tenable

CYBER THREAT ALLIANCE
Threat Intelligence Practitioners' Summit

Unveiling Cybersecurity Impact

The Role of Published Security Findings in Strengthening Internet Defense Strategies

Sławomir Grzonkowski, senior staff data scientist

October 3rd, 2024

Introduction

- The importance of cybersecurity investigations
  - Where to find data
- Best practices for cybersecurity findings publishing
- How cybersecurity is shared with organizations

Goals

- Use a scientific approach when evaluating the impact of published threat reports - keep it objective
  - Data-driven insights and how they can impact evaluation
  - Assess the impact of publishing security related findings by correlation with CVEs
- Use publicly available data for threat reports
  - Collaboration and information sharing
  - Shaping defensive strategies to mitigate cyber risks
- Evaluate the impact of reported findings on the enterprise side
- Contributing to strategic defense
  - Best practices
  - How to approach

Data

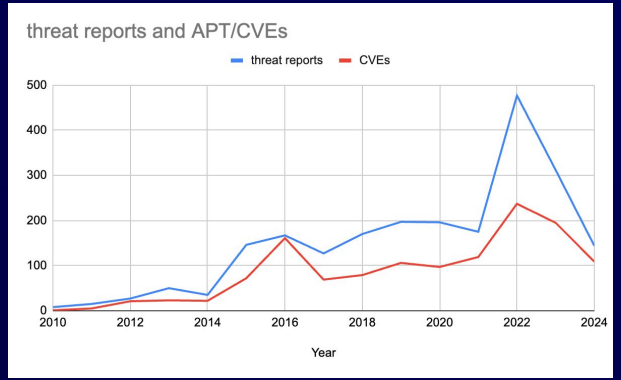
- Data in this report consists of information extracted from publicly available threat reports
  - CVE-id, report date, etc
  - Does it relate to ransomware
- Tenable focuses on threat intelligence for vulnerabilities instead of searching for threat actors
  - What and where was detected during security scans
  - Detailed information about each vulnerability

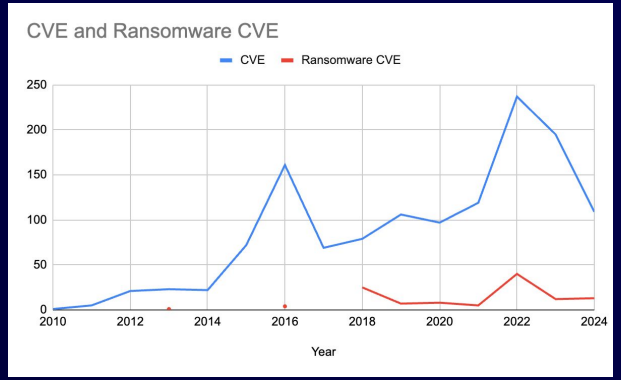
Analysed data in numbers

- 2264 threat reports published between 2010 and July 2024
- 498 of them reports mentions CVEs, some of them multiple times
- 1316 CVEs reported (449 unique)
- 256k CVEs that have been published so far

Evolution of CVEs in threat reports

		APT		Ransomware	
Year	threat reports	CVEs	Distinct CVEs	CVEs	Distinct CVEs
2010	8	1	1		
2011	15	5	5		
2012	27	21	17		
2013	50	23	9	1	1
2014	35	22	18		
2015	146	72	39		
2016	167	161	88	4	4
2017	127	69	37		
2018	170	79	43	25	10
2019	197	106	58	7	3
2020	196	97	59	8	8
2021	175	119	89	5	5
2022	477	237	106	40	29
2023	312	195	92	12	11
2024	144	109	63	13	13





Data insights

The most popular CVEs used by APT groups

- CVE-2012-0158 : 53
- **CVE-2017-11882 : 50**
- CVE-2017-0199 : 35
- CVE-2018-0802 : 24
- **CVE-2021-44228 : 21**
- **CVE-2017-5689 : 17**
- CVE-2021-26855 : 16
- CVE-2021-27065 : 15
- CVE-2022-30190 : 14
- CVE-2018-0798 : 13

The most popular CVEs used by ransomware groups

- CVE-2017-5689 : 17
- CVE-2021-44228 : 5
- CVE-2017-11882 : 4
- CVE-2021-34473 : 3
- CVE-2021-34523 : 3
- CVE-2021-31207 : 3
- CVE-2020-1472 : 2
- CVE-2019-19781 : 2
- CVE-2021-26857 : 2
- CVE-2018-8373 : 2

tenable

How vulnerability scanning works?

