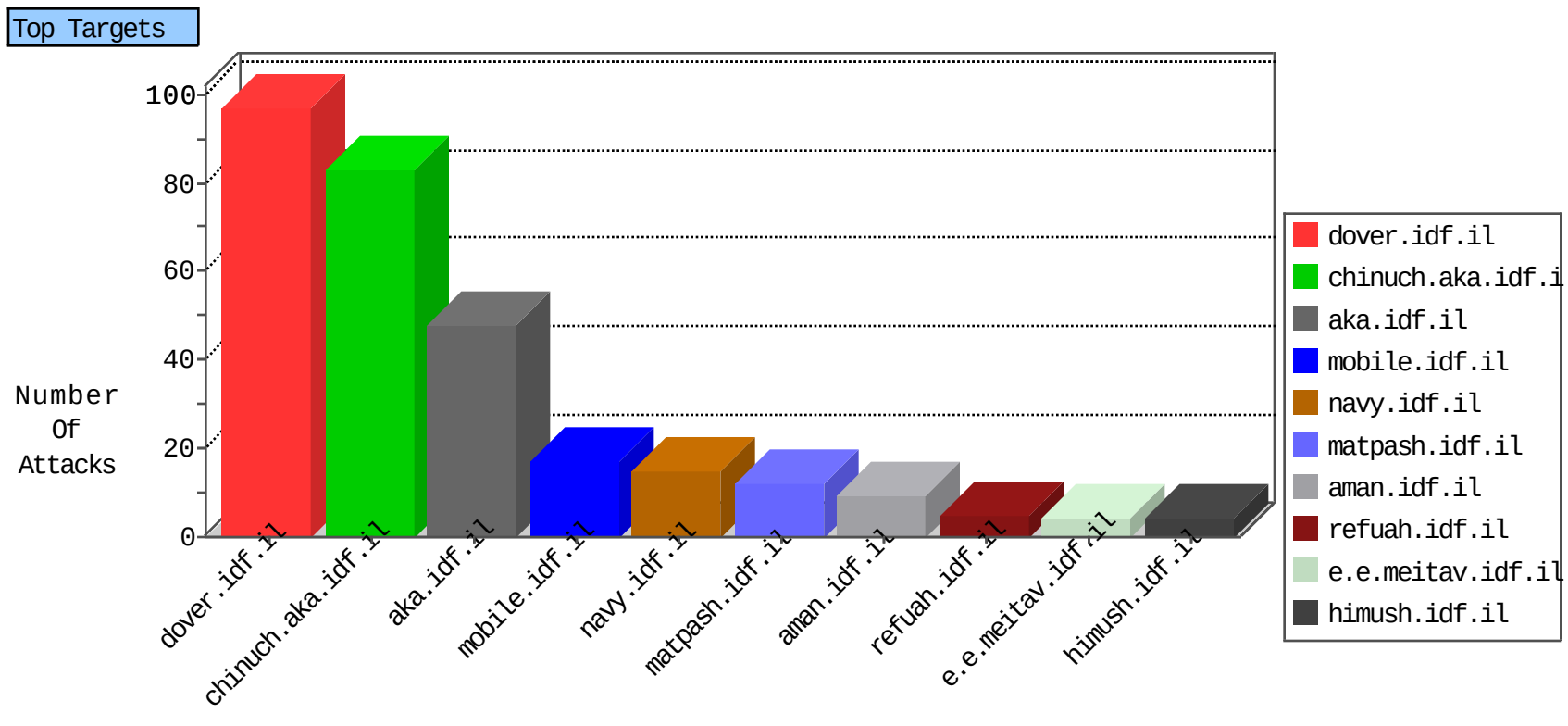
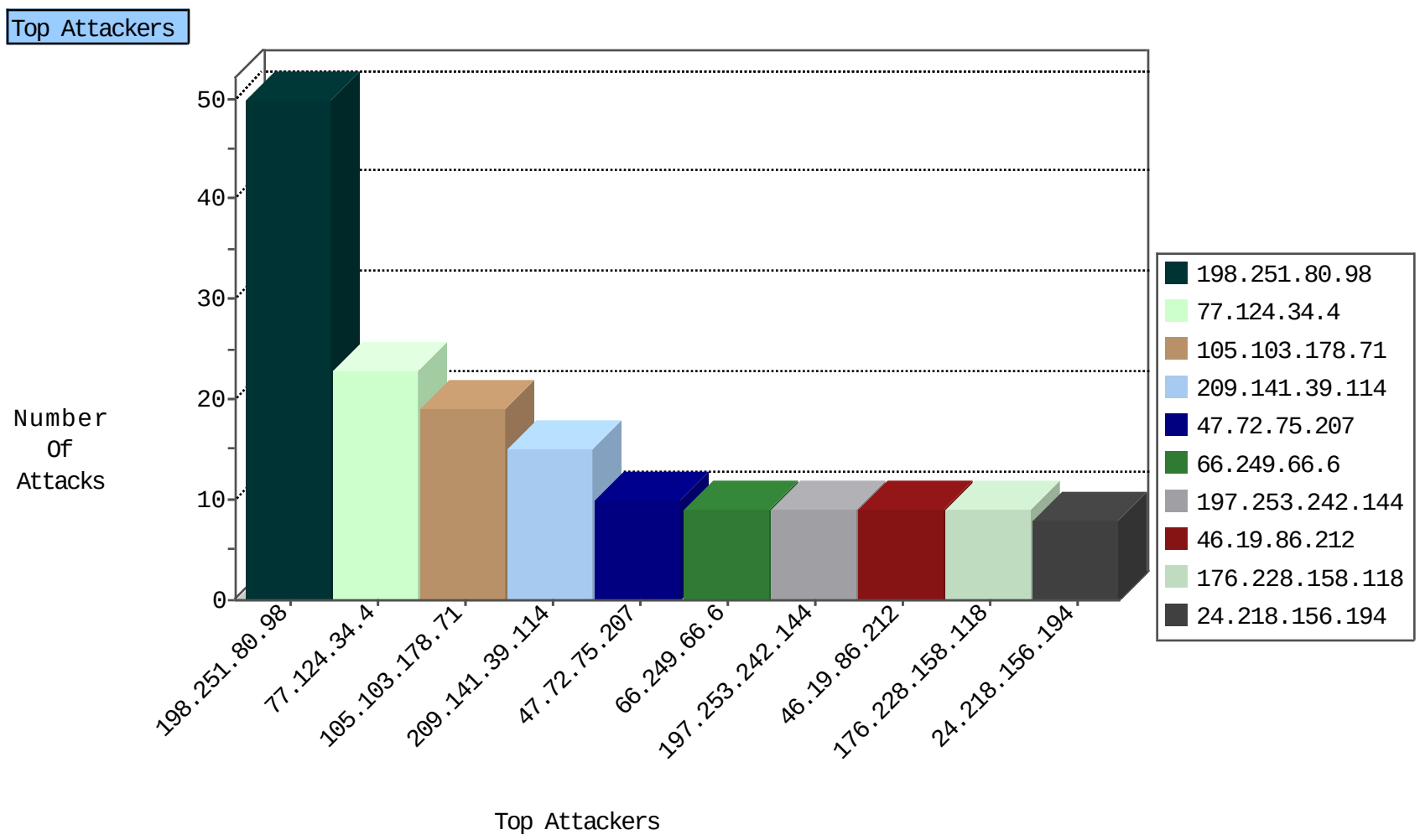
09-24-2016-00:04:04 to 09-24-2016-01:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-00:04:04 to 09-24-2016-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.i	Black List	drop	3
120.132.50.135	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
199.167.24.139	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
173.244.198.5	United States	147.237.76.176	test.ncore.idf.i	Black List	drop	1
45.32.193.80	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
77.124.34.4	Israel	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
104.238.146.105	United States	147.237.76.30	himush.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.30	himush.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
104.238.147.7	United States	147.237.76.176	test.ncore.idf.i	Black List	drop	1

