VALKYRIE COMODO

Summary

File Name: Mirillis_Action_2.8.2.0_FULL.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

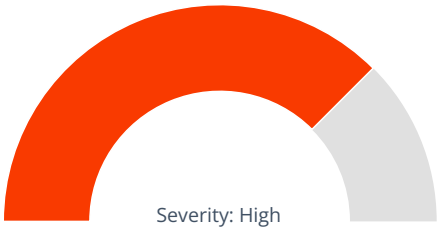
SHA1: 6172fb25474ce1f0fed4ae64e71a5e618283a641

MD5: 015c4dfc9423143fc1406f01048f0769

MALWARE

Valkyrie Final Verdict

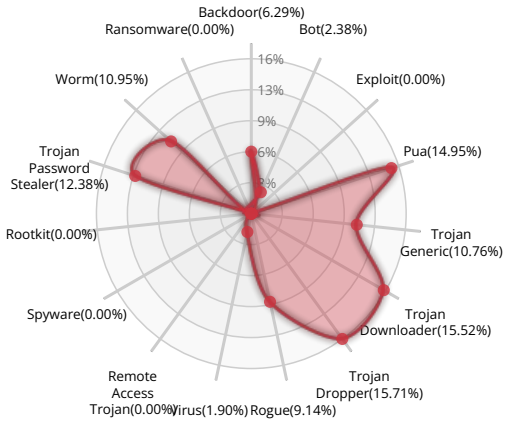
DETECTION SECTION



Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION

ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STATIC ANOMALY

Anomalous binary characteristics	Show sources

NETWORKING

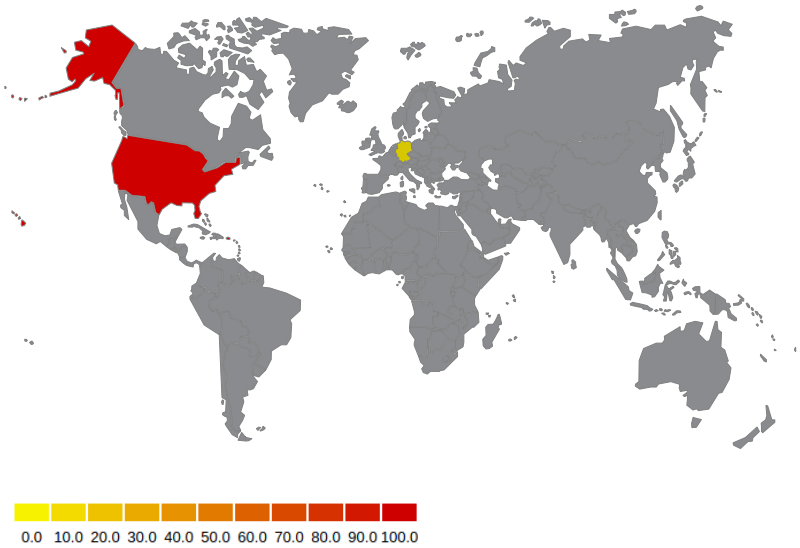
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

