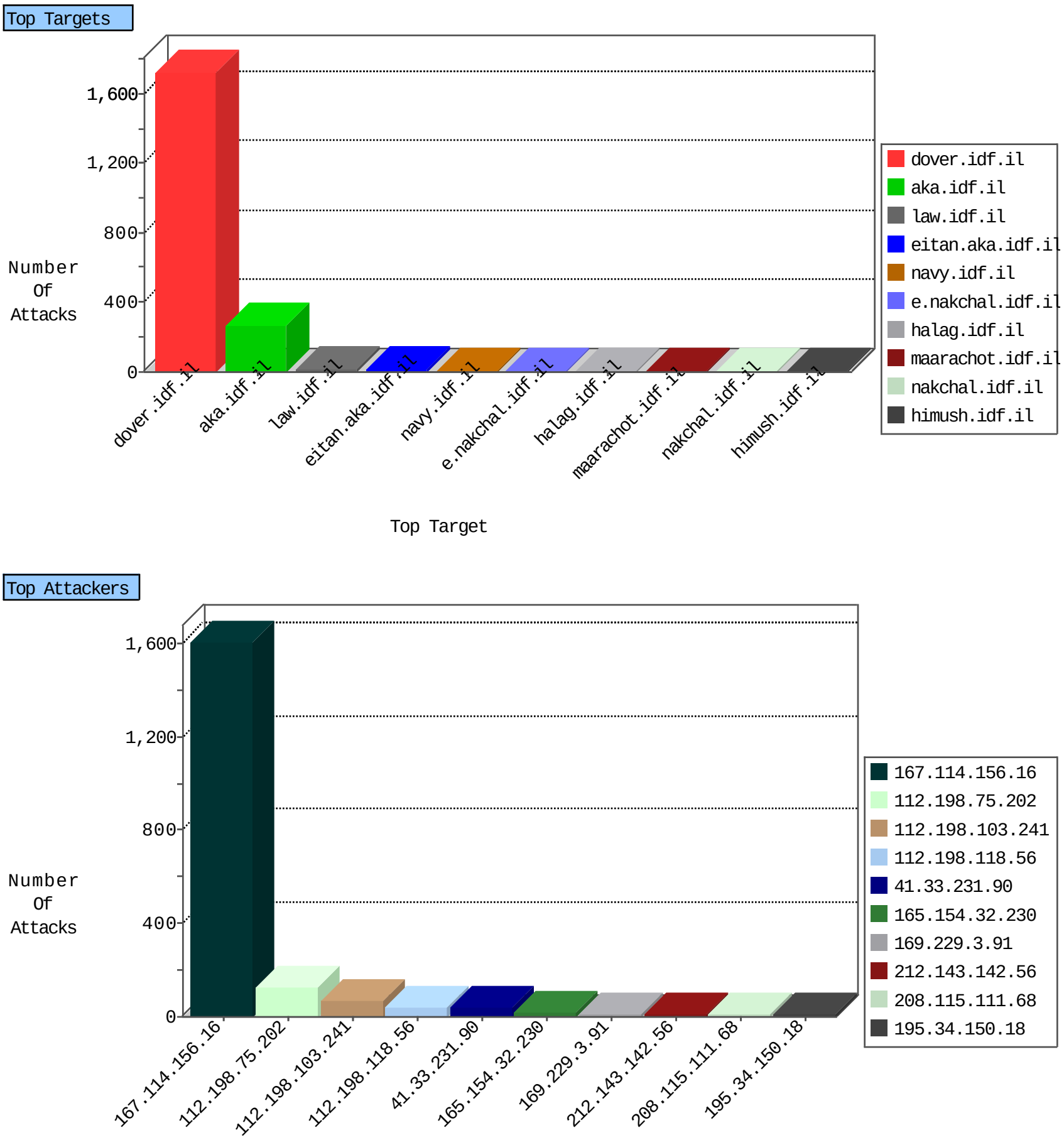
01-11-2016-04:04:01 to 01-11-2016-05:04:01

IDF Under Attack Daily Report



01-11-2016-04:04:01 to 01-11-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3286
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3026
188.138.17.120	France	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.228		147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
162.242.218.58	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.228		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
23.95.248.111	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
188.138.17.120	France	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-11-2016-04:04:01 to 01-11-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-11-2016-04:04:01 to 01-11-2016-05:04:01

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
66.249.79.6	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
31.154.253.217	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.66.25	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.76.148	Sweden	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
187.161.157.230	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.143.82.50	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
190.124.35.115	147.237.8.14	Nicaragua	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
112.198.103.253	147.237.72.166	Philippines	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
37.143.82.50	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1

01-11-2016-04:04:01 to 01-11-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
165.154.32.230	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	10
79.178.62.208	Israel	147.237.72.166	aka.idf.il	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	6
199.30.25.127	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
66.249.66.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.66.153	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
165.154.32.230	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.94	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.177	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
66.87.69.1	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.0.33	idf.il	drop	SAM rule	drop	1
141.212.122.183	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.30	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.120	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.177	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.163.234.7	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.75	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
141.212.122.184	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.99	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
193.90.12.87	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.34	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.178	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.107	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.135.158.101	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
162.242.251.130	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.80	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.100	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1

01-11-2016-04:04:01 to 01-11-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	7
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	7
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	7
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	6
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	5
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	5
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	5
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	5
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	5
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	4
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	4
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	4
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	4
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	4
179.223.98.89	Brazil	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	4
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	4
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	4
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	4
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	3
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	3
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	3
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	3
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	3
112.198.103.253	Philippines	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.118.56	Block	2
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.118.56	Block	2
31.13.113.83	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Url	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.118.56	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.118.56	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.118.56	Block	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.118.56	Block	2
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.10	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
112.198.103.241	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String /VFP[[#22]]Â-aÃš[[#20]]s.;ÂžGÂ¹ÂµAâ,ª`×,Ö´[[#23]]×¤[[#11]]z'×“2Âž[[#21]]Lâ€°ÂµjÂžÂœ[[#14]]2Ã»Ö´×±×?Â?×ª[[#6]]D•×§[[#17]]7×“×¥×²×§3Â¡J[[#30]]jâ€ Ö»!×—×,Qâ€¹â€?9zÂ¢Â²â€¡fÃ™â€”yâ€žFÂ½Ö²â€œâ,ª×ŸÆ’<h•[[#25]][[#28]]×?×—â,¬â€ž%×ž×ž{ onÂ«Â¿[[#6]]ÂµÖ¹Ã?a[[#6]]Â³Â¸×œ×ŸÖ²â€?ÂŸÂ£[[#28]]ÃŠÖµÆ’Â?auÃŸâ€¦Ã?×,Â³Â«6~[[#27]][[#8]]×Ÿ	Block	1
66.249.66.149	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 112.198.118.56	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding (2s_x2{RO4b{)]lE:Fg)X!asE2FvfFVX{)9u{%T{uO:1p{1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
112.198.118.56	Philippines	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

01-11-2016-04:04:01 to 01-11-2016-05:04:01