New Research Methods to Predict Attack Trends Using Public Information

1/25/2023
Macnica Corporation
Yutaka Sejiyama

Co.Tomorrowing

self-introduction

Yutaka Sejiyama

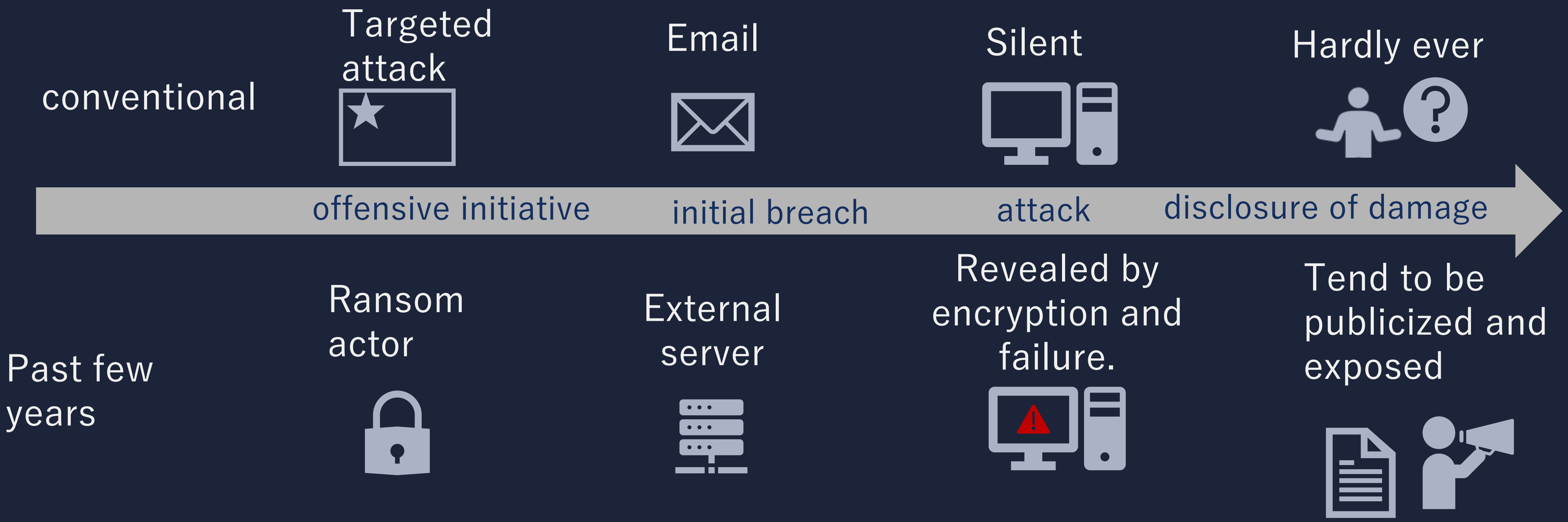
✓ **Collect and disseminate information on security threat trends**
Vulnerability-related threat trend research
Twitter @nekono_naha
The Society for the Collection of Scattered E-mails
(ISC)2 Japan Chapter Annual Conference 2022

nekono_nanomotoni
@nekono_naha

✓ Macnica Group Global CSIRT Officer
Responding to security incidents in Japan and overseas
Patch Management

✓ Macnica's own security service planning and management
Investigation of external public servers, etc.

Major trend changes over the past few years



conventional

Targeted attack

Email

Silent

Hardly ever

offensive initiative

initial breach

attack

disclosure of damage

Past few years

Ransom actor

External server

Revealed by encryption and failure.

Tend to be publicized and exposed

Incident information tends to become public for various reasons.
Can we capture attack trends and tactical changes by using public information?

Agenda for this session

✓Part 1: Analysis of recent incident occurrence trends

Leaked information by the Ransom Gang
Press Release on Damage by Japanese Companies
Public reports from security agencies/vendors

✓Part 2: Changes in the management of externally disclosed assets

RDP Publication Status
Use of out-of-support OS
Change in speed of vulnerability response (2020 vs 2022)
Status of Measures Taken by Japanese Companies

✓Part 3: Attempting to capture the attacker's change in tactics

Past survey cases (Pandora, AvosLocker, Deadbolt)
Share how to research with device search engines

Agenda for this session

✓Part 1: Analysis of recent incident occurrence trends

Leaked information by the Ransom Gang
Press Release on Damage by Japanese Companies
Public reports from security agencies/vendors

✓Part 2: Changes in the management of externally disclosed assets

RDP Publication Status
Use of out-of-support OS
Change in speed of vulnerability response (2020 vs. 2022)
Status of Measures Taken by Japanese Companies

✓Part 3: Attempting to capture the attacker's change in tactics

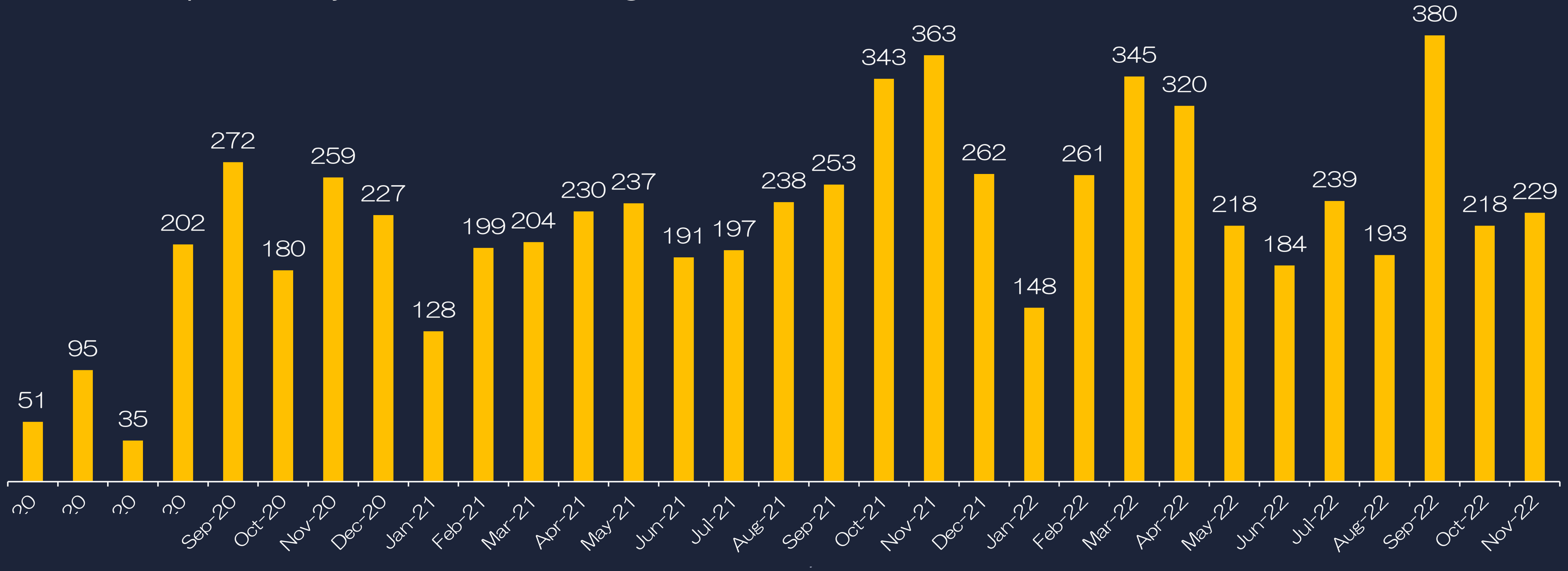
Past survey cases (Pandora, AvosLocker, Deadbolt)
Share how to research with device search engines

Number of global leaks by ransom actors

✓ Ransomware attacks, which are targeted ransoms against individual companies and industries and double threats through data encryption and information leakage, are on the rise worldwide.

✓ **Approximately 6932** exposed ransom victims (listed on the leak site) as of the end of November 2022
*Based on data from intelligence vendor DarkTracer (https://darktracer.com/)

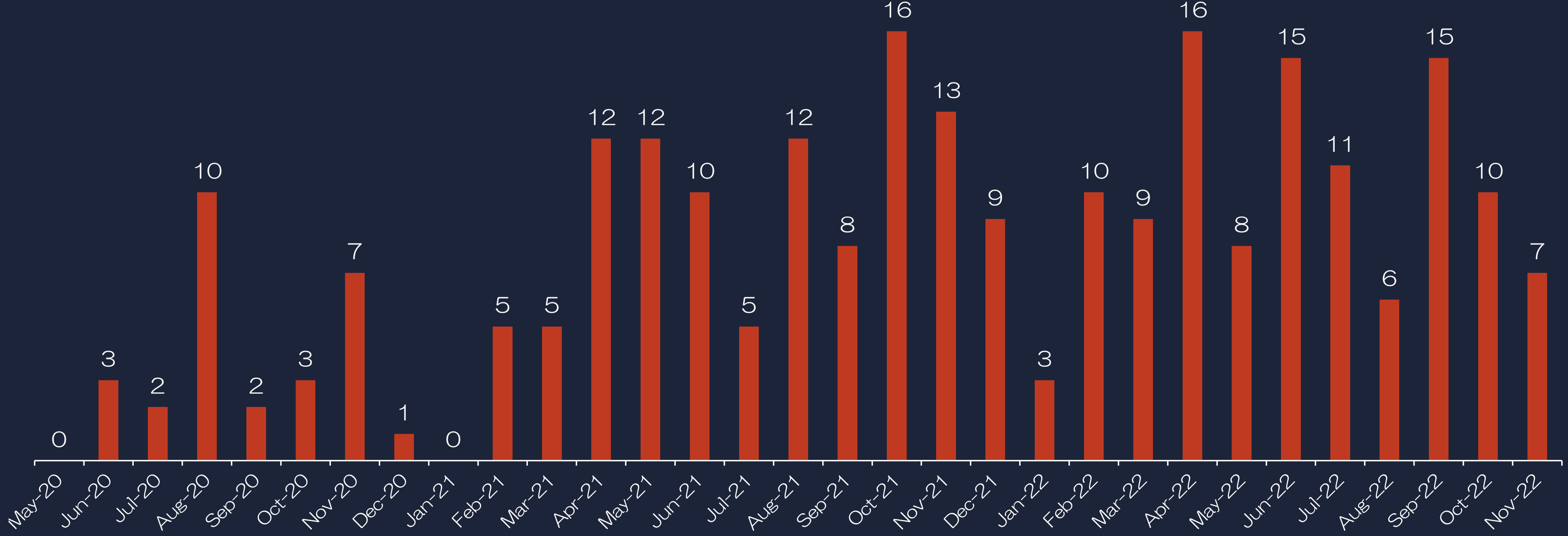
✓ If we include the number of affected companies by ransomware that has not been leaked, the number of affected companies may be several times higher than the above.



Ransom-related incidents in Japanese companies and organizations

✓ As far as we can confirmed from public information, there were **245 security incidents**

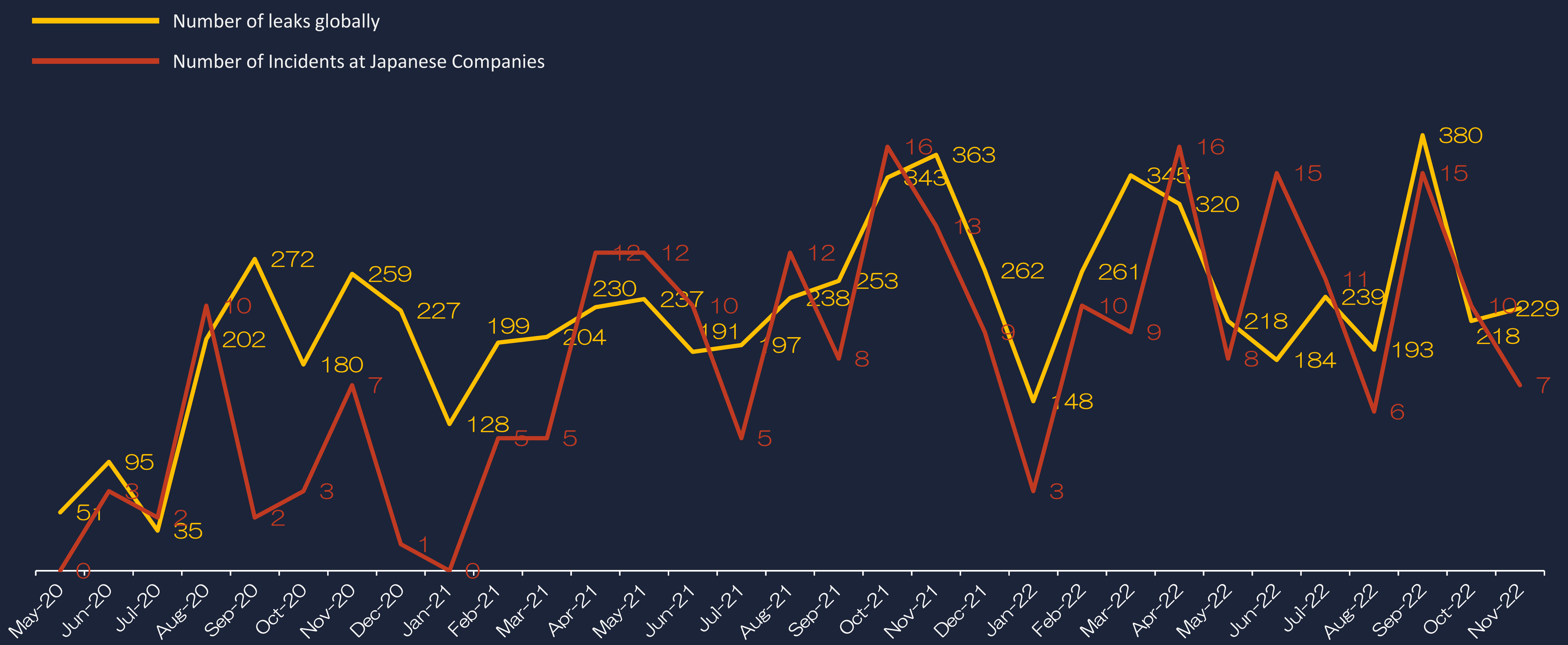
- Aggregated press releases from companies and organizations, as well as ransomware attackers' dark web statements
- Aggregated ocorporate NW intrusion incidents, mainly ransom attacks and a small number of APTs. *Excluding cases of website tampering, information leaks via websites, and Emotet infections.
- Aggregated for 31 months from May 2020 to November 2022.
- Press releases are collected using Google Alerts, news, and researcher information (@piyokango, @autumn_good_35).



Comparison of Incident Occurrence Trends

- The number of victims is increasing globally, and that of Japan increase/decrease with the global trends.

✓ Comparison of the number of incidents at global and Japanese organizations

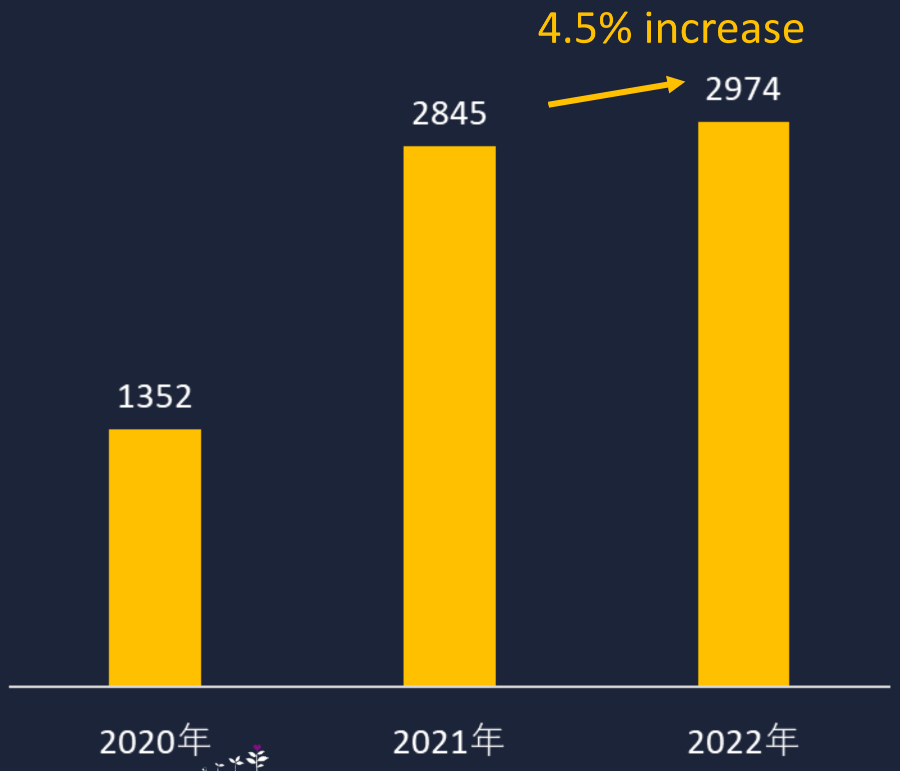


Incident Occurrence Trend Analysis *This slide only includes the number of incidents in December 2022.

- In 2022, the number of cases increased slightly both globally and in Japan
- The number of cases is slightly higher domestically than globally

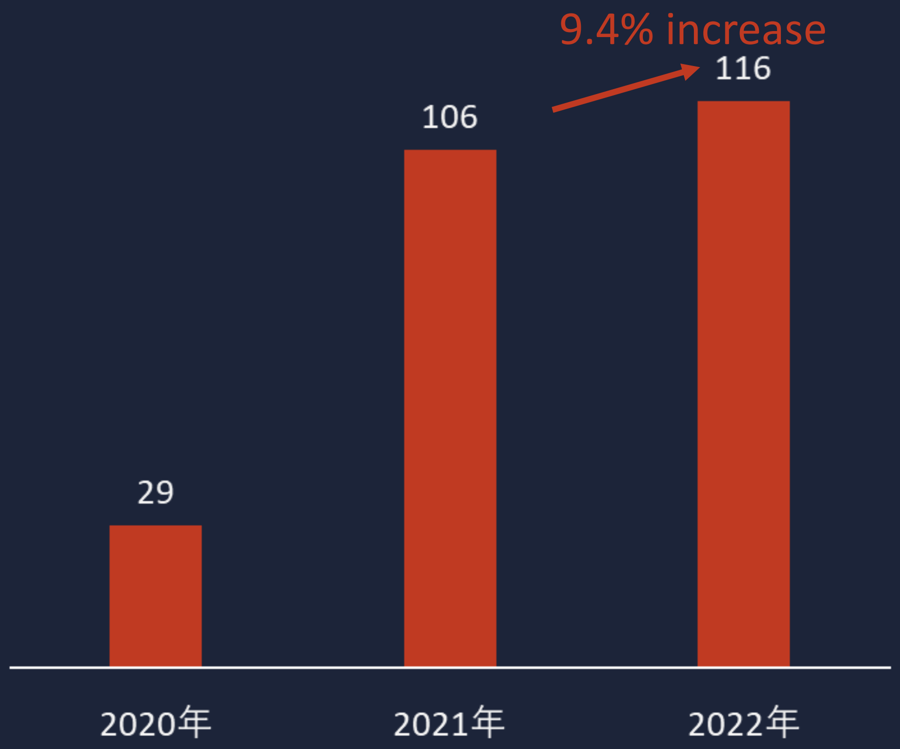
✓ Number of global (per year)

*Number of cases from January 2020 to December 2022



✓ Number of cases in Japanese organizations (per year)

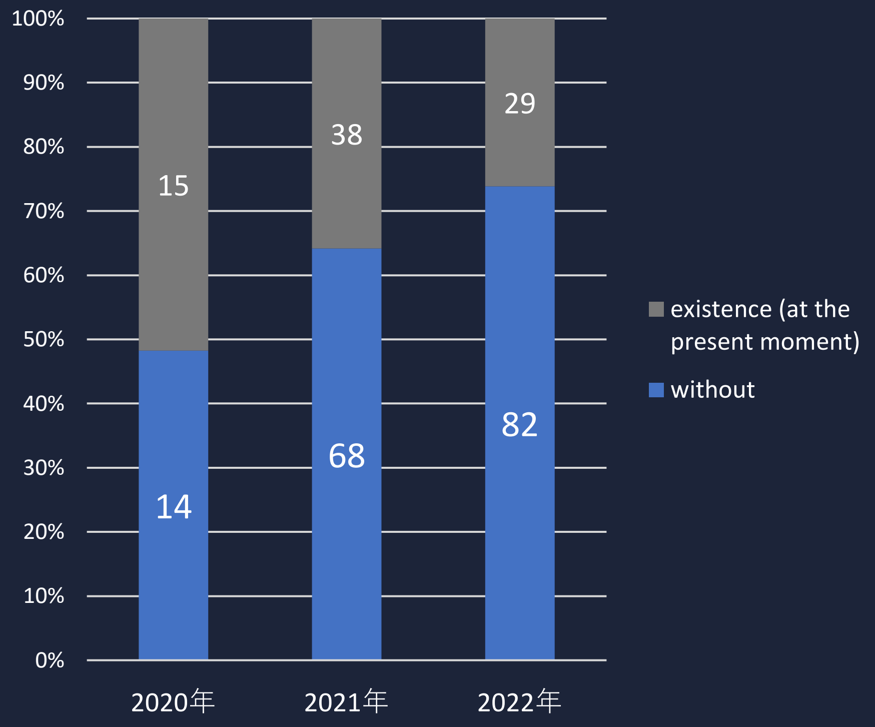
*For 2022, for the period known up to January 3, 2023.
Likely to increase by several more.



Incident Trends in Japanese Organizations

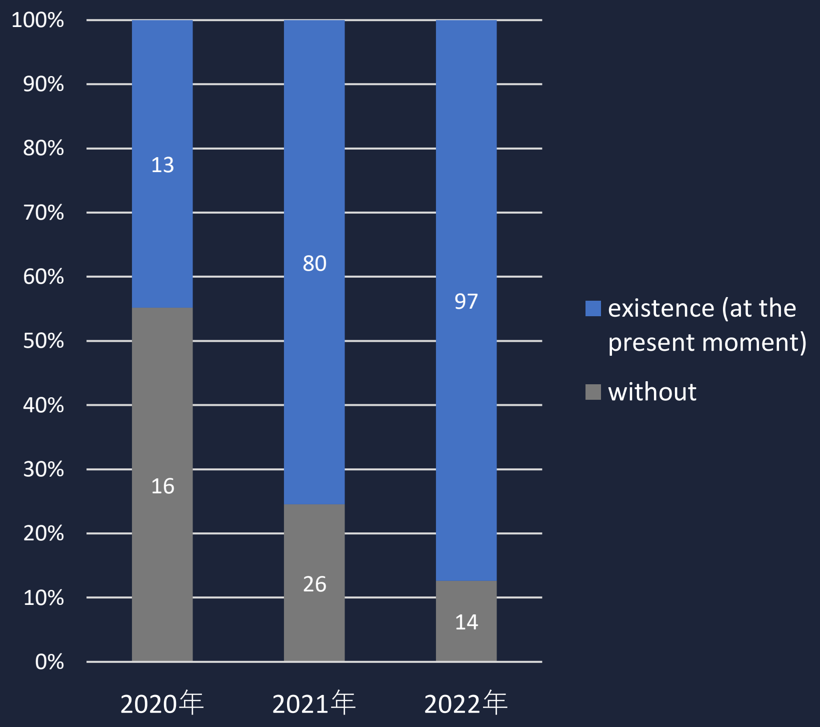
- The percentage of ransom incidents that are discovered through leaks by attackers is decreasing year by year, while the number of incidents disclosed by companies is increasing.
- The increase in the rate of public disclosure may be due to a change in the public perception of ransom incidents.

✓ Number of leaks of Japanese organizations by attackers



Only about 1/4 is leaked ≈ 4 times larger actually?
*Total damage in 2022: 2,275 x 4 = 9,100

✓ Number of publications in press releases by Japanese-affiliated organizations



Only about 1/4 is disclosed* ≈ 4 times larger actually?

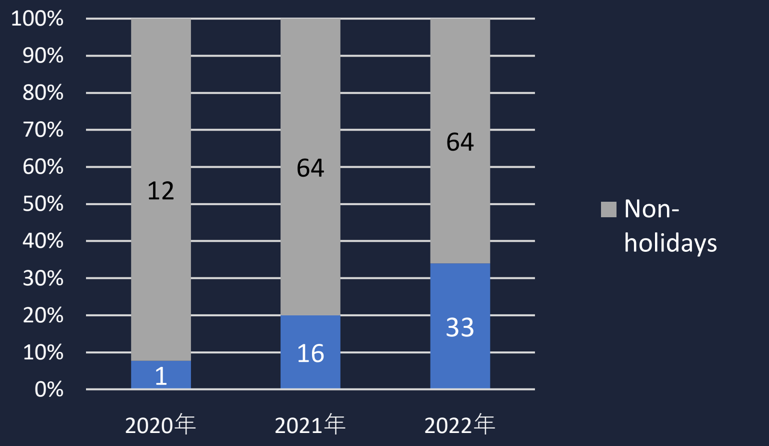
*ExtraHop 2022 CYBER CONFIDENCE INDEX:
ASIA PACIFIChttps://assets.extrahop.com/pdfs/industry-reports/cyber-confidence-index-apac.pdf

Press release analysis of Japanese-affiliated organizations

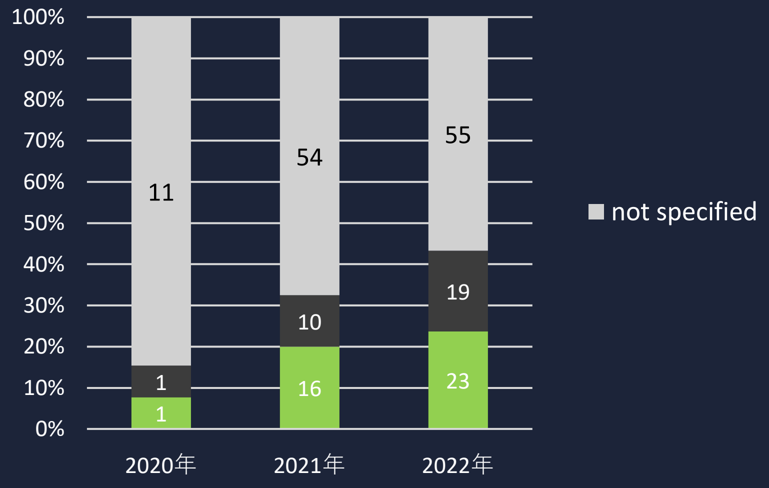
*Analysis of 190 ransom-related press releases published between April 2020 and November 2022.