- Tenable Nessus and Tenable Vulnerability Management
  - Authenticated and unauthenticated scans
  - Agent-based scans
- Vulnerability detection
  - Signature-Based Detection: Tenable uses a database of known vulnerabilities, often referred to as plugins in Nessus. Each plugin is designed to detect a specific vulnerability, misconfiguration, or compliance issue. The scanner compares the system's characteristics against these signatures to identify matches.
  - Behavioral Analysis: In addition to signature-based detection, Tenable scanning can analyze behavior patterns, such as unusual network traffic or abnormal system processes, to detect potential threats or indicators of compromise.
- Scanning
  - Scheduled
  - On demand

What affects the number of detections

- The number of detections going down
  - Patching to mitigate the threat
  - Uninstalling
- The number of detections going up
  - Adding scan profiles to look for certain vulnerabilities
  - Increasing the scan coverage
  - New plugins development

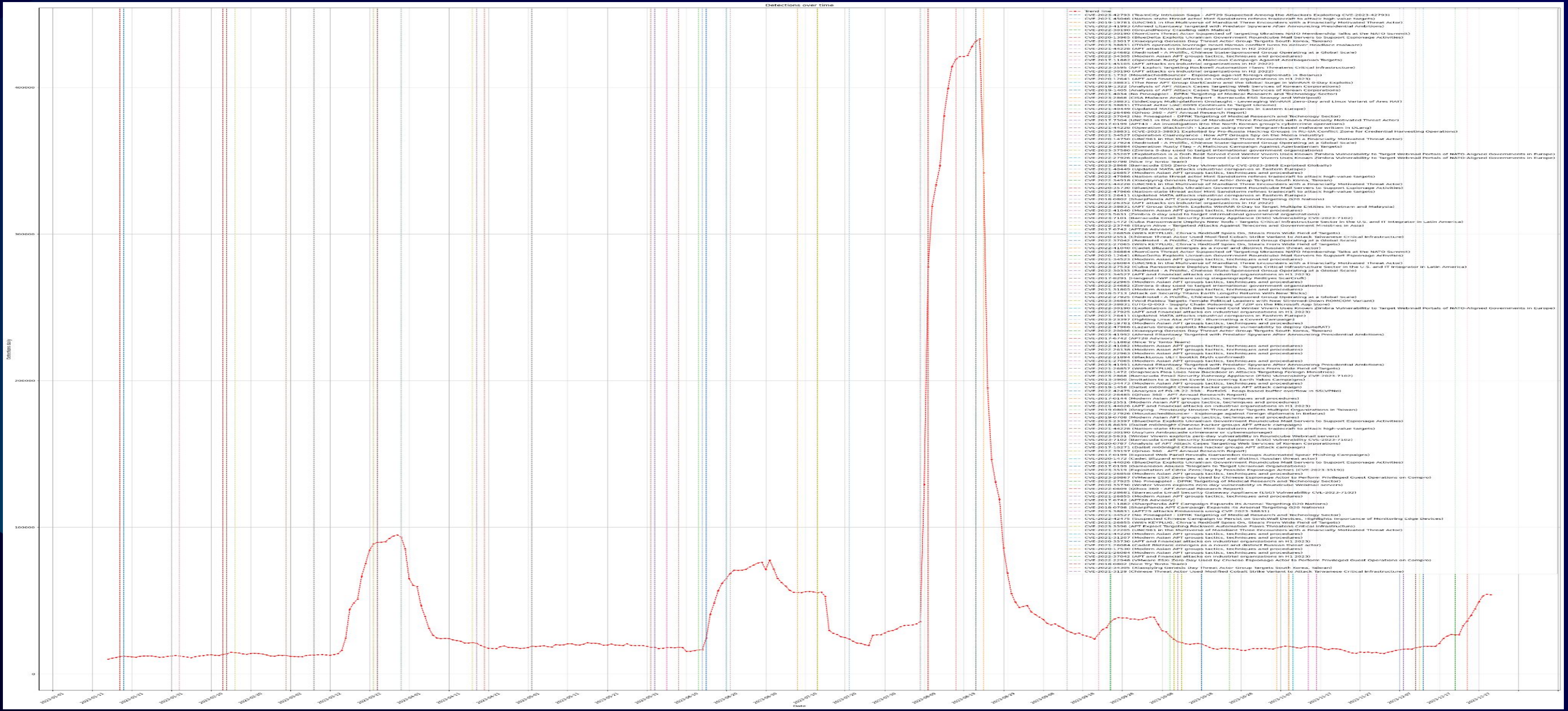
Data analysis – assumptions

- Limit threat report data to 2023 and beyond, which is the last fully completed year
- Take a representative sample of the detection data
- Assume that data from various threat reports was properly parsed and extracted
- Some Tenable plugins detect multiple similar vulnerabilities
- Try to be objective

Data analysis – plan recap

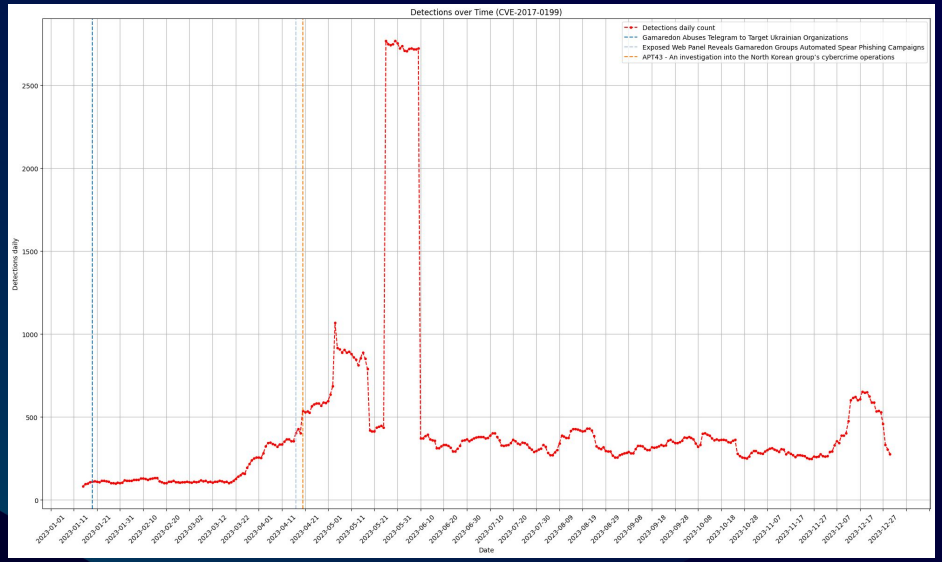
1. Take each threat report
2. Extract CVEs if any
3. Match with software
4. Obtain the trend of specific detections for a given vuln + software
5. Assess the impact or the lack of it

