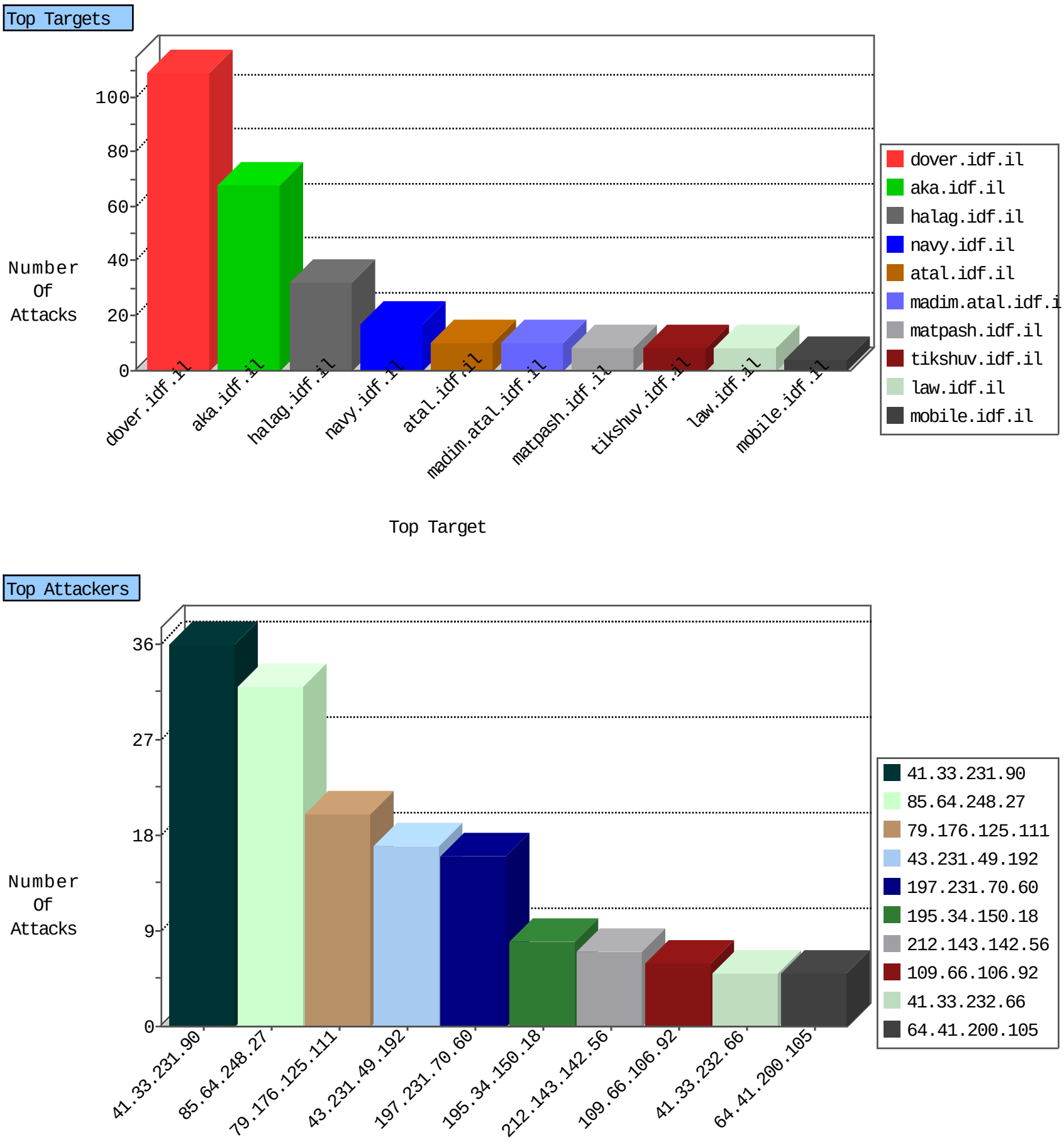
02-27-2016-08:04:02 to 02-27-2016-09:04:02

IDF Under Attack Daily Report



02-27-2016-08:04:02 to 02-27-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.167.154.90	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	4
134.147.203.115	Germany	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
179.43.141.219	Switzerland	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
95.15.91.126	Turkey	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
161.202.77.231	Netherlands	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1

02-27-2016-08:04:02 to 02-27-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.11	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.21	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.26.251.210	Vietnam	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
51.255.65.67	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.75	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
40.77.167.19	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-27-2016-08:04:02 to 02-27-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
95.45.254.123	147.237.77.216	Ireland	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
59.46.193.114	147.237.77.74	China	law.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.77.74	China	law.idf.il	GPL SCAN nmap TCP	2
41.140.253.9	147.237.77.74	Morocco	law.idf.il	ET SCAN NMAP -sS window 2048	1
223.71.251.11	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 1024	1
193.36.35.241	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
111.68.107.43	147.237.8.24	Pakistan	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
94.255.224.2	147.237.77.234	Sweden	halag.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.77.74	Morocco	law.idf.il	ET SCAN NMAP -sS window 4096	1
41.140.253.9	147.237.77.74	Morocco	law.idf.il	ET SCAN NMAP -f -sS	1
111.68.107.43	147.237.8.24	Pakistan	e.lifestyle.idf.	ET SCAN NMAP -sS window 3072	1