- The number of attacks targeting unoccupied time zones such as holidays, national holidays, nighttime, and early morning is increasing every year.
- This is thought to be a change in the attacker's tactic to expand the scope of damage (number of hosts and files to be encrypted) by delaying recognition and response.

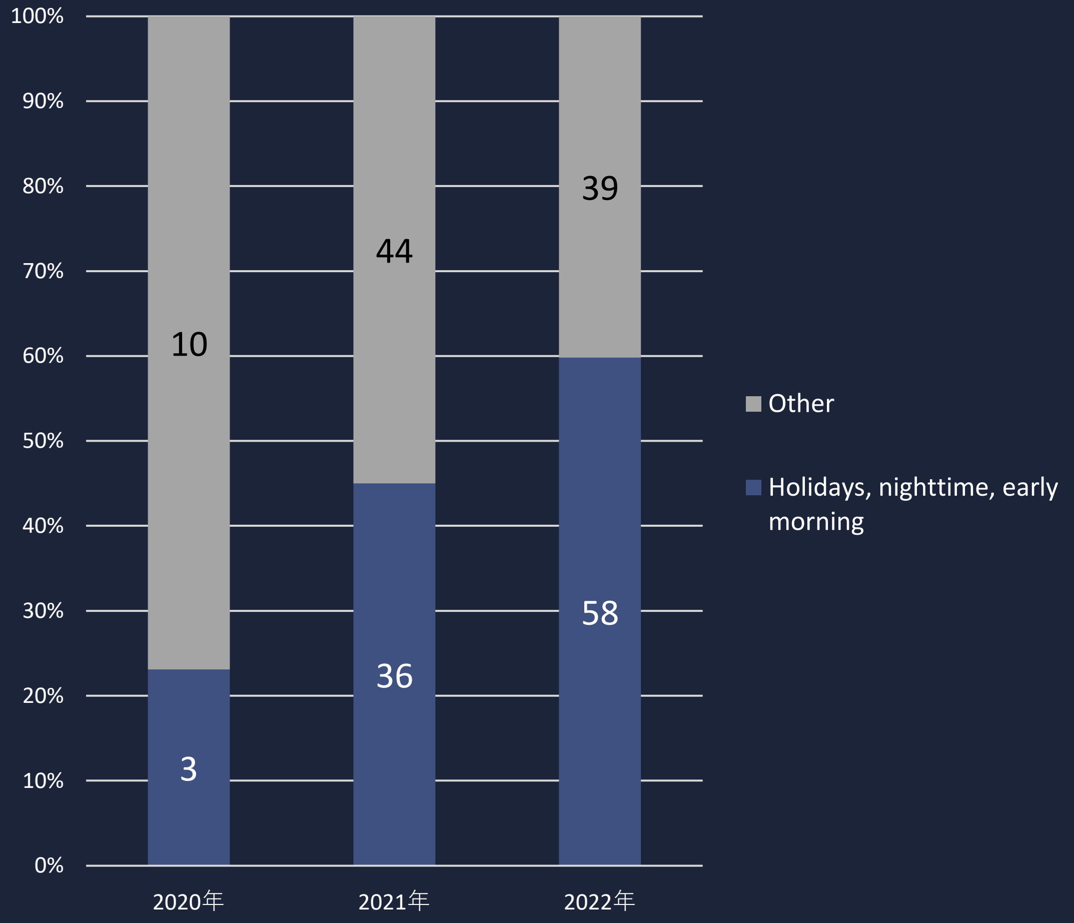
✓ Date of attack



✓ Attack Time



✓ Attacks at night, early mornings, holidays, etc.



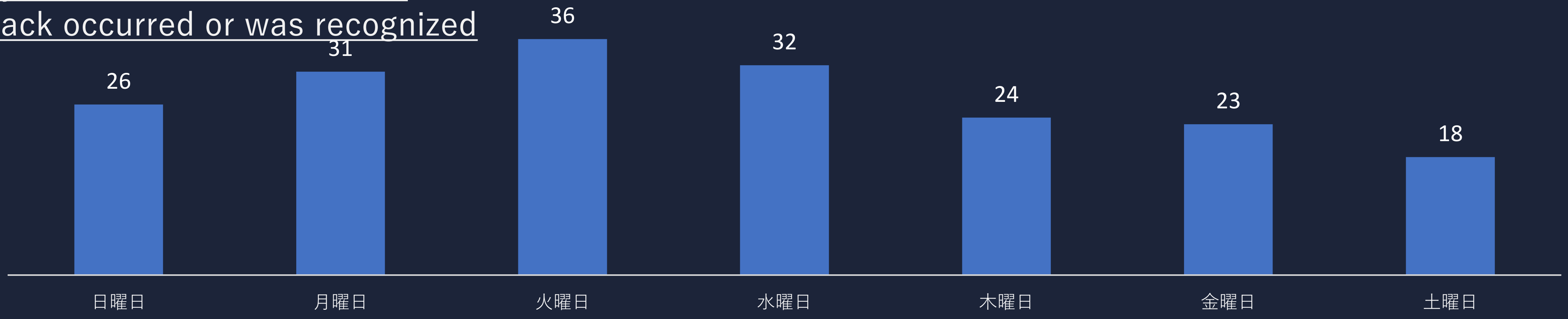
Press release analysis of Japanese-affiliated organizations

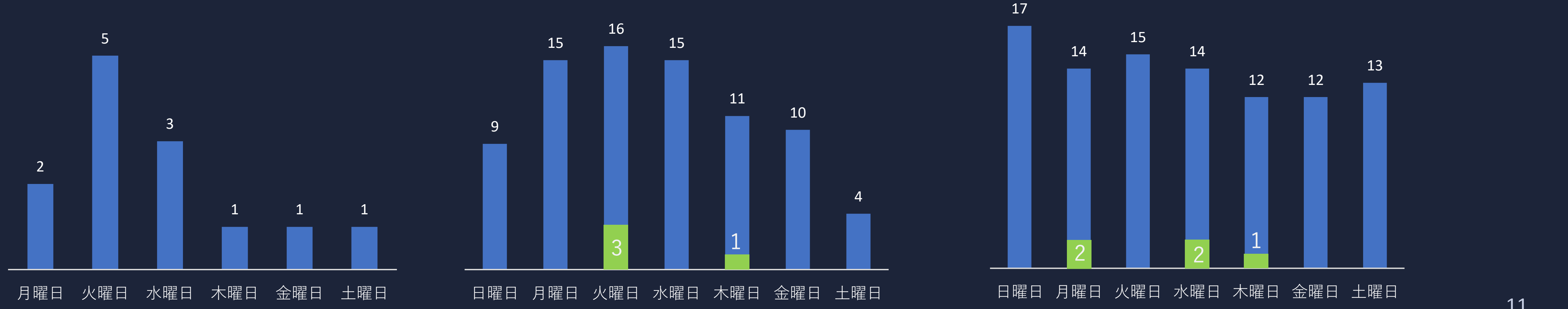
*Analysis of 190 ransom-related press releases published between April 2020 and November 2022.

- The tendency to target attacks on Saturdays, Sundays, and Fridays instead of weekdays is growing stronger every year.
- This is thought to be a change in the attacker's tactics to expand the scope of damage (number of hosts and files to be encrypted).

[

attack occurred or was recognized




✓2020

✓2021

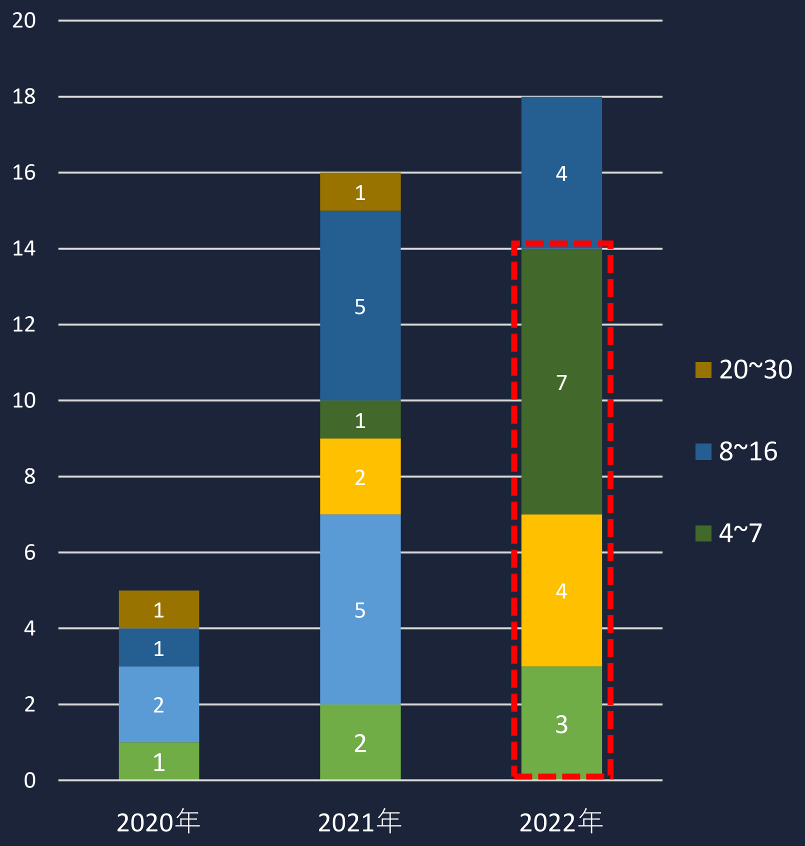
✓2022

Press release analysis of Japanese-affiliated organizations

*Analysis of 190 ransom-related press releases published between April 2020 and November 2022.

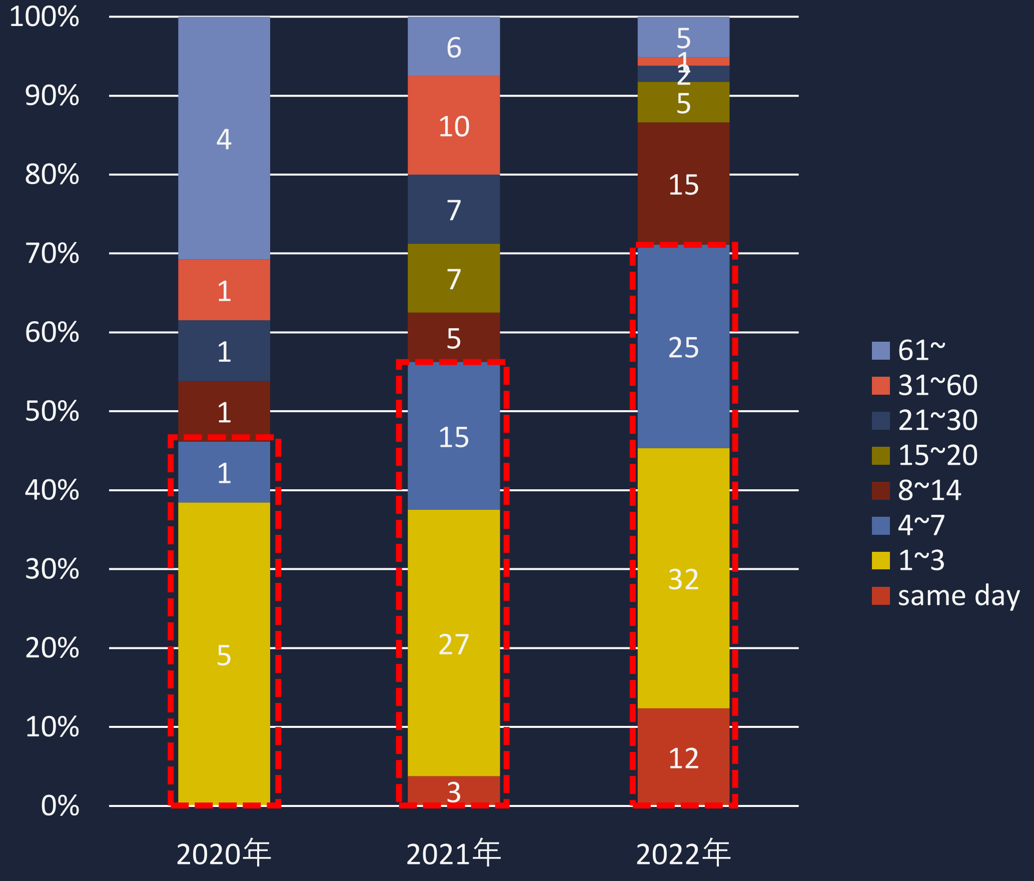
✓ Number of days from attack recognition to leak occurrence

*Total of 39 cases with leaks and press releases



- Within a week (red box) is higher 2022.

✓ Number of days from attack recognition to press release

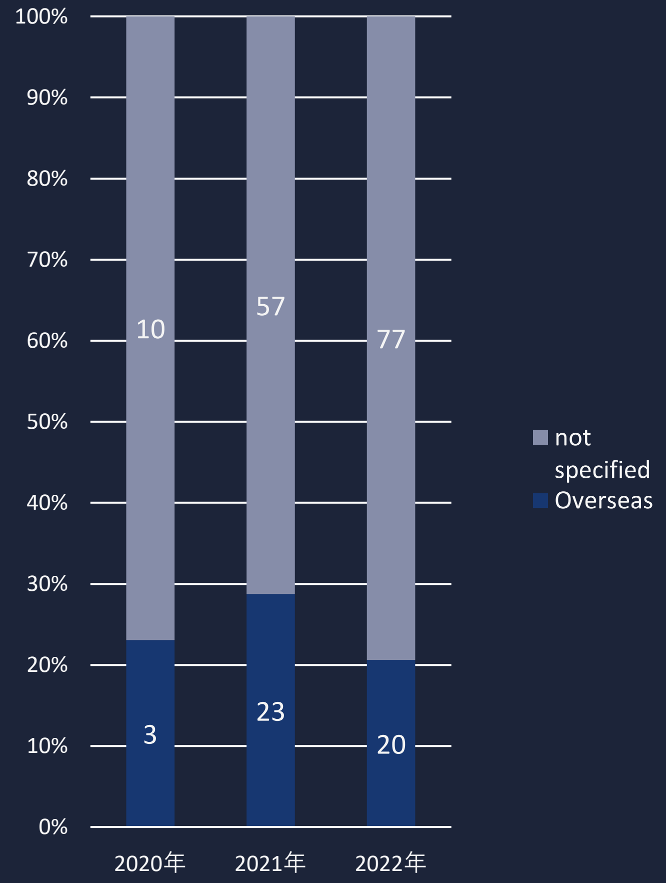


- The interval between attack recognition and pressing is also getting shorter.
- In 2022, 70% will be published within a week (red box)
- To lower psychological barriers made early incident disclosure or to make the business impact known?

Press Release Content Analysis of Japanese Companies

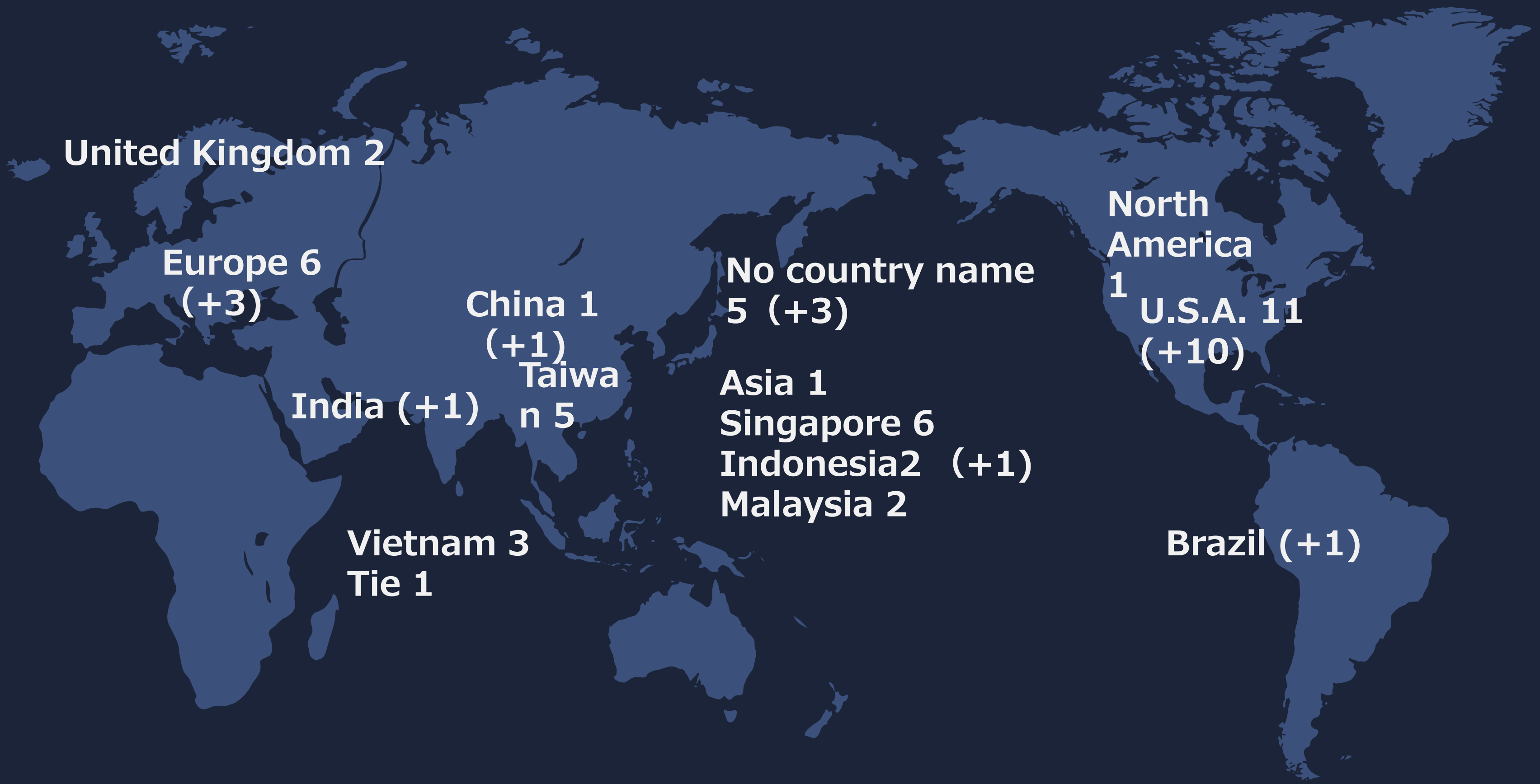
- In the past, about 30% of the damage was done overseas, but by 2022, the percentage of damage specified for overseas locations has dropped to 20%.
- This may be due in part to the fact that attackers are beginning to shift their targets from mainly large corporations to smaller organizations as their tactics change.

✓Declaration of Damage Base



✓ Distribution of sites where damage occurred

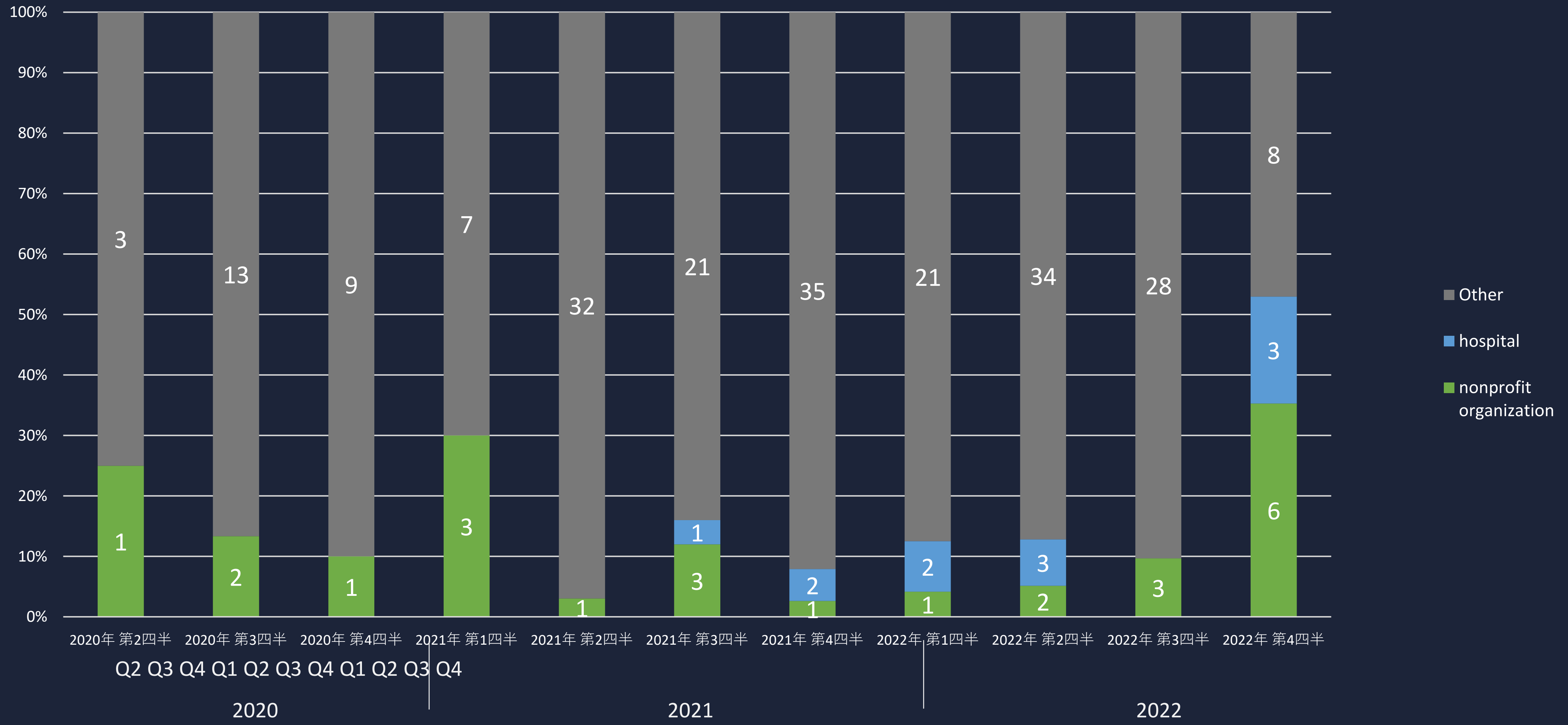
*Numbers in parentheses indicate the number of cases that were not in the press but were revealed by leaks.



Trends in Incident Occurrence at Japanese Companies

*Analysis of 245 ransom press releases and leaks that can be confirmed from April 2020 to November 2022.

- Previously in 2022 Q4, hospitals and non-profit organizations (~unions, institutions, associations, and schools) were most often affected.
- It is possible that the damage is not targeted at large organizations, but at small organizations, or by stray bullets.



Percentage of incidents that occur via external public assets

- Extracting data from public IR reports issued by various security-related organizations on the causes of incidents
- Percentage of incidents (yellow letters) originating from external servers is not small

issuing authority	Publication Date	report-name	Percentage of external public servers and vulnerabilities were the cause		Other	uniform resouce locator
SecureWorks	October 2022	2022 State of the Threat: A Year in Review	52%	Exploitation of remote services 52	Credentials 39% , Commodity malware infection 3% Drive by download 2% , Phishing 2% , Network misconfiguration 2%	https://www.secureworks.com/resources/rp-state-of-the-threat-2022
Trend Micro	October 2022	Compromise of network equipment leading directly to intrusion:. Beware of a new vulnerability, CVE-2022-40684	50% of	Via network devices 25 Via RDP 25	Via e-mail 4%, other 13%, unknown 33	https://www.trendmicro.com/ja_jp/research/22/j/fortinet.html
National Police Agency	September 2022	Threats to Cyberspace in the First Half of 2022	83%	VPN equipment 32 cases (68%) Remote desktop 7 cases (15%)	Suspicious e-mails and their attachments 4 cases (9%) Other 4 cases (9%)	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf
COVEWARE	July 2022	Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022	50%	RDP Compromise approx. ~30 Software Vulnerability approx. 20%+ Software Vulnerability approx. 20%+	Email Phishing approx. 30%～ Other: approx. 20%+	https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022
Palo Alto	July 2022	Attackers Move Quickly to Exploit High-Profile Zero Days: Insights From the 2022 Unit 42 Incident Response Report	46%.	Software vulnerabilities 31 Brute force credential attacks 9%. Previously leaked credentials 6%.	Phishing 37%, Insider Threats 5%, Social Engineering 5%, Abuse of Trusted Relationships/Trusted Tools 4%, Other 3%.	https://unit42.paloaltonetworks.jp/incident-response-report/
SOPHOS	June 2022	The Active Adversary Playbook 2022	55%	Exploited Vulnerability 47 Compromised Credentials 5% Brute Force Attack 3%	Unknown 36%, Phishing 8%, Download 1%	https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/
Arctic Wolf	June 2022	Q1 2022 Incident Response Insights from Tetra Defense	82%	External Vulnerabilities 57 RDP 25	long vowel mark (usually only used in katakana)	https://arcticwolf.com/resources/blog/q1-2022-incident-response-insights-from-tetra-defense
Group-IB	May 2022	Ransomware Uncovered 2021/2022	68%.	External remote services 47 Exploit public-facing applications 21	Phishing 26%, Other 6%.	https://www.group-ib.com/media-center/press-releases/ransomware-2022/
National Police Agency	April 2022	Threats to Cyberspace in 2021	74%.	VPN equipment 41 cases (54%) Remote desktop 15 cases (20%)	Suspicious e-mails and their attachments 5 cases (4%) Others 15 cases (20%)	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
IBM	January 2022	X-Force Threat Intelligence Index 2022	53%.	Vulnerability exploitation 47 Stolen credentials 3% Brute force 3%	Phishing 40%, Removable media 7%.	https://www.ibm.com/reports/threat-intelligence/
Kaspersky	September 2021	Incident response analyst repot	63%.	brute force attacks 31.6 Vulnerability exploits 31.5	Malicious emails 23.7%, drive-by downloads 7.89%, removable media 2.63%, insiders 2.63	https://media.kaspersky.com/jp/pdf/pr/Kaspersky_IRAnalystReport2020-PR-1056.pdf
COVEWARE	April 2021	Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound	70%	RDP Compromise approx. ~50 Software Vulnerability approx. 20-percent	Email Phishing approx. 30 Other approx. 5	https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

Warning reports on vulnerability exploitation trends

- 25 reports on vulnerability exploitation trends over the past few years were compiled and the number of times they appeared in each product was investigated.
  Only information on exploits in incidents is collected, excluding reports on the number of detected communications that exploit vulnerabilities in NW products and anti-virus software.