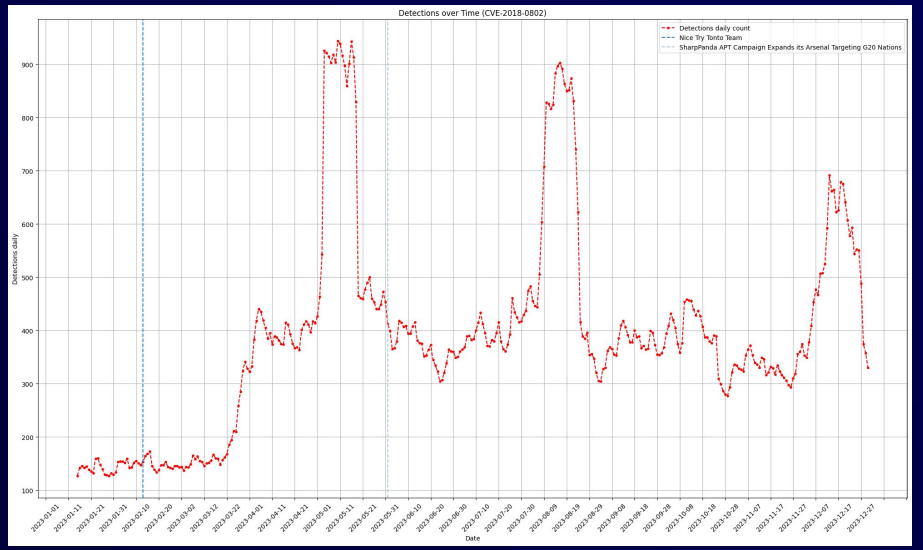
Data analysis - big picture



Data analysis

Microsoft Office: CVE-2017-0199, CVE-2018-0802

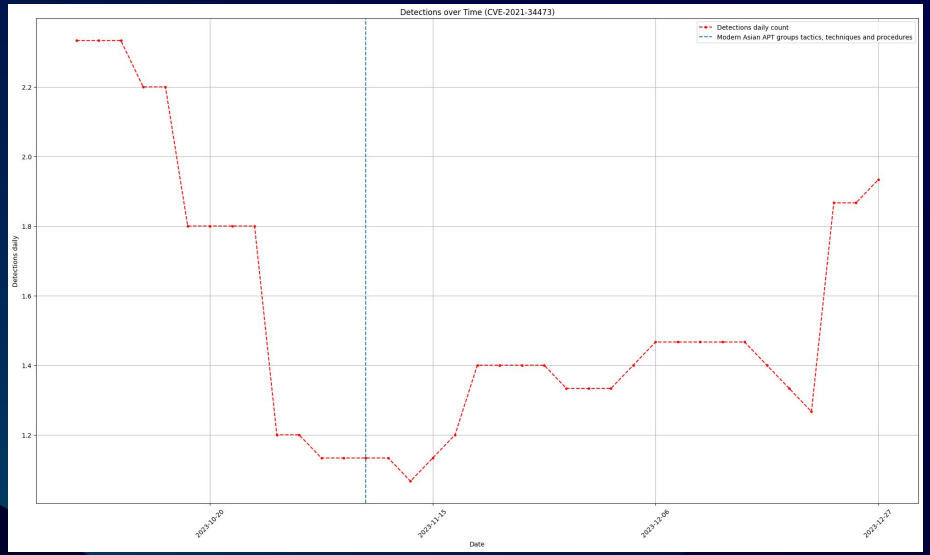


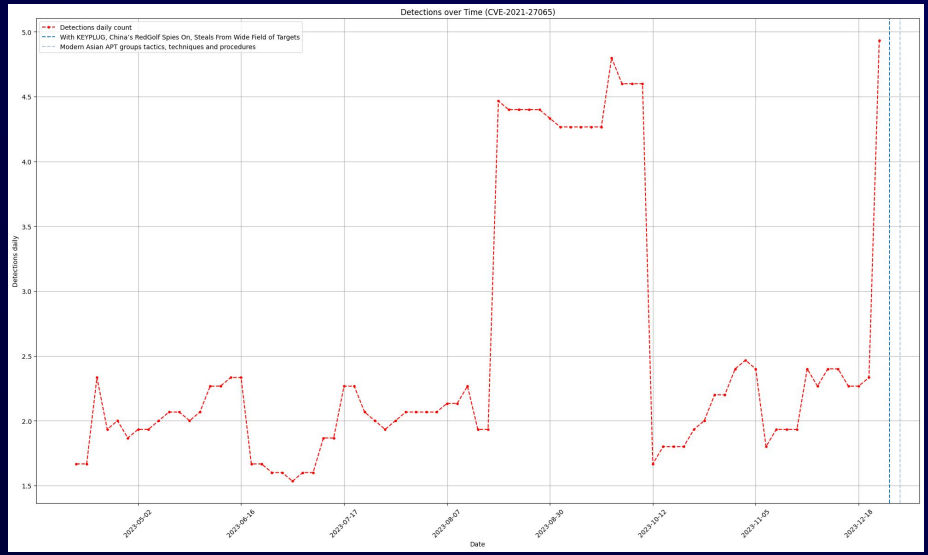


tenable

Data analysis

Microsoft Exchange: CVE-2021-34473, CVE-2021-27065



