DIVD

開

Exploring Collaboration on Coordinated Vulnerability Disclosure in Japan

Date	17 December 2024
Author	Chris van 't Hof
Editor	Serena de Pater
Version	1.0
Status	Open to public

Exploring Collaboration on Coordinated Vulnerability Disclosure in Japan

Content

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Introduction

With the support of the Dutch embassy in Tokyo, I have researched Coordinated Vulnerability Disclosure (CVD) in Japan. I had the opportunity to travel to Japan from October 22 to November 22.

During my stay, I interviewed security researchers from various governmental institutes, companies, and universities and spoke with hackers, most of whom were foreign nationals residing in Japan. I also participated in conferences and meetings: KEIO Cybersecurity Conference (30-10/1-11), Cyber Risk Meetup (1-11), TengueSec meetup (13-11), CodeBlue (14-11/15-11), and AVTokyo (16-11). One of the highlights of my trip was organizing a CVD expert meeting with the Dutch embassy on the 13th of November. The last days I spent in the beautiful coastal village of Kamakura to start writing this report.

The research questions for this mission are:

1. How does CVD practice in Japan compare to the Netherlands?
2. What are the legal risks in Japan of scanning and notifying for vulnerabilities without informed consent?
3. How do governmental policies and programs on CVD in Japan compare to those of the Netherlands?
4. Which vulnerability disclosure projects or programs in Japan can we learn from?
5. Which opportunities for future collaboration are there for DIVD in Japan?

For each of my reports on missions to Japan I select a Japanese word or text to provide broader meaning to the issue. For this report, it's the kanji sign 開, which means 'open'. It stands for the systems that are open because of unpatched vulnerabilities, but also for how DIVD works. We communicate openly to everyone: directly, for free and with our real names, not using pseudonyms as most hackers do. Open is also this report. Use of the text is under Creative Commons, and it is open for any comments to improve it for future versions. Finally, 開 is also used for the beginning of something new, in this case, our collaboration on CVD in Japan.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Background

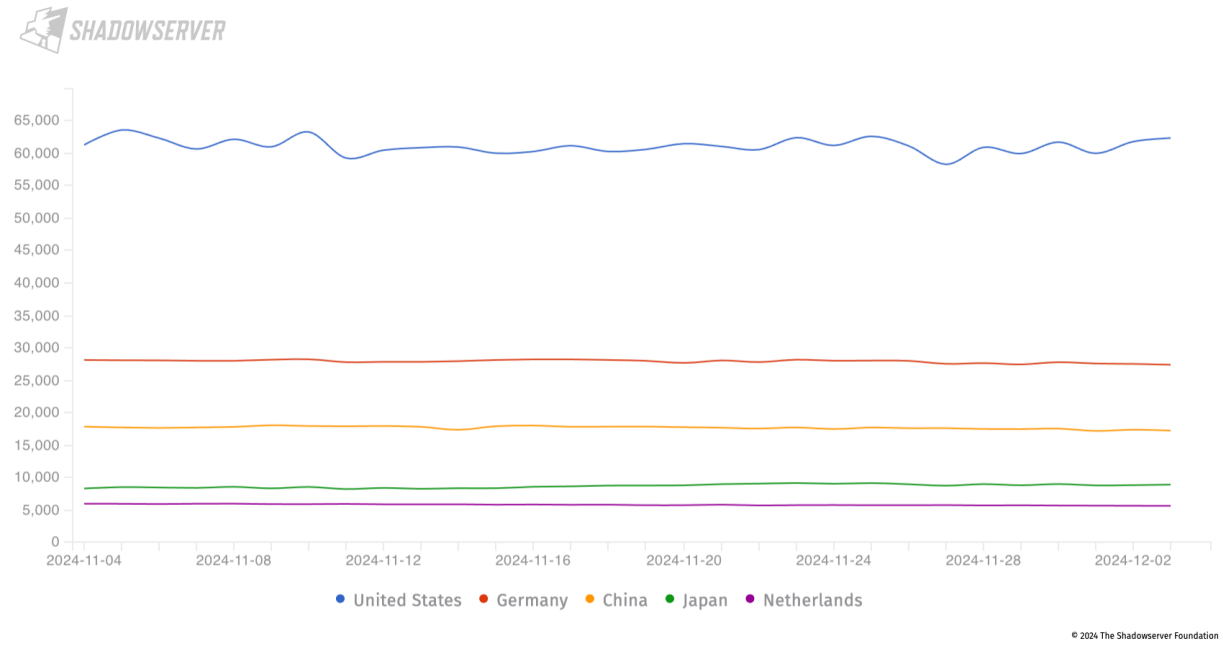
This was my sixth research mission to Japan. In the previous ones, I also investigated IT topics such as RFID, virtual worlds, healthcare robotics, and IoT—or, in Japan, more commonly known as the Ubiquitous Network Society. I carried out these projects for the Rathenau Institute, also in collaboration with the Dutch embassy in Japan. This mission is for DIVD.

