinet	FortiManager	7.0.2	01/03/2022	01/03/2024	Network Team
Medium	SAP	Business One	10	11/11/2021	11/11/2022	Apps team
High	Apache	Tomcat	9.0.18	10/01/2020	10/01/2023	Server Team
High	WordPress	WordPress	5.9.1	02/06/2021	02/06/2023	Apps team



1. Define your Crown Jewels and vital critical business processes
2. Determine the assets that are on the critical path to stealing or damaging them
3. Document them as High Risk in a spreadsheet or in your asset management system.

Prioritization Tip #1

Prioritize your crown jewel assets

Asset List Tracker			
Risk	**Vendor**	**Product**	**Version**
High	Cisco	ASA	9.14.1
Medium	Adobe	Acrobat Reader	21.007.20099
Medium	Microsoft	Teams	4.11.17.0
High	Zoom		5.9.0
High	Fortinet	FortiManager	7.0.2
Medium	SAP	Business One	10
High	Apache	Tomcat	9.0.18
High	WordPress	WordPress	5.9.1

Gather Vulnerability Announcements

- NVD
- Vendor advisory
- Cybersecurity news sites
- Twitter
- Reddit

Triage CVEs based on

- CVSS, EPSS (NVD,Vendor Advisory)
- Proof of exploit (Github, Social Media...)
- Patch
- Product/Version

Prioritization Tip #2

Prioritize trending vulnerabilities and emerging exploits

2/11/2021

CVE-2021-21017

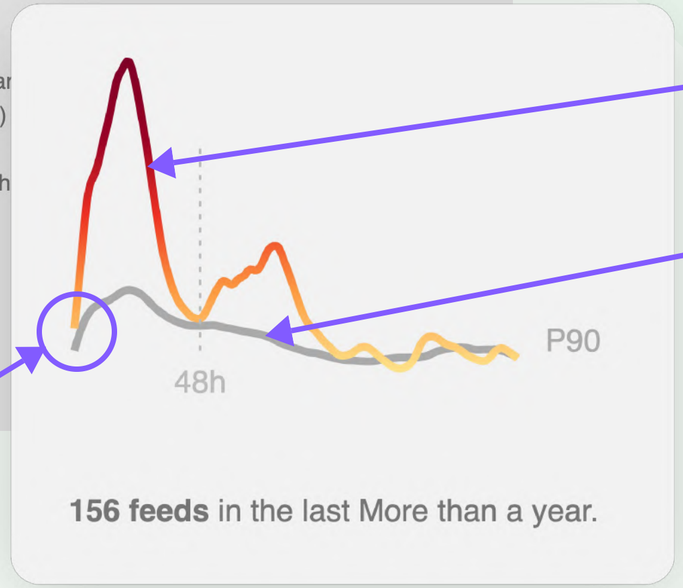
Out-of-bounds Write (CWE-787)

CVSS: **8.8 (High)** | Affected Systems: **acrobat, acrobat_dc, +2 other products**

Patched: **helpx.adobe.com**

Acrobat Reader DC versions versions 2020.013.20074 (and ear
2020.001.30018 (and earlier) and 2017.011.30188 (and earlier)
affected by a heap-based buffer overflow vulnerability. An
unauthenticated attacker could leverage this vulnerability to ach
arbitrary code execution in the context of the current user.…

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Critical vulnerabilities and 0-days that are trending on the Web and social media and gather more awareness are **more likely to be exploited**

Red line: awareness of CVE-2021-21017

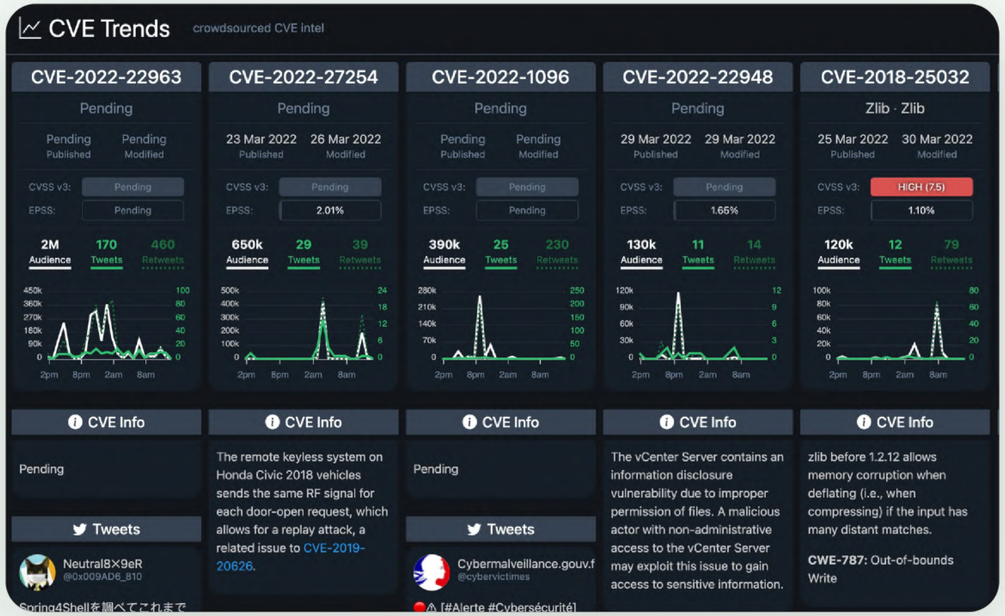
Gray line: awareness of a typical adobe vulnerability

