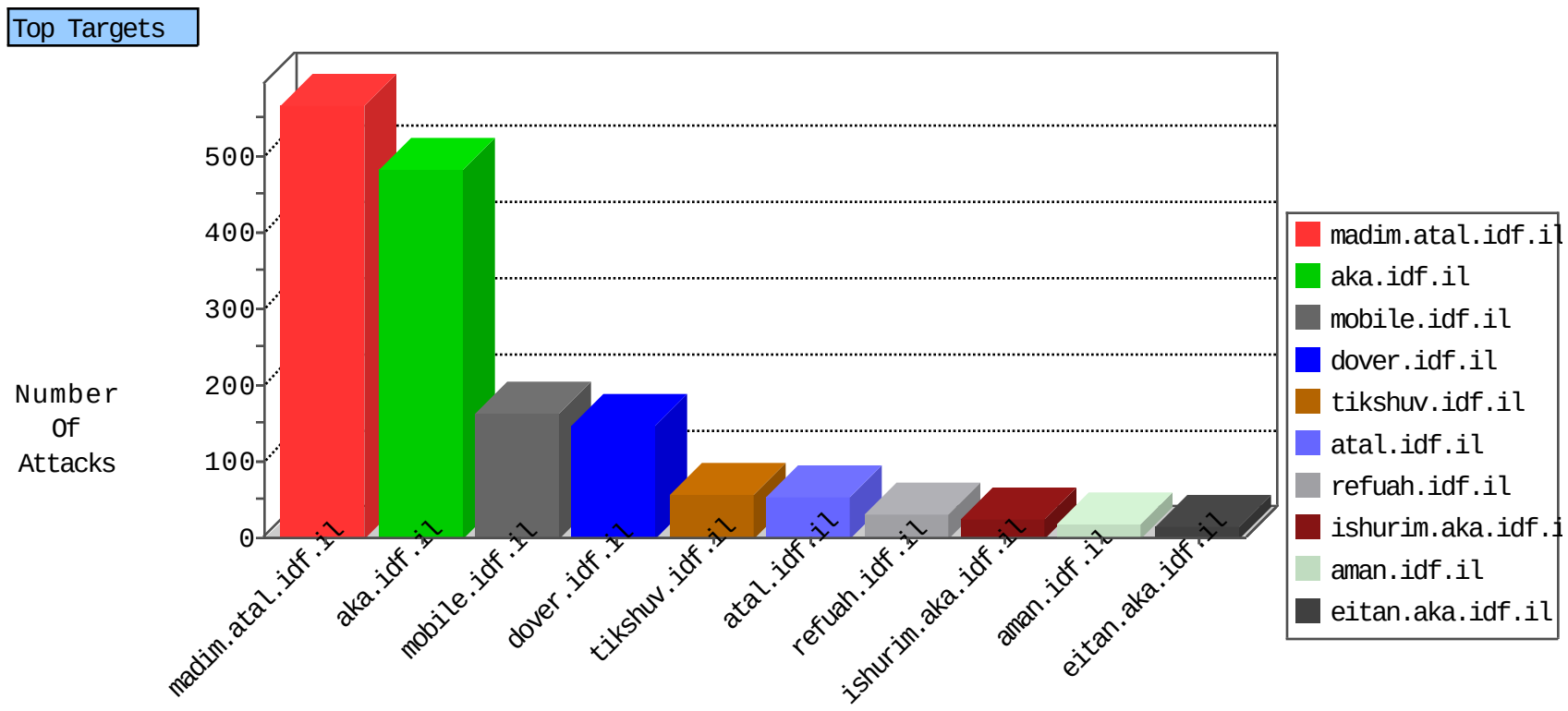
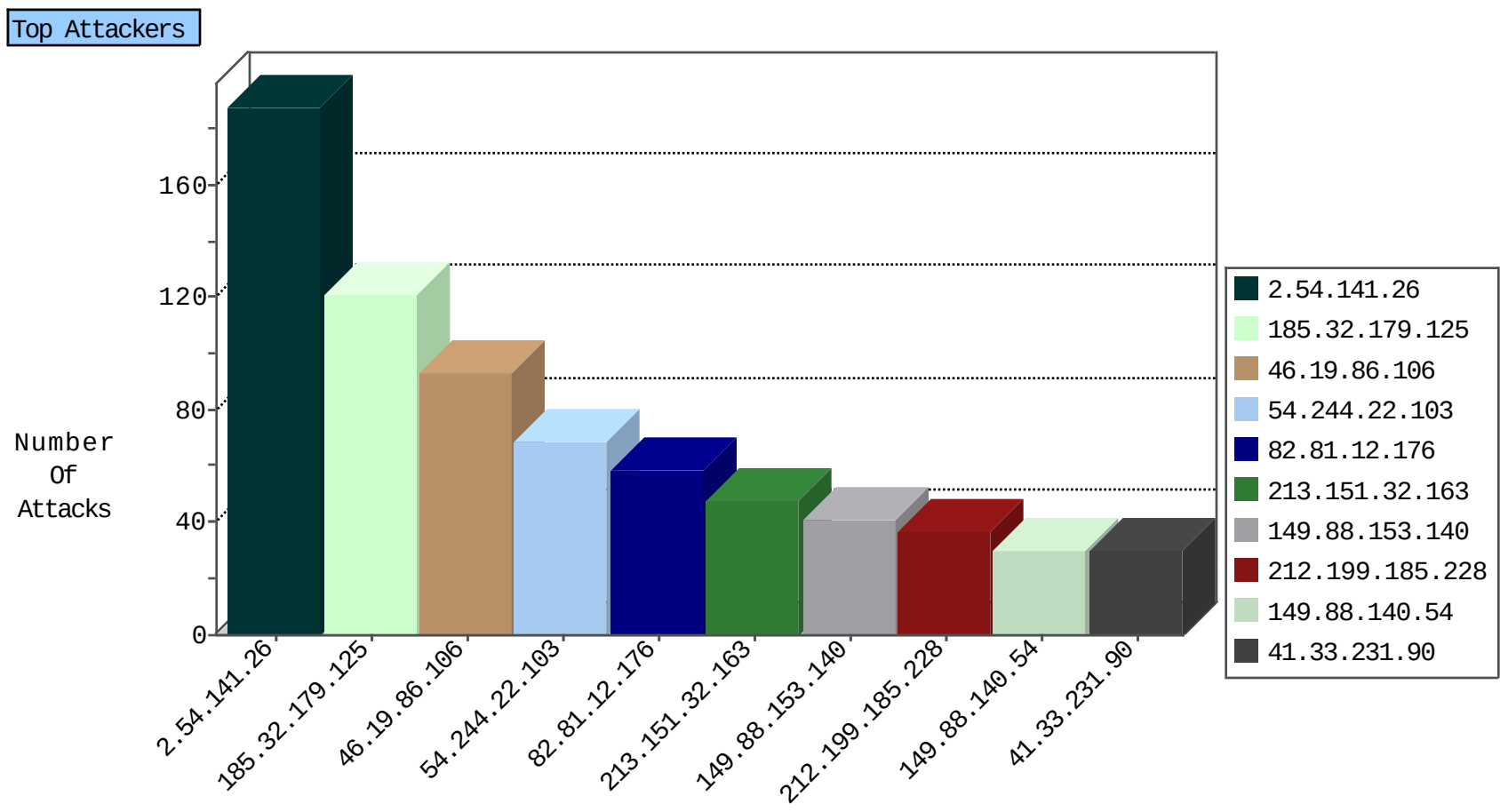
01-31-2016-14:04:03 to 01-31-2016-15:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-31-2016-14:04:03 to 01-31-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	59
185.130.5.201		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.58	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
45.63.16.166		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

01-31-2016-14:04:03 to 01-31-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-31-2016-14:04:03 to 01-31-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.57.238.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.119.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.200.205.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.162.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.244	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.121.71.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.196	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	147.237.72.156	Vietnam	aman.idf.il	ET SCAN NMAP -sS window 3072	1
125.212.232.144	147.237.72.156	Vietnam	aman.idf.il	ET SCAN NMAP -f -sS	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -f -sS	1
109.186.190.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.155.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.131.126.229	147.237.77.61	India	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.225.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.244	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
54.68.192.195	147.237.0.34	United States	tikshuv.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
185.130.5.244	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
37.142.64.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.50.77.71	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.144	147.237.72.156	Vietnam	aman.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
109.253.205.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.199.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-31-2016-14:04:03 to 01-31-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	38
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.199.185.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
149.88.140.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.9.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
192.146.6.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.177.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.187.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.26.149.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.6.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.230.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.93.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.0.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.2.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.127.10.40		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.105.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.13.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.185.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.80.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.45.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.130.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.87	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.54.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.54.9.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.121.80.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
2.54.141.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.54.141.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.54.176.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.19.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.10.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	12
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
149.88.140.54	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.23.92	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	9
2.54.25.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.64.191.148	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	7
185.32.179.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	4
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.141.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.141.26	Block	4
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	4
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
46.19.85.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.177.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 149.88.153.140	Block	3
37.26.146.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.152.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	3
2.54.175.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 149.88.153.140	Block	3
80.246.136.225	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 149.88.153.140	Block	3
147.235.185.74	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	3
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 149.88.153.140	Block	3
2.54.13.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 149.88.153.140	Block	2
80.178.138.115	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 149.88.153.140	Block	2
2.54.187.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.130.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.149.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.42.211.47	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/english/	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
185.32.179.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
10.145.25.9		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
109.253.202.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2