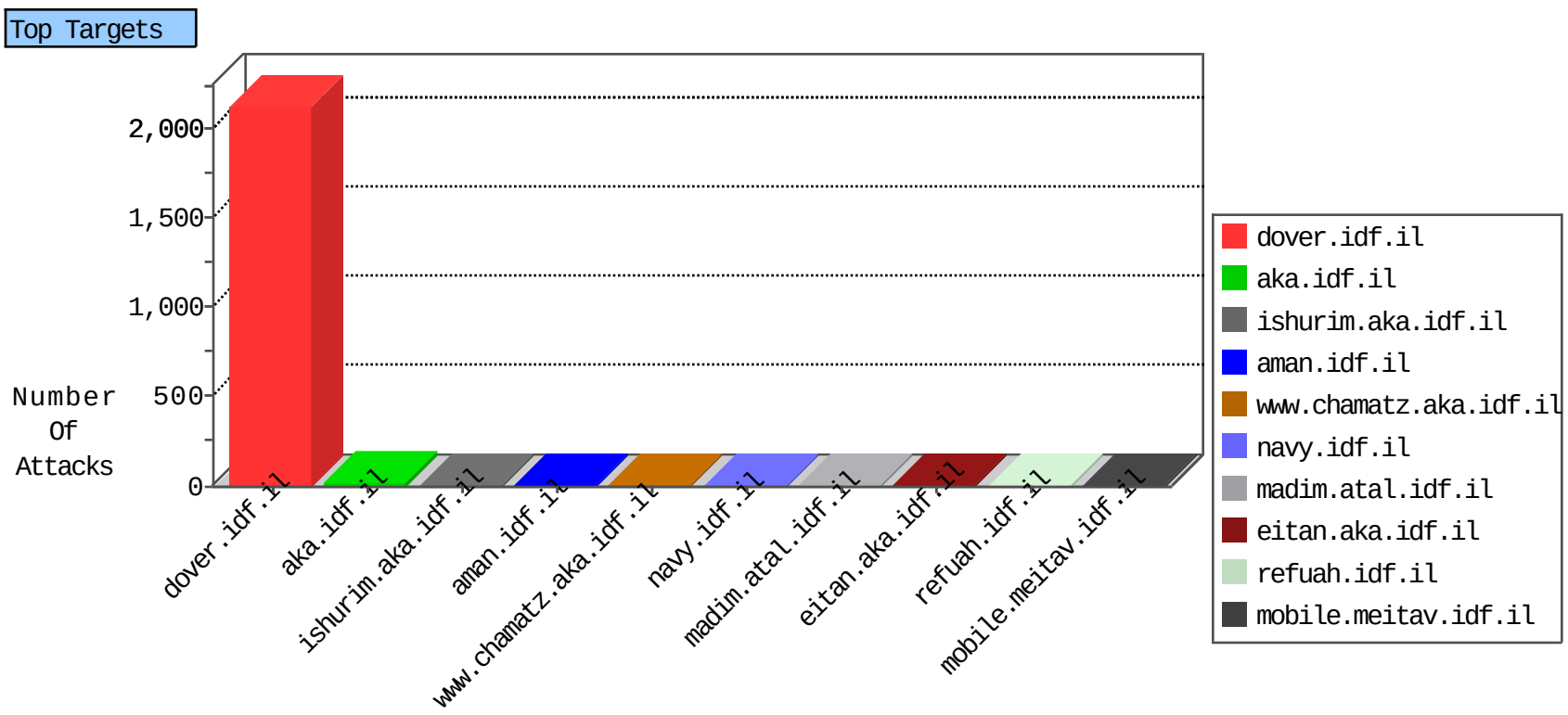
01-18-2016-04:04:00 to 01-18-2016-05:04:00

