Emdivi and the Rise of Targeted Attacks in Japan - JPCERT/CC Eyes

By JPCERT/CC

Published: 2015-11-05 · Archived: 2026-04-05 23:12:01 UTC

November 6, 2015

- Report

You may well have heard of the May cyber attack in Japan against the Japan Pension Service – a high-profile case seen in the first half of this year, where 1.25 million cases of personal data was exposed. According to the Japan Pension Service, the data leaked included names and ID numbers, and for some cases, dates of birth and home addresses.

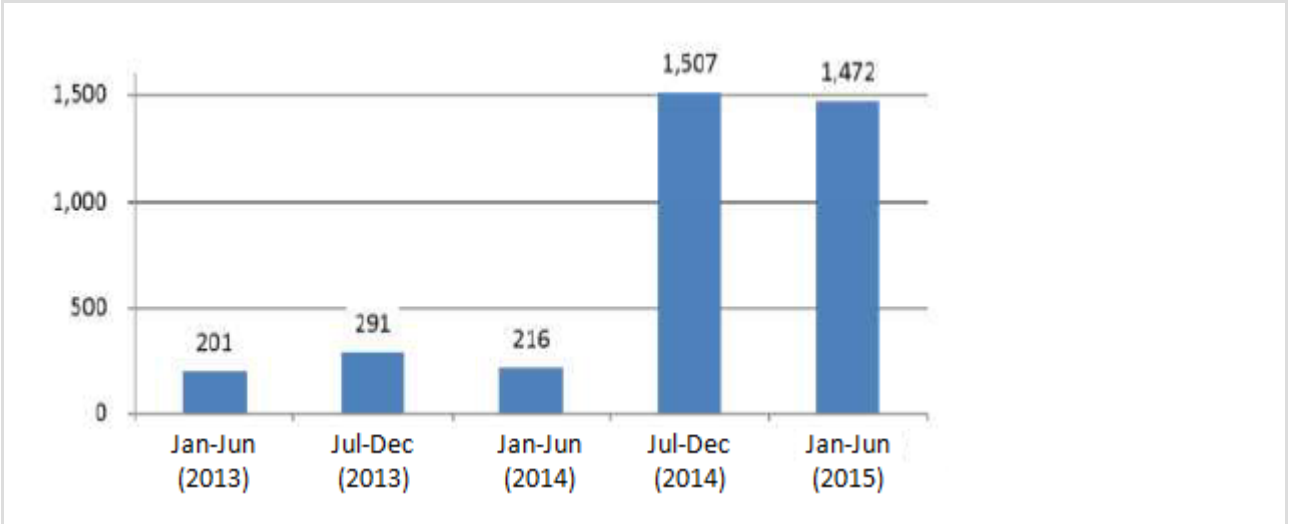
The official reports(1) say that the massive leak was caused by attackers hacking Japan Pension Service staff computers through a malicious email attachment, which was disguised as a legitimate document, but in fact was a malware. According to other various sources, the malware used is said to be “Emdivi.” This classic ploy, or targeted attack, has been around for years – however, Japan is recently experiencing a rise in this attack.

According to the National Police Agency, the number of targeted email attacks they have recognized count up to 492 cases in 2013, 1,723 in 2014 and 1,472 in the first half of 2015 alone.

Figure 1: Number of Targeted Attacks Recognized by the National Police Agency [Click to enlarge image]

> *Source: Cyberspace Threat Landscape in the first half of 2015*
> *https://www.npa.go.jp/kanbou/cybersecurity/H27_kami_jousei.pdf (Japanese only)*

