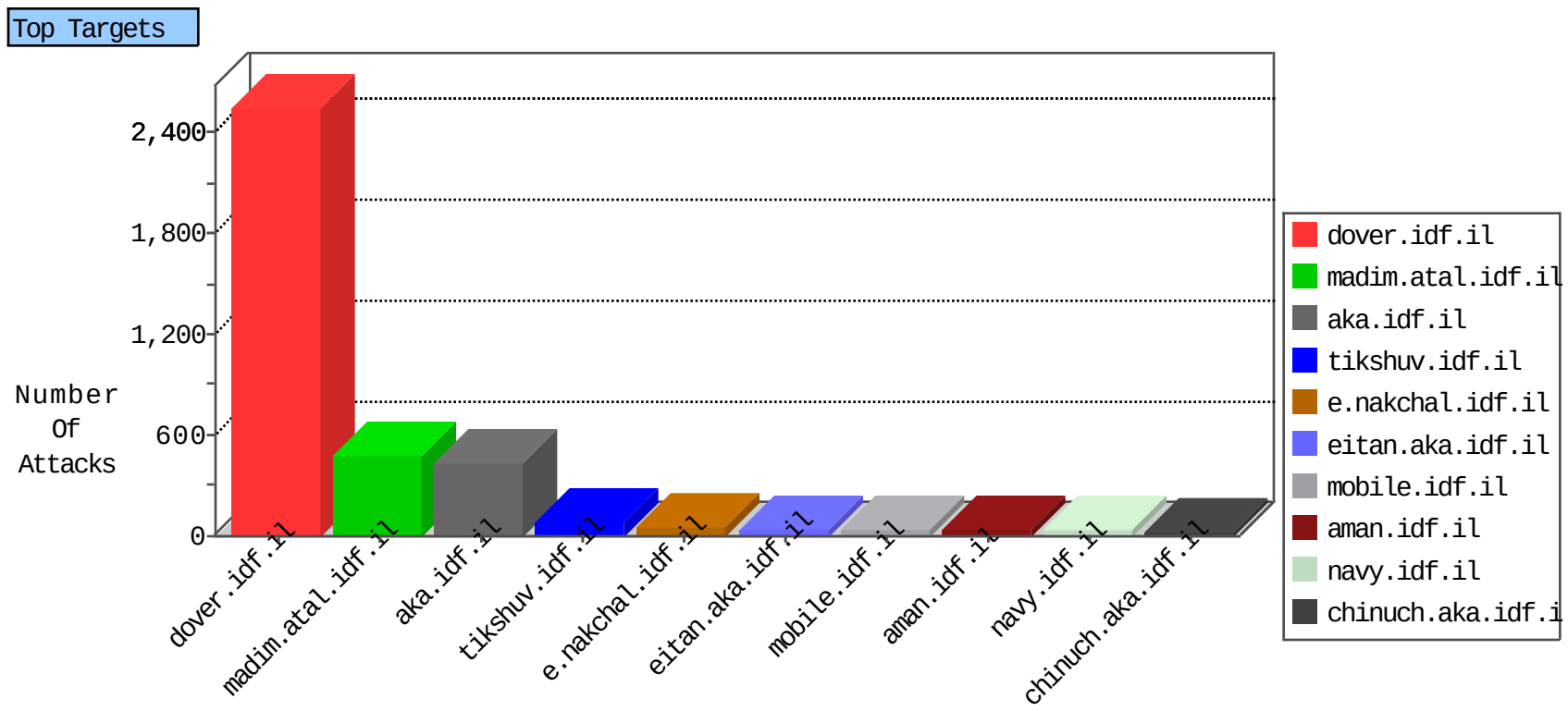
01-20-2016-18:04:04 to 01-20-2016-19:04:04

