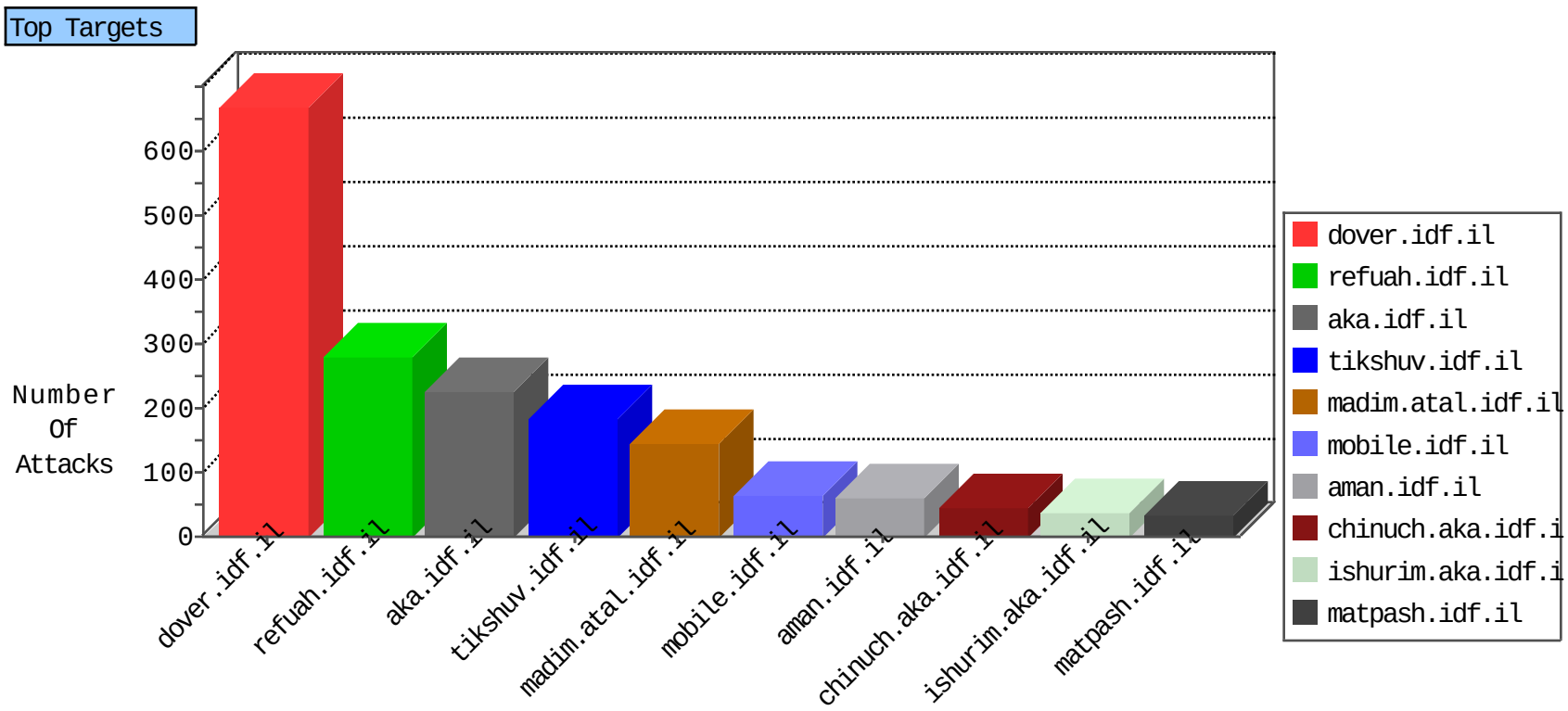
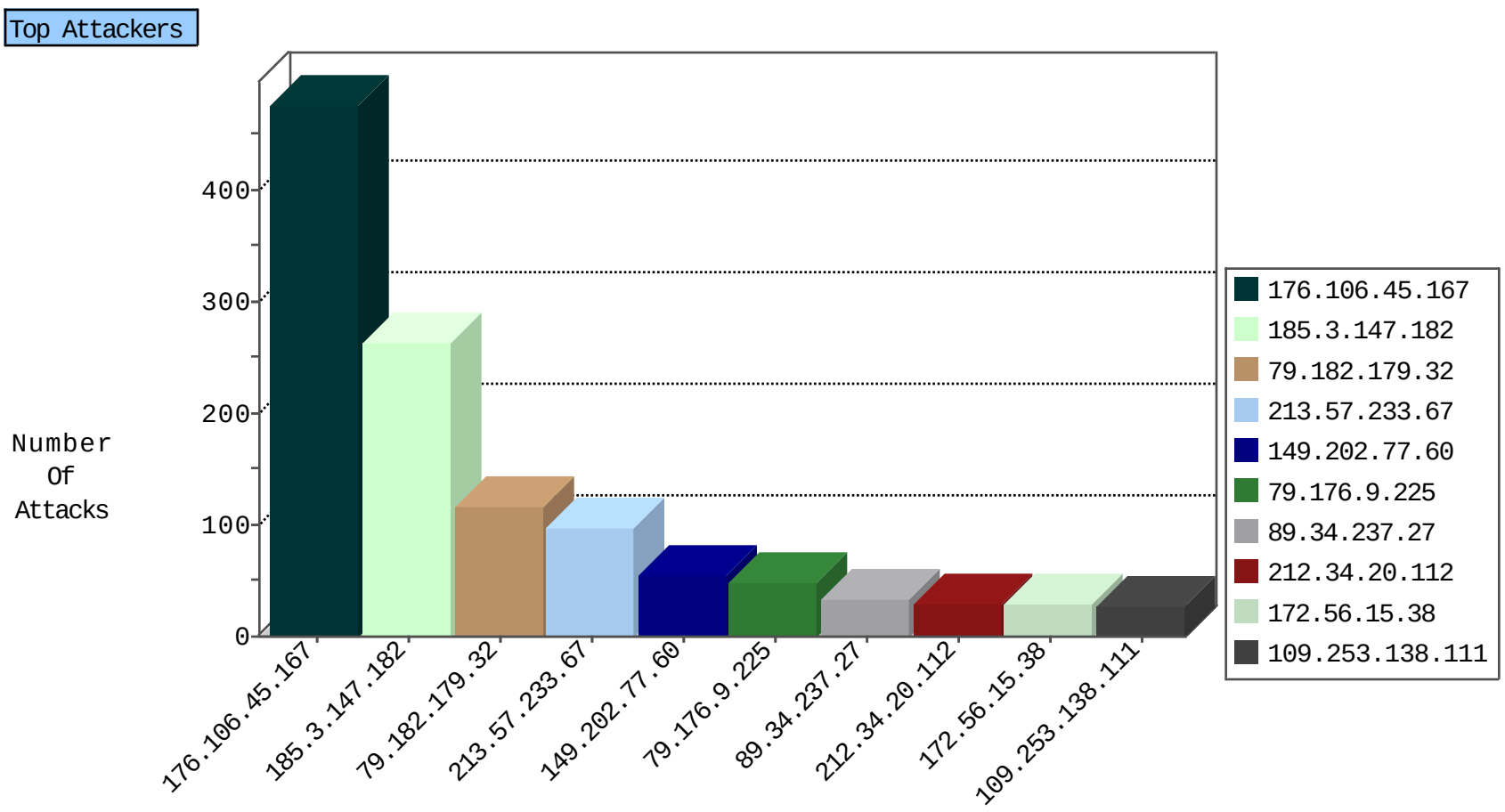
03-05-2016-20:04:00 to 03-05-2016-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-05-2016-20:04:00 to 03-05-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	432
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	42
134.147.203.115	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
183.60.48.25	China	147.237.0.19	madim.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Http	drop	2
72.143.121.34	Canada	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Http	drop	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1