You can detect the delta very early and **prioritize patching**

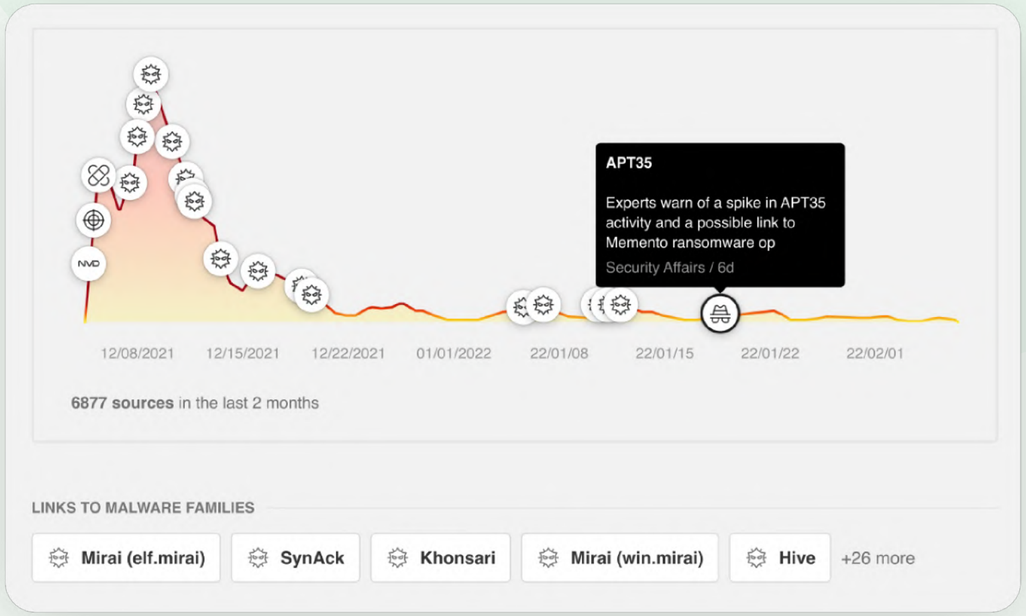
Prioritization Tip #2

Prioritize trending vulnerabilities and emerging exploits

Use CVE Trends or the Feedly CVE Intelligence cards to determine which vulnerabilities are trending