Coordinated Vulnerability Disclosure (CVD) is the core business of DIVD, the Dutch Institute for Vulnerability Disclosure. Our volunteers scan the internet for Common Vulnerabilities & Exposures (CVEs) and send the owners of these systems a notification to patch. Over the last five years, we have done 152 cases and sent 1.3 million notifications. We also search for and disclose new vulnerabilities (zero days) and registered over 100 CVEs, as DIVD is a CVE Numbering Authority (CNA). We also report open databases and report to victims of stolen credentials. We do this in a Dutch way: honest, direct, and for free.

DIVD's work is permitted in the Netherlands thanks to case law rulings and guidelines from the Dutch Public Prosecution Office and the National Cyber Security Center (NCSC). The Dutch government also recognizes DIVD as a trusted entity and we share our findings with the NCSC. Each vulnerable IP receives a notification from DIVDs CSIRT first and then another one from them. This procedure is followed by an increasing number of countries worldwide: Belgium, Germany, Denmark, Finland, Austria, Poland, Portugal, Slovenia, Slovakia, Estonia, Hungary, Ireland, UK, Israel, Brazil, Singapore, Taiwan, US and Australia. With this mission, we hope Japan will join too.

Let’s have an outside-in view of vulnerabilities in Japan and start with Shadow Server. They scan for vulnerabilities too, but less intrusive and large scale and don’t report directly to the potential victims. Country reports go to CERTs and feed the rich statistics they publish online. Naturally, we collaborate with Shadow Server, as we have a shared mission to make the digital world safer. I asked its managing director, Piotr Kijewski, how he perceives CVD in Japan. According to him, Japan is pretty safe. Compared to other countries, the number of vulnerabilities is relatively low. The graph below shows the number of unique IPs vulnerable to 100 CVEs Shadow Server scans. While Japan has a population of 125 million people and 126 million IP addresses, it scores just above the Netherlands and way under Germany, China, and the US.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl



DIVD scans one CVE at a time, more thoroughly and reports to the owners of the systems by enriching contact information. Then, a more fluctuating image appears if we take a random sample of cases and compare Japan to the rest of the internet. For some applications, there are virtually no vulnerable IP addresses, while for others, Japan takes almost 10% of the total number. The people behind these systems received a notification from DIVD, but we don't know what they thought of it or if they followed our advice. We therefore need to find an organization in Japan willing to forward our notifications, as other countries do. Perhaps they can also explain to the Japanese citizens who we are and why we do this. This is the primary goal of our mission.

Case	Total IP addresses	Unique Japanese IP	% of Japanese IP
2024-00015	1,205	4	0.33
2024-00016	7,947	303	3.81
2024-00021	2,848	282	9.9
2024-00025	8,017	642	8
2024-00028	1,742	25	1.44
2024-00030	579	0	0
2024-00032	2,490	57	2.29
2024-00039	34	1	2.94

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

General impression of CVD in Japan

The methodology for this mission is simple: go to conferences, talk to people, arrange interviews at their organizations, and ask them the questions mentioned above. My impression of these talks is that CVD in Japan is generally perceived more narrowly as reporting newly found vulnerabilities, zero-days, to the software producers. The goal is to allow the vendor to provide a patch before the vulnerability is abused. Sometimes, the disclosure is published as a CVE by one of the Japanese CVE Numbering Authorities. Scanning and notifying CVEs, as DIVD does, is only done by security teams who have their own organization as scope.