Note: The title/figure have been translated by JPCERT/CC

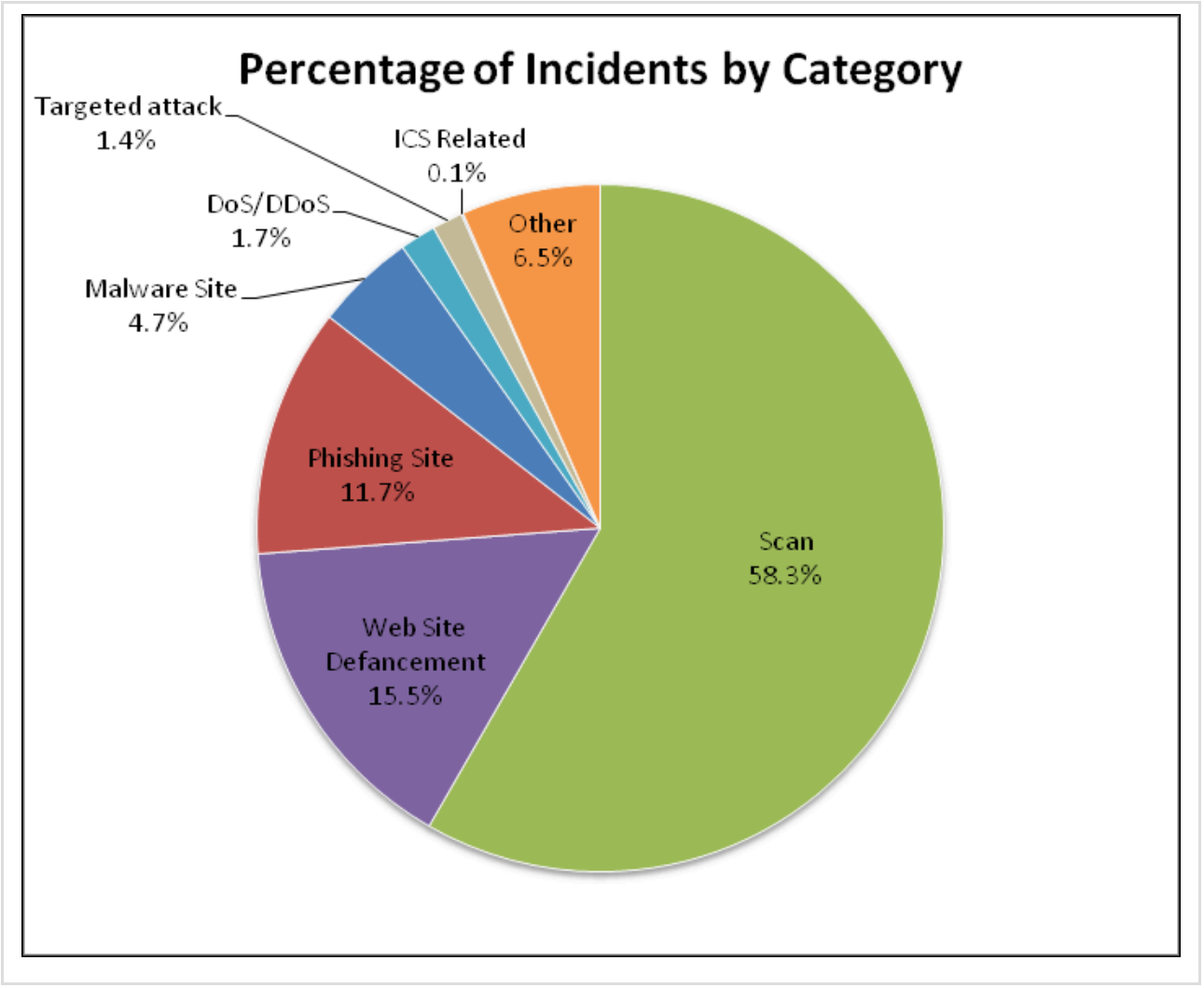


Emdivi is notoriously used in these targeted attacks, and what is distinct is that it specifically focuses on Japanese targets. The Japan Pension Service indeed drew nationwide attention, but Emdivi has victimized several other government and private organizations. This attack campaign, specifically targeting Japan, is also known as "CloudyOmega" named by Symantec, or "Blue Termite" by Kaspersky.

Following this trend, JPCERT/CC newly added a "targeted attack" category in its Incident Handling Report (April – June 2015), to count the number of targeted attack incidents reported to JPCERT/CC.

