Clustering Malware Variants Using "impfuzzy for Neo4j"

In a past article, we introduced "impfuzzy for Neo4j", a tool to visualise results of malware clustering (developed by JPCERT/CC). In this article, we will show the result of clustering Emdivi using the tool. Emdivi had been seen until around 2015 in targeted attacks against Japanese organisations. For more information about Emdivi, please refer to JPCERT/CC'sreport.

Clustering Emdivi with impfuzzy for Neo4j

For this analysis, we chose t17 and t20, the two major variants of Emdivi. Figure 1 shows the output of running impfuzzy for Neo4j.

```
mal-vm ~/neo4j % python3 impfuzzy_for_neo4j.py -l Emdivi_t17.csv
[*] Impfuzzy threshold is 30.
[*] Creating a graph data.
[*] Parse file Emdivi_t17.csv.
[*] The total number of malware is 90.
[*] The number of clusters is 4
[*] Created a graph data.
```

Figure 1: Emdivi t17's clustering result using impfuzzy for Neo4j

As a result of the analysis, 90 samples were clustered into 4 types. Figure 2 visualises the clustering results. Detailed results are documented in Appendix A. (For detailed instructions on the tool, please see our past blog article.)

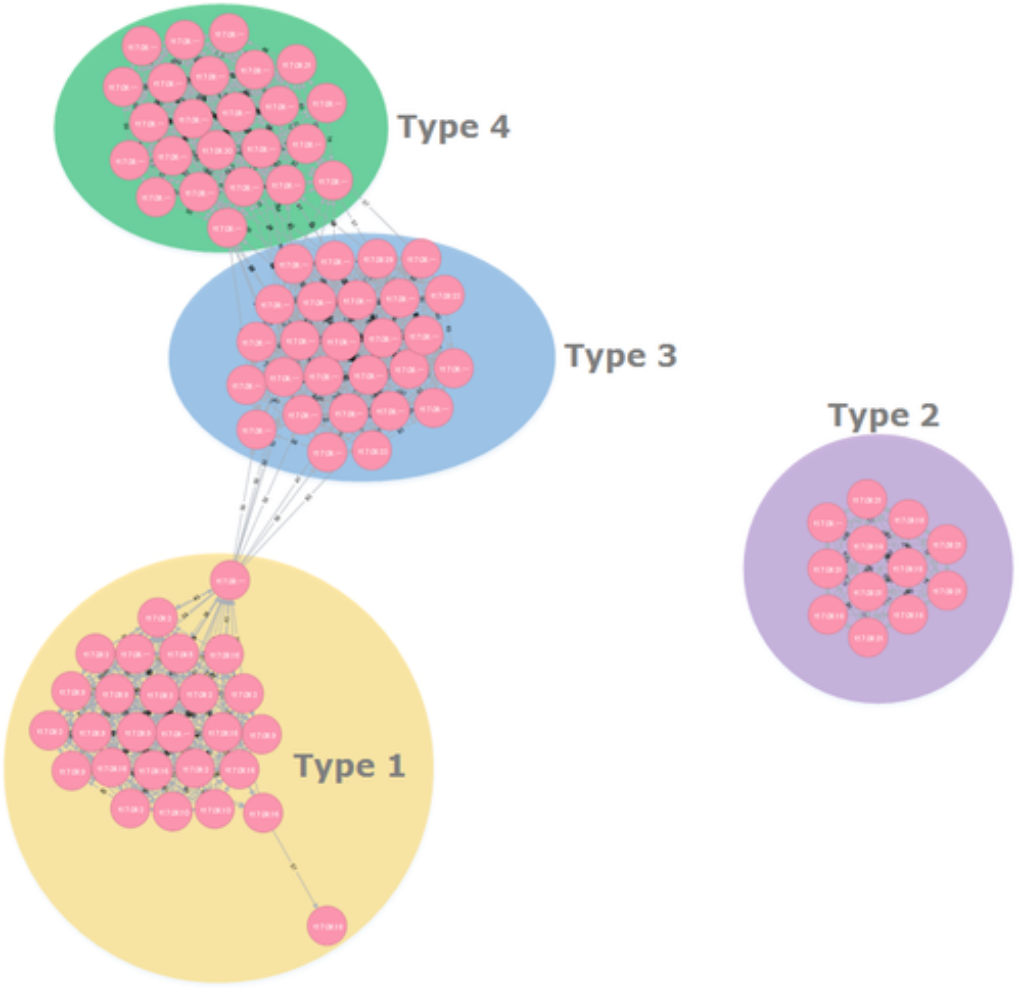

Figure 2: Visualised result of Emdivi t17 clustering (Colouring provided for better

understanding.)

