

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.

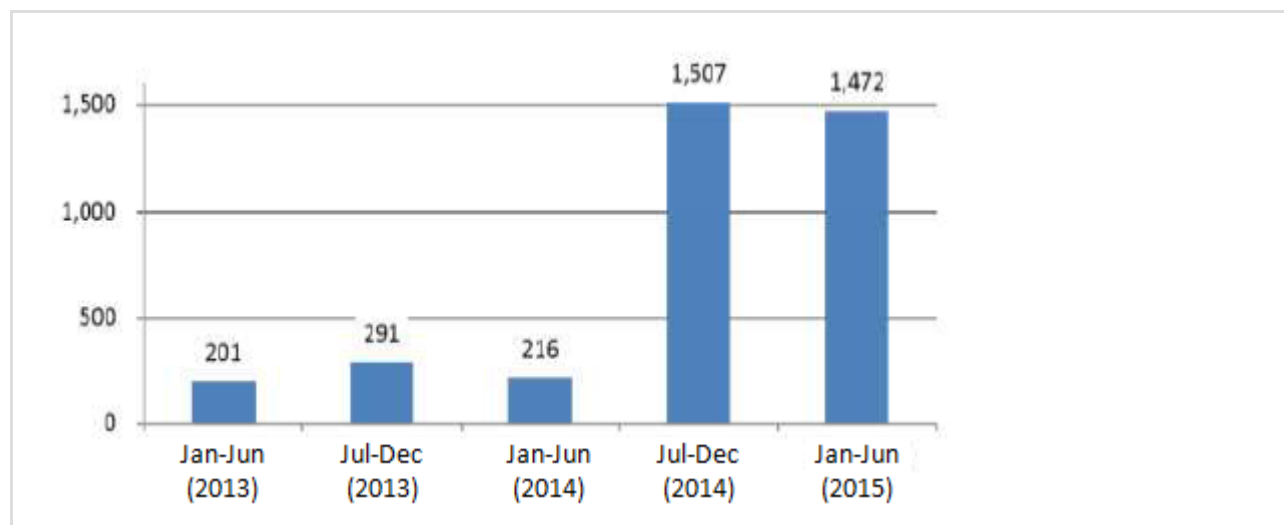
According to the National Police Agency, the number of targeted email attacks they have recognized count up to 492 cases in 2013, 1,723 in 2014 and 1,472 in the first half of 2015 alone.

