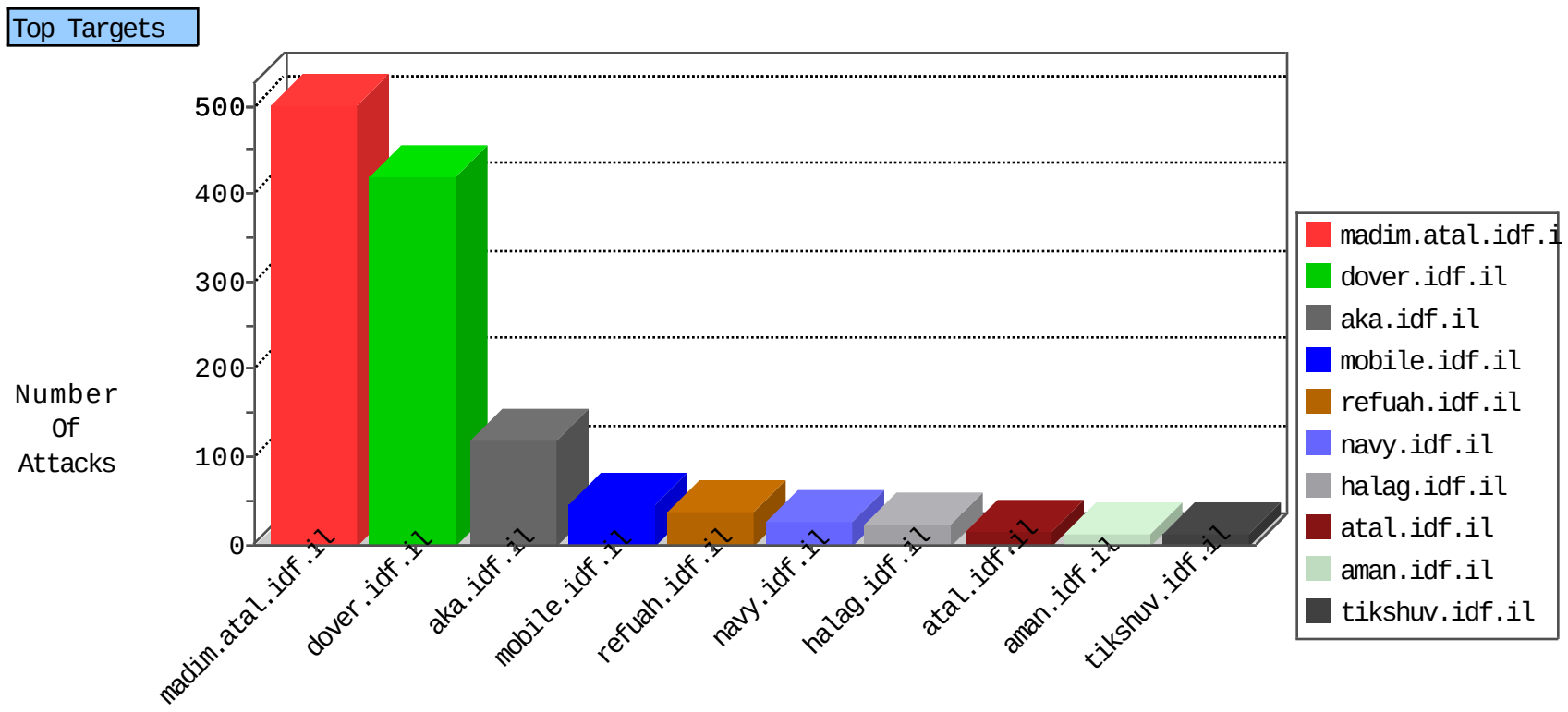
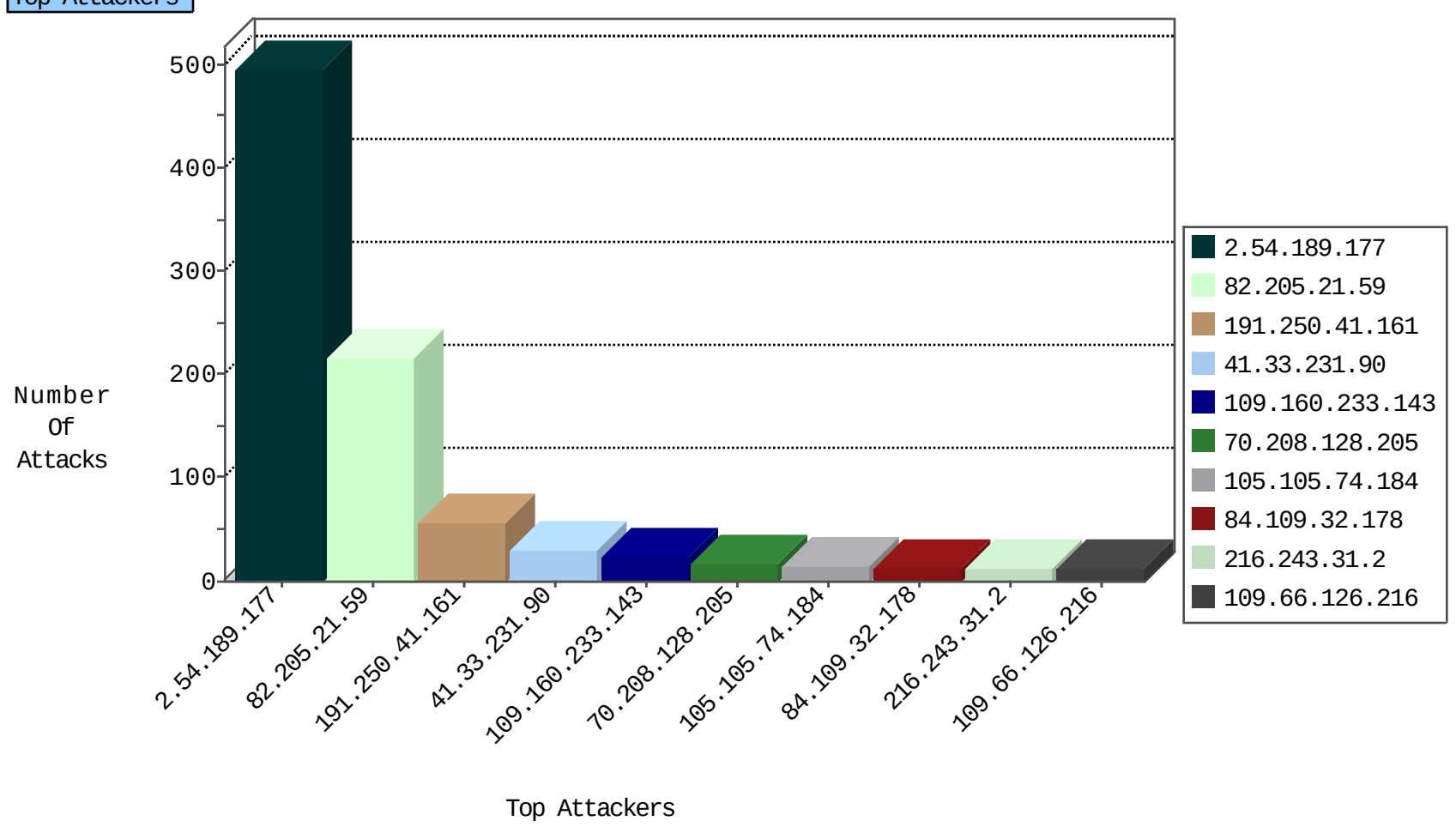
02-19-2016-20:04:07 to 02-19-2016-21:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-19-2016-20:04:07 to 02-19-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
191.250.41.161	Brazil	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	48
84.108.152.18	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
191.250.41.161	Brazil	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.74	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-19-2016-20:04:07 to 02-19-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.171	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C1000023: HTTP: administrator in URI	Block	4
84.108.186.43	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
77.127.221.29	Israel	147.237.0.34	tikshuv.idf.i	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-19-2016-20:04:07 to 02-19-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP login.htm access	7
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP admin.php access	6
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP adminlogin access	3
104.255.65.207	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
187.252.6.14	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
63.221.141.195	147.237.77.74	Hong Kong	law.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
52.77.230.145	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
104.255.65.207	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
191.250.41.161	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.169.93	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
146.185.250.2	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

02-19-2016-20:04:07 to 02-19-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
191.250.41.161	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
109.160.233.143	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
70.208.128.205	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
105.105.74.184	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
84.109.32.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
77.127.29.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.112.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.126.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
31.210.187.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
69.124.241.186	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.35.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.65.114.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.38.225	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.195.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.146.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.186.244	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.223.28	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.177.187.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.213.53.42	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.154.38.225	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.122.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.18.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.188.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.221.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.131.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.54.