It stood out that each cluster (Type 1 through Type 4) highly corresponds to the compiled date of the malware sample (see Appendix A).

Hash values of malware samples are generated by impfuzzy (Import API), which is then used to calculate the similarity. Therefore, the reason for this type clustering is unknown solely from this analysis. Manual analysis is required to examine what makes Import APIs different in each type.

The following sections will describe the reason why Emdivi t17 samples were clustered into 4 types and how the transition occurred from one type to another.

From Type 1 to 2

The clustering results in Appendix A indicate the transition from Type 1 to 2 occurred around September 2014. We noticed a change in linker versions.

PE files have header information called IMAGE_OPTIONAL_HEADER[1]. This contains MajorLinkerVersion and MinorLinkerVersion, which indicates its linker version. Looking into the linker version used when creating Emdivi t17, Type 1 mainly uses 10.0 (Visual Studio 2010) while Type 2 uses 9.0 (Visual Studio 2008). It is considered that these samples were differentiated due to the change in the linker version, which accordingly changed the Windows APIs that the malware loads.

From Type 2 to 3

It was around November 2014 when Type 2 changed to Type 3, and this transition reflects the change in the method of loading Windows API. Usually, PE file loads Windows API upon execution by specifying an API name in Import Name Table (INT) inside the PE header. (Please refer to a past blog article for more information.)

However, Type 3 samples possess some obfuscated Windows API names and load it when using Windows API. Figure 3 is the results of decoding obfuscated strings in Emdivi t17, which indicates that Type 3 contains some obfuscated Windows API names (marked in red).

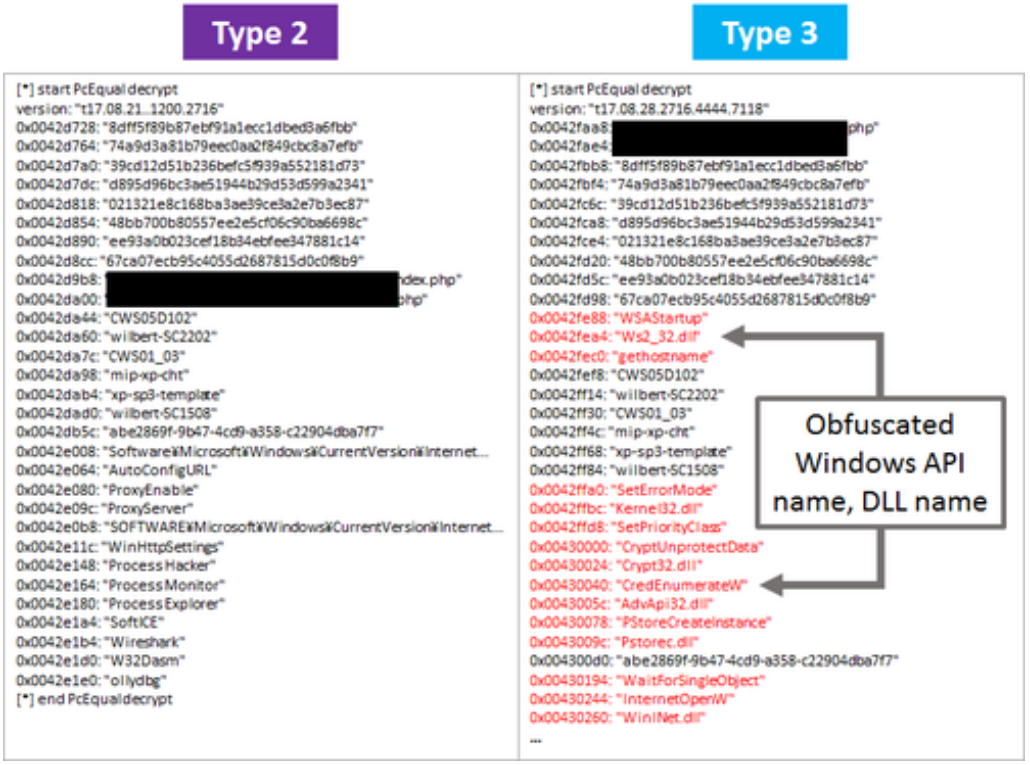

Figure 3: Comparison of decoded strings in Emdivi t17 clustered as Type 2 and 3

The Windows APIs obfuscated in Type 3 are deleted from its INT. This means that the Windows API that the malware aims to execute cannot be identified by just looking at the INT.