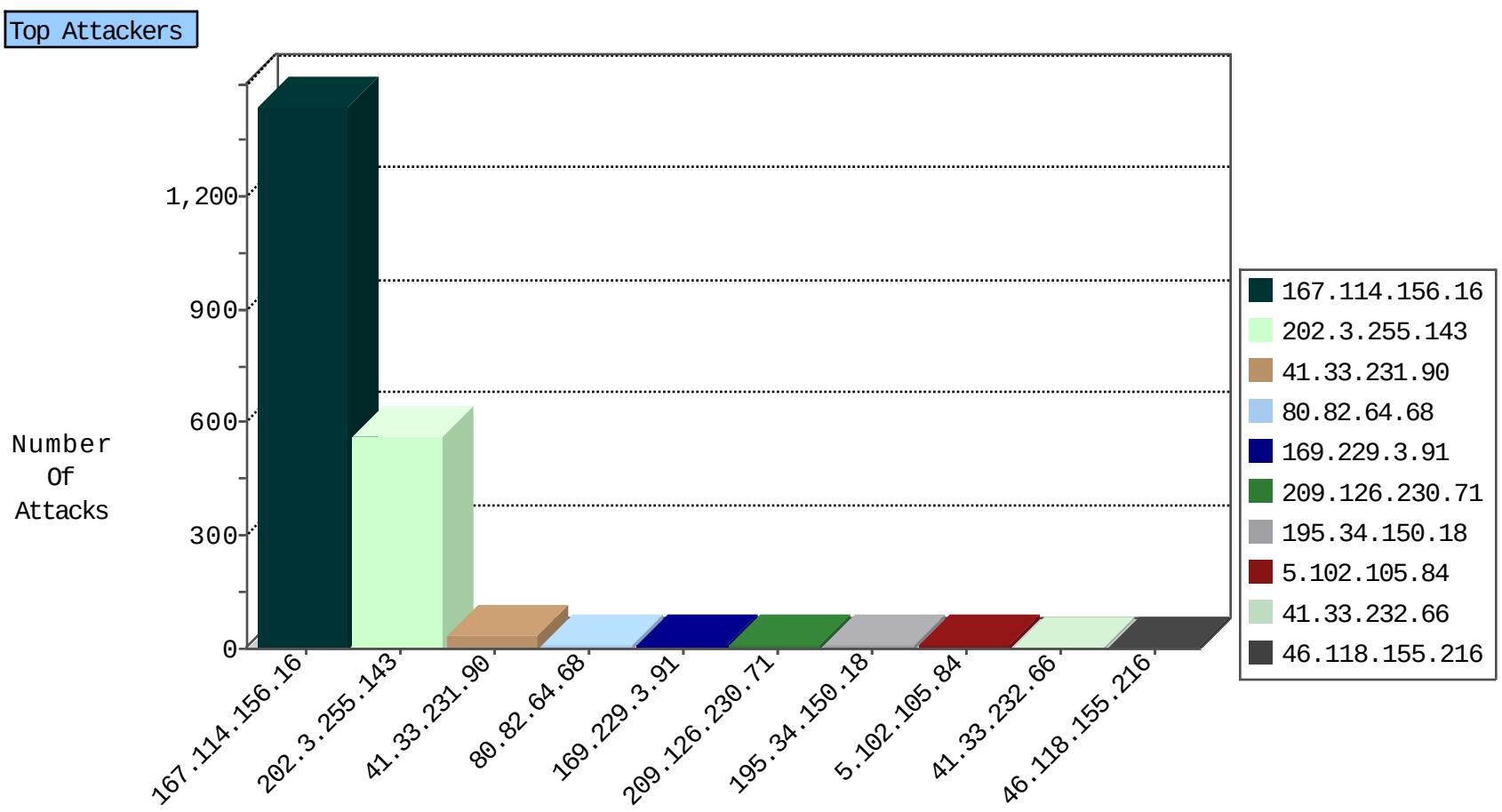
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-18-2016-04:04:00 to 01-18-2016-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3001
115.239.228.10	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
116.31.6.254	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-18-2016-04:04:00 to 01-18-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.144	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.98	France	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-18-2016-04:04:00 to 01-18-2016-05:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	528
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.75.110	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.75.110	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
209.126.230.71	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.75.110	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1

01-18-2016-04:04:00 to 01-18-2016-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.82.64.68	Netherlands	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
65.32.90.233	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
209.126.230.71	United States	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.59.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.6	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
5.102.105.84	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
125.46.26.253	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
5.102.105.84	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
49.229.57.241	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.90	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.48.80.73	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
209.126.230.71	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.22.135.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.64.68	Netherlands	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.50.210.164	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
67.80.56.251	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.34.238.100	Egypt	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
128.232.110.28	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.105.84	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.82.64.68	Netherlands	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
50.28.99.117	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.91	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
104.192.0.18	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
209.126.230.71	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
199.87.154.255	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
67.80.56.251	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.105.84	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
149.78.244.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.203.42	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.142.68.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
185.23.106.47	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
80.82.64.68	Netherlands	147.237.72.156	aman.idf.il	Unauthorized URL Access to qassam.ps/files/martyrs/37ee9280da.jpg	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/giyus/qanda/default.asp	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method Ã»ÂŒ)Âž[[#6]]ZÂ¨$Â‰ [[#31]]b*[[#4]]sÃ–a"~<gÃ‰ Ã?[[#25]]Â¼[[#31]][[#6]]Ã?Ã?2FuÃ±[[#25]]S<Ã·Â˜$XÂ?Ã″ [[#30]]sÂ¡[[#0]]	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
187.160.205.72	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.200	United States	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
80.82.64.68	Netherlands	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to qassam.ps/files/martyrs/37ee9280da.jpg	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/home	Block	1
195.154.227.118	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
31.13.110.126	Ireland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
157.55.39.225	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
209.126.230.71	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	NULL Character in Method Ã»ÂŒ)Âž[[#6]]ZÂ¨$Â‰[[#31]]b*[[#4]]sÃ–a"~<gÃ‰Ã?[[#25]]Â¼[[#31]][[#6]]Ã?Ã?2FuÃ±[[#25]]S<Ã·Â˜$XÂ?Ã″ [[#30]]sÂ¡[[#0]]	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
37.142.68.72	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
87.118.91.140	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
212.8.35.178	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Ã»ÂŒ)Âž[[#6]]ZÂ¨$Â‰ [[#31]]b*[[#4]]sÃ–a"~<gÃ‰ Ã?[[#25]]Â¼[[#31]][[#6]]Ã?Ã?2FuÃ±[[#25]]S<Ã·Â˜$XÂ?Ã″ [[#30]]sÂ¡[[#0]] in URL	Block	1
141.212.122.81	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

01-18-2016-04:04:00 to 01-18-2016-05:04:00