Behavior Graph

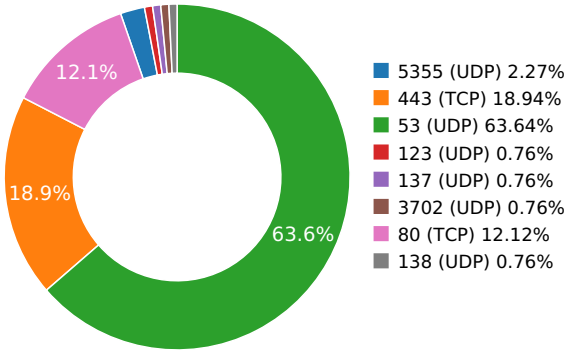
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	52.179.17.38	United States	8075	Microsoft Corporation	Malware Process
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	172.217.15.110	United States	15169	Google LLC	Malware Process
	172.217.164.131	United States	15169	Google LLC	Malware Process
	172.217.5.226	United States	15169	Google LLC	Malware Process
	204.237.142.179	United States	3257	Akamai Technologies, Inc.	OS Process
	23.46.238.216	United States	20940	Akamai Technologies, Inc.	Malware Process
	34.213.175.109	United States	16509	Amazon Technologies Inc.	Malware Process
	34.214.20.242	United States	16509	Amazon Technologies Inc.	Malware Process
	35.163.20.157	United States	16509	Amazon Technologies Inc.	Malware Process
	52.35.215.194	United States	16509	Amazon Technologies Inc.	Malware Process
	52.84.26.102	United States	16509	Amazon Technologies Inc.	Malware Process
	52.84.26.231	United States	16509	Amazon Technologies Inc.	Malware Process
	52.84.26.94	United States	16509	Amazon Technologies Inc.	Malware Process
	192.186.164.50	United States	55286	Not known	Malware Process
shavar.services.mozilla.com	34.211.202.13	United States	16509	Amazon Technologies Inc.	Malware Process
secure.informaction.com	69.195.158.194	United States	19969	Joe's Datacenter, LLC	Malware Process
easylist-downloads.adblockplus.org	213.239.192.206	Germany	24940		Malware Process
sb.l.google.com	172.217.7.174	United States	15169	Google LLC	Malware Process
a652.dscb.akamai.net	204.237.142.171	United States	20940	Akamai Technologies, Inc.	Malware Process
cx.atdmt.com	31.13.71.2	Ireland	32934		Malware Process
d39fl7ga3npck8.cloudfront.net	52.84.31.203	United States	16509	Amazon Technologies Inc.	Malware Process
fbsbx.com	31.13.71.36	Ireland	32934		Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
star.c10r.facebook.com	31.13.71.1	Ireland	32934		Malware Process
www.facebook.com	31.13.71.36	Ireland	32934		Malware Process
ocsp.pki.goog	172.217.7.227	United States	15169	Google LLC	Malware Process
star-mini.c10r.facebook.com	31.13.71.36	Ireland	32934		Malware Process
balrog-aus5.r53-2.services.mozilla.com	34.218.159.169	United States	16509	Amazon Technologies Inc.	Malware Process
scontent.xx.fbcdn.net	31.13.71.7	Ireland	32934		Malware Process
tracking-protection.cdn.mozilla.net	52.84.31.91	United States	16509	Amazon Technologies Inc.	Malware Process
facebook.com	31.13.65.36	Ireland	32934		Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Ser...	Malware Process
fbcdn.net	31.13.65.36	Ireland	32934		Malware Process
atlas.c10r.facebook.com	31.13.71.2	Ireland	32934		Malware Process
ocsp.int-x3.letsencrypt.org	204.156.15.115	United States	20940	NTT America, Inc.	Malware Process
tiles.r53-2.services.mozilla.com	52.35.250.5	United States	16509	Amazon Technologies Inc.	Malware Process
scontent-dfw5-2.xx.fbcdn.net	31.13.93.26	Ireland	32934		Malware Process
cs9.wac.phicdn.net	72.21.91.29	United States	15133	MCI Communications Ser...	Malware Process
search.r53-2.services.mozilla.com	52.88.150.81	United States	16509	Amazon Technologies Inc.	Malware Process
d1zkz3k4cclnv6.cloudfront.net	52.84.31.204	United States	16509	Amazon Technologies Inc.	Malware Process
shavar.prod.mozaws.net	54.201.6.28	United States	16509	Amazon Technologies Inc.	Malware Process
pagead46.l.doubleclick.net	172.217.15.98	United States	15169	Google LLC	Malware Process
cs.atdmt.com	31.13.71.1	Ireland	32934		Malware Process
static.xx.fbcdn.net	31.13.71.7	Ireland	32934		Malware Process
pki-goog.l.google.com	172.217.5.227	United States	15169	Google LLC	Malware Process
dcky6u1m8u6el.cloudfront.net	52.84.31.66	United States	16509	Amazon Technologies Inc.	Malware Process
ocsp.comodoca.com	204.237.142.163	United States	20940	Akamai Technologies, Inc.	OS Process
safebrowsing.cache.l.google.com	172.217.8.14	United States	15169	Google LLC	Malware Process
a771.dscq.akamai.net	204.156.15.120	United States	20940	NTT America, Inc.	Malware Process
googleads.g.doubleclick.net	172.217.7.162	United States	15169	Google LLC	Malware Process
tiles.services.mozilla.com	52.35.250.5	United States	16509	Amazon Technologies Inc.	Malware Process
self-repair.mozilla.org	52.84.31.41	United States	16509	Amazon Technologies Inc.	Malware Process
tiles-cloudfront.cdn.mozilla.net	52.84.31.65	United States	16509	Amazon Technologies Inc.	Malware Process
safebrowsing-cache.google.com	172.217.8.14	United States	15169	Google LLC	Malware Process
staticxx.facebook.com	31.13.71.7	Ireland	32934		Malware Process
aus5.mozilla.org	52.32.77.100	United States	16509	Amazon Technologies Inc.	Malware Process
external-dfw5-2.xx.fbcdn.net	31.13.93.26	Ireland	32934		Malware Process
search.services.mozilla.com	35.166.112.39	United States	16509	Amazon Technologies Inc.	Malware Process
connect.facebook.net	31.13.71.7	Ireland	32934		Malware Process
safebrowsing.google.com	172.217.7.174	United States	15169	Google LLC	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
notification.adblockplus.org	195.201.59.244	Germany	24940		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	64.9894459248
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.int-x3.letsencrypt.org	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	65.0273609161
Path: / **URI:** http://ocsp.int-x3.letsencrypt.org/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	65.1248869896
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.pki.goog	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	68.5933499336
Path: /GTSGIAG3 **URI:** http://ocsp.pki.goog/GTSGIAG3						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	70.1820809841
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	73.3271999359
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.pki.goog	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	76.4049098492
Path: /GTSGIAG3 **URI:** http://ocsp.pki.goog/GTSGIAG3						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	89.8478229046
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.comodoca.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	2	122.873462915
Path: / **URI:** http://ocsp.comodoca.com/						
ocsp.comodoca.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	2	122.941836834
Path: / **URI:** http://ocsp.comodoca.com/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6....	1	126.923913002
Path: / **URI:** http://ocsp.digicert.com/						

