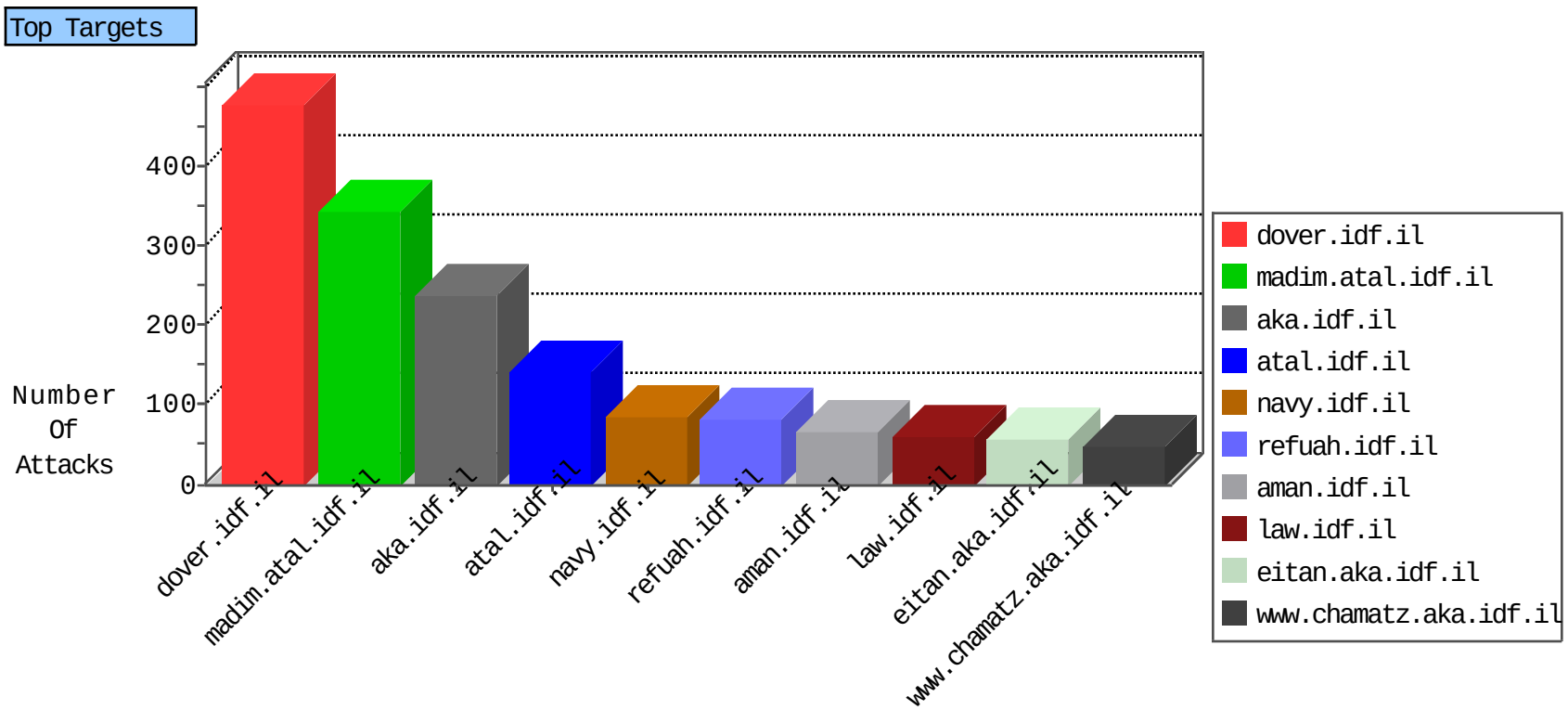
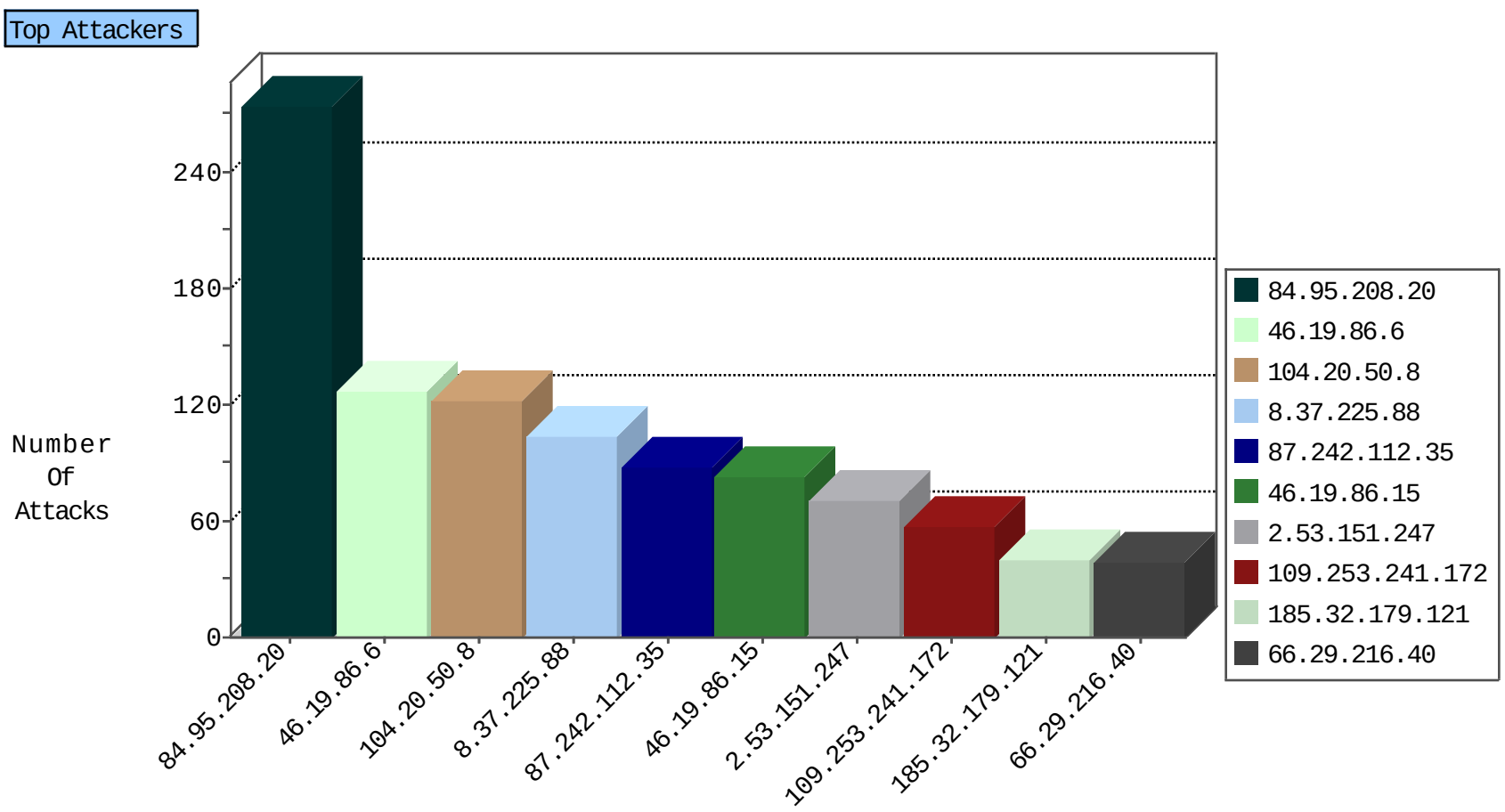
09-09-2016-12:04:09 to 09-09-2016-13:04:09