Figure 2: Category of Incidents Reported to JPCERT/CC (April – June 2015) [Click to enlarge image]

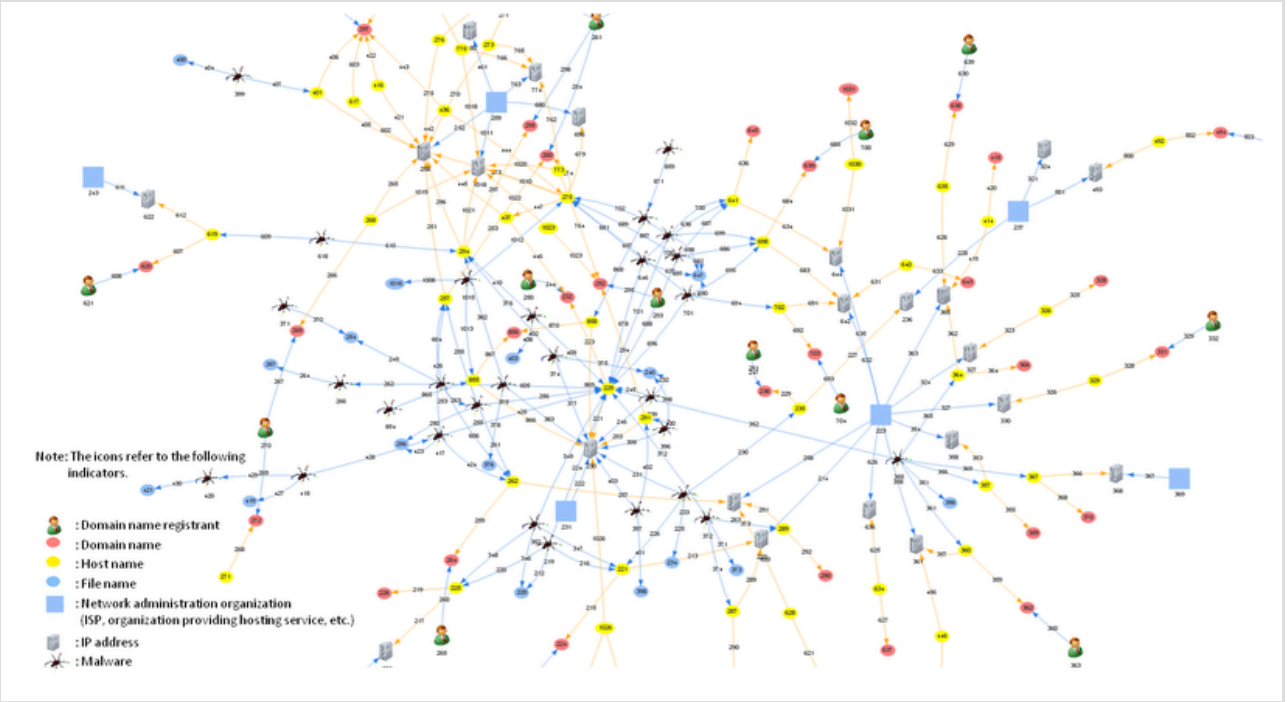
Source: JPCERT/CC



Although targeted attack accounts for a mere 1.4%, the significance and impact of the attack has forced to take as much as half the resource of our Incident Response Group, according to the Group's Manager. During the quarter, JPCERT/CC notified 66 organizations on the possibility of being victimized by targeted attacks, of which 44 were related to Emdivi. Based on the reports received, JPCERT/CC investigated the malware and attack infrastructures (C&C servers, etc.), and also developed a tool for visualizing the relation of Indicators of Compromise (IOCs) for further analysis. The visualization is shown in Figure 3.

Figure 3: Visualization of the Relation of IOCs [Click to enlarge image]

Source: JPCERT/CC



This tool aims to sort out various information relating to targeted attacks, and to give an overall picture of what is going on. While various campaigns and attack groups have been observed by security related organizations, the same campaign may have different names (as mentioned above), or different campaigns may have similar attack methods. This could cause confusion when you want to find out where a certain piece of indicator information was observed. This tool was developed to resolve this confusion. By registering the IOCs of respective attack campaigns and incidents, and also the relation of the IOCs, it is designed to visualize the big picture of the attack.

Based on these analyses, JPCERT/CC engages in sharing information with organizations that may potentially become the next target, as well as notifying organizations that are presumed to be victimized already. As Emdivi is also known for cleverly hiding itself, there is a high possibility that still several organizations are unaware of the situation, even if they are already infected. JPCERT/CC will continue to make every effort to address such situations in cooperation with other relevant parties.

In the next blog posts, our Analysis Center will introduce technical knowledge on JPCERT/CC's tools, developed to detect malware in targeted attacks as well as to analyze Emdivi. See you again there!

