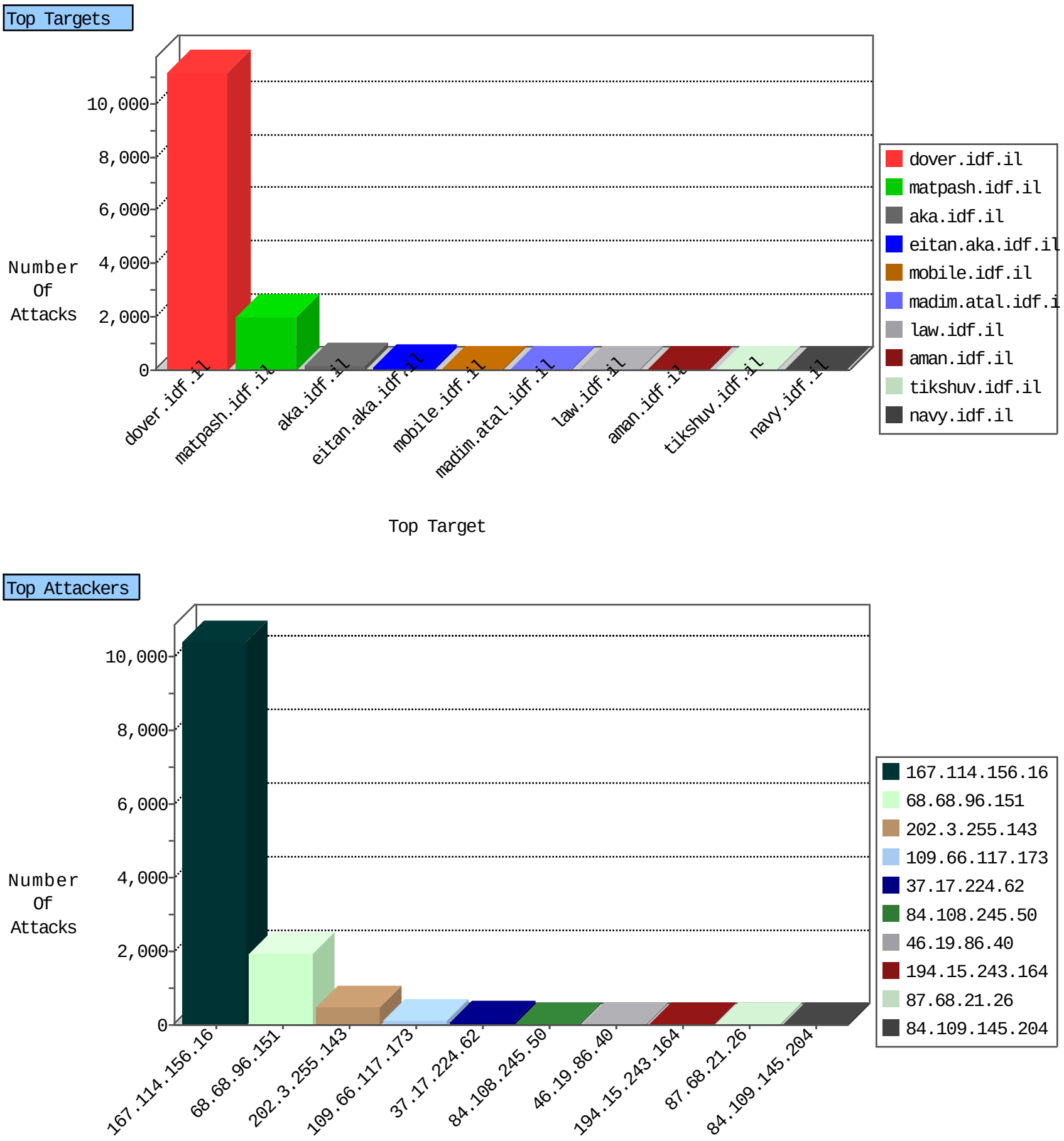
01-15-2016-15:04:02 to 01-15-2016-16:04:02