No	period of issue	report-name	Publication Date	uniform resouce locator
1	CISA	CISA Alets	2022-2022	https://www.cisa.gov/uscert/ncas/alerts
2	Fortinet	Zerobot - New Go-Based Botnet Campaign Targets Multiple Vulnerabilities	Dec-22	https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities
3	CISA	Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester	Nov-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-320a
4	CISA	StopRansomware: Hive	Nov-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
5	CISA	Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors	Oct-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-279a
6	Arctic Wolf	Root Point Product of Compromise	Sep-22	https://arcticwolf.com/resources/blog/incident-response-insights-from-arctic-wolf-labs-1h-2022/
7	CISA	Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Disk Encryption for Ransom Operations	Sep-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-257a
8	Palo Alto	Unit 42	Jul-22	https://unit42.paloaltonetworks.jp/incident-response-report/
9	Group IB	Ransomware Uncovered2021/2022	Jun-22	https://www.group-ib.com/resources/threat-research/ransomware-2022.html
10	CISA	People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices	Jun-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-158a
11	IBM	X-Force Research Update: Top 10 Cybersecurity Vulnerabilities of 2021	May-22	https://securityintelligence.com/posts/x-force-top-10-cybersecurity-vulnerabilities-2021/
12	CISA	2021 Top Routinely Exploited Vulnerabilities	Apr-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-117a
13	Tenable	Behind the Scenes: How We Picked 2021's Top Vulnerabilities - and What We Left Out	Mar-22	https://www.tenable.com/blog/behind-the-scenes-how-we-picked-2021s-top-vulnerabilities-and-what-we-left-out
14	ANSSI	Panorama de la menace informatique 2021	Mar-22	https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
15	CISA	Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure	Jan-22	https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
16	Recorded Future	2021 Vulnerability Landscape	Jan-22	https://go.recordedfuture.com/hubfs/reports/cta-2022-0210.pdf
17	CISA	Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities	Nov-21	https://www.cisa.gov/uscert/ncas/alerts/aa21-321a
18	Twitter	Top Critical Vulnerabilities Used by Ransomware Groups	Sep-21	https://twitter.com/uuallan/status/1438899102448820224
19	CISA	Top Routinely Exploited Vulnerabilities	Jul-21	https://www.cisa.gov/uscert/ncas/alerts/aa21-209a
20	National Institute of Standards and Certification	Alert Concerning Ransomware Cyber Attacks	Apr-21	https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf
21	Tenable	IN THE 2020 THREAT LANDSCAPE RETROSPECTIVE (TLR), YOU WILL READ ABOUT:	Jan-21	https://www.tenable.com/cyber-exposure/2020-threat-landscape-retrospective
22	CISA	Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets	Oct-20	https://www.cisa.gov/uscert/ncas/alerts/aa20-296a
23	CISA	APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations	Oct-20	https://www.cisa.gov/uscert/ncas/alerts/aa20-283a
24	CISA	Potential for China Cyber Response to Heightened U.S.-China Tensions	Oct-20	https://www.cisa.gov/uscert/ncas/alerts/aa20-275a
25	CISA	Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity	Sep-20	https://www.cisa.gov/uscert/ncas/alerts/aa20-258a

Warning reports on vulnerability exploitation trends

- 25 reports on vulnerability exploitation trends over the past few years were compiled and the number of appearances (in yellow) for each product was investigated. Only information on exploits in incidents is collected, excluding reports on the number of detected communications that exploit vulnerabilities in NW products and anti-virus software.

Product	frequency	Report Number																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Exchange Server	19	ProxyLogon			ProxyShell	ProxyLogon,ProxyShell	ProxyShell	ProxyShell	ProxyShell,ProxyLogon	ProxyLogon,ProxyShell		ProxyLogon,ProxyShell	ProxyShell,ProxyLogon,CVE-2020-0688	ProxyLogon	PropxyLogon	ProxyLogon,CVE-2020-0688	ProxyLogon	ProxyShell	ProxyShell,ProxyLogon		ProxyLogon		CVE-2020-0688		CVE-2020-0688	CVE-2020-0688
Citrix	14	CVE-2019-19781				CVE-2019-19781					CVE-2019-19781	CVE-2019-19781	CVE-2019-19781			CVE-2019-19781			cve-2019-19781,cve-2020-8195,cve-2020-8196,cve-2019-11634	CVE-2019-19781	CVE-2019-19781	CVE-2019-19781	CVE-2019-19781	CVE-2019-19781	cve-2019-19781,cve-2020-8193,cve-2020-8195,cve-2020-8196	CVE-2019-19781
Pulse Secure Pulse Connect Secure	14	CVE-2021-22893,. CVE-2020-8260, CVE-2020-8243, CVE-2019-11510				CVE-2019-11510					cve-2019-11510,cve-2021-22893		cve-2019-11510,cve-2021-22893	CVE-2021-22893	CVE-2021-22893	CVE-2019-11510			CVE-2021-22893,. CVE-2020-8260, CVE-2020-8243, CVE-2019-11510, CVE-2019-11539	CVE 2019-11510	CVE-2021-22893,. CVE-2020-8260, CVE-2020-8243, CVE-2019-11510	CVE-2019-11510		CVE-2019-11510	CVE-2019-11510	CVE-2019-11510
Fortinet	13				CVE-2020-12812				not specified		CVE-2018-13382		CVE-2018-13379		CVE-2018-13379	CVE-2018-13379		cve-2018-13379, cve-2020-12812, cve-2019-5591	cve-2018-13379, cve-2020-12812, cve-2019-5591	CVE 2018-13379	CVE-2018-13379	CVE-2018-13379	CVE-2018-13379	CVE-2018-13379		
F5 Big-IP	10	cve-2022-1388,cve-2020-5902	CVE-2022-1388			cve-2020-5902,cve-2022-1388										CVE-2020-5902			cve 2020-5902, cve-2021-22986	CVE 2020-5902		CVE-2020-5902		CVE-2020-5902	CVE-2020-5902	CVE-2020-5902
Log4j (including VMHorizon)	9	CVE-2021-44228		CVE-2021-44228		CVE-2021-44228	CVE-2021-44228	CVE-2021-44228	not specified			CVE-2021-44228	CVE-2021-44228				CVE-2021-44228									
Accellion FTA	6	cve-2021-27101cve-2021-27102,cve-2021-27103,cve-2021-27104								CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104		CVE-2021-27101	cve-2021-27104,cve-2021-27103,cve-2021-27102,cve-2021-27101	cve-2021-27101, cve-2021-27102, cve-2021-27103, cve-2021-27104					cve-2021-27104,cve-2021-27103,cve-2021-27102,cve-2021-27101							
SonicWall	6								not specified	CVE-2021-20016			cve-2021-20038,cve-2021-20016	CVE-2021-20016					cve-2021-20016, cve-2020-5135, cve-2019-7481		CVE-2021-20016					
VMware vCenter Server	6					CVE-2021-22005							CVE-2021-21985.	CVE-2021-21985.	CVE-2021-21985.		CVE-2021-22005		CVE-2021-21985.							
ZOHO ManageEngine ADSelfService	6	CVE-2021-40539				CVE-2021-40539	CVE-2021-40539		not specified				CVE-2021-40539						CVE-2021-40539							

Warning reports on vulnerability exploitation trends

- 25 reports on vulnerability exploitation trends over the past few years were compiled and the number of appearances (in yellow) for each product was investigated. Only information on exploits in incidents is collected, excluding reports on the number of detected communications that exploit vulnerabilities in NW products and anti-virus software.

Product	frequency	Report Number																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Atlassian Confluence Server and Data Center	5					cve-2022-26134,cve-2021-26084				CVE-2021-26084			CVE-2021-26084						CVE-2021-26084						CVE-2019-3396	
Cisco	5					CVE-2021-1497					cve-2018-0171,cve-2019-1652,cve-2019-15271		CVE-2018-0171			CVE-2019-1653									cve-2019-1652,cve-2019-1653,cve-2020-3118	
MobileIron	4											CVE-2020-15505								CVE 2020-15505				CVE-2020-15505	CVE-2020-15505	
QNAP QTS and QuTS hero	4										cve-2019-7192,cve-2019-7193,cve-2019-7194,cve-2019-7195		CVE-2020-2509						cve-2020-36198, cve-2021-28799		cve-2021-28799, cve-2020-36195, cve-2020-2509					
Exim	3															CVE-2019-10149							CVE-2019-10149		CVE-2018-6789	
D-Link	3		CVE-2020-25506								CVE-2019-16920														CVE-2019-16920	
Atlassian Crowd and Crowd Data Center	2																			CVE-2019-11580					CVE-2019-11580	
DrayTek	2										CVE-2020-8515														CVE-2020-8515	
GitLab CE/EE	2					CVE-2021-22205											CVE-2021-22205									
Kaseya VSA	2									CVE-2021-30116				cve-2021-30116, cve-2021-30119, cve-2021-30120												

Warning reports on vulnerability exploitation trends

- 25 reports on vulnerability exploitation trends over the past few years were compiled and the number of appearances (yellow letters) for each product was investigated. Only information on exploits in incidents is collected, excluding reports on the number of detected communications that exploit vulnerabilities in NW products and anti-virus software.

Product	frequency	Report Number																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Oracle WebLogic Server	2															cve-2019-2725,cve-2020-14882									CVE-2015-4852	
Palo Alto	2																		CVE-2019-1579, CVE-2020-2021					CVE-2020-2021		
Progress Telerik UI	2												CVE-2019-18935												CVE-2019-18935	
Sitecore XP	2					CVE-2021-42237							CVE-2021-42237													
VMware Workspace ONE Access	2	cve-2022-22954,cve-2022-22960														CVE-2020-4006										
Zimbra	2	cve-2022-24682,cve-2022-27924,cve-2022-37042,cve-2022-27925,cve-2022-30333														CVE-2019-9670										
Zoho ManageEngine ServiceDesk Plus	2	CVE-2021-44077																							CVE-2020-10189	
ForgeRock OpenAM server	2											CVE-2021-35464	CVE-2021-35464													
Hikvision Webserver	2		CVE-2021-36260			CVE-2021-36260																				
Zyxel.	2		CVE-2022-30525								CVE-2020-29583															

Agenda for this session

✓ Part 1: Analysis of recent incident occurrence trends

Leaked information by the Ransom Gang
Press Release on Damage by Japanese Companies
Public reports from security agencies/vendors

✓ Part 2: Changes in the management of externally disclosed assets

RDP Publication Status
Use of out-of-support OS
Change in speed of vulnerability response (2020 vs. 2022)
Status of Measures Taken by Japanese Companies

✓ Part 3: Attempting to capture the attacker's change in tactics

Past survey cases (Pandora, AvosLocker, Deadbolt)
Share how to research with device search engines

Survey on RDP 3389/TCP

Survey the number of servers and PCs that expose RDP (3389/TCP) to the outside world using Shodan

- Globally, there are 4.3 million cases and approximately 120,000 units in the domestic market.
- In Japan, the number of cases increased significantly around the time of the Corona disaster, but peaked at 143,671 in March 2021 and has been on a downward trend since then.
- While many of the PCs are for personal use, we can clearly see at least 500 PCs that are used by at least 500 companies.

Top 30 countries with the highest number of3389/TCPs published

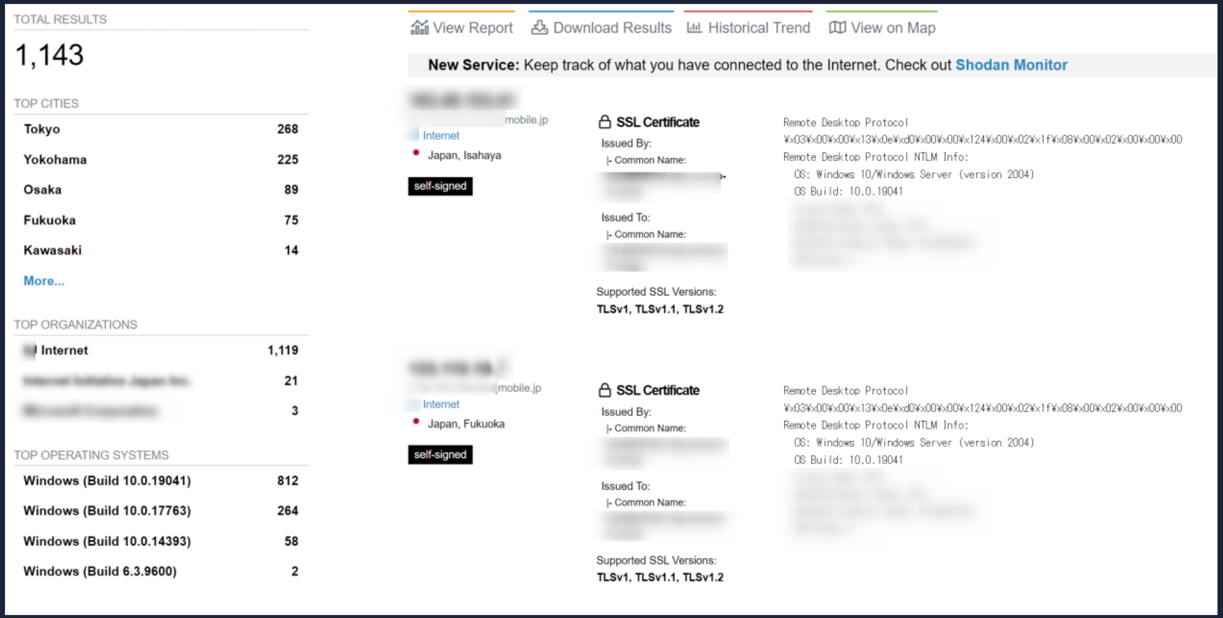
Country		Nov-2019	May-2020	Nov-2020	May-2021	Nov-2021	May-2022	Nov-2022	fluctuation
	Global	5,548,173	5,246,373	4,574,509	5,326,991	4,872,514	4,629,133	4,329,536	-22%.
1	United States	2,465,109	1,775,745	1,512,654	1,675,269	1,641,343	1,398,938	1,281,178	-48%
2	China	1,252,901	1,485,333	1,137,537	1,412,295	1,274,560	1,216,480	1,234,529	-1%.
3	Germany	157,910	195,439	190,848	224,883	213,436	219,561	204,047	29%
4	Japan	95,499	106,456	109,979	128,105	127,740	122,696	120,375	26%.
5	Netherlands	108,227	123,904	117,754	150,779	135,745	126,445	112,322	4%
6	UK	97,892	110,345	128,085	135,266	118,249	123,375	105,318	8%
7	Hong Kong	64,445	83,439	81,176	140,919	122,775	121,117	95,544	48%
8	Singapore	63,051	71,371	81,654	87,687	109,980	117,955	92,763	47%.
9	Russia	99,283	108,936	107,153	125,012	112,107	103,944	90,156	-9%
10	Korea	87,110	98,430	89,274	104,676	91,285	103,532	85,012	-2%
11	France	95,681	106,573	108,828	146,557	82,744	89,499	82,128	-14%.
12	India	49,107	54,196	56,413	69,310	72,923	79,263	81,815	67%.
13	Brazil	104,606	112,926	87,252	90,793	73,802	72,023	67,068	-36%.
14	Canada	68,073	69,149	65,763	88,981	73,978	72,836	60,859	-11%.
15	Turkey	30,524	32,263	31,373	36,956	33,772	37,466	40,698	33%.
16	Australia	43,427	46,921	51,000	51,995	45,711	65,386	39,161	-10%.
17	Viet Nam	28,953	37,532	40,616	40,645	33,046	37,219	36,841	27% of
18	Ireland	40,246	45,590	41,571	40,719	39,349	36,558	34,615	-14%.
19	Israel	6,593	7,679	12,518	14,220	13,437	5,888	32,191	388% (in.)
20	Italy	38,898	41,578	36,864	40,957	31,942	32,524	29,236	-25%.
21	Taiwan	46,139	45,088	40,318	40,986	31,095	32,476	29,230	-37%.
22	Mexico	34,758	36,284	31,550	35,846	28,361	28,606	25,544	-27%.
23	Spain	37,627	38,960	35,146	35,042	27,731	28,133	24,951	-34%.
24	Thailand	21,275	25,777	21,326	24,589	21,950	22,896	21,978	3
25	South Africa	30,225	24,397	19,389	21,142	17,313	17,751	17,178	-43%.
26	Finland	6,934	9,007	10,533	16,307	15,287	16,730	16,758	142%.
27	Poland	19,691	18,470	22,515	23,356	17,513	18,511	16,648	-15%.
28	Indonesia	10,851	12,377	11,823	14,502	16,861	13,963	15,647	44%
29	Sweden	15,115	14,339	14,255	15,210	13,813	17,553	14,646	-3%.
30	Czechia	19,281	18,646	16,928	16,949	14,633	13,963	13,587	-30%.

Survey on RDP 3389/TCP

More than 3,000 PCs with SIMs for telework use can be confirmed based on NW information, etc.

✓ Telework PC of a certain A company

✓ Telework PC of a certain B company



TOTAL RESULTS

1,143

TOP CITIES	
Tokyo	268
Yokohama	225
Osaka	89
Fukuoka	75
Kawasaki	14
More...	

TOP ORGANIZATIONS	
Internet	1,119
[redacted]	21
[redacted]	3

TOP OPERATING SYSTEMS	
Windows (Build 10.0.19041)	812
Windows (Build 10.0.17763)	264
Windows (Build 10.0.14393)	58
Windows (Build 6.3.9600)	2

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]
[redacted]mobile.jp
Internet
Japan, Isahaya
self-signed

SSL Certificate
Issued By:
|- Common Name:
[redacted]
Issued To:
|- Common Name:
[redacted]
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
¥x03¥x00¥x00¥x13¥x0e¥xd0¥x00¥x00¥x124¥x00¥x02¥x1f¥x08¥x00¥x02¥x00¥x00¥x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server (version 2004)
  OS Build: 10.0.19041
```
[redacted]

[redacted]
[redacted]mobile.jp
Internet
Japan, Fukuoka
self-signed

SSL Certificate
Issued By:
|- Common Name:
[redacted]
Issued To:
|- Common Name:
[redacted]
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
¥x03¥x00¥x00¥x13¥x0e¥xd0¥x00¥x00¥x124¥x00¥x02¥x1f¥x08¥x00¥x02¥x00¥x00¥x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server (version 2004)
  OS Build: 10.0.19041
```
[redacted]

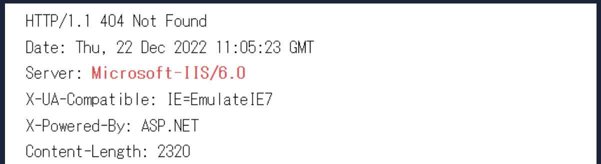
Survey on Out-of-Support Windows Operating Systems

Investigate the number of out-of-support units by using Shodan to infer the Windows Version

- 1.32 million units are available globally, with approximately 14,000 units in Japan (the 15th largest number in the world).
- Comparing November 2019 and November 2022 volumes, the rate of decline is not good across the board in Asia.

IIS6.0

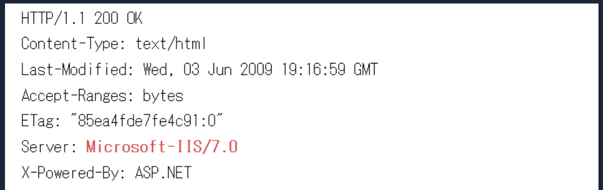
Windows 2003 Server /July 2015 EOL



```
HTTP/1.1 404 Not Found
Date: Thu, 22 Dec 2022 11:05:23 GMT
Server: Microsoft-IIS/6.0
X-UA-Compatible: IE=EmulateIE7
X-Powered-By: ASP.NET
Content-Length: 2320
```

IIS7.0

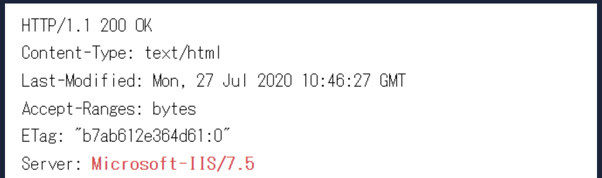
Windows Server 2008/January 2020 EOL



```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 03 Jun 2009 19:16:59 GMT
Accept-Ranges: bytes
ETag: "85ea4fde7fe4c91:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
```

IIS7.5

Windows Server 2008 R2/January 2020 EOL



```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 27 Jul 2020 10:46:27 GMT
Accept-Ranges: bytes
ETag: "b7ab612e364d61:0"
Server: Microsoft-IIS/7.5
```

Top 30 countries with the most units

	Country	Nov-2019	Nov-2020	Nov-2021	Nov-2022
-	Global	5,500,255	2,945,700	1,824,451	1,323,633
1	China	774,106	641,059	595,457	493,195
2	United States	2,532,017	1,179,770	464,793	267,506
3	Hong Kong	439,127	253,189	184,906	155,440
4	Korea	54,005	43,262	40,050	31,894
5	Germany	108,929	67,073	41,567	28,097
6	United Kingdom	96,194	57,877	35,205	24,441
7	Brazil	39,669	28,709	26,012	16,954
8	Taiwan	34,680	27,580	21,784	16,457
9	Russian Federation	42,891	25,668	22,133	16,390
10	Italy	36,255	35,095	23,007	16,177
11	Canada	54,564	36,209	24,249	15,776
12	Australia	54,620	35,652	20,983	15,047
13	India	52,305	23,670	21,235	14,841
14	Malaysia	17,225	15,359	19,530	14,662
15	**Japan**	**32,103**	**30,691**	**30,880**	**13,932**
16	France	38,415	31,900	18,905	12,923
17	Argentina	16,165	15,008	13,578	11,121
18	Singapore	19,026	24,818	7,480	9,079
19	Netherlands	43,270	27,106	12,646	9,042
20	Spain	22,457	15,991	12,153	8,987
21	Mexico	19,867	14,399	11,100	8,449
22	South Africa	628,316	82,357	7,945	8,187
23	Turkey	23,963	21,369	12,560	7,974
24	Thailand	13,758	9,801	9,602	7,962
25	Indonesia	11,815	5,810	5,333	5,592
26	Iran	20,750	10,840	10,839	5,482
27	Viet Nam	10,617	8,815	6,918	5,004
28	Ireland	13,862	9,514	7,459	4,828
29	Sweden	14,402	9,737	6,833	4,088
30	Czechia	11,354	7,582	5,750	3,913

In order of decreasing rate of decrease

	Country	Percentage change
1	Malaysia	-15%.
2	Argentina	-31%.
3	China	-36%.
4	Korea	-41%.
5	Thailand	-42%.
6	Singapore	-52%.
7	Taiwan	-53%
8	Indonesia	-53%
9	Viet Nam	-53%
10	Italy	-55%.
11	**Japan**	**-57%**
12	Brazil	-57%
13	Mexico	-57%
14	Spain	-60%.
15	Russian Federation	-62%.
16	Hong Kong	-65%.
17	Ireland	-65%.
18	Czechia	-66%%
19	France	-66%%
20	Turkey	-67%%
21	Canada	-71%%
22	Sweden	-72%%
23	India	-72%%
24	Australia	-72%%
25	Iran	-74%.
26	Germany	-74%.
27	United Kingdom	-75%.
28	Netherlands	-79%
29	United States	-89%
30	South Africa	-99%.

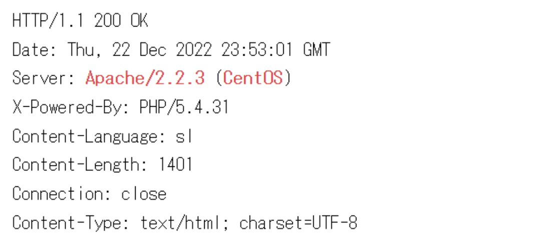
Survey on out-of-support CentOS

Investigate the number of out-of-support units by using Shodan to infer the CentOS version

- Approximately 380,000 units have been released globally, and over 70,000 units can be found in Japan (the second largest number in the world)
- CentOS5 series has the largest number in the world with less than 20,000 units in Japan.

