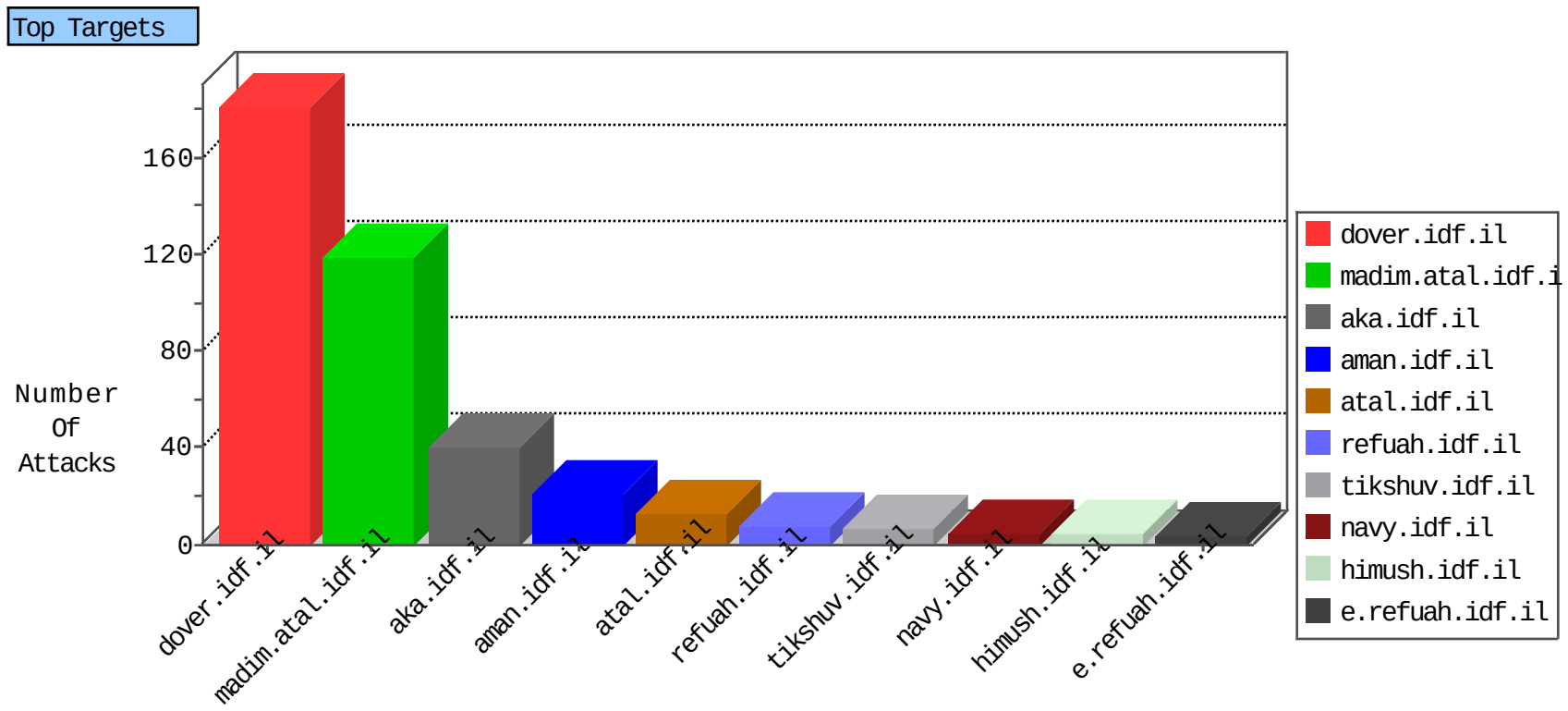
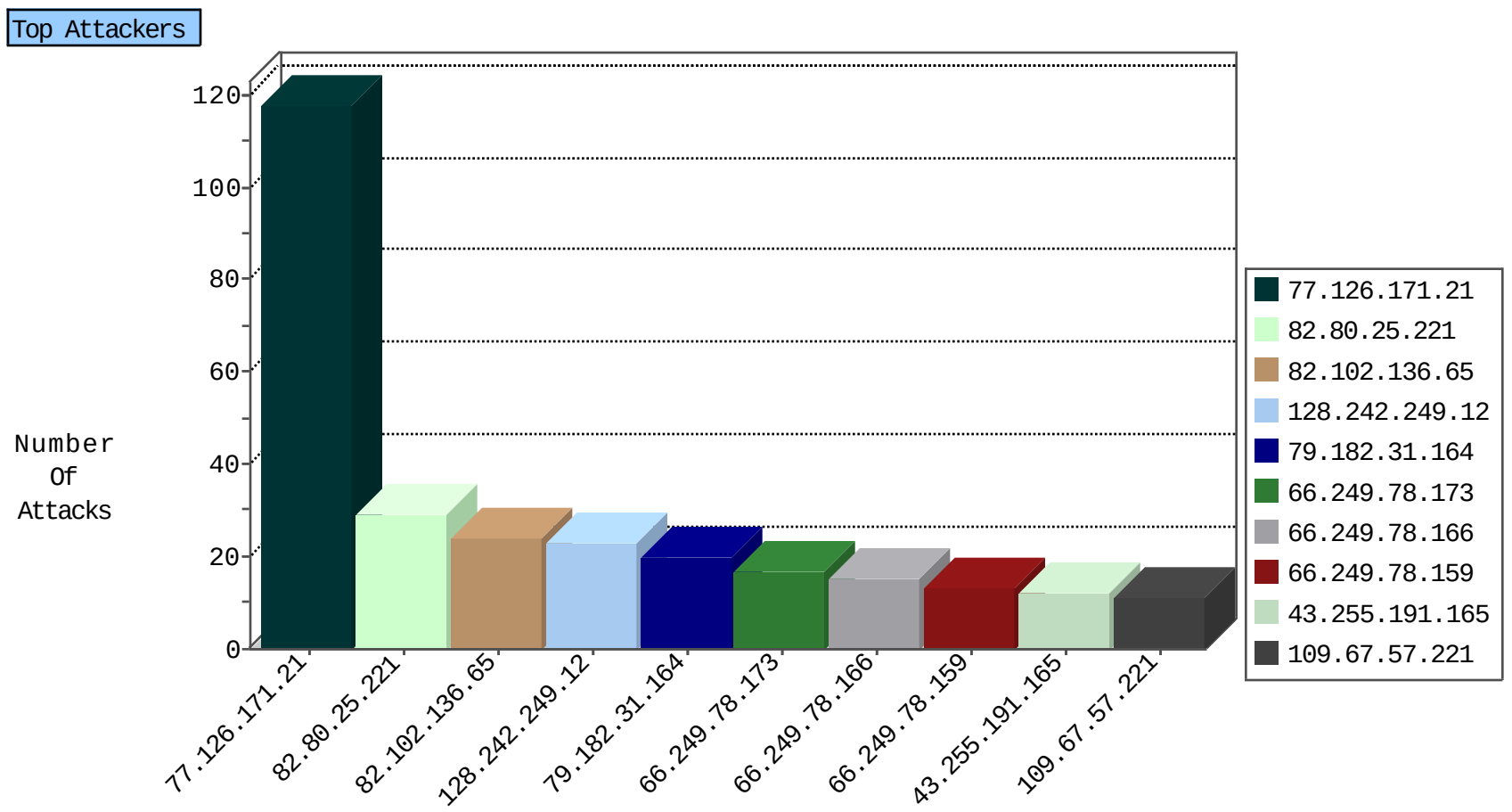
03-29-2015-01:03:01 to 03-29-2015-02:03:01

