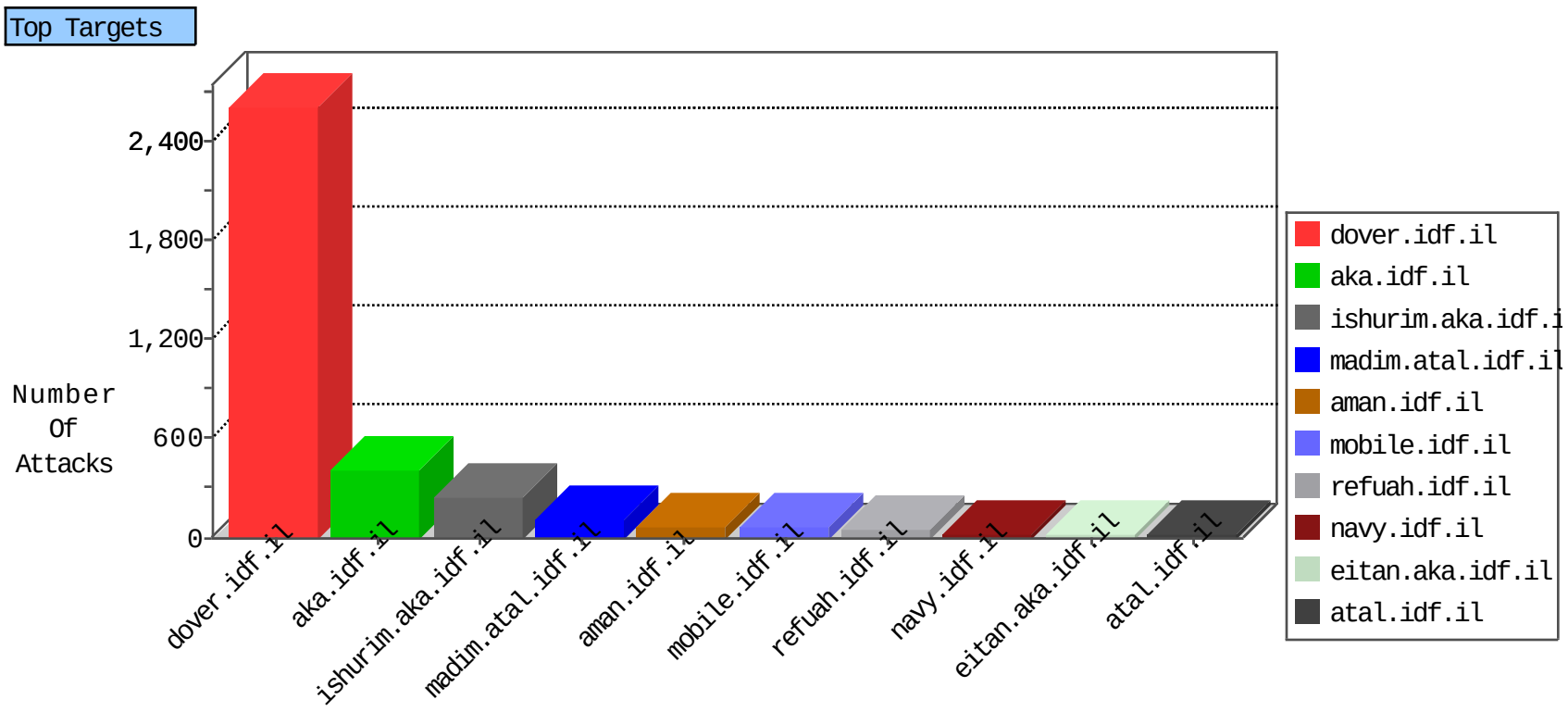
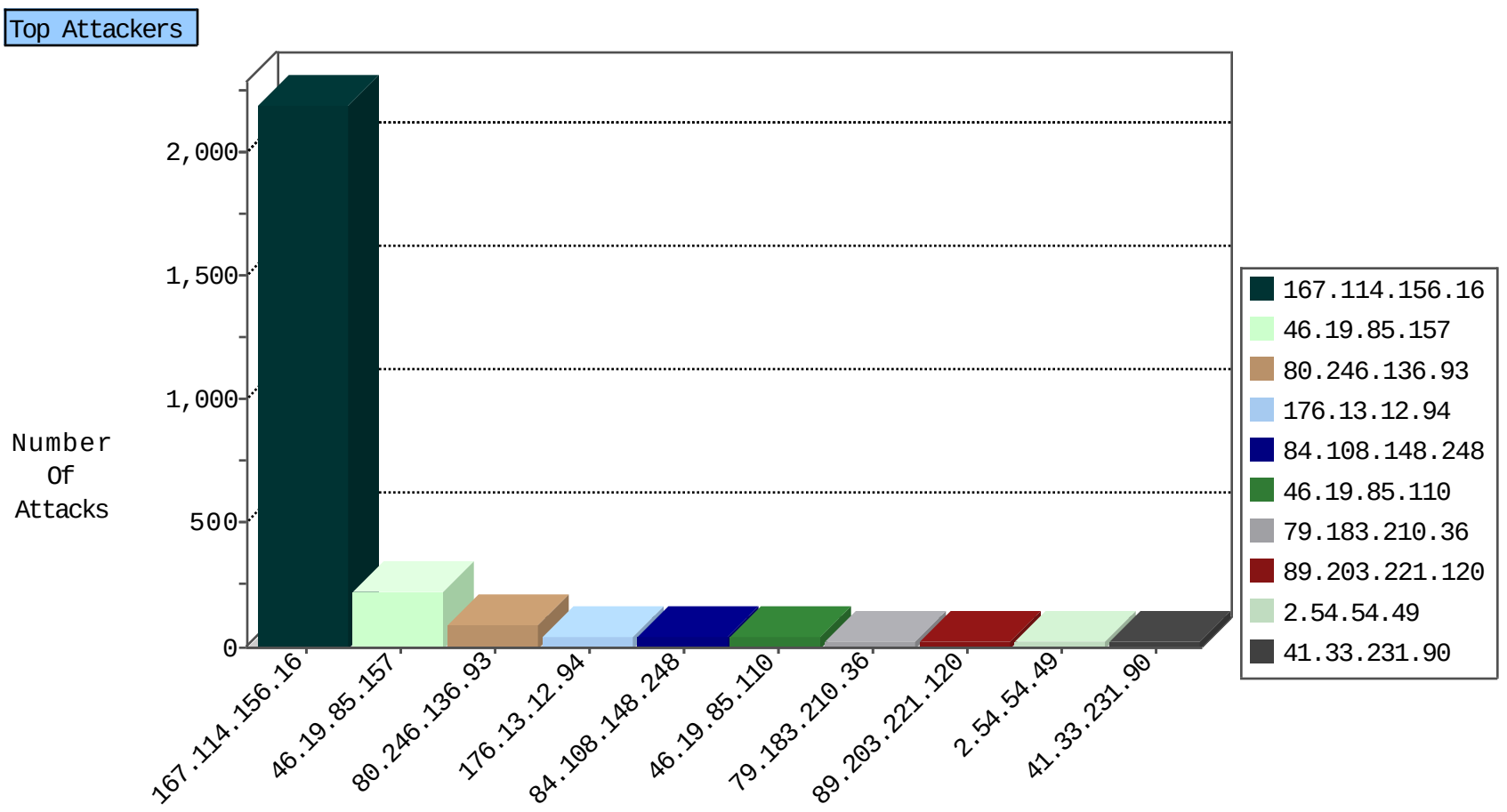
12-20-2015-16:04:09 to 12-20-2015-17:04:09

