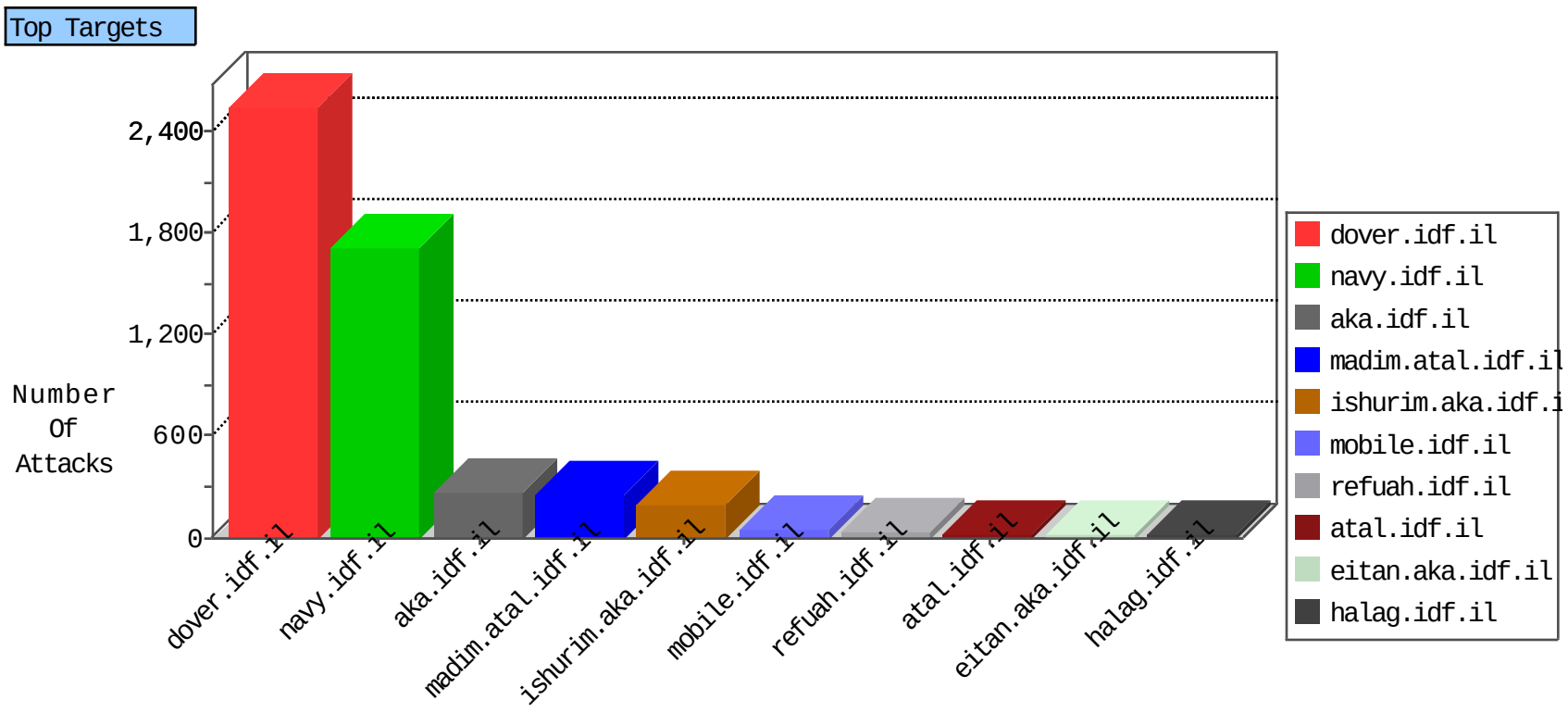
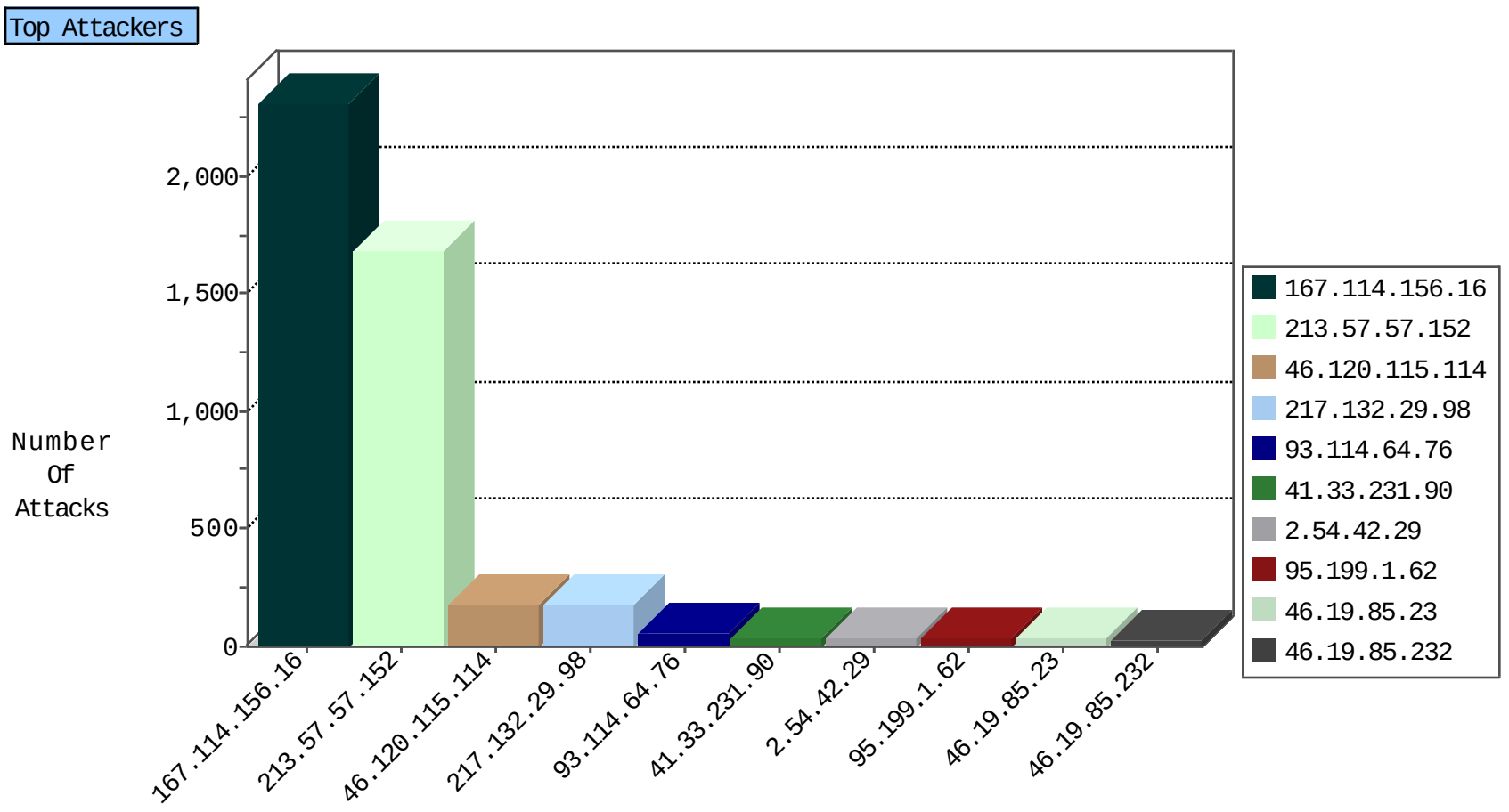
12-18-2015-12:04:09 to 12-18-2015-13:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-18-2015-12:04:09 to 12-18-2015-13:04:09

