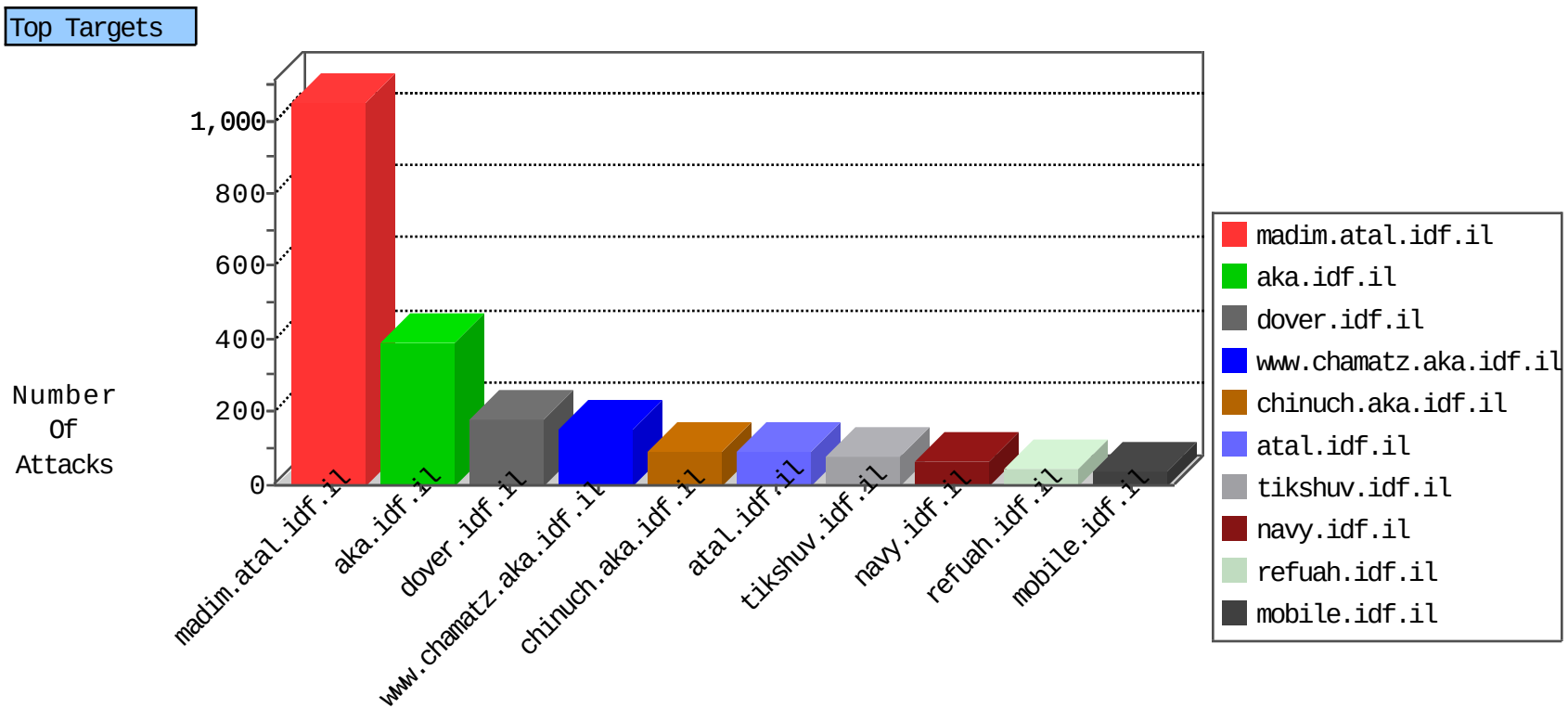
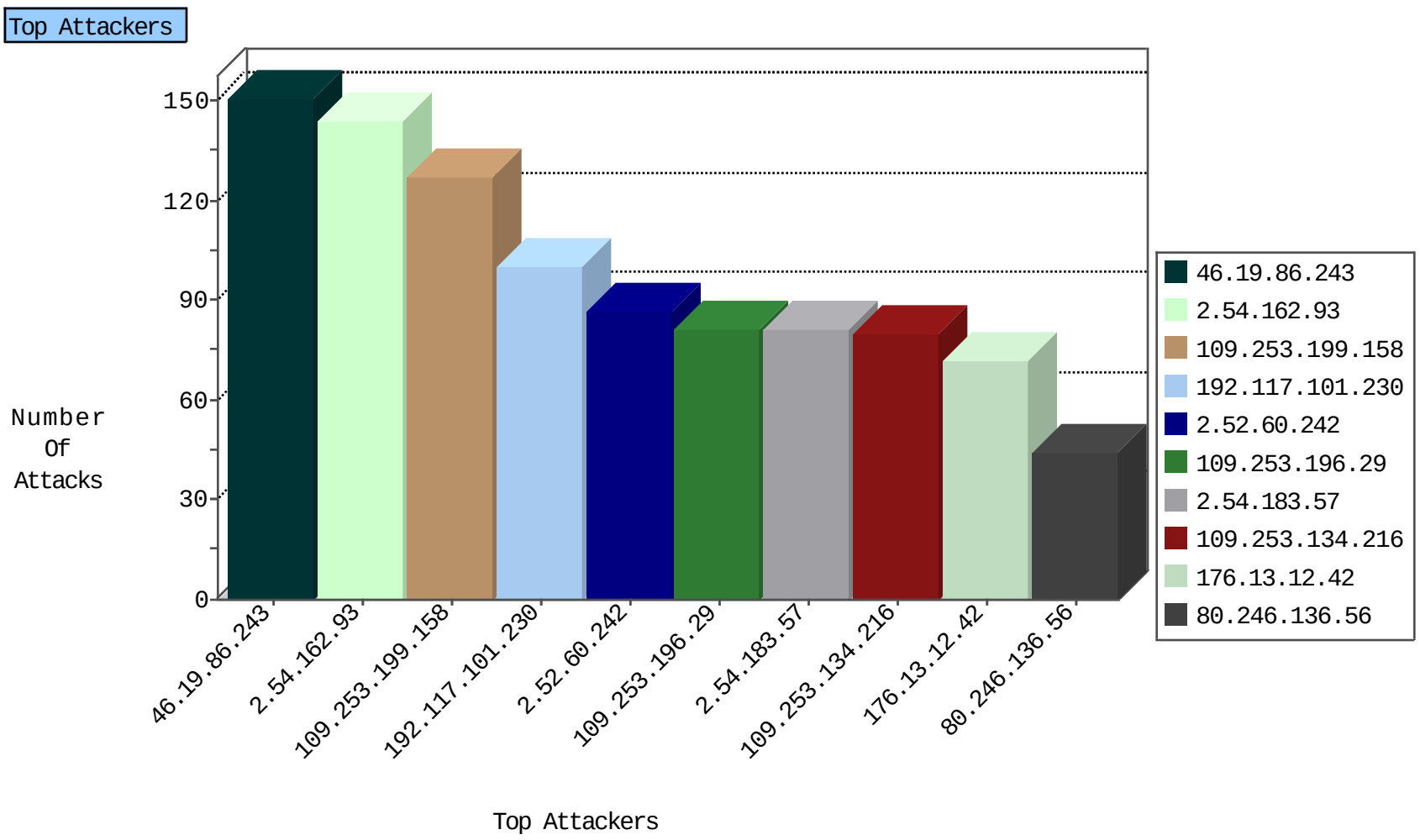
01-28-2016-14:04:06 to 01-28-2016-15:04:06