This change in Windows API load method is thought to be the reason for the difference between Type 2 and 3.

From Type 3 to 4

Transition from Type 3 to 4 occurred around May 2015. This is due to a new bot (remote control) function being added. Here is the list of bot functions that Type 4 has. “GOTO” is the new function to Type 4.

- GOTO
- DOABORT
- DOWNBG
- GETFILE
- LOADDLL
- SETCMD
- SUSPEND
- UPLOAD
- VERSION

The added bot function resulted in new Windows APIs being used, which distinguishes Type 4 from 3.

Summary

It is not practical to manually analyse a large number of malware samples. It is rather important to automate malware clustering process to find new types of malware and changes in malware features. With the analysis example, we demonstrated an example of effective malware analysis using impfuzzy for Neo4j by focusing on samples with different features. The tool is available on

Github, and we hope this helps your malware analysis.

- Shusei Tomonaga

(Translated by Yukako Uchida)

Reference

[1] Microsoft: IMAGE_OPTIONAL_HEADER structure

https://msdn.microsoft.com/en-us/library/windows/desktop/ms680339(v=vs.85).aspx

Appendix A Emdivi t17 Clustering Results

Table 1: List of Emdivi t17 Clustering Results

No.	Compile Time	EmdiviVersion	LinkerVersion	Type	SHA256
1	2013-11-21 17:00:52	t17.08.2	10.0	1	6b0192ec4f0290c0c00517eeb75648e340dacc58189d9d6adee844283cda4a5f
2	2013-12-24 12:13:21	t17.08.2	10.0	1	c162df8761e09c95160e9d432d310a4673d53615c2ff837a1a6f322e45038180
3	2014-01-06 11:33:48	t17.08.2	10.0	1	bf8cba80f4d80e13f11c8231477f0b96c3a9e9abc8da798e6cede052f6801aa8
4	2014-01-06 11:48:05	t17.08.2	10.0	1	742c70238ea0b2b0a1d66660913b18deaff2af35c6dc5b19e9d2158249cae433
5	2014-01-19 16:12:41	t17.08.2	10.0	1	18dfb3ff38c802f54c66c7d06380e7aff4834ac7a0c9ea35e50f46cf40266c3a
6	2014-01-21 12:29:03	t17.08.2	10.0	1	08a542fe7f8450d2c66b5e428872860d584bc5be714a50293a10aef415310fe8
7	2014-01-21 20:07:01	t17.08.2	10.0	1	bf9229b342c144970358308ccb017802cb2ff5c2086bf0367d9d72f34556b7c1
8	2014-01-23 16:32:01	t17.08.2	10.0	1	2bf87ec696356a685b081b9e0aec88c3ac3e3353927f712e978db0d2f5a9476b
9	2014-02-28 10:52:43	t17.08.5	10.0	1	396c7766eb8873227c270eae2b13357dbcd68fa7f07053dd280375418eeee614
10	2014-03-13 13:05:13	t17.08.9	10.0	1	138e7c2e5cf0caba02d005752686a66482df23f4b4b648f446f2afada32a5750
11	2014-04-01 12:08:03	t17.08.9	10.0	1	4df19e155cac0735500cffae49007b3d971979cccca779a5af685db489b4b042
12	2014-05-07 13:52:46	t17.08.10	10.0	1	b97ab11d1154fae07d2cfab055cdc6b745a5117fc1d8e557f6a244040ba7cce3
13	2014-05-08	t17.08.10	10.0	1	04b9a6ef5ef6cdaf42e90431039bd56b68082c5056889cf4b9ababc6e0834b56