Apache/2.2.3 (CentOS)

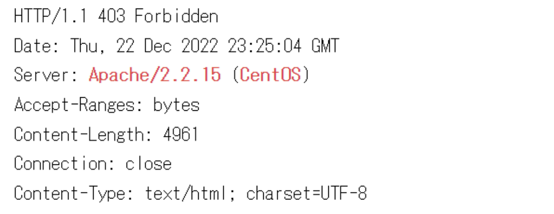
CentOS 5/2017 EOL



```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2022 23:53:01 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.4.31
Content-Language: sl
Content-Length: 1401
Connection: close
Content-Type: text/html; charset=UTF-8
```

Apache/2.2.15 (CentOS)

CentOS 6/2020 EOL



```
HTTP/1.1 403 Forbidden
Date: Thu, 22 Dec 2022 23:25:04 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Content-Length: 4961
Connection: close
Content-Type: text/html; charset=UTF-8
```

Top 30 countries with the most units

	Country	Nov-2019	Nov-2020	Nov-2021	Nov-2022
-	Global	1,138,405	993,855	570,403	378,597
1	United States	361,371	273,302	151,814	96,675
2	**Japan**	**132,819**	**113,143**	**94,122**	**71,338**
3	Russian Federation	54,011	61,206	26,318	17,264
4	France	38,811	34,308	21,912	16,778
5	China	54,530	40,911	24,467	14,973
6	Korea, Republic of	20,895	21,251	16,349	14,082
7	Italy	18,685	21,392	14,894	11,248
8	Canada	48,816	27,309	16,311	10,679
9	Germany	40,460	36,758	22,471	9,994
10	United Kingdom	39,284	33,149	15,410	9,734
11	Taiwan	11,618	12,811	9,205	7,704
12	Ukraine	20,407	21,921	19,063	7,671
13	Brazil	17,541	15,268	9,751	6,707
14	Netherlands	26,970	23,528	10,267	6,097
15	India	30,809	28,609	14,021	5,164
16	Hong Kong	11,904	11,212	6,575	4,728
17	Thailand	7,102	6,090	5,235	4,157
18	Singapore	14,146	17,709	5,272	4,123
19	Spain	9,470	7,683	4,721	3,419
20	Malaysia	4,788	4,388	3,312	3,344
21	Indonesia	8,239	6,020	3,925	3,112
22	Mexico	5,262	2,968	2,491	3,101
23	Czechia	7,227	5,979	3,607	2,897
24	Romania	10,125	7,356	4,539	2,571
25	Argentina	4,105	2,891	2,551	2,355
26	Australia	8,972	6,414	3,665	2,276
27	Turkey	14,703	22,119	3,222	2,221
28	Poland	7,148	6,069	4,990	1,967
29	Bulgaria	6,248	3,449	3,524	1,839
30	Viet Nam	5,466	5,599	2,214	1,656

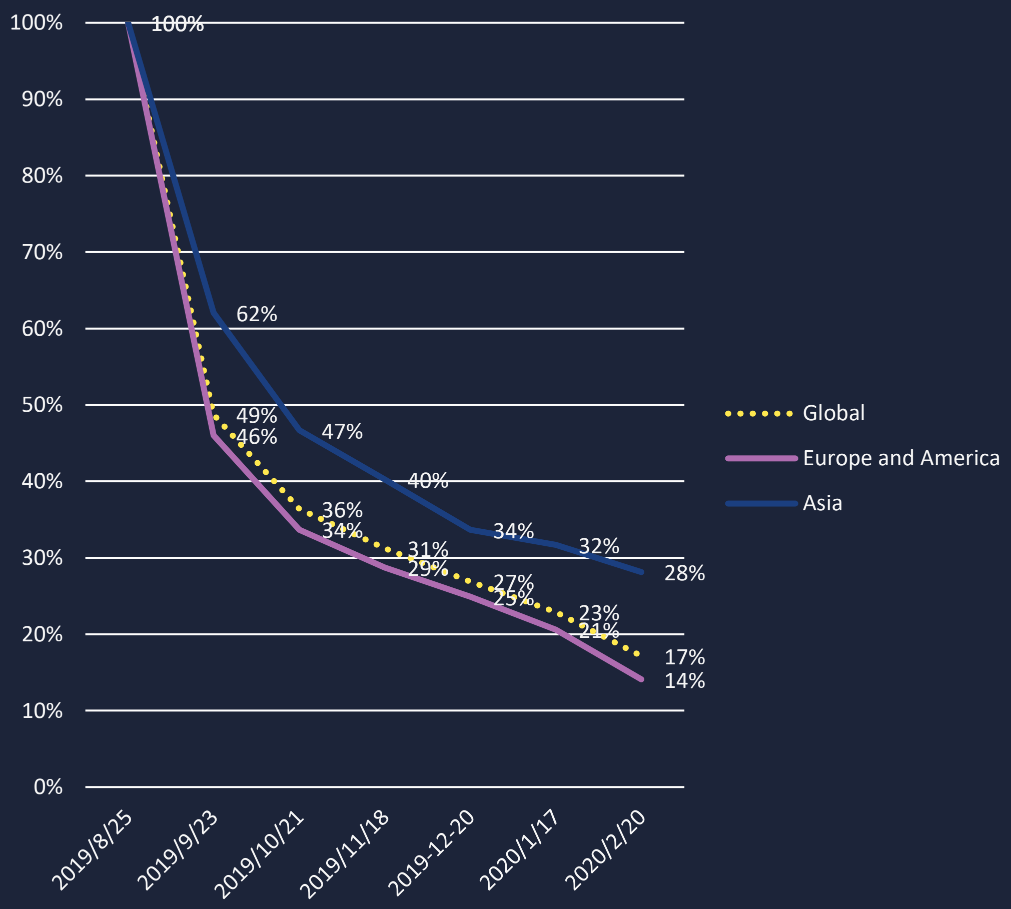
In order of decreasing rate of decrease

	Country	Percentage change
1	Malaysia	-30%.
2	Korea	-33%.
3	Taiwan	-34%.
4	Italy	-40%.
5	Mexico	-41%.
6	Thailand	-41%.
7	Argentina	-43%.
8	**Japan**	**-46%.**
9	France	-57%
10	Czechia	-60%.
11	Hong Kong	-60%.
12	Brazil	-62%.
13	Indonesia	-62%.
14	Ukraine	-62%.
15	Spain	-64%
16	Global	-67%%
17	Russian Federation	-68%.
18	Viet Nam	-70%.
19	Bulgaria	-71%%
20	Singapore	-71%%
21	Poland	-72%%
22	China	-73%.
23	United States	-73%.
24	Romania	-75%.
25	Australia	-75%.
26	United Kingdom	-75%.
27	Germany	-75%.
28	Canada	-78%
29	India	-83%%
30	Turkey	-85%.

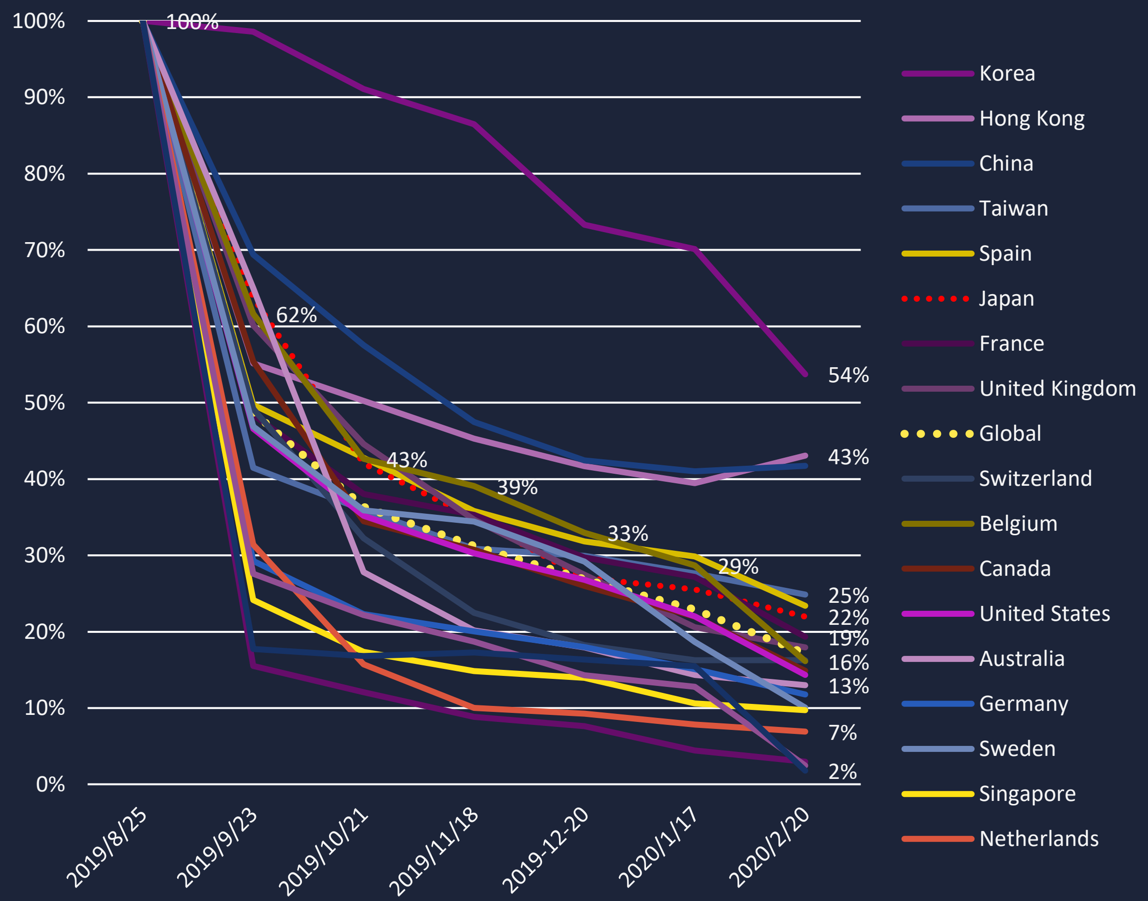
Country-specific countermeasure trends for Pulse Secure/CVE-2019-11510 vulnerabilities

- Patch released in April 2019; attacks increased following announcement by DEVCORE Orange at BlackHat and others in August of the same year.
- Speed of countermeasures by region and country based on scan data published by Bad Packets (@bad_packets)
- Western countries are coping fast and Asian countries are slow. It can be seen that Japan is coping at a slightly slower pace than the global average.

Percentage change in vulnerable servers (by region)



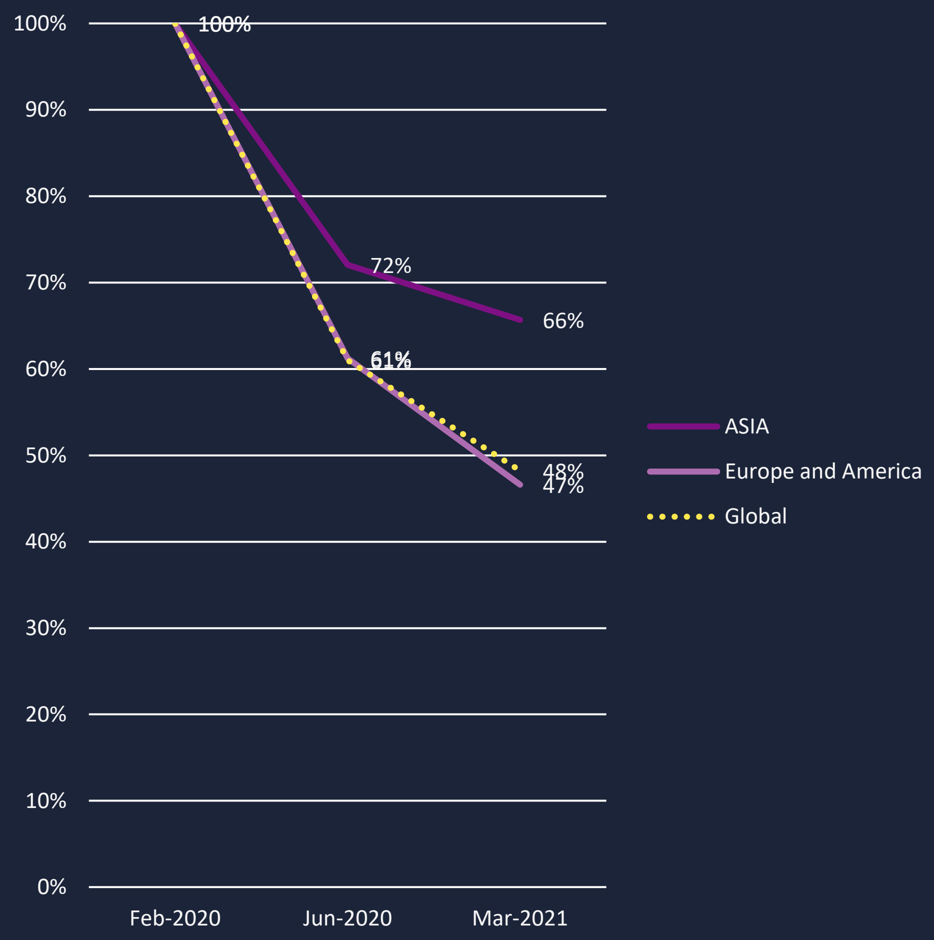
Percentage change of vulnerable servers (by country)



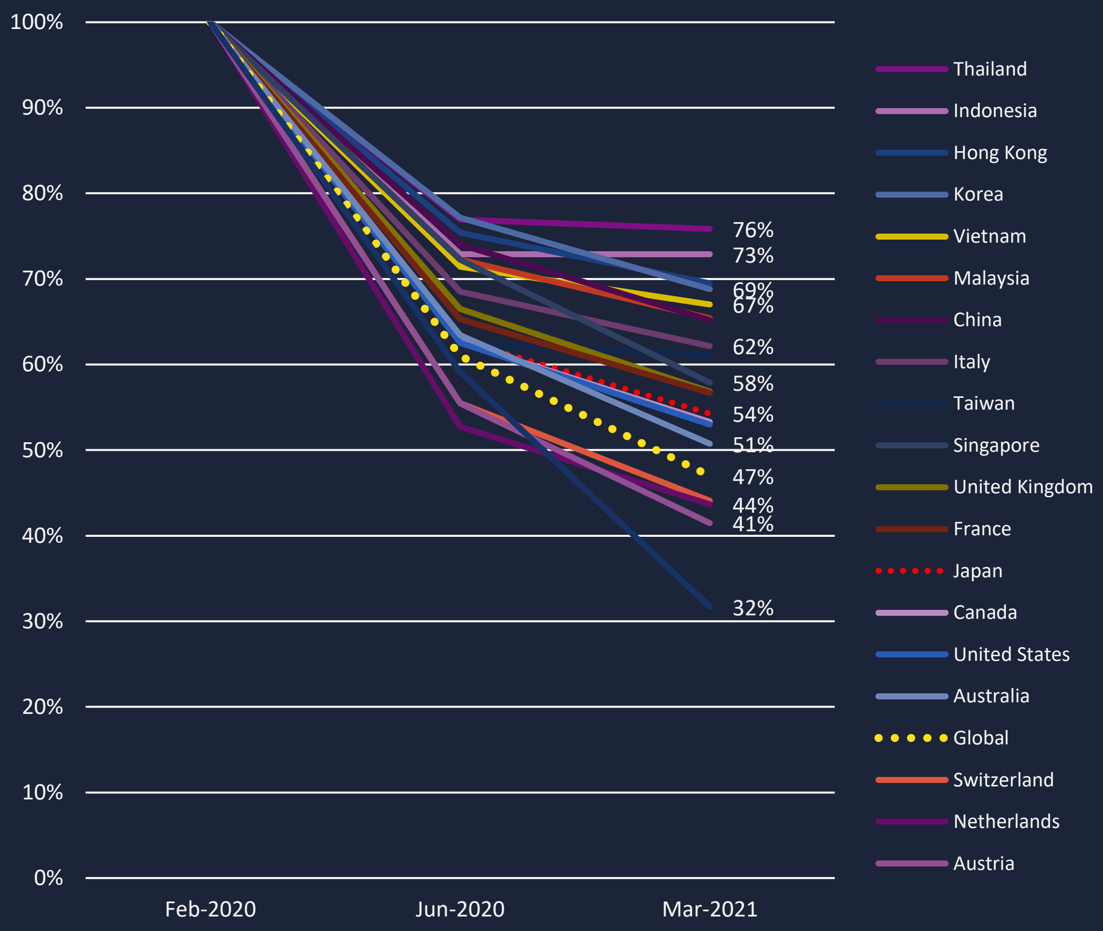
Exchange Server/CVE-2020-0688 Vulnerability Countermeasure Trends by Country

- A patch was released on February 25, 2020, and attack activity began to be actively observed around March of the same year.
- In the Western world, 39% of servers were addressed in six months and 52% in one year, while in Asia, 28% were addressed in six months and 34% in one year.

Percentage change in vulnerable servers (by region)



Percentage change of vulnerable servers (by country)

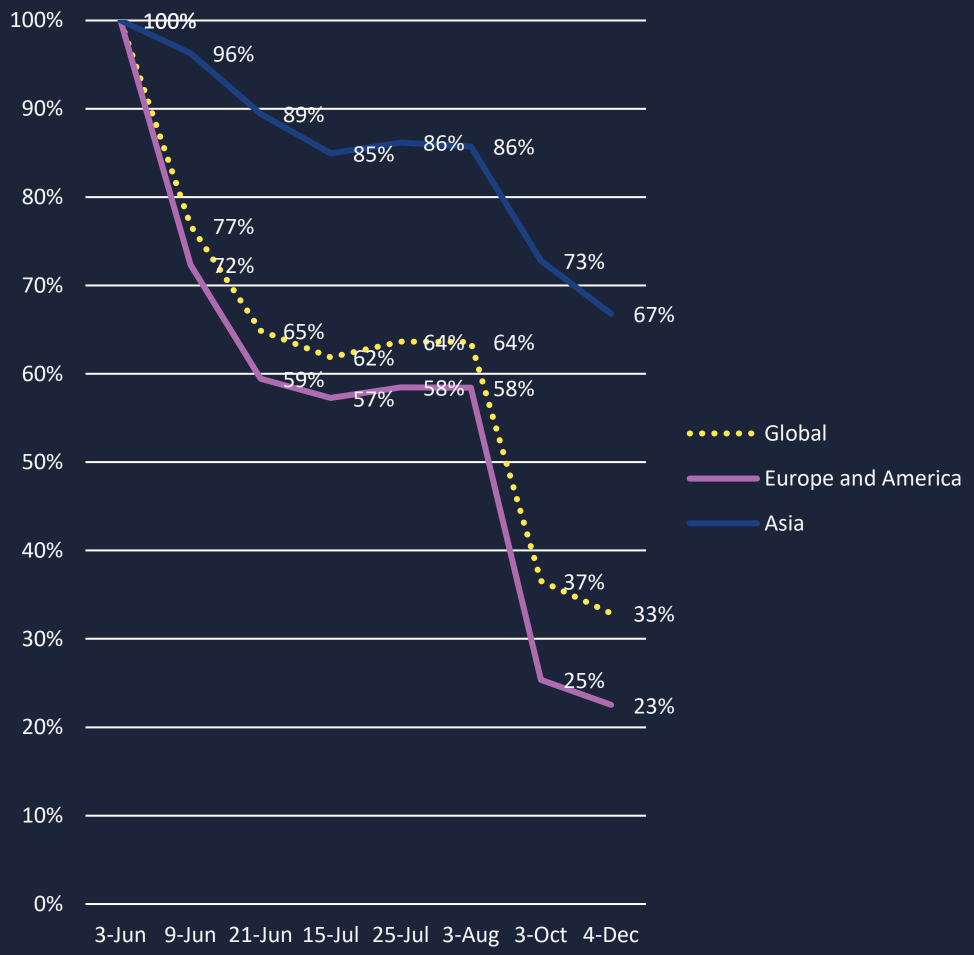


Note that the dates in the graphs are not evenly spaced due to the timing of data acquisition.

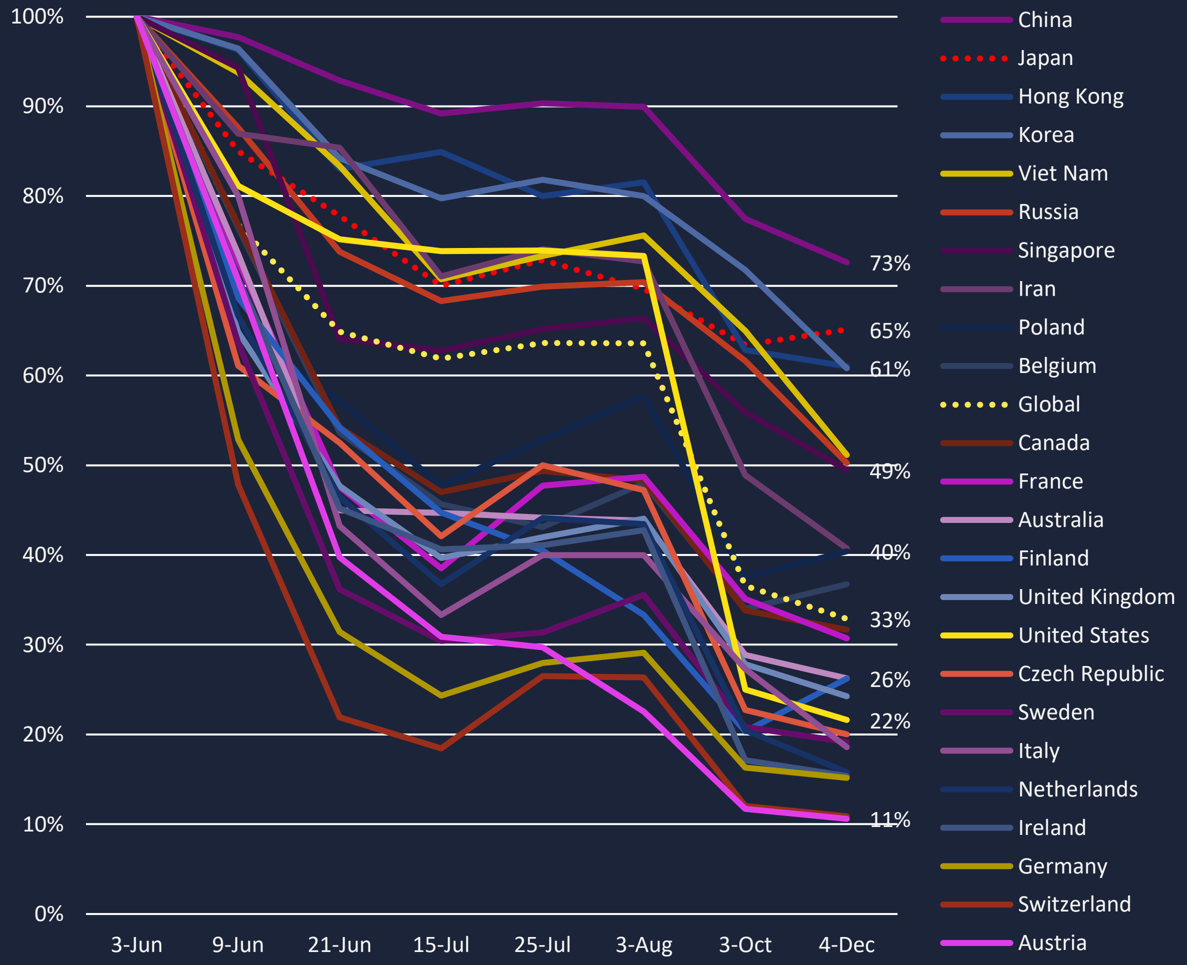
Country-specific countermeasure trends for the Atlassian Confluence/CVE-2022-26134 vulnerability

- Zero-day vulnerability with a patch released on June 2, 2022, and ongoing reports of exploits since then.
- As of 12/4/2022, 2303 of 7001 units globally and 28 of 43 units in Japan remain vulnerable
- Six Months After Patch Release, Vulnerable Servers Decrease to 20% in Europe and the U.S., but remains 70% in Asia

Percentage change in vulnerable servers (by region)



Percentage change of vulnerable servers (by country)

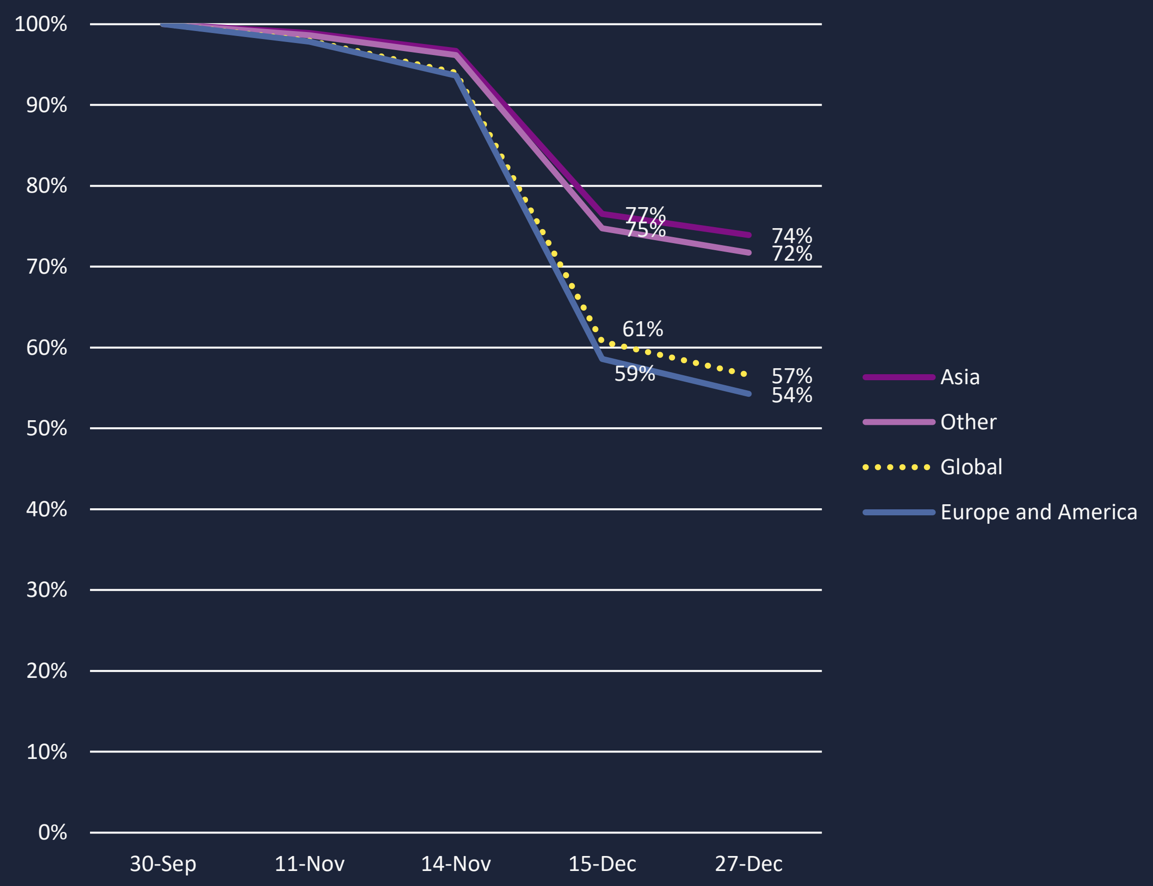


Note that the dates in the graphs are not evenly spaced due to the timing of data acquisition.

