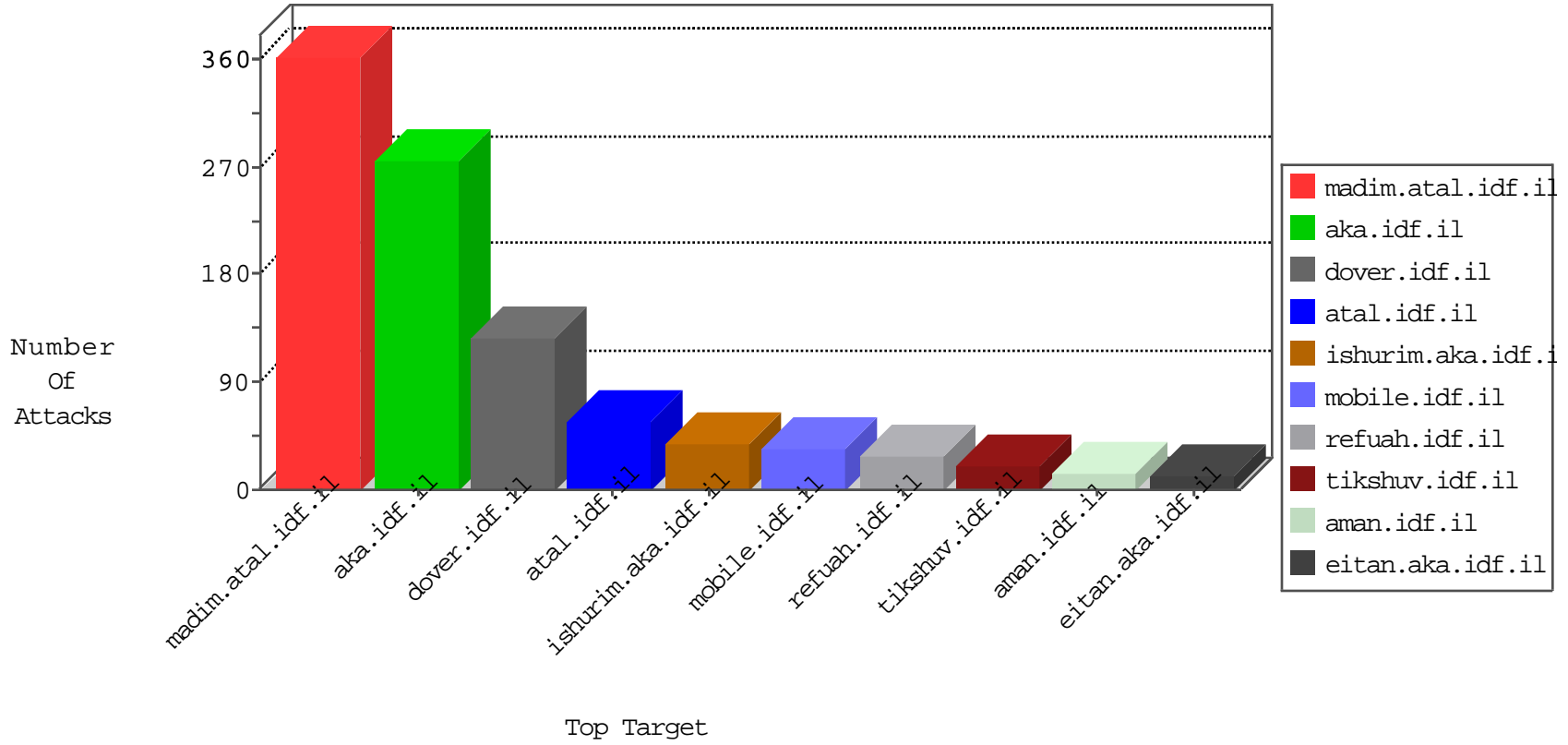


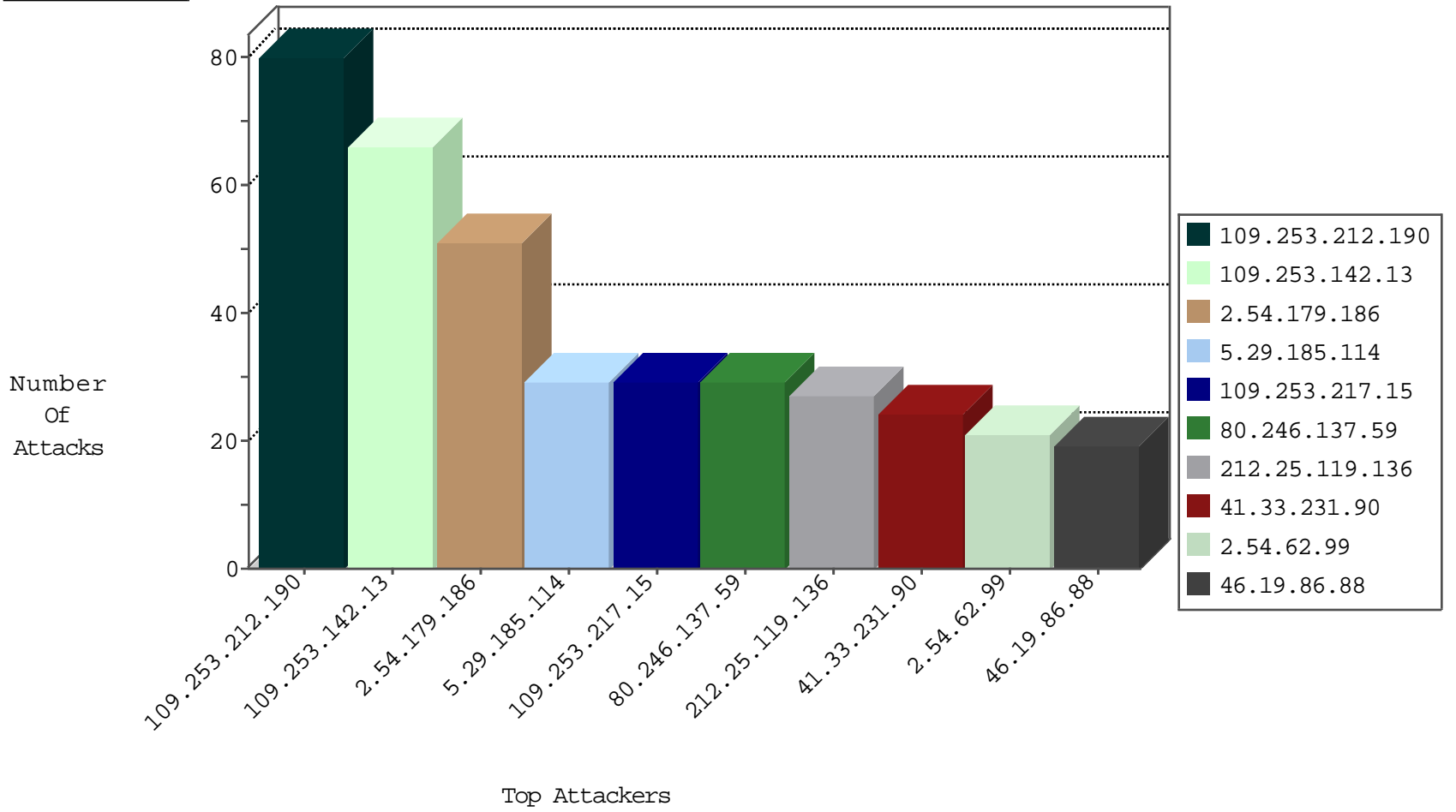
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
198.103.180.1	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.41	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.0.34	tikshuv.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.28.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
208.115.113.89	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.78.11.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.1.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.172.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.197	China	e.hinush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
212.199.244.112	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
212.25.69.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.193.158.54	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.243.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.150.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
5.29.185.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
212.25.119.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.86.88	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.118.12.102	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
109.253.136.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.188.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.136.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.33.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.156.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.32.179.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.65.54.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.199.152.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.153	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.61.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
85.130.219.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.130.83	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
91.200.12.141	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
2.54.61.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.110	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.219.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.130.227.133	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.36.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.118.12.102	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.128.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.182.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.231.94	Bulgaria	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.217.15	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.230.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.35.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.150.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
77.126.85.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.209.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.57.156.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
79.178.99.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.3.144.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.182.177.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-11-2016-14:04:02 to 02-11-2016-15:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.142.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.212.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
2.54.179.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
80.246.137.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.217.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.54.62.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
109.253.212.190	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.212.190	Block	16
79.183.189.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
82.166.85.141	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 82.166.85.141	Block	12
2.54.191.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.150.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
37.26.147.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.147.243	Block	8
5.29.185.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.2.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	4
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.135.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.168.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.25.119.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	3
109.253.135.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.8.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.176.64.152	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.176.64.152	Block	2
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.58	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
94.213.250.148	Netherlands	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
81.218.133.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jqwhv_ljvqftps0&t=2e2045e2	Block	1
79.181.134.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questi on\$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.132.61.255	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
192.80.186.110	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1043-en/cogat.aspx	Block	1
109.226.26.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
85.64.24.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
2.54.138.244	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtContent in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9331-he/refuah.aspx	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1515-en/dover.asp	Block	1
54.67.110.194	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
184.105.139.70	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
94.213.250.148	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to ww.eitan.aka.idf.il/xmlrpc.php	Block	1
31.154.164.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
128.194.131.235	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 128.194.131.235	Block	1