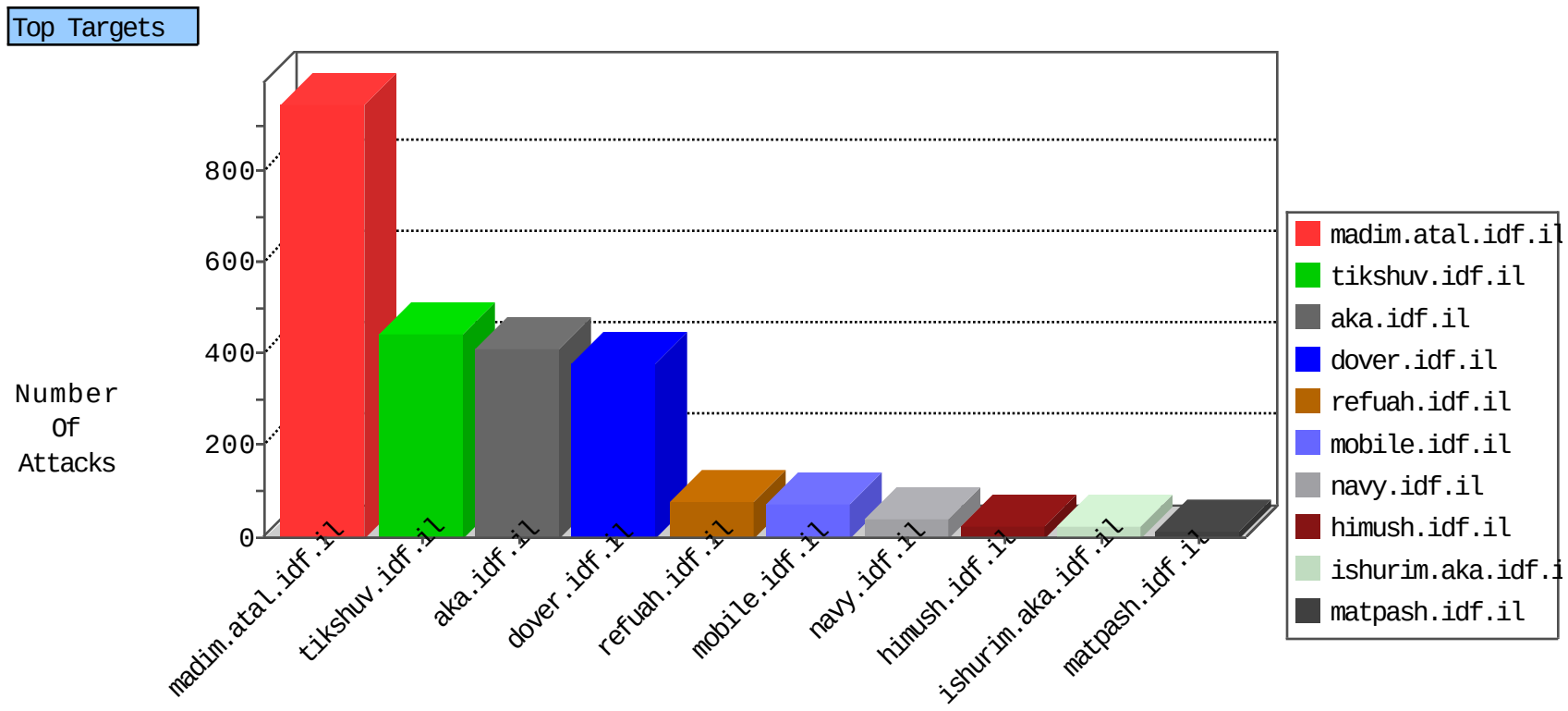
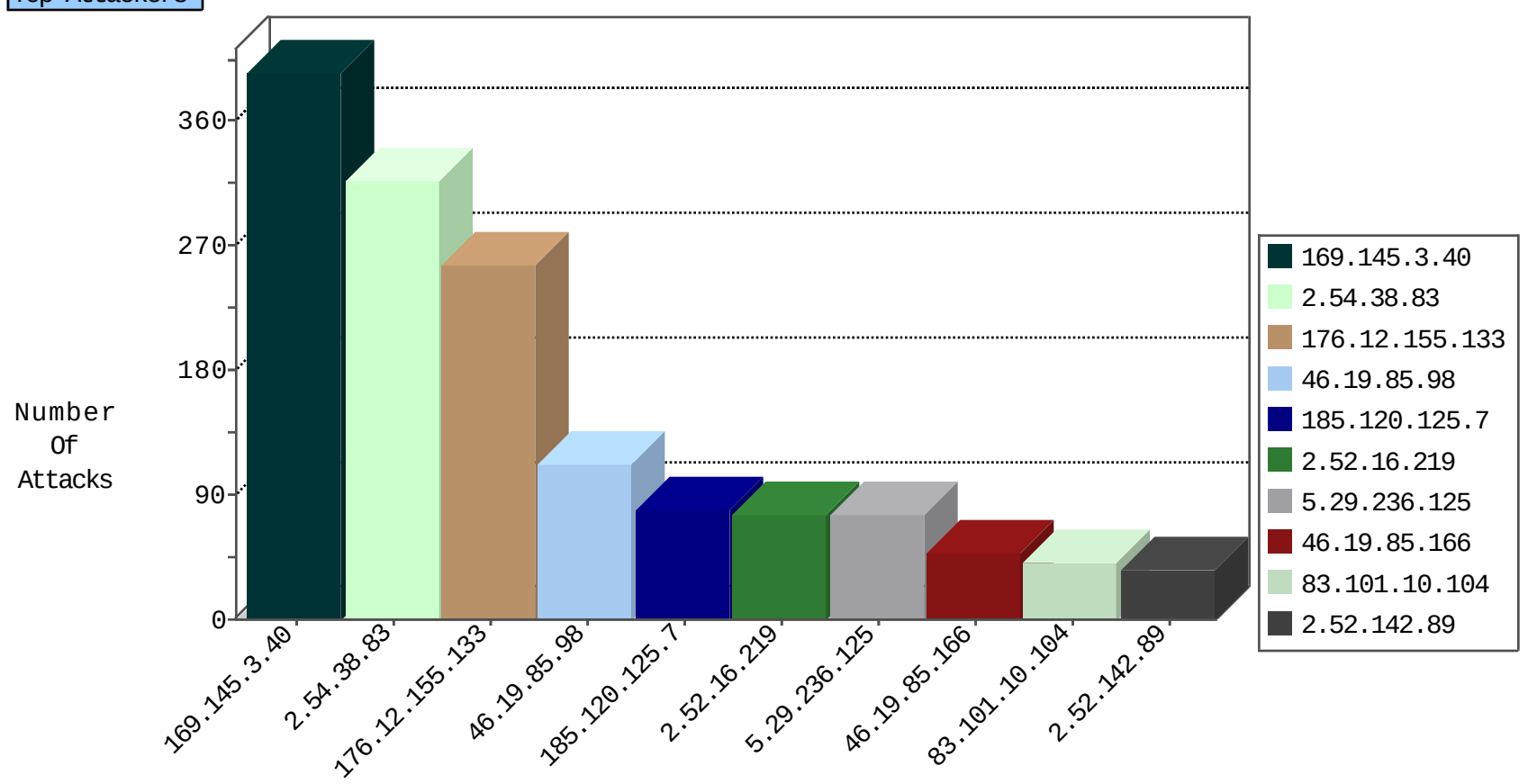
02-01-2016-21:04:01 to 02-01-2016-22:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-01-2016-21:04:01 to 02-01-2016-22:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
46.19.85.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
37.142.64.102	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.178.101.213	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
185.35.62.60	Switzerland	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
178.239.62.139	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
79.180.71.161	Israel	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
178.239.62.139	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1

