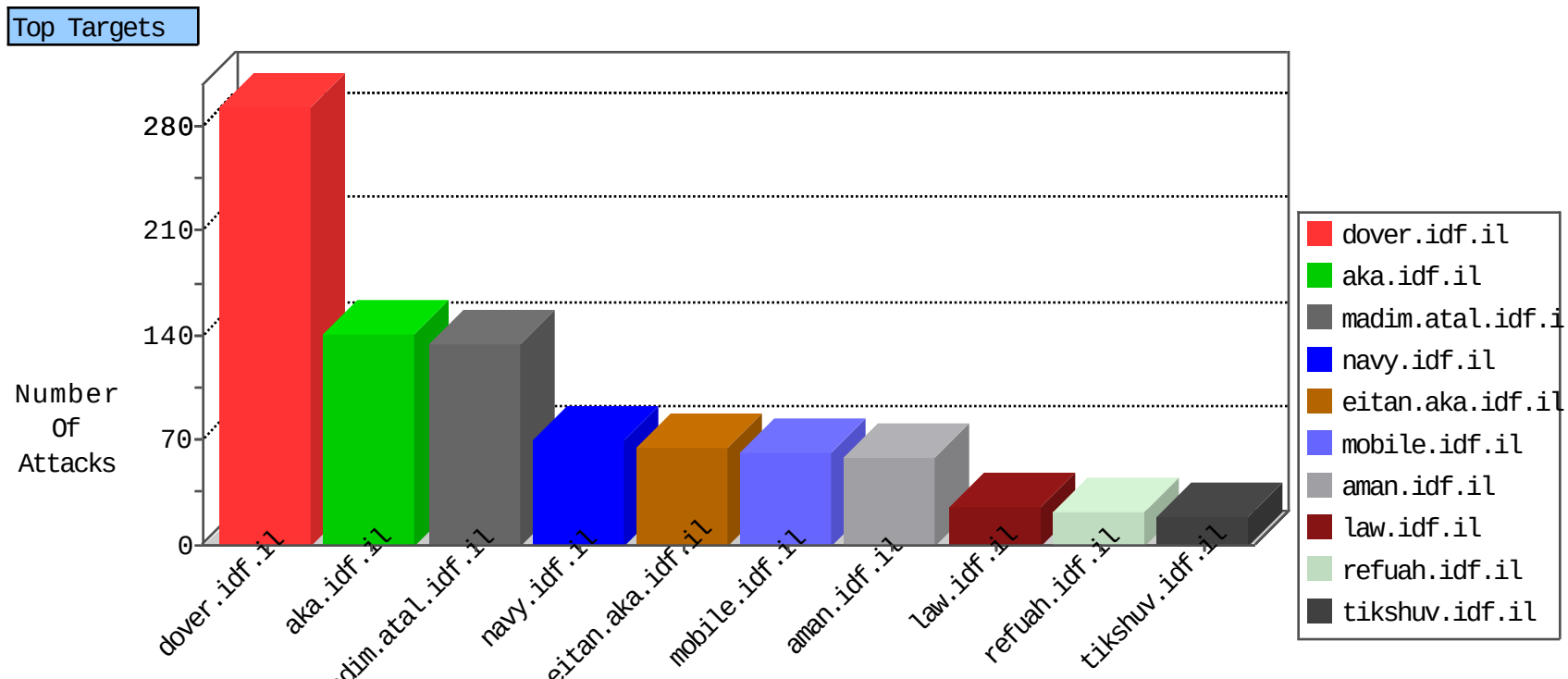
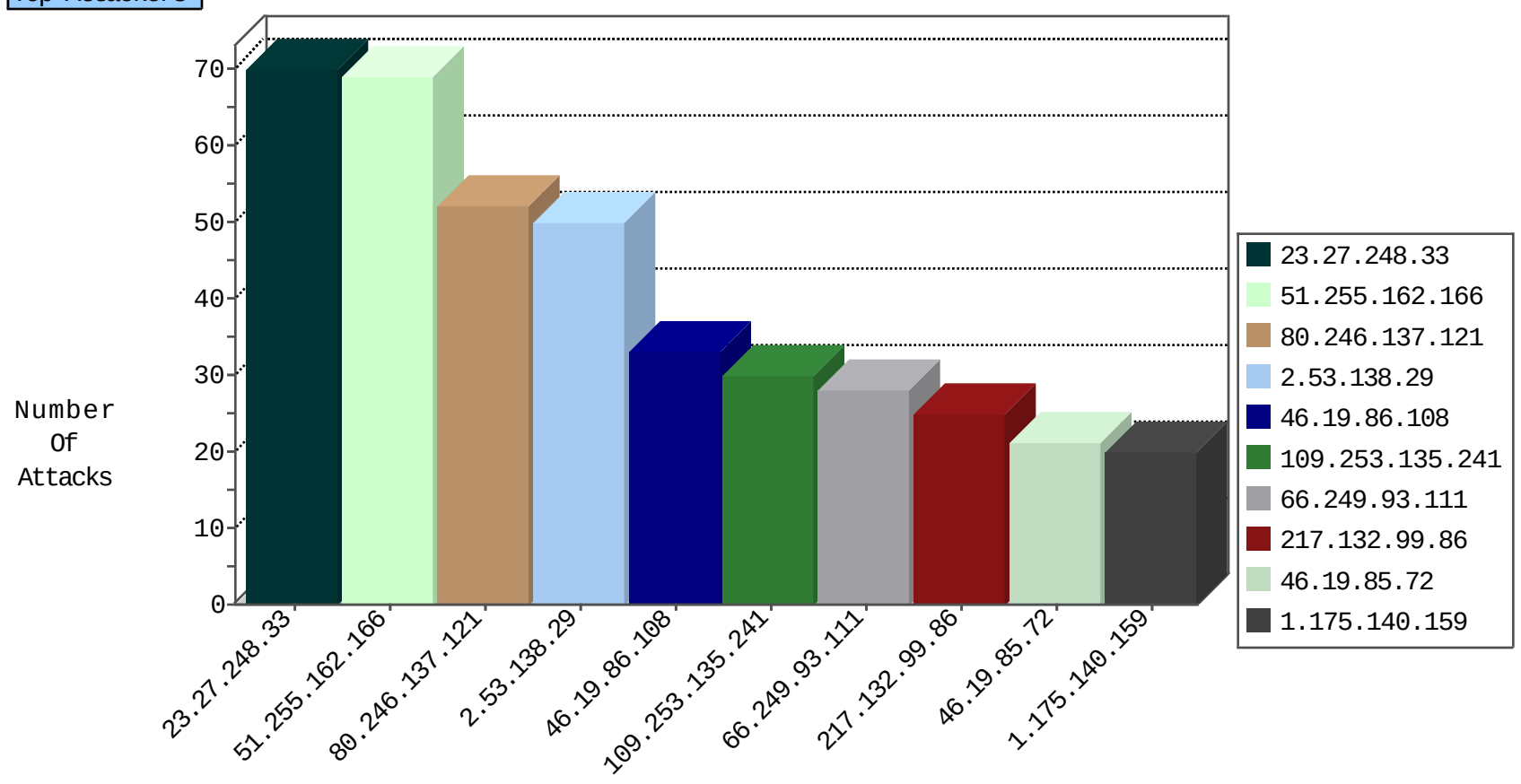
09-04-2016-16:04:02 to 09-04-2016-17:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-16:04:02 to 09-04-2016-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
38.229.1.13	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.176	matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-04-2016-16:04:02 to 09-04-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.162.166	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	40
51.255.162.166	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
51.255.162.166	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
51.255.162.166	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
197.35.68.128	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
198.134.125.78	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
41.187.94.250	Egypt	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
89.138.185.186	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
148.163.73.86	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
198.20.87.98	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-04-2016-16:04:02 to 09-04-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.35.68.128	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	4
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
197.35.68.128	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
91.121.78.198	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
104.197.206.193	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
50.116.123.135	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.87.191.219	147.237.76.34	Taiwan	yohalan.idf.il	ET SCAN Potential SSH Scan	1
87.71.52.226	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
12.68.215.78	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
218.161.112.80	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.70.45.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.120.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.105.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.167.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.100.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.139.216.38	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
193.251.4.99	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.50.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.197.206.193	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
62.128.48.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.87.191.219	147.237.76.148	Taiwan	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.139.127.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.87.191.219	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Potential SSH Scan	1
87.71.19.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.206.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.6.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.222.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.88.157.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.108.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.58.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.56.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.16.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.252.120.115	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
77.124.9.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-04-2016-16:04:02 to 09-04-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
23.27.248.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.135.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
46.19.86.201	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	20
37.142.10.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
46.19.86.108	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
93.104.215.125	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.108	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.43	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
197.35.68.128	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
217.132.21.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.55.59.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
