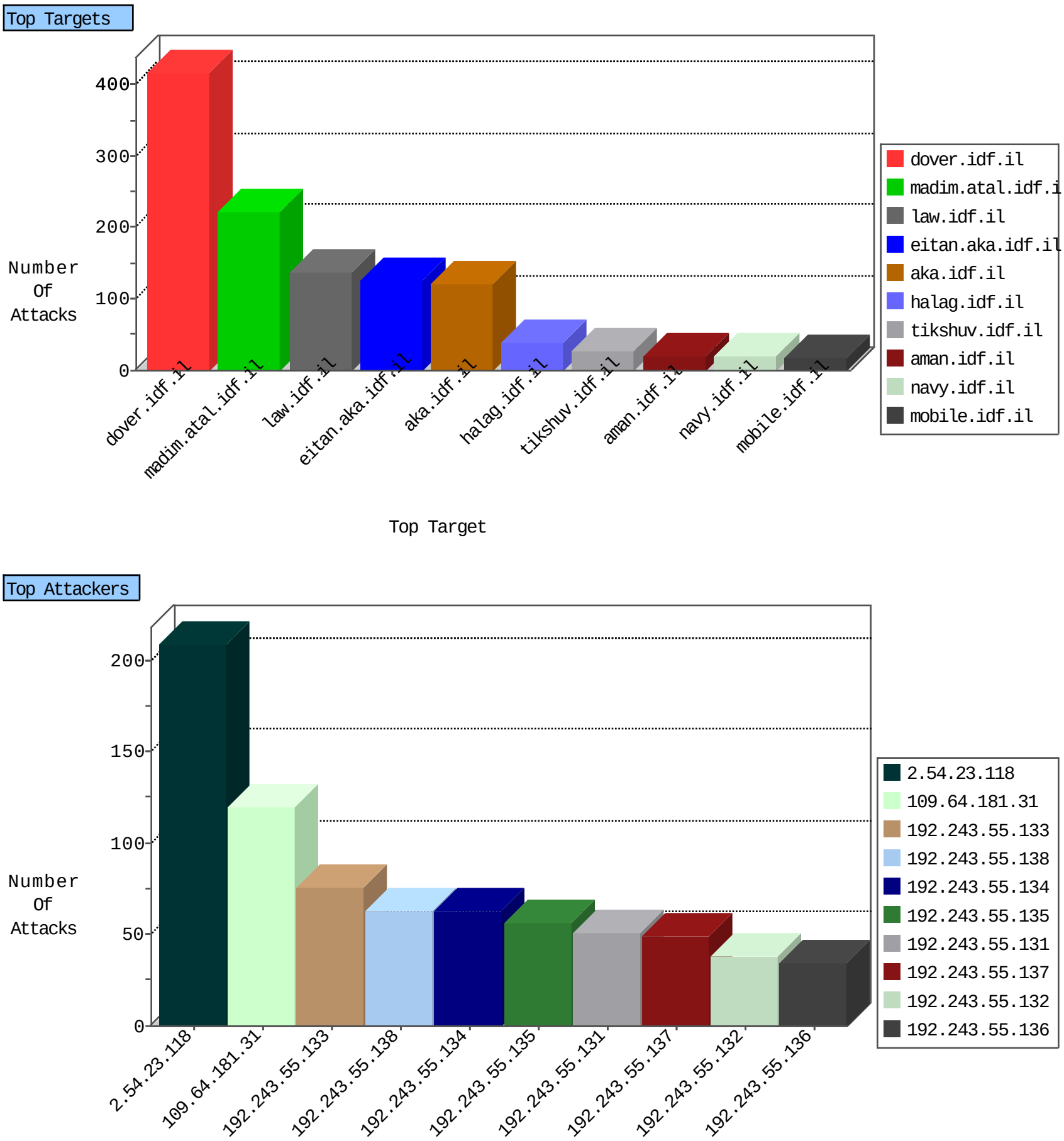
03-04-2016-18:04:04 to 03-04-2016-19:04:04

IDF Under Attack
Daily Report



03-04-2016-18:04:04 to 03-04-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	175
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-04-2016-18:04:04 to 03-04-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.217.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.93.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.109.93.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
68.228.64.54	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
46.19.85.125	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
66.249.93.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.101	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-18:04:04 to 03-04-2016-19:04:04

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
61.182.170.38	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
40.76.80.17	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
37.139.27.231	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
172.87.221.214	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 4096	1
117.190.233.21	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.12.83	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.182.170.38	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
40.76.80.17	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 4096	1
40.76.80.17	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
172.87.221.214	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
95.130.13.220	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
88.248.58.201	147.237.0.35	Turkey	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.65.161.188	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

03-04-2016-18:04:04 to 03-04-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.181.31	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
132.64.27.171	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
176.228.44.15	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
94.159.145.170	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
94.159.145.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
79.180.58.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.42.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.246	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

03-04-2016-18:04:04 to 03-04-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.23.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	209
185.32.179.206	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
109.253.213.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
37.142.64.28	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.155.171	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/1294-he/halag.aspx" id="ctl00_ucheader_ucnavbar_rptcat_ctl02_rptinnercat_ctl02_ainnercatlink	Block	2
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.12.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 212.227.254.68	Block	1
180.76.15.148	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Malformed URL †hu%%	Block	1
77.125.161.172	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 212.227.254.68	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0303-1.stm,	Block	1
46.117.205.24	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
92.76.72.249	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.69.11.101	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 212.227.254.68	Block	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.71.12.83 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.126.166.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Malformed URL from 212.227.254.68	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
62.219.132.70	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
94.21.90.58	Hungary	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 212.227.254.68	Block	1
32.213.145.16	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 212.227.254.68	Block	1
79.183.232.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
65.55.210.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method [[#2]]7XúT[[#28]] §Hñ€µwr·ìXíÞ)¶ö[[#5]]ë?‹¦sF©Ã³—æröçý„ú/î[[#15]]•• ¶õR\;[[#14]]µÑ² ç[[#16]]“ÙÇþðj÷	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 212.227.254.68	Block	1
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem	Block	1
37.113.184.158	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method [[#2]]7XúT[[#28]] §Hñ€µwr·ìXíÞ)¶ö[[#5]]ë?‹¦sF©Ã³—æröçý„ú/î[[#15]]•• ¶õR\;[[#14]]µÑ² ç[[#16]]“ÙÇþðj÷ in URL †hu%%	Block	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 212.227.254.68	Block	1
80.246.136.77	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
132.64.27.171	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.71.12.83	Israel	147.237.72.156	aman.idf.il	Illegal URL Path Encoding †hu%%	Block	1
70.89.4.9	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.227.254.68	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 212.227.254.68	Block	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-04-2016-18:04:04 to 03-04-2016-19:04:04