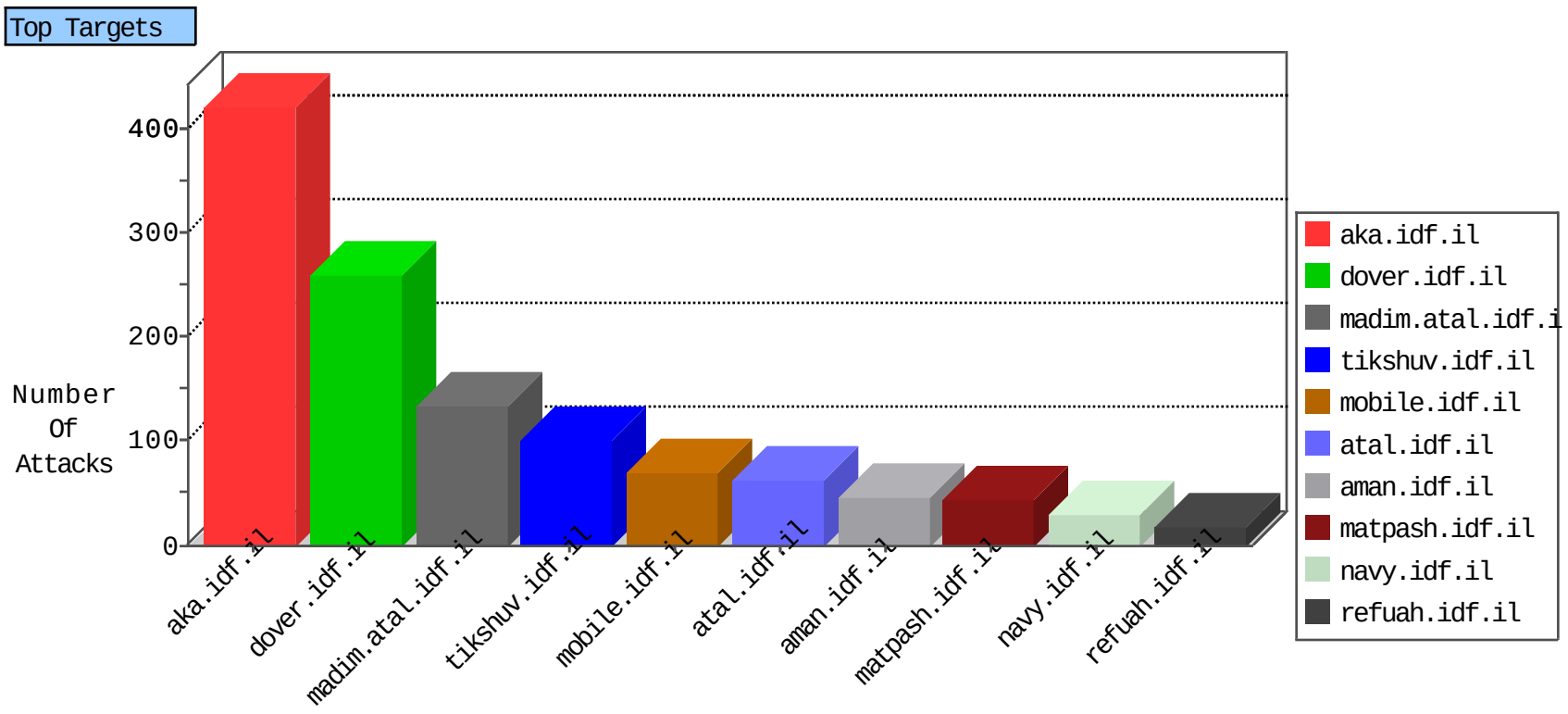
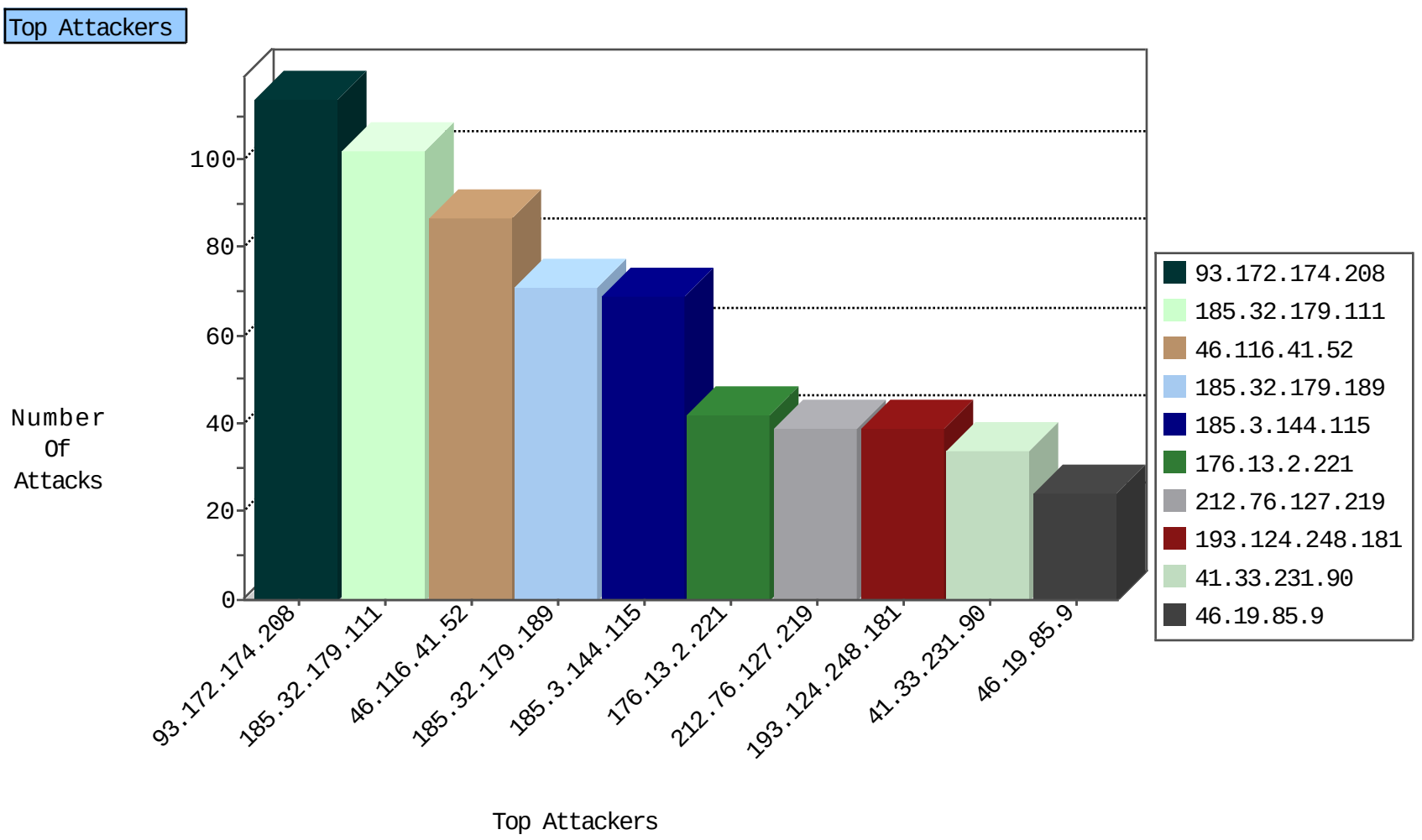
02-11-2016-21:04:06 to 02-11-2016-22:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016-21:04:06 to 02-11-2016-22:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.94.111.1		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.217	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.210	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
46.174.50.30	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-21:04:06 to 02-11-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-11-2016-21:04:06 to 02-11-2016-22:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.151.32.163	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
198.12.82.58	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.106.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.167	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.64.68	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.73.84	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
204.151.15.32	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
198.12.82.58	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
175.6.228.149	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
80.82.79.104	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
204.151.15.32	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

