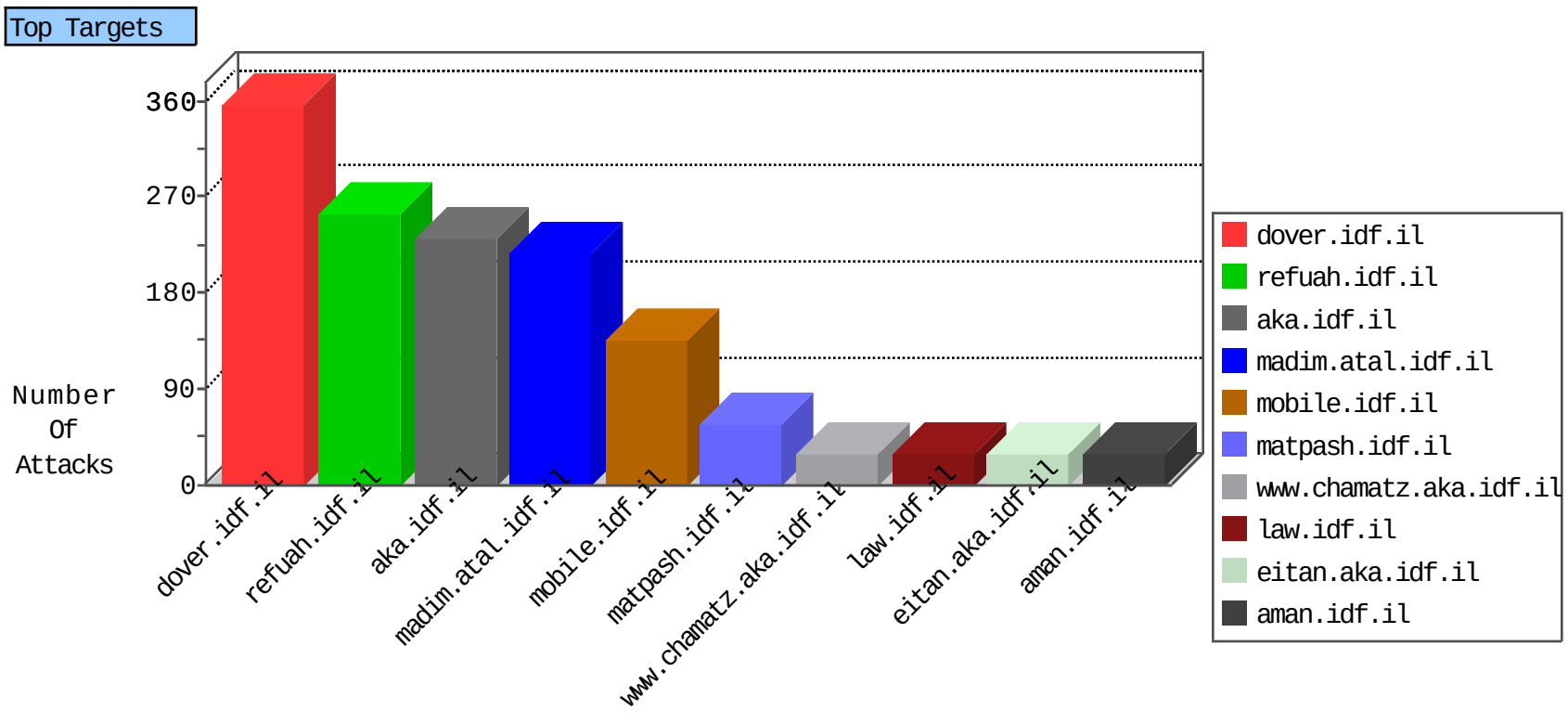
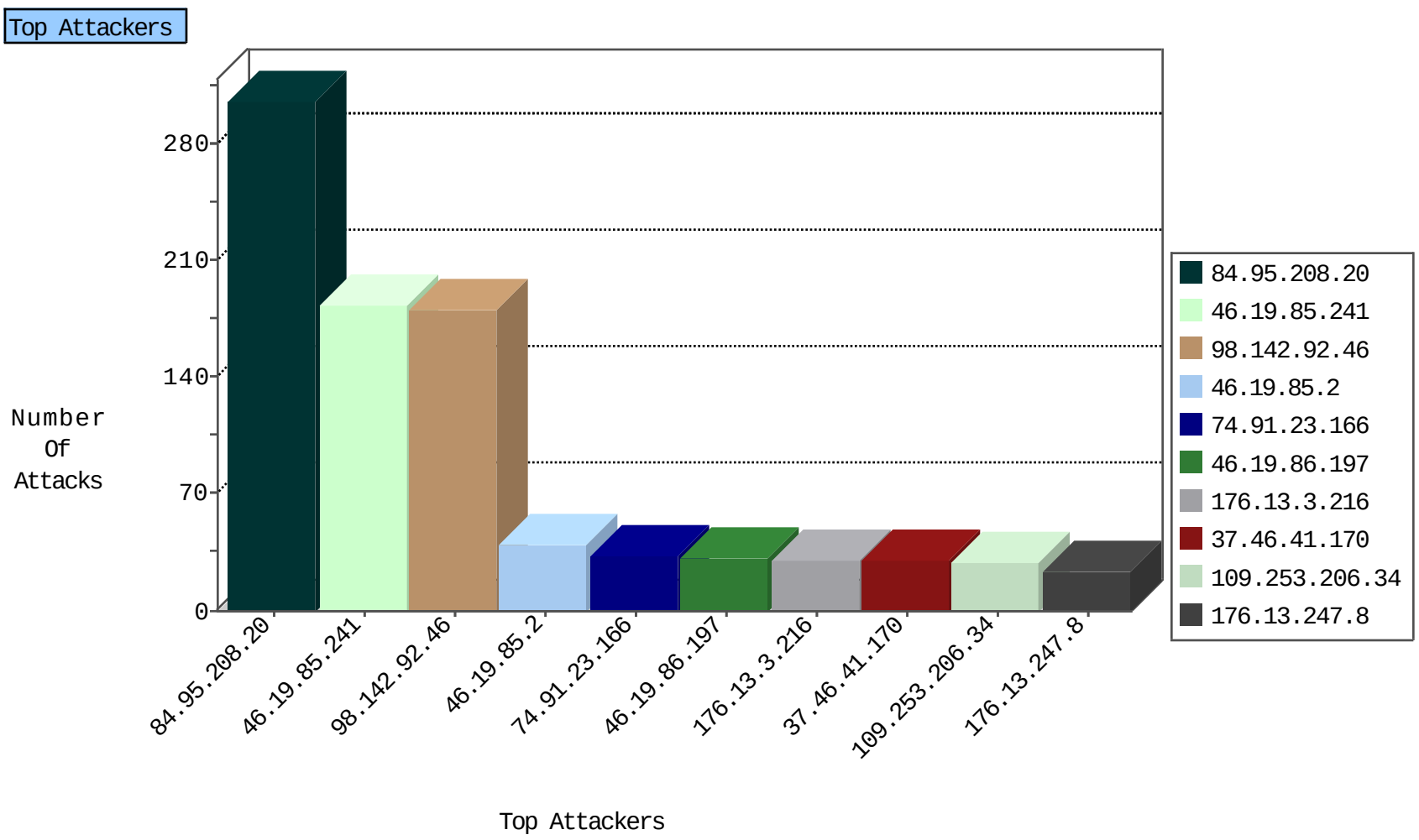
10-02-2016-10:04:02 to 10-02-2016-11:04:02