cvetrends.com by Simon J. Bell

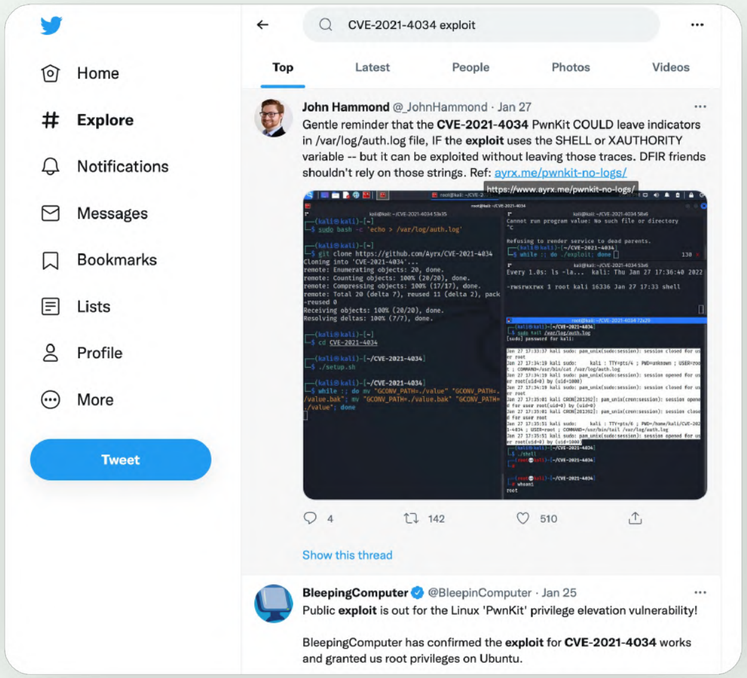


cve.feedly.com by Feedly

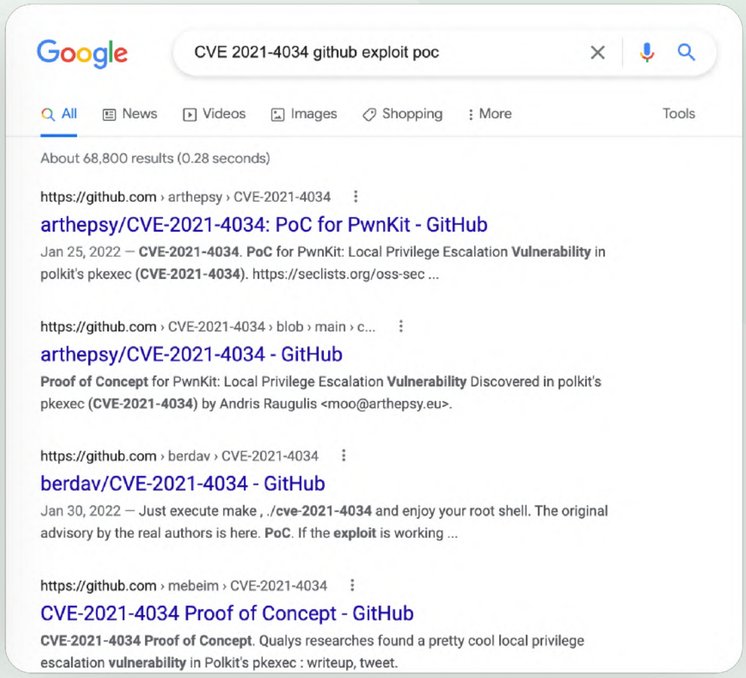
Prioritization Tip #2

Prioritize trending vulnerabilities and emerging exploits

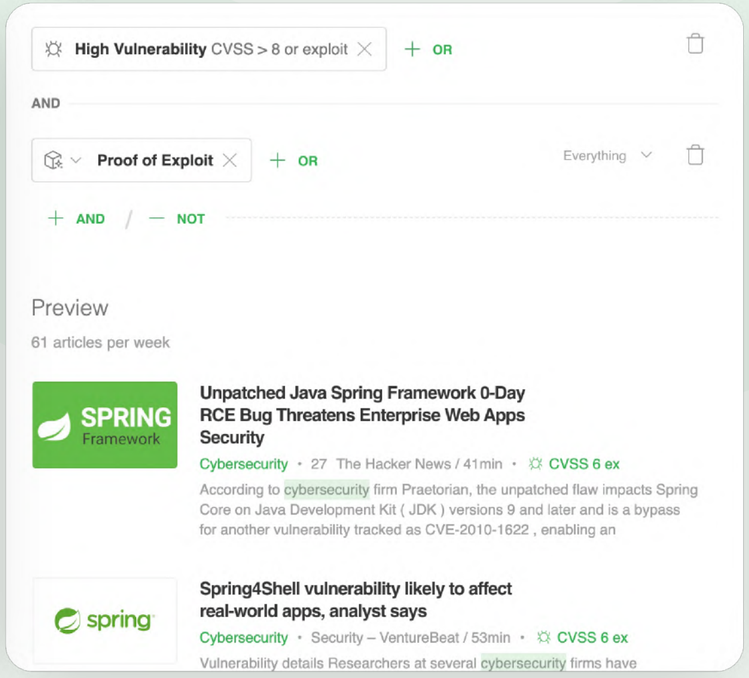
New exploits can give a new life to existing vulnerabilities. Use Twitter, Google Alerts, GitHub, or Feedly to track proof of exploits



Twitter Advanced Search



Google Alerts



Feedly's AI Engine

Prioritization Tip #3

Prioritize your primary adversaries

Track cyber attacks in your industry / against a list of peers to identify active adversaries. List top 15 adversaries in a spreadsheet or in your TIP

Threat Actor Tracking

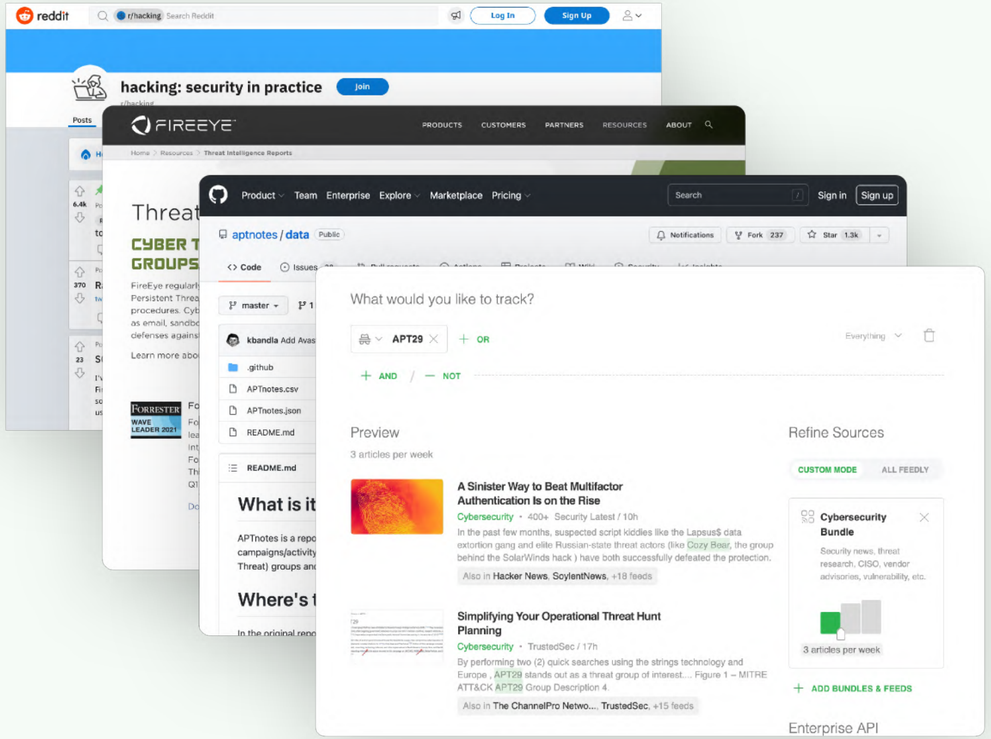
Russia

Group Name	Other Aliases	Description
APT29	Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, APT29, Cozy Bear, The Dukes, Minidionis, SeaDuke, Hammer Toss, YTTRIUM, Iron Hemlock, Grizzly Steppe	APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015
Sandworm	Sandworm Team, Black Energy, BlackEnergy, Quedagh, Voodoo Bear, TEMP.Noble, Iron Viking	Sandworm is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455. This group has been active since at least

