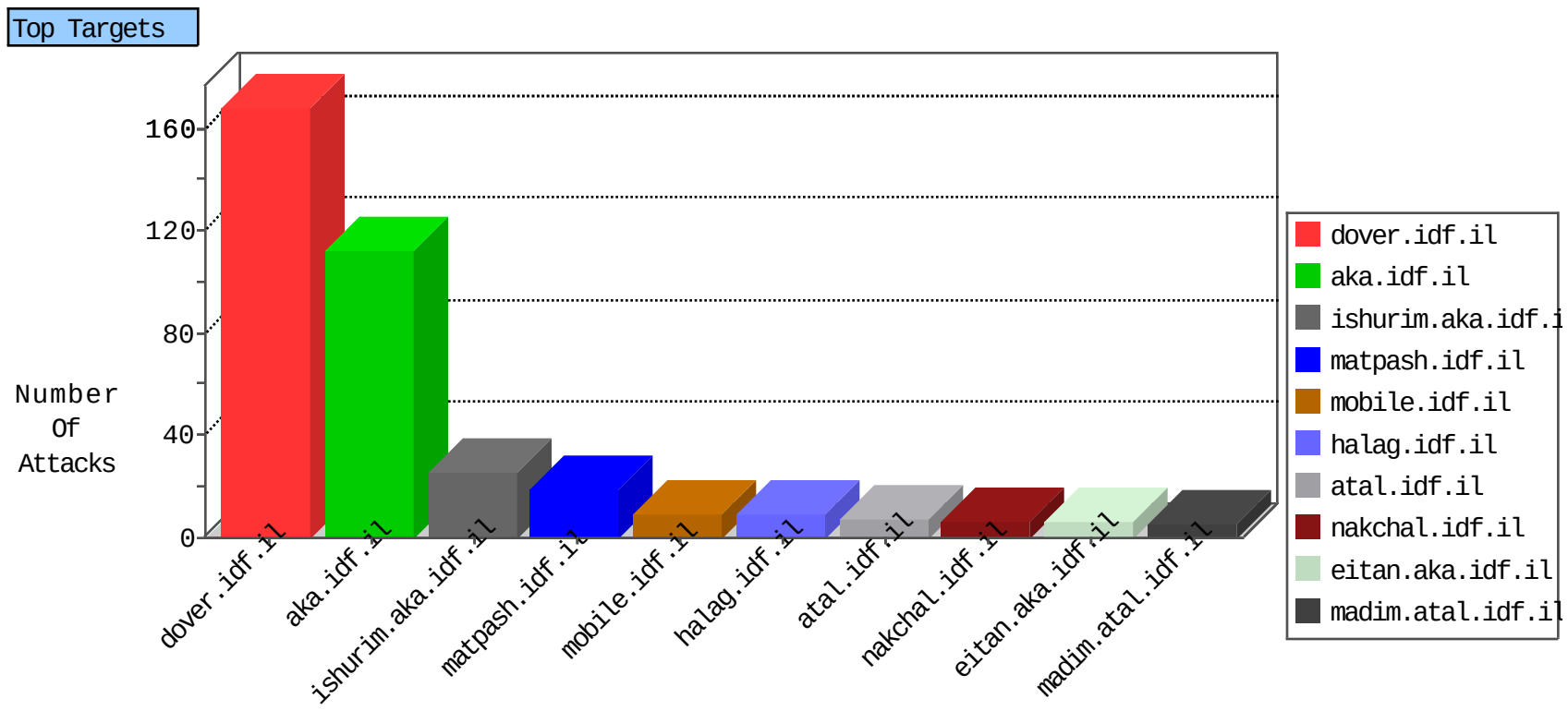
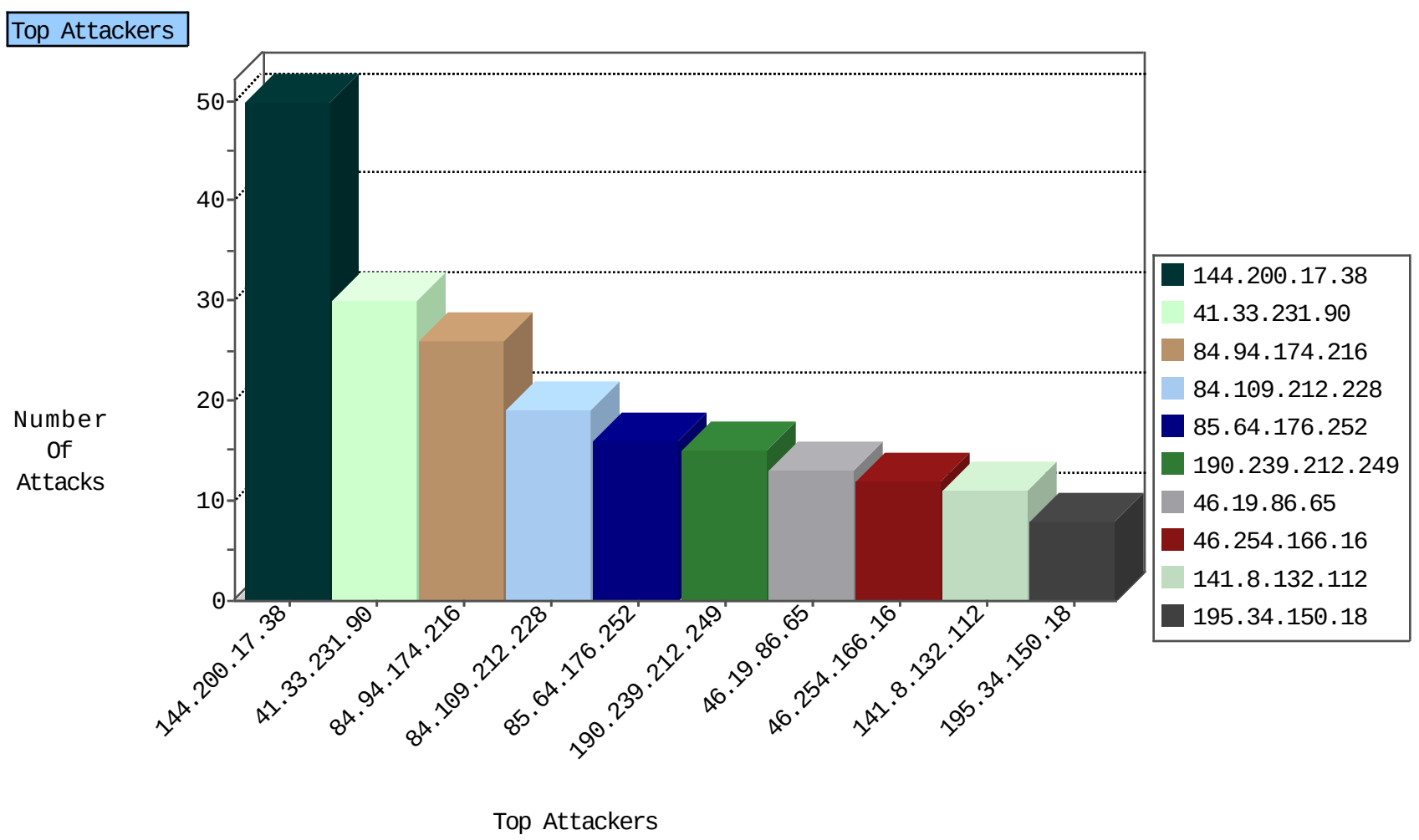
02-16-2016-01:07:30 to 02-16-2016-02:07:30

