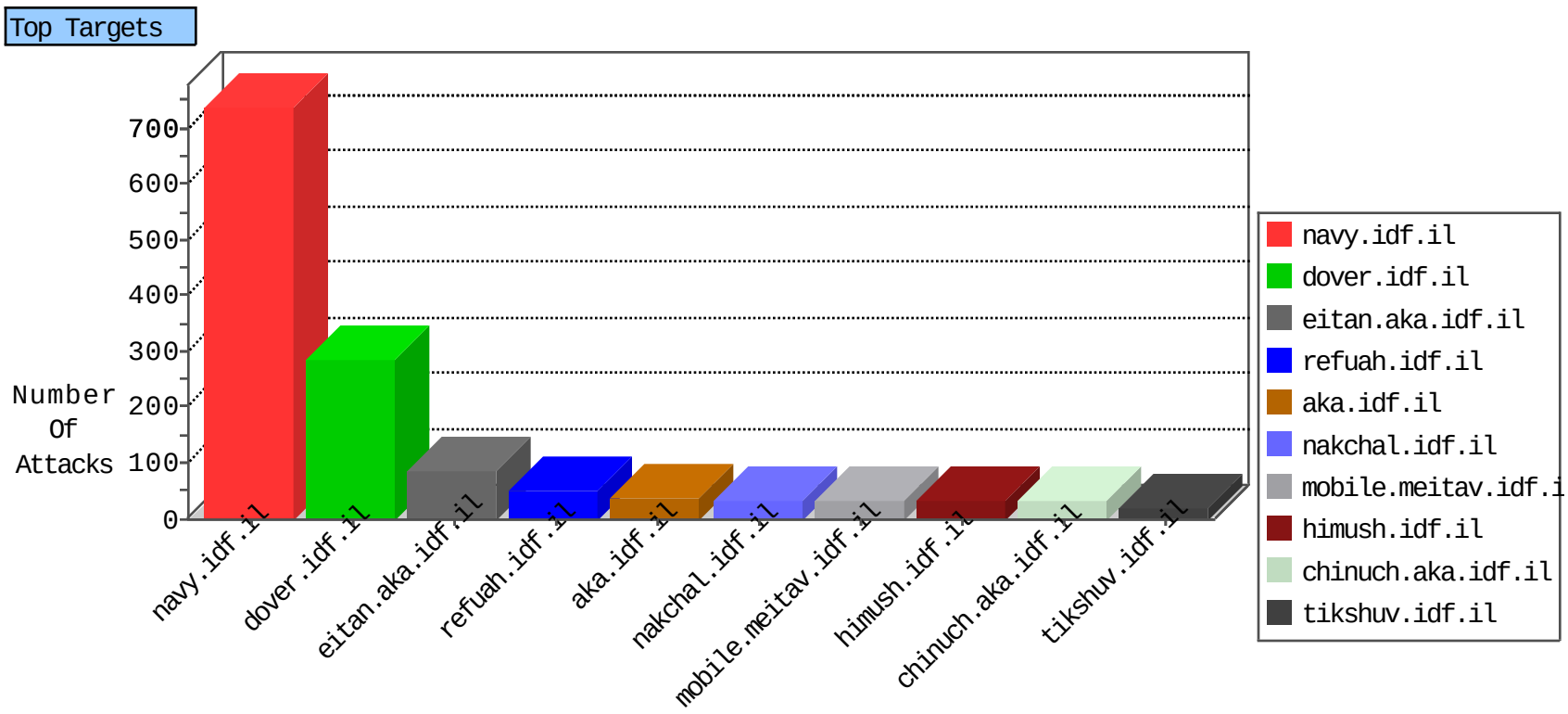
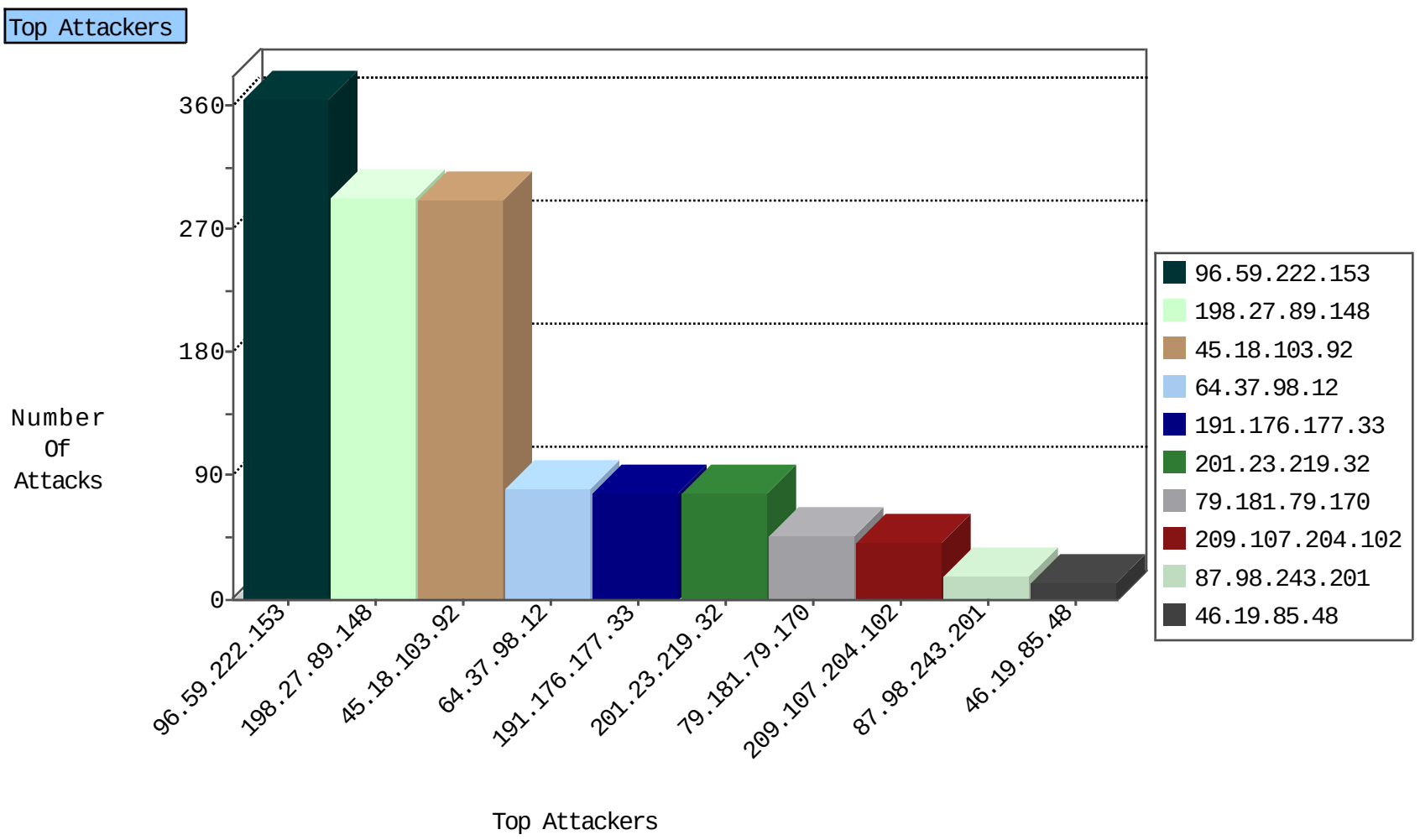
09-10-2016-02:04:03 to 09-10-2016-03:04:03