213.8.204.28	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
95.35.133.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.121.12.93	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
81.218.106.146	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
82.81.46.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.229.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
1.175.140.159	Taiwan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.229.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.54.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.245.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.90.215.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.81.46.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
89.138.98.117	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
1.175.140.159	Taiwan	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
100.92.20.194		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
1.175.140.159	Taiwan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
194.9.252.237	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
80.246.133.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.243.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.179.215.221	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.121.12.93	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.245.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.153	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.243.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.123	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
109.253.245.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
193.251.4.99	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-04-2016-16:04:02 to 09-04-2016-17:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.53.138.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.135.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
80.246.139.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
98.223.23.29	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 98.223.23.29	Block	5
2.53.52.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.146.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.227.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.88.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.46.137.18	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
77.139.203.85	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
37.26.147.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.126.123	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
5.22.134.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	2
212.179.247.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.88.144	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.149.230	Block	2
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
31.174.238.232	Poland	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.182.37.139	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מא ירָ שחמו|.aspx	Block	1
176.13.234.11	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.117.152.114	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.152.114	Block	1
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
77.125.52.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl54.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
66.249.66.241	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.253.141.27	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
212.143.90.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/console/core/doc_mgr/tel:03-7379500	Block	1
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version deflate	Block	1
157.55.39.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16782-en/dover.a spx	Block	1
66.249.88.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
66.102.9.2	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
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	Distributed Illegal HTTP Version	Block	1
79.181.3.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.111	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
84.108.70.15	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1

09-04-2016-16:04:02 to 09-04-2016-17:04:02