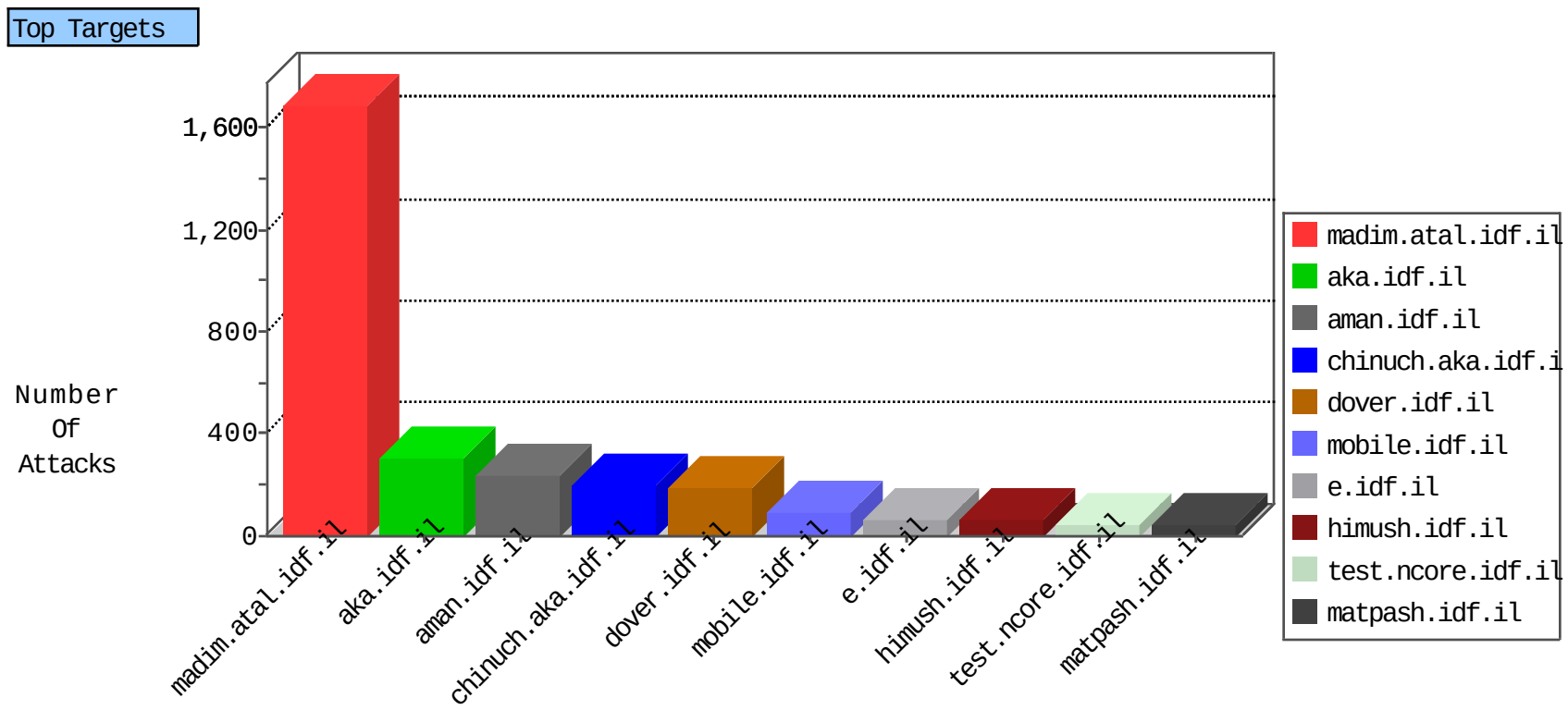
01-26-2016-09:04:07 to 01-26-2016-10:04:07

