SSL CBC 暴力破解帳號密碼事件分析

資安事件名稱: SERVER-OTHER SSL CBC ENCRYPTION MODE WEAKNESS BRUTE FORCE ATTEMPT

前言

- ASOC在三月份報告中，統計出SSL CBC 暴力破解帳號密碼事件量為當月第二名。
- 查詢開單系統紀錄中，此規則是去年12月月底才新增，而且1月、2月的事件量並非很多。

年份	月份	事件數量(單位:筆)
2017	12	5
2018	1	44
	2	22
	3	251
	4	350 (截至4/27統計)

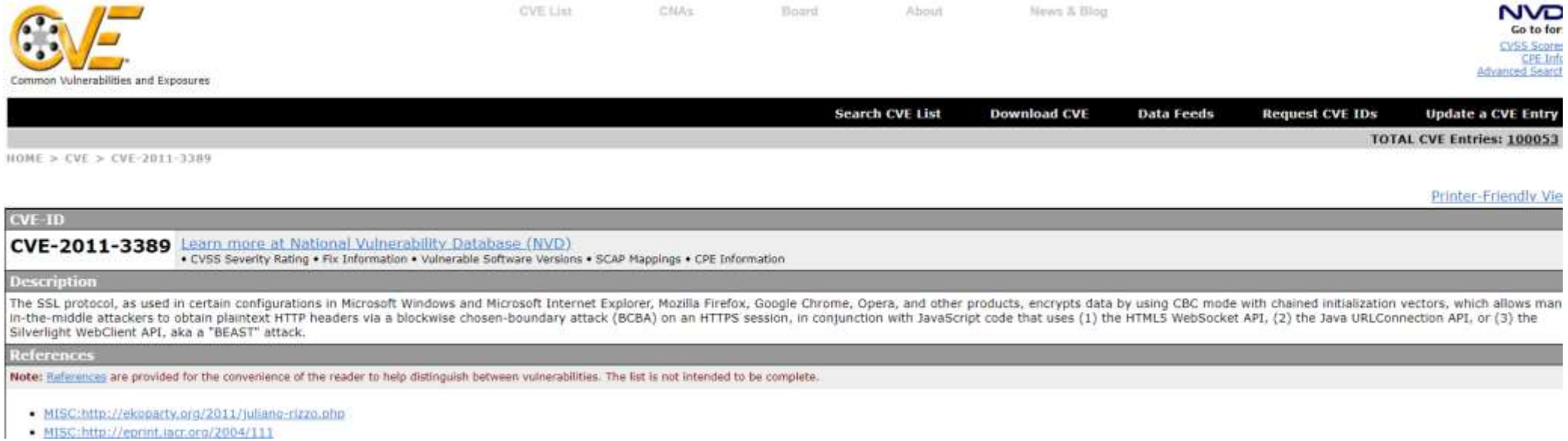
IPS攔截封包紀錄

Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message
2018-04-09 19:13:39	medium			120.107.162.108	TWN	140.112.10.220	TWN	64782 / tcp	55536 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:12:21	medium			120.107.162.108	TWN	140.112.10.220	TWN	64771 / tcp	55537 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:11:06	medium			120.107.162.108	TWN	140.112.10.220	TWN	64753 / tcp	55536 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:09:08	medium			120.107.162.108	TWN	140.112.10.220	TWN	64739 / tcp	55537 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:06:01	medium			120.107.162.108	TWN	140.112.10.220	TWN	64727 / tcp	55545 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:04:59	medium			120.107.162.108	TWN	140.112.10.220	TWN	64715 / tcp	55539 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:02:50	medium			120.107.162.108	TWN	140.112.10.220	TWN	64695 / tcp	55553 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 19:01:17	medium			120.107.162.108	TWN	140.112.10.220	TWN	64675 / tcp	55558 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 18:59:54	medium			120.107.162.108	TWN	140.112.10.220	TWN	64662 / tcp	55540 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 18:57:10	medium			120.107.162.108	TWN	140.112.10.220	TWN	64628 / tcp	55536 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 18:53:27	medium			120.107.162.108	TWN	140.112.10.220	TWN	64588 / tcp	55536 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 18:52:24	medium			120.107.162.108	TWN	140.112.10.220	TWN	64576 / tcp	55562 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 18:50:35	medium			120.107.162.108	TWN	140.112.10.220	TWN	64557 / tcp	55547 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 12:10:25	medium			140.135.57.220	TWN	140.112.254.38	TWN	64480 / tcp	83 (mit-ml-dev) / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 08:10:56	medium			163.20.242.76	TWN	140.124.104.173	TWN	61612 / tcp	2092 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-09 08:04:22	medium			163.20.242.76	TWN	140.124.104.173	TWN	61063 / tcp	2092 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-08 22:54:59	medium			150.116.192.112	TWN	140.124.104.173	TWN	58655 / tcp	2365 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 01:50:09	medium			118.150.148.22	TWN	203.64.154.27	TWN	20773 / tcp	2443 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 21:24:38	medium			61.60.61.62	TWN	140.124.104.173	TWN	37143 / tcp	2094 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 21:10:13	medium			61.60.61.62	TWN	140.124.104.173	TWN	48971 / tcp	2094 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 20:09:40	medium			150.117.8.8	TWN	203.71.63.17	TWN	59037 / tcp	2205 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 19:51:14	medium			150.117.8.8	TWN	203.71.63.17	TWN	58740 / tcp	2205 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 19:34:48	medium			150.117.8.8	TWN	203.71.63.17	TWN	58336 / tcp	2205 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 19:22:55	medium			150.117.8.8	TWN	203.71.63.17	TWN	57718 / tcp	2205 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc
2018-04-05 19:05:11	medium			61.60.61.62	TWN	140.124.104.173	TWN	62966 / tcp	2094 / tcp	Unknown (Unknown)	101	SERVER-OTHER SSL CBC encryption mode weakness brute forc

