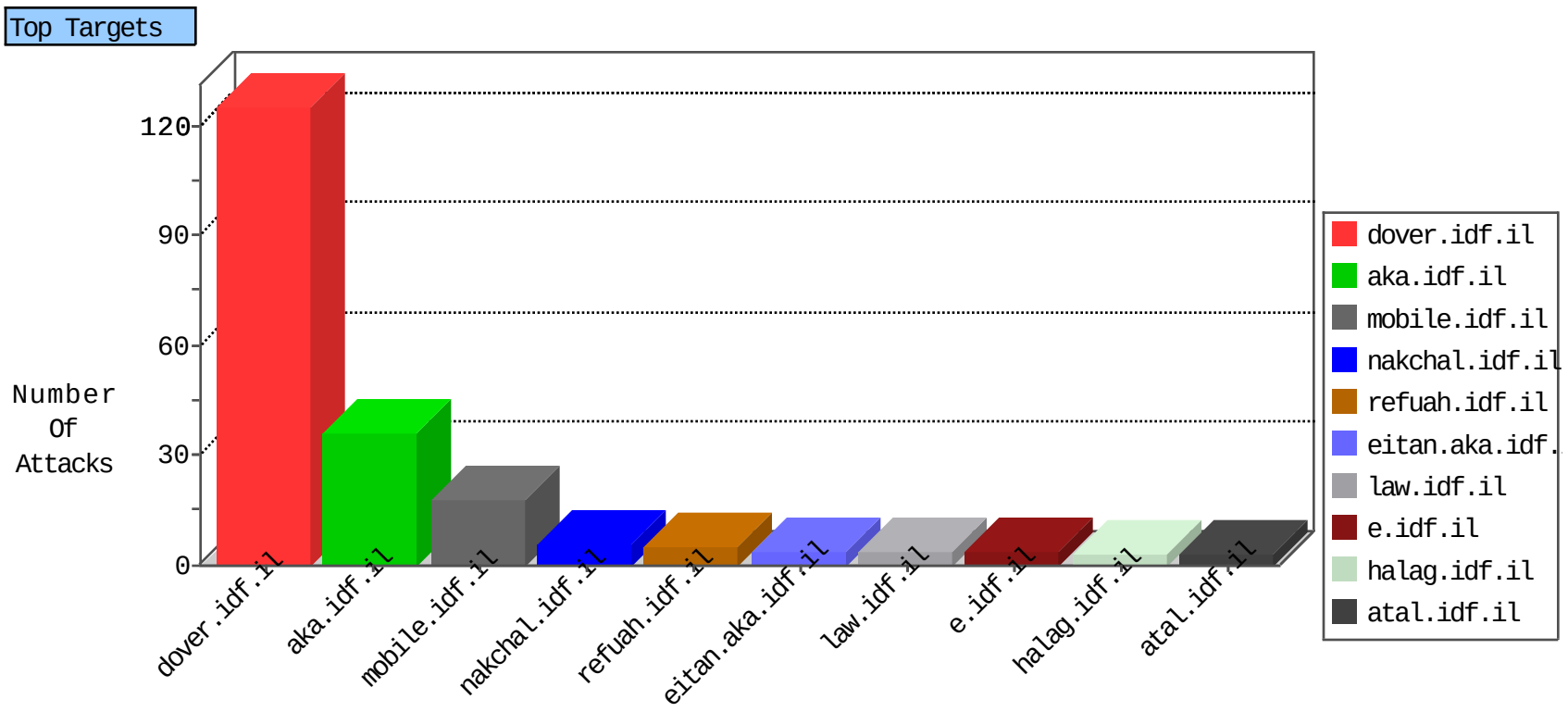
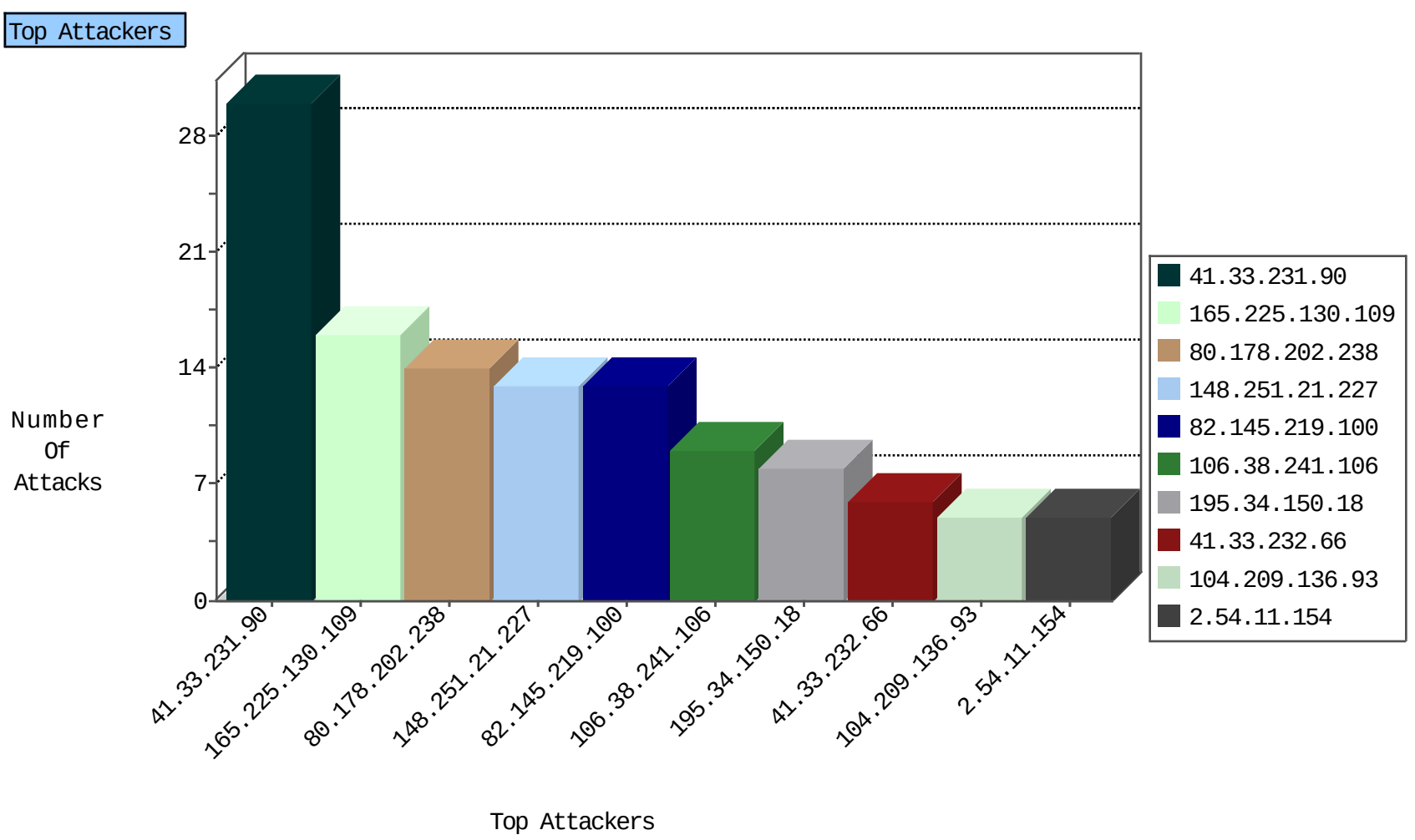
02-28-2016-03:04:08 to 02-28-2016-04:04:08