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

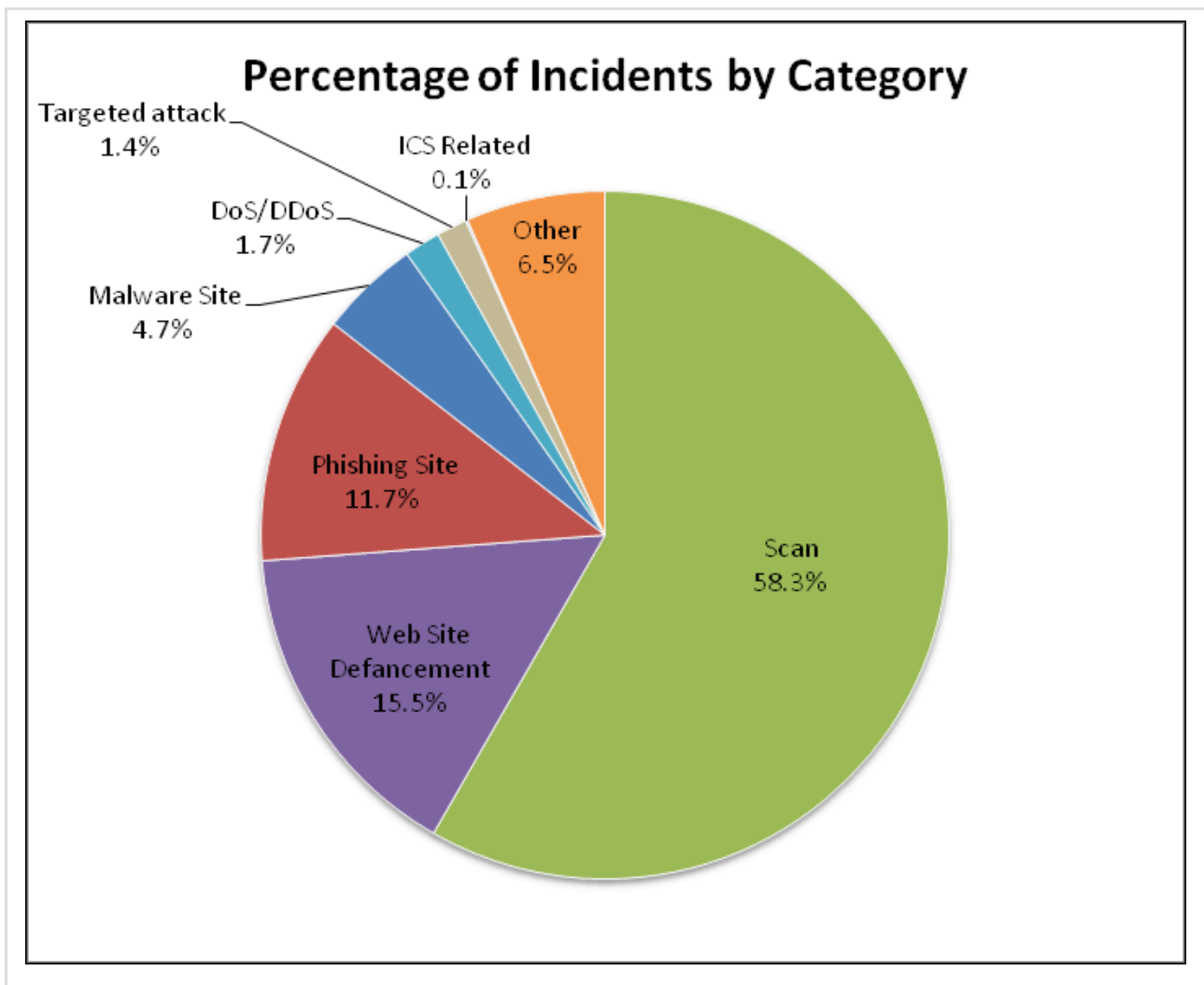


Emdivi is notoriously used in these targeted attacks, and what is distinct is that it specifically focuses on Japanese targets. The Japan Pension Service indeed drew nationwide attention, but Emdivi has victimized several other government and private organizations. This attack campaign, specifically 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]

