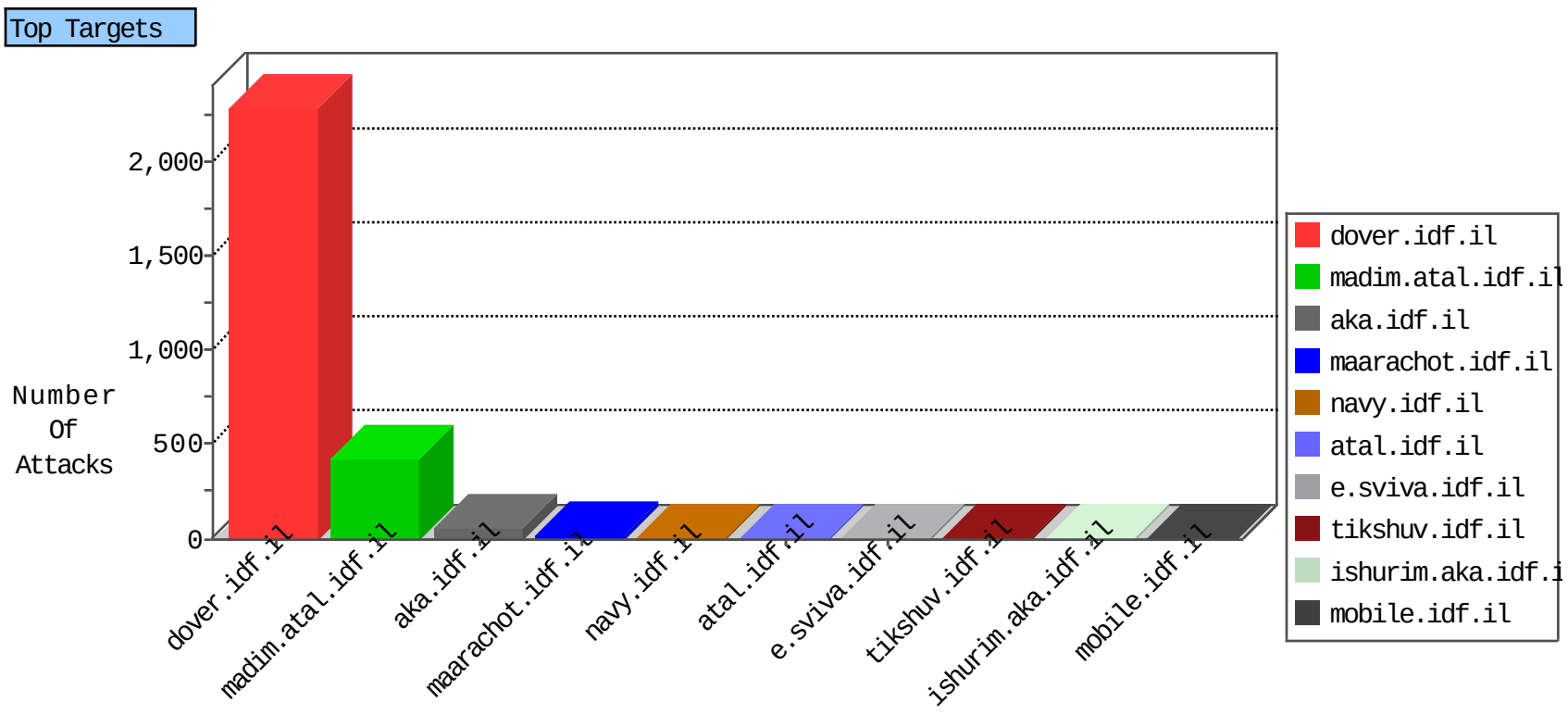
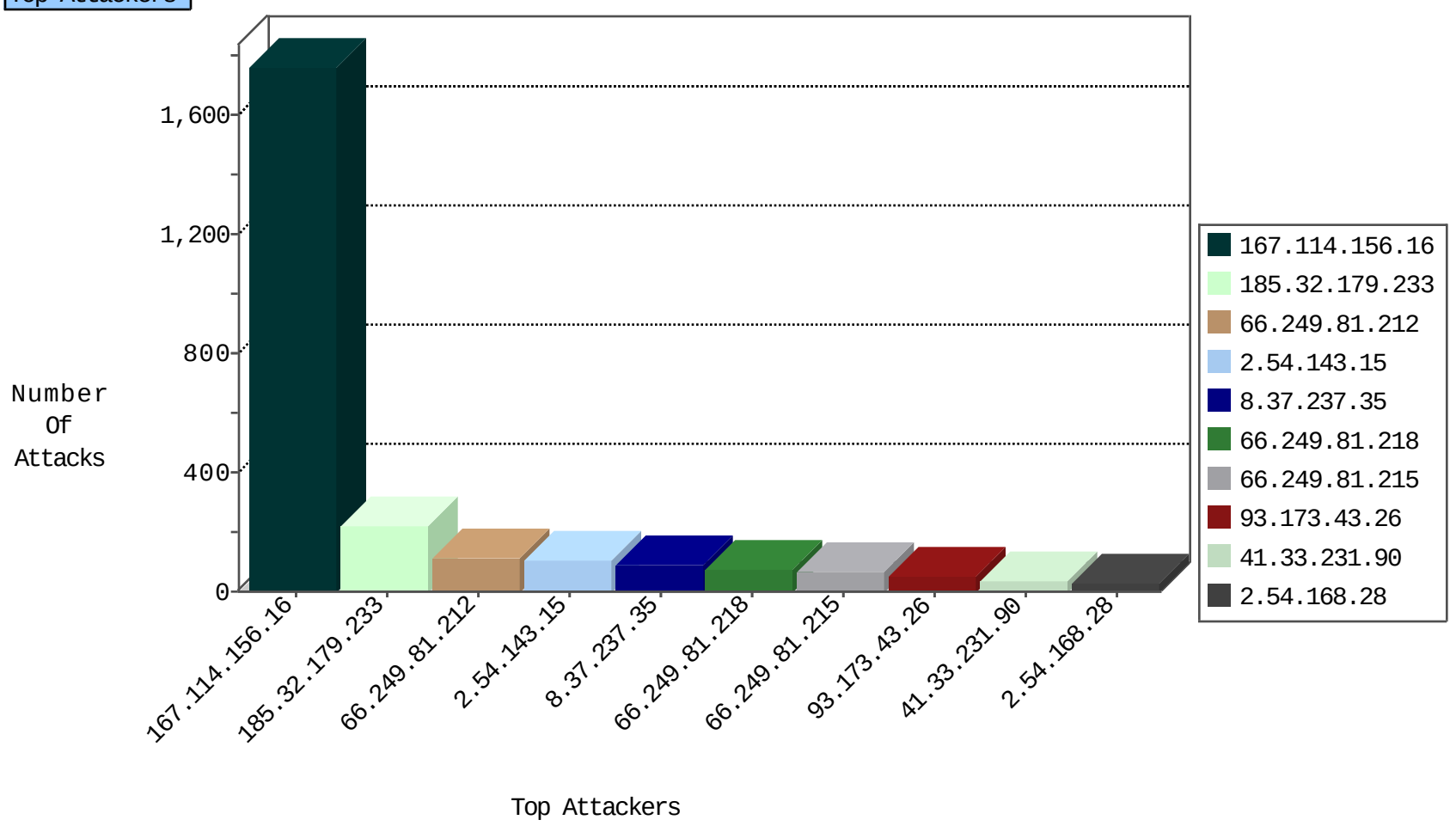
01-04-2016-06:04:09 to 01-04-2016-07:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-04-2016-06:04:09 to 01-04-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3193
222.186.30.233	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Http	drop	3
59.41.80.84	China	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
222.186.30.233	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
8.37.237.35	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
77.247.178.132	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
103.28.120.17	Bangladesh	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
111.40.86.154	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

