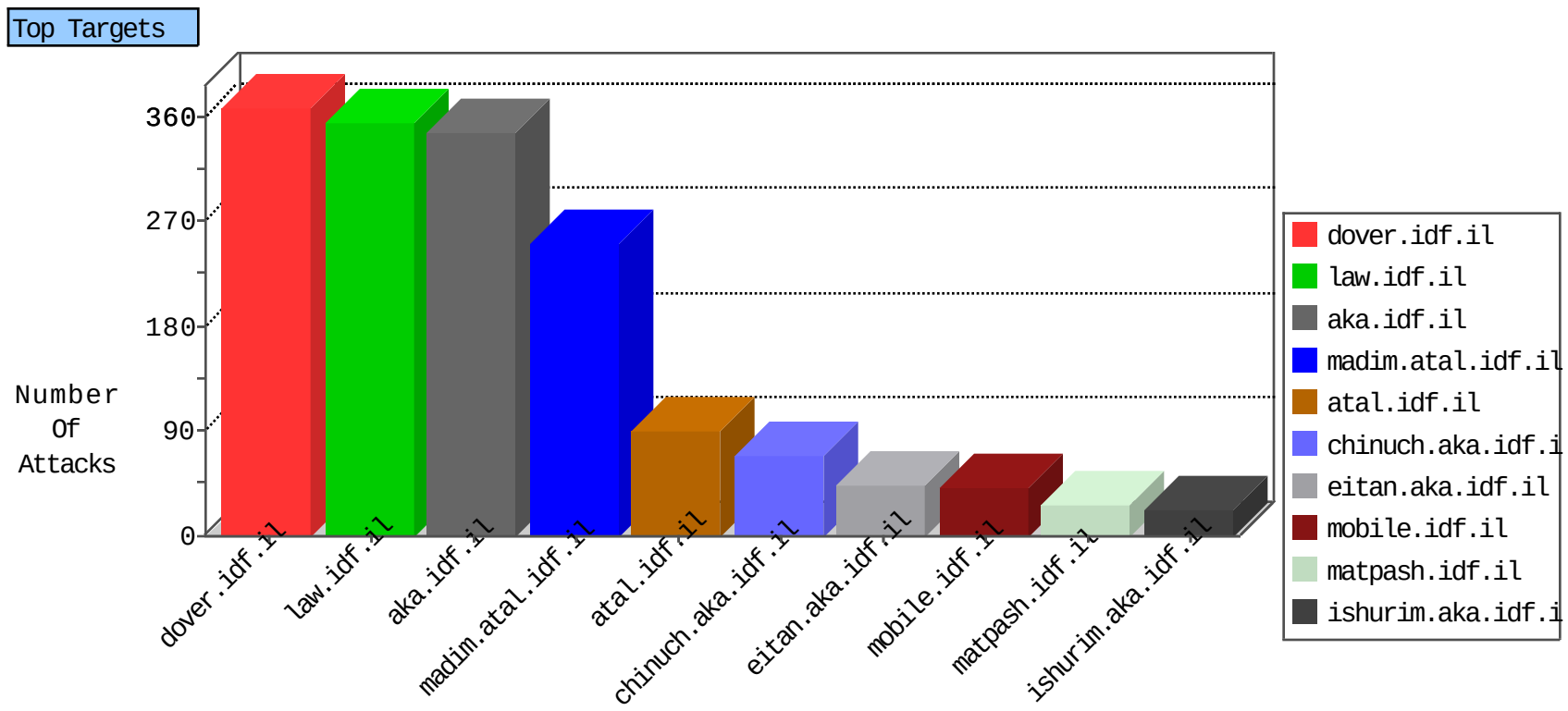
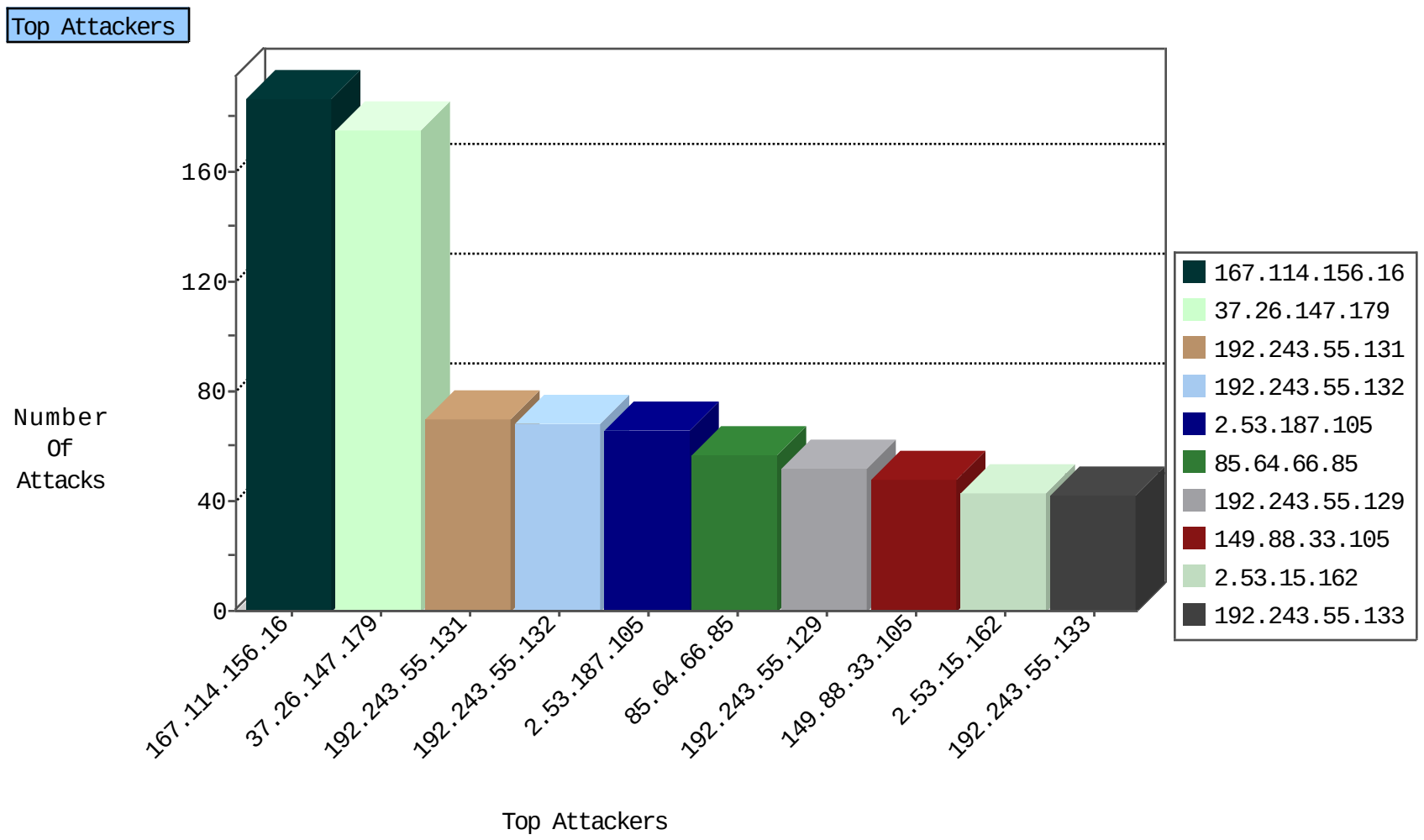
04-23-2016-20:04:07 to 04-23-2016-21:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-23-2016-20:04:07 to 04-23-2016-21:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	12492
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3838
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
74.91.23.108	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
104.238.135.152	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
69.30.202.229	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
222.228.159.22	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.46.100.170	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
74.91.17.178	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
94.102.49.116	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
74.91.17.179	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
94.102.49.116	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