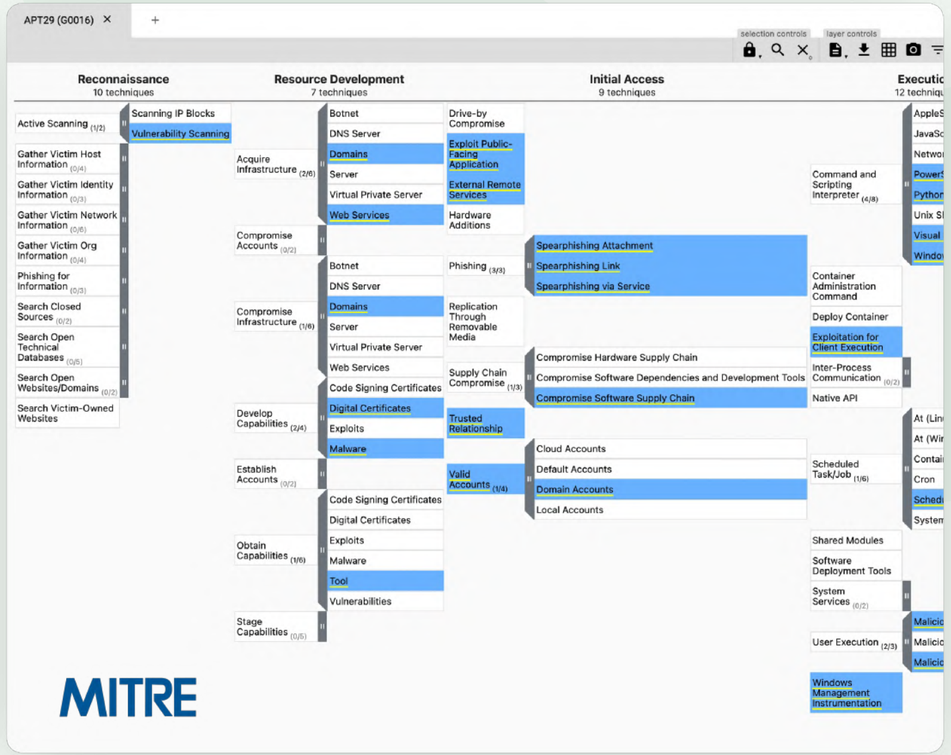
Prioritization Tip #3

Prioritize your primary adversaries

Research threat intelligence reports and news articles related to those top adversaries and map their TTPs into the MITRE ATT&CK Navigator to understand their behaviors