09-24-2016-00:04:04 to 09-24-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4

09-24-2016-00:04:04 to 09-24-2016-01:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.253.242.144	147.237.77.216	Morocco	dover.idf.il	GPL SCAN nmap TCP	4
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.155	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
115.47.12.162	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
81.27.85.27	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.102.60.185	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.201	Algeria	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.197	Algeria	e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.148	Algeria	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
105.103.178.71	147.237.76.44	Algeria	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.34	Algeria	yohalan.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.30	Algeria	himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.178	Ukraine	e.matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
115.47.12.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.202	Algeria	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.200	Algeria	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.196	Algeria	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.161.56.12	147.237.77.216	India	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
105.103.178.71	147.237.76.86	Algeria	navy.idf.il	ET SCAN Potential SSH Scan	1
14.141.53.145	147.237.77.216	India	dover.idf.il	Tehila - Perl LWP with fake user agent	1
105.103.178.71	147.237.76.39	Algeria	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
105.103.178.71	147.237.76.31	Algeria	nakchal.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-00:04:04 to 09-24-2016-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.124.34.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.249.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.158.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
213.57.152.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.43.204.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
209.141.39.114	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
46.19.86.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
209.141.39.114	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
80.246.136.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.43.204.49	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
209.141.39.114	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.253.242.144	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.25	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.170.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.218.156.194	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
98.200.249.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.228.158.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
209.141.39.114	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
24.218.156.194	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
98.200.249.145	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.226.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
47.72.75.207	New Zealand	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.147.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
100.92.184.126		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.237.37	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
47.72.75.207	New Zealand	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
185.3.147.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.12.94.255	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
217.132.27.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.27.105.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
24.218.156.194	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
47.72.75.207	New Zealand	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
197.253.242.144	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
47.72.75.207	New Zealand	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.1.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
47.72.75.207	New Zealand	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.253.231.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
24.182.114.157	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
125.77.28.26	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-24-2016-00:04:04 to 09-24-2016-01:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.124.34.4	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.124.34.4	Block	5
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.232	Block	2
77.124.41.5	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.253.47.93	Spain	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
79.182.41.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
176.228.158.118	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
80.200.125.54	Belgium	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
179.7.91.56	Peru	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.62	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
109.253.135.192	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
180.76.15.11	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.108	Block	1
141.226.218.7	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2378.jpg	Block	1
213.57.152.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.40.10	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/iturim/asp/search.asp	None	1
157.55.39.32	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3467.jpg	Block	1

09-24-2016-00:04:04 to 09-24-2016-01:04:04