No notification without informed consent

In Japan, doing CVD on a broader scope and without informed consent is perceived as very rare. Security researchers generally fear prosecution as they may violate cyber security and privacy laws. Hackers at security meetings also stated they would get into trouble if their boss knew about their CVD activities and would only disclose vulnerabilities if they were sure they would not be prosecuted. Some told me they were holding over a hundred zero-days and didn't know what to do with them.

A common statement at hacker events was: "I only report if they provide a bug bounty." This is not only for the financial gains but also to ensure the receiving side is open to their reports. Talking to companies and the bug bounty platform Bug Crowd, I learned very few Japanese organizations have a bug bounty program. Also, I found none with a CVD policy or vulnerability notification page.

Active cyber defense

CVD also received very little attention at the cyber security conferences I visited. The main focus appears to be combating APTs, most notably Chinese. Fueled by the American delegations, the Japanese government is called upon to leave its pacifistic standpoint and join in hacking back adversaries. The keyword here is "active cyber defense" to avoid the sensitive meaning of "offensive cyber capabilities." Several speakers urged legislation to make hacking back possible.

A form of active cyber defense that seems to fit Japanese culture more is putting honey pots online and monitoring network traffic. Panasonic for example, puts each new IoT device online to monitor any attack and improve the product. NICT has over 300.000 unused

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

IP addresses as black hole sensors, swallowing malicious traffic without the threat actor knowing it. This way, they let the adversaries do the work by monitoring the attacks and learn how to deal with them.

I believe active cyber defense should also involve large-scale vulnerability disclosure, but there appeared to be no room for that in this discourse. At KEIO, Yuji Ukai (CEO, FFRI Security, Inc.) talked about grassroots intel sharing and appealed to us to embrace these communities and formalize information exchange. No one responded. A panel of five hackers was interviewed, but only on threats, not on what they could do with the vulnerabilities they find. Finally, I addressed some delegates of the Mitre Corporation, the American organization that co-hoasted the conference and started the Common Vulnerability Scoring System (CVSS) 25 years ago. I asked them why vulnerability disclosure wasn't on the agenda. The head of the delegation stated: "Oh, that's for the engineers. We do high strategic level."

Yes we scan

After three days of cyber security talks and no vulnerability disclosure, I was pleasantly surprised by the presentation of Kondo Reiko. She is the Deputy Director-General for ICT R&D and Cybersecurity Policy at the Ministry of Internal Affairs and Communications. First, she gave an overview of what her ministry does to help Japanese citizens become more secure. Then she stated that the Japanese government itself actively scans all IoT devices within the Japanese IP space for weak passwords, vulnerabilities, and botnet infections. The cabinet changed privacy laws to do this. The project is called NOTICE, which stands for National Operation Towards IoT Clean Environment and it is carried out by NICT, the National Institute of Information and Communications Technology.

So, my first impression of the practice of CVD in Japan is that it refers in the narrow sense of disclosing zero days to vendors. Scanning and notifying on known vulnerabilities without informed consent is only done by the government and is uncommon for citizens who just want to help out too. So, how strict is the Japanese law on hacking for good? And, more importantly, will DIVD and I get into trouble for doing so? We must dive into the legal aspects and compare these to how CVD policy works. I, therefore, visited JPCERT/CC, and NICT, and asked them to join our CVD expert meeting at the Dutch embassy.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

The legal aspects of CVD in Japan

At the CVD expert meeting, we were honored by the participation of two attorneys of law who have a long track record in investigating CVD: Mayu Arimoto and Ikuo Takahashi. My impression of their analysis is that the legality of CVD is similar to that of many other countries. In principle, one might infringe on several laws by doing security research on systems without informed consent and risk prosecution. Still, few researches led to a court case. For those that did: what laws applied and did ruling lead to useful jurisprudence?

Japanese criminal laws on hacking

The most relevant law in this context is the Penal Code (刑法 Keihō) of Japan. It is one of six Codes that form the foundation of modern Japanese law. The penal code is also called "ordinary criminal law" or "general criminal law" as it relates to general crimes. These are the articles that are aimed at cybercriminals compromising businesses, such as: "Damage to Credibility; Obstruction of Business" (art. 233) and "Forcible Obstruction of Business" (art. 234), specified in article 234-2 as "Obstruction of Business by Damaging a Computer". Article 168-2 of the Act on "Making of Electronic or Magnetic Records Containing Unauthorized Commands" is one the most precise descriptions of what hacking involves.