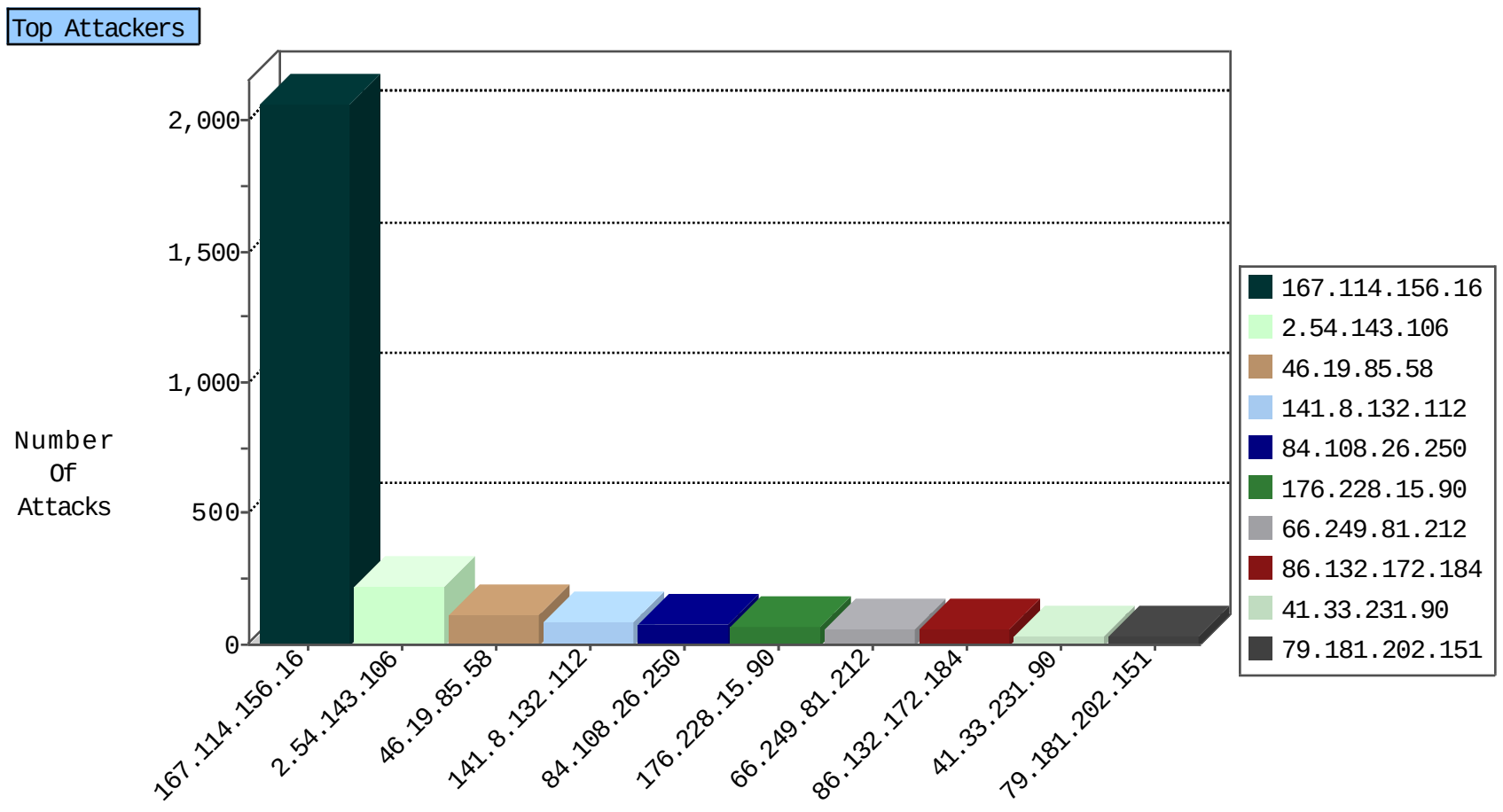
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-20-2016-18:04:04 to 01-20-2016-19:04:04

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	3111
86.132.172.184	United Kingdom	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	56
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
162.243.3.218	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
222.163.195.35	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2

01-20-2016-18:04:04 to 01-20-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.176	France	147.237.0.15	kosher-kravi.idf.i	C228: HTTP: AhrefBot crawler	Block	1