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	3606
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
207.46.13.180	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
208.67.1.66	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
203.170.107.73	Korea, Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
208.67.1.66	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
203.170.107.73	Korea, Republic of	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.56.238	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.66	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

12-18-2015-12:04:09 to 12-18-2015-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-18-2015-12:04:09 to 12-18-2015-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.114.64.76	147.237.77.216	Romania	dover.idf.il	Tehila - Perl LWP with fake user agent	22
213.57.57.152	147.237.76.86	Israel	navy.idf.il	SERVER-WEBAPP apache directory disclosure attempt	18
213.57.57.152	147.237.76.86	Israel	navy.idf.il	GPL WEB_SERVER apache directory disclosure attempt	17
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.82.64.141	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.224.113.73	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 4096	1
103.254.207.66	147.237.0.35	India	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.141	147.237.72.14	Netherlands	dover.idf.il(old	ET SCAN Potential SSH Scan	1
189.219.239.208	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 3072	1

12-18-2015-12:04:09 to 12-18-2015-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
95.199.1.62	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.176.112.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.149.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.132.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Command Injection	command injection detected in URL: 'shadow'	monitor	10
213.57.57.152	Israel	147.237.76.86	navy.idf.il	HTTP Format Sizes	URL length exceeded allowed maximum length of 2048 bytes	monitor	9
46.120.240.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Response out of state	monitor	9
46.19.85.139	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.42.29	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.176.112.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.218.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.120.115.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.117.244.101	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.251.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.114.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.17.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.76.42	refuah.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
109.66.30.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
149.78.31.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.244.101	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.250.110.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.201	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.1.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.229.161.201	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.65	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4

