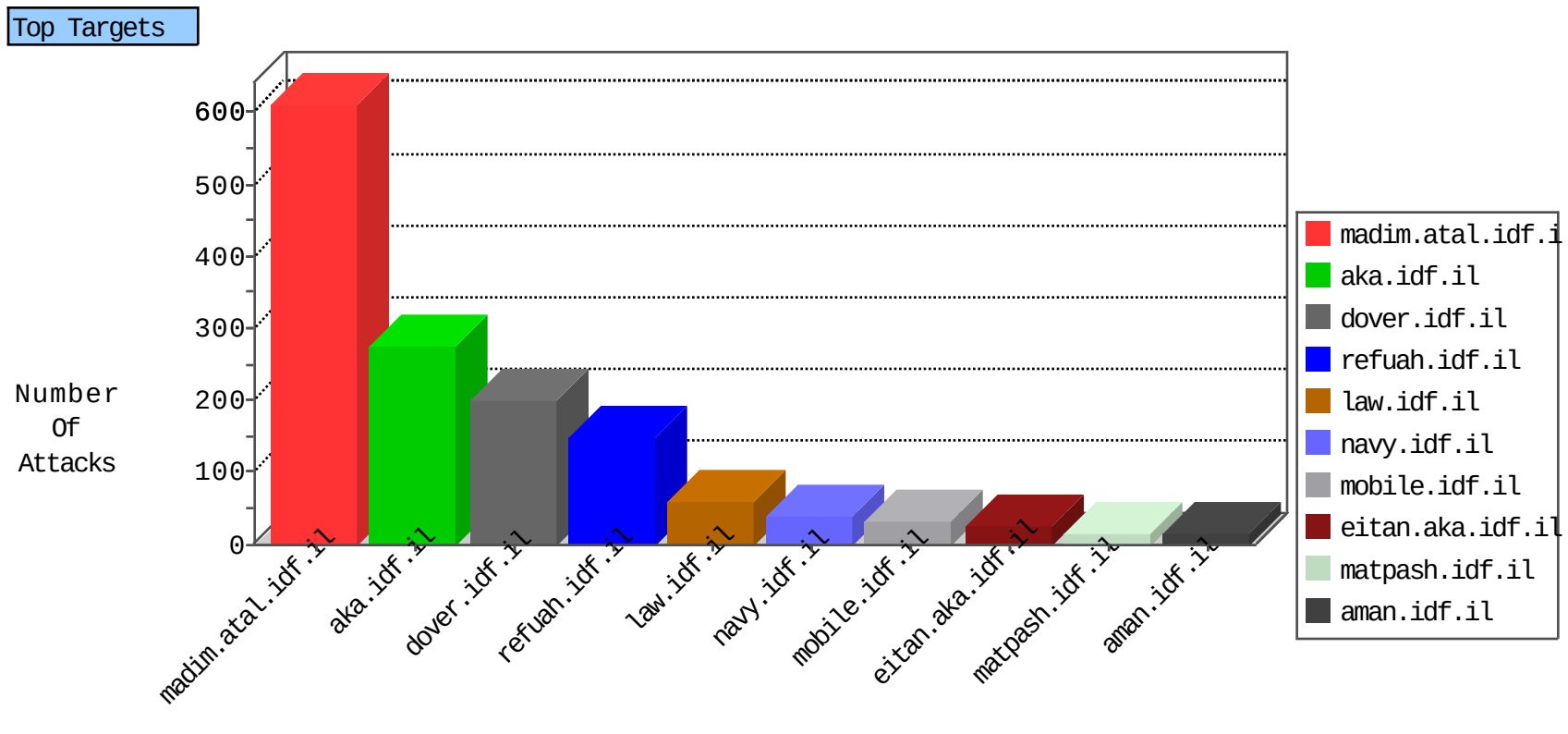
02-08-2016-23:04:03 to 02-09-2016-00:04:03