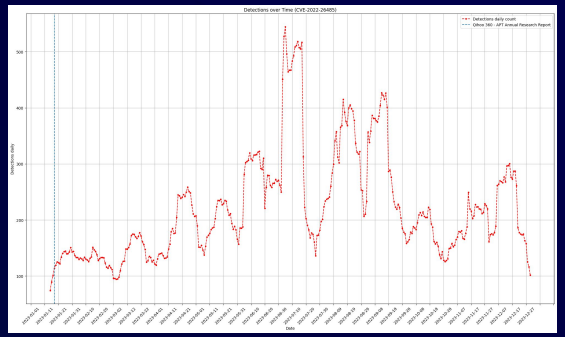


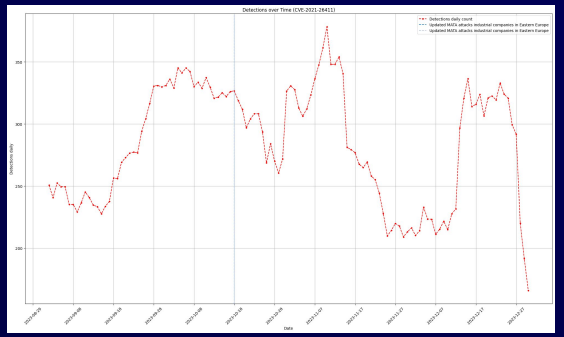
tenable

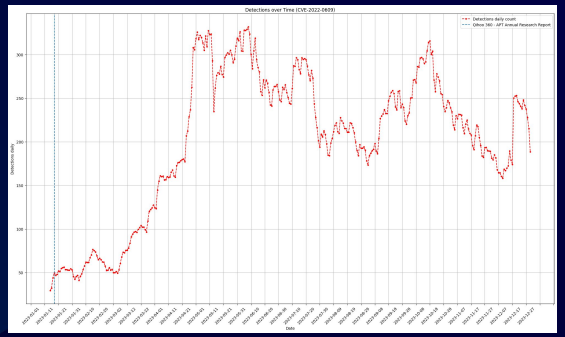
Data analysis

Browser-related exploits

- Firefox
  - CVE-2022-26485
  - CVE-2022-26486
- Internet Explorer
  - CVE-2021-26411
- Chrome
  - CVE-2022-0609





