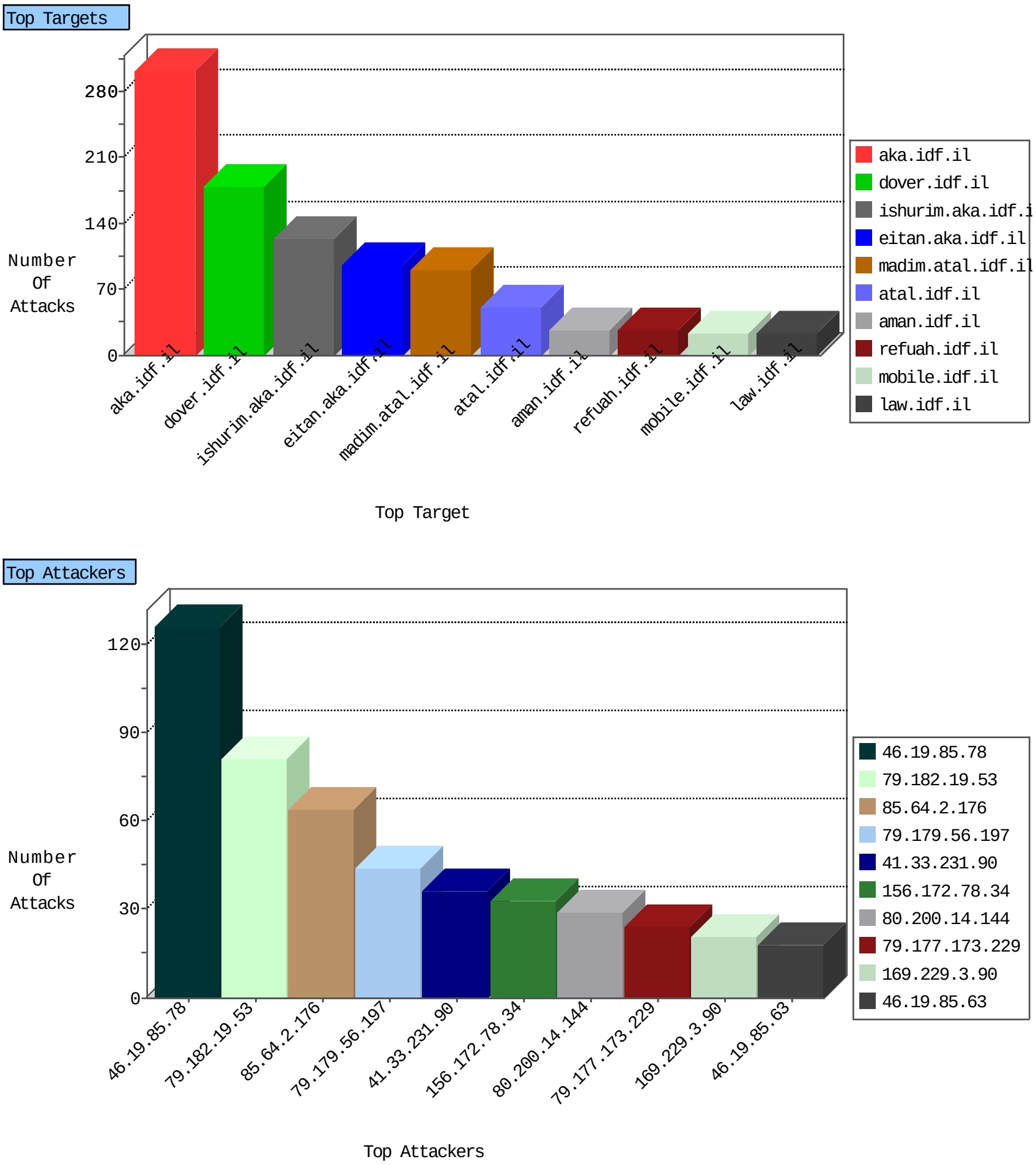
01-09-2016-16:04:05 to 01-09-2016-17:04:05

