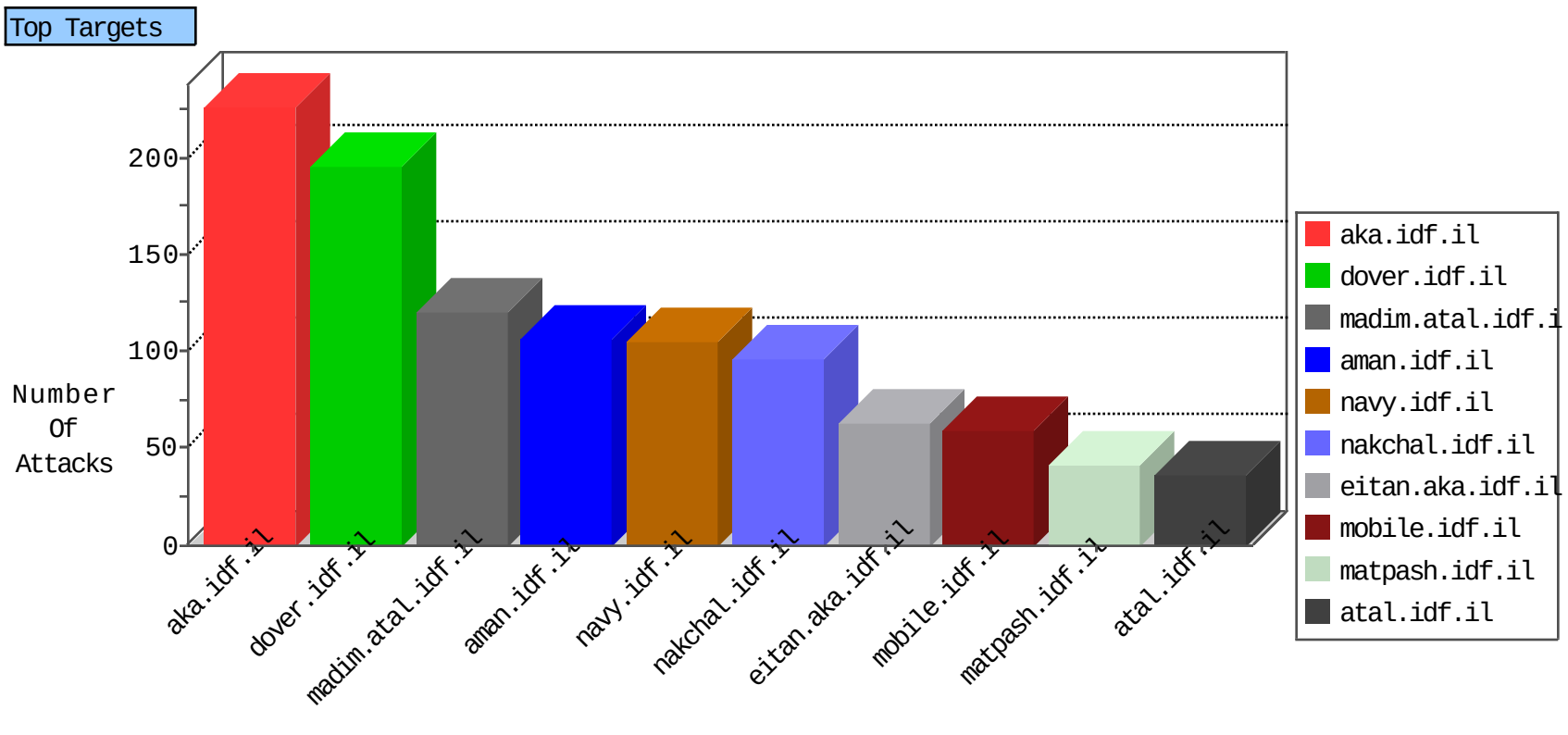
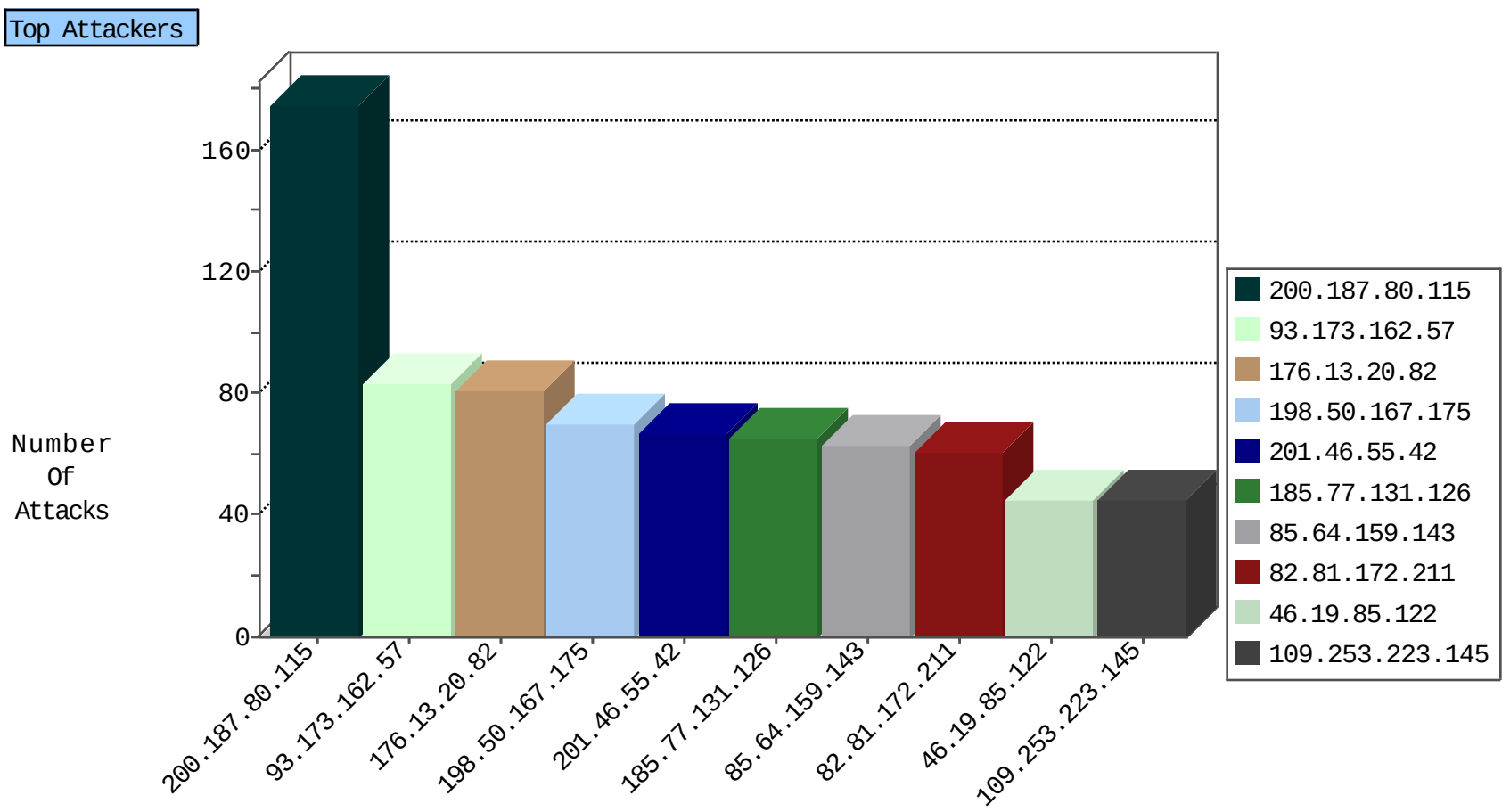
09-10-2016-22:04:00 to 09-10-2016-23:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-10-2016-22:04:00 to 09-10-2016-23:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
201.55.179.62	Brazil	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
201.55.179.62	Brazil	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
201.55.179.62	Brazil	147.237.77.234	halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-10-2016-22:04:00 to 09-10-2016-23:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
209.58.178.49	Singapore	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
209.58.178.49	Singapore	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-10-2016-22:04:00 to 09-10-2016-23:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.129.15	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.129.15	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
139.162.225.219	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
106.38.241.105	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
23.239.31.132	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.130.189.4	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
212.116.72.226	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.90.133	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
176.58.124.35	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.129.15	147.237.76.148	United Kingdom	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.129.15	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
139.162.160.132	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.201.236.50	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
46.227.67.158	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
23.92.20.154	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.177.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.141.78.56	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.153	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
198.58.110.199	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-10-2016-22:04:00 to 09-10-2016-23:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.162.57	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	79
109.253.223.145	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
185.77.131.126	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
85.64.159.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	26
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
82.81.172.211	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
185.77.131.126	Netherlands	147.237.76.86	navy.idf.il	SYN Attack		monitor	23
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
82.81.172.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.121.82.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
185.77.131.126	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
85.64.159.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
82.81.172.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
85.64.159.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
5.102.253.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.142.3.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.253.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
85.64.159.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
5.102.242.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
200.187.80.115	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
200.187.80.115	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.102.242.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
200.187.80.115	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
200.187.80.115	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
200.187.80.115	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
200.187.80.115	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
200.187.80.115	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
200.187.80.115	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
200.187.80.115	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.156	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
200.187.80.115	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
87.69.49.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