事件分析

CVE弱點描述

- 此事件是跟CVE-2011-3389相關:
  1. 使用CBC加密模式時，因SSL 3.0和TLS 1.0 舊版通訊協定中的設計缺點，所造成資訊洩漏的問題，這個弱點會使加密的 SSL/TLS 流量遭到解密
  2. 瀏覽器(IE, Firefox, Chrome, Opera等)為主要攻擊媒介
  3. 此弱點又稱為BEAST Attack (Browser Exploit Against SSL/TLS Attack，野獸攻擊)



IPS偵測規則 (snort id:20212)

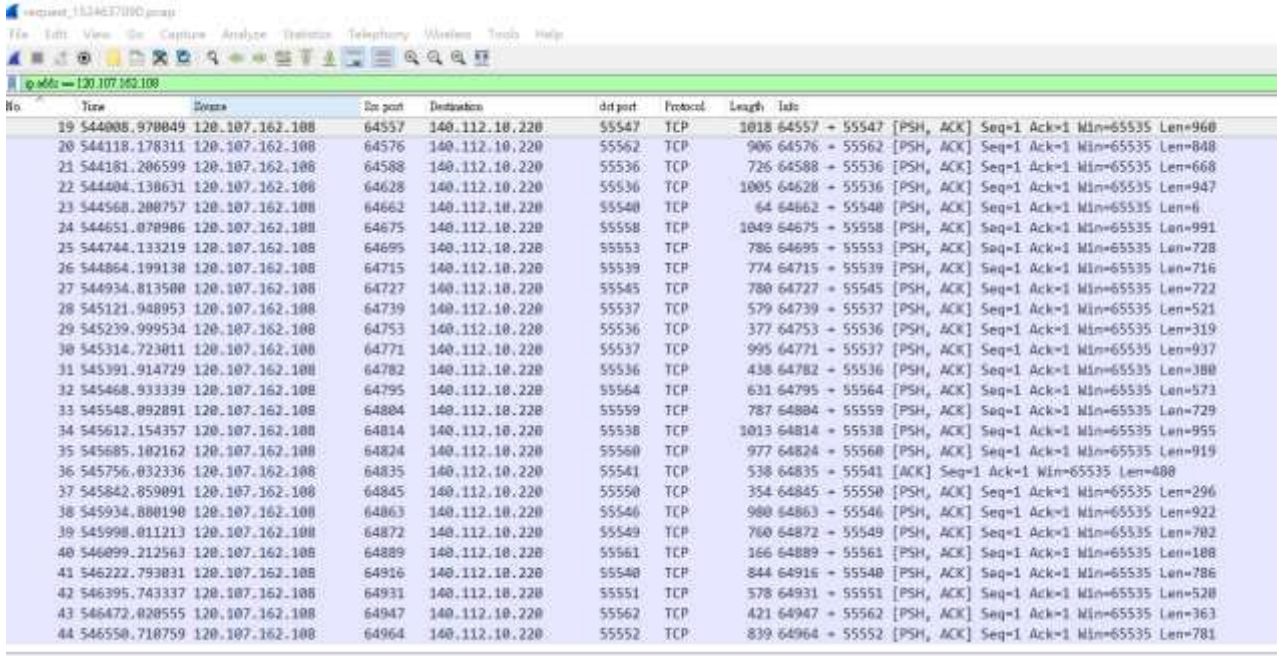
1. 外對內攻擊
2. 跟行為有關:在短時間內的連線次數大於某個門檻值以上 (非正常連線行為)
3. 跟封包內容無關:規則說明中沒有提到封包內容要符合任何關鍵字