IDF Under Attack
Daily Report





01-28-2016-14:04:06 to 01-28-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	548
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
79.176.58.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.166.20.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.142.182.119	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
149.78.47.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-28-2016-14:04:06 to 01-28-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
171.8.152.200	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

01-28-2016-14:04:06 to 01-28-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	10
192.115.67.2	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
185.27.105.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.255.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
140.242.217.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.138.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.209.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.215.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.144.224	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
185.32.179.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
149.78.12.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.190.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.244.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.99.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.185.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-28-2016-14:04:06 to 01-28-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.162.93	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.60.242	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
79.177.16.23	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
84.95.134.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
198.100.144.55	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
84.95.134.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
176.13.17.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
84.95.215.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
176.13.17.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
109.160.169.246	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
109.160.169.246	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.116.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.14.47	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.0.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.198.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
12.222.13.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.154.171.51	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.154.171.51	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.171.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.168.89.105	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
176.13.0.212	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.0.212	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.6.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.237.113	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.13.109.120	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
217.194.194.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
62.219.233.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.54	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.16.23	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
82.145.216.176	Europe	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.28.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.138.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.108.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.29.35.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.0.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-28-2016-14:04:06 to 01-28-2016-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.199.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
192.117.101.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
109.253.196.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
176.13.12.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
109.253.134.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.183.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
84.111.32.88	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.32.88	Block	43
80.246.136.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.53.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.6.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.2.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.49.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.54.183.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.243	Block	23
109.253.199.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
109.253.134.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
62.128.35.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
2.52.132.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.17.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.132.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.4.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.15.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
149.78.196.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.196.28	Block	5
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	4
109.253.217.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.26.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.58.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.116.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.116.52	Block	2
2.54.142.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.22.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.154.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.152.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
164.138.127.158	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 164.138.127.158	Block	2
176.13.0.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.164.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.22.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.87.192	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.87.192	Block	2
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.58.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
46.60.40.25	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2

01-28-2016-14:04:06 to 01-28-2016-15:04:06