12-18-2015-12:04:09 to 12-18-2015-13:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.57.57.152	Block	1012
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.57.152	Block	581
217.132.29.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
217.132.29.98	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 217.132.29.98	Block	33
2.54.186.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.54.42.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 213.57.57.152	Block	25
93.114.64.76	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.114.64.76	Block	15
93.114.64.76	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
109.253.220.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
213.57.57.152	Israel	147.237.76.86	navy.idf.il	Multiple WEB-MISC apache DOS attempt(+) from 213.57.57.152	Block	8
84.108.138.120	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	8
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed HTTP Header Line from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed URL from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Illegal Byte Code Character in Header Value from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple NULL Character in Header Name from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Illegal Byte Code Character in Method from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Unknown HTTP Request Method from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Abnormally Long Header Line from 46.120.115.114	Block	6
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Illegal Byte Code Character in Header Name from 46.120.115.114	Block	5
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Abnormally Long Request from 46.120.115.114	Block	5
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Illegal Byte Code Character in URL	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.179.33.180	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.191.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.251.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.179.33.180	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.179.33.180	Block	2
149.88.149.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.168.78	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.168.78	Block	2
109.66.153.52	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/resource/userfollowresource/create/	Block	2
79.176.112.48	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
217.132.29.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Header Value	Block	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.170.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.149	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1085-en/eitan.aspx	None	1
80.246.137.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Illegal URL Path Encoding Â±â€?â€šÃ3zâ€¡*8×¤2{Â?×•×ªÃ™5[[#16]]{Æ’ ×£hÂ¼Â¾â€˜;Â¶× â,¬*Ö¶â,¬Â«j[[#21]]Ã»×²Ëœmb×²â€ º=z×©5hÖ¼/t*Ö³sdf×±×œ[[#2]]â€º×´Â?Ö¹:×˜ÂšÖ¾×¦6Ã»â€“Â½'â€ ¢7/[[#27]]'oÂ°Âš×žÂ«ÂŽÃœ8Â«â,ªÖ¸Â¼vÃšâ,¬Â©â€˜ Â¶[[#1]]rv×?×³×³%[[#24]]o2[[#16]]Â-×¢â,¬Â?r0â€˜[[#23]]Ö´ÃŠÖ¶7â, ª[[#22]]$Ëœ×¡s×ƒÂ¢[[#19]]nÃ¿ÃžÃŠÖµÂ±×§×°(}Ö´\Â±×›ÂŽ[[#23]]Ã·Â²â€ ?Â°Â¸. Âœâ€Žnâ€¢Âœd~@Â¾Â·×?[[#20]]`Â²Â¶Ö¿Ö·Ë†tÂ?×™)×‘ q[[#25]]Â·×£â€°n×žjq×œ[[#18]]â€°[[#25]]ng*ccvË†)rË†i[[#23]]Âœjâ,ª ‘pÂ´mu,â€žÂŽlâ€?lÂ»4ldÖ´Â-[[#31]]_	Block	1
122.160.165.209	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.179.33.180	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
213.57.169.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	Abnormally Long Header Line request header name	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.120.115.114	Israel	147.237.72.167	ishurim.aka.idf.i	NULL Character in Method ÃŸÂ‡Ã¹,Â²h7>pD•Ã“QÂ£[[#17]]Â qJÃŠ Â?Ã?[[#16]]Â–Ã?Ã•Ã‡Â¿_Ã±tÃ¥aEÃ“Ã, [[#11]]CnLÃ²Ã¦:Ã³Â°Ã¥\[[#11]]3Â¦[[#6]]On/Ã'/Ã‰[[#29]]Ã°Â˜Â®U[[#8]]Â¸ GG*lÃ´Ã½-ÃŒÂ§Â¢Ã?gÃ€Ã»U[[#1]]'"Â¸ IÃ˜Â˜Â›EÂ,z9u6EÂšÃŸ VÂºÃ¾[[#23]]%Ã¿ÂœÃŽ[[#0]]ÃŽ{[[#21]]Ã…@T*Ã„5z[[#26]]DÃ?pÂ› -Â¸Ã¿@[[#4]]Ã•LÂ…#Ã-Ã¬Ã•cÃ·[[#18]]fÃ–[[#15]])Â´Â¾	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

12-18-2015-12:04:09 to 12-18-2015-13:04:09