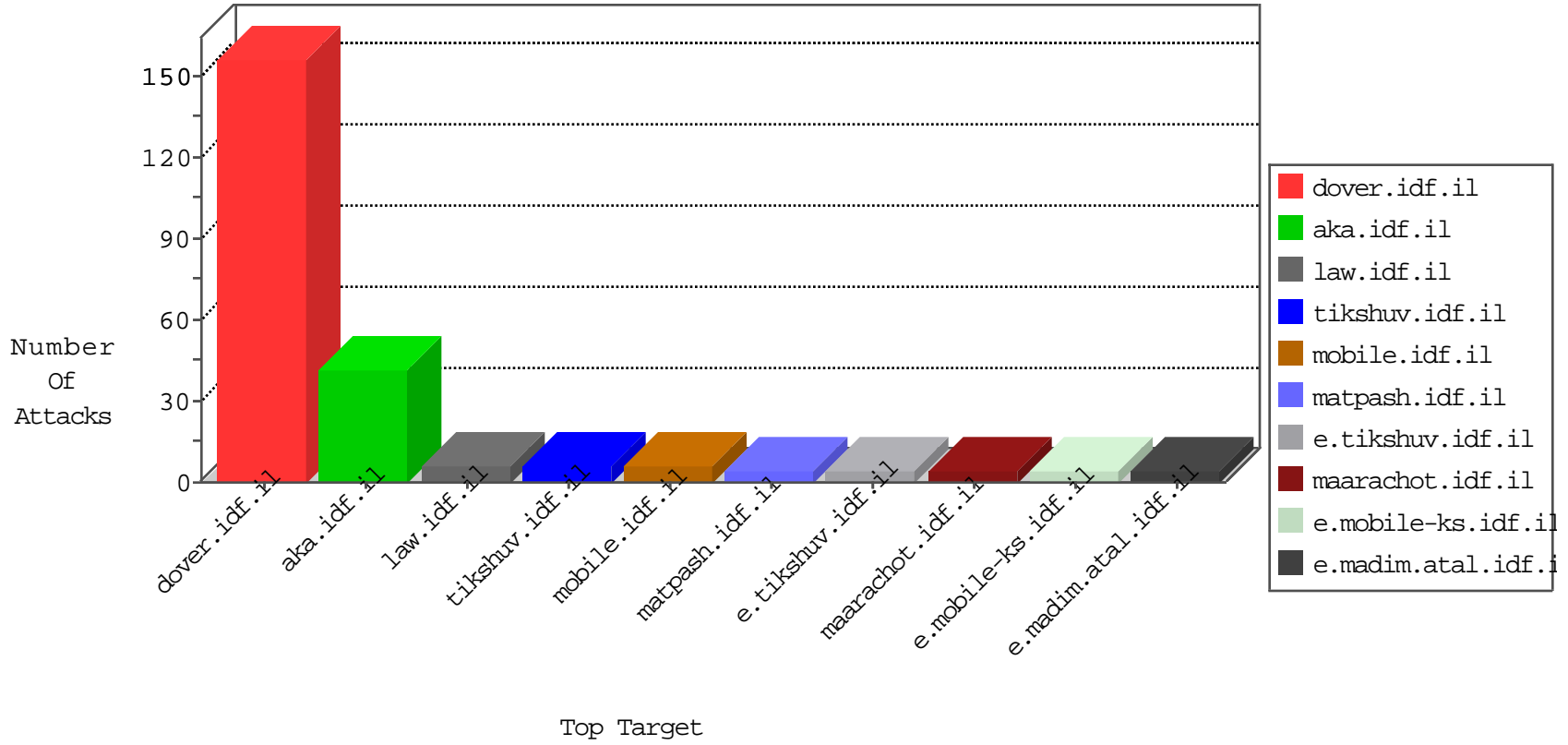


IDF Under Attack

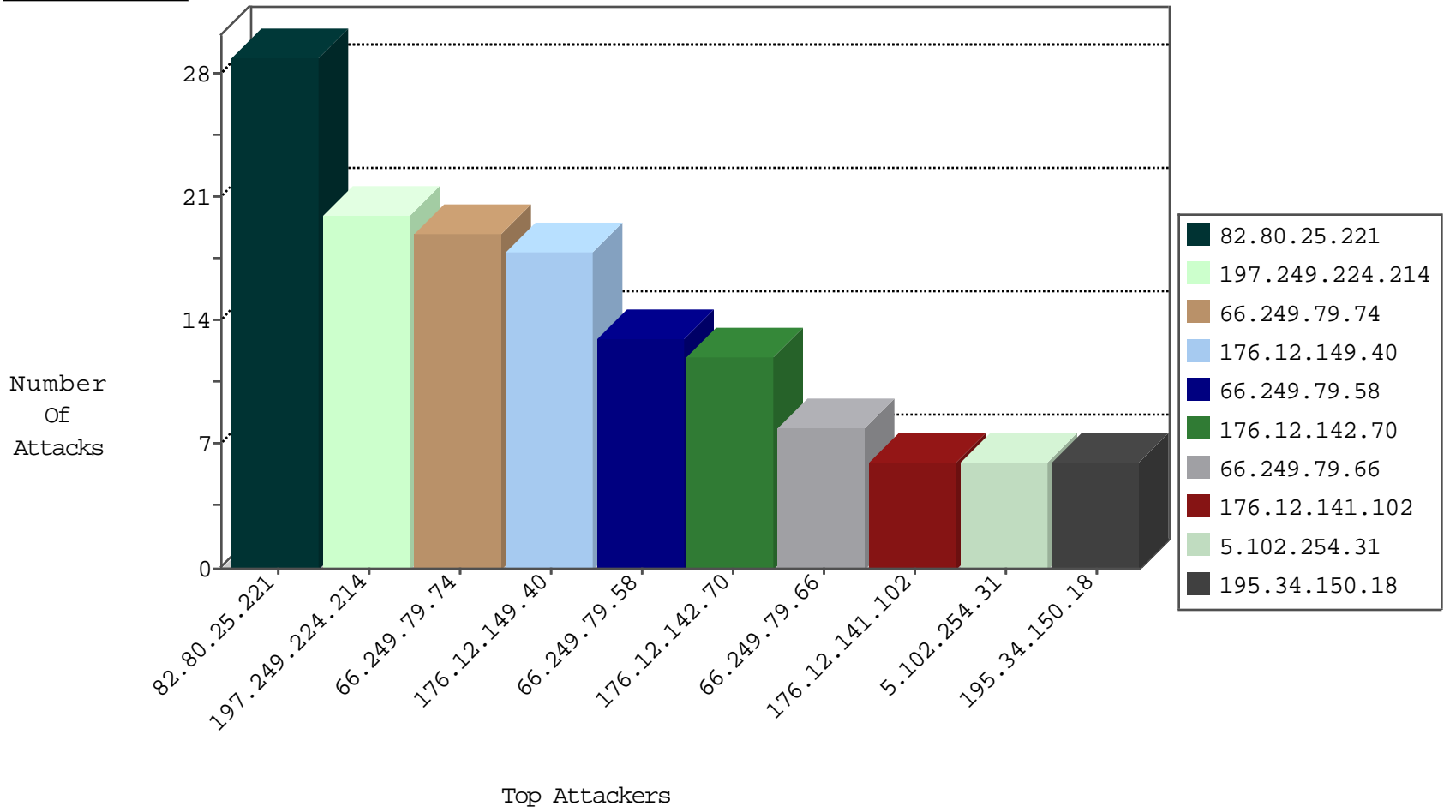
03-27-2015-20:03:06



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
------------------	------------------	----------------	----------	-----------	---------------	-------

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.25.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
63.240.94.244	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
94.126.171.132	Portugal	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
37.26.147.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.158.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
208.115.198.240	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
27.50.132.61	China	147.237.76.198	e.yochalan.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.149.40	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.141.102	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.102.254.31	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
197.249.224.214	Mozambique	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
217.132.66.26	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
83.142.185.198	Poland	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
197.249.224.214	Mozambique	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
5.102.254.88	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
197.249.224.214	Mozambique	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
79.181.28.248	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
197.249.224.214	Mozambique	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
197.249.224.214	Mozambique	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.46.39.134	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
217.132.66.26	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.234	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.23	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
85.64.116.119	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
66.249.81.227	United States	147.237.77.176	matpash.idf.il	directory traversal overflow	Directory Traversal	monitor	1
37.46.39.134	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.82	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.102.254.52	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.64.116.119	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.176.180.156	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
222.92.145.185	China	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.111.226.102	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.250.2.214	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.229.107.175	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
37.26.148.240	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
104.245.146.198		147.237.76.34	yohalan.idf.il		drop	drop	1
80.246.130.193	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.228	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.160.119	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.229.107.175	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.73.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigation.asp	Block	4