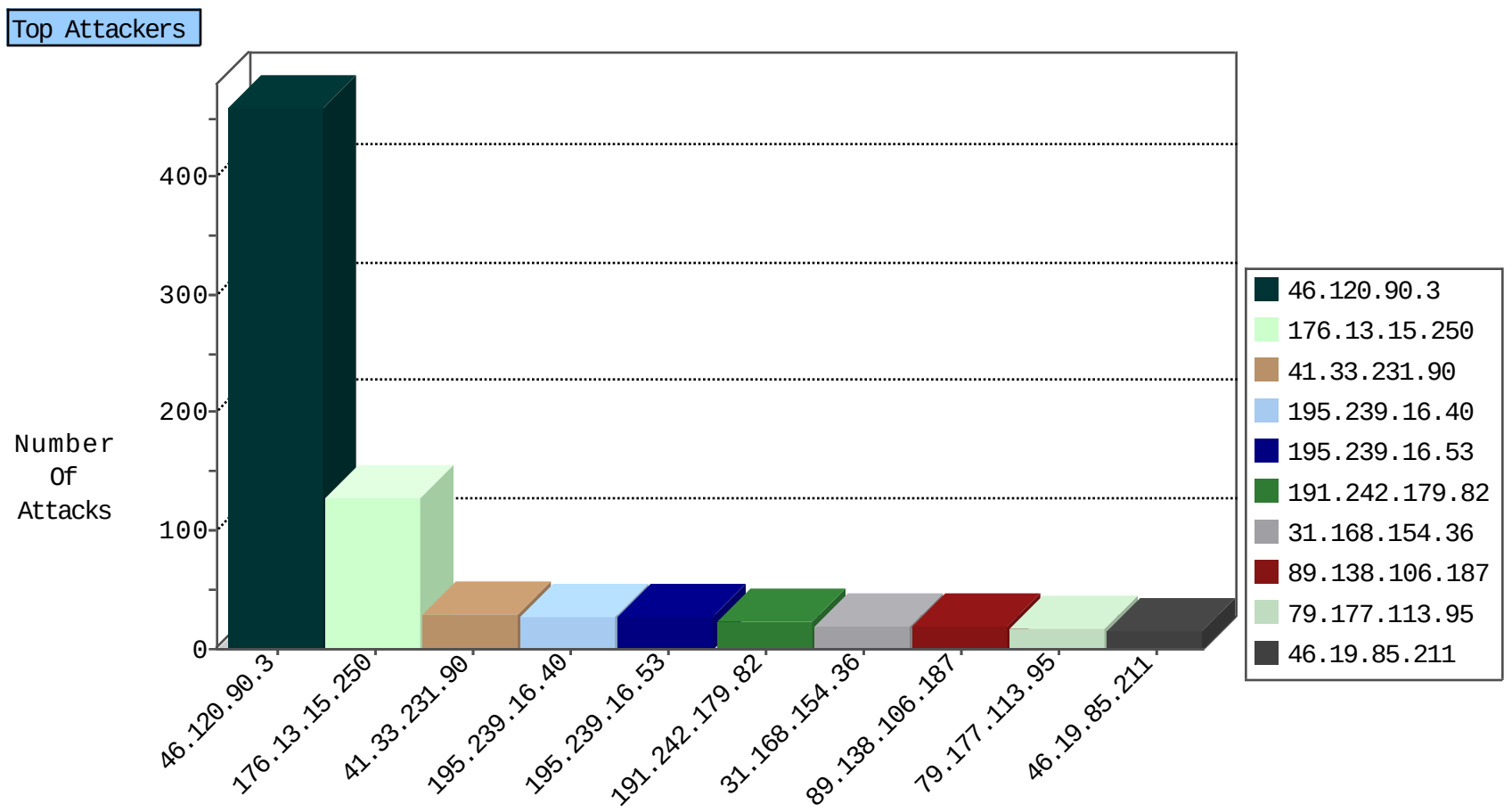
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-08-2016-23:04:03 to 02-09-2016-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.8.79.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.33.66.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
139.196.4.19	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
115.239.228.10	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
74.91.28.58	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
208.69.30.158	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.54	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-23:04:03 to 02-09-2016-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	C164: HTTP: BanglaDos	Block	4

02-08-2016-23:04:03 to 02-09-2016-00:04:03

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	4
66.249.93.219	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
149.88.147.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.74.39.160	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
54.67.38.74	147.237.8.45	United States	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.45.137.67	147.237.0.35	Turkey	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
187.161.226.176	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.74.39.160	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
96.57.189.67	147.237.77.233	United States	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
54.67.38.74	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
54.67.38.74	147.237.0.34	United States	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.45.137.67	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

02-08-2016-23:04:03 to 02-09-2016-00:04:03

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	30
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
31.168.154.36	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
79.177.113.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.3.144.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
179.99.195.45	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
80.246.133.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
85.130.248.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.106.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
162.204.30.9	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.89.217.228		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.230		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.3.147.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.89.217.231		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.89.217.232		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
79.178.101.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.89.217.229		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
79.179.36.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.211	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.89.217.226		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
89.138.106.187	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.26.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.73.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.28.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.202.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.149	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.181.138.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.211	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
79.182.64.67	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.176.99.226	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.136.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
89.139.164.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.126.112.171	Iraq	147.237.77.216	dover.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	4
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.90.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	251
46.120.90.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	105
46.120.90.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.15.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
176.13.15.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
89.138.180.33	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.138.180.33	Block	11
2.54.28.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.105.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.99.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.201.123.243	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.201.123.243	Block	3
79.178.59.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	2
109.201.123.243	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
84.108.95.183	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.93.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
93.172.155.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
79.179.36.176	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.179.36.176	Block	1
61.135.190.71	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
109.201.123.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.187	Block	1
85.65.233.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$36 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
178.232.4.46	Norway	147.237.77.74	law.idf.il	PHP Attempt	Block	1
96.57.189.67	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version deflate, sdch	Block	1
79.181.138.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/109284.pdf	Block	1
109.253.202.101	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method s=56b90cfe44a11515000 in URL	Block	1
8.37.70.81	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx&usg=alkjrhjlijgutwueysglunsypjp0cqkadg	Block	1
85.65.233.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.229.164.102	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
178.232.4.46	Norway	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
109.160.148.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
79.183.59.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
149.78.63.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
54.67.38.74	United States	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.89.217.235		147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png	Block	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.187	Block	1
80.246.133.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/105714.pdf	Block	1
37.142.191.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
54.67.38.74	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.187	Block	1