Gather intelligence reports from across the Web

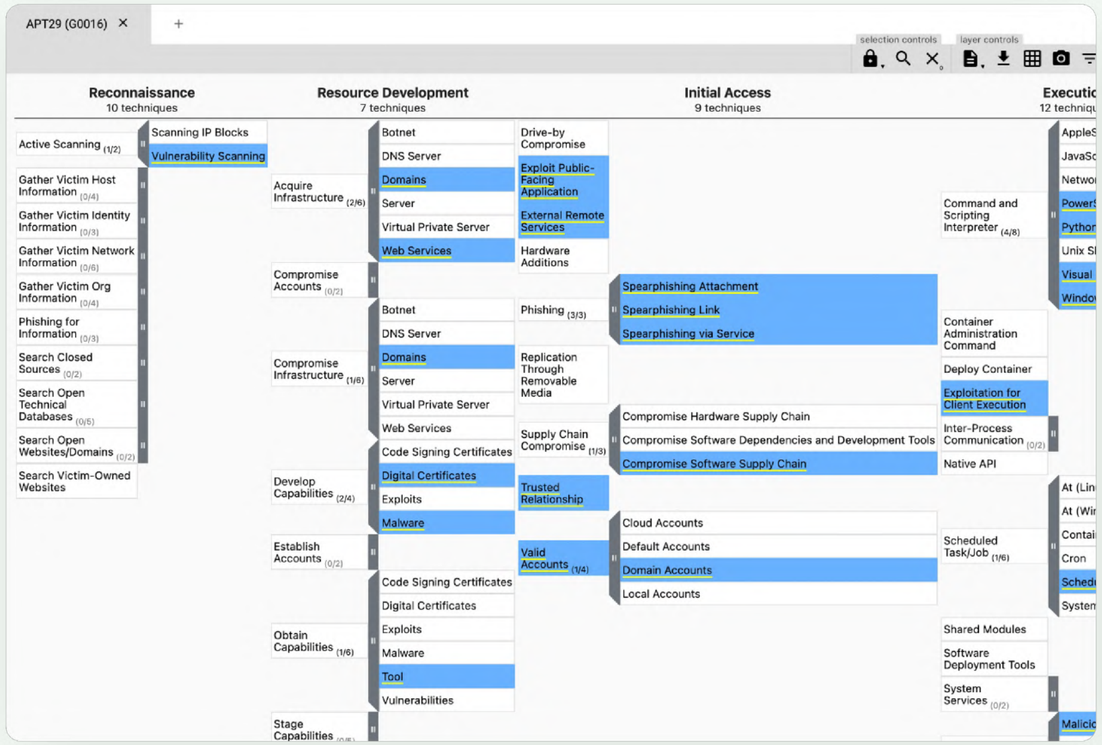


Map Threat Actor TTPs into MITRE ATT&CK

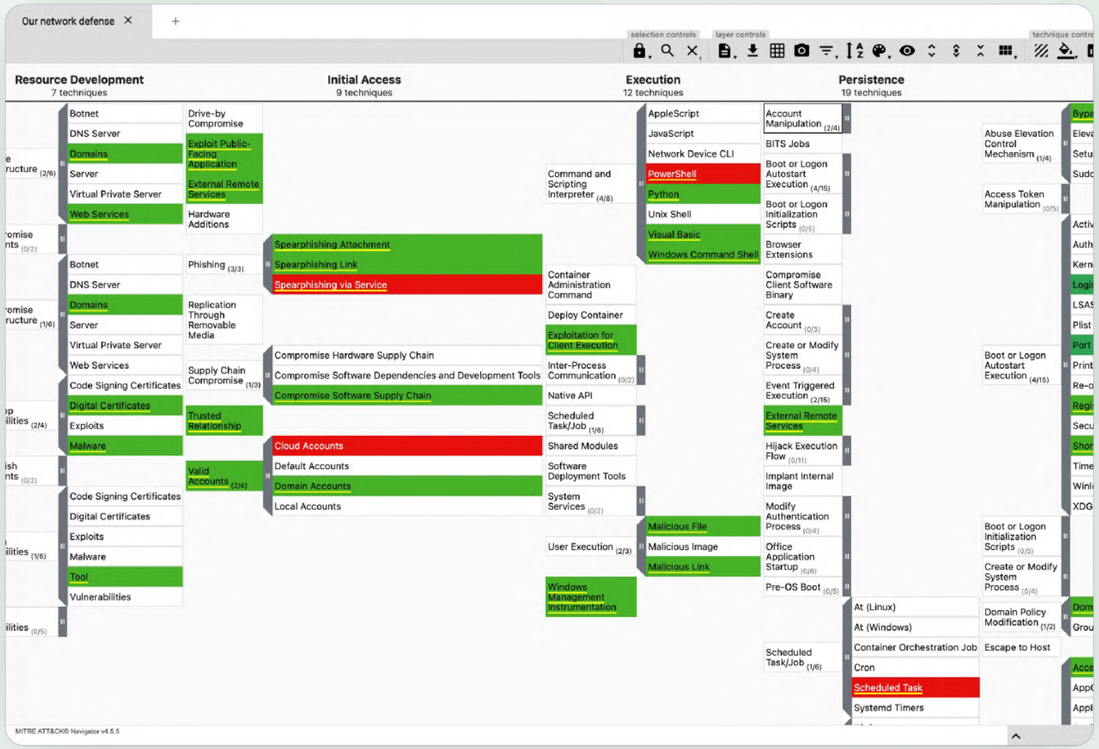
Prioritization Tip #4

Prioritize your defensive gaps

Compare adversary behaviors with your network defenses to identify weaknesses.
You can also compare campaigns over time to discover behavioral changes.