02-01-2016-21:04:01 to 02-01-2016-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.225.121	France	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
151.80.31.150	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-01-2016-21:04:01 to 02-01-2016-22:04:01

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	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.62.52.41	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.32.179.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.77.19	Turkey	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.0.75.114	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.163.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.83.135.131	147.237.77.235	Georgia	sviva.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.227	Georgia	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.205	Georgia	prisha.idf.il	ET SCAN Potential SSH Scan	1
46.120.227.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.14.14.106	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.17.11.120	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
146.0.75.114	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.201.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.83.135.131	147.237.77.243	Georgia	mobile.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.233	Georgia	atal.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.212	Georgia	e.dover.idf.il	ET SCAN Potential SSH Scan	1

02-01-2016-21:04:01 to 02-01-2016-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
169.145.3.40	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	396
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
79.176.100.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
141.0.14.193	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.27.105.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.67.200.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
105.239.222.66	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.130.234.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.14	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
141.0.15.216	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.121.37.45	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
209.140.44.114	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.140.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.142.89	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.15.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.142.89	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
176.12.154.109	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.142.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.230.69.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.142.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.142.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.182.207.4	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.101.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
154.103.121.144	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.141	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.207.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.121.37.45	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
149.50.74.173	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.9.122.202	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.38.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	162
176.12.155.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	131
2.54.38.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.12.155.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
2.52.16.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
176.12.155.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	45
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
2.54.38.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	37
84.228.122.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.122.173	Block	25
84.108.189.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
5.102.234.136	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
37.142.68.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.54.38.83	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	12
176.12.154.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
176.12.154.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
37.26.149.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
5.22.131.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.22.131.106	Block	5
2.54.15.136	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
94.230.86.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
176.12.155.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
62.219.160.224	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.160.224	Block	3
188.165.225.121	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.225.121	Block	3
37.26.148.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/home.aspx	Block	3
185.27.105.73	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
176.12.155.30	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
2.54.48.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.169.144.135	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.169.144.135	Block	2
176.12.155.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.155.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.108.21.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.154.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.138.28	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.93	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/news/news.asp	Block	1
2.52.16.219	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected , Observed **********	None	1
94.199.151.22	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.22.131.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
65.208.151.112	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
104.131.147.112	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.121	Block	1
191.232.136.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.228.163.176	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
79.181.55.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.192	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1