"A person who, without legitimate grounds, creates or provides any of the following records (electronic or magnetic records that give unauthorized commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention) including electronic or magnetic records for the purpose of using them for executing commands on another person's computer is punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen."

One might think this article could also be used to prosecute researchers with good intentions. Still, according to Muya, it is: "more used for computer malware, instead of hacking. We call this crime as 'computer malware crime'. For hacking, Articles 233 and 234 of the Penal Code is more often used than 168-2". So, it's not about accessing computers but rather about the damage one may inflict by doing so. Here, two acts are more applicable.

First, there is the "Act on Prohibition of Unauthorized Access". This Act prohibits unauthorized computer access (3 yr / 1M JPY), obtaining or wrongfully storing someone else's credentials, facilitating unauthorized computer access and illicitly requesting the input of credentials (1 yr / 0.5M JPY). Second, there is the Radio Act. Article 109-2 states that:

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

"When any person, who has intercepted encrypted communications or mediates encrypted communications and has received the relevant encrypted communications, has decoded their content for the purposes of divulging or taking advantage of secrets contained in the relevant encrypted communications, that person is punished by imprisonment for a period not exceeding 1 year or a fine not exceeding 500,000 yen."

Cracking encryption for the sole purpose of proving it's weak can in some way be perceived as "taking advantage of secrets". Still, here article 35 of the Penal Code is relevant: "An act performed in accordance with laws and regulations or in the pursuit of lawful business is not punishable." This Leaves us with the question: when is hacking judged as a lawful business?

Case law on hacking

As in the Netherlands and many other countries, Japan has had its court cases too, leading up to jurisprudence, which may serve as a guideline for future verdicts. The most relevant example is a hacker who succeeded in getting free access to an organization's paid online content and presented his findings at a hacker conference before notifying the organization. He was prosecuted and was convicted guilty with a suspended sentence. Unfortunately, the court did not clearly state whether the act of entering the systems to prove its vulnerability was in itself a lawful business. The court just judged that presenting the finding without informed consent was improper and sentenced him. There are three other cases, but they have an even less clear verdict in favor of helpful hackers. So in the end, there is virtually none.

In the Netherlands, we had a similar case, that did lead up to useful jurisprudence. It is known as "Henk Krol versus Diagnostiek voor U" of 2014. Here an amateur hacker showed his proof to the media without giving the system owners any chance to take measures. The owner turned out to be a hospital and took Krol to court. To the Dutch government, this case was a test for the new guidelines published by the Dutch Public Prosecution Office. These legal guidelines determine a hack is justified if it serves a societal need (improves security), the means are proportional (make systems safer, not unsafer) and the researcher followed subsidiarity (took the least severe means at hand).

As in the Japanese case, publishing without giving time to fix was deemed improper. Still, the very act of entering systems to prove they are vulnerable was perceived as a societal need and therefore legal business, as in some preceding Dutch court cases. It's just that the hacker had downloaded too much data (proportionality) and could have used less

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

severe means of disclosure (subsidiarity). Ever since, it is quite clear to Dutch hackers what is meant by legal business. Moreover, in most countries, these three principles apply to intelligence and law enforcement agencies, while in the Netherlands, they also apply to helpful hackers.

According to the lawyers and other participants at the expert meeting, Japan has no such guidelines from the Public Prosecution Office in CVD. The experts think that in Japan, there is much room for discussion and interpretation to reach a consensus on court cases like these. Still, one must not underestimate the deterrence effect of the possibility of being prosecuted, which is precisely what I noticed when talking to hackers in Japan.

Japan does have more general guidelines on CVD. They are from METI, the Ministry of Economy, Trade and Industry, and a number of organizations that have been involved in CVD policy since 2004. Will these help to determine whether our work is legal business?

