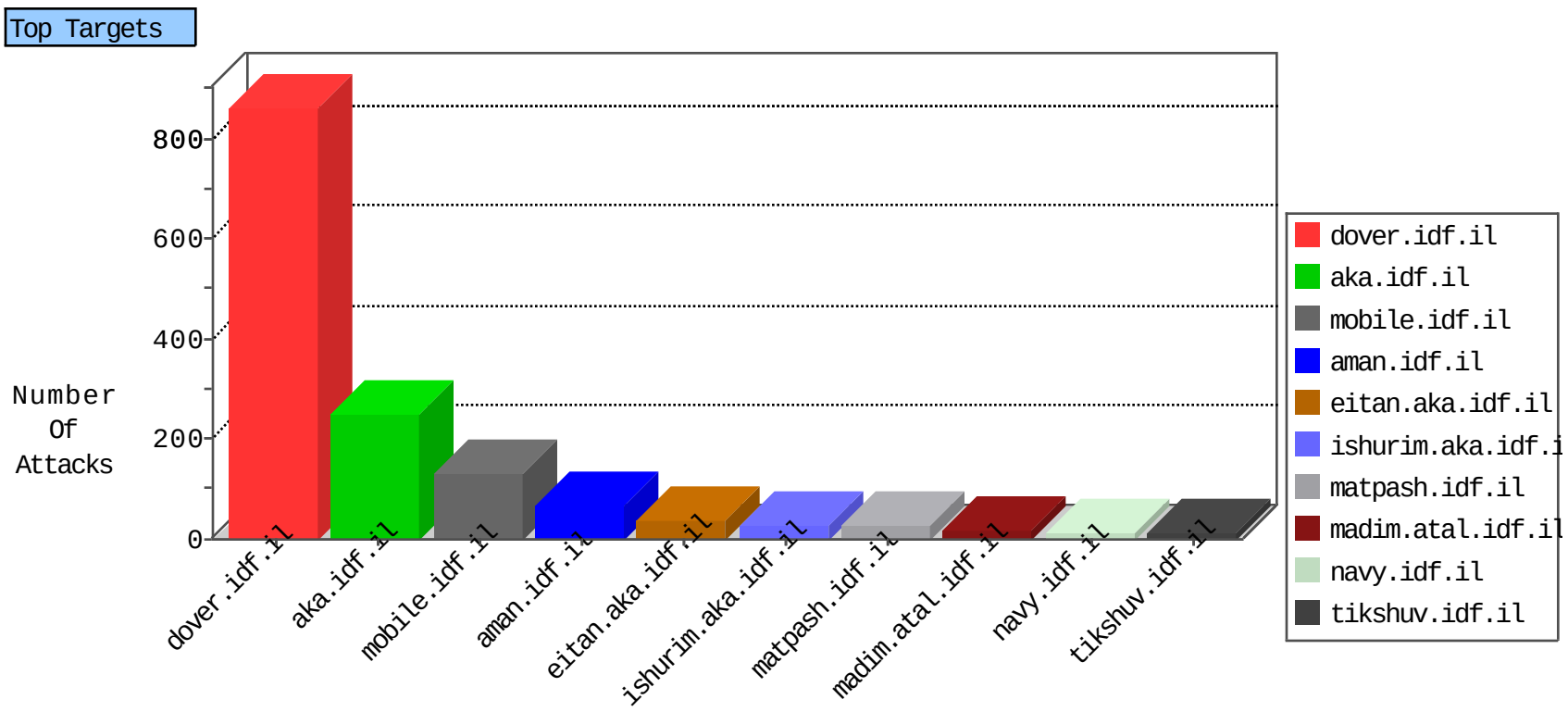
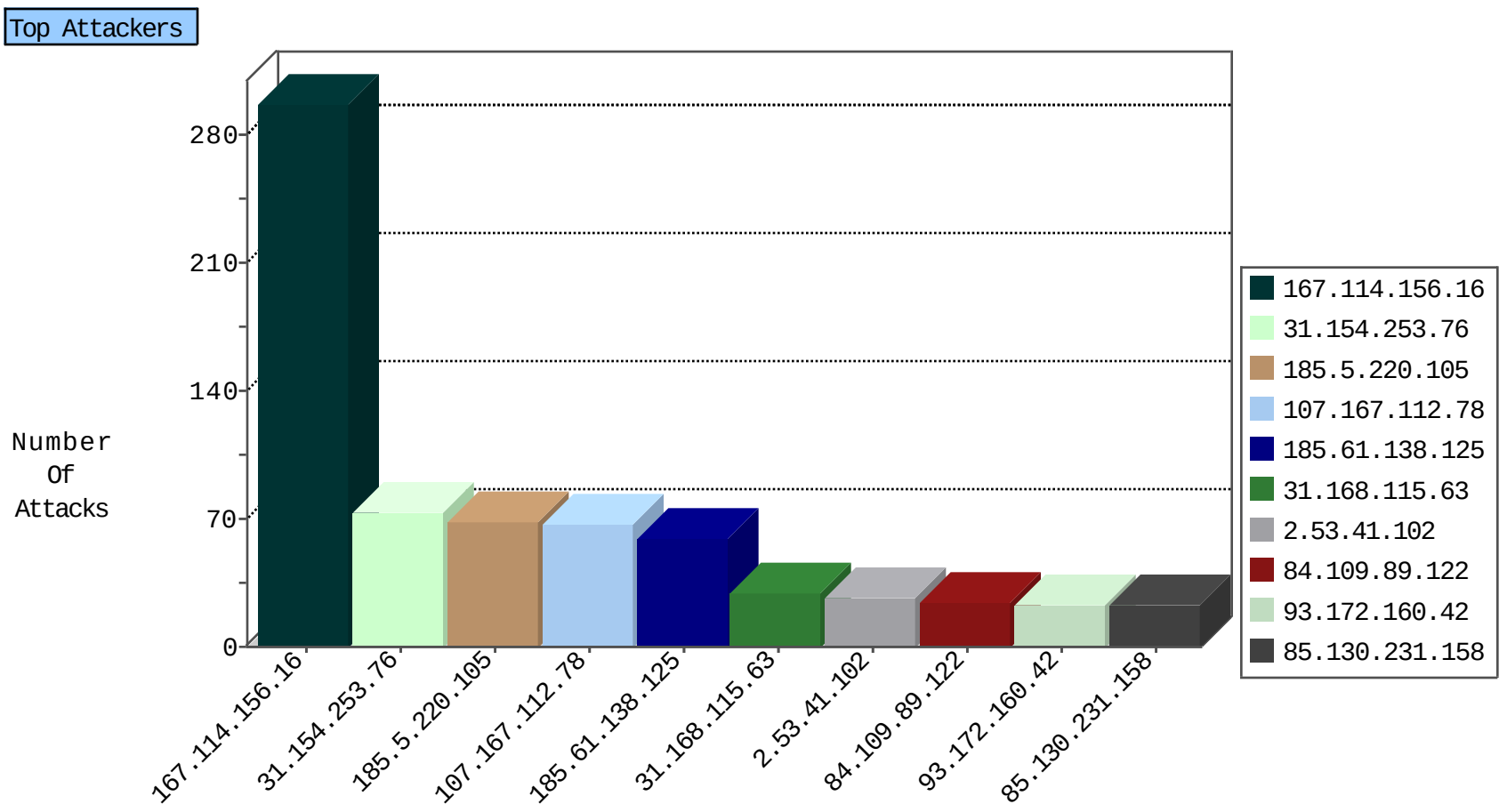
04-28-2016-10:04:05 to 04-28-2016-11:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-10:04:05 to 04-28-2016-11:04:05