02-27-2016-08:04:02 to 02-27-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.64.248.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
197.231.70.60	Gabon	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.66.106.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.125.111	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	5
197.231.70.60	Gabon	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
172.58.232.83	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.176.125.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.121	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.125.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.237.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.125.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.65.185.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.125.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.78		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.230.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.54.147.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
199.30.25.47	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
101.226.167.232	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.176.125.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
173.254.216.69	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
47.88.188.162	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
138.36.0.3		147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.186.189.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
101.226.167.232	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.129.62.62		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.111.38.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.106	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.125.183.165	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
114.112.90.54	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
46.19.86.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
107.189.32.16	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
71.75.249.88	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.186.189.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.187.253.17	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.111.38.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.119	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
121.54.54.59	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.120.91.137	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

02-27-2016-08:04:02 to 02-27-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.54.54.52	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
85.64.119.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.23.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
79.176.226.172	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
64.41.200.105	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 43.231.49.192	Block	1
203.133.168.40	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL ק₪•½,sun¸%v, [[#20]][[#28]]*s»Ÿi+•x1[[#24]]“‡[[#20]]'‰1“gÿƆd-®œ‡¢n[[3#]]i[[#7]]™×£l	Block	1
64.41.200.105	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 43.231.49.192	Block	1
121.54.54.56	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
207.46.13.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal HTTP Version Šƒ‹[[#12]]¾ww‘Z½[[#7]]àVæ#[[#29]][[#4]]„œ»Ûj^ËÎu[[#31]]³¼ªžw#011^H[[#8]]?LNø¥Hìæ=±eâcÇº•¯á¡“œµ›,jSSæ¬íiÆuÎk@€KeÊŠs÷¸:rËc¾\m8,;²7c!˜.	Block	1
64.41.200.105	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 43.231.49.192	Block	1
157.55.39.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ¸Fþ[[#8]][[#17]]ÏE,[[#1]]³J÷I]¹Š†•¬š‹4¹J»XÏŽ]Œ±0{tá[[#31]]L‹,•°•ÛOÉ¦¸ý…KCÑ/×‡t÷Îm¦w–jà<[[#16]][[#27]][[#22]]þ[[#27]]çÝF[[#14]]–¦éê;§øtX½l-r7¥R@[[#19]]×[[#23]]}•pE‡mh~Ã_2[[#22]],×kä[[#14]]mw[[#7]]¬cXÁ}Kbæ—/åE¬<›\ô¢•¨Y#g’Ø³Pò9Q…[[#2]],CÏt²œ‘ˆ°-Íp in URL ק₪•½,sun¸%v, [[#20]][[#28]]*s»Ÿi+•x1[[#24]]“‡[[#20]]'‰1“gÿƆd-®œ‡¢n[[3#]]i[[#7]]™×£l	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal URL Path Encoding ק₪•½,sun¸%v,[[#20]][[#28]]*s»Ÿi+•x1[[#24]]“‡i[[#7]]™×£l]]#3[[n¢‡Dd-®œ“‰1ÿg'']]#20[[	Block	1
95.45.254.123	Ireland	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
64.41.200.105	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 43.231.49.192	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 1	Block	1
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
101.226.168.246	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
64.41.200.105	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 43.231.49.192	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method ¸Fþ[[#8]][[#17]]ÏE,[[#1]]³J÷I]¹Š†•¬š‹4¹J»XÏŽ]Œ±0{tá[[#31]]L‹,•°•ÛOÉ¦¸ý…KCÑ/×‡t÷Îm¦w–jà<[[#16]][[#27]][[#22]]þ[[#27]]çÝF[[#14]]–¦éê;§øtX½l-r7¥R@[[#19]]×[[#23]]}•pE‡mh~Ã_2[[#22]],×kä[[#14]]mw[[#7]]¬cXÁ}Kbæ—/åE¬<›\ô¢•¨Y#g’Ø³Pò9Q…[[#2]],CÏt²œ‘ˆ°-Íp	Block	1
84.111.224.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
46.117.128.65	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Malformed URL ק₪•½,sun¸%v,[[#20]][[#28]]*s»Ÿi+•x1[[#24]]“‡[[#20]]'‰1“gÿi[[#7]]™×£l]]#3[[n¢‡Dd-®œƆ	Block	1
43.231.49.192	Japan	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1

02-27-2016-08:04:02 to 02-27-2016-09:04:02