Adversary Behavior



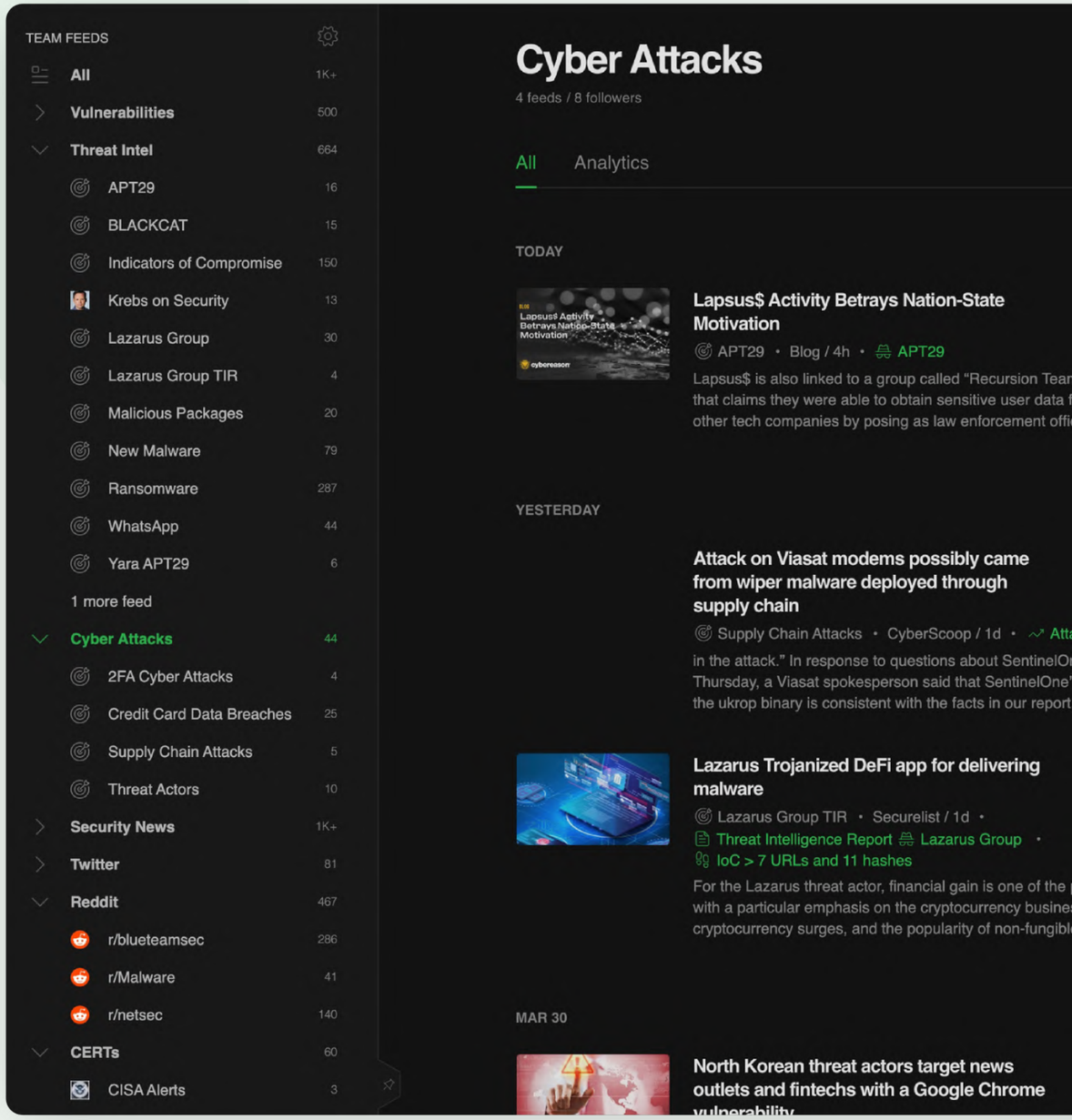
Defense & Gaps

Prioritization Tip #5

Monitor emerging threats proactively

Set up an “indications and warning” monitoring system for what might be coming down the “cyber pipeline” for the next big attack

Track emerging threats (ransomware, malicious packages, third-party attacks), cyber attacks, threat intelligence reports, advisories, etc.