DNS QUERIES

Request	Type
secure.informaction.com	A
Answers - 69.195.158.196 (A) - 69.195.158.198 (A) - 69.195.158.195 (A) - 69.195.158.197 (A) - 69.195.158.194 (A)	
www.facebook.com	A
Answers - star-mini.c10r.facebook.com (CNAME) - 31.13.71.36 (A)	
search.services.mozilla.com	A
Answers - 34.213.175.109 (A) - 35.166.112.39 (A) - search.r53-2.services.mozilla.com (CNAME) - 52.88.150.81 (A)	
star-mini.c10r.facebook.com	A
search.r53-2.services.mozilla.com	A
secure.informaction.com	AAAA
search.r53-2.services.mozilla.com	AAAA
star-mini.c10r.facebook.com	AAAA
Answers - 2a03:2880:f112:83:face:b00c:0:25de (AAAA)	
ocsp.int-x3.letsencrypt.org	A
Answers - 23.46.238.216 (A) - a771.dscq.akamai.net (CNAME) - ocsp.int-x3.letsencrypt.org.edgesuite.net (CNAME) - 23.46.238.234 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
cs9.wac.phicdn.net	A
a771.dscq.akamai.net	A
a771.dscq.akamai.net	AAAA
Answers - 2600:1408:20::172e:eeea (AAAA) - 2600:1408:20::172e:eed8 (AAAA)	
cs9.wac.phicdn.net	AAAA
tiles.services.mozilla.com	A

Request	Type
Answers - 52.39.131.77 (A) - 54.186.163.246 (A) - 52.43.40.243 (A) - 34.208.7.98 (A) - 52.41.78.152 (A) - 52.43.91.152 (A) - 34.214.20.242 (A) - tiles.r53-2.services.mozilla.com (CNAME) - 54.149.115.79 (A)	
tiles.r53-2.services.mozilla.com	A
Answers - 52.26.103.165 (A)	
tiles.r53-2.services.mozilla.com	AAAA
tiles-cloudfront.cdn.mozilla.net	A
Answers - 52.84.26.118 (A) - 52.84.26.13 (A) - dcky6u1m8u6el.cloudfront.net (CNAME) - 52.84.26.220 (A) - 52.84.26.102 (A)	
dcky6u1m8u6el.cloudfront.net	A
dcky6u1m8u6el.cloudfront.net	AAAA
static.xx.fbcdn.net	A
Answers - 31.13.71.7 (A) - scontent.xx.fbcdn.net (CNAME)	
cs.atdmt.com	A
Answers - star.c10r.facebook.com (CNAME) - 31.13.71.1 (A)	
scontent-dfw5-2.xx.fbcdn.net	A
Answers - 31.13.93.26 (A)	
external-dfw5-2.xx.fbcdn.net	A
Answers - scontent-dfw5-2.xx.fbcdn.net (CNAME)	
facebook.com	A
scontent.xx.fbcdn.net	A
scontent-dfw5-2.xx.fbcdn.net	AAAA
Answers - 2a03:2880:f034:11a:face:b00c:0:3 (AAAA)	
facebook.com	AAAA
Answers - 2a03:2880:f128:83:face:b00c:0:25de (AAAA)	

Request	Type
safebrowsing.google.com	A
Answers - 172.217.15.110 (A) - sb.l.google.com (CNAME)	
star.c10r.facebook.com	A
sb.l.google.com	A
scontent.xx.fbcdn.net	AAAA
Answers - 2a03:2880:f012:8:face:b00c:0:1 (AAAA)	
sb.l.google.com	AAAA
Answers - 2607:f8b0:4004:811::200e (AAAA)	
star.c10r.facebook.com	AAAA
Answers - 2a03:2880:f012:1:face:b00c:0:1 (AAAA)	
ocsp.pki.goog	A
Answers - pki-goog.l.google.com (CNAME) - 172.217.164.131 (A)	
pki-goog.l.google.com	A
pki-goog.l.google.com	AAAA
Answers - 2607:f8b0:4004:814::2003 (AAAA)	
safebrowsing-cache.google.com	A
Answers - 172.217.7.174 (A) - safebrowsing.cache.l.google.com (CNAME)	
safebrowsing.cache.l.google.com	A
safebrowsing.cache.l.google.com	AAAA
Answers - 2607:f8b0:4004:800::200e (AAAA)	
fbcdn.net	A
fbcdn.net	AAAA
Answers - 2a03:2880:f103:83:face:b00c:0:25de (AAAA)	
self-repair.mozilla.org	A
Answers - 52.84.26.231 (A) - 52.84.26.230 (A) - d39fl7ga3npck8.cloudfront.net (CNAME) - 52.84.26.100 (A) - 52.84.26.103 (A) - self-repair.r53-2.services.mozilla.com (CNAME)	
staticxx.facebook.com	A

Request	Type
d39fl7ga3npck8.cloudfront.net	A
d39fl7ga3npck8.cloudfront.net	AAAA
Answers - 2600:9000:2038:3000:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:6800:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:6200:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:8c00:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:7a00:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:c400:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:800:13:9d43:b600:93a1 (AAAA) - 2600:9000:2038:4200:13:9d43:b600:93a1 (AAAA)	
googleads.g.doubleclick.net	A
Answers - pagead46.l.doubleclick.net (CNAME) - 172.217.5.226 (A)	
pagead46.l.doubleclick.net	A
Answers - 172.217.15.66 (A)	
pagead46.l.doubleclick.net	AAAA
Answers - 2607:f8b0:4004:814::2002 (AAAA)	
cx.atdmt.com	A
Answers - 31.13.71.2 (A) - atlas.c10r.facebook.com (CNAME)	
fbsbx.com	A
Answers - 31.13.66.35 (A)	
atlas.c10r.facebook.com	A
fbsbx.com	AAAA
atlas.c10r.facebook.com	AAAA
Answers - 2a03:2880:f012:2:face:b00c:0:1 (AAAA)	
teredo.ipv6.microsoft.com	A
Answers - (NXDOMAIN)	
connect.facebook.net	A
shavar.services.mozilla.com	A
Answers - shavar.prod.mozaws.net (CNAME) - 34.212.119.231 (A) - 52.35.21.241 (A) - 54.187.176.55 (A) - 52.35.215.194 (A) - 52.88.72.192 (A) - 54.201.6.28 (A)	