Comparing governmental policy on CVD in Japan and the Netherlands

In the Netherlands, CVD has been governed since 2013, mainly by the National Cyber Security Center, which falls under the Ministry of Justice & Security. The first “Guideline for the Practice of Responsible Disclosure” was published in 2013, along with those of the Public Prosecution Office mentioned above. A revised “Guideline for Coordinated Vulnerability Disclosure” was published by the NCSC in 2017. Together with the Digital Trust Center of the Ministry of Economic Affairs and CSIRT-DSP (Computer Incident Response Team - Digital Service Providers), the NCSC has been coordinating vulnerability disclosures in the Netherlands from the governmental side. In 2025, the three will merge into one center.

In Japan, the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs & Communication (MIC) have been actively regulating and promoting CVD for over 20 years. Several institutes participate in vulnerability disclosure, each with a different relationship to Japan’s government. There is also a Guideline for CVD, but to my impression, it only provides practical rules for CVD in a narrow sense of disclosure zero days to vendors and provides no legal base to support helpful hackers as the Dutch guideline does. Nonetheless, Japan looks very effective in solving vulnerabilities in IoT devices, not by hackers, but by the government itself.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Institutionalizing cyber security in Japan

Looking at the organizational charts in presentations and on governmental websites, we can see a broad range of institutes, from top-down, across, and next to the Japanese government. These are:

Cybersecurity Strategic Headquarters

This headquarters was established under the Cabinet in November 2014 to effectively and comprehensively promote cybersecurity policies. It is headed by the Chief Cabinet Secretary, with his deputy, the Minister in charge of Cybersecurity, and is composed of the Chairman of the National Public Safety Commission, the other relevant Ministers, and experts from academia and business sectors.

National center of Incident readiness and Strategy for Cybersecurity

NISC was established in 2015. It's a follow-up of the National Information Security Center, which was established in 2005, under the same abbreviation. It currently functions as a secretariat of the Cybersecurity Strategy Headquarters, working with the public and private sectors on various activities to create a free, fair, and secure cyberspace. Departments relevant to CVD are its Incident Handling and External Collaboration Unit and the Cyber Response and Intelligence Unit. NISC is currently reorganized to integrate more governmental agencies.

National Institute of Information and Communications Technology

NICT operates under the Ministry of Internal Affairs & Communication (MIC), runs the National Cyber Observation Center and executes the NOTICE project (see section below).

Information technology Promotion Agency

IPA is affiliated with METI. As the title implies, this agency provides a broad range of services to improve the adoption of Information Technology in Japan. Regarding CVD, any researcher can report web-facing vulnerabilities to the agency, which will forward the reports to the website operator or JPCERT-CC.

JPCERT/CC

The Japanese Computer Emergency Response Team Coordination Center is an independent institute founded in 1996 and currently funded by METI. The center handles incidents,

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

analyses and shares information on online threats, monitors internet traffic, and has published Vulnerability Notes with Advisories since 2004. They use the feeds of Shadow Server, with which DIVD collaborates. It's also been Japan's Root CNA since 2010 and assigned 309 CVE IDs in FY2023.

Next to these institutes, Japan has a Cybersecurity Coordination Office and Cyber Task Force at MIC, an independent Cybersecurity Council and AIST, the National Institute of Advanced Industrial Science and Technology who may play a role in CVD. In Japan, ten companies are also CVE Numbering Authority: LY, Mitsubishi, NEC, Toshiba, Hitachi, Panasonic, Canon, Yokogawa Group, OpenAM Consortium and OMRON. Universities have their own CSIRT network, with 194 members. Many experts I spoke claim the CSIRT community in Japan is very active, which could explain the low number of online vulnerabilities Shadow Server finds in scanning Japan.

METI guiding CVD partnerships

The first CVD guideline was METI's Standards for Handling Information Related to Vulnerabilities in Software, which was enacted in 2004 and revised in 2014 as Handling Regulations for Information Related to Vulnerabilities in Software Products. It was newly enacted in 2017 and again revised and published in September 2024. The way processes are set up aligns with the ISO/IEC 29147 standard on vulnerability disclosure.

A summary of how the guideline works in practice is provided by JPCERT-CC in their "Information Security Early Warning Partnership - Overview of Vulnerability Handling Process" (12 September 2024). The scope for CVD contains "vulnerabilities that may affect many or unspecified persons, specifically software products widely used in Japan and web applications that run on websites deemed to be accessed primarily from Japan (for example, websites written in Japanese, websites running on a ".jp" domain)".