IDF Under Attack Daily Report





09-10-2016-02:04:03 to 09-10-2016-03:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
221.210.200.245	China	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
93.174.95.106	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1

09-10-2016-02:04:03 to 09-10-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.198.143.123	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.198.143.123	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-10-2016-02:04:03 to 09-10-2016-03:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.221.160	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
91.121.136.34	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
91.201.236.50	147.237.76.196	Ukraine	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.255.90.133	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.14.42.2	147.237.8.27	Bulgaria	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
195.88.208.193	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.216.44	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
69.24.208.162	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
85.14.42.2	147.237.8.27	Bulgaria	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
221.210.200.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.14.42.2	147.237.8.27	Bulgaria	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
195.88.208.193	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.216.37	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
139.162.225.219	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.102.9.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
93.158.203.147	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.172.71.251	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.200	Ukraine	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.92.20.154	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-10-2016-02:04:03 to 09-10-2016-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
96.59.222.153	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	366
45.18.103.92	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	292
201.23.219.32	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
191.176.177.33	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
79.181.79.170	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
198.27.89.148	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
198.27.89.148	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.27.89.148	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.155	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.27.89.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
198.27.89.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.27.89.148	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
198.27.89.148	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
198.27.89.148	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
198.27.89.148	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
209.107.204.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.27.89.148	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
198.27.89.148	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.134.235	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
209.107.204.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
198.27.89.148	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
198.27.89.148	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
198.27.89.148	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
198.27.89.148	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5

09-10-2016-02:04:03 to 09-10-2016-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.174.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
66.249.64.33	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2339.jpg	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Distributed Unknown HTTP Request Method	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	NULL Character in Header Name at	Block	1
87.12.200.87	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.64.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/935-4493-he/patzar.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Illegal Byte Code Character in Header Name	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9269-he/dover.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	NULL Character in Method [[#0]]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]]	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Illegal Byte Code Character in Method [[#0]]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]]	Block	1
68.180.228.162	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.253	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Abnormally Long Request method	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Multiple Illegal Byte Code Character in Method from 139.162.13.205	Block	1
68.180.230.33	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2356.jpg	Block	1
195.154.41.132	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Distributed Malformed URL	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.i	Multiple NULL Character in Method from 139.162.13.205	Block	1
77.139.163.207	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1

09-10-2016-02:04:03 to 09-10-2016-03:04:03