	12:22:24				
14	2014-05-11 15:44:46	t17.08.9	10.0	1	83620f29a19a4d372e256d98ebfd2d3e5cb4b8db97b385c2942914298b8d2870
15	2014-06-03 10:41:46	t17.08.9	10.0	1	4422d1568f729c316e8d02a35fe147c4c36c91d650989e9ac3caa6fbbc086b37
16	2014-07-17 10:48:24	t17.08.9	10.0	1	e7ae0995e3d4dd9c3fed51d5bca73ea9fa3edd90e2e87fc0cfac58165afdf4e8
17	2014-07-22 17:40:31	t17.08.9	10.0	1	7875c21473cf5f8d936f1335c049ae6df9e0b0574b263060d7a526f3d53cbf07
18	2014-07-28 18:01:59	t17.08.16	10.0	1	c805af2204c1d8612cd929b93fc5c38a448a03561d410d7a198c313553e47e39
19	2014-08-04 13:57:34	t17.08.16	10.0	1	3243925baa06dc69731da91da49242fd73aea38afe46e171708de4ecd4e53b80
20	2014-08-05 12:51:43	t17.08.18	8.0	1	92860e0a9e7dc49c43a0db87d4fb345294000ac3191af1dc6d702b89628c97eb
21	2014-08-06 09:22:32	t17.08.16	10.0	1	df97dd9607f0fdcc10f9ba99e6c3d01eb8453ceeeab840ef6b965458e24485bc
22	2014-08-12 18:09:41	t17.08.16	10.0	1	d26eb51e2787353b18c8f290f0710510423e3925a796697ff15aafd14fea6f2d
23	2014-08-18 12:21:10	t17.08.16	10.0	1	37f43f9c4298dc41f6b1ed03396cc1f7da664ed25e97c4263e6c360f59f3a51b
24	2014-08-19 20:01:29	t17.08.16	8.0	1	9fc76d0fb4f01819c0d9af09a0357dab6c33a4d5f6e41cafebeb9ef7ae35c99e
25	2014-09-09 13:34:21	t17.08.18	9.0	2	f017218f05d225cdb62f3081c4dac4b09a3fb2b93c01096bd4141b67d3eb3bbf
26	2014-09-18 09:26:42	t17.08.18	9.0	2	139e22abe7aaec635e2b570935636c4894a19a7b284516b77f190b78a369c4d6
27	2014-09-22 09:51:33	t17.08.18	9.0	2	a00e37d1d3fe990ebac26a4805a7ab42bd1dcf7ef65f151906204eee7b0c71fd
28	2014-09-25 10:34:10	t17.08.18	9.0	2	3d084155e6f79b45acba165cd4a17a3bed42daba478c14a795dc2c2809f302b6
29	2014-09-28 20:52:36	t17.08.18	9.0	2	196364b3e78add557b6f0471fb32061468bb2b20e16acd1a7686122234c984a7
30	2014-09-30 12:10:55	t17.08.21	9.0	2	8c3666940afd65835e4251fbd14942d210323d46adf57c5e8f29b61d552fd386
31	2014-10-07 11:50:57	t17.08.21	9.0	2	878937da134339ccd8c6bbc5ac020472c20a42fb1f07b56152cfcc1656077d62

32	2014-10-08 18:31:01	t17.08.21	9.0	2	b99f08be6a476d359820c48345ddf4f2f0fcc1ca041f3630680635c675a1d7be
33	2014-10-21 15:13:53	t17.08.21	9.0	2	1209d8b3c83c72df781b805a2c17a0939c841384aadc32e4e9005536a3bba53f
34	2014-10-24 17:16:08	t17.08.21.3	9.0	2	c89823eba2bdcdfcae33b33fb358154debe3fd88c75c684aa6b510e2d4b3ca53
35	2014-10-27 10:29:00	t17.08.21	9.0	2	884cbc1f0e70efae4815127bda7bab50883a707581d9d4061d268249c154ff2d
36	2014-10-28 12:48:54	t17.08.21	9.0	2	682b6c9d468e8d0ab8b5d4080cecf52a9dd66b59b99936a4941b8190c5f3fff9
37	2014-11-04 19:15:32	t17.08.23	9.0	3	23449109f0d4b07fd8010bb36b3b1084b48d5ac515725b68bf32322b4902397e
38	2014-11-05 21:15:57	t17.08.23	9.0	3	a79cfba79489d45a928ef3794d361898a2da4e1af4b33786d1e0d2759f4924c3
39	2014-11-05 22:00:42	t17.08.23	9.0	3	9801caaf44ce9a6be3f497e706f5b71dcc7c50351374c33dc2c9fcbb55f55e05
40	2014-11-06 13:55:46	t17.08.23	9.0	3	b19a233b07a1342f867aef1b3fb3e473b875bd788832bb9422cacb5df1bda04e
41	2014-11-13 10:52:56	t17.08.23	10.0	1	6c4c3bc7b0dfe531790bfb023b141c23f3c17a9971fed704d1b46e43f97d41c1
42	2014-11-13 11:34:31	t17.08.23	10.0	1	21a51f69d08aaf0aaaeb5b8413bb710c1727d9d08a9a1f46883f6f93691e0870
43	2014-11-14 13:10:40	t17.08.25	9.0	3	28a774235865924a7fec405aaf6463164a03f6e646c9fd964c3191304e59d35b
44	2014-11-18 11:56:13	t17.08.25	9.0	3	29a480579353c85e48b996ebc38cad9313ad6b9e495a3a69bf1519837acab04f
45	2014-12-08 15:19:29	t17.08.25	9.0	3	34bc147423f565bf38100913d25f85057e252755eef622abc1b788d511caf605
46	2014-12-11 18:28:38	t17.08.25	9.0	3	a188b87e495e4b0aad0d0595987677f9758479b120fb2ed3a04fba308a66830a
47	2014-12-16 18:13:13	t17.08.25	9.0	3	e39b1b36a5da4ad0f9c103478ab469b13a0528540ddbd1679eb24349a6726dbf
48	2014-12-24 10:37:26	t17.08.25	9.0	3	037b0dbfc2643a4a4779f6e3a8e5c8c41cbcd64533d2245c9a26dfd1d4f55dd8
49	2015-01-12 11:58:46	t17.08.25	9.0	3	9e74825e251a4f4cef9bc98273082f3b58695a224b1ed16ba6dedaa4c154cb21