The Process Overview recommends "actions to achieve an appropriate flow of vulnerability-related information to relevant parties." These parties include vulnerability finders, software developers, and website operators. If researchers find a vulnerability, they can report it to IPA, which will validate the finding. IPA will ask finders not to share the vulnerability with third parties and if their contact information can be shared.

If it's a software vulnerability, IPA will forward the report to JPCERT/CC, which will try to contact the software developer. If the software developer cannot be reached, the name may be published to contact the developer publicly. Ideally, they respond, fix the software,

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

publish or have JPCERT/CC publish a CVE and credit the finder. If there is no response and a year has passed since the initial report, the finders may issue a withdrawal request to IPA and disclose information on the discovered vulnerability themselves. The document does not state if the finder gets any support if the publication gets them in trouble.

If the reported vulnerability is found on a website, IPA will try to contact the website operator and urge them to fix the vulnerability, warn its users, and report to IPA on progress. The operator is expected to respond within three months. Here, too, finders are on their own when reporting themselves.

The IPA website presents the number of reports. According to it, the cumulative number of reports made to IPA in the past 20 years is 19,123. Of these, 5,904 were on software products, and the rest, 13,219, were on websites. Currently, IPA handles a stable average of four reports a day.

Are you allowed to hack for good?

The Process Overview does not mention what would happen if the operator doesn't want to fix the vulnerability or does not respond at all. Therefore, finders might still get into trouble if the mediation by IPA or JPCERT doesn't work out and they decide to publish the vulnerability themselves. The Process Overview does help them by providing some examples of disclosures that may not violate laws:

- "In a case where a user of a web application accesses the application normally by logging in using valid procedures and where the existence of a vulnerability can be inferred by observing the content of the communication between the browser and the server."
- "You enter a text string containing HTML tags into a data entry field on a web page, and the entered text string is displayed as-is and if it is predicted that this could cause a security problem on the website."
- "In a case where a user replaces a string of numbers in a URL that is assumed to represent a date or page number with a different string of numbers for the purpose of normal random page browsing, not for the purpose of evading access control restrictions, and where, as such result, the user accidentally accesses a website that is presumed to be inaccessible according to social standards. (Provided, however, that an act of actively trying many different strings of numbers may be considered as an attempt to evade such restrictions.)"

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

So, a researcher would get away with a Cross Site Scripting (XSS) or testing an Insecure Direct Object Reference (IDOR). But these are very common and primarily low-impact vulnerabilities any script kiddy can do. CVEs that score high mostly involve something more challenging, such as Remote Code Execution or crypto weaknesses. These are apparently perceived as too invasive and, therefore not “lawful business”.

There is one significant exception on these cautious guidelines: the NOTICE project. It aims to prevent cyber-attacks and mitigate their damages by promoting enhanced security measures for IoT devices by scanning IoT devices on weak passwords by attempting to log in. These activities run parallel to the Handling Regulations for Information Related to Vulnerabilities in Software Products and clearly violate cyber security laws. In order to proceed on this endeavor, the Cabinet overruled the Act on Prohibition of Unauthorized Computer Access by a special law, which provided NICT the mandate. To my knowledge, this is unique in the world.

In the Netherlands, it’s the other way around: the government cannot do active CVD on citizens' devices, while independent security researchers can. Within the Dutch guideline, you are allowed to use heavier techniques if you can demonstrate your intentions are good and the research and disclosure don’t weaken the system's security but improve it. The Dutch guideline does, for example, rule out DDoS, brute forcing, building backdoors and downloading large amounts of data - for good reasons. For the most common penetration testing techniques, you are pretty well off the hook.

Case study: how NOTICE scans and notifies Japanese IoT

NOTICE stands for National Operation Towards IoT Clean Environment. The project aims to prevent cyber-attacks and mitigate their damages by promoting enhanced security measures for IoT devices. Its a collaboration of the Ministry of Internal Affairs and Communications (MIC), NICT and the Japanese Internet Service Providers. After MICs presentation on it at KEIO conference, I visited NICT to meet the project leader of NOTICE Masashi Eto and Research Engineer Masaki Kubo to learn more about the project. Masaki also participated in the expert meeting.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

The Specially Authorized Survey

NICT started scanning for devices with weak credentials on February 20, 2019, with a tool known as the Specially Authorized Survey. It tries to log in online to users' IoT devices with easily guessable user names and passwords to observe whether they are at risk of being abused in cyberattacks. If a log-in attempt seems to work, a notification is forwarded through the ISP to the user to change the credentials to more secure ones.