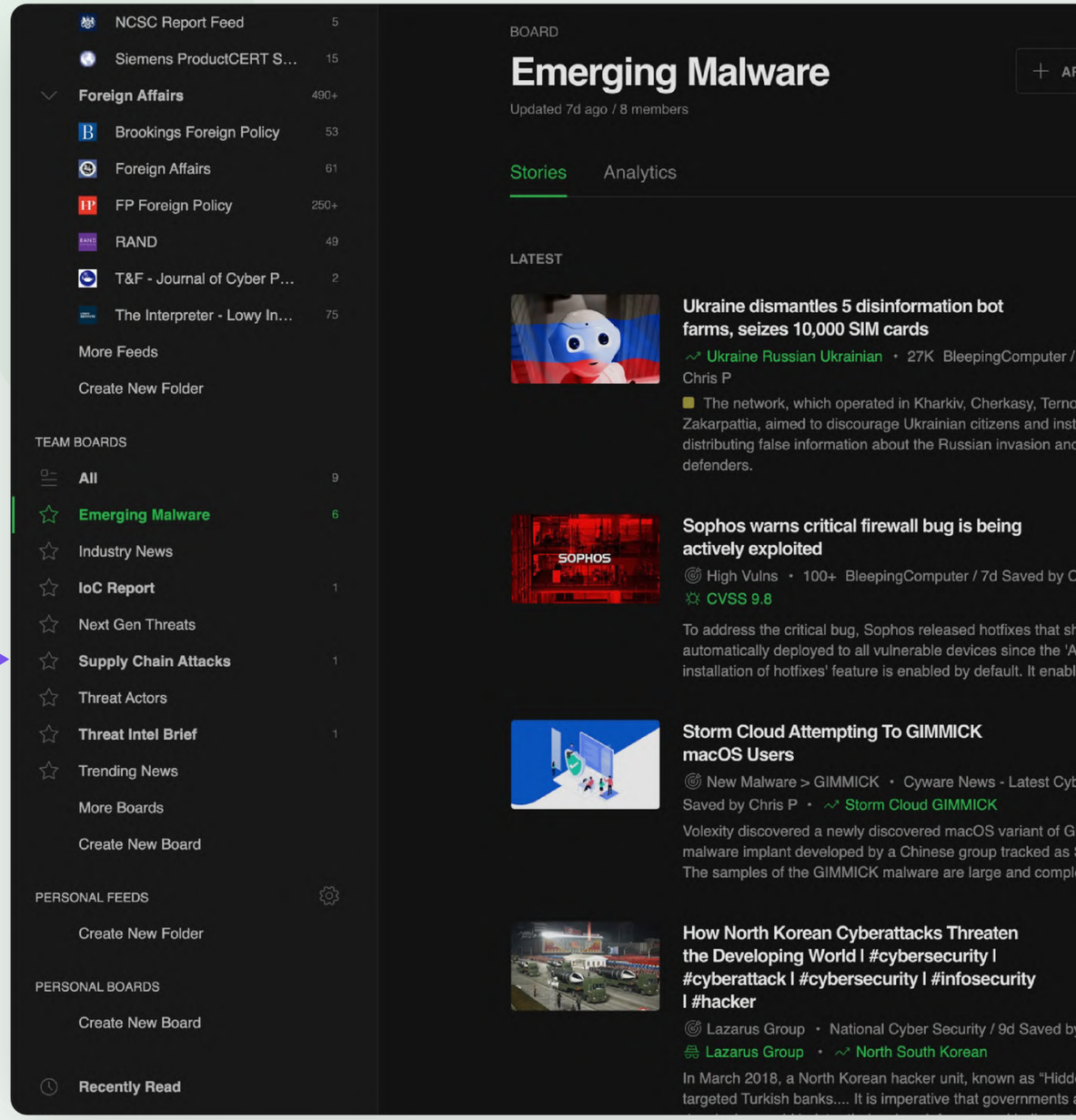
Bonus Tip

Improve your intelligence sharing process

Daily curation process

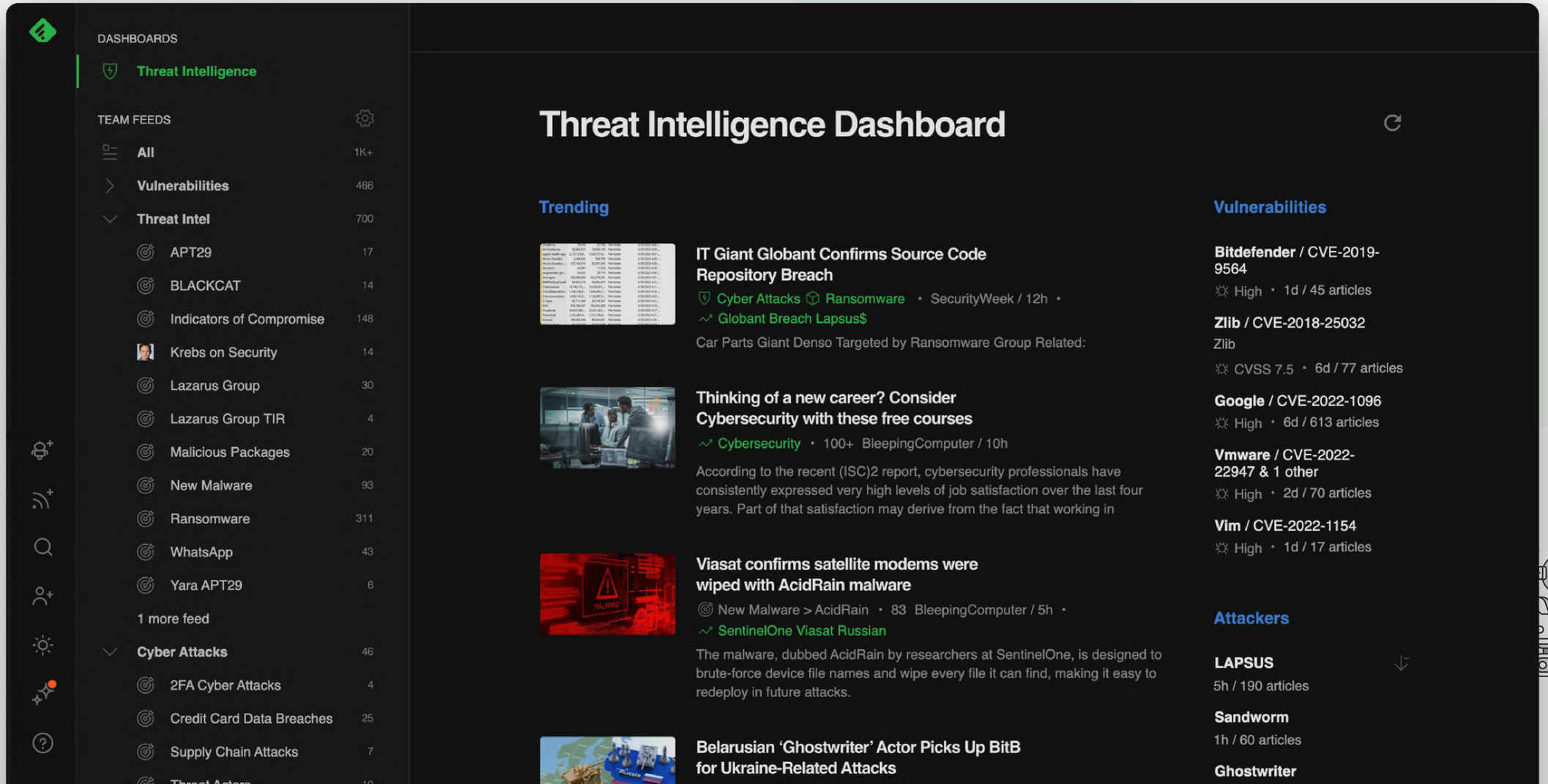
Weekly or daily review, discussion, and prioritization stand-ups