IDF Under Attack
Daily Report



01-09-2016-16:04:05 to 01-09-2016-17:04:05

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	166
79.182.8.181	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
119.138.90.203	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.213	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
107.150.60.246	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
142.54.160.214	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
27.221.10.43	China	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
107.150.60.246	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
146.185.239.100	Russian Federation	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

01-09-2016-16:04:05 to 01-09-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.140.66.228	Morocco	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
79.180.135.104	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
197.53.73.214	Egypt	147.237.77.216	dover.idf.il	12618: HTTP: WebCruiser Vulnerability Scanner	Block	1

01-09-2016-16:04:05 to 01-09-2016-17:04:05

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	4
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
80.200.14.144	147.237.76.202	Belgium	e.halag.idf.il	ET SCAN Potential SSH Scan	2
80.200.14.144	147.237.76.197	Belgium	e.himush.idf.il	ET SCAN Potential SSH Scan	2
80.200.14.144	147.237.77.216	Belgium	dover.idf.il	ET SCAN Potential SSH Scan	2
80.200.14.144	147.237.77.176	Belgium	matpash.idf.il	ET SCAN Potential SSH Scan	2
80.200.14.144	147.237.77.226	Belgium	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
80.200.14.144	147.237.76.31	Belgium	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.178	Belgium	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.72.156	Belgium	aman.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.74	Belgium	law.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.200.14.144	147.237.76.148	Belgium	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
111.240.208.55	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.200.14.144	147.237.76.86	Belgium	navy.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.243	Belgium	mobile.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.76.39	Belgium	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.233	Belgium	atal.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.76.34	Belgium	yohalan.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.72.166	Belgium	aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.200.14.144	147.237.72.14	Belgium	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.61	Belgium	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.200.14.144	147.237.76.201	Belgium	e.atal.idf.il	ET SCAN Potential SSH Scan	1
175.107.53.212	147.237.76.31	Pakistan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.200.14.144	147.237.76.196	Belgium	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
156.172.78.34	147.237.77.233		atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
80.200.14.144	147.237.76.147	Belgium	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
103.6.223.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.76.44	Belgium	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.77.235	Belgium	sviva.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.76.38	Belgium	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

01-09-2016-16:04:05 to 01-09-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.78	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	108
79.182.19.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
85.64.2.176	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.177.173.229	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
156.172.78.34		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.183.109.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.59.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
128.127.107.108	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
87.69.188.28	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.228.62.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.190.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.181.194	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.238.249.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.14.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
156.172.78.34		147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.15.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.238.249.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.163.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
128.127.107.108	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
156.172.78.34		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
37.142.64.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.29.204.204	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.22.235.120	Spain	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.106.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.120.125.20		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.25.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.129.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.42.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.38.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.31.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.54.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.61.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.177.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.238.249.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.191.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.184.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.138	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.56.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.20.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
77.127.212.168	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 77.127.212.168	Block	12
149.78.40.113	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 149.78.40.113	None	5
2.54.31.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.114.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
84.109.5.191	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
197.53.73.214	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.53.73.214	Block	2
149.78.226.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
46.120.28.27	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
77.127.212.168	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (403) in Session from 77.127.212.168	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
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	2
79.173.219.200	Jordan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
216.18.193.134	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
37.142.64.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
188.121.37.142	Netherlands	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
79.181.219.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.212.168	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/login/greencolumn.jpg"	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3261.jpg	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58562&docid=35709	Block	1
84.228.0.64	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.129.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/favicon.ico	Block	1
79.176.165.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.24	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/additional_content.php	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
109.169.50.31	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/xmlrpc.php	Block	1
73.180.169.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.120.28.27	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation SearchText in www.logistics.atal.idf.il/938-he/halag.aspx	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/tizmoret	None	1
89.138.187.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.183.188.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.18.193.134	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
40.77.167.8	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/×'×™×œ×™ ×•× ×•× ª	Block	1
188.121.37.142	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
77.127.212.168	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per Session	Block	1
197.53.73.214	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/shared/usercontrols/headerupper/	Block	1
149.88.87.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3403.jpg	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/dover.aspx?searchtext=×—×™×œ ×"×ž×•×"×™ ×¢×™×Ÿ	Block	1
85.65.114.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
5.28.180.4	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1