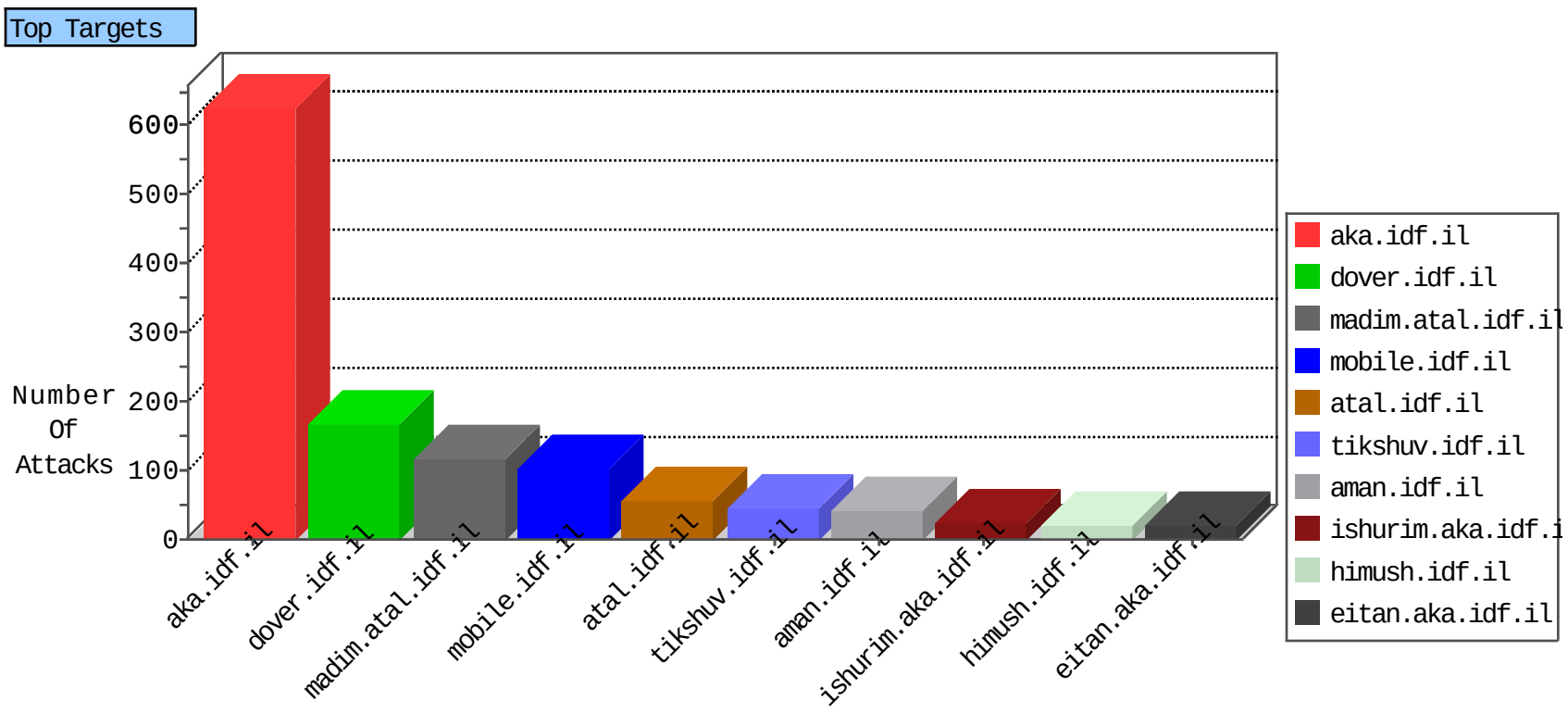
01-28-2016-18:04:08 to 01-28-2016-19:04:08