Request	Type
shavar.prod.mozaws.net	A
Answers - 54.187.144.104 (A) - 34.211.202.13 (A) - 52.34.90.23 (A) - 52.33.113.226 (A) - 52.89.170.53 (A) - 54.200.76.177 (A)	
shavar.prod.mozaws.net	AAAA
tracking-protection.cdn.mozilla.net	A
Answers - 52.84.26.94 (A) - 52.84.26.59 (A) - d1zkz3k4cclnv6.cloudfront.net (CNAME) - 52.84.26.210 (A) - 52.84.26.177 (A)	
d1zkz3k4cclnv6.cloudfront.net	A
d1zkz3k4cclnv6.cloudfront.net	AAAA
easylist-downloads.adblockplus.org	A
Answers - 178.63.13.4 (A) - 88.99.186.148 (A) - 88.99.186.153 (A) - 148.251.238.203 (A) - 148.251.12.230 (A) - 178.63.50.140 (A) - 95.216.27.30 (A) - 94.130.76.59 (A) - 5.9.15.86 (A) - 88.99.186.158 (A) - 176.9.127.15 (A) - 94.130.73.104 (A) - 88.198.17.12 (A) - 144.76.137.80 (A) - 195.201.59.236 (A) - 88.99.186.150 (A) - 144.76.137.234 (A) - 144.76.197.80 (A)	
notification.adblockplus.org	A
Answers - 95.216.27.37 (A) - 46.4.68.226 (A) - 195.201.59.248 (A) - 95.216.14.109 (A) - easylist-downloads.adblockplus.org (CNAME) - 176.9.146.200 (A) - 136.243.58.99 (A) - 195.201.59.240 (A) - 94.130.136.91 (A)	
easylist-downloads.adblockplus.org	AAAA

