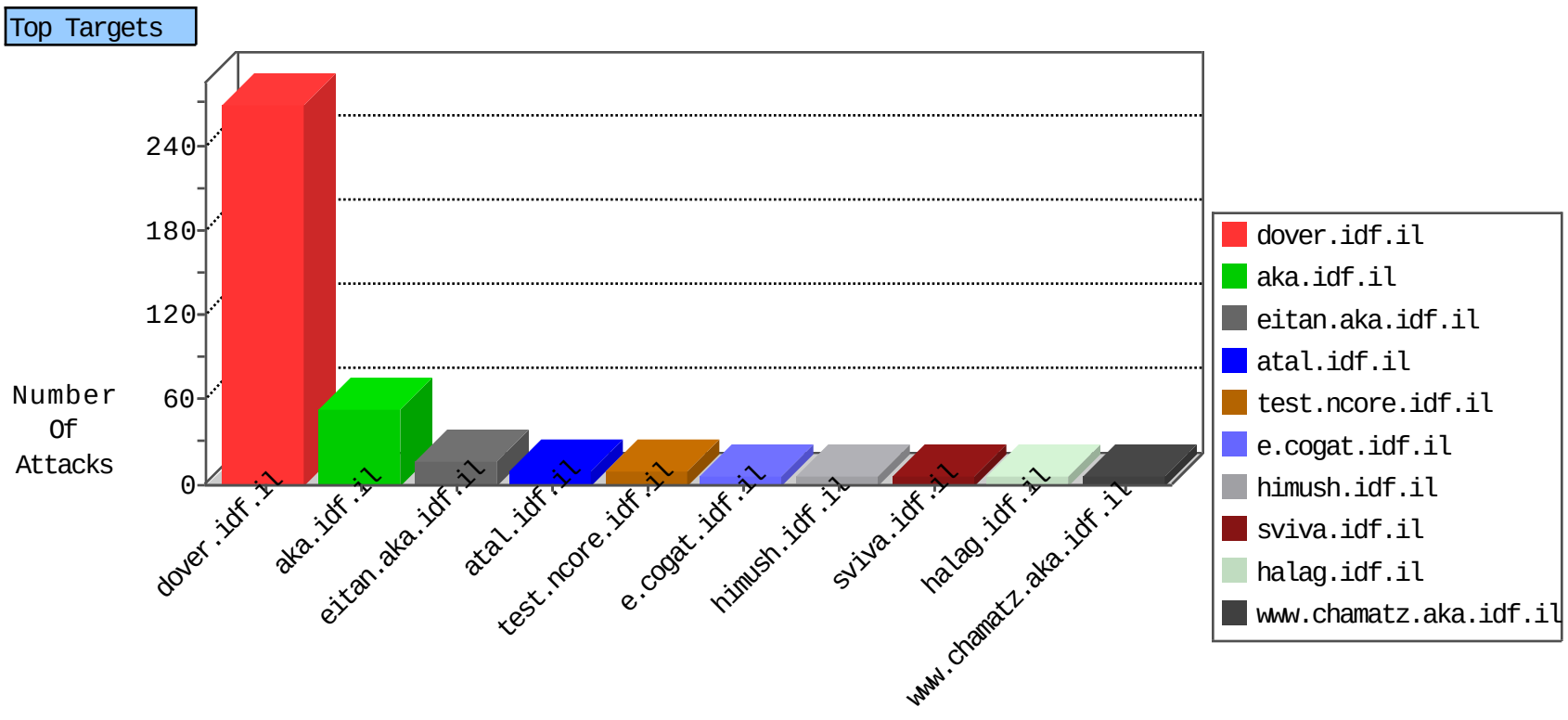
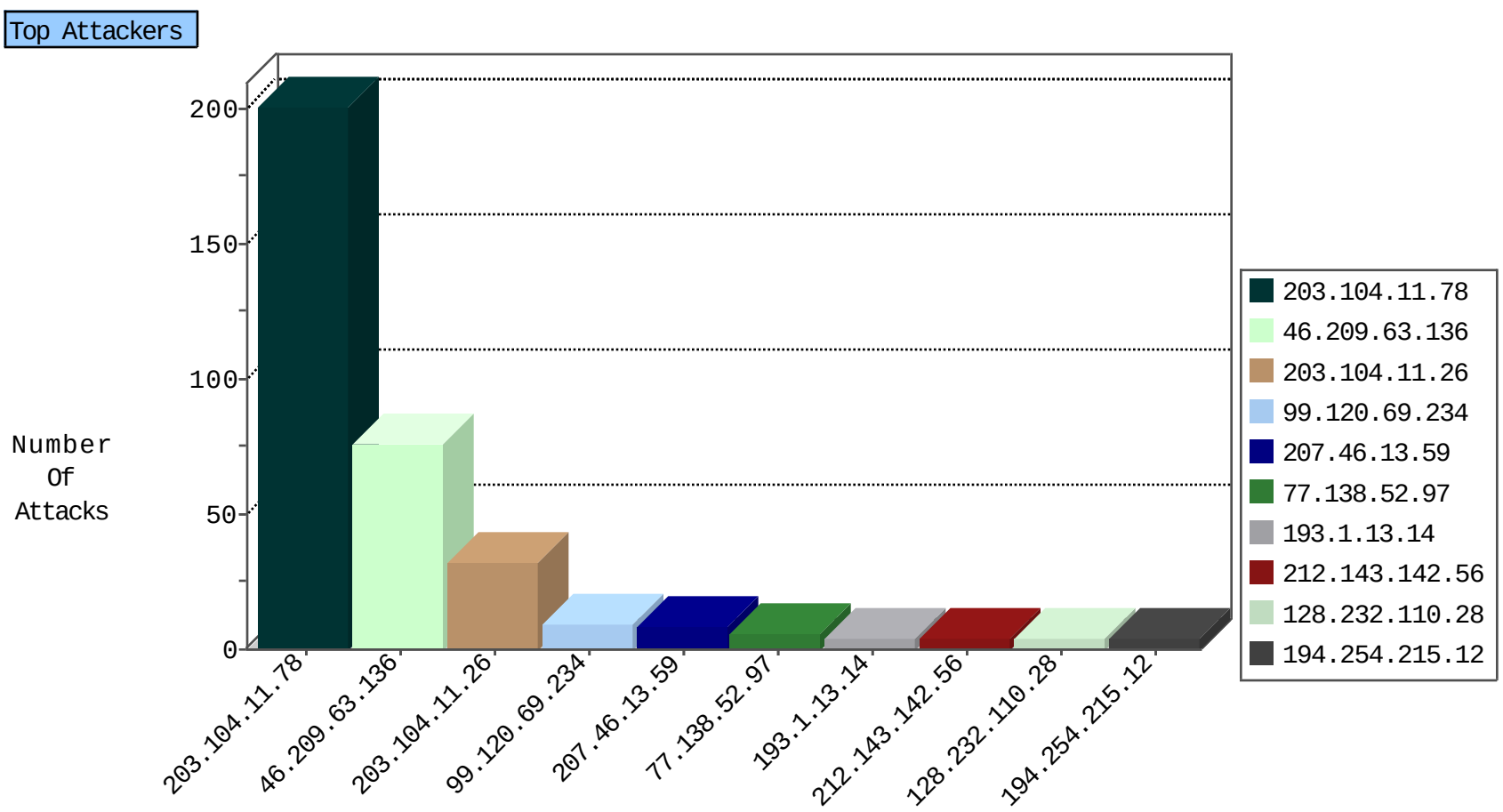
09-12-2016-05:04:06 to 09-12-2016-06:04:06

