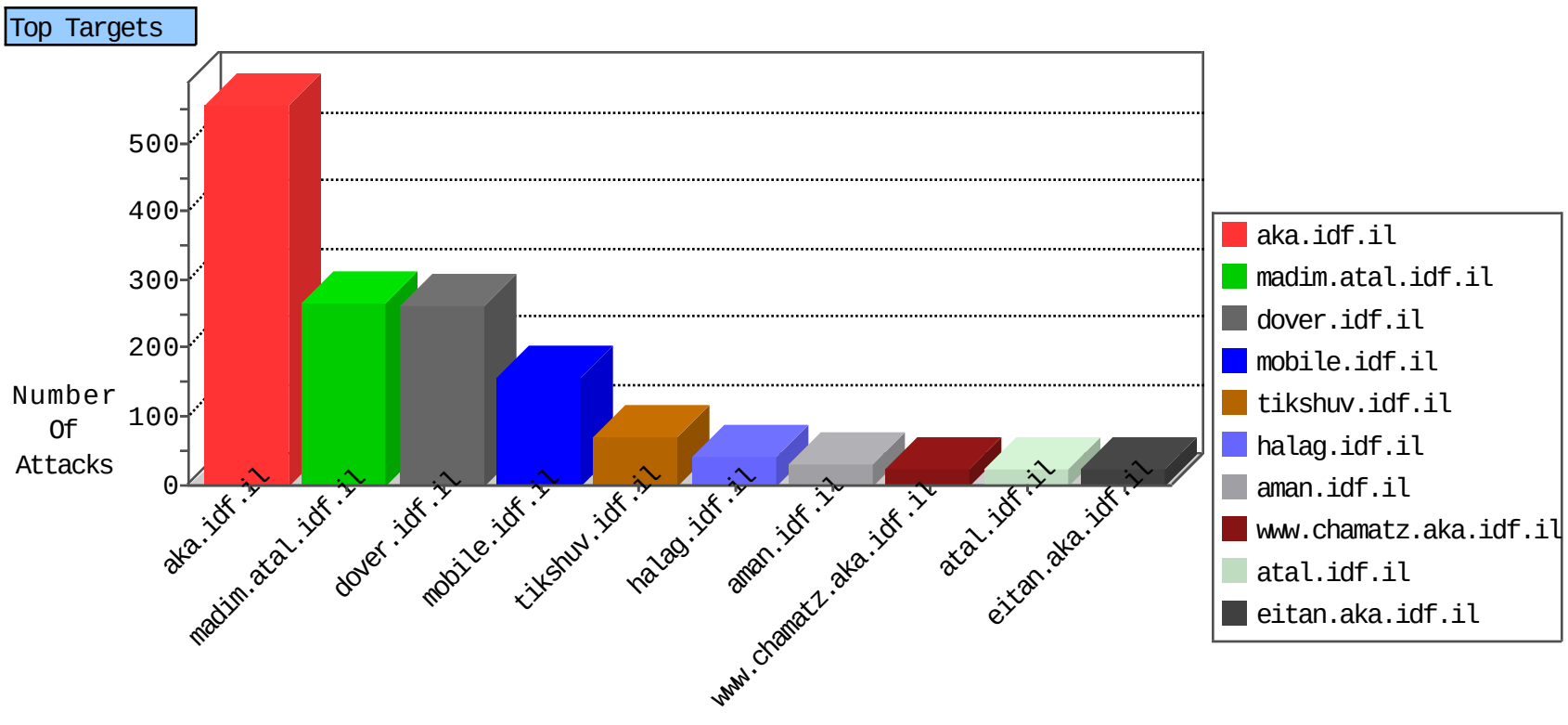
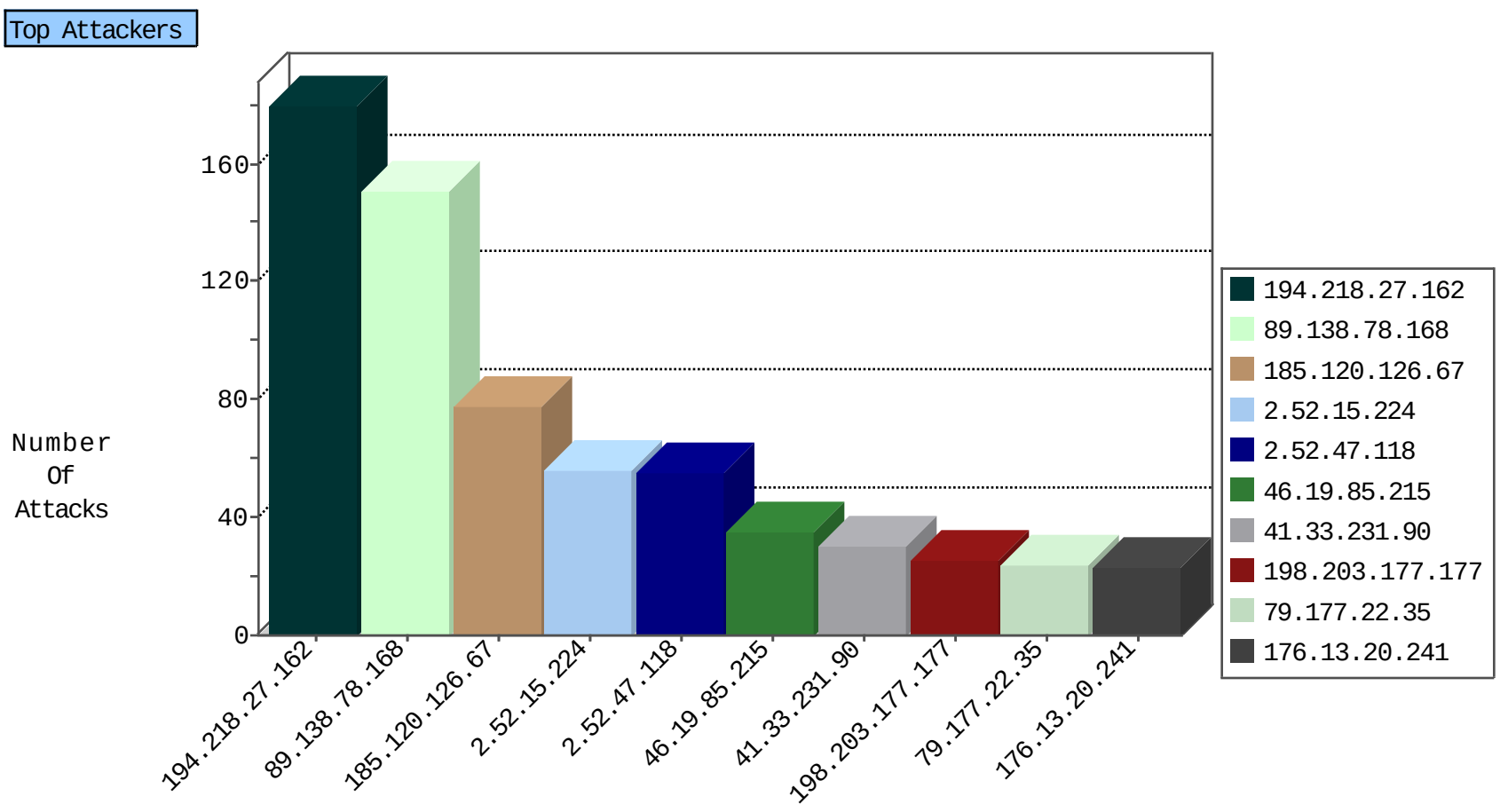
02-28-2016-19:04:00 to 02-28-2016-20:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-19:04:00 to 02-28-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.74	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
82.145.208.74	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	3
185.94.111.1		147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-28-2016-19:04:00 to 02-28-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.143.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
79.176.233.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.179.201.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.121.37.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
85.64.2.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
173.234.153.122	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
85.64.99.12	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
173.234.153.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
77.126.161.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
173.234.153.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.139.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
31.154.159.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.188.136	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
149.78.221.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-28-2016-19:04:00 to 02-28-2016-20:04:00

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
185.56.28.72	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.210	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.28.72	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.8.24	Morocco	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
185.56.28.72	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.26.115.52	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
110.241.200.178	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.25.119.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.183.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.17.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.228	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.56.28.72	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.176.160.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.56.28.72	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
46.117.14.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.56.28.72	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.8.24	Morocco	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.48.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.163.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.177.58.243	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.57.233.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.202.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
109.66.56.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
85.130.235.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.56.28.72	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
79.180.228.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-19:04:00 to 02-28-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
79.177.22.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
198.203.177.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
2.52.15.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
79.178.236.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
176.13.15.35	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.176.111.81	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
2.54.182.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.178.218.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.79.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
87.71.65.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