04-23-2016-20:04:07 to 04-23-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-20:04:07 to 04-23-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.147.179	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
62.212.130.196	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
59.56.111.170	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.56.111.170	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.219.80.81	147.237.0.33	Mozambique	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.56.111.170	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.214.11.162	147.237.0.34	Poland	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.244.15.191	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.56.111.170	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.56.111.170	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.56.111.170	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
162.244.15.191	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
154.47.160.107	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.255.224.2	147.237.72.156	Sweden	aman.idf.il	ET SCAN Potential SSH Scan	1

04-23-2016-20:04:07 to 04-23-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.187.105	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
149.88.33.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
79.183.106.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
109.65.132.108	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	30
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
107.167.106.244	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
188.120.148.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.78.59.82	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
176.13.21.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.53.39.68	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.120.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.10.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.179.15.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.205.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.17.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.120.40.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.120.40.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.65.12.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
46.18.22.15	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.146.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.25.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.187	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

04-23-2016-20:04:07 to 04-23-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
2.53.15.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.53.19.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 85.64.66.85	Block	5
37.26.148.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 85.64.66.85	Block	5
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 85.64.66.85	Block	4
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 85.64.66.85	Block	4
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 85.64.66.85	Block	4
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 85.64.66.85	Block	4
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	4
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 85.64.66.85	Block	4
46.119.127.129	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
37.26.147.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 85.64.66.85	Block	3
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	3
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.66.85	Block	3
2.53.183.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 85.64.66.85	Block	2
72.9.148.10	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 72.9.148.10	Block	2
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 85.64.66.85	Block	2
5.102.222.86	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/421-he/patzar.aspx	Block	2
37.142.68.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
66.249.65.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ²§‰j¸¯℅w˛[[¬#28¬]]¥;Ú:c¯• [[#4]]w)[[#11]]0\[[#29]]ע••„[[#8]]°[[˛Ɔ#23eŸv˙y]]⊐‡[[82#]]	Block	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
201.138.183.96	Mexico	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen204	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
149.88.120.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ÷¬÷Ë~ÀVxÑe	Block	1
74.91.17.178	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.gege1.com/	Block	1
62.219.227.44	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name ƞƒ_…‡u7¯)˛ H[[#27]][fOü}Bu¢U[[#31]]¶/ף2]]6#[[]]6#[[@]]42#[[µÊr•'ן]]71#[[Ù'÷λnio‡	Block	1
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.197	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.44.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.115.111.71	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/...	Block	1
157.55.39.1	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
74.91.18.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	NULL Character in Method ßÀ¢üb—âšX_%¶U#QJà[[#22]]M•žø¨µ[[#11]]ªòvëu[[#15]]D•[[#0]]20ë¨» _Ëð«ŠÂBmêI‡ü%±°œ–Õ¯Ö•[[#21]]Þ[[#16]]xRh)[[#1]]Õ	Block	1
65.55.210.70	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String ƞƒ_…‡u7¯)˛ H[[#27]][fOü}Bu¢U[[#31]]¶/ף2]]6#[[]]6#[[@]]42#[[µÊr•'ן]]71#[[Ù'÷λnoo‡	Block	1

04-23-2016-20:04:07 to 04-23-2016-21:04:07