01-04-2016-06:04:09 to 01-04-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-04-2016-06:04:09 to 01-04-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.32.179.233	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
114.226.241.65	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.72.166	Canada	aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.224	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
175.161.98.170	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.25.155.164	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
117.25.155.164	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
110.52.185.161	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.72.166	Canada	aka.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.224	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
117.25.155.164	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1

01-04-2016-06:04:09 to 01-04-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.237.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	23
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	23
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
2.54.143.15	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.0.81.17	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
46.19.85.146	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.198.7	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.149.97	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.168.28	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.0.101.201	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.176.200.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.45.254.226	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.123	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.28.83	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.177.191.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.66.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
131.253.36.202	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.183.149.53	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.108.88.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
189.122.197.177	Brazil	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.253.137.75	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1

01-04-2016-06:04:09 to 01-04-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.233	Block	136
2.54.143.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
93.173.43.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
2.54.143.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
2.54.168.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 185.32.179.233	Block	19
93.172.251.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/5196.jpg	Block	3
109.253.136.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.51.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
104.199.141.224	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 104.199.141.224	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
104.199.141.224	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 104.199.141.224	Block	2
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/5196.jpg	Block	2
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/5196.jpg	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
109.201.138.237	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.118.24.206	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
176.13.11.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-23059-he/dover	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL [[#0]][[#0]][[#0]][[#5]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#11]][[#0]][[#0]][[#0]][[#7]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#21]][[#1]]%[[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1
68.180.230.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.201.154.130	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.146.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.102	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.120.168.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/.aspx	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/2.0	Block	1
79.182.116.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/5196.jpg	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	NULL Character in Method [[#0]][[#0]][[#6]][[#4]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]]@[[#0]][[#0]][[#0]][[#0]][[#0]][[#8]][[#6]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]][[#8]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]@[[#0]][[#0]][[#0]][[#0]][[#0]]&[[#1]]%[[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]]Â,Â„Â‡AÂˆÃ±Ã£Ã,Ã¦Â’UÃ?GS[[#3]]*/*zÂ?Âªià’ÂšÃ„Ã€ WmpÂ-•[[#7]][[#31]][[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#3]][[#0]][[#0]][[#0]][[#1]][[#0]]Â,Â„Â‡Ã	Block	1
37.26.149.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
54.183.191.180	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
5.102.228.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/exampcert/	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	Illegal URL Path Encoding [[#0]][[#0]][[#0]][[#5]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#11]][[#0]][[#0]][[#0]][[#7]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#21]][[#1]]%[[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1
82.118.24.204	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
121.200.231.194	Australia	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	NULL Character in URL [[#0]][[#0]][[#0]][[#5]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#11]][[#0]][[#0]][[#0]][[#7]][[#0]]â€šâ€žâ€¡Ö°Â¿Â¾[[#0]][[#0]][[#21]][[#1]]%[[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1

01-04-2016-06:04:09 to 01-04-2016-07:04:09

01-04-2016-06:04:09 to 01-04-2016-07:04:09