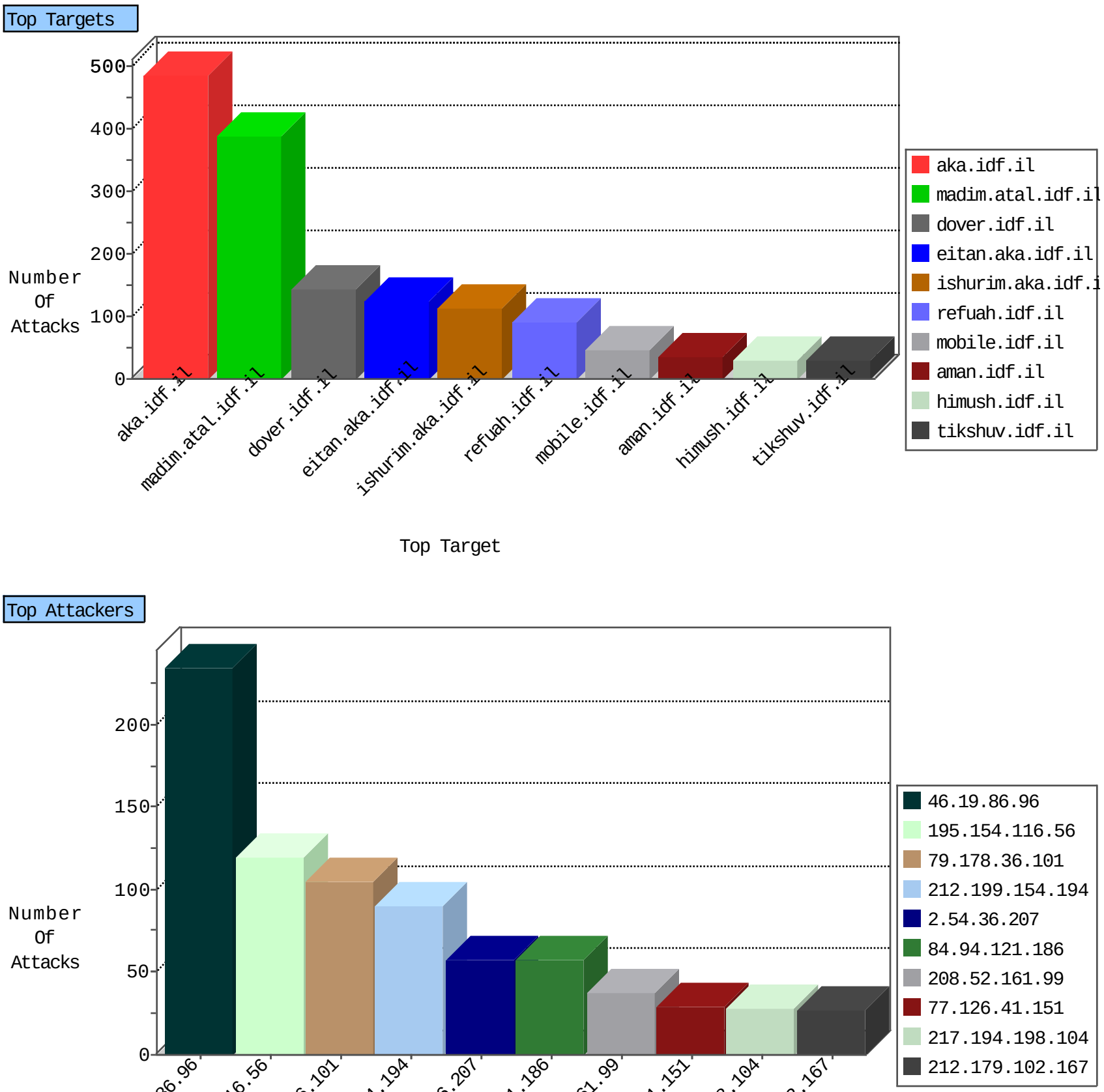
02-02-2016-13:04:08 to 02-02-2016-14:04:08