IDF Under Attack Daily Report





10-02-2016-10:04:02 to 10-02-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
93.174.95.106	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
94.23.115.240	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	1

10-02-2016-10:04:02 to 10-02-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
208.51.63.37	United States	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1

10-02-2016-10:04:02 to 10-02-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
112.66.56.154	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.40.4.208	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
175.211.230.65	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
49.228.76.148	147.237.76.176	Thailand	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
154.16.199.48	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
24.37.68.226	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.0.34	Singapore	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
5.255.90.133	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
123.16.253.141	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.80.116.202	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
114.80.116.202	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.40.4.208	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
107.138.98.174	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.33	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
24.37.68.226	147.237.0.33	Canada	idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.77.176	Singapore	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
24.37.68.226	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
124.243.134.208	147.237.77.176	Australia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
116.109.34.185	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.80.116.202	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

10-02-2016-10:04:02 to 10-02-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
98.142.92.46	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	181
74.91.23.166	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
37.46.41.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.3.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.65.69.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
194.77.48.121	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
87.71.31.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.117.220.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.139.236.200		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
31.146.114.66	Georgia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
66.249.65.10	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.120.124.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.2	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
188.247.74.17	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.85.2	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.183.58.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
52.3.127.144	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	7
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.89.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
115.28.218.121	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
77.127.89.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
196.53.60.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
115.28.218.121	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
115.28.218.121	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
184.204.182.76	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
176.13.247.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
184.204.182.76	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.247.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
52.3.127.144	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
188.161.30.166	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
184.204.182.76	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
196.106.122.81	Kenya	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
176.106.47.35	Palestinian Territory, Occupied	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
115.28.218.121	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4

10-02-2016-10:04:02 to 10-02-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	132
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	95
109.253.206.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
208.51.63.37	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
109.65.69.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
208.51.63.37	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.51.63.37	Block	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
77.139.64.50	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	3
176.13.246.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu/s	Block	3
46.117.220.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
31.154.45.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.100.23	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.139.139.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
109.66.105.15	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
169.229.3.91	United States	147.237.77.74	law.idf.il	NULL Character in Method SÿÒ[[#20]]¬[[#0]]Ïëþa(¦[[#20]][[#31]]™i[[#16]]0¼}h»[[#25]](6¡ÁK[[#24]]·6[[#16]]BÆÌyr•ˆ[[#24]]©™xëg[[#28]]µ	Block	1
77.138.146.157	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
157.55.39.144	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/drushim/misrot.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
85.64.176.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default	Block	1
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
195.167.55.5	Greece	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/piwik.php	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
139.162.13.205	Singapore	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
66.249.64.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/61150.pdf	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method SÿÒ[[#20]]¬[[#0]]Ïëþa(¦[[#20]][[#31]]™i[[#16]]0¼}h»[[#25]](6¡ÁK[[#24]]·6[[#16]]BÆÌyr•ˆ[[#24]]©™xëg[[#28]]µ in URL	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8879-he/refuah.aspx	Block	1
87.71.31.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method http://www.idf.il/1133-21666-he/Dover.aspx in URL	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
139.162.13.205	Singapore	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.127.39.169	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71095.pdf	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1

10-02-2016-10:04:02 to 10-02-2016-11:04:02