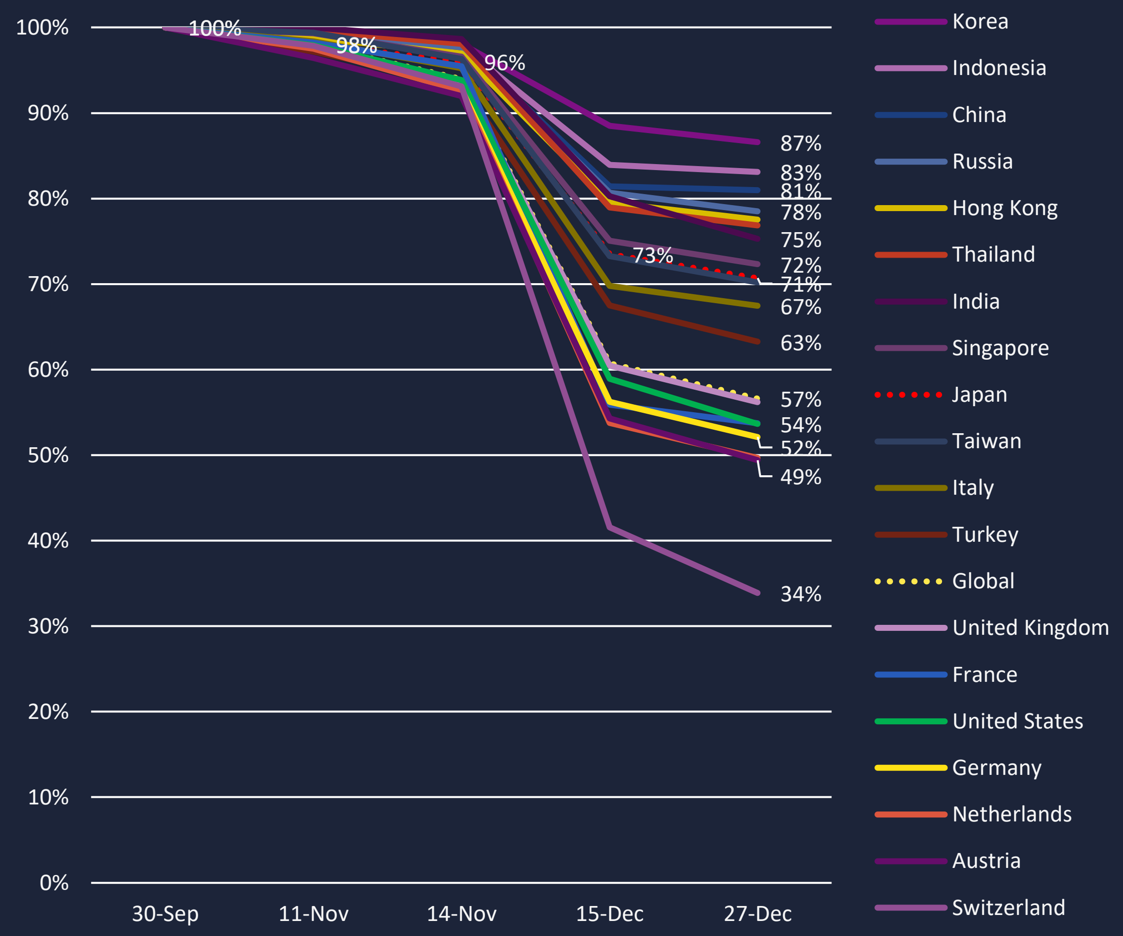
Exchange Server/ProxyNotShell Vulnerability Countermeasure Trends by Country

- Reported as a zero-day in September 2022 and patch released November 9, 2022 (CVE-2022-41040, CVE-2022-41082)
- Since some versions of a narrow range of Exchange Server are affected, we counted only the number of servers using the affected version and the number of servers using the fixed vulnerability version to investigate the percentage of vulnerable servers.

Percentage change in vulnerable servers (by region)



Percentage change of vulnerable servers (by country)

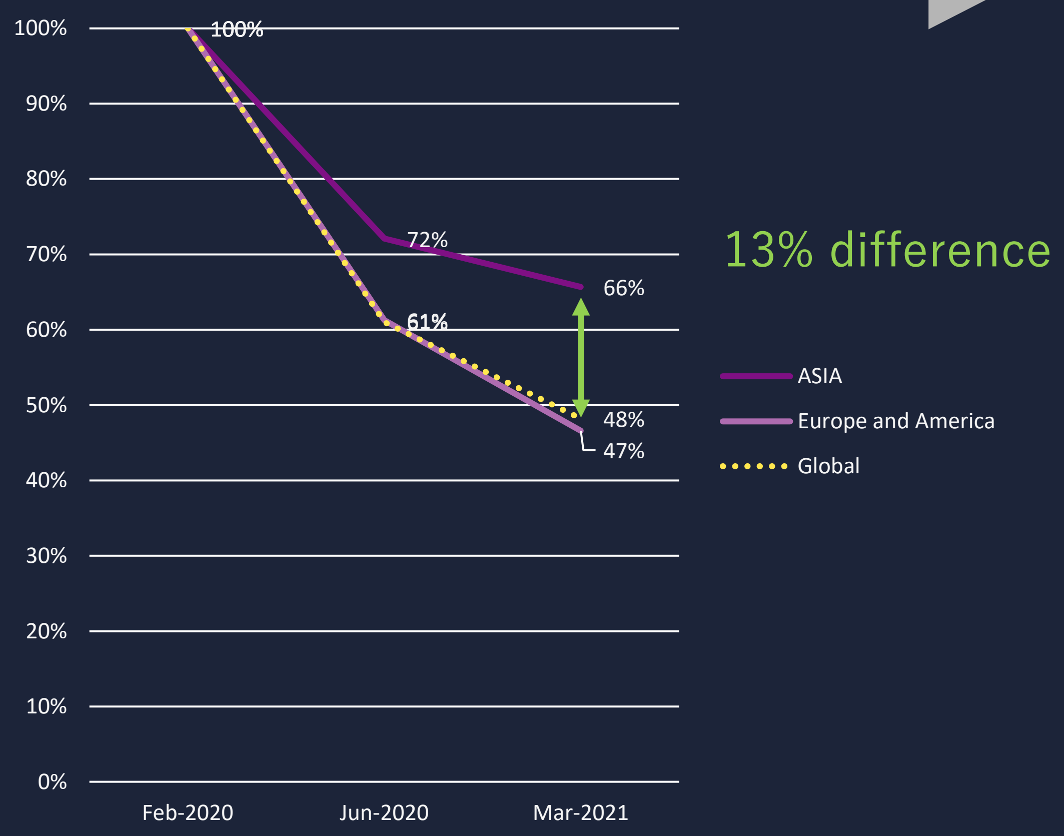


Note that the dates in the graphs are not evenly spaced due to the timing of data acquisition.

2020 vs 2022 Exchange Server Vulnerability Addressed

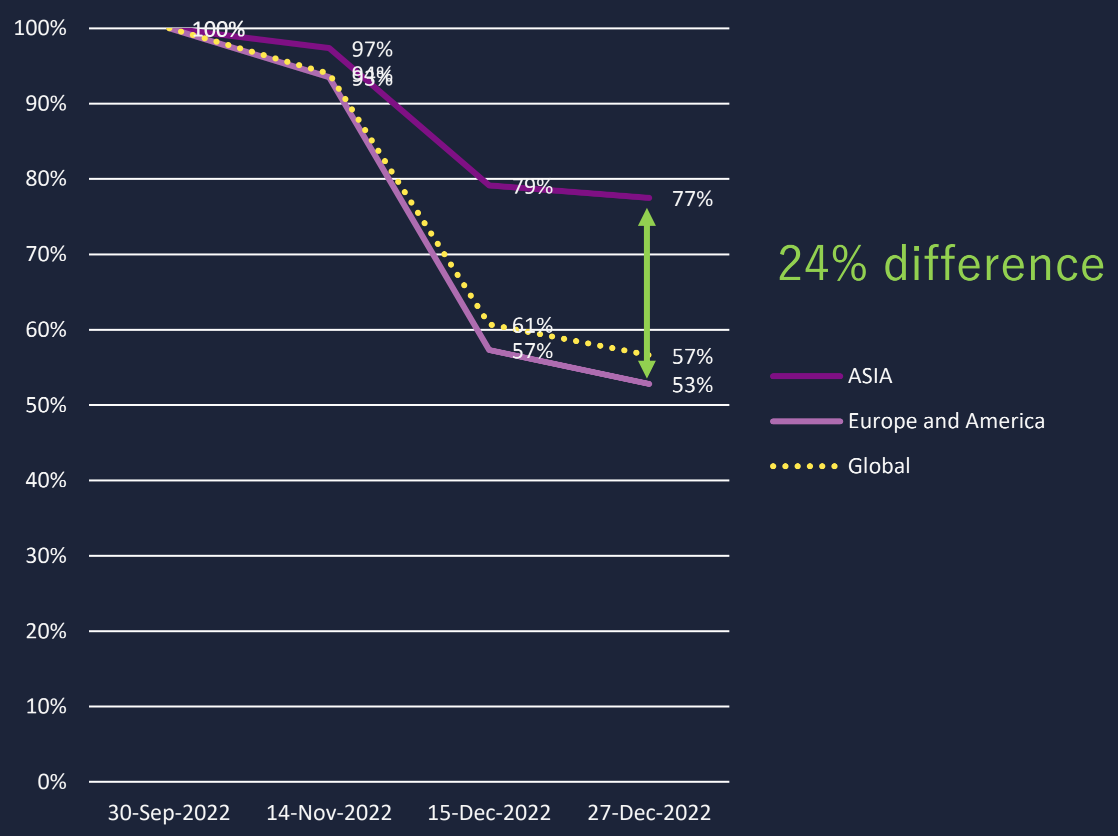
- Comparison of the speed of dealing with CVE-2020-0688 fixed in February 2020 and ProxyNotShell fixed in November 2022 for the same country
- In Europe and the U.S., the progress of about 50% in addressing vulnerabilities, which took about one year in 2020, will be achieved in about one month in 2022. It is possible that this is related to the fact that ProxyNotShell was a vulnerability that affected relatively new versions (many people are highly aware of the need to apply patches).
- After about 2 years, the gap between the Asian and Western regions is widening in terms of the speed of coping.

Percentage change in vulnerability to ✓CVE-2020-0688, by region



13% difference

Percentage Trends Vulnerable to ✓ProxyNotShell, by Region



24% difference

Note that the dates in the graphs are not evenly spaced due to the timing of data acquisition.

2020 vs 2022 Exchange Server Vulnerability Addressed

- Comparison of CVE-2020-0688 fixed in February 2020 and ProxyNotShell fixed in November 2022 for the same country
- There is little turnover in the order of coping speed (red box)

country	area	CVE-2020-0688 Percentage of vulnerable servers after approx. 1 year	ProxyNotShell Percentage of vulnerable servers after approx. 1.5 months	gap	Progress on CVE-2020-066 after approx. ranking of the worst countries	Progress after about 1.5 months of ProxyNotShell ranking of the worst countries
Korea	ASIA	69%.	87%	18%	4	1
Indonesia		73%.	83%	10% (%)	2	2
China		65% of	81%	16%	7	3
Vietnam		67%.	78% of	11%.	5	4
Malaysia		65% of	78% of	12%.	6	5
Hong Kong		69%.	78% of	8%	3	6
Thailand		76% of	77%	1	1	7
Singapore		58%	72%	14%.	10	8
Japan		54%	71%	16%	13	9
Taiwan		61%.	70% (of the total)	9%.	9	10
Italy	Europe and America	62%	67%.	5% (of the total)	8	11
Canada		53%.	56% of	3	14	12
United Kingdom		57%	56% of	-1%.	11	13
Australia		51%	55%	4%	16	14
France		57%	54%	-3%.	12	15
United States		53%.	54%	1	15	16
Germany		32%	52%	20%.	20	17
Netherlands		44%	50% of	6%	18	18
Austria		41%.	49%	8%	19	19
Switzerland		44%	34%	-10%.	17	20

Reference: Investigation of the speed of vulnerability handling

- Survey methodology (when using Shodan CLI)

1. Consider a search query to identify servers affected by the vulnerability
   Shodan http.title:outlook
2. Retrieve data from the device search engine DB with a search query
   shodan download --limit -1 filename http.title:outlook
3. Repeat 2 on a regular basis, such as every month (note that the data volume is more than a few GB).
4. Parse necessary data items from the acquired data (parse items should be considered for each vulnerability)
   shodan parse --fields ip_str,port,location.country_code,data sourcefilename > targetfilename
5. Format the extracted data to make it comparable.

- It is important not to miss the opportunity to conduct a vulnerability response speed survey, as the conditions to do so are extremely rare.

1. The vulnerability must be a server vulnerability that is often exposed externally. Naturally, it is because internal servers cannot be observed by OSINT.
2. The version information and vulnerability can be determined by HTML, etc. without scanning from outside. This is because scanning is not legally allowed.
3. Version information must be stored in the data held by device search engines such as Shodan.
   *For example, SonicWall displays version information in the source of the VPN login screen, but Shodan and Censys do not retain it.
4. A PoC or attack is observed and the need for patching is widely/strongly announced (not a requirement).
5. The total number of public servers should be neither too many nor too few. If there are too few, trends cannot be read, and if there are too many, data cannot be processed.

The Situation of Japanese Companies

✓In January 2022, we surveyed the management of the external public servers of the headquarters, overseas offices, and groups of 50 specific companies selected from the former Tokyo Stock Exchange First Section.
*No vulnerability scans or server access were conducted, but the investigation was based on information from Shodan.

✓In about 40% of the cases, the headquarter company has the problem, and 90% of the companies, including overseas and even subsidiaries, were found to have the problem.
✓In addition to this survey, there are almost no other companies that have been surveyed over 100 companies and found no problems at all.

Total 50 companies

38 companies

Discovered 76% of the respondents were running out-of-support OS (Windows server, CentOS)
Older ones are Windows 2000 (2010 EOL) and Server 2003 (2015 EOL).

45 companies

90% found running out-of-support old software
Apache, PHP, OpenSSL, OpenSSH, MariaDB, Serv-U, etc.
*Excluding likely backport modifications from the survey

15 companies

30% use servers with remote desktop published
Telework PCs for 4 of the above companies.

Agenda for this session

✓ Part 1: Analysis of recent incident occurrence trends

Leaked information by the Ransom Gang
Press Release on Damage by Japanese Companies
Public reports from security agencies/vendors

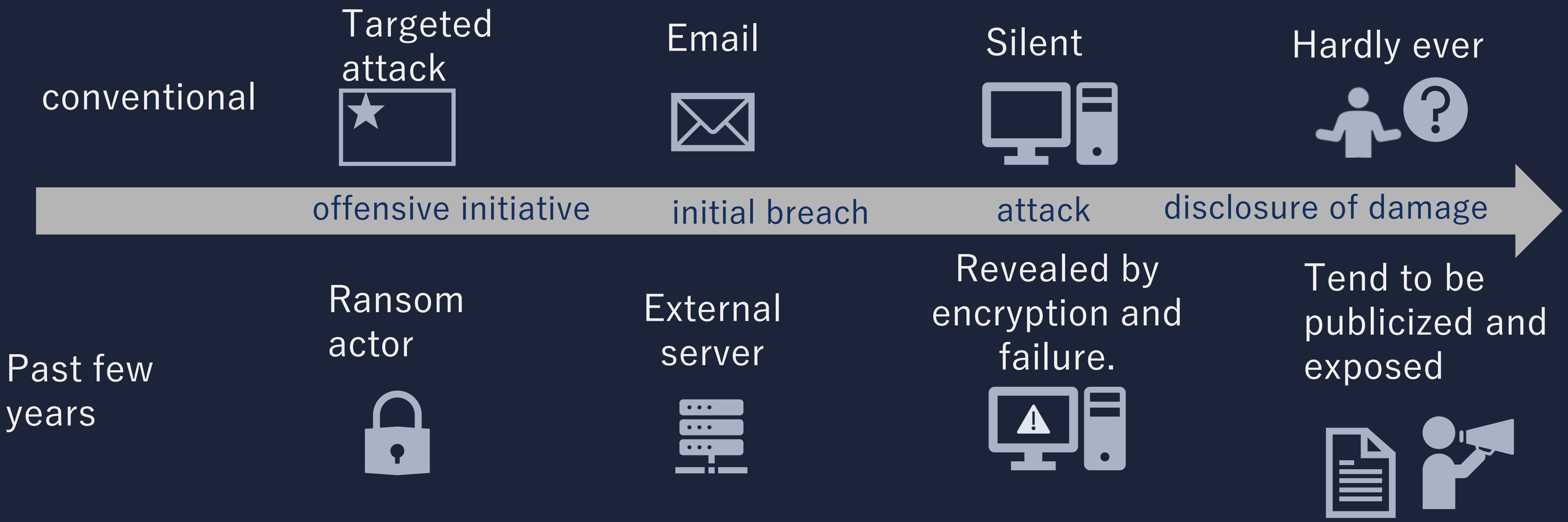
✓ Part 2: Changes in the management of externally disclosed assets

RDP Publication Status
Use of out-of-support OS
Change in speed of vulnerability response (2020 vs. 2022)
Status of Measures Taken by Japanese Companies

✓ Part 3: Attempting to capture the attacker's change in tactics

Past survey cases (Pandora, AvosLocker, Deadbolt)
Share how to research with device search engines

Major trend changes over the past few years



conventional

Targeted attack

Email

Silent

Hardly ever

offensive initiative

initial breach

attack

disclosure of damage

Past few years

Ransom actor

External server

Revealed by encryption and failure.

Tend to be publicized and exposed

Incident information tends to become public for various reasons.
Can we capture attack trends and tactical changes by using public information?

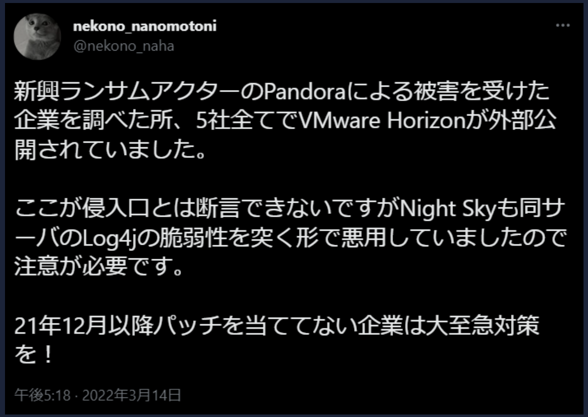
Example #1 Ransom Actor Pandora

- Three Japanese companies were also targeted by the (rebranded) ransom actor, which started its activity in March 2010 and ended soon after.
- Speculated that the victim companies commonly published VMware Horizon, which may have been an entry point.
- In June 2022, Trend Micro also mentioned the connection between the Pandora incident and VMware Horizon (Log4j).
  Log4Shell Vulnerability in VMware Leads to Data Exfiltration and Ransomware
  https://www.trendmicro.com/en_us/research/22/g/log4shell-vulnerability-in-vmware-leads-to-data-exfiltration-and-ransomware.html

List of ✓Damaged Companies

company suffering damage	Publication Date	country	suspect site
Company H	22/3/30	Japan	VMware Horizon available
Company U	22/3/30	United States of America	VMware Horizon available
Company O	22/3/13	United States of America	VMware Horizon available
Company R	22/3/13	United States of America	VMware Horizon available
Company D	22/3/13	Japan	VMware Horizon available
Company G	22/3/5	Japan	VMware Horizon available
Company J	22/3/5	United States of America	VMware Horizon available

✓Tweet alert



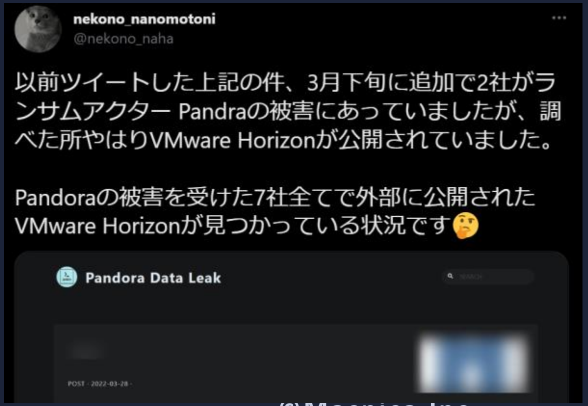
nekono_nanomotoni
@nekono_naha

新興ランサムアクターのPandoraによる被害を受けた企業を調べた所、5社全てでVMware Horizonが外部公開されていました。

ここが侵入口とは断言できないですがNight Skyも同サーバのLog4jの脆弱性を突く形で悪用していましたので注意が必要です。

21年12月以降パッチを当ててない企業は大至急対策を！

午後5:18 · 2022年3月14日



nekono_nanomotoni
@nekono_naha

以前ツイートした上記の件、3月下旬に追加で2社がランサムアクター Pandraの被害にあっていましたが、調べた所やはりVMware Horizonが公開されていました。

Pandoraの被害を受けた7社全てで外部に公開されたVMware Horizonが見つかっている状況です🤔

Pandora Data Leak

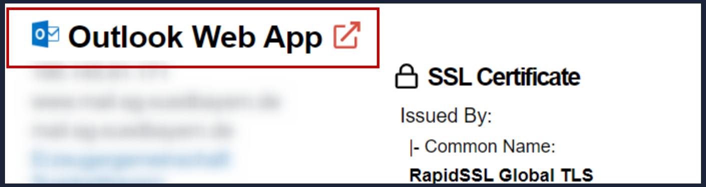
POST · 2022-03-28 ·

✓Alert on Log4j for VMwareHorizon

time	reporter	home (i.e. hometown, home country)
22/1/5	United Kingdom NHS/CC-4002	Unknown Threat Group
22/1/10	Microsoft	Ransom Actor DEV-0401 (NightSky)
22/3/14	nekono_nanomotoni	Ransom Actor Pandora
22/3/29	SOPHOS	Mining Bots
22/6/23	U.S.A. CISA/AA22-174A	Multiple threat actors including APT
22/8/16	Trend Micro	Multiple cases including Ransom Actor Pandora
22/8/25	Microsoft	Iranian/MERCURY
22/9/7	BlackBerry	Ransom Actor/MONTI
22/9/8	Cisco Thalos	Lazarus/APT38
22/9/14	U.S.A. CISA/AA22-257A	Iranian-affiliated APT/IRGC

Example #2 Ransom actor AvosLocker

- Ransomware employing a RaaS model that began activity around June 2021
- The victim companies in June 2022 commonly disclosed Exchange Server, and all of them had either the latest version or the version corresponding to ProxyShell at the time of the investigation approximately two weeks later. There is a possibility that the server was used as an entry point was inferred from the fact that it was either the latest version or the version corresponding to ProxyShell.
- In March 2022, the FBI issued an advisory indicating that multiple AvosLocker incidents were caused by the Proxy Shell.
  Indicators of Compromise Associated with AvosLocker Ransomware
  https://www.ic3.gov/Media/News/2022/220318.pdf



Outlook Web App

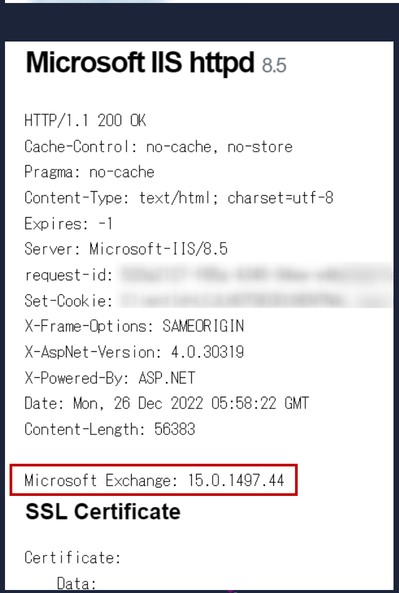
[redacted]

SSL Certificate

Issued By:

|- Common Name:

RapidSSL Global TLS



Microsoft IIS httpd 8.5

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
request-id: [redacted]
Set-Cookie: [redacted]
X-Frame-Options: SAMEORIGIN
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 26 Dec 2022 05:58:22 GMT
Content-Length: 56383