IPS記錄的封包

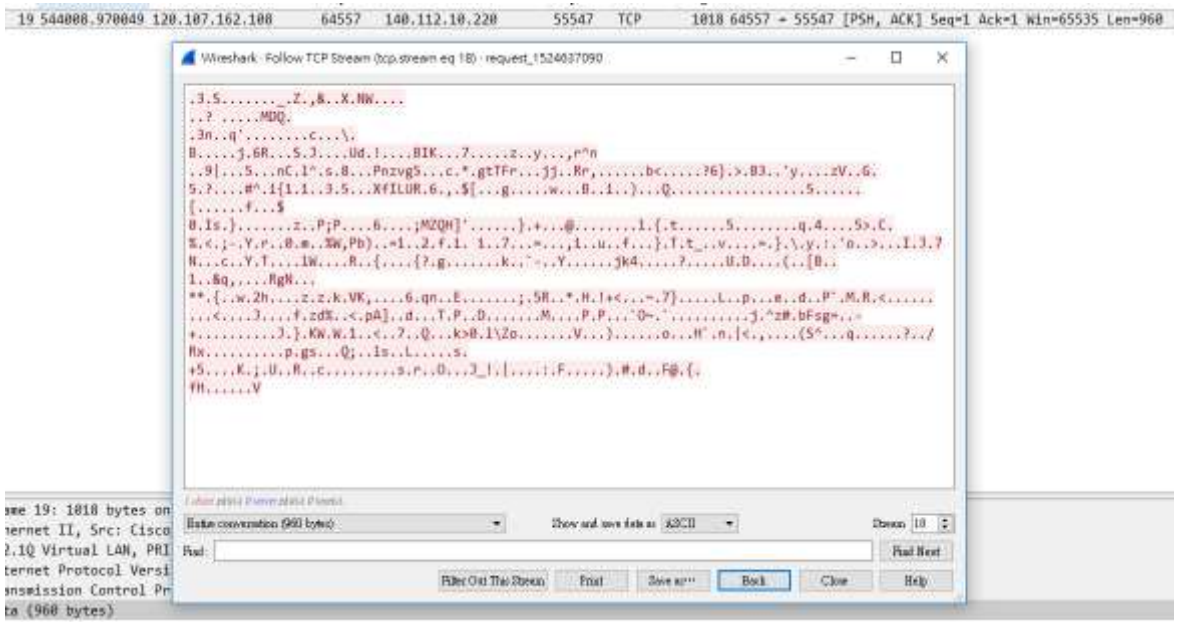
- IPS只能檢查未加密的封包內容
- IPS會根據規則，把符合規則條件的封包做阻擋並記錄
- 從IPS下載此事件封包，觀察被記錄的封包內容