In the first version, standard passwords of Telnet devices were tested along with easy to crack SSH (password authentication). Since March 2022, the Specially Authorized Survey also tests HTTP(S) Basic/Digest authentication. Since April 2023, it also tests on HTTP(S) Form-based authentication, which is quite challenging because each device has its particular format the survey needs to recognize to fill in the credentials.

In one case, NOTICE successfully logged in to over 4,000 devices with HTTP Basic authentication. The researchers were able to identify them as routers from one vendor. They contacted the ISP and confirmed that the ISP rents the routers to customers. The router vendor updated the firmware, and the ISPs updated all customer routers via the Internet.

Beating Botnets

Since April 2024, NICT has extended the Survey again. It still scans devices for weak credentials, but also for high-risk firmware vulnerabilities and malware infections. Vulnerabilities are not actually tested. The scan only determines if the device runs an old, vulnerable version, which is less invasive. Malware infections they scan for also involve botnets. NICT sees the Mirai botnet is still active on Japanese devices. One ISP I talked to claimed they notify users of the presence of botnet infections and provide instructions on how to clean their devices. If the users don't follow the advice, they get disconnected from the internet.

The total number of IP addresses of the participating ISPs is currently 126 million. Of these, an average of 13,953 a month receive a notification on weak passwords and 4,734 on high-risk firmware vulnerabilities. Scanning for malware is done daily, leading to 1,248 notifications a day.

NICT also monitors attacks on IoT. It has 300.000 Japanese IP addresses that form together the NICTER Darknet, consisting of black hole sensors, swallowing malicious traffic without the threat actor knowing it. In this way they can determine which devices are targetted with which malware, or which ones are infected themselves to execute attacks.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

For example, the Darknet has received many attacks from Buffalo wireless home routers exploited by an unknown firmware vulnerability. In May 2024, NICT started collaborating with Buffalo to address the issue, notified users, and immediately brought the number of infected routers down from 6,000 to 2,000. Another case was D-Link's wall-mounted routers exploited by a vulnerability (CVE-2021-20696). NOTICE found 13,939 IPs infected, which was brought down to 1,295 after countermeasures such as internet access controls by the ISPs.

Prospects for NOTICE are that NICT will continue developing new IoT device investigation methods and providing a platform for advanced analysis information for collaborating organizations. Unfortunately, the Specially Authorized Survey runs on proprietary software and cannot be shared outside NICT.

Which opportunities for future collaboration are there for DIVD in Japan?

My general impression of the possibility of doing large-scale CVD for DIVD in Japan does not differ that much from other countries. Strictly taking, scanning and notifying without informed consent infringes on criminal laws in Japan, but, in our case, this activity takes place in the Netherlands, where it is allowed. Looking at the room for interpretation of the laws and the established policies and practices on CVD, we have a good chance our work is perceived as a lawful business. Then it comes to who can forward our notifications to potential victims.

I believe that should be JPCERT/CC. It's an independent organization with the goal of making the internet safer and close to the way DIVD works. In other countries it's also the national CERTs we share our data with. IPA does have a procedure to notify operators on a vulnerability in their website, but this is more for single notifications under strict limitations. JPCERT/CC is used to handle more severe vulnerabilities on a larger scale and is right in the center of all CVD processes. This was also confirmed by many of the experts I talked to. One even said: "If JPCERT/CC can't do it, no one can."

During my visit at JPCERT/CC, I learned that they already use threat intel from Shadow Server, an organization we work closely with, and who forwards our data to GovCERTs. In two cases from 2023, JPCERT/CC actually used DIVD data to notify victims.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Apparently, they already have the right processes in place. The only thing we need to do is automate it.

On the level of knowledge exchange, the organizations affiliated with the government do look very interesting. In general, organizations in both countries work on a guideline for CVD, which can be complemented with the DIVD Code of Conduct (see divd.nl/code) to make it more practical. We could also collaborate with NICT to see if DIVD can set up a monitoring service like their IoT survey. Although they can't share the scanning software, we may learn from each other's methods, scope, and ways of notification.