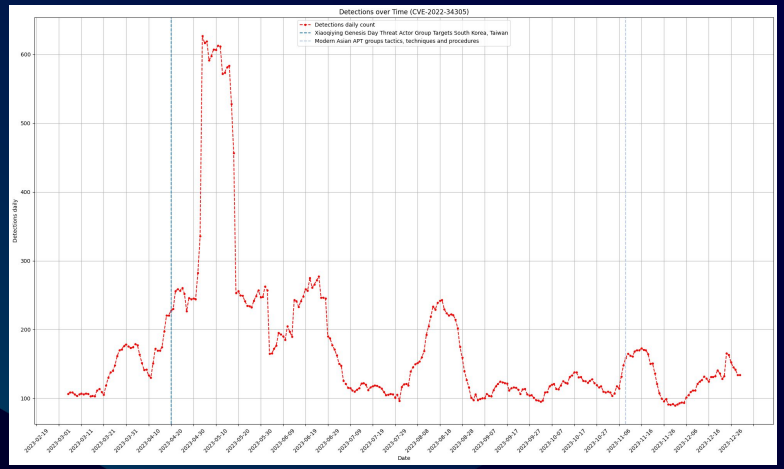


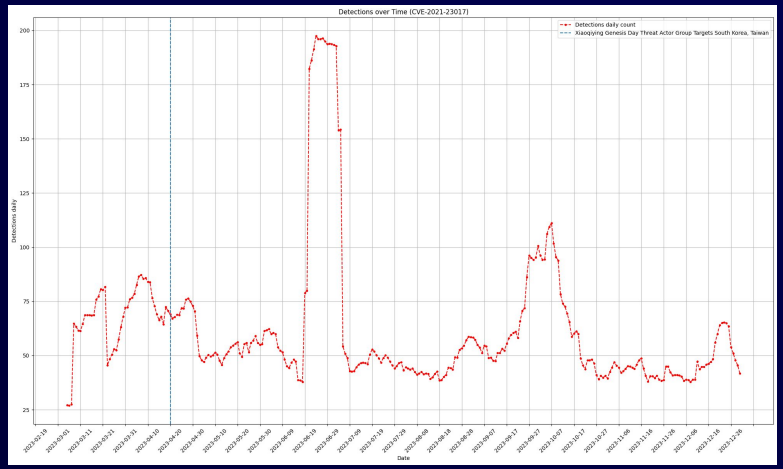
tenable

Data analysis

Web server-related vulnerabilities

- Apache tomcat
  - CVE-2022-34305
- Nginx
  - CVE-2021-23017



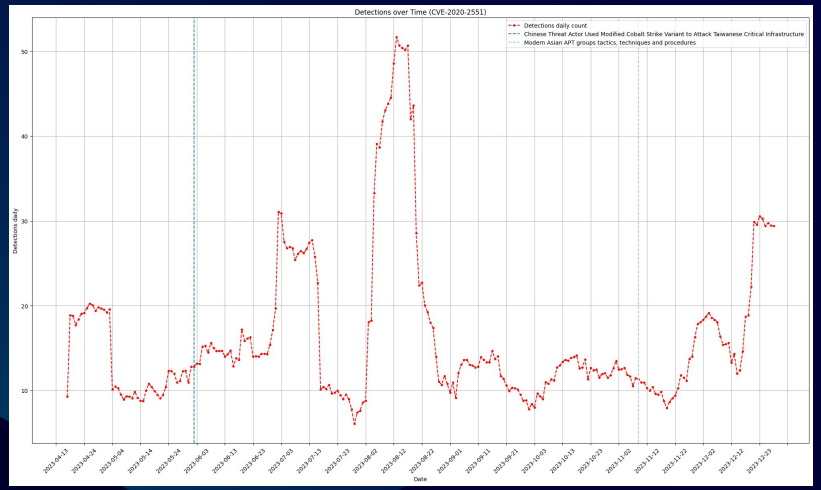


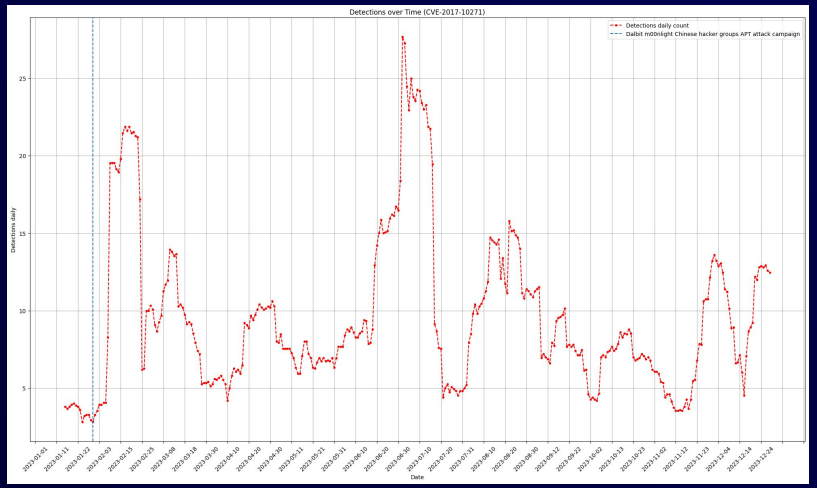
tenable

Data analysis

Web server-related vulnerabilities

- Oracle WebLogic Server
  - CVE-2017-10271
  - CVE-2020-2551



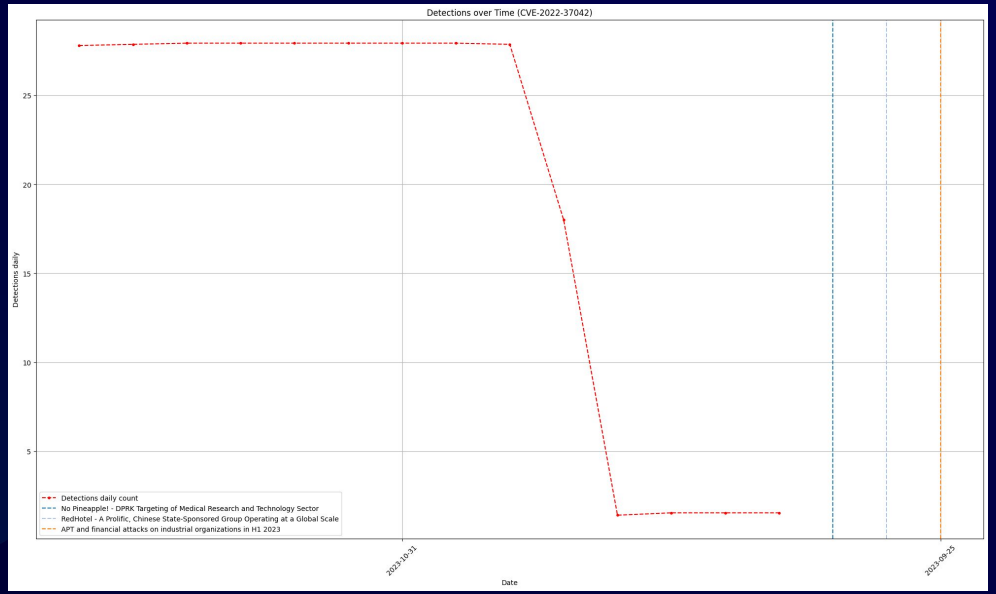


tenable

Data analysis

Zimbra Collaboration Suite (ZCS)

- CVE-2023-37580
- CVE-2022-27925
- CVE-2022-24682
- CVE-2022-27926
- CVE-2022-37042
- CVE-2022-27924
- CVE-2021-35207



tenable

Impact by affected software

	CVE impact type			
	name	no impact	impact	no data
Windows	Windows		2	2
	Other windows	2	2	
	Win32k	1	3	
	Windows Search	1		
Enterprise	Exchange	1	5	3
	MS Office		4	
	MS Outlook		1	
	SMBv1 server		1	
	BITS		1	
	Remote Desktop	1		
	Windows Print Spooler		1	
	msdn		1	
Browsers	Internet Explorer		1	
	Firefox		2	
	Google Chrome		1	

	CVE impact type			
	name	no impact	impact	no data
OS	macOS Sonoma		1	
	macOS Ventura		1	
	macOS Monterey		1	
	Linux kernel		1	
Servers	Apache Tomcat		1	
	WebLogic Server		3	
	Nginx		1	
Developm	Apache Log4j		2	
	Spring MVC		1	1
	Apache Struts		2	
Other	Winrar / Unrar	2		
	VMware / vCent	1	1	
	Roundcube Web			4
	ZCS Zirnbra	7		

Impact by affected software