01-20-2016-18:04:04 to 01-20-2016-19:04:04

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	3
192.198.151.43	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.216	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
220.231.195.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 4096	1
93.158.211.210	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.218.113.195	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.29	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
72.22.182.162	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.174.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
131.191.84.45	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
115.236.75.201	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
109.253.196.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.41.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.211.210	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.29	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.200.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.29	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.3.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.203.248.154	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.236.75.201	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.160.237.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-20-2016-18:04:04 to 01-20-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
79.181.202.151	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.52.176.51	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	21
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
188.120.148.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.205.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.39.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	11
79.181.1.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.52.191.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
221.202.205.222	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
79.181.1.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
218.60.123.19	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
175.18.112.202	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
2.52.160.18	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.168.239.154	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	9
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.253.205.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
221.206.191.2	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
222.163.195.35	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
176.13.4.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.225.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.210.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.85.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
113.5.80.68	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.149.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.4.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.199.156.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.146.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.182.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.225.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
221.202.205.190	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
61.138.61.143	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.29.246.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
222.163.195.19	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.29.246.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.250.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.206.10	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5

01-20-2016-18:04:04 to 01-20-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.143.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
2.54.143.106	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.143.106	Block	84
84.108.26.250	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
176.228.15.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
2.54.143.106	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.143.106	Block	33
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
213.57.137.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
37.26.146.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
84.109.73.121	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.73.121	Block	5
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.205	Block	5
109.253.220.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.9.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.73.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.15.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.33.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
144.76.182.139	Germany	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 144.76.182.139	Block	3
109.64.154.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
213.8.204.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	2
2.54.172.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
162.243.3.218	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.3.218	Block	2
108.49.74.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 108.49.74.166	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.139.237.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
41.34.205.214	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.127.225.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.186.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
108.49.74.166	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he/dover.aspx	Block	1
31.168.114.111	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
82.17.194.247	United Kingdom	147.237.77.216	dover.idf.il	Illegal URL Path Encoding ×œÂŒ×?â€?[[#11]]â€¦â€˜×?t^â€ ¢>9Â?o×?[[#31]]-[[#0]]•4ÃŸ[[#8]]!Ö³Â¡Ö½[[#25]]â€”bÂŒ [[#14]]×°-[[#3]]_Â³×¤-[[#24]]ÂšÂœÂ¸wâ,¬[[#8]][[#31]]!p&râ€šsk-Ã·7×˜ [[#4]]-â€°6Ö¼bl,â€¢Ö²â€“x/×—g[[#3]][[#1]]@[[#4]]â, ªÂ»[[#21]]d[[#19]][[#24]]Â?× m%(Â²<×¡Æ'vfâ€"ÃŠÃ—×?2×±=Â?Â³	Block	1
212.199.156.81	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.116.206.10	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
91.185.208.141	Slovenia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.54.167.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.239.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.20.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
2.52.191.162	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.217.141	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.177.217.141 (Unknown SSL Session)	None	1
109.253.130.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.250.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
37.26.146.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.17.194.247	United Kingdom	147.237.77.216	dover.idf.il	NULL Character in URL ×œÂŒ×?â€?[[#11]]â€¦â€˜×?t^â€ ¢>9Â?o×?[[#31]]-[[#0]]•4ÃŸ[[#8]]!Ö³Â¡Ö½[[#25]]â€”bÂŒ [[#14]]×°-[[#3]]_Â³×¤-[[#24]]ÂšÂœÂ¸wâ,¬[[#8]][[#31]]!p&râ€šsk-Ã·7×˜ [[#4]]-â€°6Ö¼bl,â€¢Ö²â€“x/×—g[[#3]][[#1]]@[[#4]]â, ªÂ»[[#21]]d[[#19]][[#24]]Â?× m%(Â²<×¡Æ'vfâ€"ÃŠÃ—×?2×±=Â?Â³	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.102.254.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.17.194.247	United Kingdom	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

01-20-2016-18:04:04 to 01-20-2016-19:04:04