139.162.13.205	Singapore	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
5.29.213.139	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
200.187.80.115	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.156	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
46.19.86.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.69.49.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
200.187.80.115	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
200.187.80.115	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.65.17.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
200.187.80.115	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.250.161.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
109.67.202.86	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

09-10-2016-22:04:00 to 09-10-2016-23:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
113.89.233.68	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.89.233.68	Block	17
213.151.35.221	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/maslulimlist.aspx	Block	6
113.89.233.68	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
62.219.98.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.98.127	Block	5
79.178.97.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.151.55.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/sitemap.aspx	Block	3
89.138.170.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.105.225	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	3
79.179.141.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.147.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.0	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$FAQListViewTemplate1$InternalSearch1$ txtFreeTextSearch in www.law.idf.il/1133-he/patzar.aspx	Block	2
109.253.221.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.151.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.133.190.10	Ukraine	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
183.160.251.14	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-12634-en/dover.aspx/trackback/	Block	1
66.102.9.6	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
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
113.89.233.68	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
95.86.71.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx[	Block	1
77.139.56.203	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
213.151.35.221	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.221	Block	1
159.203.78.72	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
5.165.244.144	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
79.181.249.107	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
207.46.13.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17968-he/dover.aspx<span style='font-family:tahoma	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Dover.aspx in URL	Block	1
128.68.41.50	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
106.38.241.105	China	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
62.219.98.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleToGo in www.aka.idf.il/main/giyus/login.aspx	None	1
31.154.3.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.102.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.81	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1
207.46.13.135	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
46.121.212.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
130.0.62.180	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
108.0.219.147	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.2.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
62.219.98.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleToGoT in www.aka.idf.il/main/giyus/login.aspx	None	1
37.142.3.104	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.73.128	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
212.76.122.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.121.252.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.111	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
109.67.202.86	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
183.160.115.35	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-he/idfg.aspx/trackback/	Block	1
62.219.155.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-10-2016-22:04:00 to 09-10-2016-23:04:00