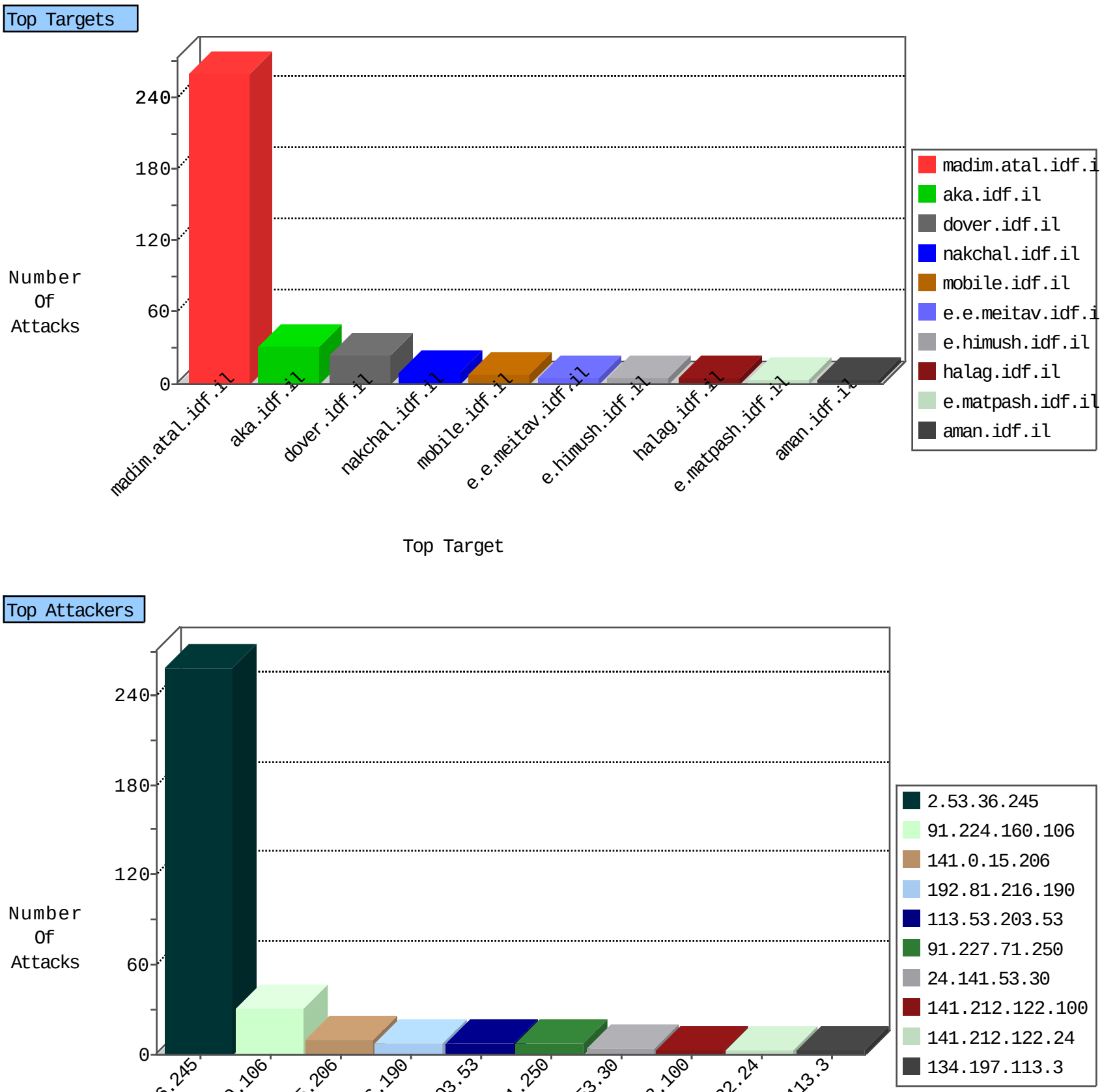
09-16-2016-04:04:01 to 09-16-2016-05:04:01

IDF Under Attack Daily Report



09-16-2016-04:04:01 to 09-16-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
192.33.90.67	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
141.212.113.180	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.234	halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
85.105.183.223	Turkey	147.237.76.147	chinuch.aka.idf.il	network flood IPv4 TCP-SYN	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-04:04:01 to 09-16-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-16-2016-04:04:01 to 09-16-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
202.29.153.142	147.237.72.167	Thailand	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
202.29.153.142	147.237.72.167	Thailand	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
179.43.141.198	147.237.8.27	Switzerland	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.85.192.97	147.237.76.177	Hong Kong	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.153.142	147.237.72.167	Thailand	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
176.47.104.145	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-16-2016-04:04:01 to 09-16-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.15.206	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
113.53.203.53	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.76.31	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
113.53.203.53	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.81.216.190	United States	147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.110	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.99	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.24	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
66.212.179.106	Canada	147.237.0.33	idf.il	drop		drop	1
141.212.122.101	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
24.141.53.30	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.94	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.186.113.169	Japan	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
156.214.100.2	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.56	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.100	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.24	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.108	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.141.53.30	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.95	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.23	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
192.81.216.190	United States	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.186.113.169	Japan	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
182.237.3.154	Hong Kong	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.245	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.100	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.25	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.30.135.177	Vietnam	147.237.0.33	idf.il	drop		drop	1
192.81.216.190	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.109	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.97	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.23	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.76.202	e.halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
113.53.203.53	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.3.147.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.212.179.106	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.100	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.102.195.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.26	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

09-16-2016-04:04:01 to 09-16-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.36.245	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	259
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 91.227.71.250	Block	3
157.55.39.25	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/robots.txt	Block	1
157.55.39.76	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1
211.233.212.72	Korea, Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
104.128.144.131	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/redirect.php	Block	1
211.233.212.72	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
80.20.237.147	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
113.53.203.53	Thailand	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
24.141.53.30	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-en/dover.aspx	Block	1

09-16-2016-04:04:01 to 09-16-2016-05:04:01