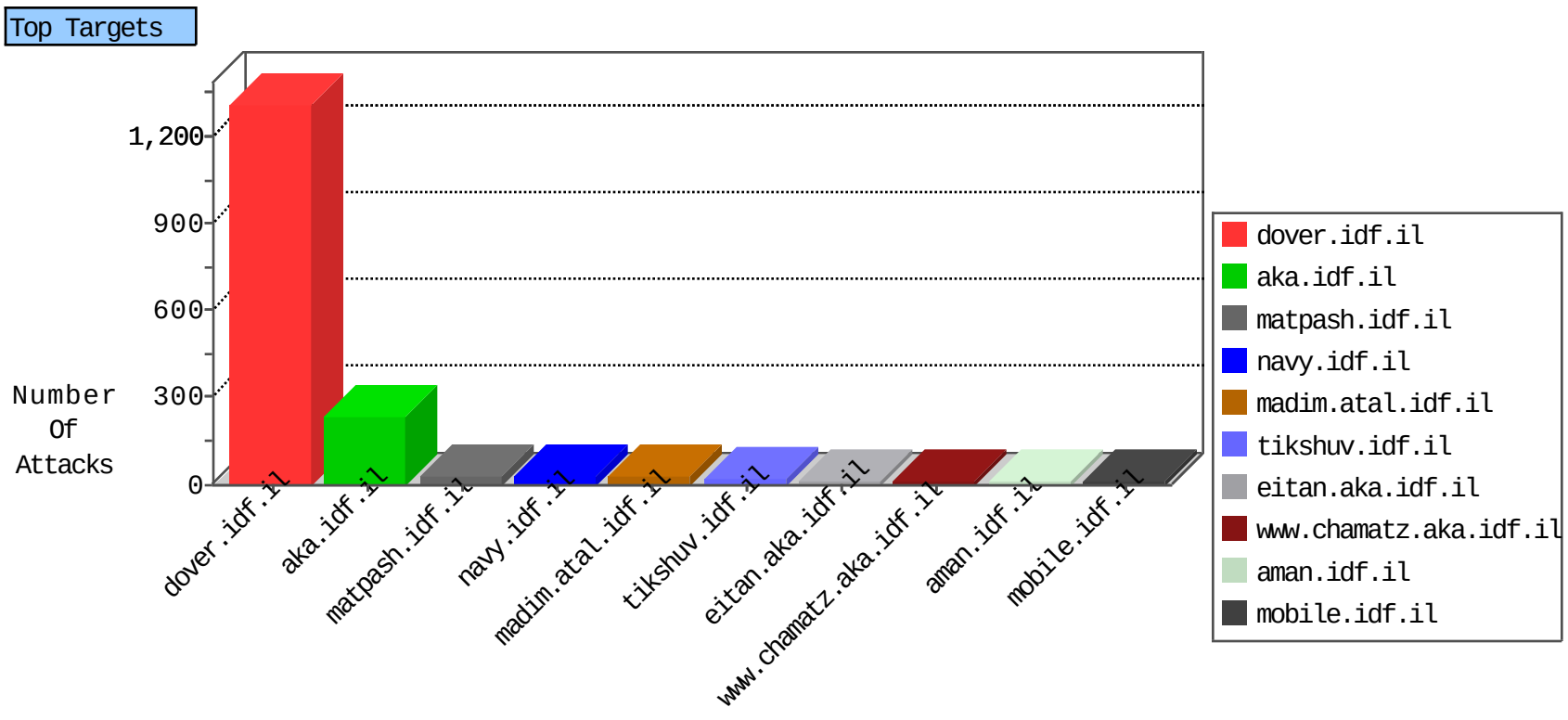
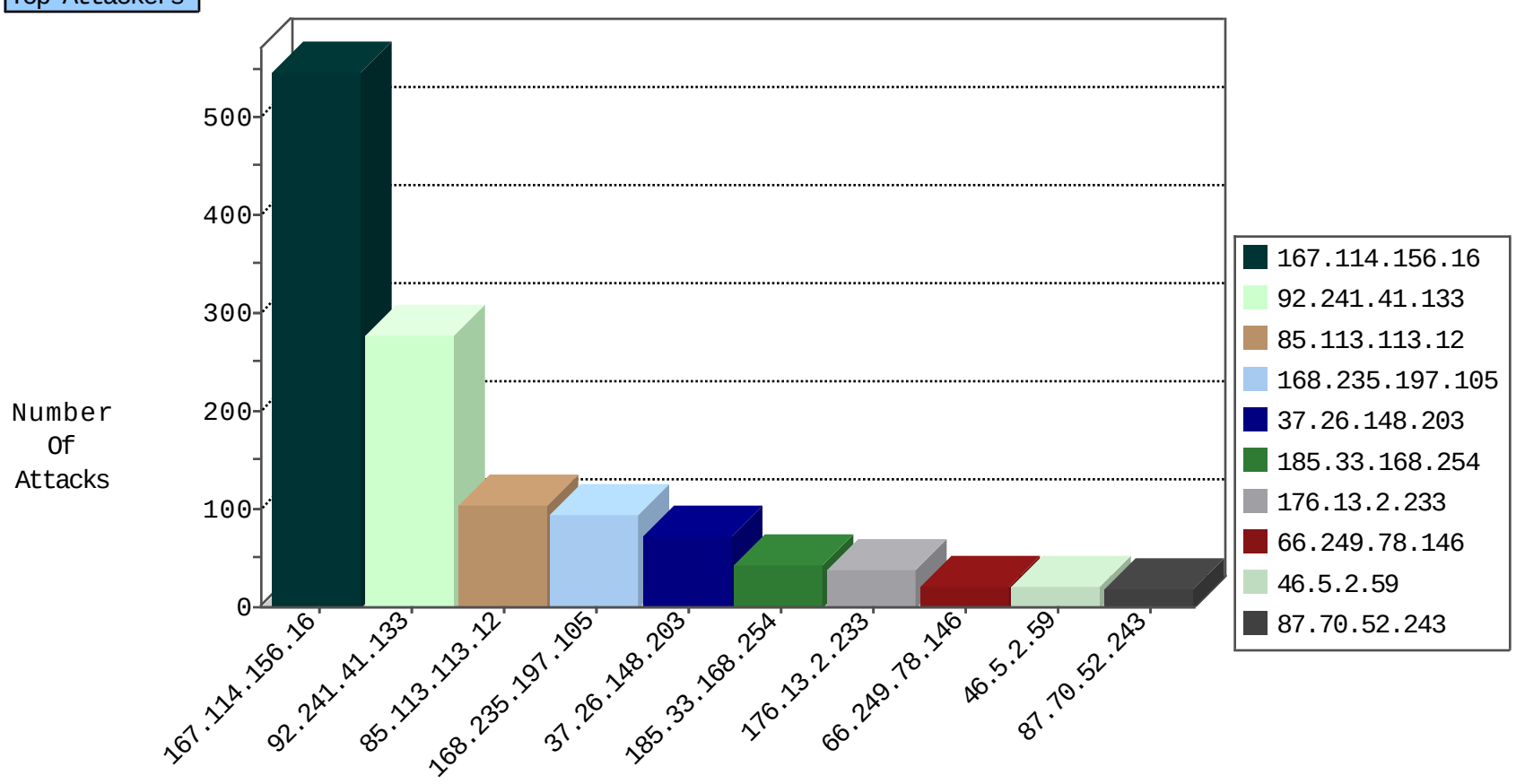
04-27-2016-20:04:03 to 04-27-2016-21:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-27-2016-20:04:03 to 04-27-2016-21:04:03