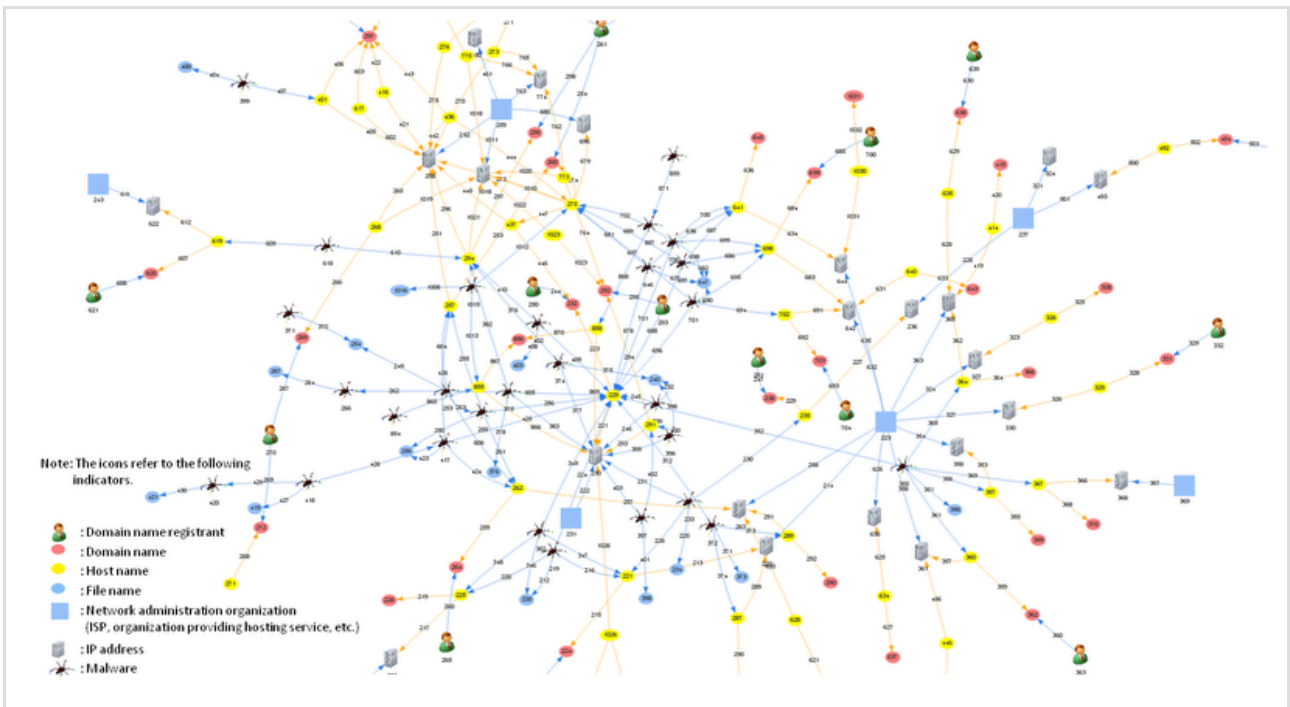
Source: JPCERT/CC



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](#)

```
"key" = 0x017c1600,
"key[4]" = 0x01593522,
"key[8]" = 0x00472834,
"key[12]" = 0x00007909,
"iv[0]" = 0x12470421,
"iv[4]" = 0x00005608,
"iv[8]" = 0x00700129,
"iv[12]" = 0x00190007,
v8 = m_ret_arg1offfeat0x350(a1 + 3);
if ( !(!CrypAcquireContext)(a1, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 0x10, 0x00000000) )
return 0;
v9 = m_ret_arg1offfeat0x350(a1 + 3);
HandleHashobj = a1 + 1;
if ( !(!CrypCreateHash)(a1, 0x0004, 0, 0, a1 + 1) )
{
LABEL_0:
if ( !a1 )
return 0;
v8 = m_ret_arg1offfeat0x350(a1 + 3);
(!CrypReleaseContext)(a1, 0);
return 0;
}
if ( !CrypHashData(HandleHashobj, key, 160, 0) )
{
v8 = m_ret_arg1offfeat0x350(a1 + 3);
v9 = a1 + 2;
(!CrypDeriveKey)(a1, 0x0000, HandleHashobj, 0x000000, a1 + 2) // CALS_AES_128
}
if ( HandleHashobj )
{
v8 = m_ret_arg1offfeat0x350(a1 + 3);
(!CrypDestroyHash)(HandleHashobj);
}
goto LABEL_0;
v10 = m_ret_arg1offfeat0x350(a1 + 3);
(!CrypSetCrypParam)(v9, 3, 0x0000, 0); // SP_PAD0200 + PRC040/7
v11 = m_ret_arg1offfeat0x350(a1 + 3);
v12 = m_ret_arg1offfeat0x350(a1 + 3); // IV = parameter
(!CrypSetCrypParam)(v8, 1, v9, 0); // SP_MODE = CBC
v13 = m_ret_arg1offfeat0x350(a1 + 3);
(!CrypCrypParam)(v9, 4, 0x0000, 0); // SP_MODE = CBC
return v9;
}
```