Request	Type
Answers - 2a01:4f8:151:8129::2 (AAAA) - 2a01:4f8:c0c:2d17::2 (AAAA) - 2a01:4f8:c0c:e3f::2 (AAAA) - 2a01:4f8:c0c:2d11::2 (AAAA) - 2a01:4f8:c0c:2d14::2 (AAAA) - 2a01:4f8:171:30::2 (AAAA) - 2a01:4f8:120:724c::2 (AAAA)	
ocsp.comodoca.com	A
Answers - ocsp.comodoca.com.edgesuite.net (CNAME) - a652.dscb.akamai.net (CNAME) - 204.237.142.179 (A) - 204.237.142.171 (A) - 204.237.142.176 (A)	
a652.dscb.akamai.net	A
Answers - 184.84.243.42 (A) - 184.84.243.34 (A)	
a652.dscb.akamai.net	AAAA
Answers - 2600:1408:20::172e:eea9 (AAAA) - 2600:1408:20::172e:eed3 (AAAA)	
aus5.mozilla.org	A
Answers - balrog-aus5.r53-2.services.mozilla.com (CNAME) - 35.164.82.230 (A) - 52.43.79.30 (A) - 54.186.118.41 (A) - 34.218.159.169 (A) - 54.148.138.18 (A) - 52.32.77.100 (A) - 52.37.35.5 (A) - 35.163.20.157 (A)	
balrog-aus5.r53-2.services.mozilla.com	A
Answers - 54.149.111.157 (A)	
balrog-aus5.r53-2.services.mozilla.com	AAAA
time.windows.com	A
Answers - 52.179.17.38 (A) - time.microsoft.akadns.net (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
64.3421568871	Sandbox	69.195.158.194	443
64.471768856	Sandbox	34.213.175.109	443
64.9894459248	Sandbox	72.21.91.29	80
64.9977040291	Sandbox	31.13.71.36	443
65.0273609161	Sandbox	23.46.238.216	80
65.2419829369	Sandbox	34.214.20.242	443
65.7802979946	Sandbox	52.84.26.102	443
68.1999359131	Sandbox	31.13.71.7	443
68.3200180531	Sandbox	172.217.15.110	443
68.5933499336	Sandbox	172.217.164.131	80
68.6016259193	Sandbox	31.13.71.7	443
68.8729469776	Sandbox	31.13.93.26	443
68.90260005	Sandbox	31.13.71.36	443
69.3357279301	Sandbox	31.13.71.1	443
69.3634068966	Sandbox	31.13.93.26	443
70.828510046	Sandbox	172.217.7.174	443
72.9414198399	Sandbox	52.84.26.231	443
73.020059824	Sandbox	31.13.71.36	443
73.0401580334	Sandbox	31.13.71.7	443
76.1204078197	Sandbox	172.217.5.226	443
76.1945898533	Sandbox	31.13.71.2	443
76.2980418205	Sandbox	31.13.71.36	443
82.4927690029	Sandbox	31.13.71.7	443
89.7442250252	Sandbox	52.35.215.194	443
90.0170488358	Sandbox	52.84.26.94	443
122.583739042	Sandbox	176.9.127.15	443
122.600513935	Sandbox	195.201.59.240	443
122.873462915	Sandbox	204.237.142.179	80
122.873850822	Sandbox	204.237.142.179	80
126.251401901	Sandbox	35.163.20.157	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03713583946	Sandbox	224.0.0.252	5355
3.03768587112	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.04122304916	Sandbox	239.255.255.250	3702
3.08006691933	Sandbox	192.168.56.255	137
5.59507894516	Sandbox	224.0.0.252	5355
9.07859802246	Sandbox	192.168.56.255	138
64.2019000053	Sandbox	8.8.4.4	53
64.2162928581	Sandbox	8.8.4.4	53
64.309057951	Sandbox	8.8.4.4	53
64.3112308979	Sandbox	8.8.4.4	53
64.3153150082	Sandbox	8.8.4.4	53
64.3230478764	Sandbox	8.8.4.4	53
64.4017310143	Sandbox	8.8.4.4	53
64.4024059772	Sandbox	8.8.4.4	53
64.4028859138	Sandbox	8.8.4.4	53
64.9611358643	Sandbox	8.8.4.4	53
64.9650080204	Sandbox	8.8.4.4	53
64.9762499332	Sandbox	8.8.4.4	53
64.9986159801	Sandbox	8.8.4.4	53
65.0345678329	Sandbox	8.8.4.4	53
65.0684888363	Sandbox	8.8.4.4	53
65.1408748627	Sandbox	8.8.4.4	53
65.1534500122	Sandbox	8.8.4.4	53
65.1782839298	Sandbox	8.8.4.4	53
65.6721429825	Sandbox	8.8.4.4	53
65.7711210251	Sandbox	8.8.4.4	53
65.865185976	Sandbox	8.8.4.4	53
68.0174708366	Sandbox	8.8.4.4	53
68.1654639244	Sandbox	8.8.4.4	53
68.1656918526	Sandbox	8.8.4.4	53
68.211370945	Sandbox	8.8.4.4	53
68.2120330334	Sandbox	8.8.4.4	53
68.2327959538	Sandbox	8.8.4.4	53
68.2332789898	Sandbox	8.8.4.4	53
68.2578229904	Sandbox	8.8.4.4	53
68.2670769691	Sandbox	8.8.4.4	53
68.2697780132	Sandbox	8.8.4.4	53
68.2776939869	Sandbox	8.8.4.4	53
68.2807400227	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
68.3046958447	Sandbox	8.8.4.4	53
68.3776929379	Sandbox	8.8.4.4	53
68.3780169487	Sandbox	8.8.4.4	53
68.3782529831	Sandbox	8.8.4.4	53
68.5466618538	Sandbox	8.8.4.4	53
68.5788040161	Sandbox	8.8.4.4	53
68.6067938805	Sandbox	8.8.4.4	53
70.7861659527	Sandbox	8.8.4.4	53
70.8135418892	Sandbox	8.8.4.4	53
70.8392930031	Sandbox	8.8.4.4	53
72.1835868359	Sandbox	8.8.4.4	53
72.1961920261	Sandbox	8.8.4.4	53
72.220790863	Sandbox	8.8.4.4	53
72.2328698635	Sandbox	8.8.4.4	53
72.2377429008	Sandbox	8.8.4.4	53
72.2857890129	Sandbox	8.8.4.4	53
72.3822698593	Sandbox	8.8.4.4	53
73.8967039585	Sandbox	8.8.4.4	53
73.9253559113	Sandbox	8.8.4.4	53
73.9519398212	Sandbox	8.8.4.4	53
74.2022628784	Sandbox	8.8.4.4	53
74.2423679829	Sandbox	8.8.4.4	53
74.2432539463	Sandbox	8.8.4.4	53
74.2538080215	Sandbox	8.8.4.4	53
74.2652668953	Sandbox	8.8.4.4	53
76.7140119076	Sandbox	8.8.4.4	53
77.2409129143	Sandbox	8.8.4.4	53
89.6424059868	Sandbox	8.8.4.4	53
89.6551618576	Sandbox	8.8.4.4	53
89.666383028	Sandbox	8.8.4.4	53
89.9714589119	Sandbox	8.8.4.4	53
90.0075829029	Sandbox	8.8.4.4	53
90.0431799889	Sandbox	8.8.4.4	53
122.464685917	Sandbox	8.8.4.4	53
122.467715979	Sandbox	8.8.4.4	53
122.476569891	Sandbox	8.8.4.4	53
122.486727953	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
122.494123936	Sandbox	8.8.4.4	53
122.75959301	Sandbox	8.8.4.4	53
122.85809803	Sandbox	8.8.4.4	53
122.955804825	Sandbox	8.8.4.4	53
126.15068388	Sandbox	8.8.4.4	53
126.264261007	Sandbox	8.8.4.4	53
126.275615931	Sandbox	8.8.4.4	53
130.060531855	Sandbox	8.8.4.4	53
130.153758049	Sandbox	8.8.4.4	53
130.195530891	Sandbox	8.8.4.4	53
162.788383961	Sandbox	8.8.4.4	53
164.347262859	Sandbox	52.179.17.38	123
206.894263029	Sandbox	8.8.4.4	53
206.929996967	Sandbox	8.8.4.4	53
206.968973875	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES
disable_antivirus
hijack_network
escalate_priv
screenshot
keylogger
win_registry
win_token
win_private_profile
win_files_operation
Borland
BobSoftMiniDelphiBoBBobSoft

