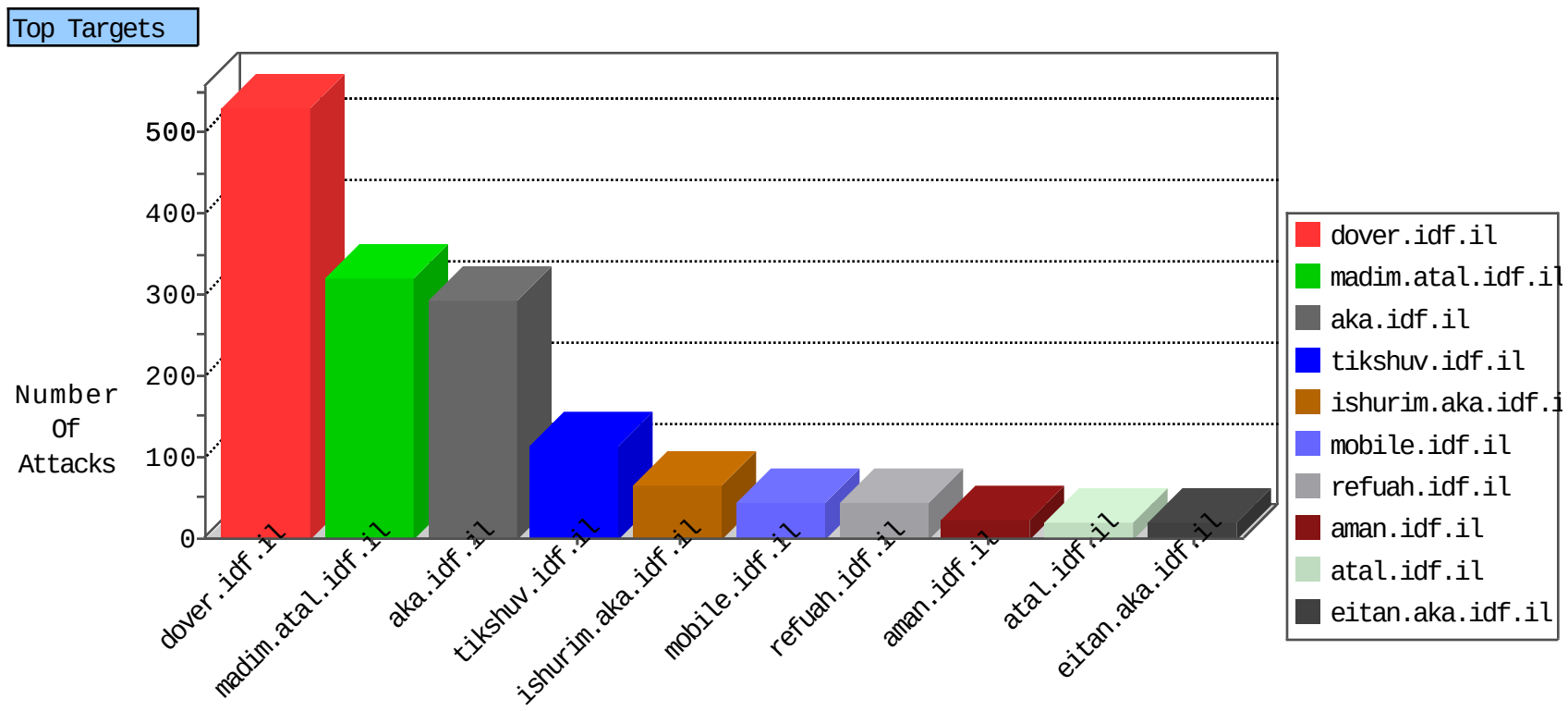
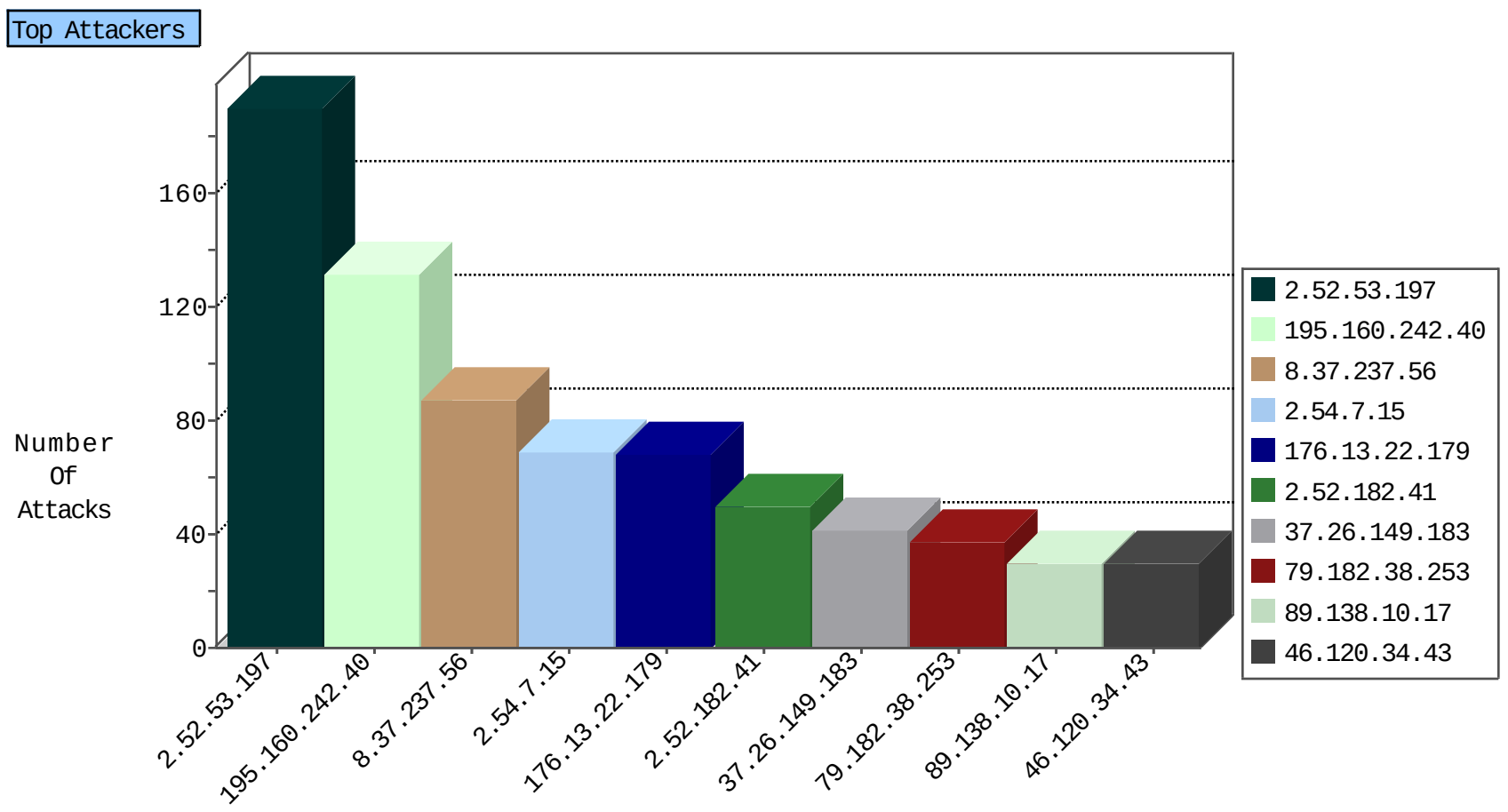
02-15-2016-14:04:03 to 02-15-2016-15:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-15-2016-14:04:03 to 02-15-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.7.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	48
89.138.10.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
82.80.181.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
213.57.138.197	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.174.39	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
8.37.237.56	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
78.161.35.161	Turkey	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-15-2016-14:04:03 to 02-15-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.215.239.56	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-15-2016-14:04:03 to 02-15-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
213.57.144.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.199.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.50	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.131.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.1	147.237.0.200		m4u.idf.il	ET SCAN NMAP -f -sS	1
132.68.56.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.151	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.109.115.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.130.103.146	147.237.76.38	Israel	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.232.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.236.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.173.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.1	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.183.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.20.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.166.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.136.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.130.103.146	147.237.76.44	Israel	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.66.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-14:04:03 to 02-15-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
8.37.237.56	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	85
195.160.242.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.54.7.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
81.218.171.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.7.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.149.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
85.130.226.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.149.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.218	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
89.138.192.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.210.186.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.149.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
37.60.144.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.81.128.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
89.138.10.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
