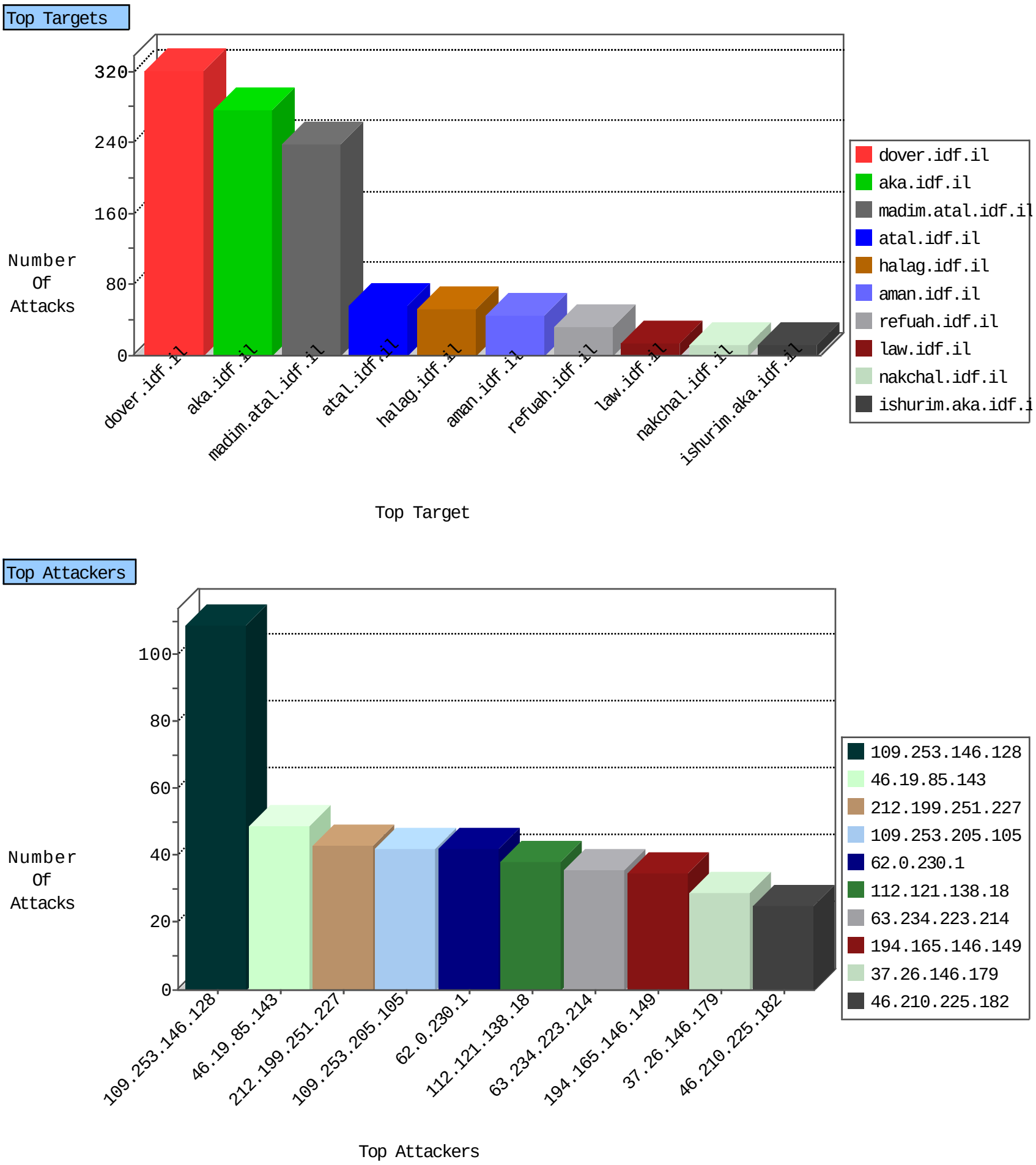
09-22-2016-10:04:04 to 09-22-2016-11:04:04

IDF Under Attack
Daily Report



09-22-2016-10:04:04 to 09-22-2016-11:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.225.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
157.55.39.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.143.211.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.180.94.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
207.46.13.63	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.65.102.161	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

09-22-2016-10:04:04 to 09-22-2016-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
123.126.68.99	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-22-2016-10:04:04 to 09-22-2016-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.70.50.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
82.205.58.131	147.237.77.226	Palestinian Territory, Occupied	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
31.154.25.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.177.168.117	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.61.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.5.109.236	147.237.76.148	Indonesia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.1.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.16.127.148	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.253.140.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.16.127.148	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
79.180.69.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.110.132.201	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
37.46.39.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.19.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.31.41.199	147.237.0.33	Vietnam	idf.il	ET SCAN NMAP -sS window 1024	1
199.203.92.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.186.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.16.127.148	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.64.58.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.239.108.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
79.178.229.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.116.219.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.72.166	Ukraine	aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-10:04:04 to 09-22-2016-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.251.227	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	39
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
46.19.85.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
62.0.197.85	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	21
112.121.138.18	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
112.121.138.18	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
63.234.223.214	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
62.0.207.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
63.234.223.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
63.234.223.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
148.177.168.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.18.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
85.130.132.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
162.243.253.50	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
2.55.182.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.48	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.230.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.3.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.138	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.185.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.182.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.146.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
109.253.220.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.138	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.231.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.237	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.201.233.140	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.0.200.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.146.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.55.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.0.202.1	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4

09-22-2016-10:04:04 to 09-22-2016-11:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.146.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
109.253.205.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.148.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.205.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.253.159.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.154.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.130.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.137.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
148.177.168.117	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
109.253.240.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.67.168	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.67.168	Block	2
109.65.90.205	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.198.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.129.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
194.177.16.3	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 194.177.16.3	Block	1
79.178.181.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.181.75	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.248.198.216	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/blogs/wp-login.php	Block	1
85.199.244.27	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method Ë°Iÿ4O¶[[#0]]a“þ–[[#6]][[#28]]„[[#2]]†ŒSG®TÞÈŽ$™[[#27]]¬g*ÔI´[[#5]]1¾-]§ÝF in URL	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.132.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/piwik.php	Block	1
2.53.26.141	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
194.177.16.3	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	1
79.178.181.75	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method Ë°Iÿ4O¶[[#0]]a“þ–[[#6]][[#28]]„[[#2]]†ŒSG®TÞÈŽ$™[[#27]]¬g*ÔI´[[#5]]1¾-]§ÝF	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	1
89.138.115.160	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.53.173.154	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
77.138.140.197	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
148.177.168.117	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
212.199.251.227	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.182.86.61	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Malformed URL	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
31.154.81.72	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
91.221.145.225	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
81.240.114.149	Belgium	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
148.177.168.117	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

09-22-2016-10:04:04 to 09-22-2016-11:04:04