STATIC FILE INFO

File Name:	Mirillis_Action_2.8.2.0_FULL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	6172fb25474ce1f0fed4ae64e71a5e618283a641
MD5:	015c4dfc9423143fc1406f01048f0769
First Seen Date:	2018-01-05 22:07:01.415426 (5 years ago)
Number Of Clients Seen:	7
Last Analysis Date:	2019-01-25 20:21:44.632372 (4 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[53.2, u'InstallShield setup'], [17.5, u'Win32 Executable Delphi generic'], [16.1, u'Windows screen saver'], [5.5, u'Win32 Executable (generic)'], [2.5, u'Win16/32 Executable Delphi generic']]
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	Mirillis
FileDescription	Action! 2.8.2.0 Installation
FileVersion	2.8.2.0
Comments	
CompanyName	Mirillis
Translation	0x0409 0x04e4
Entry Point	0x425468 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	19018299
Ssdeep	393216:YdsvXwsJSix8N2yizfJ0bGSymoHrunFOpohN17u:YdsvAsJnx8QyizfCfLIpoH17u
Sha256	e405f788f5445c7bdf9c5617604053fcec7a4860eea877b9441425d8f0310133
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/1/7/2/6172fb25474ce1f0fed4ae64e71a5e618283a641', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2019:01:25 15:32:34+00:00', u'EXE:InitializedDataSize': 314880, u'File:FileModifyDate': u'2018:01:05 22:06:24+00:00', u'EXE:FileVersionNumber': u'2.8.2.0', u'EXE:FileVersion': u'2.8.2.0 ', u'File:FileSize': u'18 MB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Mirillis ', u'File:FileName': u'6172fb25474ce1f0fed4ae64e71a5e618283a641', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'1992:06:19 22:22:17+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Mirillis ', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/1/7/2', u'EXE:FileDescription': u'Action! 2.8.2.0 Installation ', u'EXE:EntryPoint': u'0x25468', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 148992, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2018:01:05 22:06:24+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'0.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	c9adc83b45e363b21cd6b11b5da0501f

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x244cc	0x24600	6.59442804845	5e14e4ede2e2215bc7d72837b9871f8f
DATA	0x26000	0x2894	0x2a00	3.79375704099	abafcbfbd7f8ac0226ca496a92a0cf06
BSS	0x29000	0x10f5	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x2b000	0x1798	0x1800	4.88554506065	a4e0ac39d5ed487ceea059fa23dfce5e
.tls	0x2d000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x2e000	0x18	0x200	0.20448815744	c4fdd0c5c9efb616fcc85d66056ca490
.reloc	0x2f000	0x1884	0x1a00	6.58664786461	867a1120317d51734587a74f6ee70016
.rsrc	0x31000	0x46f60	0x47000	5.79644438	eb8e41ac06d7921f08b4cf7f5395db62

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc
  - LocalFree
  - LocalAlloc
  - GetVersion
  - GetCurrentThreadId
  - WideCharToMultiByte
  - GetThreadLocale
  - GetStartupInfoA
  - GetLocaleInfoA
  - GetCommandLineA
  - FreeLibrary
  - ExitProcess
  - WriteFile
  - UnhandledExceptionFilter
  - RtlUnwind
  - RaiseException
  - GetStdHandle
- user32.dll
  - GetKeyboardType
  - MessageBoxA
- advapi32.dll
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegCloseKey
- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
- kernel32.dll
  - TlsSetValue
  - TlsGetValue
  - LocalAlloc
  - GetModuleHandleA
- advapi32.dll
  - RegCloseKey
  - OpenThreadToken
  - OpenProcessToken
  - GetTokenInformation
  - FreeSid
  - EqualSid
  - AllocateAndInitializeSid
  - AdjustTokenPrivileges
- kernel32.dll
  - WriteFile
  - WinExec
  - WaitForSingleObject
  - TerminateProcess
  - SystemTimeToFileTime
  - Sleep

    - SetFileTime
    - SetFilePointer
    - SetErrorMode
    - SetEndOfFile
    - ReadFile
    - OpenProcess
    - MultiByteToWideChar
    - LocalFileTimeToFileTime
    - LoadLibraryA
    - GlobalFree
    - GlobalAlloc
    - GetVersion
    - GetUserDefaultLangID
    - GetProcAddress
    - GetModuleHandleA
    - GetLocalTime
    - GetLastError
    - GetFileTime
    - GetFileSize
    - GetExitCodeProcess
    - GetCurrentThread
    - GetCurrentProcess
    - FreeLibrary
    - FindClose
    - FileTimeToSystemTime
    - FileTimeToLocalFileTime
    - DosDateTimeToFileTime
    - CompareFileTime
    - CloseHandle
- gdi32.dll
    - StretchDIBits
    - StretchBlt
    - SetWindowOrgEx
    - SetTextColor
    - SetStretchBltMode
    - SetRectRgn
    - SetROP2
    - SetPixel
    - SetDIBits
    - SetBrushOrgEx
    - SetBkMode
    - SetBkColor
    - SelectObject
    - SaveDC
    - RestoreDC
    - OffsetRgn
    - MoveToEx
    - IntersectClipRect
    - GetStockObject
    - GetPixel
    - GetDIBits
    - ExtSelectClipRgn
    - ExcludeClipRect
    - DeleteObject
    - DeleteDC
    - CreateSolidBrush
    - CreateRectRgn
    - CreateDIBitmap
    - CreateDIBSection
    - CreateCompatibleDC
    - CreateCompatibleBitmap
    - CreateBrushIndirect
    - CreateBitmap
    - CombineRgn
    - BitBlt
- user32.dll
    - WaitMessage
    - ValidateRect
    - TranslateMessage
    - ShowWindow
    - SetWindowPos
    - SetTimer
    - SetParent
    - SetForegroundWindow
    - SetFocus