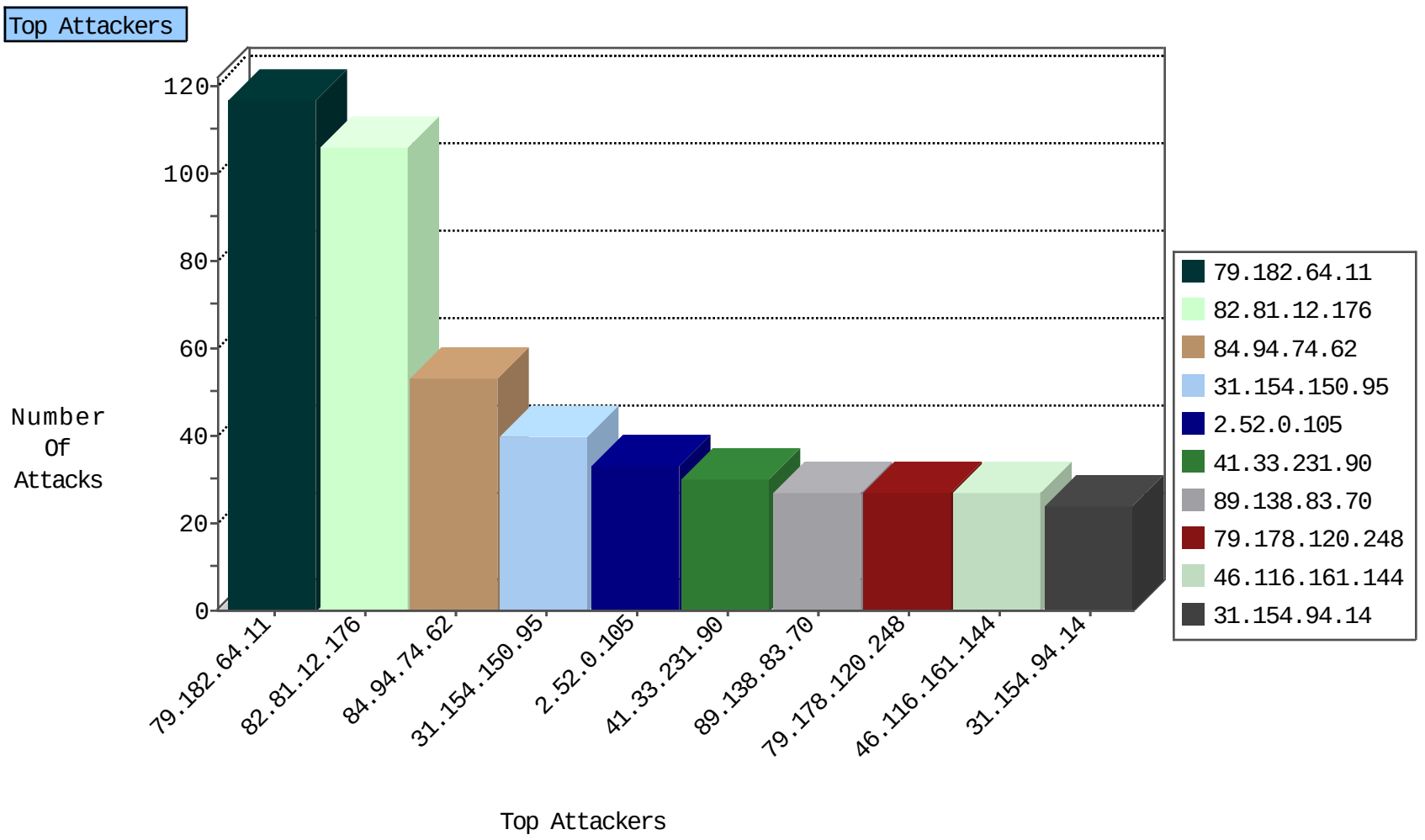
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-28-2016-18:04:08 to 01-28-2016-19:04:08

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	106
31.168.146.45	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
198.56.164.154	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
198.56.164.154	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

01-28-2016-18:04:08 to 01-28-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.229.252.191	Ukraine	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.121	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-28-2016-18:04:08 to 01-28-2016-19:04:08

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
193.201.227.10	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
84.108.98.134	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.10	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.10	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
87.68.152.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.227.10	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.10	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
37.142.68.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
31.154.94.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.29.203.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.10	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
149.78.135.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
95.183.51.251	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.10	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.240.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
46.151.53.217	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
193.201.227.10	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
31.154.94.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.77.234	Ukraine	halag.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.10	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
23.96.118.28	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	1
193.201.227.10	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.10	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.10	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential SSH Scan	1
5.22.135.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
109.65.208.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-28-2016-18:04:08 to 01-28-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
2.52.0.105	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.116.161.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
31.154.150.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
31.154.150.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
46.19.86.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.183.229.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.225	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
31.154.94.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
5.102.254.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.172.53.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.154.94.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
89.138.83.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
31.154.94.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
31.154.94.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
199.203.215.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
199.203.215.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.68.149	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
88.7.178.154	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.88.58.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.138.83.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
85.64.68.149	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.111.0.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.58.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.36.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.120.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
89.138.83.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.78.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.154.94.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.33.131	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.154.94.15	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.146.91	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.131.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.142.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.78.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.94.15	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.65.154.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.154.94.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.154.94.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

01-28-2016-18:04:08 to 01-28-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.74.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.215.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	8
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	8
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	8
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	7
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	6
84.94.184.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.164.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	6
176.13.12.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	4
93.172.237.149	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	4
46.19.86.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	4
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.178.120.248	Block	3
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.178.120.248	Block	3
46.19.86.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.182.64.11	Block	3
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.178.120.248	Block	3
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	3
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.182.64.11	Block	3
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.178.120.248	Block	3
79.183.229.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.160.199.60	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.52.4.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.193.33	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
2.54.139.120	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
93.172.53.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.55.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.139.229.128	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.104.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.171.228.117	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method BÂˆ[[#3]]Ã›Ã”ÃŽ)[[#31]]Â€ p[[#31]]j[[#1]]{Â¬Â¦Â,Âª}Â‰Ã,uÃ-Â«Â¿ÂƒÃ¢Ã±Â–ÃžpÃ˜ÃŠÃ®[[#24]]Ãƒ %Ã†Â¥'Ã?Ã¡Ã¾Â‡Ãš Ã¥Ã¬Â¨Â¬[[#11]][[#21]][[#21]][[#4]]Â°Â¯F[[#22]]Â¿wÃ?Ã¶Ã«Ã¬%m[[#24]]Ã §Â«Ã¢[[#15]]Âž in URL	Block	1
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.111.0.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.94.5	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.55.21.50	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding /Â°Ö¹Ö°×“Ö¹[[#26]]3b2×’h[[#1]]hÂŒÂŽ Â?=Ã»×¨×¡Â°×–Â°â€?Ã¼Æ’%×€'â€ c*$Ã™×?klqÂŒÂ¼â€°[[#21]]× â€™ vh([[#12]]Â¢bâ€™×ž3f-Ö»[[#5]][[#15]]Â¯$â€Žâ€¡_h&$!× â„¢r[[#7]]v	Block	1
79.178.120.248	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
95.86.69.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.180.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-28-2016-18:04:08 to 01-28-2016-19:04:08