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	TCP handshake violation, first packet not syn	drop	48570
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	14721
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2573
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2127
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	92
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
168.235.197.105	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
176.67.111.43	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
78.134.6.49	Italy	147.237.8.24	e.lifestyle.idf	L4 Source or Dest Port Zero	drop	1
212.205.48.146	Greece	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.148.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
216.66.121.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.249.55.100	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
84.20.63.93	Switzerland	147.237.77.170	maarachot.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
187.167.253.1	Mexico	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.103.80	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.214.25.64	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.97.234	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
220.150.7.156	147.237.76.31	Japan	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -f -sS	1
203.86.29.220	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
61.182.170.38	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
104.214.25.64	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
104.156.230.199	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.150.7.156	147.237.76.31	Japan	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.230.74	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.216.176.244	147.237.77.226	Latvia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.103.252.142	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.113.113.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	99
168.235.197.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
37.26.148.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
176.13.2.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.5.2.59	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
176.13.10.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.130.98	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
216.66.121.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.157.120	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.66.13	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
166.137.242.31	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.2.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.216.2.72	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.205.48.146	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.172.139.233	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.242.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.157	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.67.111.43	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.102.242.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
85.130.237.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack		reject	4
199.30.25.132	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.186.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.19.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
104.32.253.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.42.175	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.15.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.216.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.134.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.23.164	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.130.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.112.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.205.83.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.241.41.133	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/com	Block	272
109.65.41.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.177.169.247	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	6
93.173.44.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.113.113.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/147.237.77.216:80/	Block	4
31.210.176.149	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
85.113.113.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.113.113.12	Block	2
2.55.26.127	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.64.232.68	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in URL ˙+[[Ɔ#0[[]]#0[[]]#28¸+¸/¸]]0¸[[¸,#	Block	1
188.154.19.11	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
54.193.117.219	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/yohalan/main/main.asp	Block	1
141.212.122.161	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]#ý%öÉV¦Èææ Ø'[[#8]]4uQ·²[[#22]]³óéÓ <E•8	Block	1
87.71.63.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar/login/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/4.asp	Block	1
217.132.111.253	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version À[[#20]]À	Block	1
82.47.13.169	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/15710.jpg	Block	1
149.78.172.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.139.52.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in URL ˙+[[Ɔ#0[[]]#0[[]]#28¸+¸/¸]]0¸[[¸,#19¸]]	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71576.pdf	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
176.52.44.13	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/'	Block	1
37.26.148.232	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
109.253.224.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Malformed HTTP Header Line 2	Block	1
84.94.84.124	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
162.243.188.75	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on /	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19831-he/kkkkkkk=d9eccbcakkkkkkk_d9eccbca	Block	1
41.102.177.134	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1846-he/dover.aspx'	Block	1
138.128.112.11	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL ˙+[[Ɔ#0[[]]#0[[]]#28¸+¸/¸]]0¸[[¸,#19¸]]	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
213.251.186.65	France	147.237.77.216	dover.idf.il	Malformed URL 212.74.50.8:80	Block	1
167.114.171.96	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on proxyjudge.us/judge.php	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]#ý%öÉV¦Èææ Ø'[[#8]]4uQ·²[[#22]]³óéÓ <E•8 in URL ˙+[[Ɔ#0[[]]#0[[]]#28¸+¸/¸]]0¸¸, [[#19]]¸	Block	1
79.176.72.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
222.198.128.207	China	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]#ý%öÉV¦Èææ Ø'[[#8]]4uQ·²[[#22]]³óéÓ <E•8	Block	1

04-27-2016-20:04:03 to 04-27-2016-21:04:03

Attacker Address	Attacker Country	Target Address	**Site**	Signature	Device Action	Count
180.76.15.137	China	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-27-2016-20:04:03 to 04-27-2016-21:04:03