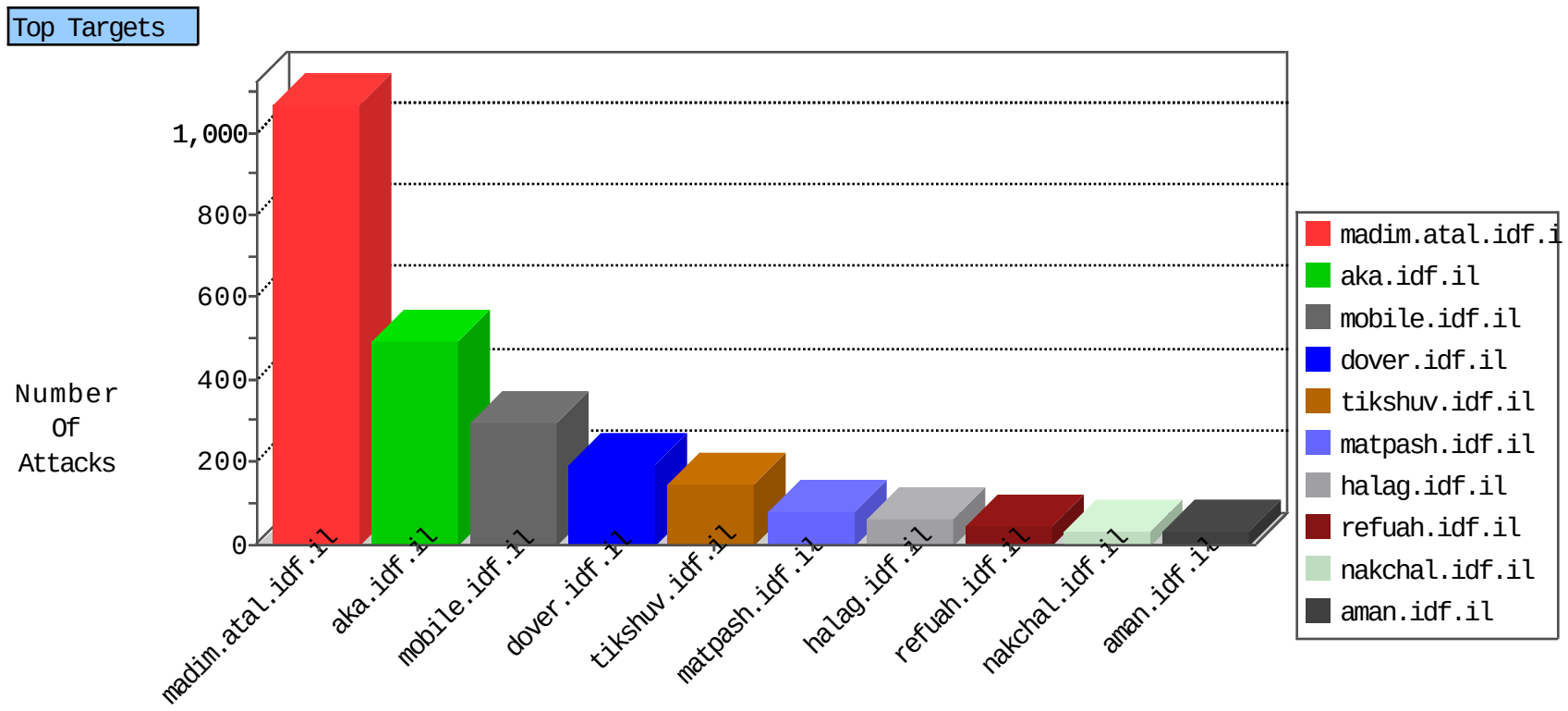
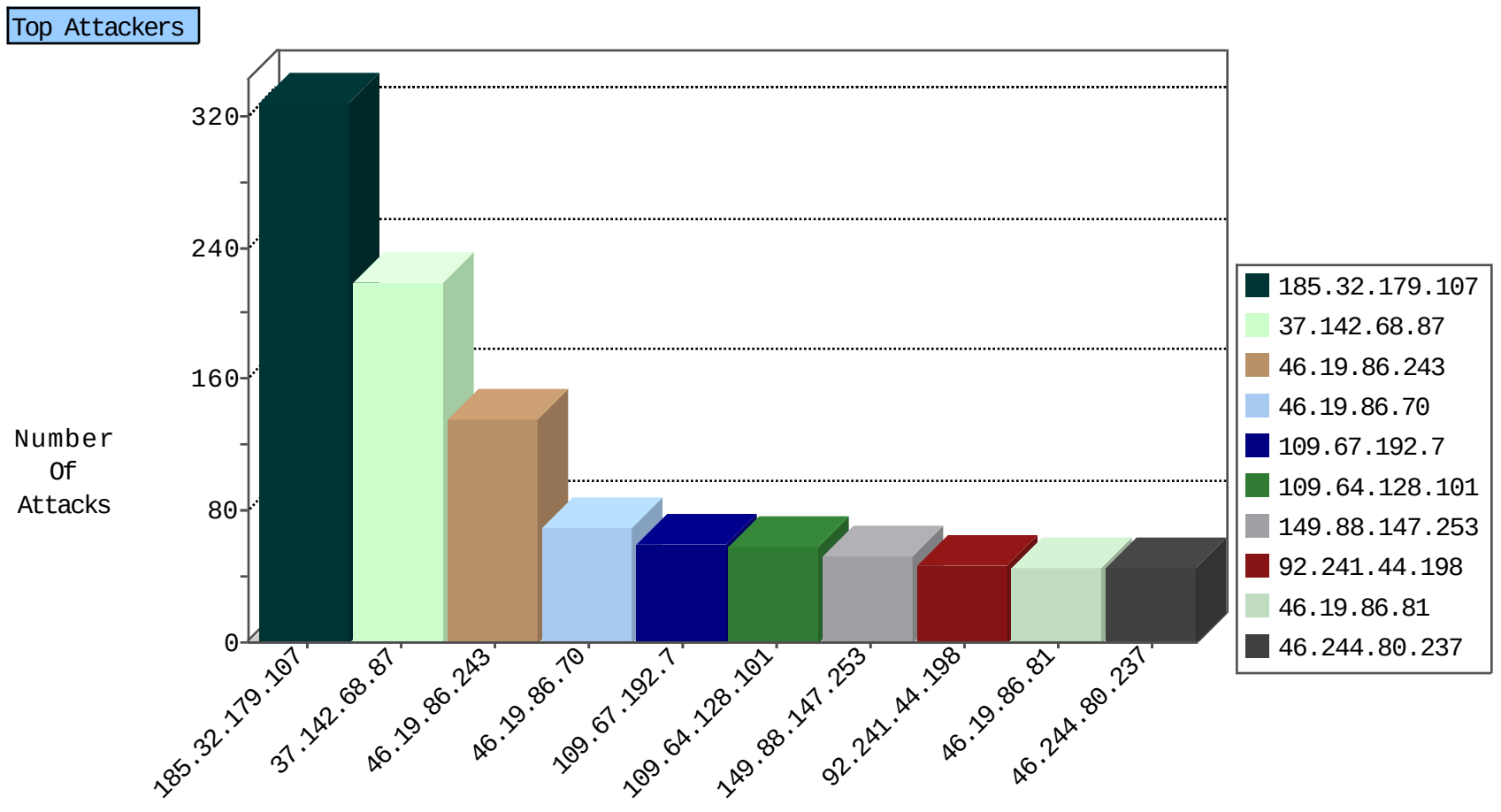
01-26-2016-19:04:07 to 01-26-2016-20:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-19:04:07 to 01-26-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2
74.91.28.62	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
183.33.62.91	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-26-2016-19:04:07 to 01-26-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0363: HTTP: Protected File Access (/etc/motd)	Permit	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
123.125.125.30	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0345: HTTP: Shell Command Execution (uname -a)	Block	1

01-26-2016-19:04:07 to 01-26-2016-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.152	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.83.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
92.241.44.198	147.237.0.34	Jordan	tikshuv.idf.il	SQL xp_cmdshell attempt	2
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.230.78.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
77.125.240.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.252.193.52	147.237.8.14	Turkey	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.230.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.255.112.188	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.37.187.183	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
95.110.234.9	147.237.77.243	Italy	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
92.241.44.198	147.237.0.34	Jordan	tikshuv.idf.il	SQL Injection - Select From	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.148.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.118.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.109.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.34.12.134	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
181.64.140.127	147.237.0.35	Peru	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.186.167.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.18.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.37.187.183	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
85.65.57.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-19:04:07 to 01-26-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.144	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.204.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.221.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.52.141.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
37.217.14.138	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
5.29.250.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.244.80.237	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
109.253.219.168	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.54.173.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.178.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.126.14.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.158.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.244.80.237	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.244.80.237	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
94.230.86.193	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	8
84.228.56.141	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
149.88.147.253	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.175.138	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.9.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.230.198	Bulgaria	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
31.210.186.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.20.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.230.198	Bulgaria	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	166
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
185.32.179.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.67.192.7	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
109.64.128.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
185.32.179.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	51
176.13.8.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
149.88.147.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
87.68.58.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
176.13.23.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
185.32.179.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.142.68.87	Block	15
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 92.241.44.198	Block	11
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.52.141.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.253.221.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.204.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.246.139.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
85.64.110.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.14.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
84.108.13.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	4
178.137.85.67	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 178.137.85.67	Block	3
2.54.173.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
79.180.139.154	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
80.246.137.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.139.154	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	3
37.26.147.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.221.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.125.123.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.242.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.242.25	Block	3
185.120.126.72		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.83.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.205.97	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
2.54.12.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.88.200.21	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.20.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.94.48.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2

01-26-2016-19:04:07 to 01-26-2016-20:04:07