IDF Under Attack Daily Report



02-02-2016-13:04:08 to 02-02-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	647
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
125.164.39.13	Indonesia	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	3
59.55.238.216	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
59.55.238.216	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
59.55.238.216	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
59.55.238.216	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

02-02-2016-13:04:08 to 02-02-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.52.161.99	United States	147.237.77.205	prisha.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.30	himush.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.235	sviva.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.200	eitan.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.34	tikshuv.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
208.52.161.99	United States	147.237.77.74	law.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.72.156	aman.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.226	www.chamatz.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.39	mobile.meitav.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.170	maarachot.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.72.166	aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.233	atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.17	m.my-kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.176	matpash.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.72.167	ishurim.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.234	halag.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.147	chinuch.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.19	madim.atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1

02-02-2016-13:04:08 to 02-02-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.151.53.217	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.119.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.184.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.93.50.130	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.244	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.107.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.197.47	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
79.176.54.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
69.30.254.186	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
212.199.135.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.129.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.244.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.210.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.99.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.108.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.155.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.251.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.194.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
69.30.254.186	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
213.57.238.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.231.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.71.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-02-2016-13:04:08 to 02-02-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.36.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
84.94.121.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	56
195.154.116.56	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
92.225.45.103	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
46.19.85.116	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	13
176.12.154.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.159.147.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.160.166.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.160.166.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.160.166.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.107.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.217.103	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.12.155.217	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.154.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.241.236.19	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.98.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.41.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
208.109.97.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.145.135	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.28.143.232	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
113.233.129.234	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.118.30.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.40.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.97	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.12.155.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.68.10.201	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.112.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.221.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-02-2016-13:04:08 to 02-02-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.96	Block	129
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.36.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
77.126.41.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.13.129	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 2.54.13.129	Block	22
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
176.12.155.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
77.125.138.99	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.138.99	Block	10
2.54.31.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.12.154.200	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	6
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	5
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	5
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
195.154.116.56	France	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	4
37.26.149.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	3
79.180.183.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 212.179.102.167	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	3
80.246.138.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	3
87.69.107.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	3
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 212.179.102.167	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
195.154.116.56	France	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 195.154.116.56	Block	2
80.246.136.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.155.31	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	2
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 212.179.102.167	Block	2
109.64.51.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	2
37.142.68.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.224.250	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
176.12.154.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	2
46.19.85.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
212.179.102.167	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#27]]Ã“•;2Ã”[[#24]][[#24]]Â” Â¢cÂ´`[[#0]] Â·Ã´eÃ¢LÂ?ÂƒÂŽ[[#17]]Ã¼Ã°Â•l#Ã”ÂŽ}sÂ Â‘Ã¢IÃ½-Â²Ã€ Ã´Ã•Â˜`[[#7]]vÃ?Âƒ Ã¢k;aÂ?Ã½wÃ“I=3Â¨Ã‰Ã¬Ã¥SGÃ•Ã‹&Â—Âœ Ã¤Â®[[#0]])•Â· Â˜qÃ¤Ã¹Â³ÃžÃ‰Xq7	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter c@Id in www.aka.idf.il/main/giyus/general.aspx	None	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method A,YÂ?Â¾Ã“Â¦pXÂ²[[#30]]ÂƒÃ¶WQÃšÃ” CÃ¤.<ÂµRU;kÃŒ[[#18]]Ã•[[#8]][[#8]]SÂ¡("6[[#24]]a]Â£ÃŠ.ÂŠ Â±Ã¼k[[#11]]Â?[[#3]]IÂ‡ÂšÃ£Ã¿hÂ,ÃžÃŠ[[#22]][[#30]][[#5]]c	Block	1

02-02-2016-13:04:08 to 02-02-2016-14:04:08