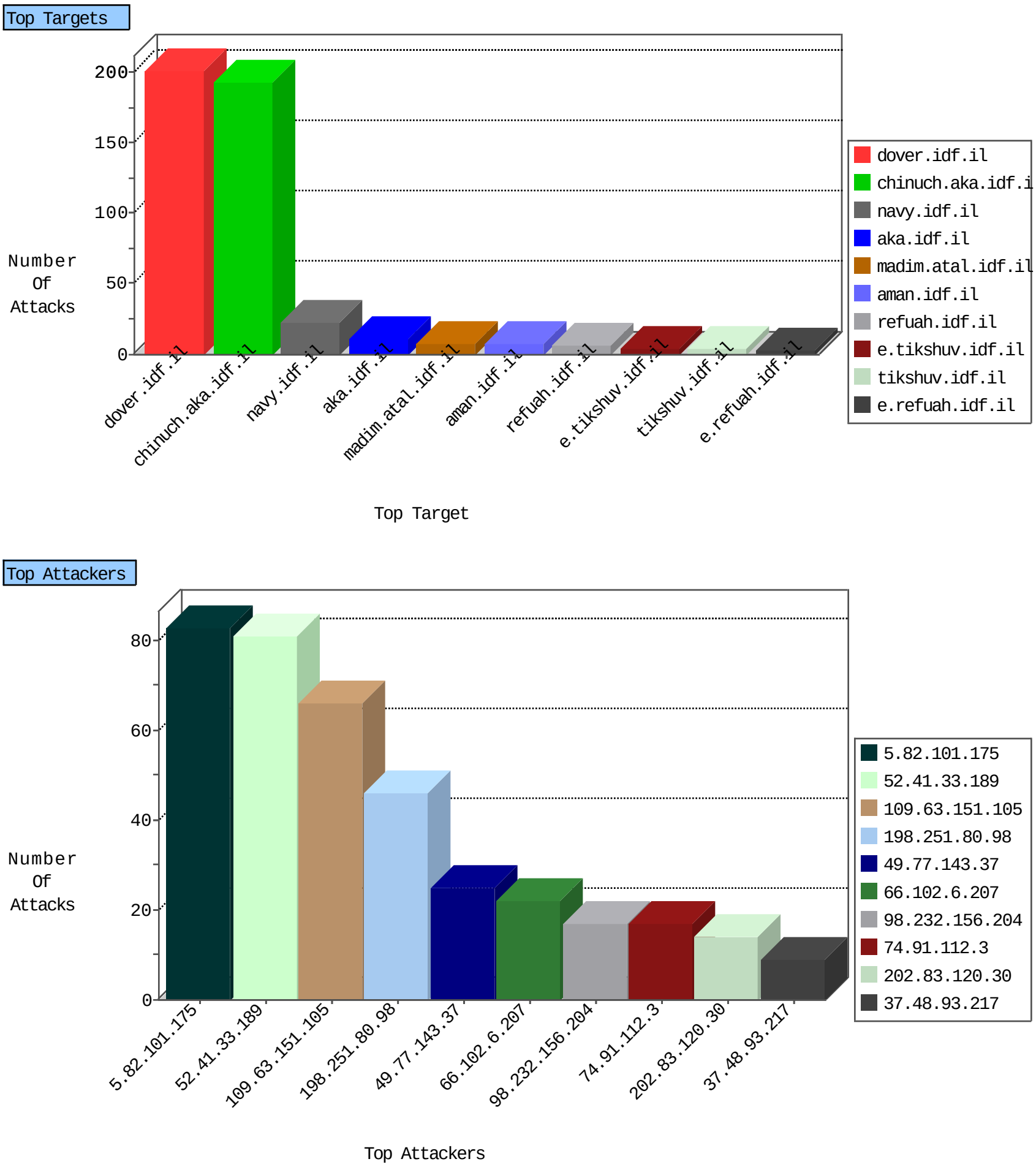
09-27-2016-04:04:06 to 09-27-2016-05:04:06

IDF Under Attack
Daily Report



09-27-2016-04:04:06 to 09-27-2016-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.200.182	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
45.32.204.130	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
45.32.205.113	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
45.32.200.117	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
93.158.200.70	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-27-2016-04:04:06 to 09-27-2016-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.211.51.34	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

09-27-2016-04:04:06 to 09-27-2016-05:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.6.207	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	22
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
161.106.88.6	147.237.72.217	France	e.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
218.56.33.73	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.106.88.6	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
218.56.33.73	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
156.211.51.34	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
218.56.33.73	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.48.93.217	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
189.238.140.131	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
37.48.93.217	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.238.140.131	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.102.6.31	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
179.43.144.18	147.237.77.205	Switzerland	prisha.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
161.106.88.6	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
218.56.33.73	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
156.211.51.34	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	1
218.56.33.73	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.48.93.217	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
149.255.108.192	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.56.33.73	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.48.93.217	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
189.238.140.131	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.107.113.255	147.237.76.202	Hungary	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-27-2016-04:04:06 to 09-27-2016-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.82.101.175	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
109.63.151.105	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
98.232.156.204	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
162.198.203.158	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	8
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
66.249.76.67	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.67.200.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
198.211.123.189	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
49.77.143.37	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack		monitor	2
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
141.212.122.164	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.102	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.26.117.126	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.251.69.10	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.87.114.184	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
156.211.51.34	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.189.190.238	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
70.26.117.126	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
109.253.159.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.87.114.184	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
5.189.190.238	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
75.1.211.226	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.41.33.189	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1

09-27-2016-04:04:06 to 09-27-2016-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.77.143.37	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 49.77.143.37	Block	16
49.77.143.37	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
197.38.176.231	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	3
157.55.39.18	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	3
217.66.152.101	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	3
217.66.152.101	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1399-en/dover.aspx	Block	2
180.76.15.148	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9712-he/refuah.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8911-he/refuah.aspx	Block	1
70.199.194.66	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/klali/default.asp	Block	1
49.77.143.37	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8859-he/refuah.aspx	Block	1
144.75.175.204	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/chinuch/klali/default.asp	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.56	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.56	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
207.46.13.56	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/aman	Block	1
68.180.229.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headeruppe r/	Block	1
157.55.39.186	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.89	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
68.180.229.184	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1

09-27-2016-04:04:06 to 09-27-2016-05:04:06