03-05-2016-20:04:00 to 03-05-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.181.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.176.162.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.121.87.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.14.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.108.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.57.233.67	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.147.253	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
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-05-2016-20:04:00 to 03-05-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.191.97.51	147.237.77.216	Ghana	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
213.136.91.26	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
190.239.234.201	147.237.76.30	Peru	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.139.54.71	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.249	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.141.236.69	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
107.191.47.70	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.91.26	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.177.172.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.249	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
61.139.54.71	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.28.150.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.249	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
181.53.62.244	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.136.91.26	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
89.134.135.22	147.237.76.34	Hungary	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

03-05-2016-20:04:00 to 03-05-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.147.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	233
213.57.233.67	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	92
185.3.147.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	30
79.176.9.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
149.202.77.60	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.85.193	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
172.56.15.38	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.202.77.60	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
109.253.138.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
89.34.237.27	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
89.34.237.27	Romania	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
176.13.9.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.91.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.106.45.167	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.182.109.10	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
79.176.9.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
79.176.9.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.22.130.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
106.38.241.151	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
98.82.54.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.139.232	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.67.197.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
185.3.147.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.63.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.181.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.179.32	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.192.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.38.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.180.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
93.172.236.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.102.254.161	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.41.249	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.197.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.52.173	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
172.56.15.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.27.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
98.82.54.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
141.0.14.18	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.228.8.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant		monitor	4
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
89.34.237.27	Romania	147.237.72.156	aman.idf.il	SYN Attack		reject	3
79.179.177.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.163.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.59.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

03-05-2016-20:04:00 to 03-05-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.179.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
109.253.138.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 212.34.20.112	Block	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 212.34.20.112	Block	5
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 212.34.20.112	Block	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.177.223.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
94.159.148.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.157.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.195.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 212.34.20.112	Block	3
2.52.62.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.154.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.192.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.75.218	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.75.218	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
95.86.88.219	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71817-he/maarachot.aspx&sa=u&ved=0ahukewjwrqwynarlah vddjokhdb6ci8qfggimaa&sig2=hy37urpn0crn5_yolscqvw&usg=afqjcnhorn3fyp t4w3vxtqs7wqyyu5fz8q	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.111.188.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteykatava	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name [[#21]][[#8]]¨?Ú¸d[[#6]]šÊ§·1÷ג!א in ¬Ž]]Y¶ [[#3]]2[[#14]]“;¡[[#4]][[#19(·ב‍Cג	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 85.64.123.61	Block	1
2.54.188.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.34.20.112	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 in URL	Block	1
85.64.118.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
109.253.192.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
46.120.81.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String [[#21]][[#8]]¨?Ú¸d[[#6]]šÊ§·1÷גג!אכ‍ב ·(Y¶ [[#3]]2[[#14]]“;¡[[#4]][[#19]]¬Ž on	Block	1
79.178.218.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	1
95.86.88.219	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 95.86.88.219	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 85.64.123.61	Block	1
5.102.200.247	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
207.241.237.227	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/general	Block	1
149.255.208.37	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
54.243.53.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12386-en/dover.aspx	Block	1
87.71.49.254	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
66.249.69.169	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/searchpage.aspx	Block	1
85.64.123.61	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 85.64.123.61	Block	1
31.168.241.9	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

03-05-2016-20:04:00 to 03-05-2016-21:04:00