Microsoft Exchange: 15.0.1497.44
```

SSL Certificate

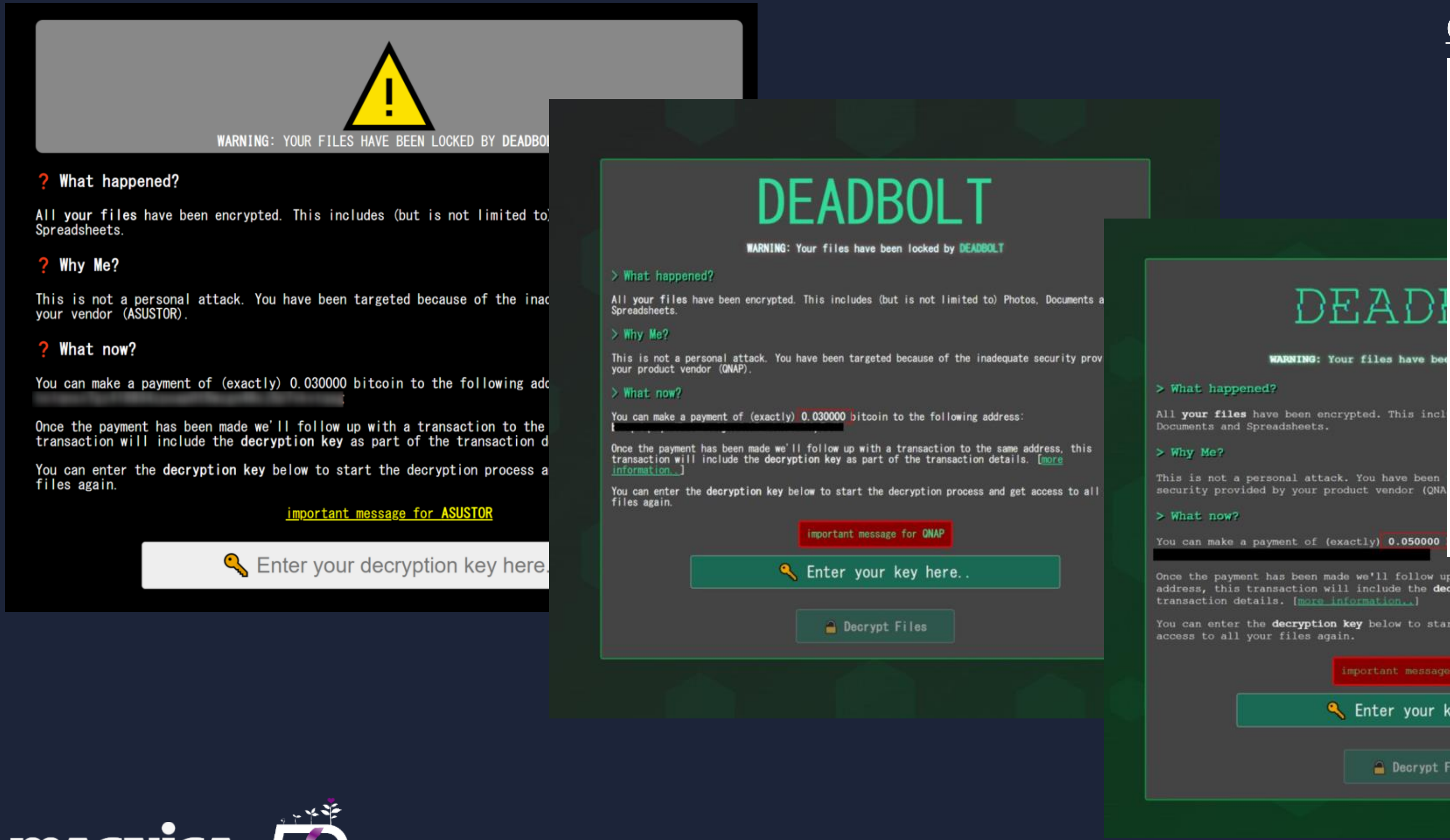
```
Certificate:
    Data:
```

Date of leak site publication	Name of company affected	Exchange Yes/No	Exchange Version *As of late June 2010
2022/6/17	C****	ant	unaccessible
2022/6/17	B********	ant	latest version
6/8/2022	L*********	ant	Applicable to ProxyShell
6/7/2022	Y****************	ant	latest version
6/7/2022	C************	ant	latest version
6/7/2022	C********	ant	Applicable to ProxyShell
6/3/2022	T**************	ant	latest version
6/3/2022	C**********************	ant	Applicable to ProxyShell
6/3/2022	P**********************	undiscovered	long vowel mark (usually only used in katakana)
6/3/2022	B**************	undiscovered	long vowel mark (usually only used in katakana)
6/3/2022	C**************	undiscovered	long vowel mark (usually only used in katakana)
2022/4/6	K************	undiscovered	long vowel mark (usually only used in katakana)
2022/4/6	M*****************	undiscovered	long vowel mark (usually only used in katakana)
2022/4/6	A**********************	undiscovered	long vowel mark (usually only used in katakana)

Example #3 DeadBolt ransomware

- Ransomware targeting NAS manufactured by QNAP and ASUSTOR since around January 2022
- Multiple campaigns were launched in January, May, June, and around August during 2022, causing a lot of damage in Japan and abroad.
- Directly supplemental information on the number and version of NAS units affected as threats are displayed on the login screen

Ransom note displayed on affected NAS



WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBO

? What happened?

All **your files** have been encrypted. This includes (but is not limited to)
Spreadsheets.

? Why Me?

This is not a personal attack. You have been targeted because of the inac
your vendor (ASUSTOR).

? What now?

You can make a payment of (exactly) 0.030000 bitcoin to the following add
[redacted]

Once the payment has been made we'll follow up with a transaction to the
transaction will include the **decryption key** as part of the transaction d

You can enter the **decryption key** below to start the decryption process a
files again.

important message for ASUSTOR

Enter your decryption key here

DEADBOLT

WARNING: Your files have been locked by DEADBOLT

> What happened?

All **your files** have been encrypted. This includes (but is not limited to) Photos, Documents a
Spreadsheets.

> Why Me?

This is not a personal attack. You have been targeted because of the inadequate security prov
your product vendor (QNAP).

> What now?

You can make a payment of (exactly) 0.030000 bitcoin to the following address:
[redacted]

Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [more information..]

You can enter the **decryption key** below to start the decryption process and get access to all files again.

important message for QNAP

Enter your key here..

Decrypt Files

DEAD

WARNING: Your files have bee

> What happened?

All **your files** have been encrypted. This incl
Documents and Spreadsheets.

> Why Me?

This is not a personal attack. You have been
security provided by your product vendor (QNA

> What now?

You can make a payment of (exactly) 0.050000
[redacted]

Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [more information..]

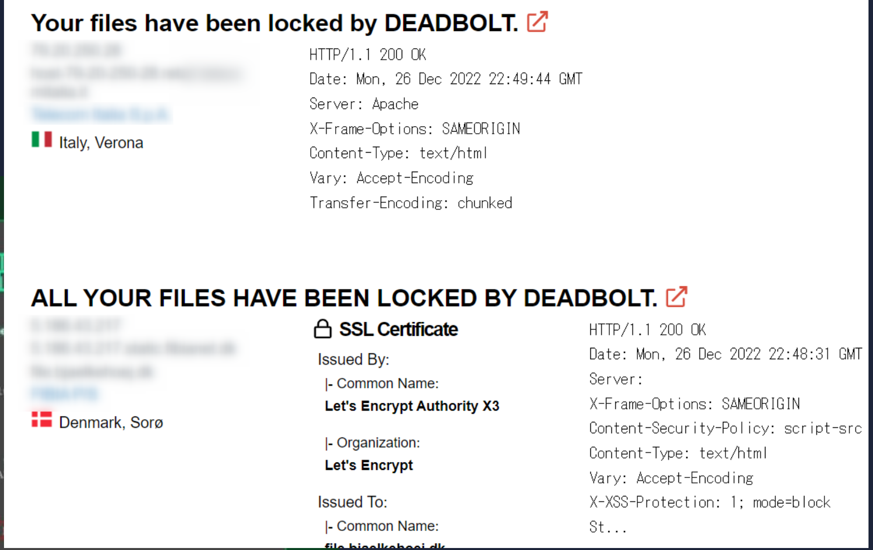
You can enter the **decryption key** below to start the decryption process and get access to all your files again.

important message for QNAP

Enter your key here..

Decrypt Files

Capture of damaged NAS in Shodan



Your files have been locked by DEADBOLT.

[redacted]

Italy, Verona

```
HTTP/1.1 200 OK
Date: Mon, 26 Dec 2022 22:49:44 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT.

[redacted]

Denmark, Sorø

SSL Certificate

Issued By:
|- Common Name:
Let's Encrypt Authority X3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:

```
HTTP/1.1 200 OK
Date: Mon, 26 Dec 2022 22:48:31 GMT
Server:
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: script-src
Content-Type: text/html
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
St...
```

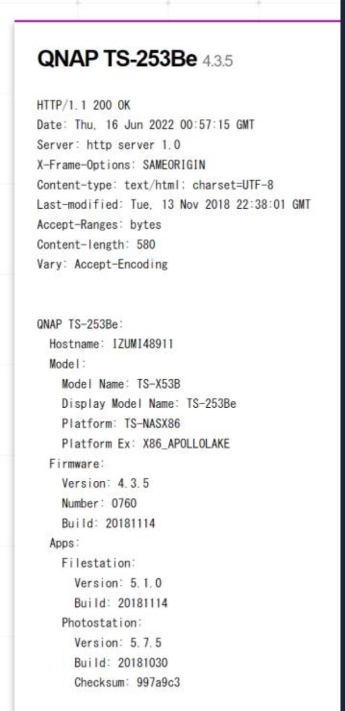
Example #3 DeadBolt ransomware

- In each campaign, the number of affected units was significantly different from the total number of QNAP NAS (327,000 units), suggesting that specific versions or models may have been targeted.
- Investigations were conducted and specific versions/models were targeted from the first to the third round. QNAP was notified, and the results were used to raise awareness both domestically and internationally.

Number of damages per campaign

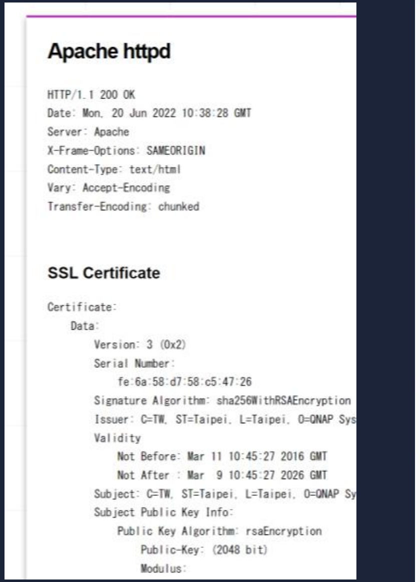
month	Number of Damages	remarks
January	1,889	First Offensive Campaign
February	3,566	
March	3,678	
April	2,300	
May	3,696	Second Offensive Campaign
June	6,494	Third Offensive Campaign
July	1,5017	Fourth Offensive Campaign

Server response before and after encryption



QNAP TS-253Be 4.3.5

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 00:57:15 GMT
Server: http server 1.0
X-Frame-Options: SAMEORIGIN
Content-type: text/html; charset=UTF-8
Last-modified: Tue, 13 Nov 2018 22:38:01 GMT
Accept-Ranges: bytes
Content-length: 580
Vary: Accept-Encoding


QNAP TS-253Be:
  Hostname: IZUMI48911
  Model:
    Model Name: TS-X53B
    Display Model Name: TS-253Be
    Platform: TS-NASX86
    Platform Ex: X86_APOLLOLAKE
  Firmware:
    Version: 4.3.5
    Number: 0760
    Build: 20181114
  Apps:
    Filestation:
      Version: 5.1.0
      Build: 20181114
    Photostation:
      Version: 5.7.5
      Build: 20181030
      Checksum: 997a9c3
```



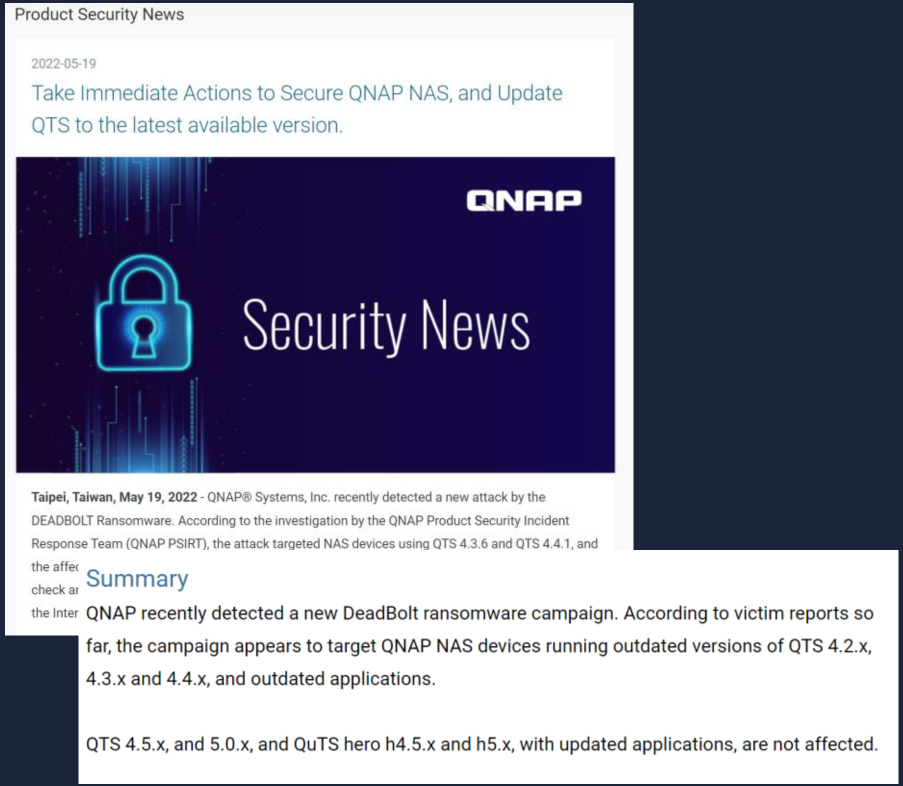
Apache httpd

```
HTTP/1.1 200 OK
Date: Mon, 20 Jun 2022 10:38:28 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fe:6a:58:d7:58:c5:47:26
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=TW, ST=Taipei, L=Taipei, O=QNAP Sys
        Validity
            Not Before: Mar 11 10:45:27 2016 GMT
            Not After : Mar  9 10:45:27 2026 GMT
        Subject: C=TW, ST=Taipei, L=Taipei, O=QNAP Sy
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

Security alerts from QNAP, Inc.



Product Security News

2022-05-19

Take Immediate Actions to Secure QNAP NAS, and Update QTS to the latest available version.

Taipei, Taiwan, May 19, 2022 - QNAP® Systems, Inc. recently detected a new attack by the DEADBOLT Ransomware. According to the investigation by the QNAP Product Security Incident Response Team (QNAP PSIRT), the attack targeted NAS devices using QTS 4.3.6 and QTS 4.4.1, and the affec

check ar

the Inter

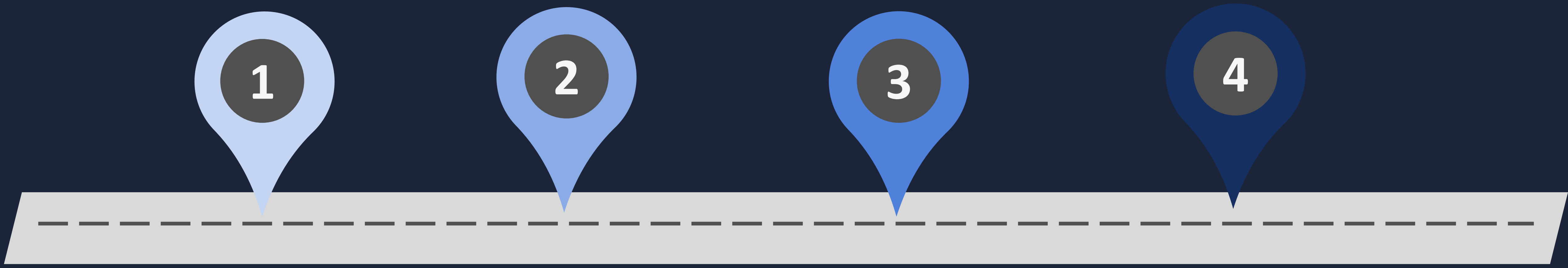
Summary

QNAP recently detected a new DeadBolt ransomware campaign. According to victim reports so far, the campaign appears to target QNAP NAS devices running outdated versions of QTS 4.2.x, 4.3.x and 4.4.x, and outdated applications.

QTS 4.5.x, and 5.0.x, and QuTS hero h4.5.x and h5.x, with updated applications, are not affected.

https://www.qnap.com/en-me/security-news/2022/take-immediate-actions-to-secure-qnap-nas-and-update-qts-to-the-latest-available- version
https://www.qnap.com/ja-jp/security-advisory/QSA-22-19

Sharing survey methodology



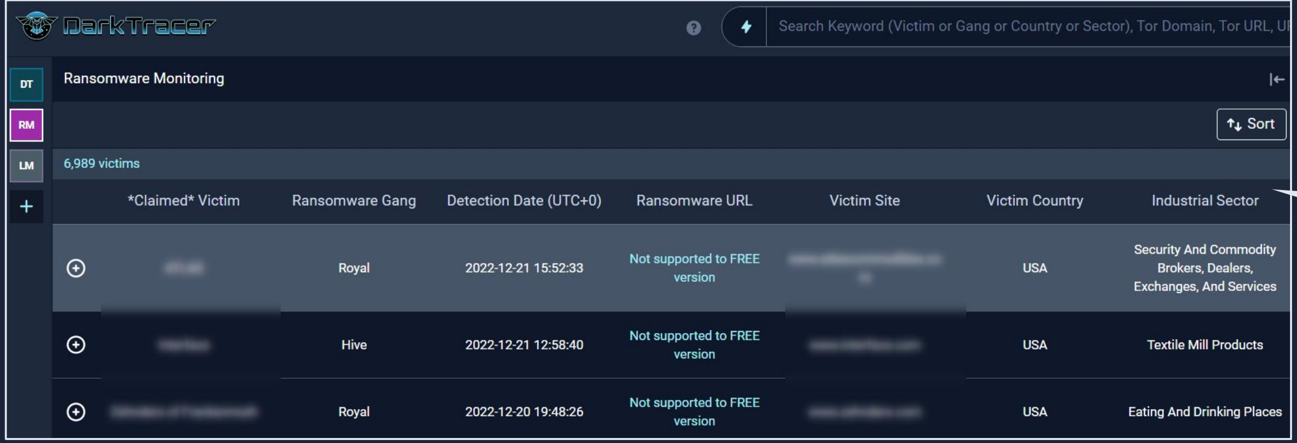
1. Leak Information check
2. Victim company server OSINT
3. Suspected initial point of entry Extract points in common
4. Status monitoring of server outages, version upgrades, etc.

Note: The main focus of this report is to introduce methods to efficiently investigate at no cost or with minimal man-hours.
OSINT methods that utilize expensive paid tools and intelligence will not be explained at this time due to time and practical feasibility.

Note: Since there are various perspectives and methods of product identification, only representative points are listed. Methods described does not capture servers 100%. Please also aware that there may be products that are not intended in the search.

Check for leaked information

- Monitor the attacker’s leak site and keep track of the victim companies.
  *A free account with DarkTracer is also recommended, as tracking by yourself is time-consuming.
  https://xoxo.darktracer.com/
- Gather domain information of the victim company from the leaked information



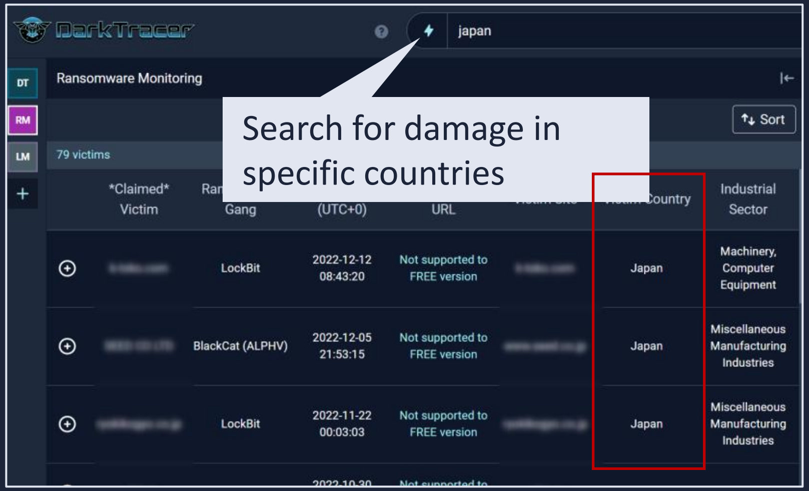
Search Keyword (Victim or Gang or Country or Sector), Tor Domain, Tor URL, U

Ransomware Monitoring

6,989 victims

	Claimed Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
⊕	[redacted]	Royal	2022-12-21 15:52:33	Not supported to FREE version	[redacted]	USA	Security And Commodity Brokers, Dealers, Exchanges, And Services
⊕	[redacted]	Hive	2022-12-21 12:58:40	Not supported to FREE version	[redacted]	USA	Textile Mill Products
⊕	[redacted]	Royal	2022-12-20 19:48:26	Not supported to FREE version	[redacted]	USA	Eating And Drinking Places

Name of company affected
Ransom Gang Name
Publication Date
URL/Domain of the affected company
country
type of industry



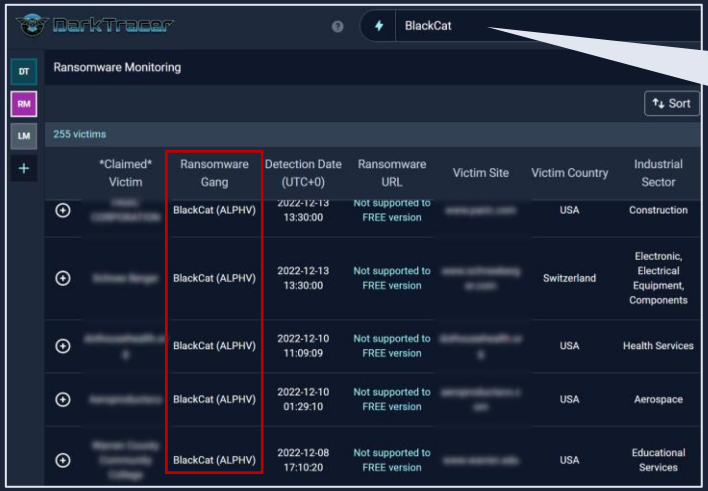
japan

Ransomware Monitoring

79 victims

Search for damage in specific countries

	Claimed Victim	Ran Gang	(UTC+0)	URL		Country	Industrial Sector
⊕	[redacted]	LockBit	2022-12-12 08:43:20	Not supported to FREE version	[redacted]	Japan	Machinery, Computer Equipment
⊕	[redacted]	BlackCat (ALPHV)	2022-12-05 21:53:15	Not supported to FREE version	[redacted]	Japan	Miscellaneous Manufacturing Industries
⊕	[redacted]	LockBit	2022-11-22 00:03:03	Not supported to FREE version	[redacted]	Japan	Miscellaneous Manufacturing Industries
			2022-10-30	Not supported to			



BlackCat

Ransomware Monitoring

255 victims

	Claimed Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
⊕	[redacted]	BlackCat (ALPHV)	2022-12-13 13:30:00	Not supported to FREE version	[redacted]	USA	Construction
⊕	[redacted]	BlackCat (ALPHV)	2022-12-13 13:30:00	Not supported to FREE version	[redacted]	Switzerland	Electronic, Electrical Equipment, Components
⊕	[redacted]	BlackCat (ALPHV)	2022-12-10 11:09:09	Not supported to FREE version	[redacted]	USA	Health Services
⊕	[redacted]	BlackCat (ALPHV)	2022-12-10 01:29:10	Not supported to FREE version	[redacted]	USA	Aerospace
⊕	[redacted]	BlackCat (ALPHV)	2022-12-08 17:10:20	Not supported to FREE version	[redacted]	USA	Educational Services

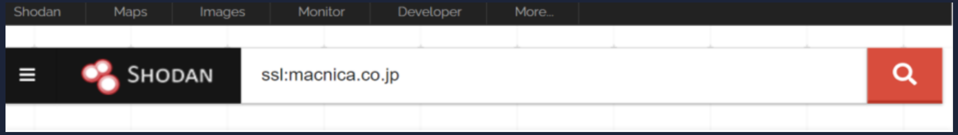
Search for damage caused by a specific ransomware gangs

Identification of Victim Company Servers

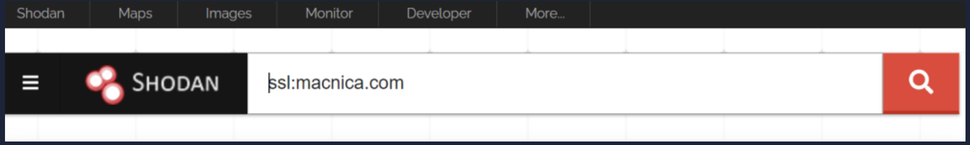
- SSL search with device search services (Shodan, Censys, ZoomEye, etc.) based on collected domain information
- Efficiently identify servers with domain information owned by the affected organization ≒ servers managed/owned by the organization

Access the following URL and search for the domain identified in STEP 1 as follows
https://www.shodan.io/dashboard
ssl:domain of the affected organization e.g. ssl:macnica.co.jp

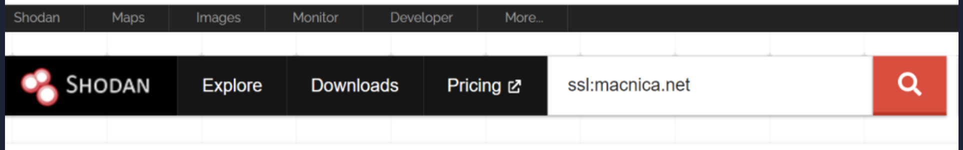
This search allows servers with the relevant domain in the SSL certificate to be searched at once.



ssl:macnica.co.jp

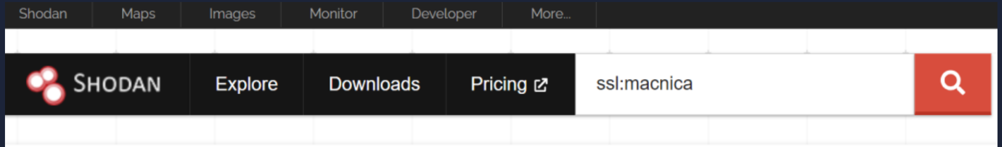


ssl:macnica.com



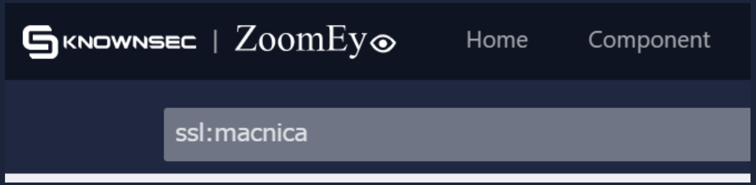
ssl:macnica.net

If your company name is unusual or unique, you can use the top or second level of the domain name.
If omitted, search at once is more efficient



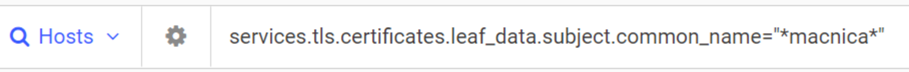
ssl:macnica

For ZoomEye



ssl:macnica

For Censys



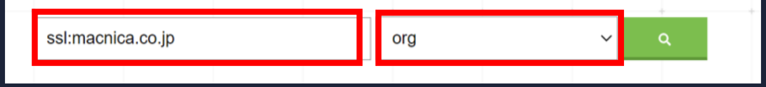
services.tls.certificates.leaf_data.subject.common_name="*macnica*"

The following patterns should also be searched depending on the target location
services.tls.certificates.leaf_data.subject_dn="*targetname*"
services.tls.certificates.leaf_data.issuer_dn ="*targetname*"
services.tls.certificates.leaf_data.issuer.common_name ="*targetname*"
services.tls.certificates.leaf_data.issuer.organization ="*targetname*"
services.tls.certificates.leaf_data.subject.common_name ="*targetname*"
services.tls.certificates.leaf_data.subject.organization ="*targetname*"

Identification of Victim Company Servers

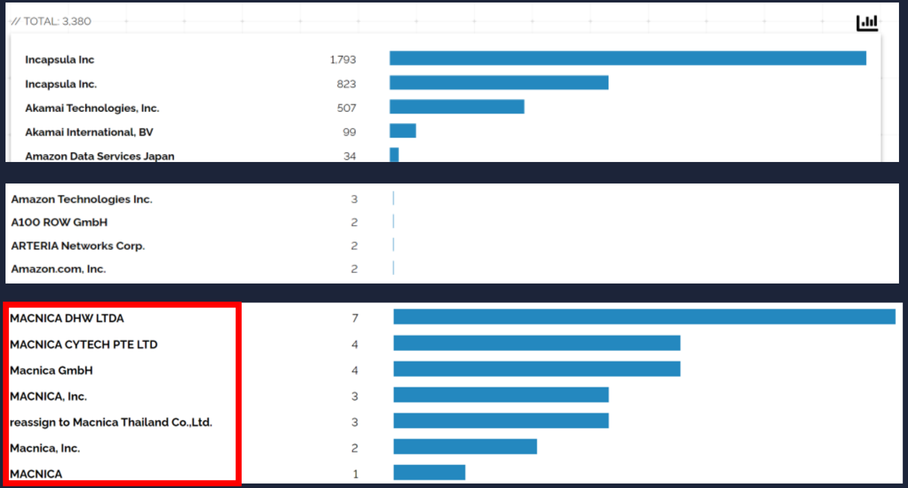
- Search the results of the SSL search on the previous page to determine the IP address range owned by the company (Shodan only)

Access the following URL
https://www.shodan.io/search/facet
Enter the domain you searched for on the previous page on the left side
On the right, search with "org" set from the list.


ssl:macnica.co.jp
org

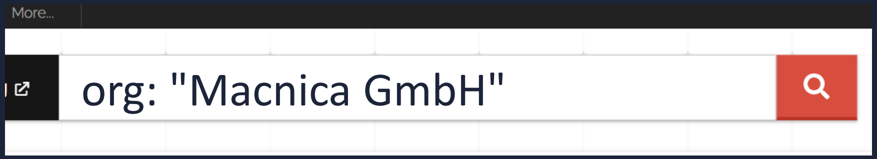
The server with the SSL certificate to be searched is owned by which company?
Able to check how many units are operating in an IP address segment

If the name of the company is mentioned, copy and paste the name and write it down in a memo.

