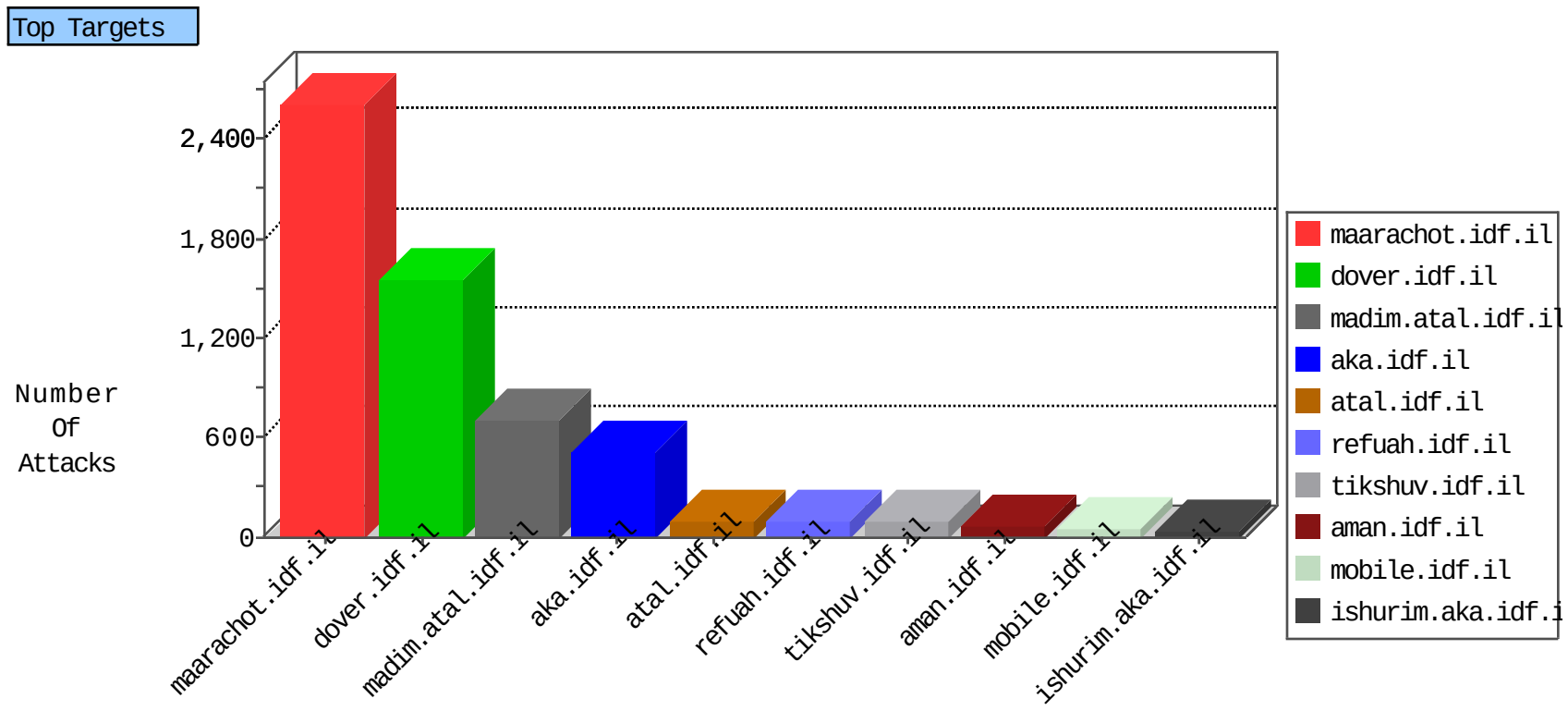
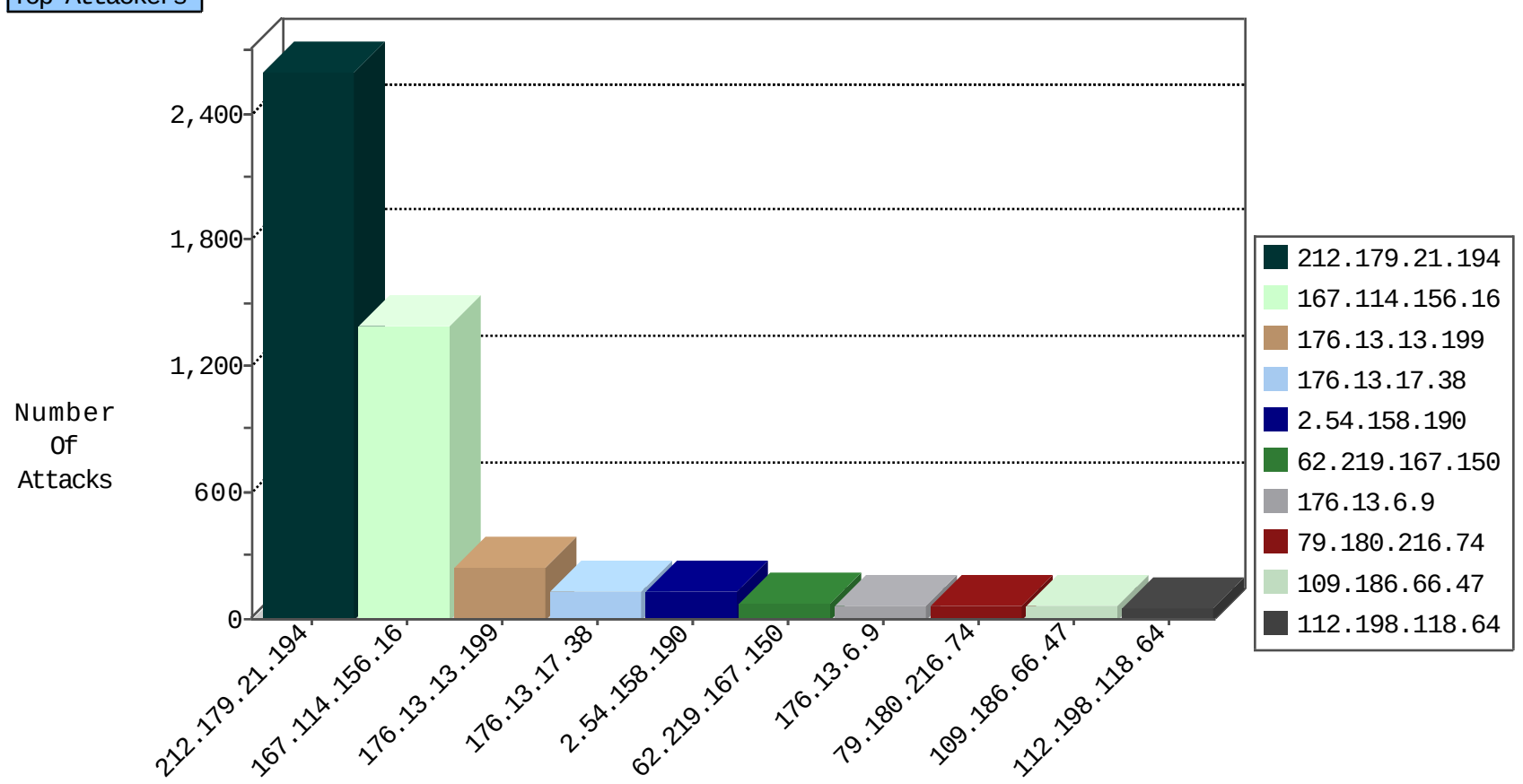
01-10-2016-12:04:05 to 01-10-2016-13:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-10-2016-12:04:05 to 01-10-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3902
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3075
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

01-10-2016-12:04:05 to 01-10-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.75	United States	147.237.77.212	e.dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-10-2016-12:04:05 to 01-10-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
172.98.200.238	147.237.76.148		gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
149.88.202.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.8.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.26.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.76.148		gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
93.174.93.203	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
80.246.137.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

01-10-2016-12:04:05 to 01-10-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2602
79.180.216.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
62.219.167.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
62.219.167.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
85.114.117.169	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
85.64.36.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
109.253.206.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.19.85.238	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.206.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.206.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
149.78.135.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.166.57.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
46.19.85.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
79.176.139.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.63.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.241.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.73.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.219	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.154.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
62.219.167.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.182.35.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.163.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
89.138.194.223	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.245	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.87.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.45	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.194.223	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.169	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.136.123	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.96.128	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
46.121.134.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.39.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.77	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.14	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
2.54.137.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
2.54.158.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
176.13.17.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
176.13.13.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
176.13.6.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
109.186.66.47	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
176.13.17.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
2.52.180.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
87.68.161.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.158.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
79.181.36.80	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.36.80	Block	12
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
31.210.187.250	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	7
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	5
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	4
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.118.64	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.118.64	Block	3
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.158.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.118.64	Block	3
176.13.4.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.210.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.235.83.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/3/	Block	3
80.179.7.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.7.63	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.118.64	Block	3
212.235.83.202	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.83.202	Block	3
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.180.154.105	Block	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.118.64	Block	2
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.199.53.226	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.54.46.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 79.180.154.105	Block	2
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 79.180.154.105	Block	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.118.64	Block	2
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.31.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 79.180.154.105	Block	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.180.139.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m×˜×™× ×˜×’×¨×œ×™ ×?ain/giyus/general.aspx	Block	2
109.253.196.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 79.180.154.105	Block	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.118.64	Block	2
79.180.154.105	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 79.180.154.105	Block	2
46.19.85.59	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.218.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2