85.130.244.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.116	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.41.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.139.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.15.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.52.15.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.15.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.52.15.224	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	8
66.249.79.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.177.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.179.14.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.9	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.165.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.14.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.199	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.69.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.175.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.51.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.206.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.220	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.151.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.66.113.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
104.232.181.118		147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	5
5.102.254.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.66.228	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.131.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
40.77.167.38	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.78.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
2.52.47.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.20.241	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	20
109.253.158.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.64.180	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.64.180	Block	6
2.54.182.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
149.78.71.253	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
109.253.196.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
62.90.142.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	5
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	5
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
85.65.117.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
85.64.41.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.177.189.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
91.228.197.248	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
93.172.173.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.143.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
117.26.248.204	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
37.26.148.190	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.228.197.248	Poland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.228.197.248	Block	2
80.246.139.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.66.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.206.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.18	Block	2
37.142.191.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
109.65.185.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$60 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
217.132.131.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.183.138.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.12	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/113338.pdf	Block	1
157.55.39.148	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/www.pc.co.il/	Block	1
117.26.248.204	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 117.26.248.204	Block	1
73.182.247.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.78.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.26.148.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1755	Block	1
199.30.24.31	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
66.249.64.149	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.175.210.230	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.13.112.118	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15693-he/dover.aspx	Block	1
157.55.39.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.228	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1