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-16-2016-01:07:30 to 02-16-2016-02:07:30

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-01:07:30 to 02-16-2016-02:07:30

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.44	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.90	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-16-2016-01:07:30 to 02-16-2016-02:07:30

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
121.141.225.10	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.114.146.155	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
59.96.186.128	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.141.225.10	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.60.36.203	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.114.109.141	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
121.141.225.10	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-16-2016-01:07:30 to 02-16-2016-02:07:30

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
144.200.17.38	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
85.64.176.252	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.94.174.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.147.120	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
84.94.174.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.109.212.228	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	6
84.94.174.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.94.174.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
104.34.95.103	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.187.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.35.60.197	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.212.228	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.194	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.85	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.2.128	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.109.212.228	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.154.160.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.212.228	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.254.2.244	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.212.228	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
38.81.65.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
97.75.150.206	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
144.200.17.38	Switzerland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.68.16.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
88.1.103.95	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.230.17.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
144.200.17.38	Switzerland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.154.189.15	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.215	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.1.101.123	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
190.239.212.249	Peru	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	7
46.254.166.16	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
190.239.212.249	Peru	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 190.239.212.249	Block	6
46.254.166.16	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.254.166.16	Block	5
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	5
176.205.65.186	United Arab Emirates	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
176.205.65.186	United Arab Emirates	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	3
186.56.87.194	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
188.120.148.221	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
157.55.39.95	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
88.1.103.95	Spain	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main/	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method : in URL asp.net_sessionid=au5z4q45lv0i2k2oameai1qr	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.25.148.240	Poland	147.237.77.235	sviva.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
104.236.104.128		147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20477-he/dover.aspx	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Malformed URL asp.net_sessionid=au5z4q45lv0i2k2oameai1qr	Block	1
190.239.212.249	Peru	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
157.55.39.234	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
14.139.227.147	India	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
41.207.3.138	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
185.49.14.190	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
104.236.107.34		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.160	Block	1
14.139.227.147	India	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
104.131.182.54	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
41.207.3.138	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
185.49.14.190	Poland	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
104.236.110.34		147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
79.178.55.248	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.160	Block	1
23.106.244.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
104.236.92.149		147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
46.254.166.16	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
104.236.111.245		147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
79.178.55.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
190.239.212.249	Peru	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/phpmoadmin/moadmin.php	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.160	Block	1
185.25.148.240	Poland	147.237.77.234	halag.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
37.187.114.171	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /sap/hana/admin/	Block	1
104.236.93.11		147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1