- Summary includes only those vulns of reported usage in 2023

Category	Impact Chance
Windows	53.85%
Enterprise	73.68%
Browsers	100.00%
OS	100.00%
Servers	100.00%
Development	83.33%
Other	6.67%

Data analysis – impact

	date	title	impactful	other	total
1	2023-11-09	Modern Asian APT groups tactics, techniques and procedures	7	14	21
2	2023-01-18	Qihoo 360 - APT Annual Research Report	3	1	4
3	2023-03-24	(ransomware) APT attacks on industrial organizations in H2 2022	3	1	4
4	2023-01-31	Dalbit m00nlight Chinese hacker groups APT attack campaign	3	0	3
5	2023-02-13	Nice Try Tonto Team	3	0	3
6	2023-09-22	Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambiti	3	0	3
7	2023-06-01	SharpPanda APT Campaign Expands its Arsenal Targeting G20 Nations	3	0	3
8	2023-04-20	Xiaoqiying Genesis Day Threat Actor Group Targets South Korea, Taiwan	3	1	4
9	2023-10-18	Updated MATA attacks industrial companies in Eastern Europe	2	0	2
10	2023-07-13	APT Exploit Targeting Rockwell Automation Flaws Threatens Critical Infrastructure	2	0	2
11	2023-04-18	Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets	2	2	4
12	2023-08-22	Analysis of APT Attack Cases Targeting Web Services of Korean Corporations	2	1	3
13	2023-03-23	(ransomware) UNC961 in the Multiverse of Mandiant Three Encounters with a Financial	2	4	6
14	2023-02-02	No Pineapple! - DPRK Targeting of Medical Research and Technology Sector	2	2	4