50	2015-01-20 11:10:12	t17.08.26	9.0	3	5e221bd0eef231b7a948d8f6a2f660f8d6685cf2711fe50311485227ebcf9e51
51	2015-01-20 11:59:37	t17.08.26	9.0	3	635b43f7c0508f5e2cbf26f81daf0a730a0f0b06303c54c747b780f91430bb7f
52	2015-01-22 11:25:49	t17.08.26	9.0	3	efa57d43145de9a1e3c7541f94837a9c7b76d604b779d9847637d4a55b1ee723
53	2015-01-22 16:06:33	t17.08.26	9.0	3	9ace48ecef568bb9f5ccd462ca3efb4c2fbc15f0316323f1729e88cbe184158d
54	2015-01-23 10:14:46	t17.08.26	9.0	3	42e6b7afe4da672ab9bf647e73201135b3faf2121b629612b35307dc0d8698e4
55	2015-01-26 10:15:10	t17.08.26	9.0	3	9ebef65f00fc6ad70f591f7fb1f39f0f6b1766ff3fd9f47693ce669e70f84abb
56	2015-02-03 11:35:23	t17.08.26	8.0	3	6aed51b108d9f9f197842e17b0f58d4dec3709ca1eae4d42146d0bba0c145eaf
57	2015-03-02 10:18:13	t17.08.27	9.0	3	f6fce0464f1ad8044092e6812bdfb8545e1df5ee23aba828b4dcb86fb6d0e62b
58	2015-03-04 13:08:13	t17.08.27	9.0	3	fca765c535d1870d71ee152e5b004e73515ade1ee1c9a512a0858a508380465d
59	2015-03-05 12:59:51	t17.08.27	9.0	3	eac8441227077edb28adf096c5493710e2ca1978f4e4c4b2b93d481cd482d890
60	2015-03-17 12:50:29	t17.08.27	9.0	3	9f66ad282373b8b0df45dd32723dcdfcd4821e22cba4912678c3c8632e722730
61	2015-03-19 16:03:19	t17.08.27	9.0	3	77fa012060884d17eea1e54d97176a7a88c499f03315dfd602c1e1e17e556ede
62	2015-03-20 11:44:49	t17.08.27	9.0	3	3cade660e227faadad0060d793b69cb778842a514ac6996bc6aaddb6a055f445
63	2015-03-20 13:04:19	t17.08.27	9.0	3	6c3b955ad677ff26428d95a35b3a22ca3d523265674f08b6a0b59df270e6bf19
64	2015-03-24 13:07:23	t17.08.27	9.0	3	400a08b4a067b1e2fb3bee509bf933a746cf3ef2d000bb3181c7176344641a01
65	2015-04-22 12:29:48	t17.08.29	9.0	3	e3a2d62a997d4e9ee581fd86d312ac34caddd3165c07ca30c6741b4c21088d08
66	2015-04-24 12:07:43	t17.08.29	10.0	1	782b3bed336eab77a49df51e697bc64d830f7f11a32ff49abc599fe5b074e0b9
67	2015-05-20 12:52:28	t17.08.30	9.0	4	e03e6f7d98b214b5051b7484e4099ce5bd8c46e49faf44002c8ba146977127ef