89.138.10.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.147.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.147.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.21.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.147.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.85.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.156.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.11	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.77	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.221.5	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.186.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.16	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.226.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.150.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.253.150.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-15-2016-14:04:03 to 02-15-2016-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.53.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
176.13.22.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
2.52.182.41	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 2.52.182.41	Block	48
2.52.53.197	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.53.197	Block	44
176.13.23.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.120.34.43	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
46.120.166.49	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
176.13.9.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.218.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
140.242.217.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	6
109.253.136.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
5.29.210.124	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 79.182.38.253	Block	4
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.182.38.253	Block	4
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 79.182.38.253	Block	4
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.182.38.253	Block	4
81.215.239.56	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.215.239.56	Block	4
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 52.48.22.169	Block	3
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple NULL Character in Header Name from 79.182.38.253	Block	3
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 52.48.22.169	Block	3
81.215.239.56	Turkey	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 52.48.22.169	Block	3
46.116.2.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Header Line from 79.182.38.253	Block	3
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 52.48.22.169	Block	3
5.29.60.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.53.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 79.182.38.253	Block	3
46.19.86.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.182.38.253	Block	2
80.246.133.44	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
81.215.239.56	Turkey	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 81.215.239.56	Block	2
2.52.150.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
109.253.144.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 79.182.38.253	Block	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/news/	Block	1
80.246.133.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.35.253.161	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal HTTP Version	Block	1
46.35.253.161	Russian Federation	147.237.76.31	nakchal.idf.il	Parameter Type Violation lang in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
85.250.244.244	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
81.215.239.56	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
185.89.217.233		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.54.5.77	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.140.93	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

02-15-2016-14:04:03 to 02-15-2016-15:04:03