IDF Under Attack Daily Report





09-12-2016-05:04:06 to 09-12-2016-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
203.104.11.78	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.226	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

09-12-2016-05:04:06 to 09-12-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.69.74	United States	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-12-2016-05:04:06 to 09-12-2016-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.209.63.136	147.237.77.235	Iran, Islamic Republic of	sviva.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.77.233	Iran, Islamic Republic of	atal.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.76.200	Iran, Islamic Republic of	eitan.aka.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.76.176	Iran, Islamic Republic of	test.ncore.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.77.234	Iran, Islamic Republic of	halag.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.77.226	Iran, Islamic Republic of	www.chamatz.aka.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET DOS SSL Bomb DoS Attempt	4
46.209.63.136	147.237.76.30	Iran, Islamic Republic of	himush.idf.il	ET DOS SSL Bomb DoS Attempt	4
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
99.120.69.234	147.237.72.166	United States	aka.idf.il	ET WEB_SERVER Poison Null Byte	1
222.186.58.197	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.197	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.2.0.135	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.177	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.209.63.136	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.58.197	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.2.0.135	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
218.2.0.135	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-12-2016-05:04:06 to 09-12-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
203.104.11.78	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	200
203.104.11.26	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
207.46.13.59	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.209.63.136	Iran, Islamic Republic of	147.237.77.234	halag.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
172.56.38.112	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
128.232.110.28	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.200	eitan.aka.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
181.211.16.148	Ecuador	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.176	test.ncore.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.235	sviva.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.233	atal.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.111.62.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.61	e.cogat.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
128.232.110.28	United Kingdom	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.209.63.136	Iran, Islamic Republic of	147.237.77.226	www.chamatz.aka.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
46.209.63.136	Iran, Islamic Republic of	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
190.183.60.253	Argentina	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
95.59.136.118	Kazakstan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
131.253.27.100	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.183.50.161	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.243.55.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.89	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.107	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.65.112.122	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.211	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.111.62.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
198.20.69.74	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.90	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.209.63.136	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
115.230.125.146	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.84	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-12-2016-05:04:06 to 09-12-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.138	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method q[[#0]][[#0]][[#0]][[#23]]¤VÆ‰š6®[[#25]]áì•¿Ä[[#28]]ç	Block	1
46.116.22.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method q[[#0]][[#0]][[#0]][[#23]]¤VÆ‰š6®[[#25]]áì•¿Ä[[#28]]ç in URL °'+Ý¬Ûd•5¯n©¤×x©	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/69845.pdf	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL °'+Ý¬Ûd•5¯n©¤×x©;[[#21]]	Block	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.209.63.136 (Unsupported Cipher)	None	1
104.162.133.48	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
46.209.63.136	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
186.77.192.159	Nicaragua	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Malformed URL °'+Ý¬Ûd•5¯n©¤×x©;[[#21]]	Block	1
58.10.55.65	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
99.120.69.234	United States	147.237.72.166	aka.idf.il	NULL Character in Method q[[#0]][[#0]][[#0]][[#23]]¤VÆ‰š6®[[#25]]áì•¿Ä[[#28]]ç	Block	1
66.249.66.56	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1

09-12-2016-05:04:06 to 09-12-2016-06:04:06