IDF Under Attack
Daily Report





02-28-2016-03:04:08 to 02-28-2016-04:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.219.100	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	2
134.147.203.115	Germany	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
184.105.247.234	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.71	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
119.92.133.104	Philippines	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
119.92.133.104	Philippines	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
205.209.185.11	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
165.225.130.109	United States	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08

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
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.216.176.244	147.237.76.42	Latvia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
183.55.121.129	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
165.225.130.109	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP admin.php access	1
104.209.136.93	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
104.209.136.93	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.209.136.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.238.176.44	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.31	United States	nakchal.idf.il	ET DROP Dshield Block Listed Source	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.76.34	Latvia	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.240	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
180.245.188.142	147.237.77.212	Indonesia	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.42	China	refuah.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1
104.209.136.93	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.209.136.93	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.44.133.108	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
213.165.89.84	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08

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
80.178.202.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.226.203	Israel	147.237.72.166	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
185.3.144.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.120.126.50		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.31.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.6	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.171.122	Israel	147.237.77.234	halag.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.162.16.100	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
54.162.16.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
149.255.232.128	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.253.25.235	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.227	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.11.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.233	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
43.245.56.97	Fiji	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.54.11.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.234	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.240.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.54.11.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.135.189.121	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.149.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.251	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.240.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.11.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
175.156.130.240	Singapore	147.237.77.243	mobile.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.11.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	7
165.225.130.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 165.225.130.109	Block	5
165.225.130.109	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	4
46.118.114.75	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
165.225.130.109	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 165.225.130.109	Block	3
77.154.202.27	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	2
80.178.202.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
41.141.91.79	Morocco	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
114.112.90.54	China	147.237.76.42	refuah.idf.il	Illegal Host Name	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
213.57.226.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/artillery	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
165.225.130.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
130.193.51.80	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1498-he/atal.aspx об этом же в своих исследованиях говорит бригадный генерал раутио	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
165.225.130.109	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
99.237.127.155	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
178.33.179.251	France	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
69.141.130.206	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.64.93.34	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
198.20.69.74	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
76.64.250.60	Canada	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/gen204	Block	1
113.76.90.154	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.79.144	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מא aspx.|יר שחמו	Block	1
199.30.25.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-28-2016-03:04:08 to 02-28-2016-04:04:08