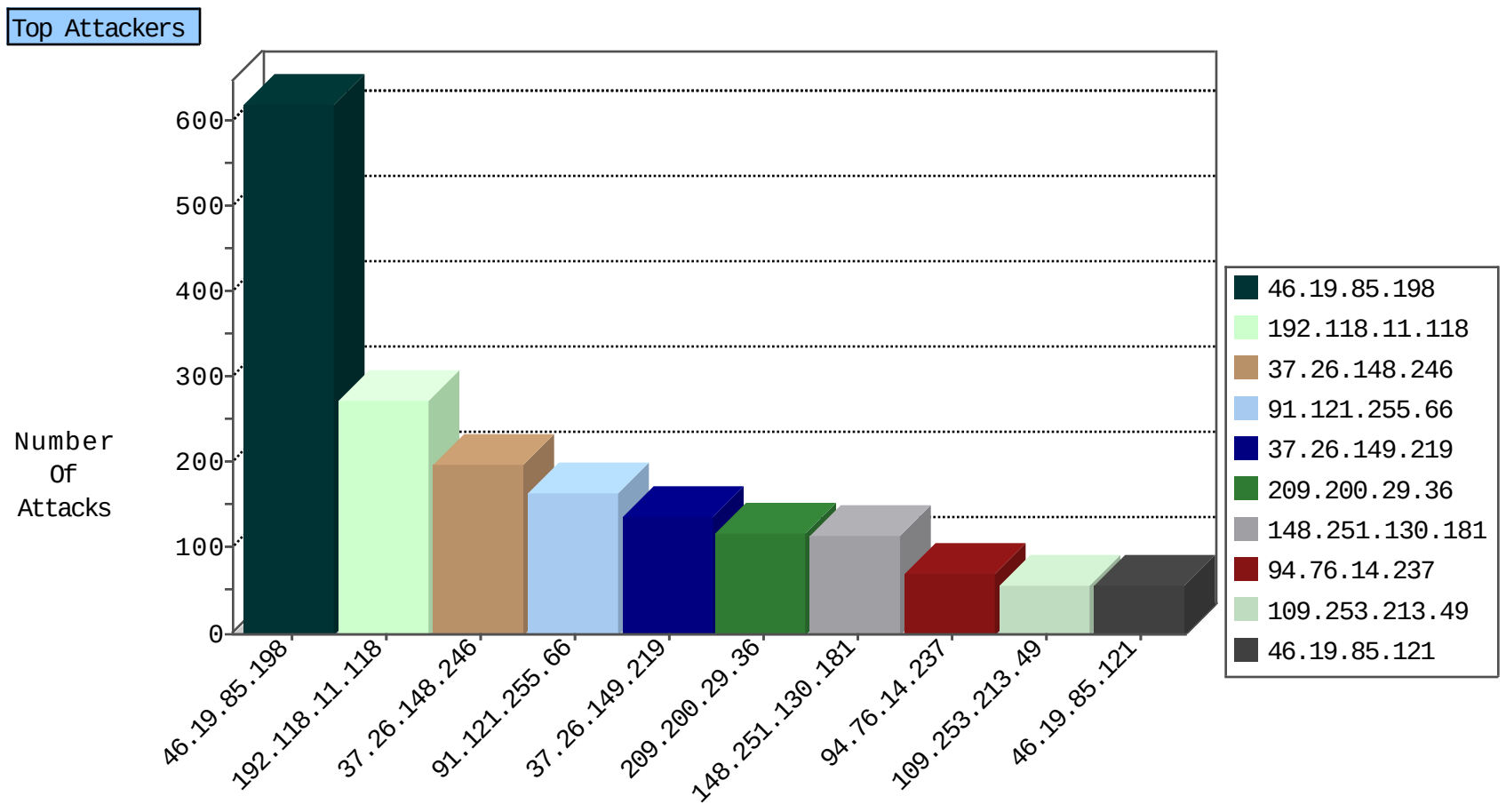
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-09:04:07 to 01-26-2016-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
94.76.10.253	Bahrain	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
183.56.159.141	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.58	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

01-26-2016-09:04:07 to 01-26-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.108.170.158	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	3
94.76.10.253	Bahrain	147.237.77.216	dover.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
136.243.103.165	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

01-26-2016-09:04:07 to 01-26-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.76.14.237	147.237.76.176	Bahrain	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	4
94.76.10.253	147.237.77.216	Bahrain	dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.18.162	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
94.76.14.237	147.237.77.226	Bahrain	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.10.253	147.237.77.226	Bahrain	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.233.76.49	147.237.77.74	Russian Federation	law.idf.il	Tehila - Perl LWP with fake user agent	1
77.125.89.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.77.233	Hong Kong	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.18.162	147.237.76.196	Lithuania	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.76.14.237	147.237.77.227	Bahrain	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-09:04:07 to 01-26-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	82
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	71
94.76.14.237	Bahrain	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	64
209.200.29.36	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
209.200.29.36	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
148.251.130.181	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
148.251.130.181	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.8.38	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
176.13.8.38	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
94.76.10.253	Bahrain	147.237.76.176	test.ncore.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	20
94.76.10.253	Bahrain	147.237.76.176	test.ncore.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.54.168.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.169.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
172.56.16.124	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.66.122.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.66.122.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	11
46.19.86.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.179.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.139.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.218.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.173.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.179.218.166	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
212.179.218.166	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.177.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.169.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.0.242.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.174	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.76	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.155.251	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.218.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.81.49.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.101	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.136.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

01-26-2016-09:04:07 to 01-26-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	397
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
192.118.11.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
37.26.148.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
192.118.11.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	79
37.26.148.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
109.253.213.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
212.150.82.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	50
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
80.246.136.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
89.139.155.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
192.118.11.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	29
84.109.119.147	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	26
46.210.212.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
109.253.207.221	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	11
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	11
2.54.12.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.217.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 80.179.223.31	Block	6
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	6
37.26.148.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.178.239.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.9.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.6.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.187.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	3
213.57.93.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
109.253.139.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.165.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.168.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.233.76.49	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	2
31.44.130.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/&sa=u&ved=0ahukewjdkox_gmfkahufkywkhcz7ae0qfgghmaa&usg=afqjcngtye6ot01bsuxslf0zyszjzlzzqw	Block	2
212.150.82.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
85.233.76.49	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-admin/admin-ajax.php	Block	2
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.247.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.19.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.144.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2

01-26-2016-09:04:07 to 01-26-2016-10:04:07