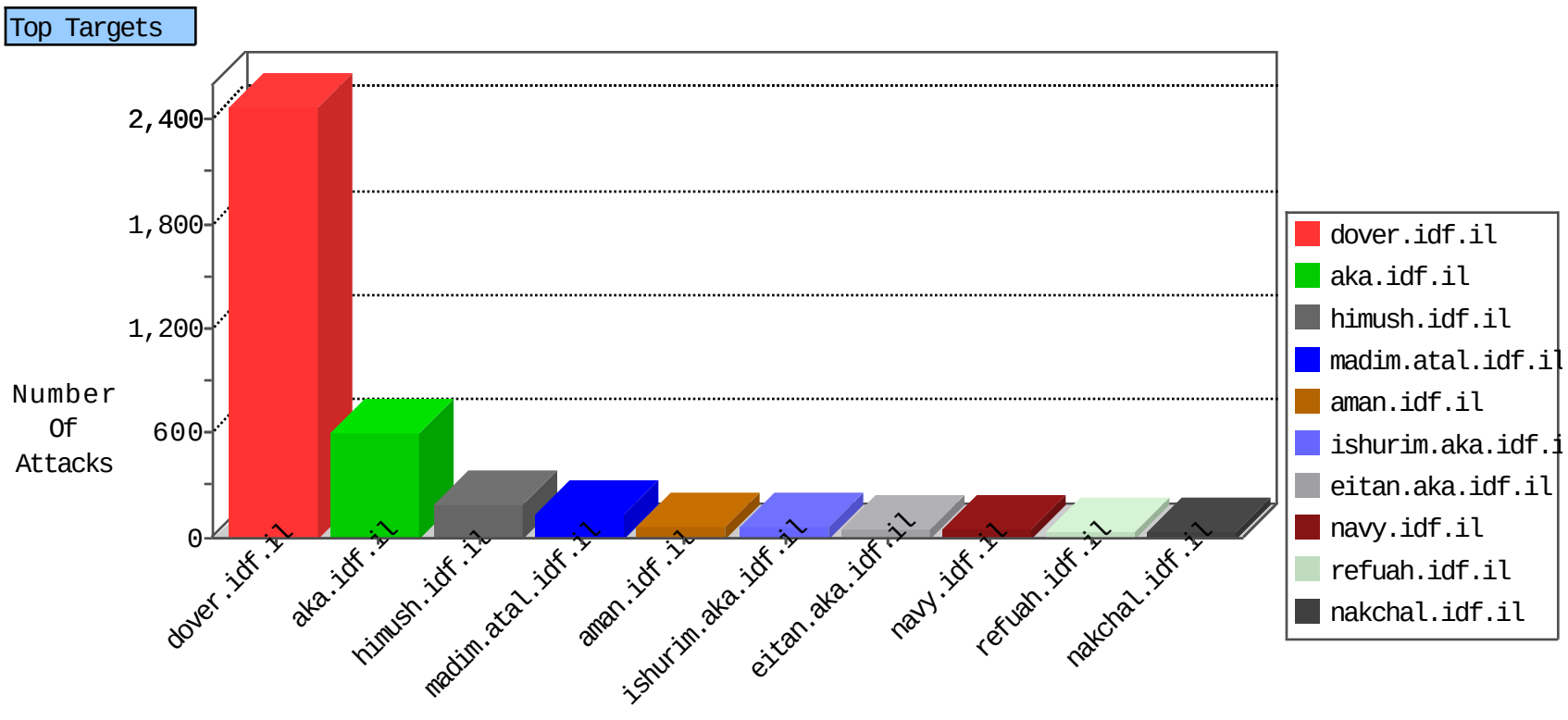
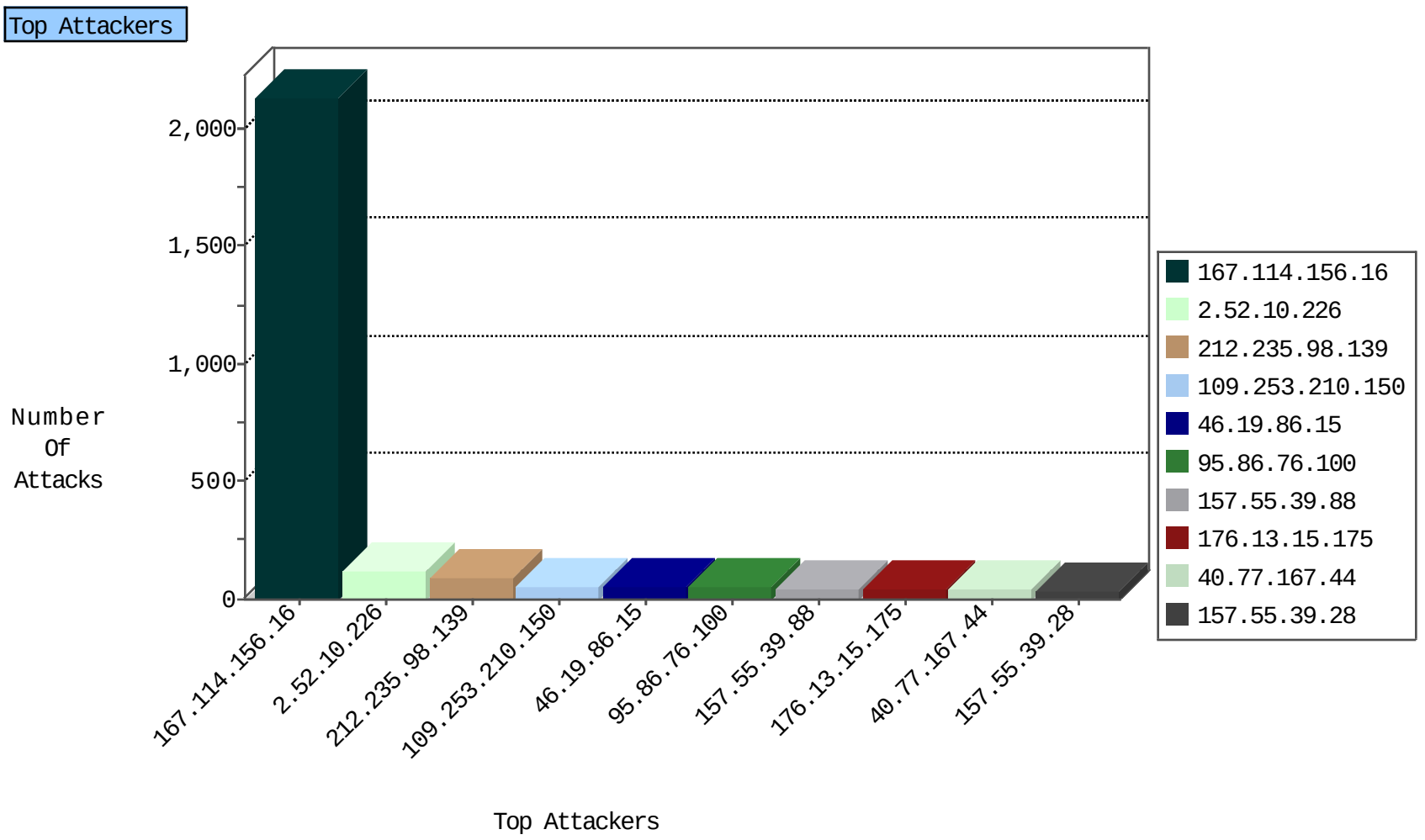
12-16-2015-12:04:05 to 12-16-2015-13:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-16-2015-12:04:05 to 12-16-2015-13:04:05