68	2015-05-21 16:38:39	t17.08.30	9.0	4	28426751f30de4091dee898c70f49ec2ece607b6b642b45f5dcd9ae73ac38739
71	2015-05-22 12:51:18	t17.08.30	9.0	4	09178fa9c4be32982619a183b8b76bfc2ff57486aac04c8fed654a4d9fe91436
69	2015-05-22 12:51:18	t17.08.30	9.0	4	cb3976965f2105492193889f3f58f2ef2ccfeb8604e2b9448055ec6608d4aa85
70	2015-05-22 12:51:18	t17.08.30	9.0	4	de8759fe34eb2f395574be79479832402aa4d113e102d6945df493abee3d8b34
72	2015-05-28 13:48:14	t17.08.30	9.0	4	05ef4e0de8d57e6cd10d1673fcfca9c03b6e9a271d54028781e96235c4530e15
73	2015-06-02 12:15:26	t17.08.30	9.0	4	07b7041016c16341ea1f35a8c5fb5312d15f089ed5e925f78ffdd2568a8cf17c
74	2015-07-06 11:34:56	t17.08.31	9.0	4	c59ebe1fa6abe52c85f5f56a7da810a35e44c4772746bc829fa7d9e4e6a59477
75	2015-07-10 09:40:15	t17.08.31	9.0	4	3e850306025c231f09fa1922d1bb8e1a40bd8acc142d92219d9e9c8f8911b77d
76	2015-07-10 10:58:16	t17.08.31	9.0	4	008f4f14cf64dc9d323b6cb5942da4a99979c4c7d750ec1228d8c8285883771e
77	2015-07-13 01:23:13	t17.08.31	9.0	4	e919ae6a3bdc6abe6b695215a53b74072a39b86757e049f930866b3f69000957
78	2015-07-13 11:46:27	t17.08.31	9.0	4	567fa6bf28862ce7d14a2f3cf5b718780213fa3ee73f59557c29525f8daa200c
79	2015-07-14 10:57:44	t17.08.31	9.0	4	a94bf485cebeda8e4b74bbe2c0a0567903a13c36b9bf60fab484a9b55207fe0d
80	2015-07-14 11:16:54	t17.08.31	9.0	4	5a30f9010a316cc74ed271e732741c6d5d38f0e1c6f3b547176adcd40cb547ae
81	2015-07-14 18:44:14	t17.08.31	9.0	4	bfcd987ca3e79bd7ba8dde95a392dbba02ffa30242954a0cfa35ec81182f0cc8
82	2015-07-16 10:10:07	t17.08.31	9.0	4	3caf60dd3bb551d4da244dffaeb68fe01b59cd19bd0f0509611b706048b3382f
83	2015-07-28 13:56:35	t17.08.31	9.0	4	280371475442917b782f6a834003313f3aa0e5bb65f0acac5aab673d04336ba4
84	2015-08-05 09:51:31	t17.08.31	9.0	4	3cebf71221af741ea0b0883b45c092f900b513de3a004f81d3c595648311b7e9
85	2015-08-07 10:23:11	t17.08.34	8.0	4	90d07ea2bb80ed52b007f57d0d9a79430cd50174825c43d5746a16ee4f94ea86
	2015-				

86	08-13 09:48:01	t17.08.34	8.0	4	6a331c4e654dd8ddaa2c69d260aa5f4f76f243df8b5019d62d4db5ae5c965662
87	2015-08-13 10:35:15	t17.08.34	8.0	4	17e646ca2558a65ffe7aa185ba75d5c3a573c041b897355c2721e9a8ca5fee24
89	2015-08-19 10:16:01	t17.08.34	8.0	4	22957429e8ab527ff8bb45fbc50aa8400ea643a68de8d43da3fee3239e2159d4
88	2015-08-19 10:16:01	t17.08.34	8.0	4	3553c136b4eba70eec5d80abe44bd7c7c33ab1b65de617dbb7be5025c9cf01f1
90	2015-10-13 10:52:52	t17.08.34	8.0	4	e68e835904aaef2da5b38e9532036117996d58d3fba05cbe454f9d418be60ef4

Posted on Jul 05, 2017 in **#Incident management**, **#Threats**, **#Trends in Japan** | **Permalink**