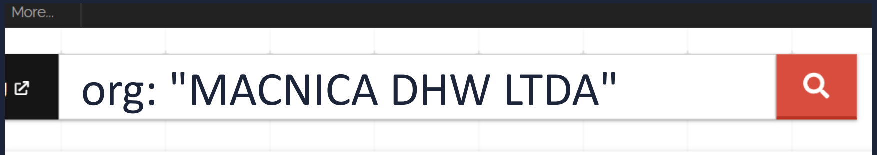

// TOTAL: 3,380

Incapsula Inc	1,793
Incapsula Inc.	823
Akamai Technologies, Inc.	507
Akamai International, BV	99
Amazon Data Services Japan	34
Amazon Technologies Inc.	3
A100 ROW GmbH	2
ARTERIA Networks Corp.	2
Amazon.com, Inc.	2
MACNICA DHW LTDA	7
MACNICA CYTECH PTE LTD	4
Macnica GmbH	4
MACNICA, Inc.	3
reassign to Macnica Thailand Co.,Ltd.	3
Macnica, Inc.	2
MACNICA	1

Access Shodan's regular search page
https://www.shodan.io/
Search as follows using the organization names identified in STEP3-1.
org: "organization name"



org: "Macnica GmbH"



org: "MACNICA DHW LTDA"

This search will find the name of the searched organization in the IP address range registered in Whois.
Possible to identify servers that are running
If the organization's name is unique, a search using only the company name is easier.
It may be possible (e.g., org:macnica)
If the organization name includes a comma, such as MACNICA, Inc.,
you need to remove the right side and search.
Example: org: "MACNICA, Inc." → org: "MACNICA"

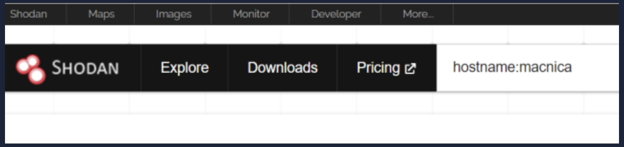
*ZoomEye also allows searches like org:macniac, but unlike Shodan, it also includes servers that ZoomEye has determined to be relevant
*Censys has a weak organization name supplement on Whois and
Difficult to use because wildcard search is not available in autonomous_system.name=.

Identification of Victim Company Servers

- What if the suspect server does not appear using the method?

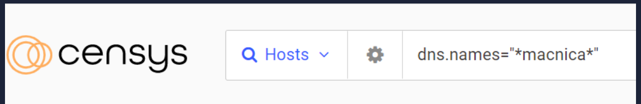
1. hostname search

hostname:targetname



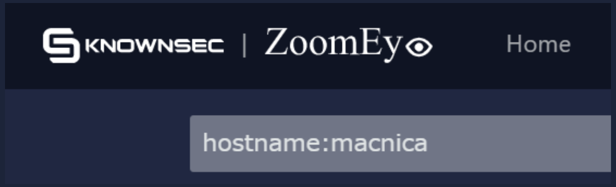
hostname:macnica

dns.names="*targetname*"



dns.names="*macnica*"

hostname:targetname

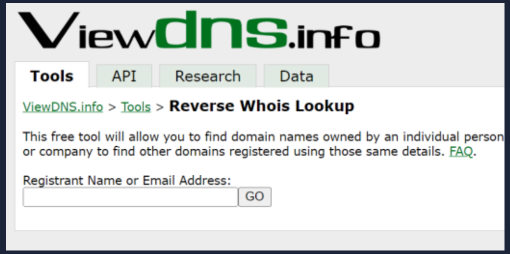


hostname:macnica

2. Expand the domain to be surveyed

Viewdns.info

https://viewdns.info/reversewhois/



ViewDNS.info > Tools > **Reverse Whois Lookup**

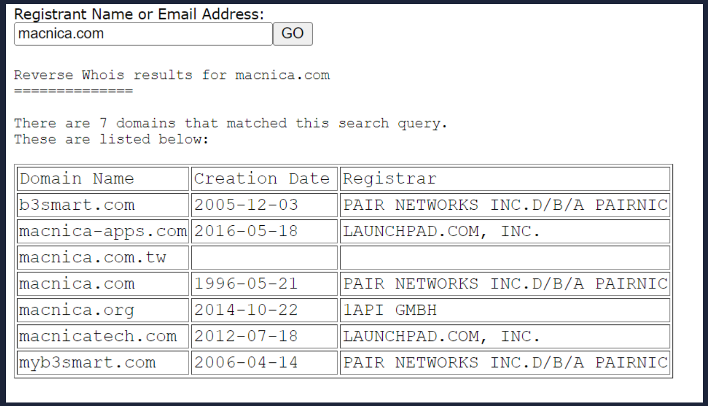
This free tool will allow you to find domain names owned by an individual person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

There is a relationship between the search target domain and the Whois information.

Automatic enumeration of domains (with noise sometimes)



Registrant Name or Email Address:

macnica.com GO

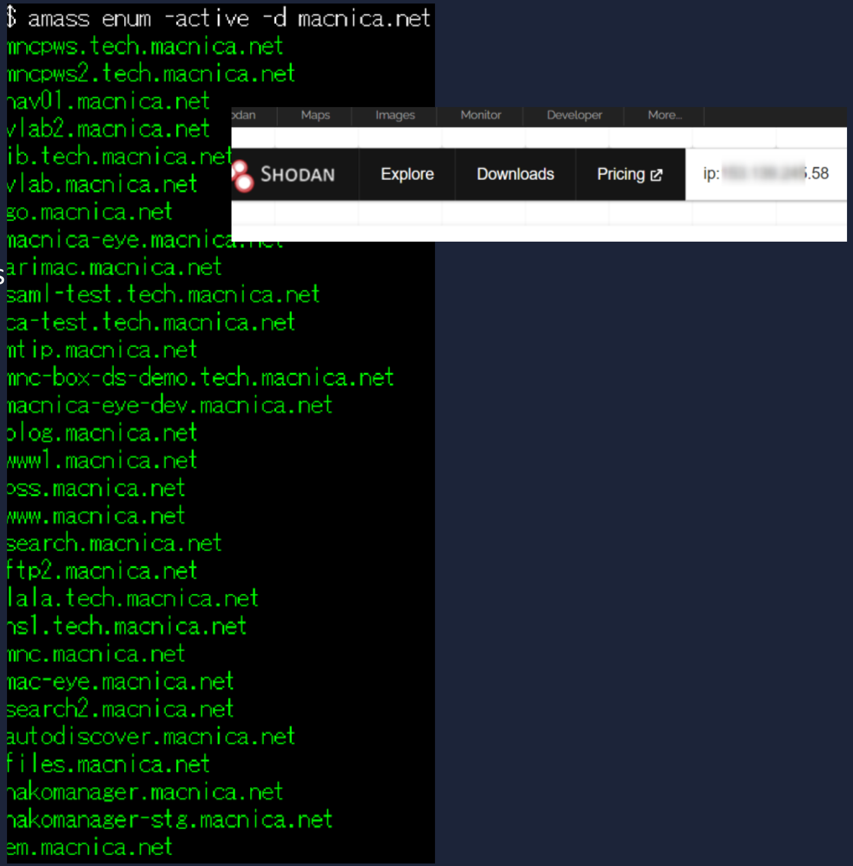
```
Reverse Whois results for macnica.com
==============

There are 7 domains that matched this search query.
These are listed below:
```

Domain Name	Creation Date	Registrar
b3smart.com	2005-12-03	PAIR NETWORKS INC.D/B/A PAIRNIC
macnica-apps.com	2016-05-18	LAUNCHPAD.COM, INC.
macnica.com.tw		
macnica.com	1996-05-21	PAIR NETWORKS INC.D/B/A PAIRNIC
macnica.org	2014-10-22	1API GMBH
macnicatech.com	2012-07-18	LAUNCHPAD.COM, INC.
myb3smart.com	2006-04-14	PAIR NETWORKS INC.D/B/A PAIRNIC

3. List subdomain -> list IP address -> IP search

OWASP Amass

https://github.com/OWASP/Amass



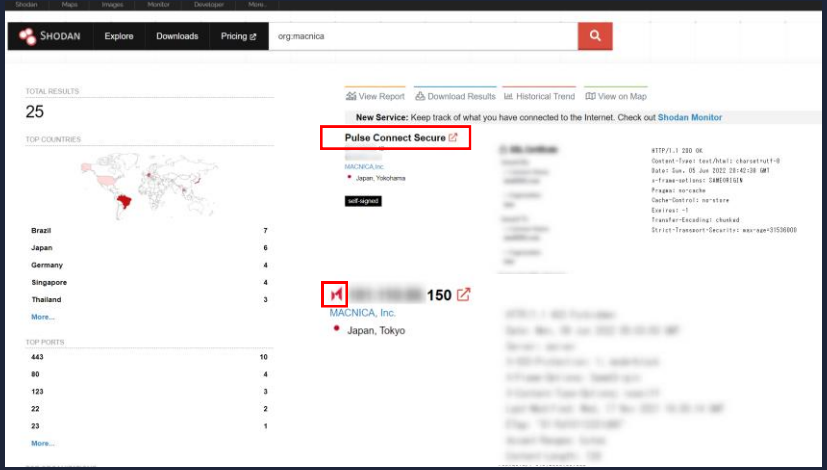
```
$ amass enum -active -d macnica.net
mncpws.tech.macnica.net
mncpws2.tech.macnica.net
nav01.macnica.net
vlab2.macnica.net
ib.tech.macnica.net
vlab.macnica.net
go.macnica.net
macnica-eye.macnica.net
arimac.macnica.net
saml-test.tech.macnica.net
ca-test.tech.macnica.net
mtip.macnica.net
mnc-box-ds-demo.tech.macnica.net
macnica-eye-dev.macnica.net
blog.macnica.net
www1.macnica.net
oss.macnica.net
www.macnica.net
search.macnica.net
ftp2.macnica.net
lala.tech.macnica.net
ns1.tech.macnica.net
mnc.macnica.net
mac-eye.macnica.net
search2.macnica.net
autodiscover.macnica.net
files.macnica.net
nakomanager.macnica.net
nakomanager-stg.macnica.net
em.macnica.net
```

ip: [redacted].58

Points to focus on when checking search results

For Shodan and ZoomEye

Product identification is done visually from HTTP title and favicon



org:macnica

TOTAL RESULTS

25

TOP COUNTRIES

Brazil	7
Japan	6
Germany	4
Singapore	4
Thailand	3
More...	

TOP PORTS

443	10
80	4
123	3
22	2
23	1
More...	

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Pulse Connect Secure

[redacted]

MACNICA,Inc.

Japan, Yokohama

self-signed

[redacted]

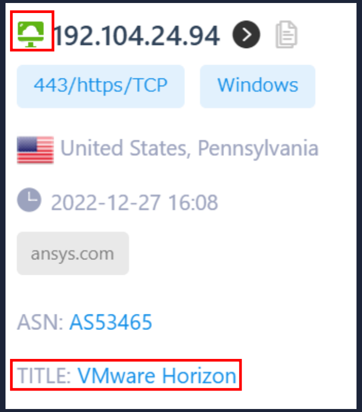
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sun, 05 Jun 2022 20:42:30 GMT
x-frame-options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Expires: -1
Transfer-Encoding: chunked
Strict-Transport-Security: max-age=31536000
```

[redacted] 150

MACNICA, Inc.

Japan, Tokyo

[redacted]



192.104.24.94

443/https/TCP | Windows

United States, Pennsylvania

2022-12-27 16:08

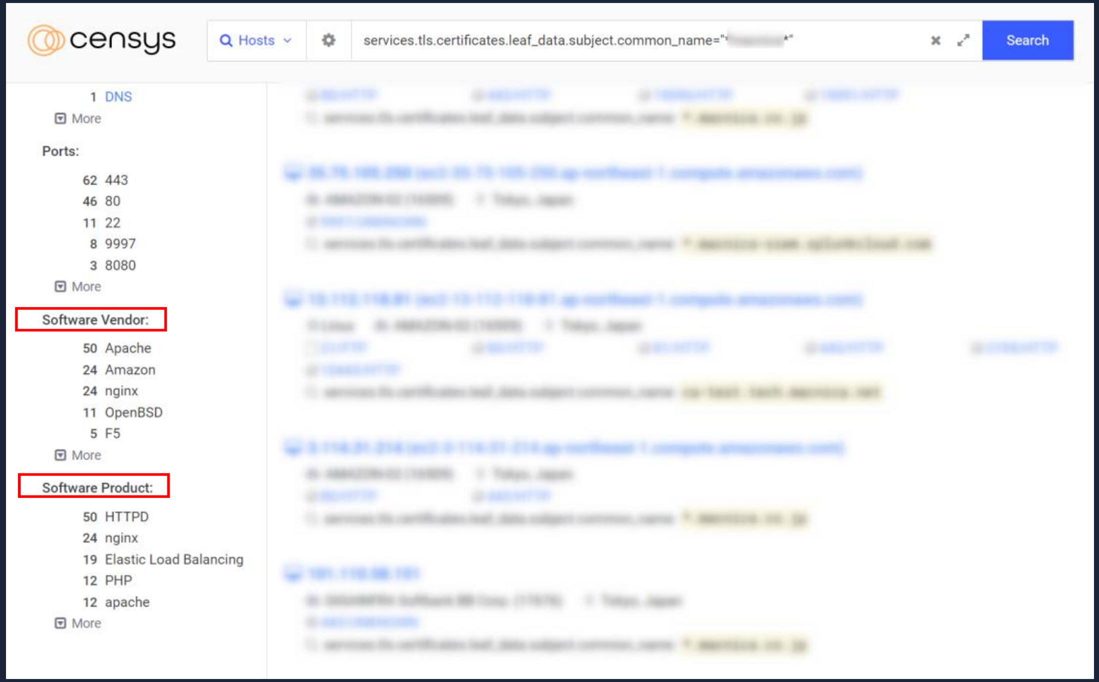
ansys.com

ASN: AS53465

TITLE: VMware Horizon

For Censys

Note the Software Vendor and Software Product in the search results.
*Note the title for some products that do not support identification.



services.tls.certificates.leaf_data.subject.common_name="[redacted]"

1 DNS
More

Ports:

62	443
46	80
11	22
8	9997
3	8080

More

Software Vendor:

50	Apache
24	Amazon
24	nginx
11	OpenBSD
5	F5

More

Software Product:

50	HTTPD
24	nginx
19	Elastic Load Balancing
12	PHP
12	apache

More

[redacted]

Summary: Pros and cons of each device search engine

- Search and check results according to the characteristics of device search engines

Shodan and ZoomEye

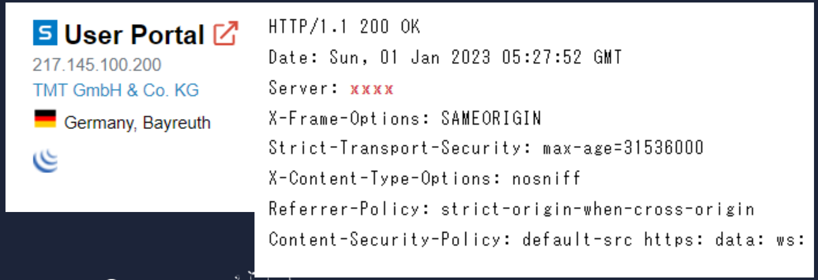
Easier extraction of victim corporate servers because strings in SSL/TLS certificates can be searched at once.

ssl:targetname

Can perform targeted searches for organization names in Whois for IP addresses

org:targetname

Due to the weak ability of search engines to identify products, it is necessary to remember and refer to HTTP titles, favicons, and server banners in search results.



User Portal
217.145.100.200
TMT GmbH & Co. KG
Germany, Bayreuth