IDF Under Attack
03-29-2015-01:03:01

Top Targets



Top Attackers



03-29-2015-01:03:01 to 03-29-2015-02:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-29-2015-01:03:01 to 03-29-2015-02:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	23
83.6.8.179	Poland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1

03-29-2015-01:03:01 to 03-29-2015-02:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
109.67.57.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
208.39.68.33	United States	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
176.12.136.227	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.63.161.216	Korea, Republic of	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.28.203.202	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.214.71.176	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
14.63.161.216	Korea, Republic of	147.237.77.216	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.28.206.86	Switzerland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
14.63.161.216	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.28.202.243	Switzerland	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

03-29-2015-01:03:01 to 03-29-2015-02:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
79.177.100.21	Israel	147.237.76.30	himush.idf.il	First packet isn't SYN	drop	drop	5
188.120.148.172	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
109.67.57.221	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
176.12.136.227	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
2.54.173.162	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
176.12.136.227	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
83.6.8.179	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.173.162	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
84.109.37.120	Israel	147.237.76.42	refuah.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.192	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
185.11.11.51	Yemen	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.158	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.50.9	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.142.7	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.28.203.171	Switzerland	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.29.33.206	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.206	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.192	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
185.11.11.51	Yemen	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.29.93.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
197.202.20.106	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.84.144	United States	147.237.77.176	matpash.idf.il	directory traversal overflow	Directory Traversal	monitor	1
85.130.247.20	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.28.203.171	Switzerland	147.237.0.33	idf.il		drop	drop	1
2.54.173.162	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.142.7	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.28.203.171	Switzerland	147.237.0.35	akaws.idf.il		drop	drop	1
5.29.33.206	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.138.17.205	France	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.174	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