IDF Under Attack Daily Report





09-09-2016-12:04:09 to 09-09-2016-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.88	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
109.253.198.205	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
204.42.253.2	United States	147.237.76.176	test.ncore.idf.i	Black List	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	2
1.32.192.81	Singapore	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.242.116.60	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-09-2016-12:04:09 to 09-09-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	21
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
97.74.215.165	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
88.208.252.129	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
66.29.216.40	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
88.208.252.129	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
66.29.216.40	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.151.208.90	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.216.40	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.171.93.66	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.74.215.165	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.106.184.160	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.111.194.18	Ukraine	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.74.38.14	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
210.169.203.81	Japan	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1

09-09-2016-12:04:09 to 09-09-2016-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.242.112.35	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	31
66.29.216.40	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
97.74.215.165	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
88.208.252.129	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	20
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	20
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	12
79.177.116.137	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	9
212.111.194.18	147.237.77.74	Ukraine	law.idf.il	SQL Injection - Select From	8
71.171.93.66	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
188.165.250.173	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	8
212.247.61.153	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	8
109.64.86.171	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	6
195.74.38.14	147.237.76.42	Sweden	refuah.idf.il	SQL Injection - Select From	3
69.164.205.7	147.237.77.235	United States	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
201.38.68.132	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.8.27	Jamaica	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
190.232.195.18	147.237.76.30	Peru	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.235.188.61	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.31.42.130	147.237.76.196	France	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
212.247.61.153	147.237.0.34	Sweden	tikshuv.idf.il	SQL Injection - Select From	1
202.134.171.186	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
72.252.24.133	147.237.8.27	Jamaica	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
66.249.66.242	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
176.31.42.130	147.237.76.196	France	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
5.29.162.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1

09-09-2016-12:04:09 to 09-09-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
46.19.86.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
195.74.38.14	Sweden	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	28
8.37.225.88	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
79.180.134.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.253.231.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
81.177.24.40	Russian Federation	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	drop	SAM rule	drop	18
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.85.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.26.146.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.38.129	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
98.19.222.133	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
46.19.85.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
104.20.50.8	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
104.20.50.8	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.205.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.21.187.203	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
104.20.50.8	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
184.168.27.33	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.143.255	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
104.20.50.8	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
213.174.55.11	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
104.20.50.8	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.20.50.8	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.180.236.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
104.20.50.8	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.125.56.126	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
104.20.50.8	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
104.20.50.8	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.159.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

09-09-2016-12:04:09 to 09-09-2016-13:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	133
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	90
2.53.151.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.241.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
185.32.179.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	17
183.11.4.25	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 183.11.4.25	Block	17
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	9
84.108.19.241	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
183.11.4.25	China	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
87.69.113.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.67.124.224	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 109.67.124.224	Block	4
37.26.147.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.138.143.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
88.201.150.238	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
79.181.200.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
124.73.6.250	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-he/idfg.aspx/trackback/	Block	1
68.180.230.56	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx	Block	1
84.108.19.241	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.108.19.241	Block	1
183.11.4.25	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
77.138.229.39	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
104.200.17.117	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 104.200.17.117 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
149.202.59.192	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
69.164.205.7	United States	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
183.11.4.25	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
79.178.7.24	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
109.67.124.224	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Value at 523 for www.aman.idf.il/modiin/questionnaires.aspx	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
71.235.241.119	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
37.26.149.176	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.126.164	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
37.142.228.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/givus	Block	1
79.180.134.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
188.120.154.90	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/displayallsoldiers.asp	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
2.53.59.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
77.138.167.221	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1

09-09-2016-12:04:09 to 09-09-2016-13:04:09