```
HTTP/1.1 200 OK
Date: Sun, 01 Jan 2023 05:27:52 GMT
Server: xxxx
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src https: data: ws:
```

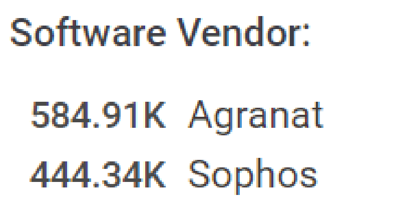
Censys

It is not possible to search for strings in SSL/TLS certificates all at once.
Need to search by Issuer or Subject of the certificate.

services.tls.certificates.leaf_data.subject_dn="*targetname*"
services.tls.certificates.leaf_data.issuer_dn ="*targetname*"
services.tls.certificates.leaf_data.issuer.common_name ="*targetname*"
services.tls.certificates.leaf_data.issuer.organization ="*targetname*"
services.tls.certificates.leaf_data.subject.common_name ="*targetname*"
services.tls.certificates.leaf_data.subject.organization ="*targetname*"

Cannot perform a targeted search for the organization name in the Whois of an IP address.
*Supplementation of the organization name in Whois also seems to be weak

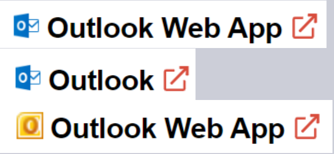
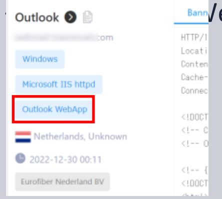
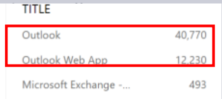
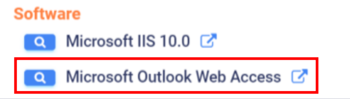
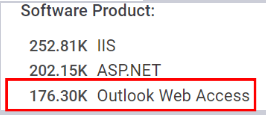
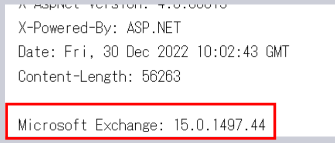
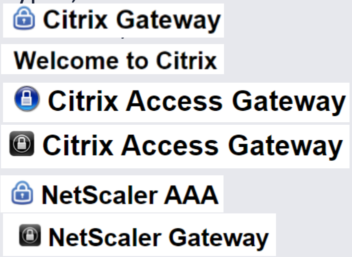
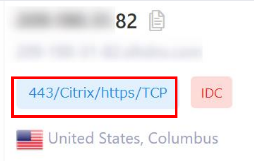
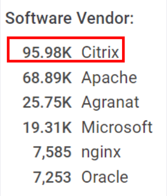
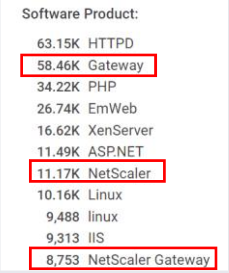
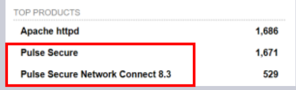
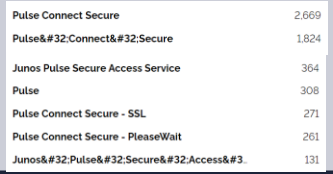
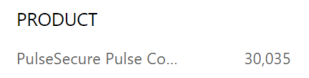
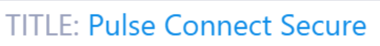
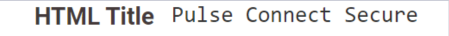
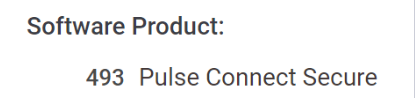
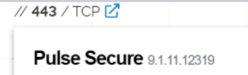
Because Censys performs product identification to some extent automatically
It is easy to extract the suspected infiltration sites. Some of them do not support identification, but that is done from the title and favicon hash.



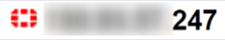
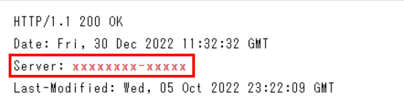
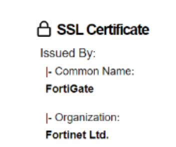
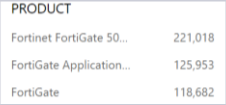
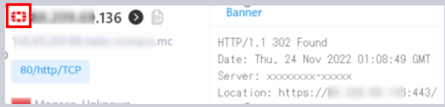
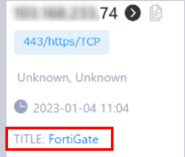
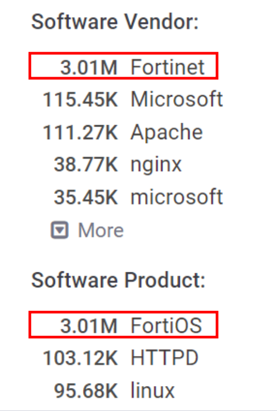
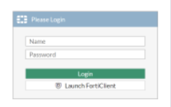
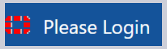
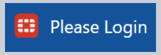
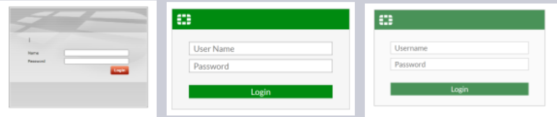
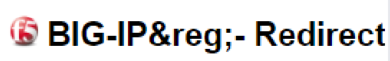
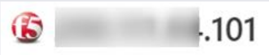
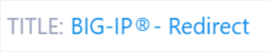
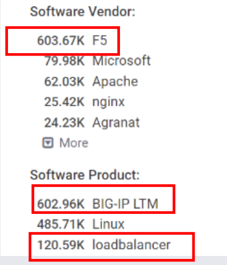
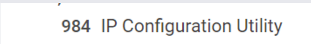
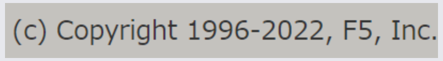
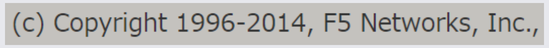
Software Vendor:

584.91K	Agranat
444.34K	Sophos

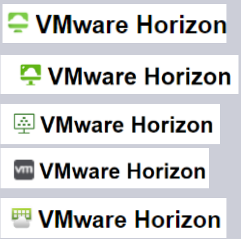
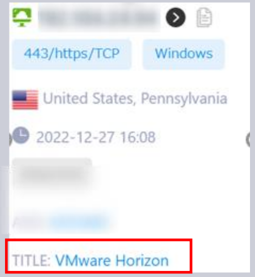
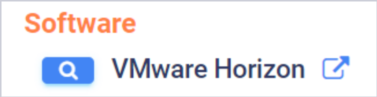
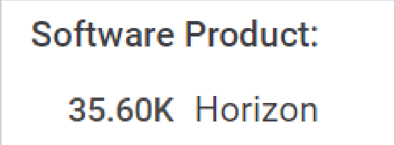
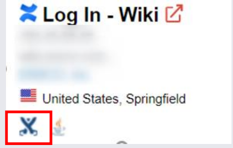
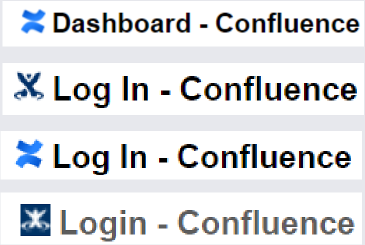
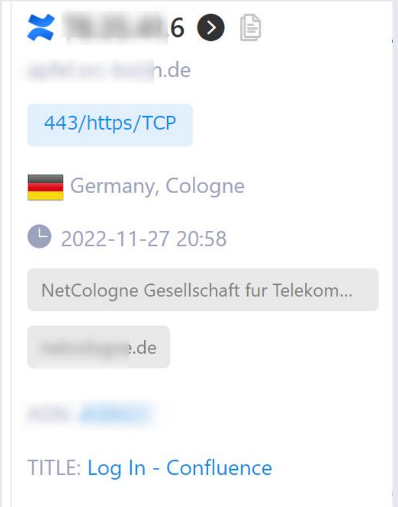
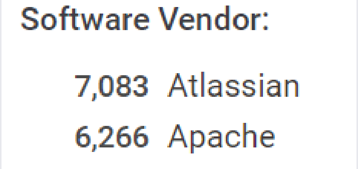
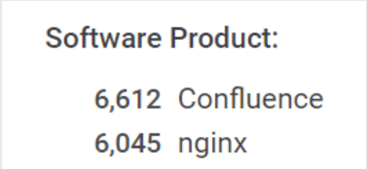
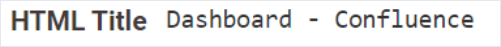
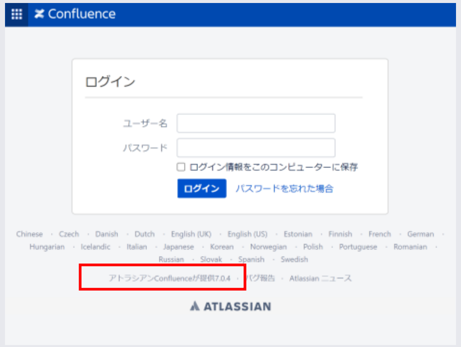
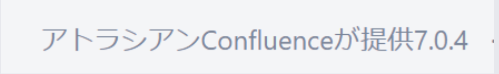
Product Identification Methods

Product	Shodan	ZoomEye	Censys	remarks
Exchange Server	Identified by HTTP title and favicon below  Outlook Web App Outlook Outlook Web App	The following queries can be used to identify the software, but due to weak capture, it is recommended to identify the software from the TITLE as in Shodan  Outlook [redacted].com Windows Microsoft IIS httpd Outlook WebApp Netherlands, Unknown 2022-12-30 00:11 Eurofiber Nederland BV  TITLE Outlook 40,770 Outlook Web App 12,230 Microsoft Exchange -... 493	Software identification is possible *But 2010 series are unidentifiable and must be determined from the title.  Software Microsoft IIS 10.0 Microsoft Outlook Web Access  Software Product: 252.81K IIS 202.15K ASP.NET 176.30K Outlook Web Access	The organization's domain is often tied to the certificate and is highly specific. Shodan records detailed versions so that patch levels and vulnerability presence can be determined (some information is missing from Censys and ZoomEye).  X-Powered-By: ASP.NET Date: Fri, 30 Dec 2022 10:02:43 GMT Content-Length: 56263 Microsoft Exchange: 15.0.1497.44
Citrix	Identified by HTTP title and favicon below (only some are listed due to the large number of types, note the words Citrix and  Citrix Gateway Welcome to Citrix Citrix Access Gateway Citrix Access Gateway NetScaler AAA NetScaler Gateway	software identifiable +app: "citrix"  [redacted]82 [redacted] 443/Citrix/https/TCP IDC United States, Columbus Also, as with Shodan, the HTTP title identifies	Vendor and software identification is possible. Note "Citrix" in the Vendor column and Netscaler and Gateway in the Software column.  Software Vendor: 95.98K Citrix 68.89K Apache 25.75K Agranat 19.31K Microsoft 7,585 nginx 7,253 Oracle  Software Product: 63.15K HTTPD 58.46K Gateway 34.22K PHP 26.74K EmWeb 16.62K XenServer 11.49K ASP.NET 11.17K NetScaler 10.16K Linux 9,488 linux 9,313 IIS 8,753 NetScaler Gateway	The organization's domain is often tied to the certificate and is highly specific. There is also information that detailed version and vulnerability can be determined from the HTML content. https://blog.fox-it.com/2022/12/28/cve-2022-27510-cve-2022-27518-measuring-citrix-adc-gateway-version-adoption-on-the-internet/
Pulse Secure	product: "Pulse Secure" can be used to identify the product, and the HTTP title can also be used to identify the product.  TOP PRODUCTS Apache httpd 1,686 Pulse Secure 1,671 Pulse Secure Network Connect 8.3 529  Pulse Connect Secure 2,669 Pulse Connect&#32;Secure 1,824 Junos Pulse Secure Access Service 364 Pulse 308 Pulse Connect Secure - SSL 271 Pulse Connect Secure - PleaseWait 261 Junos&#32;Pulse Secure&#32;Access&#3.. 131	Software identification is possible. +app: "PulseSecure Pulse Connect Secure"  PRODUCT PulseSecure Pulse Co... 30,035 Also, as with Shodan, the HTTP title identifies  TITLE: Pulse Connect Secure	Software identification is possible, but the accuracy is low, so as with Shodan, identification by HTTP title is recommended.  HTML Title Pulse Connect Secure  Software Product: 493 Pulse Connect Secure	The organization's domain is often tied to the certificate and is highly specific. Version identification is possible from the HTTP response (Shodan normalizes and displays the version).  // 443 / TCP Pulse Secure 9.1.11.12319 https://gist.githubusercontent.com/lz-censys/856ab8f2b68c2504d036ce34fdf3965d/raw/92f84c7e4753ed4de43bcaf9112d100501dbdbdc/pulse_vuln_matrix.csv

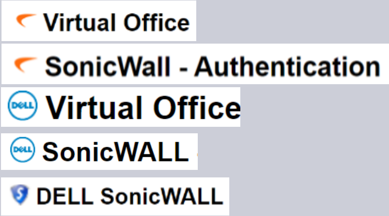
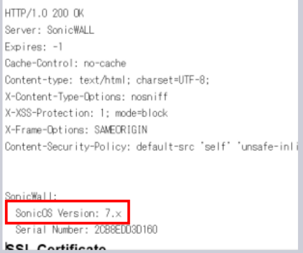
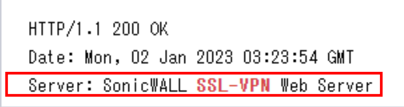
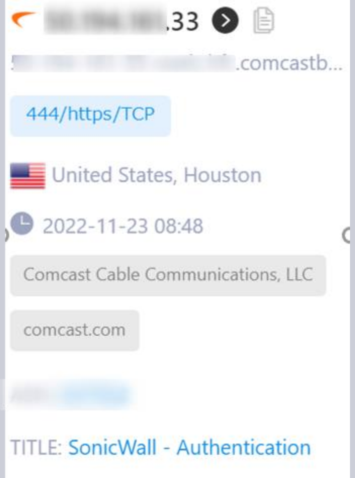
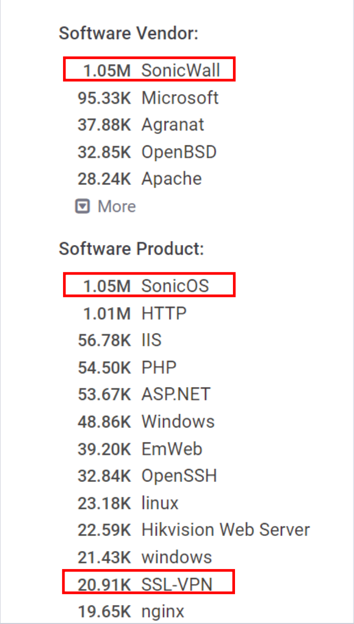
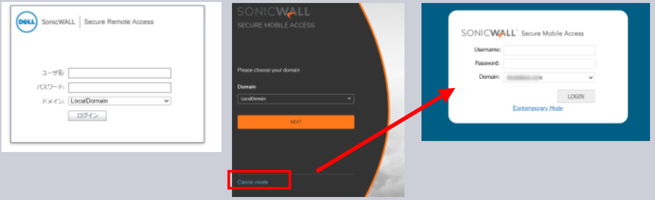
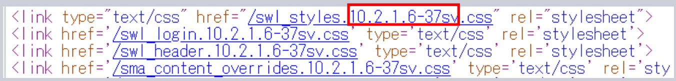
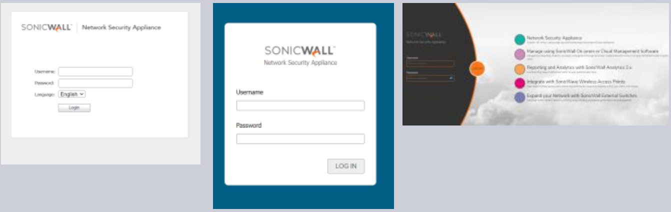
Product Identification Methods

Product	Shodan	ZoomEye	Censys	remarks
Fortinet	Favicon (displayed on all screens for users and administrators of Series 6 and below) *Series 7 favicons are not captured by Shodan and do not appear in search results.  [redacted]247 Judging from the responses characteristic of the login screen for users and administrators of Series 6 and the screen for users of Series 7  HTTP/1.1 200 OK Date: Fri, 30 Dec 2022 11:32:32 GMT Server: xxxxxxxx-xxxxx Last-Modified: Wed, 05 Oct 2022 23:22:09 GMT Determined from FortiGate/Fortinet in the certificate  SSL Certificate Issued By: |- Common Name: FortiGate |- Organization: Fortinet Ltd.	Software identification is possible +app: "FortiGate" +app: "Fortinet"  PRODUCT Fortinet FortiGate 50... 221,018 FortiGate Application... 125,953 FortiGate 118,682 Like Shodan, it can be identified by either the favicon hash or the title, but since not many cases are captured, the title is a better way to determine the identity.  [redacted].136 [redacted].mc 80/http/TCP Banner HTTP/1.1 302 Found Date: Thu, 24 Nov 2022 01:08:49 GMT Server: xxxxxxxx-xxxxx Location: https://[redacted]:443/  [redacted]74 443/https/TCP Unknown, Unknown 2023-01-04 11:04 TITLE: FortiGate	Vendor and software identification possible (Both Series 6 and below and Series 7 can be identified)  Software Vendor: 3.01M Fortinet 115.45K Microsoft 111.27K Apache 38.77K nginx 35.45K microsoft More Software Product: 3.01M FortiOS 103.12K HTTPD 95.68K linux	It is necessary to refer to the organization name in the IP address because the certificate issued by the product is configured and the organization is often not identifiable by SSL lookup. Login screen hash for right users http.html_hash:-1454941180  Please Login Name Password Login Launch FortiClient The major version can be identified from the favicon design on the login screen for users and administrators. Series 6 on the left, Series 7 on the right.  Please Login  Please Login Login screen hash for administrators (Series 6 and below only) http.html_hash:-1968569468 Login screen hash for administrators (Series 7 and below only) http.headers_hash:-841816352 The control panel can identify approximate versions by color and shape. From left to right: Series 5, Series 6, Series 7 (pastel in color)  *Screen colors for Series 6 and above are customizable, so other colors are available.
F5 BIG-IP	Identified by HTTP title and favicon  BIG-IP&reg;- Redirect	Notice the favicon and title similar to Shodan's.  [redacted].101  TITLE: BIG-IP® - Redirect +app: "F5 BIG-IP load balancer" can be used to identify the product, but the login screen of the same device is not displayed. It doesn't come out.	Vendor and software identification is possible, but it does not bring up a product login screen.  Software Vendor: 603.67K F5 79.98K Microsoft 62.03K Apache 25.42K nginx 24.23K Agranat More Software Product: 602.96K BIG-IP LTM 485.71K Linux 120.59K loadbalancer  984 IP Configuration Utility The following query identifies the login screen	It is necessary to refer to the organization name in the IP address because the certificate issued by the product is configured and the organization is often not identifiable by SSL lookup. It may be possible to infer a rough version from the notation in the footer of the login screen.  (c) Copyright 1996-2022, F5, Inc.  (c) Copyright 1996-2014, F5 Networks, Inc.,

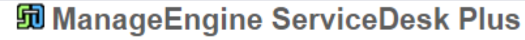
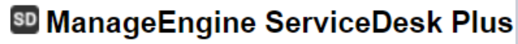
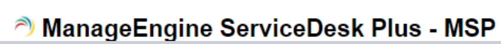
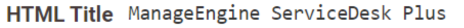
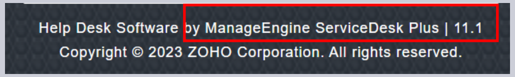
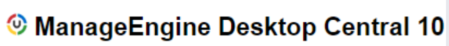
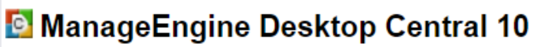
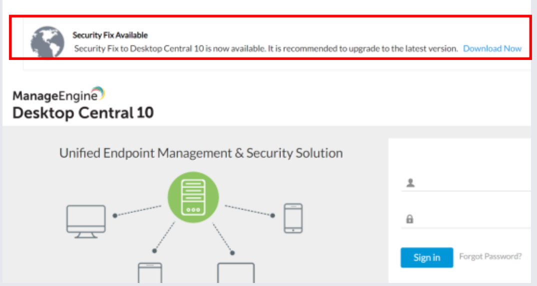
Product Identification Methods

Product	Shodan	ZoomEye	Censys	remarks
VMware Horizon	Identified by HTTP title and favicon  VMware Horizon VMware Horizon VMware Horizon VMware Horizon VMware Horizon	+app: "VMware Horizon" to identify the product, also identifiable by HTTP title and favicon.  [redacted] 443/https/TCP Windows United States, Pennsylvania 2022-12-27 16:08 [redacted] TITLE: VMware Horizon	Vendor and software identification possible  Software VMware Horizon  Software Product: 35.60K Horizon	The organization's domain is often tied to the certificate and is highly specific. Log4j vulnerability inherent in the product is often exploited, but it is not possible to identify the version or determine the vulnerability in OSINT from the outside.
Atlassian Confluence	Can be identified by HTTP.COMPONENT:Confluence (note the mark in the red box)  Log In - Wiki [redacted] United States, Springfield HTTP titles and favicons can also be identified, but note that titles and favicons are often customized.  Dashboard - Confluence Log In - Confluence Log In - Confluence Login - Confluence	+Software can be identified by HTTP title and favicon.  [redacted]6 [redacted]n.de 443/https/TCP Germany, Cologne 2022-11-27 20:58 NetCologne Gesellschaft fur Telekom... [redacted]e.de [redacted] TITLE: Log In - Confluence	Vendor and software identification possible  Software Vendor: 7,083 Atlassian 6,266 Apache  Software Product: 6,612 Confluence 6,045 nginx  HTML Title Dashboard - Confluence	The name of the company is often included in the certificate, making the organization highly identifiable. The version is displayed in the footer of the login screen so that vulnerability can be determined  Confluence ログイン ユーザー名 パスワード □ ログイン情報をこのコンピューターに保存 ログイン パスワードを忘れた場合 Chinese · Czech · Danish · Dutch · English (UK) · English (US) · Estonian · Finnish · French · German · Hungarian · Icelandic · Italian · Japanese · Korean · Norwegian · Polish · Portuguese · Romanian · Russian · Slovak · Spanish · Swedish アトラシアンConfluenceが提供7.0.4 · バグ報告 · Atlassian ニュース ATLASSIAN  アトラシアンConfluenceが提供7.0.4 ·

Product Identification Methods

Product	Shodan	ZoomEye	Censys	remarks
SonicWall	Product: Can be identified by "SonicWALL". Can be identified in search results by HTTP title and favicon  Virtual Office SonicWall - Authentication Virtual Office SonicWALL DELL SonicWALL The Nsa series of UTM/FW has a major version notation in the following location of the server response in the search results  HTTP/1.0 200 OK Server: SonicWALL Expires: -1 Cache-Control: no-cache Content-type: text/html; charset=UTF-8; X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN Content-Security-Policy: default-src 'self' 'unsafe-inli SonicWall: SonicOS Version: 7.x Serial Number: 2C88ED03D160 SSL Certificate The SMA series of SSL VPNs have the following response  HTTP/1.1 200 OK Date: Mon, 02 Jan 2023 03:23:54 GMT Server: SonicWALL SSL-VPN Web Server	+app: "SonicWALL" to identify it  [redacted].33 [redacted].comcastb... 444/https/TCP United States, Houston 2022-11-23 08:48 Comcast Cable Communications, LLC comcast.com [redacted] TITLE: SonicWall - Authentication	Vendor and software identification possible  Software Vendor: 1.05M SonicWall 95.33K Microsoft 37.88K Agranat 32.85K OpenBSD 28.24K Apache More Software Product: 1.05M SonicOS 1.01M HTTP 56.78K IIS 54.50K PHP 53.67K ASP.NET 48.86K Windows 39.20K EmWeb 32.84K OpenSSH 23.18K linux 22.59K Hikvision Web Server 21.43K windows 20.91K SSL-VPN 19.65K nginx *SSL-VPN identifies the SMA series of VPNs.	It is necessary to refer to the organization name in the IP address because the certificate issued by the product is configured and the organization is often not identifiable by SSL lookup. Refer to the HTML source of the login screen of the following design for SecureMobileAccess and Secure Remote Access series to check the detailed version and identify the vulnerability. *Need to switch to ClassicMode (rightmost) as it is not displayed in Contemporary Mode (second from left) even in SMA. *Not identifiable on similarly designed Network Security Appliance and its SSLVPN login screen  SonicWALL Secure Remote Access ユーザ名: パスワード: ドメイン: LocalDomain ログイン SONICWALL SECURE MOBILE ACCESS Please choose your domain Domain LocalDomain NEXT Classic mode SONICWALL Secure Mobile Access Username: Password: Domain: LOGIN Contemporary Mode  <link type="text/css" href="/swl_styles.10.2.1.6-37sv.css" rel="stylesheet"> <link href='/swl_login.10.2.1.6-37sv.css' type='text/css' rel='stylesheet'> <link href='/swl_header.10.2.1.6-37sv.css' type='text/css' rel='stylesheet'> <link href='/sma_content_overrides.10.2.1.6-37sv.css' type='text/css' rel='sty The Nsa series of UTM/FWs listed as Network Security Appliance can be identified by the design of the login screen as major versions, from left to right: Series 5, 6, and 7 (Series 5 and 6 also have DELL logos). However, the detailed version cannot be identified.  SONICWALL Network Security Appliance Username Password LOG IN

Product Identification Methods

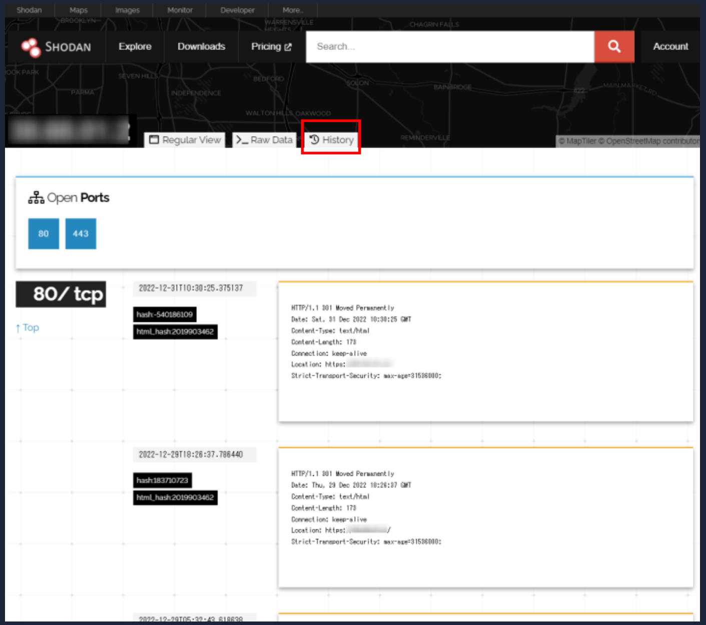
Product	Shodan	ZoomEye	Censys	remarks
Zoho ManageEngine ServiceDesk Plus	Identified by HTTP title and favicon  ManageEngine ServiceDesk Plus  ManageEngine ServiceDesk Plus  ManageEngine ServiceDesk Plus - MSP	Judging from HTML title as the product is not identifiable (no favicon is collected) TITLE: ManageEngine ServiceDesk ...	Judging from the HTML title as the product is not identifiable.  HTML Title ManageEngine ServiceDesk Plus	If HTTPS is set up, the name of the company is often listed in the certificate, making it highly possible to identify the organization. Version information is displayed in the footer of the login page, so it is possible to know the approximate version.  Help Desk Software by ManageEngine ServiceDesk Plus | 11.1 Copyright © 2023 ZOHO Corporation. All rights reserved.
Zoho ManageEngine Desktop Central	Identified by HTTP title and favicon  ManageEngine Desktop Central 10  ManageEngine Desktop Central 10	Judging from HTML title as the product is not identifiable (no favicon is collected) TITLE: ManageEngine Desktop Cen...	Since the product is not identifiable, we can only judge from the HTML title, but only one hit was found, and it is possible that the title of the same product was not captured by Censys.	If HTTPS is set up, the name of the company may be listed in the certificate, and the organization may be identified. The version information is not displayed on the login screen, but the Security patch application notification is displayed, so the version information may be identifiable from this.  Security Fix Available Security Fix to Desktop Central 10 is now available. It is recommended to upgrade to the latest version. Download Now ManageEngine Desktop Central 10 Unified Endpoint Management & Security Solution Sign in Forgot Password?

Check for version upgrades and server outages

- Continuously confirming the status of the server suspected of intrusion provides useful information for guessing the intrusion route.
  - Inference of version upgrades (patching) from server responses
  - Check for communication by accessing the Web. Inaccessible ≒ Possibility of removal

- Device search engines also provide a function to refer to past results, so make use of this function as appropriate.

See Shodan:History tab



[redacted]

2022-12-31T10:30:25.375137

hash:-540186109

html_hash:2019903462

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 31 Dec 2022 10:30:25 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: https:[redacted]
Strict-Transport-Security: max-age=31536000;
```

2022-12-29T18:26:37.786440

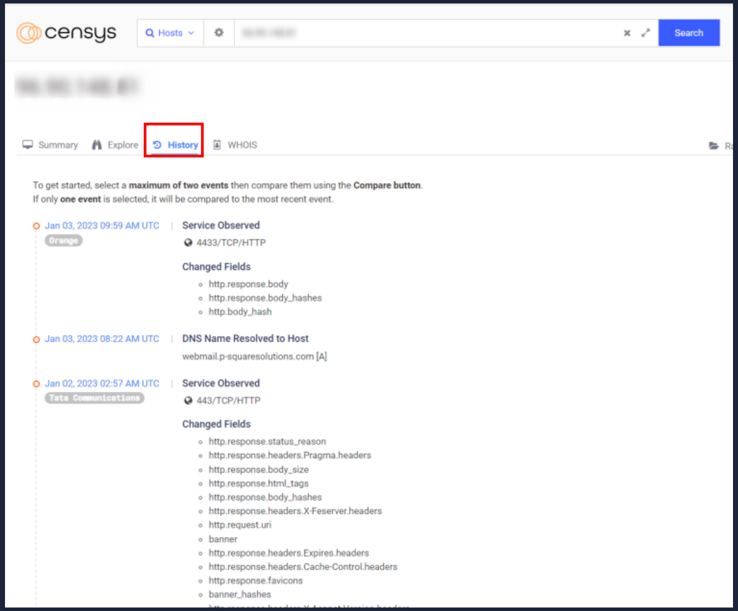
hash:183710723

html_hash:2019903462

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 29 Dec 2022 18:26:37 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: https:[redacted]/
Strict-Transport-Security: max-age=31536000;
```

2022-12-29T05:32:43.618638

See Censys:History tab



[redacted]

To get started, select a **maximum of two events** then compare them using the **Compare button**.
If only **one event** is selected, it will be compared to the most recent event.

Jan 03, 2023 09:59 AM UTC | **Service Observed**
Orange
4433/TCP/HTTP

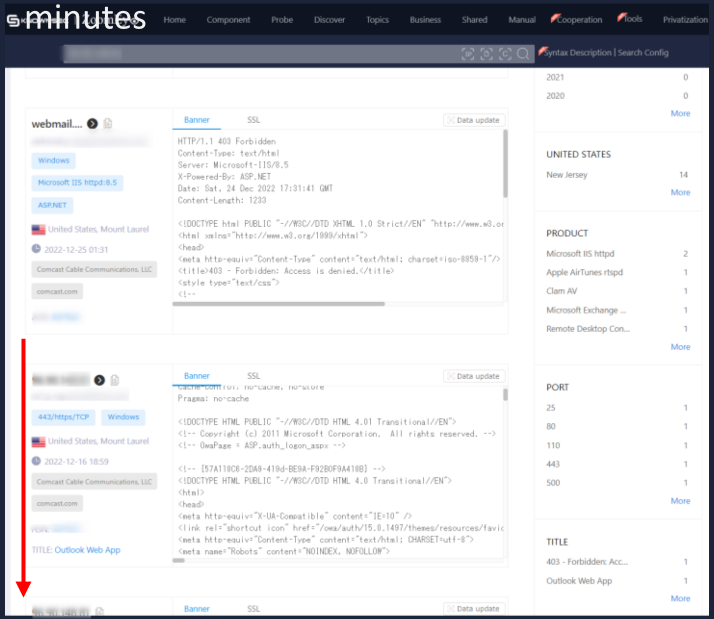
Changed Fields
- http.response.body
- http.response.body_hashes
- http.body_hash

Jan 03, 2023 08:22 AM UTC | **DNS Name Resolved to Host**
webmail.p-squaresolutions.com [A]

Jan 02, 2023 02:57 AM UTC | **Service Observed**
Tata Communications
443/TCP/HTTP

Changed Fields
- http.response.status_reason
- http.response.headers.Pragma.headers
- http.response.body_size
- http.response.html_tags
- http.response.body_hashes
- http.response.headers.X-Feserver.headers
- http.request.uri
- banner
- http.response.headers.Expires.headers
- http.response.headers.Cache-Control.headers
- http.response.favicons
- banner_hashes

ZoomEye: Scroll through search results to view past minutes



2021	0
2020	0
UNITED STATES	
New Jersey	14
PRODUCT	
Microsoft IIS httpd	2
Apple AirTunes rtspd	1
Clam AV	1
Microsoft Exchange ...	1
Remote Desktop Con...	1
PORT	
25	1
80	1
110	1
443	1
500	1
TITLE	
403 - Forbidden: Acc...	1
Outlook Web App	1

webmail....

Windows
Microsoft IIS httpd:8.5
ASP.NET
United States, Mount Laurel
2022-12-25 01:31
Comcast Cable Communications, LLC
comcast.com

```
HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 24 Dec 2022 17:31:41 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.or
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
```

[redacted]

443/https/TCP
Windows
United States, Mount Laurel
2022-12-16 18:59
Comcast Cable Communications, LLC
comcast.com
TITLE: Outlook Web App

```
Cache-Control: no-cache, no-store
Pragma: no-cache

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<!-- Copyright (c) 2011 Microsoft Corporation.  All rights reserved. -->
<!-- OwaPage = ASP.auth_logon_aspx -->

<!-- {57A118C6-2DA9-419d-BE9A-F92B0F9A418B} -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=10" />
<link rel="shortcut icon" href="/owa/auth/15.0.1497/themes/resources/favic
<meta http-equiv="Content-Type" content="text/html; CHARSET=utf-8">
<meta name="Robots" content="NOINDEX, NOFOLLOW">
```

[redacted]

In Closing

We believe that identifying and defending the external public servers that attackers target will remain an important measure in the coming years.

Especially in the Asian region, including Japan, the speed of response is not fast enough, so it is necessary to strengthen some countermeasures.
We hope that we can move the current situation in a better direction with all of you here today.

The third part of the survey method needs additional validation.
If you have any questions, we would be happy to hear from you at the account on the right.