03-29-2015-01:03:01 to 03-29-2015-02:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.126.171.21	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.171.21	Block	117
87.68.231.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	4
109.160.249.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.67.57.221	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.57.221	Block	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
80.246.138.144	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	2
14.63.161.216	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 14.63.161.216	Block	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	2
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
14.63.161.216	Korea, Republic of	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 14.63.161.216	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
94.124.5.10	Poland	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0828-4.stm	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at Ã–[[#17]]Ã?Â*f*cT[[#8]]lÃ?Ãž9Ã¾\Ã¾Ã…Na[[#11]][Âº`RÃ?Â¼Â‹rÃ¹Â¤Ã¢Â›ÃŸÂ¶zYaÃ…ÂžÃ¦T)4-V[[#19]]Ã…$TNÂ*f*Â„Â?[[#8]]Ã©Â„dÃ–Ã‹Ã–Ã¸zÂ¦m[[#22]]Ã¸3[[#3]]Ã³#[[#1]]ÂŠÃ·#Â¬MD{Ã^Ã–O'Â±tÃ?8W+Â¾=Ã¼5Ã‡[[#15]]ÃŽ[[#0]]Ãš[[#8]]>fÃ¹Â•ac/Â Ã‰Â¬Ãª[[#28]]Â‡[[#18]]Â¥Ã“a	Block	1
14.63.161.216	Korea, Republic of	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/muieblackcat	Block	1
213.189.150.227	Switzerland	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0101-7.stm	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Value at 22 for y×¥[[#27]]~Ã–Â¢Â½[[#18]]â€˜crÃ¼Â§Â¬Â½cÂ¡uâ€ ×›Ö¶0u5•{(×œÂ§Â¹[[#19]]yy~[[#14]][[#4]]Â-Ã¼Â·vÖ»Â±uËœÖ³â€ pËœÂ¿	Block	1
77.126.171.21	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.64.138	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 79.182.31.164	Block	1
5.29.123.19	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0202-2.stm	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name Ã–[[#17]]Ã?Â*f*cT[[#8]]lÃ?Ãž9Ã¾\Ã¾Ã…Na[[#11]][Âº`RÃ?Â¼Â‹rÃ¹Â¤Ã¢Â›ÃŸÂ¶zYaÃ…Âž Ã¦T)4-V[[#19]]Ã…$TNÂ*f*Â„Â?[[#8]]Ã©Â„dÃ–Ã‹Ã– Ã¸zÂ¦m[[#22]]Ã¸3[[#3]]Ã³#[[#1]]ÂŠÃ·#Â¬MD{Ã^Ã–O'Â±tÃ?8W+Â¾=Ã¼5Ã‡[[#15]]ÃŽ[[#0]]Ãš[[#8]]>fÃ¹Â•ac/Â Ã‰Â¬Ãª[[#28]]Â‡[[#18]]Â¥Ã“a	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0112-5.stm	Block	1
109.67.57.221	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.67.57.221	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	NULL Character in URL y×¥[[#27]]~Ã–Â¢Â½[[#18]]â€˜crÃ¼Â§Â¬Â½cÂ¡uâ€ ×›Ö¶0u5•{(×œÂ§Â¹[[#19]]yy~[[#14]][[#4]]Â-Ã¼Â·vÖ»Â±uËœÖ³â€ pËœÂ¿;×²fÂµv× â€”Â±vÖ½xÂžÂ¡×“[[#8]]Ö·[[#8]]Â¾Âšu×¨Ö¼[â„¢Â¬Â-n×¢Â¿lâ€™[[#17]]×žÂ·Â½ÂžÂŽgj0Ã–p*Ã–ei×ªg[[#11]][[#28]]m%jv×,â€¦×´[[#0]]Â¢xÖ¼oÂ?Â¶[[#4]]xÂ¿r[[#16]]â€”hoq][[#17]][[#26]]	Block	1
14.63.161.216	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/muieblackcat	Block	1
213.189.150.227	Switzerland	147.237.72.166	aka.idf.il	Multiple signatures from 213.189.150.227	Block	1
180.76.4.98	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String Â?Ã»× xª×‘×‘Â³×§[[#23]]Ö¹iÃ–7ÂŽÖ´#=â€?Ö¾:Â©7×§N'x×¨z@Ãš6[[#14]]×°^×“rÂŠÂ»Â¶×œÂŽ•Ö¾ÃŠÂ¡A×œÂ-×³3[[#8]] on y×¥[[#27]]~Ã–Â¢Â½[[#18]]â€˜crÃ¼Â§Â¬Â½cÂ¡uâ€ ×›Ö¶0u5•{(×œÂ§Â¹[[#19]]yy~[[#14]][[#4]]Â-Ã¼Â·vÖ»Â±uËœÖ³â€ pËœÂ¿	Block	1
109.253.136.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.69.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
84.108.16.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 79.182.31.164	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.84.144	United States	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
213.189.150.227	Switzerland	147.237.72.166	aka.idf.il	SQL injection on parameter catid in www.aka.idf.il/main/giyus/general.aspx	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL y×¥[[#27]]~Ã–Â¢Â½[[#18]]â€˜crÃ¼Â§Â¬Â½cÂ¡uâ€ ×›Ö¶0u5•{(×œÂ§Â¹[[#19]]yy~[[#14]][[#4]]Â-Ã¼Â·vÖ»Â±uËœÖ³â€ pËœÂ¿;×²fÂµv× â€”Â±vÖ½xÂžÂ¡×“[[#8]]Ö·[[#8]]Â¾Âšu×¨Ö¼[â„¢Â¬Â-n×¢Â¿lâ€™[[#17]]×žÂ·Â½ÂžÂŽgj0Ã–p*Ã–ei×ªg[[#11]][[#28]]m%jv×,â€¦×´[[#0]]Â¢xÖ¼oÂ?Â¶[[#4]]xÂ¿r[[#16]]â€”hoq][[#17]][[#26]]	Block	1
79.179.186.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

03-29-2015-01:03:01 to 03-29-2015-02:03:01

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
125.209.235.184	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0312-3.stm	Block	1
66.249.75.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/faq/5.stm	Block	1
79.182.31.164	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 79.182.31.164	Block	1

03-29-2015-01:03:01 to 03-29-2015-02:03:01