Data analysis – impactful threat reports

- Out of 60 reports that mentioned CVEs, 38 had corresponding data showing some impact.
- Bigger impact is proportional to the amount of included vulnerabilities
  - So annual reports or an aggregation of cases will be more impactful
- If ransomware is involved, higher impact
- Impactful reports can come from any region
- Many of them are from smaller but specialized organizations
- Impact is observed rather quickly
  - E.g., A report published in November is still impactful in the same year

Data analysis – impactful threat reports

- Why do certain reports despite having great findings don't get attention in the security community?
  - The vulnerability was already well-known and patched by users
  - Visibility of some specific software in telemetry could be poor, e.g., certain regions
  - No detection plugin was developed during the described event

Information sharing - how to improve

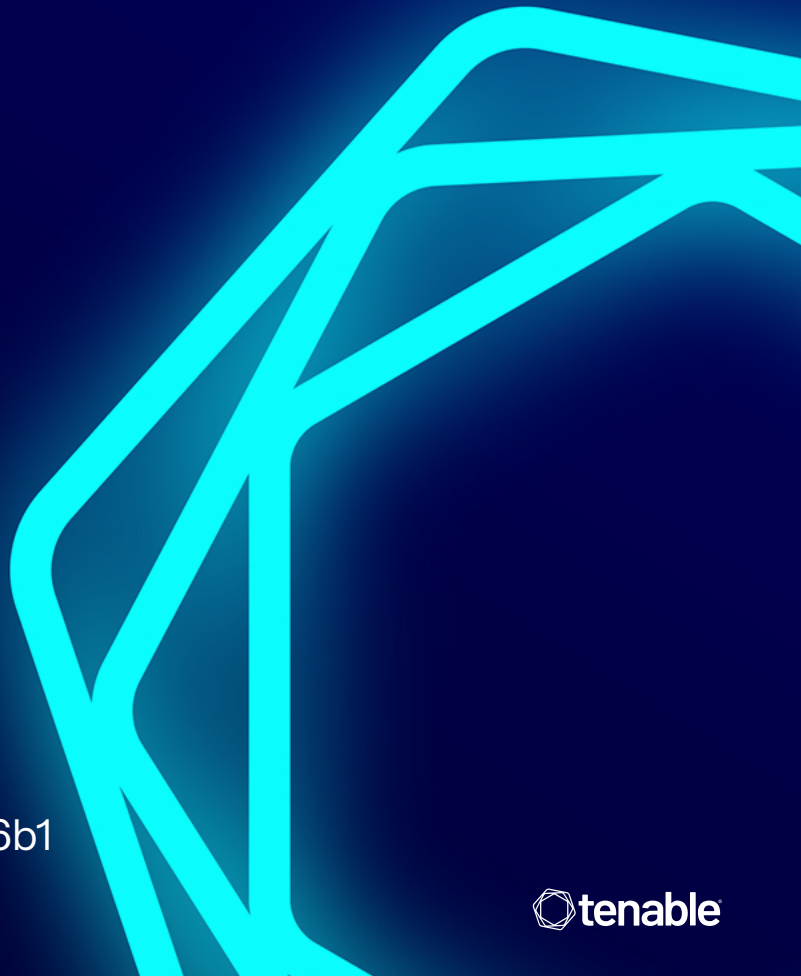
- The impact of the publishing source
  - Does it depend on the publisher?
  - Nation-state, zero-day, targets, ransomware
- Unify threat reports publications
  - Currently researchers have to track multiple sources so new sources can be overlooked
  - Include the threat report source type (ransomware, APT) and publisher

Questions?

tenable

Thank you!

sgrzonkowski@tenable.com
https://ie.linkedin.com/in/slawomir-grzonkowski-a0416b1



tenable