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	HTTP-POST-Segmented-DoS	dest-reset	11446
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1627
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
222.186.21.61	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
172.82.142.122	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
123.249.27.29	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
172.82.142.122	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
153.226.43.202	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
190.253.212.51	Colombia	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-28-2016-10:04:05 to 04-28-2016-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.248.12.153	Netherlands	147.237.77.170	maarachot.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1

04-28-2016-10:04:05 to 04-28-2016-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
163.172.140.23	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.217.27.204	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.103.193	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
13.82.25.17	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
173.193.130.50	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.217.27.204	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -f -sS	1
13.92.103.193	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
173.193.130.50	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.140.23	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-10:04:05 to 04-28-2016-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.112.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
185.61.138.125	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
85.130.231.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
93.172.160.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
31.154.253.76	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
31.168.115.63	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
31.154.253.76	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
109.253.158.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.1.115.50	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.114.124.151	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
217.132.129.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.6.3.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.102.225.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.253.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
188.161.186.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.154.253.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
54.157.251.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.9.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.168.115.63	Israel	147.237.76.200	eitan.aka.idf.i	drop	First packet isn't SYN	drop	8
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.65.68.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.89.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.130.224.22	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.253.76	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
84.109.89.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.190.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.74	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.89.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.74	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.89.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.213.0.42	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