02-11-2016-21:04:06 to 02-11-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.144.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	39
193.124.248.181	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	38
176.13.2.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.32.179.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
141.0.15.1	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
185.32.179.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	18
185.3.144.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	18
185.32.179.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
185.32.179.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
185.32.179.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.32.179.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
176.13.15.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.32.179.189	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	13
185.32.179.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
136.0.98.173	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.30.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.32.179.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.179.236.105	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.32.179.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
173.13.178.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.9	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.126.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.24.207.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.139.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.176.212	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
46.19.85.9	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.188.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.136.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.4.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.197.177	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
185.3.144.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.117.136.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
165.91.12.33	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5

02-11-2016-21:04:06 to 02-11-2016-22:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.174.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
46.116.41.52	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
109.253.213.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
93.172.174.208	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.174.208	Block	14
165.91.12.33	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 165.91.12.33	Block	9
176.13.2.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
84.94.83.115	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.83.115	Block	3
176.13.20.110	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.20.110	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
37.26.149.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
84.109.167.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$22 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
165.91.12.33	United States	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
128.194.135.73	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 128.194.135.73	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dov	Block	1
80.246.139.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.88.209.87	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
84.109.191.229	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.109.191.229	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
128.194.135.73	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name User-agent	Block	1
212.76.124.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21154-he/dover.aspx&sa=u&ved=0ahukewibpvwxv_dkahxe1xokhahaaz84chawcbqwba&sig2=-xolm2_b77t9s3rc2u_ktq&usg=afqjcnhlkv_l1tggamhwnwq3kiazg_bhpa	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
128.93.90.1	France	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 128.93.90.1 (Unsupported Cipher)	None	1
85.95.254.184	Turkey	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.160	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
128.194.135.73	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 128.194.135.73	Block	1
5.22.131.8	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
104.236.76.230		147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
213.57.105.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.94.83.115	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
46.116.51.253	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
165.91.12.33	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
128.93.90.1	France	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
86.127.177.35	Romania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
176.13.20.110	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
142.54.160.210	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.1916wh.com/	Block	1
105.154.151.209	Morocco	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.94.83.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	1
213.151.50.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
128.194.135.73	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name User-agent	Block	1
86.127.177.35	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
188.230.88.25	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	1
79.179.177.213	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1408-he/atal.aspx	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
149.78.253.183	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
105.154.151.209	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1

02-11-2016-21:04:06 to 02-11-2016-22:04:06