IDF Under Attack Daily Report





12-20-2015-16:04:09 to 12-20-2015-17:04:09

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	3480
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1673
66.249.64.165	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	745
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
173.206.138.44	Canada	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

12-20-2015-16:04:09 to 12-20-2015-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	18
192.95.55.218	Canada	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2

12-20-2015-16:04:09 to 12-20-2015-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	2
37.143.82.50	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
132.66.201.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.17.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	1
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	1
212.76.99.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.177.7.210	147.237.77.233	Hong Kong	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.254.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.229.182.50	147.237.77.216	Taiwan	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
91.201.236.113	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.94.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.152.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	1
208.80.155.223	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1
46.121.12.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.95.55.218	147.237.77.176	Canada	matpash.idf.il	Tehila - Perl LWP with fake user agent	1

12-20-2015-16:04:09 to 12-20-2015-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.157	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	228
80.246.136.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	32
79.183.210.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.176.135.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
84.108.148.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	17
80.246.136.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
80.246.136.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
80.246.136.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.246.136.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
66.249.81.144	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	13
2.54.165.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
77.125.2.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
213.57.247.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.128.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
116.22.164.238	China	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
108.171.128.165	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.139	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
203.81.85.2	Myanmar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.138.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.54.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
84.108.148.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.146.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.133.45	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.223	Israel	147.237.77.216	dover.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
46.19.86.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.166.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.45.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.22.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.53.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.75.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.39.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.154.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.148.248	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
95.129.32.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.149.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.148.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

12-20-2015-16:04:09 to 12-20-2015-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.54.15.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.130.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.43	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	3
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.43	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	3
84.111.233.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.195.145	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
80.246.136.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.236.8.111	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
79.180.204.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.236.160.57	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.64.26.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
194.90.216.187	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.13.110.96	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1153-22822-he/	Block	1
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 91.228.248.251	Block	1
2.54.55.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.27.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
58.218.213.44	China	147.237.77.216	dover.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 58.218.213.44	None	1
176.13.10.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
79.176.135.160	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
212.76.98.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
176.13.22.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.28.179.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.255.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.117.229.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.139.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.163.114	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.181.102.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.189.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.149.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.149.105	Block	1
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
194.90.216.187	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.63.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.166.17	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
58.218.213.44	China	147.237.77.216	dover.idf.il	Multiple signatures from 58.218.213.44	Block	1
46.19.86.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

12-20-2015-16:04:09 to 12-20-2015-17:04:09