封包內容

- 可參考下面兩張圖

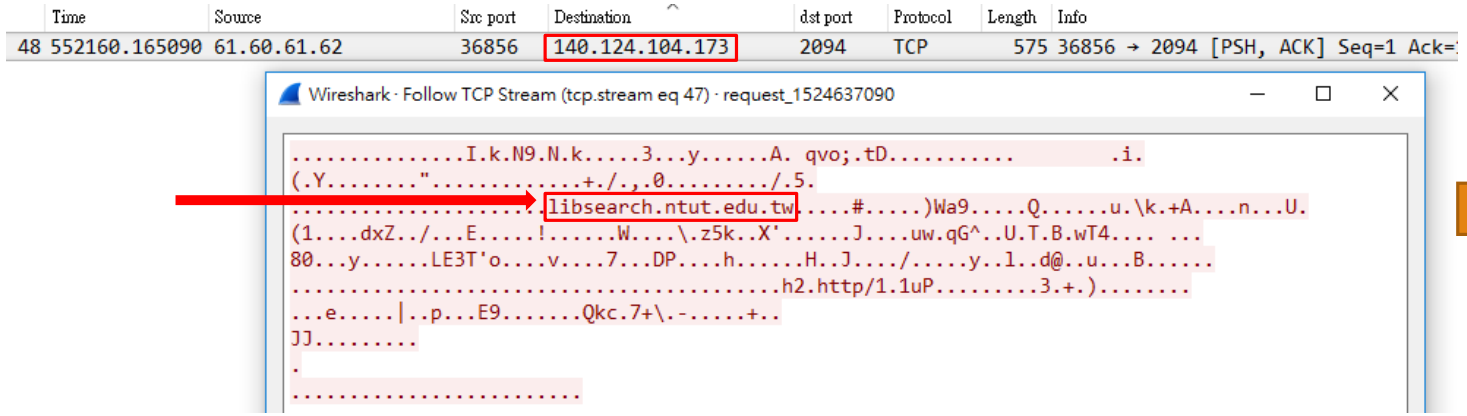


No.	Time	Source	Src port	Destination	dst port	Protocol	Length	Info
19	544008.970049	120.107.162.108	64557	140.112.10.220	55547	TCP	1018	64557 → 55547 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=960
20	544118.178311	120.107.162.108	64576	140.112.10.220	55562	TCP	906	64576 → 55562 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=848
21	544181.206599	120.107.162.108	64588	140.112.10.220	55536	TCP	726	64588 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=668
22	544404.138631	120.107.162.108	64628	140.112.10.220	55536	TCP	1005	64628 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=947
23	544568.208757	120.107.162.108	64662	140.112.10.220	55540	TCP	64	64662 → 55540 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=6
24	544651.078986	120.107.162.108	64675	140.112.10.220	55558	TCP	1049	64675 → 55558 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=991
25	544744.133219	120.107.162.108	64695	140.112.10.220	55553	TCP	786	64695 → 55553 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=728
26	544864.199130	120.107.162.108	64715	140.112.10.220	55539	TCP	774	64715 → 55539 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=716
27	544934.813500	120.107.162.108	64727	140.112.10.220	55545	TCP	780	64727 → 55545 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=722
28	545121.948953	120.107.162.108	64739	140.112.10.220	55537	TCP	579	64739 → 55537 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=521
29	545239.999534	120.107.162.108	64753	140.112.10.220	55536	TCP	377	64753 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=319
30	545314.723011	120.107.162.108	64771	140.112.10.220	55537	TCP	995	64771 → 55537 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=937
31	545391.914729	120.107.162.108	64782	140.112.10.220	55536	TCP	438	64782 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=380
32	545468.933339	120.107.162.108	64795	140.112.10.220	55564	TCP	631	64795 → 55564 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=573
33	545548.092891	120.107.162.108	64804	140.112.10.220	55559	TCP	787	64804 → 55559 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=729
34	545612.154357	120.107.162.108	64814	140.112.10.220	55538	TCP	1013	64814 → 55538 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=955
35	545685.102162	120.107.162.108	64824	140.112.10.220	55560	TCP	977	64824 → 55560 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=919
36	545756.032336	120.107.162.108	64835	140.112.10.220	55541	TCP	538	64835 → 55541 [ACK] Seq=1 Ack=1 Win=65535 Len=480
37	545842.859091	120.107.162.108	64845	140.112.10.220	55550	TCP	354	64845 → 55550 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=296
38	545934.880190	120.107.162.108	64863	140.112.10.220	55546	TCP	980	64863 → 55546 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=922
39	545998.011213	120.107.162.108	64872	140.112.10.220	55549	TCP	760	64872 → 55549 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=702
40	546099.212563	120.107.162.108	64889	140.112.10.220	55561	TCP	166	64889 → 55561 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=108
41	546222.793831	120.107.162.108	64916	140.112.10.220	55540	TCP	844	64916 → 55540 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=786
42	546395.743337	120.107.162.108	64931	140.112.10.220	55551	TCP	578	64931 → 55551 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=520
43	546472.020555	120.107.162.108	64947	140.112.10.220	55562	TCP	421	64947 → 55562 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=363
44	546550.718759	120.107.162.108	64964	140.112.10.220	55552	TCP	839	64964 → 55552 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=781



分析封包

- 幾乎大部分的封包內容是沒有特定的特徵值
- 極少數的封包有殘留的關鍵字(如下圖，此種封包數量約10~20個，約3%~6%)
- 查詢下圖關鍵字，會連線到台北科技大學圖書館登入頁面；連線到此IP也會是同個畫面



結論

- 依照目前現有的證據推論:
  1. 此資安事件名稱命名不精準，會有誤導處理資安事件的方向；可能是因為以CVE-2011-3389弱點描述而命名此規則
  2. ASOC認為此事件處理方向要從觸發規則條件著手，本事件重點在試圖暴力破解帳號密碼
  3. 要關注在連線行為上，會短時間內的大量連線到網頁不是正常使用網路行為

建議

- 更新作業系統與瀏覽器到最新版本
- 如果觸發本資安事件，請使用者先使用防毒軟體掃描電腦主機
- 檢查正在使用的程式是否會產生大量連線的行為
- 檢查自身使用電腦的習慣

資料來源

1) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2011-3389
2) https://docs.microsoft.com/zh-tw/security-updates/SecurityAdvisories/2011/2588513
3) https://docs.microsoft.com/zh-tw/security-updates/SecurityBulletins/2012/ms12-006
4) https://vnhacker.blogspot.tw/2011/09/beast.html
5) http://securityalley.blogspot.tw/2014/07/ssltls-beast.html