    - SetCursor
    - SendMessageA
    - ScreenToClient
    - ReleaseDC
    - PostQuitMessage
    - OffsetRect
    - KillTimer
    - IsZoomed
    - IsWindowVisible
    - IsWindowEnabled
    - IsWindow
    - IsIconic
    - InvalidateRect
    - GetWindowRgn
    - GetWindowRect
    - GetWindowDC
    - GetUpdateRgn
    - GetSystemMetrics
    - GetSystemMenu
    - GetSysColor
    - GetParent
    - GetWindow
    - GetKeyState
    - GetFocus
    - GetDCEx
    - GetDC
    - GetCursorPos
    - GetClientRect
    - GetCapture
    - FillRect
    - ExitWindowsEx
    - EnumWindows
    - EndPaint
    - EnableWindow
    - EnableMenuItem
    - DrawIcon
    - DestroyWindow
    - DestroyIcon
    - DeleteMenu
    - CopyImage
    - ClientToScreen
    - BeginPaint
    - CharLowerBuffA
- winmm.dll
    - timeKillEvent
    - timeSetEvent
- oleaut32.dll
    - SysAllocStringLen
- ole32.dll
    - OleInitialize
- comctl32.dll
    - ImageList_Draw
    - ImageList_SetBkColor
    - ImageList_Create
    - InitCommonControls
- shell32.dll
    - SHGetFileInfoA
- user32.dll
    - wvsprintfA
    - SetWindowLongA
    - SetPropA
    - SendMessageA
    - RemovePropA
    - RegisterClassA
    - PostMessageA
    - PeekMessageA
    - MessageBoxA
    - LoadIconA
    - LoadCursorA
    - GetWindowTextLengthA
    - GetWindowTextA
    - GetWindowLongA
    - GetPropA
    - GetClassLongA
    - GetClassInfoA

    - FindWindowA
    - DrawTextA
    - DispatchMessageA
    - DefWindowProcA
    - CreateWindowExA
    - CallWindowProcA
- gdi32.dll
    - GetTextExtentPoint32A
    - GetObjectA
    - CreateFontIndirectA
    - AddFontResourceA
- kernel32.dll
    - WritePrivateProfileStringA
    - SetFileAttributesA
    - SetCurrentDirectoryA
    - RemoveDirectoryA
    - LoadLibraryA
    - GetWindowsDirectoryA
    - GetVersionExA
    - GetTimeFormatA
    - GetTempPathA
    - GetSystemDirectoryA
    - GetShortPathNameA
    - GetPrivateProfileStringA
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetFullPathNameA
    - GetFileAttributesA
    - GetDiskFreeSpaceA
    - GetDateFormatA
    - GetComputerNameA
    - GetCommandLineA
    - FindNextFileA
    - FindFirstFileA
    - ExpandEnvironmentStringsA
    - DeleteFileA
    - CreateFileA
    - CreateDirectoryA
    - CompareStringA
- advapi32.dll
    - RegSetValueExA
    - RegQueryValueExA
    - RegQueryInfoKeyA
    - RegOpenKeyExA
    - RegEnumKeyExA
    - RegCreateKeyExA
    - LookupPrivilegeValueA
    - GetUserNameA
- shell32.dll
    - ShellExecuteExA
    - ShellExecuteA
- cabinet.dll
    - FDIDestroy
    - FDICopy
    - FDICreate
- ole32.dll
    - OleInitialize
    - CoTaskMemFree
    - CoCreateInstance
    - CoUninitialize
    - CoInitialize
- shell32.dll
    - SHGetSpecialFolderLocation
    - SHGetPathFromIDListA
    - SHGetMalloc
    - SHChangeNotify
    - SHBrowseForFolderA

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 201376, u'sha256': u'656453d85cd9b2f5d6e13300af37fff561b3fc05f02f0fcfdf06af568c5d98cb', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 202504, u'sha256': u'5dc2f7c255d948a42795cc941c33a2e08573de885ef14c1f5a43dace2fba7886', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 204944, u'sha256':

u'da2ea1c0097e75c2677345eee13d53ad55e6581eac6a9ef35cf2868541161c77', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 209208, u'sha256': u'583b52c9b248794539a41158d9d201afa7234d72b557eed1f600f13e27a8a44e', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 218848, u'sha256': u'6cda1c94f4a168c4de5c5a5114f3feb955b60f737987ae38275702b48edeffeb', u'type': u'dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 16777215, next used block 16777215', u'size': 270376}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 489224, u'sha256': u'88d14cc6638af8a0836f6d868dfab60df92907a2d7becaefbbd7e007acb75610', u'type': u'Sendmail frozen configuration ', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 489240, u'sha256': u'0d9a7ca2193a69f7048c46748a3e98e7e101bda4e5bbe903858539e20ffed78d', u'type': u'data', u'size': 272}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 489512, u'sha256': u'956a9528d0fe75126c1628391a8f48d38b15048fd1d817b29635b2a5eea5e1c2', u'type': u'MS Windows icon resource - 5 icons, 16x16', u'size': 76}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_VERSION', u'offset': 489588, u'sha256': u'bb2e91b28b55fbc496b313a31219c0c912eb93f22c30d5df601a1b47d502dab2', u'type': u'data', u'size': 884}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_MANIFEST', u'offset': 490472, u'sha256': u'1e9cffb6544cb40c042cf9413e0481026699ef5f8e74613293bd60ae098f3c09', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 886}