IDF Under Attack Daily Report



01-15-2016-15:04:02 to 01-15-2016-16:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1730
36.83.119.219	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
8.29.198.25	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.158.166	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
201.206.5.158	Costa Rica	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
58.97.111.9	Thailand	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
125.109.179.196	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
58.97.111.10	Thailand	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

01-15-2016-15:04:02 to 01-15-2016-16:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.89.16.110	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-15-2016-15:04:02 to 01-15-2016-16:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	435
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
141.138.154.126	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
77.109.38.223	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.109.38.223	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.60.36.203	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
77.109.38.223	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.109.38.223	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.109.38.223	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
5.39.222.253	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-15-2016-15:04:02 to 01-15-2016-16:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8908
68.68.96.151	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1950
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1050
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	365
109.66.117.173	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.17.224.62	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	35
84.108.245.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
194.15.243.164	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.17.224.62	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
31.168.239.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.109.145.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
193.191.129.42	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.131.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.120.24.155	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.253.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.108.168.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.108.68.133	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.10	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.128.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.146	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
68.68.96.151	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.170	United States	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.254.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.243.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.131	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
62.176.112.77	Bulgaria	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.228.200.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.115	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
85.130.236.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.145.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.98.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.236.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.109.212.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.22.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.187.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-15-2016-15:04:02 to 01-15-2016-16:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.198.68	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 213.57.198.68	Block	15
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.54.7.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.109.145.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.154.162.173	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
85.130.131.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.130.131.82	Block	4
46.19.86.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.157.34	Block	3
31.168.239.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
84.228.185.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.9.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.253.200.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.136.78	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
109.64.39.235	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.64.39.235	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at Ã°•ÃªÃ´]{Ã–Ã‹f[[#0]]Ã£}&=vÂ³	Block	1
77.126.97.201	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
46.19.86.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
31.168.239.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.243.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.130.131.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
79.181.16.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.170.133.252	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
69.171.230.121	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 87.68.21.26	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method jÂ¬Â?mÂ³	Block	1
176.228.174.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.127.60.14	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
46.120.47.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Malformed URL ×°Ã¿9[[#18]],Ö¿Â§Ã»g×¥×™lâ€ dÂœ gc)[[#17]]:Â¾Â©[[#4]]pkÂ?[[#12]]Â¶m5Âœ#×²×—×"[[#22]]z×—fzÂ§ â‚ª[[#2]]Ãž[[#16]]qÖ¹-2ËœÖ¼Â¾d+Â?Ã¼ÂŠÃŠâ€°×¨×?/[[#8]]7r_×š Ö¸Â¿lz%[Ö¶a[[#18]]Ãž{i[[#25]]×£[[#7]]0×•â€")Ãž Ã¿bÂµ=k;j@Â«Â½1Â«â€"3p-Â¹:[[#20]]kÂ?Ö»â€?~	Block	1
37.142.252.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.202.115	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
79.181.103.250	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 87.68.21.26	Block	1
69.171.230.123	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
217.132.231.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
87.68.21.26	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL ×°Ã¿9[[#18]],Ö¿Â§Ã»g×¥×™lâ€ dÂœ gc)[[#17]]:Â¾Â©[[#4]]pkÂ?[[#12]]Â¶m5Âœ#×²×—×"[[#22]]z×—fzÂ§ â‚ª[[#2]]Ãž[[#16]]qÖ¹-2ËœÖ¼Â¾d+Â?Ã¼ÂŠÃŠâ€°×¨×?/[[#8]]7r_×š Ö¸Â¿lz%[Ö¶a[[#18]]Ãž{i[[#25]]×£[[#7]]0×•â€")Ãž Ã¿bÂµ=k;j@Â«Â½1Â«â€"3p-Â¹:[[#20]]kÂ?Ö»â€?~	Block	1
185.120.125.35		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
85.64.86.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-15-2016-15:04:02 to 01-15-2016-16:04:02