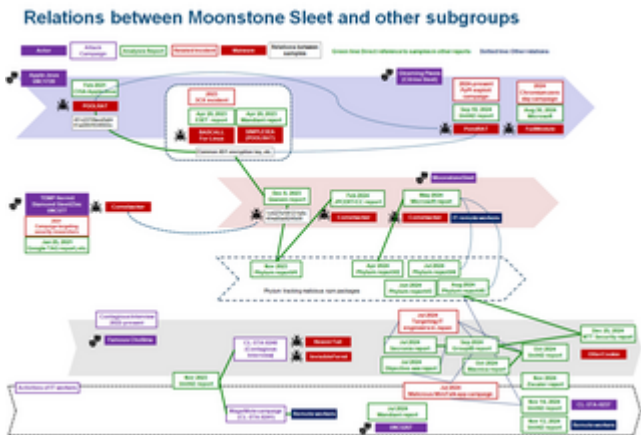
[Update on Attacks by Threat Group APT-C-60](#)

```
python parse_crossc2beacon_config.py beacon.bin
[+] Decoded Config Data
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Encode to ASCII
000000 29 01 00 00 7F 00 00 01 B3 15 00 00 09 00 00 00 ).....
000010 31 32 37 2E 30 2E 30 2E 31 00 00 00 0C 01 00 127.0.0.1.....
000020 00 2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42 4C -----BEGIN.PUBL
000030 49 43 20 4B 45 59 2D 2D 2D 2D 2D 2D 2D 0A 4D 49 47 66 I.C.KEY-----,MIGF
000040 4D 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 MA0GCSqGS1b3DQEB
000050 41 51 55 41 41 34 47 4E 41 44 43 42 69 51 4B 42 AQUAA4GNADCB1QKB
000060 67 51 43 4E 53 33 38 6C 48 50 32 56 33 4A 44 34 gQCNs381HP2V3JD4
000070 47 54 39 55 63 61 4C 68 41 6B 70 4D 64 51 41 47 GT9UcalhAkPmdQAGRn6Nw6
000080 52 6E 36 4E 77 36 52 48 6E 56 35 54 2F 69 48 4A Rn6Nw6RHNvST/1HJ
000090 2B 7A 48 4C 48 38 32 71 37 58 4B 6D 6F 2B 72 55 +zHLH82q7Xkmo+rU
0000A0 2B 49 7A 59 70 58 6E 57 55 37 70 4D 73 69 53 64 +IzYpXmU7pMs1Sd
0000B0 71 2B 63 52 78 4D 6F 54 4C 6D 68 4E 6F 71 32 55 q+cRxMoTLmHNoq2U
0000C0 54 57 4B 39 6F 39 52 6F 64 63 5A 7A 5A 58 73 6B TWK9o9RodcZtZXsk
0000D0 62 4D 37 54 7A 4B 37 55 5A 6A 79 61 70 54 49 4A bM7TzK7UZjyapTIj
0000E0 66 63 71 36 42 57 4D 64 73 4D 78 36 67 48 34 4F fcq6BwMdsMx6gH4O
0000F0 73 6C 42 2F 35 77 6E 63 33 77 51 78 55 62 4F 61 s1B/Swnc3wXubOa
000100 71 45 6F 6B 4B 6F 72 5A 77 6D 68 55 33 77 49 44 qEokKorZumHU3wID
000110 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44 20 50 55 AQAB-----END.PU
000120 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 41 41 41 BLIC.KEY-----AAA
000130 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 .....
[+] Config Data
C2: 127.0.0.1:5555
PUBLICKEY: -----BEGIN PUBLIC KEY-----
MIGFMA0GCSqGS1b3DQEBQUAA4GNADCB1QKBgQCNS381HP2V3JD4GT9UcalhAkPmdQAGRn6Nw6
RHNvST/1HJ+zHLH82q7Xkmo+rU+IzYpXmU7pMs1Sdq+cRxMoTLmHNoq2UTWK9o9RodcZtZXsk
bM7TzK7UZjyapTIjfcq6BwMdsMx6gH4Os1B/Swnc3wXubOaqEokKorZumHU3wIDAQAAB
-----END PUBLIC KEY-----
```

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

```
movsx ecx, cs:num7
movd xmm1, ecx
cvttdq2pd xmm1, xmm1
movsx ecx, cs:num3
movd xmm0, ecx
cvttdq2pd xmm0, xmm0
addsd xmm0, xmm0
subsd xmm1, xmm0
mulsd xmm1, xmm2
movsd [rbp+1410+ph0Prev], xmm1
call ret2
movsx r9d, al
call ret0
movsx ecx, al
imul r9d, ecx
call ret7
movsx eax, al
add eax, r9d
movsx ecx, cs:num9
add ecx, ecx
movsx ecx, cs:num8
xor edx, edx
div ecx
movsx ecx, cs:num1
cmp eax, ecx
jz short loc_7FF85B1895C8
call ret1
movsx edx, al
movsx eax, cs:num0
imul edx, eax
lee r8d, [rdx+rdx*2]
add r8d, r8d
call ret9
movsx ecx, al
sub r8d, ecx
call ret6
movsx ecx, al
add r8d, ecx
movsx ecx, cs:num3
add ecx, r8d
```

[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](#)

Source: <https://blogs.jpCERT.or.jp/en/2015/11/emdivi-and-the-rise-of-targeted-attacks-in-japan.html>