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.160.169.83	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.241	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.68.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.216.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.117.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.13.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.52.139.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.42.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-19-2016-20:04:07 to 02-19-2016-21:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.66.126.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
37.46.41.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.189.177	Block	252
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.189.177	Block	102
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 82.205.21.59	Block	67
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.205.21.59	Block	63
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	41
37.26.149.157	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
131.253.25.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.54.144.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.156.183	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	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.36.103	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.121.233.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.154.89.59	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.89.59	Block	2
69.124.241.186	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 69.124.241.186	Block	2
207.46.13.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.36.103	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.36.103	Block	2
85.64.156.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/undefined	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
212.34.23.117	Jordan	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1
98.213.53.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
212.34.23.117	Jordan	147.237.77.176	matpash.idf.il	Malformed URL http/1.1	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
109.66.126.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
84.109.32.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1100-he/nakhal.aspx	Block	1
37.187.114.171	France	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to /sap/hana/admin/	Block	1
176.13.1.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.71.31.161	Block	1
212.34.23.117	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method pts/ui/i18n/jquery-ui-i18n.js in URL www.cogat.idf.ilhttp/1.1	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.160.233.143	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.35.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.156.183	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.64.156.183	Block	1
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.71.31.161	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 87.71.31.161	Block	1
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
217.69.133.244	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/kishur/default.asp	Block	1
31.154.89.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/myunselectquestionnaire/aspx	Block	1
69.124.241.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
212.34.23.117	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
87.71.31.161	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1