This also counts for the hackers I met in Japan. They seemed pretty reluctant to do CVD in Japan, as they fear legal consequences, but they were very interested in our work. DIVD had a sister organization for that: CSIRT.global, which has already set up chapters in 20 other countries. The first hacker already signed up. They, and other Japanese hackers can share their zero days with DIVDs CNA, to get published as CVE and perhaps start a case if it's an impactful one.

This mission was supported by the Dutch embassy in Japan. They have shown the Japanese cyber security sector we Dutch have something valuable to offer for free. We will be available to join future events, such as cyber security conferences or perhaps the World Exhibition in Osaka 2025, where the Netherlands will host a high-tech village. Dutch embassies worldwide could follow the Japanese example, enable DIVD missions in their countries and help us help the world become a safer place.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Credits

The online sources I used for this research are mentioned in the text. Most of the information retrieved for this research comes from the interviews and meetings. They are listed below: the formal meetings with name and affiliation, the more informal meetings - mostly during hacker events - only their first names as they could not check this report before publishing. Serena de Pater did a great job editing the first and final version. A big thanks to all these people who were willing to support this mission: どうもありがとうございます!

- April-October, preparational meetings: Ernst Noorman, Ambassador at Large for Cyber Affairs of the Netherlands; Peter van der Hoest, Diplomat at the Dutch embassy and Counsellor Economic Security at the Dutch Ministry of External Affairs; Wouter Hoiting and Akio Tamura of the Dutch Embassy in Tokyo.
- 16 October, online with Kazuo Noguchi, Senior Manager at Hitachi America and Senior Researcher at Keio.
- 23 October, the Dutch Embassy in Tokyo: Peter van der Hoest, diplomat; Wouter Hoiting, trainee; and Mae, trainee.
- 24 October, Security Days Fall 2024 開催のご案内.
- 28 October, JPCERT/CC: Koichiro Komiyama, Director, Global Coordination Division; Tomo Ito, Global CVD Project Lead; Yukako Ouchida, Global Coordination Division Manager; and Peter van der Hoest, diplomat.
- 29 October: Benny Ketelslegers, SOC Lead at a Japanese company.
- 30 October, panel at KEIO conference: Jun Osawa, Senior Fellow of the Sasakawa Peace Foundation; Mayu Arimoto, Principal Attorney at Alesia International Law Office and Visiting researcher of Japan Defense Technology Foundation; and Shinya Kabashima, Director for Strategic Analysis of Ecenomic Security Office METI.
- 1 November, Cyber Risk Meet-up: Aapo, Tripp, Kamel, James, Lauri, Vijayakumar, Gil, Mariko and Akira.
- 5 November, NTT Security Holdings: Takeshi Nakatsuru, Senior Research Engineer and Senior Vice President Cyber Security Crisis Management; Itaru Kamiya, project lead; Ryo Fukuyama, project lead; Wataru Matsuda, Senior Research Engineer.
- 7 November, Paul Sebastian Ziegler, CEO reFlare.
- 12 November, NICT, National Institute of Information and Communications Technology: Masaki Kubo, Executive Research Engineer; and Masashi Eto, project leader of NOTICE.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

- 13 November, Tengue Sec Meet-up: Kamel, Tripp.
- 13 November, CVD Expertmeeting at Embassy of the Kingdom of the Netherlands in Tokyo: Peter van der Hoest; Takayuki Uchiyama, Panasonic Holdings Corporation and Vulnerability Analys; Tomo Ito, Global Coordinated Vulnerability Disclosure Lead at JPCERT; Masaki Kubo, Executive Research Engineer at the National Institute of Information and Communications Technology; Ikuo Takahashi, Attorney at Law at Komazawa legal chambers and CEO at IT Research Art; Mayu Arimoto, Principal Attorney at Alesia International Law Office and Visiting researcher of Japan Defense Technology Foundation.
- 14-15 November, Code Blue: Vangelis, Takayuki, Tatsuo, Kosuke, Masafumi and Dion.
- 16 November, AVTokyo: Juuso, Evgeny, Keng Wei, Kotaro, Jesica, Yuji, David, Joshua and Maria.

閉

(close)

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl