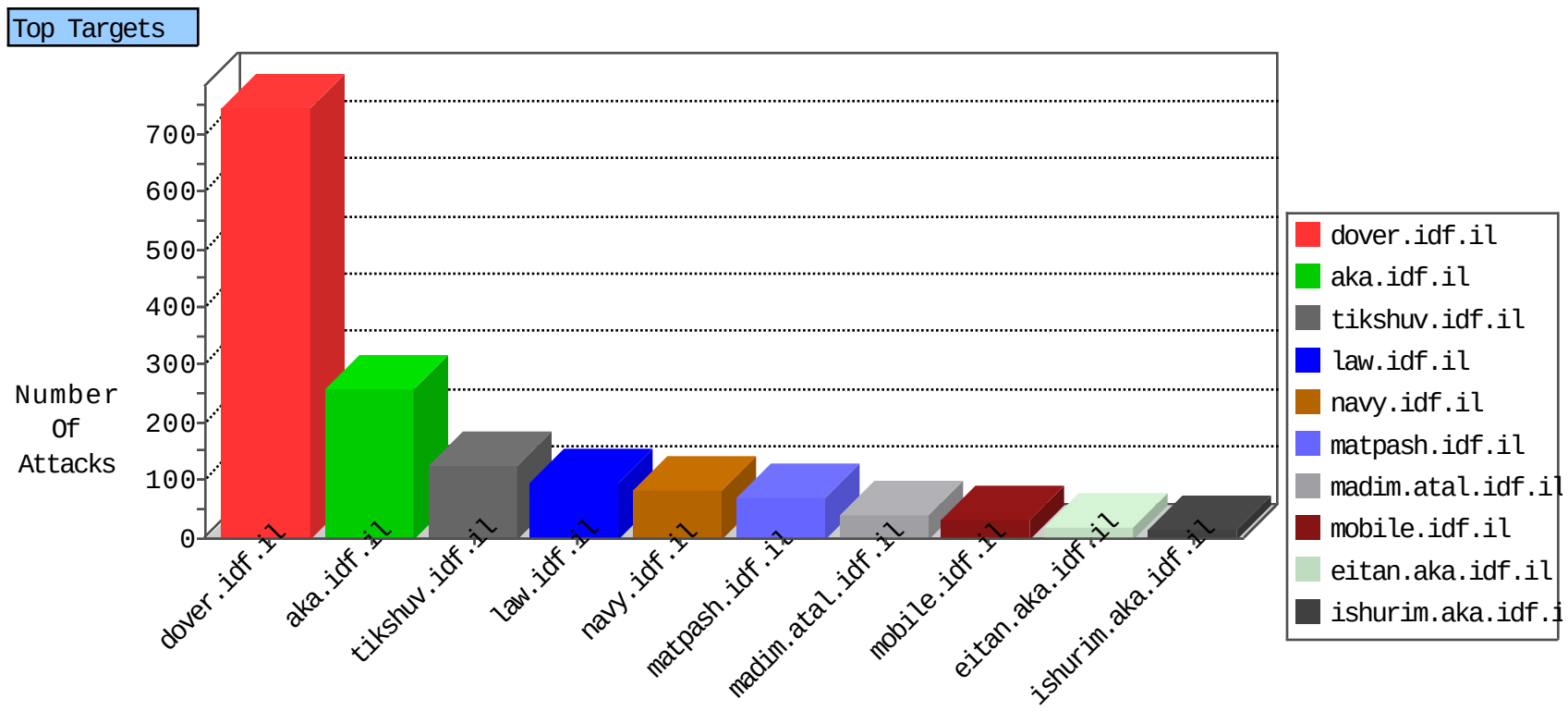
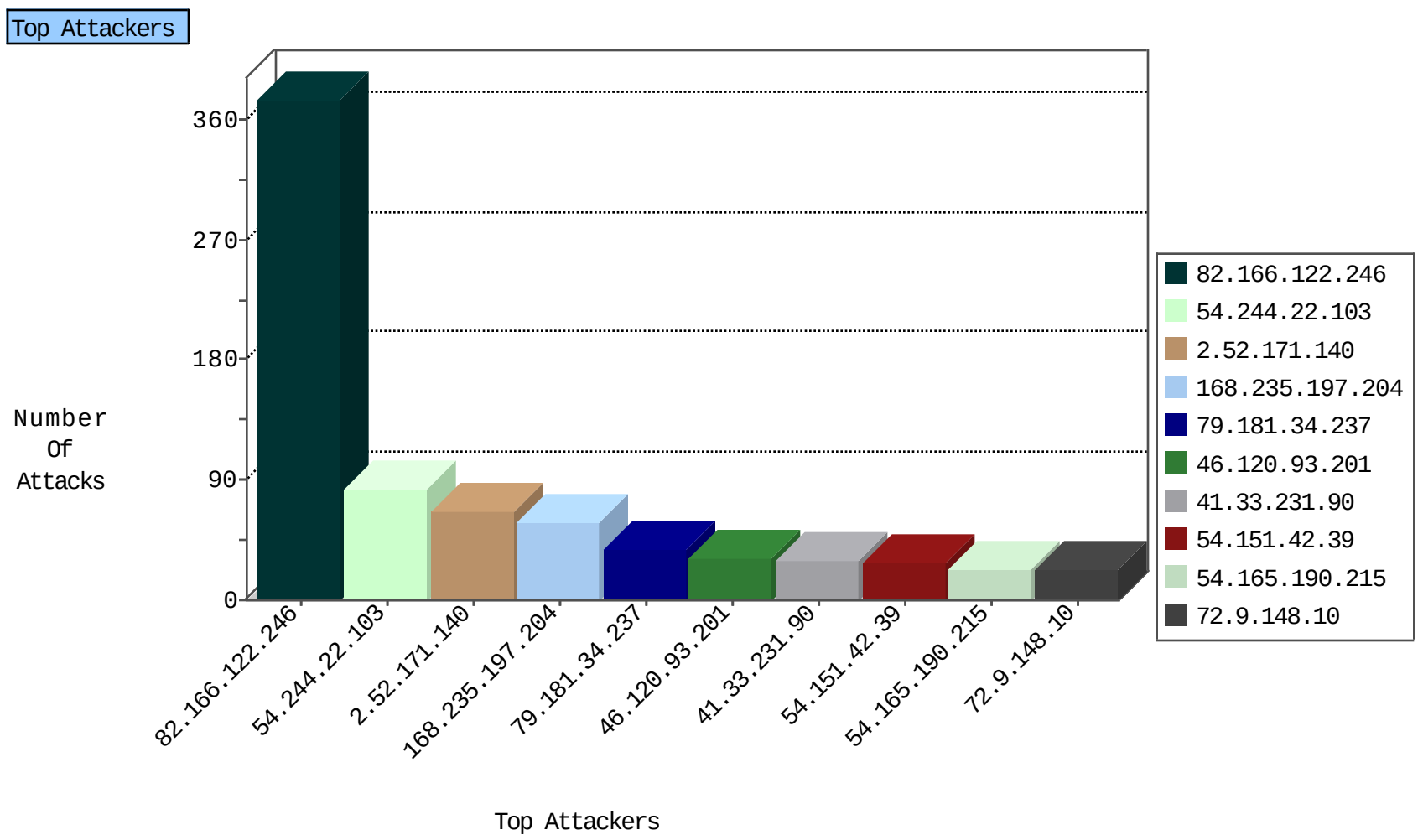
02-14-2016-18:04:07 to 02-14-2016-19:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-14-2016-18:04:07 to 02-14-2016-19:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.21.158	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
168.235.197.204	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.46.189	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
123.151.42.61	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
168.235.197.204	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-18:04:07 to 02-14-2016-19:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-14-2016-18:04:07 to 02-14-2016-19:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP WEB-INF access	16
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.166.122.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
54.242.197.57	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
95.86.67.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.175.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.116.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.210.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
193.201.227.57	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.147.103.155	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.57	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.147.103.155	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
182.234.150.46	147.237.8.46	Taiwan	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.50.87.208	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.155.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.159	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
217.65.46.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.227.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.109.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.57	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.147.103.155	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.57	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.147.103.155	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
149.88.147.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-14-2016-18:04:07 to 02-14-2016-19:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	333
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	73
168.235.197.204	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	53
2.52.171.140	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.151.42.39	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	28
54.165.190.215	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
2.52.171.140	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
2.52.171.140	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.52.171.140	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.148.141	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.116.110.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.185.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.29.203.98	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.105.1	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
176.34.244.157	Ireland	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.120.93.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
147.235.8.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.120.93.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.93.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
82.166.100.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.12.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.100.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.93.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
50.17.121.178	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.149.255	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.235.8.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
2.54.141.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.51.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.166.122.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
147.235.8.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
212.150.177.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.141.68	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-14-2016-18:04:07 to 02-14-2016-19:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.34.237	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	14
2.54.7.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
82.166.148.41	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	7
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
64.233.173.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.183.218.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.218.137	Block	3
185.32.179.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
109.66.0.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.0.22	Block	2
84.94.174.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
64.233.173.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.88.153.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
23.254.243.17	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
192.117.12.65	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/webresource.axd	None	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.212.122.112	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /x	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
79.183.218.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.220.152.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.209	Block	1
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.52.173.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.30.24.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
80.246.137.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.255.253.18	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.9.135.38	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/	Block	1
109.66.0.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method d-With: in URL com.facebook.katana	Block	1
37.26.149.214	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.26.149.214 (Unknown SSL Session)	None	1
84.108.227.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×’×™××•×¡	Block	1
199.30.24.248	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.115.73	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
173.252.122.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.232.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Malformed URL com.facebook.katana	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Directory Traversal (In Cookies/Parameters Value)	Block	1
23.254.138.210	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
192.117.12.65	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.214	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
84.109.116.248	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1294-he/	Block	1

02-14-2016-18:04:07 to 02-14-2016-19:04:07