85.250.173.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
188.138.17.205	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/19.stm	Block	1
109.66.110.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationsservice.aspx/getuserdetails	Block	1
85.64.222.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
77.126.235.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.139.194.149	Thailand	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
173.36.113.102	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.67.22	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx	Block	1
94.126.171.132	Portugal	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 94.126.171.132	Block	1
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.102.251.11	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
66.249.81.227	United States	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/./favicon.ico	Block	1
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
85.65.202.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04	Block	1
79.177.11.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct101 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
173.36.113.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.79.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/yeelon.stm	Block	1
94.126.171.132	Portugal	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/stories/kediri.php.phpgif	Block	1
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1224-5.stm	Block	1
46.19.86.84	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
79.183.197.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	1
208.115.198.240	United States	147.237.77.216	dover.idf.il	Multiple signatures from 208.115.198.240	Block	1
180.76.4.32	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
109.64.80.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.47.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter captcha in www.aka.idf.il/main/giyus/authenticationsservice.aspx/authenticate	None	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.116.155.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.88.101.199	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.25.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.197.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
208.115.198.240	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
180.76.6.29	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-ar/cogat.aspx	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
5.28.158.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.102.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.4.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.200.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0207-3.stm	Block	1
66.249.65.161	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
93.173.59.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationsservice.aspx/getuserdetails	Block	1