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	3262
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
188.138.1.218	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
58.148.118.75	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
115.231.222.40	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
31.168.23.187	Israel	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

12-16-2015-12:04:05 to 12-16-2015-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-16-2015-12:04:05 to 12-16-2015-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.116.126.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.157.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.193.252.211	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.202.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.193.252.211	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.156.251.10	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.86.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.124.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.176	Sweden	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.226.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.193.252.211	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
27.206.66.48	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.188.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.131.108.230	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
95.35.156.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
223.4.174.30	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.251.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.219.234.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-16-2015-12:04:05 to 12-16-2015-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.10.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	103
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	86
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.10	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.181.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
107.167.107.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
2.52.189.19	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.86.139	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
81.218.190.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.52.189.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
149.78.108.247	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.85.160	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.64.184.19	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.139	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.86.76.100	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.64.145.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.20.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.216.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.131.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.60	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.169	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.21.73	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.0.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.219.130.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.105.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.139.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.68.55.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.117.125.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.90.209.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4

12-16-2015-12:04:05 to 12-16-2015-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.210.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
157.55.39.88	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	47
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
95.86.76.100	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
40.77.167.44	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	40
157.55.39.28	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	34
207.46.13.95	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	33
2.54.25.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.25.68	Block	19
207.46.13.127	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.127	Block	17
2.54.131.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.219.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
157.55.39.29	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	5
79.180.52.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.46.16	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
176.13.6.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
109.253.197.186	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
5.29.76.50	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
95.134.121.18	Ukraine	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.36	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/×‘ ×‘×‘×?	Block	2
46.118.156.84	Ukraine	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
176.12.150.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.150.42	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
212.25.103.10	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.181.85	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
2.54.23.87	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
95.86.76.100	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	1
62.219.161.153	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
192.114.91.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
86.123.240.150	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
176.13.18.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.157.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.220.241	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$captchaText in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
217.194.207.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
2.54.52.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.131.108.230	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2430.jpg	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
180.76.15.30	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
93.172.141.2	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.150.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.181.107	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.181.181.107	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/10937.jpg	Block	1

12-16-2015-12:04:05 to 12-16-2015-13:04:05