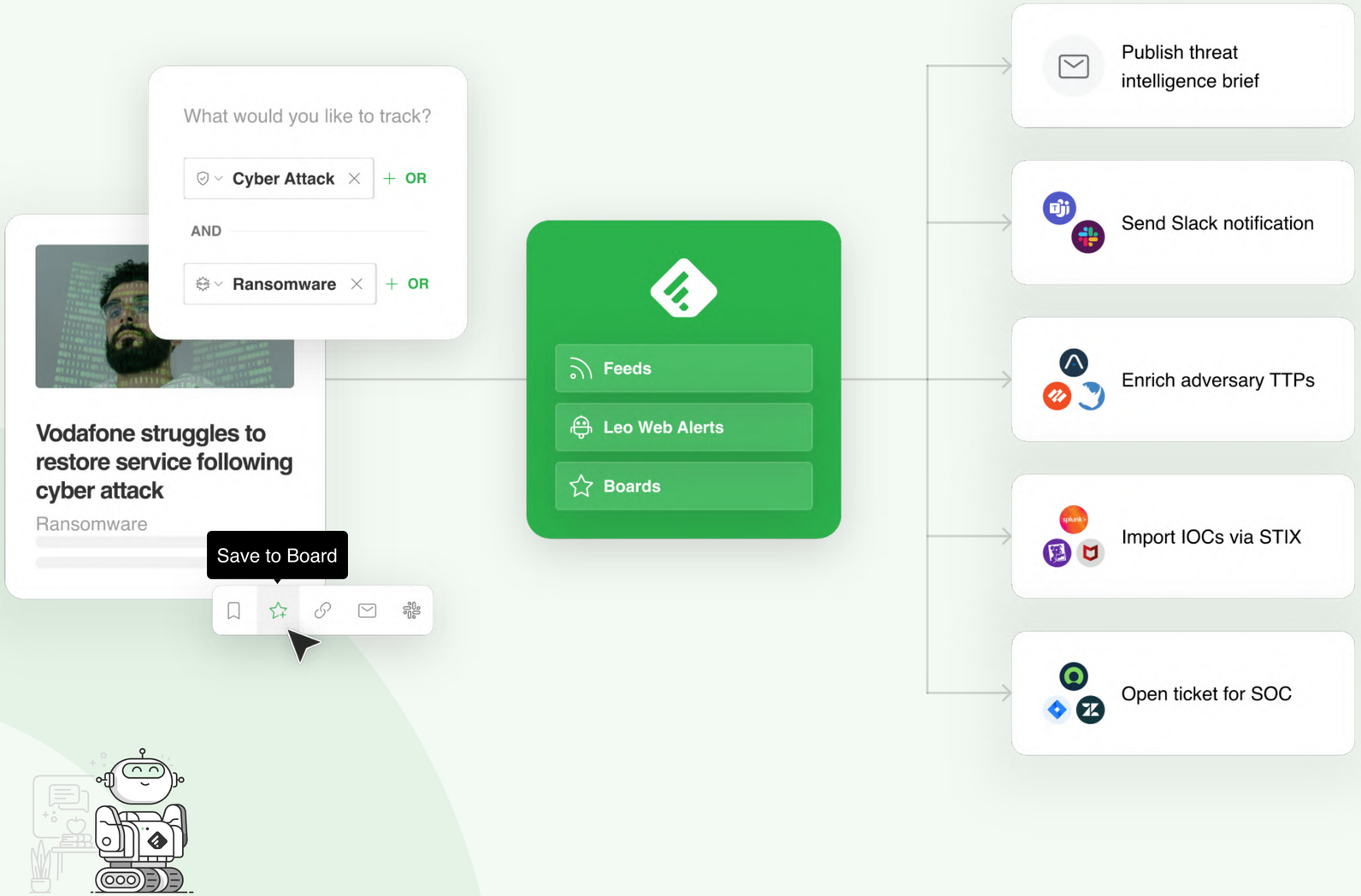
Example of "Feedly Friday" Research Prioritization Boards



Demo

How to leverage machine learning to automate your threat intelligence?





Feedly for Threat Intelligence

The fastest way to discover, prioritize, and share emerging security threats

Use Cases

- ✓ Understand the threat landscape around your industry
- ✓ Monitor critical vulnerabilities and zero-days
- ✓ Research the behavior of malware families and threat actors

Differentiation

- ✓ Machine learning models that automatically gather, analyze, and prioritize intelligence from millions of sources, in real-time.
- ✓ Getting smarter every week

Validation

- ✓ 200+ cybersecurity teams
- ✓ 8 of the top 12 tech companies

More resources

cve.feedly.com

Next generation CVE intelligence cards. Our gift back to the threat intelligence community

JOIN BETA

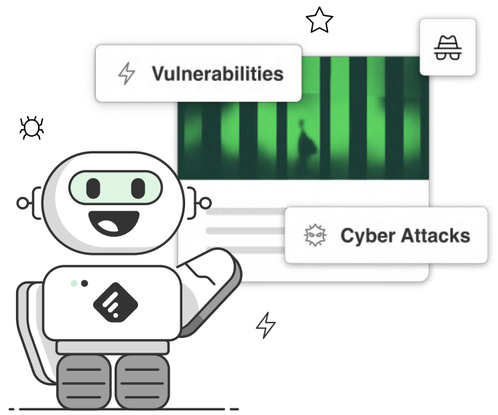
ahead

Threat intelligence community where experts share tips and best practices

JOIN COMMUNITY

Feedly for Threat Intelligence

The fastest way to discover, prioritize, and share emerging security threats



START 30-DAY FREE TRIAL