04-28-2016-10:04:05 to 04-28-2016-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.128.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
213.57.233.213	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	5
109.253.158.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.94.54.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.236	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.9.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.190.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20786-he/dover.aspx.	Block	2
157.55.39.106	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.106	Block	2
109.253.226.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.132.126.98	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
66.249.64.182	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name oy•ù[[#15]]p{1 üâ	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi .idf.il	Illegal Byte Code Character in Method ça	Block	1
46.19.85.40	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.61.138.125	Ukraine	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
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 12	Block	1
89.138.121.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
149.78.146.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Too Many Headers per Request - 30 Headers	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi .idf.il	Illegal Byte Code Character in URL	Block	1
46.19.86.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Malformed URL …™i[[#24]]•zp‘;ח1[[מ)#21]]1″וב iv"h¾fšrt»¸„f<’¸[[„:>ר#21oŸ]]•ר!¯>[–ו4ד]]2#[[’„]]5#[[ƒl‡ɔʊ°¬¸†ûÿ>]]6#[[z–t[[#28]]¸[[#30]][[#7]]¶×ɔDq;¸'/¢•	Block	1
93.172.160.42	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage	Block	1
46.121.209.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ïŒÛV˜¿îùûŸØä7K™[[#2]][-[[#18]]©ÌŒ<2[[#1]]’[[#11]]´[[#25]]ü{yï[[#3]];Å[[#21]]æ[[#21]]º÷[[#24]]=[[#14]]Û†•ª‹[[#0]]ƒ"[[#30]]z˜\í2ýýCé}[[#4]]N)[[#19]]•Â±Aa¯“Ü in URL …™i[[#24]]•zp‘	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method ïŒÛV˜¿îùûŸØä7K™[[#2]][-[[#18]]©ÌŒ<2[[#1]]’[[#11]]´[[#25]]ü{yï[[#3]];Å[[#21]]æ[[#21]]º÷[[#24]]=[[#14]]Û†•ª‹[[#0]]ƒ"[[#30]]z˜\í2ýýCé}[[#4]]N)[[#19]]•Â±Aa¯“Ü	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71709.pdf	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi .idf.il	Unknown HTTP Request Method ça in URL	Block	1
46.120.160.160	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 46.120.160.160	Block	1
2.53.22.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	NULL Character in Header Name at ÓîºÖ%•u¢fêÐ~ym[[#31]]G[[#6]]±éI#Úu¼[[#5]]_[[#15]][[#19]]Ú¡[[#25]]ÿ″[[#16]]Õ[[#29]]ª³[[#17]]Â&šb’«Ù‹½‡^[[#21]]g‡’«(v³«¶.t0áIb•[[#11]]Wæ´8«/è!ÑýçËçã[[#29]]jn@•“˜ÁÑ‰‡¾ŸúÝ[[#25]]£[[#30]]cí[[#28]]x×´'g[[#5]]oý[[#31]]•ÙRï1ºÆBö[[#18]]«§Ù[[#16]]À[[#16]]S\0´[[#2]]›YÈ¢š%[[#3]]#012fÝ¦5ã[[#19]]¨*4$®=-[[#31]]M«–O3¸é’tUL[[#5]]~øƒÌ³	Block	1
105.203.254.5	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.208.151.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/dover.aspx|’½¿|’×’₪’½¿	Block	1
37.26.148.130	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
130.185.155.10	Sweden	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.6.17.144	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
185.5.220.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL …™i[[#24]]•zp‘;ח1[[מ)#21]]1″וב iv"h¾fšrt»¸„f<’¸[[„:>ר#21oŸ]]•ר!¯>[–ו4ד]]2#[[’„]]5#[[ƒl‡ɔʊ°¬¸†ûÿ>]]6#[[z–t[[#28]]¸[[#30]][[#7]]¶×ɔDq;¸'/¢•	Block	1

04-28-2016-10:04:05 to 04-28-2016-11:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
46.120.160.160	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7535-	Block	1
2.53.41.102	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

04-28-2016-10:04:05 to 04-28-2016-11:04:05