- Keishi Kubo and Shiori Kubo

Reference

(1) Official Reports:

- "Report on Investigation Results" published by Japan Pension Service (Japanese only)

> - ”Investigation Results of the Cause related to Japan Pension Service’s Personal Data Leak Incident” published by NISC (National center of Incident readiness and Strategy for Cybersecurity) (Japanese only)
> - ”Verification Report – by the Verification Committee for Japan Pension Service’s Data Leak Incident through Unauthorized Access” published by the Ministry of Health, Labour and Welfare (Japanese only)
>
> *Note: The titles of the reports have been translated by JPCERT/CC*

JPCERT/CC

Please use the below contact form for any inquiries about the article.

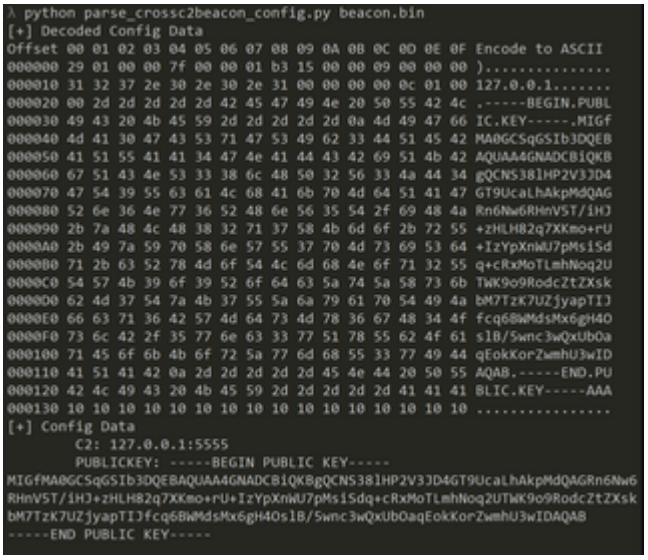
Related articles

- 

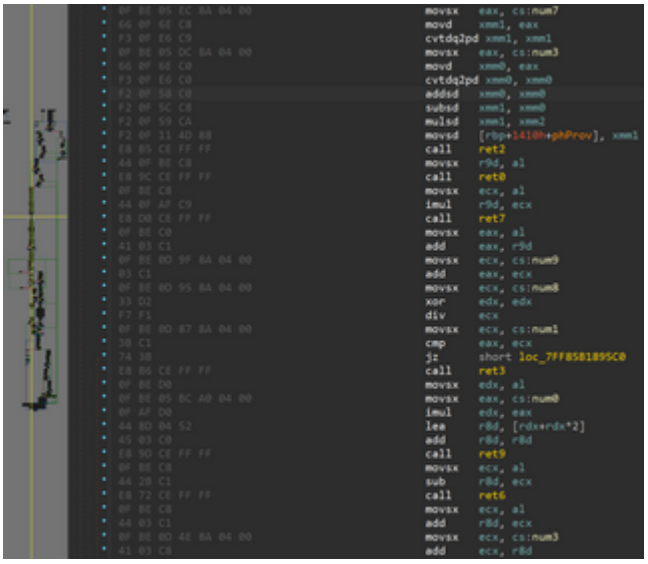
  Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise

- 

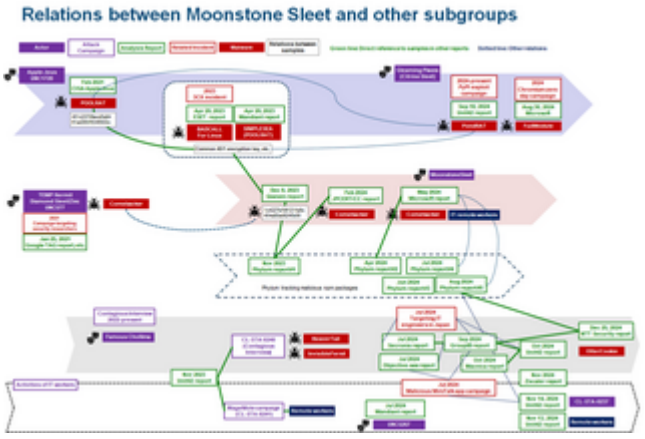
  Update on Attacks by Threat Group APT-C-60



- [CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks]



- [Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities]



- [Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup]