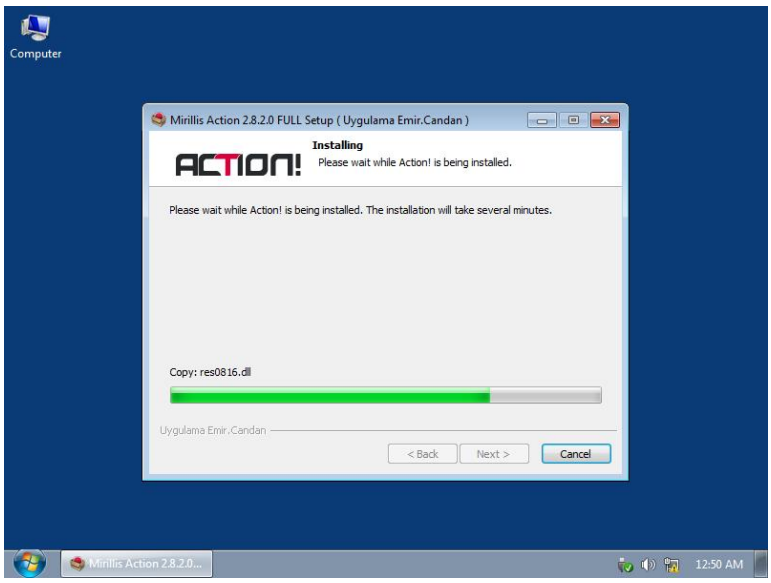
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM

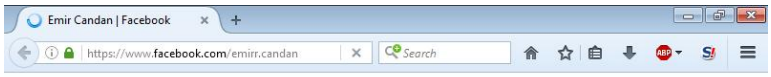

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:53 AM

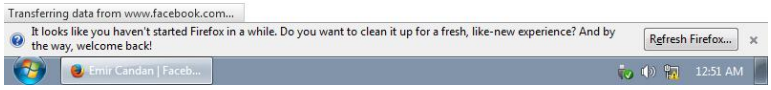

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: res0816.dll
Uygulama Emir.Candan
< Back
Next >
Cancel
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:53 AM

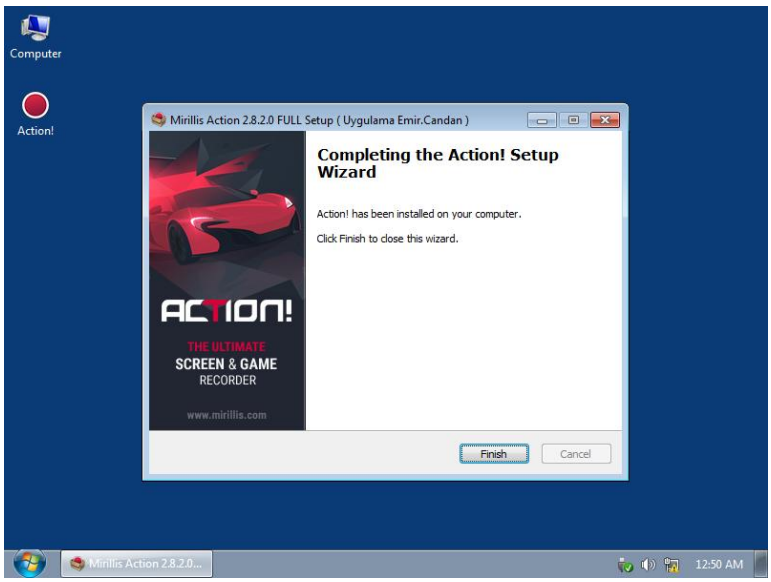

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM

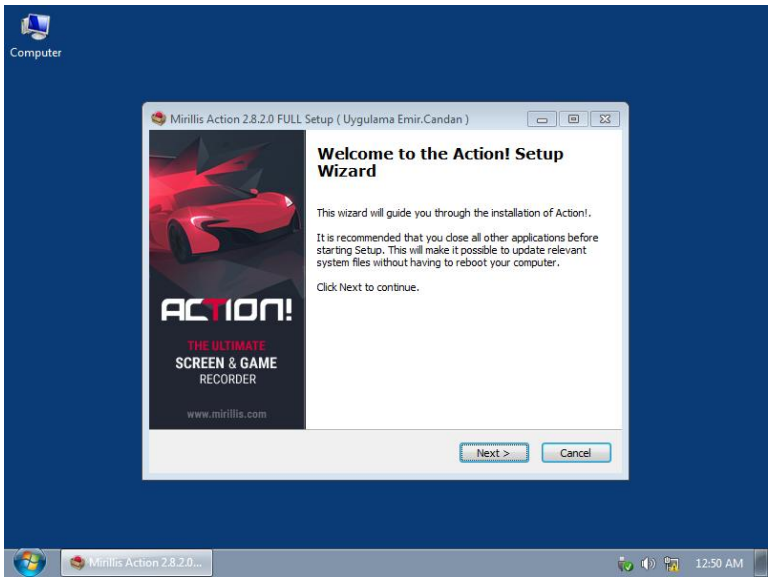

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:51 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search


Transferring data from www.facebook.com...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:51 AM

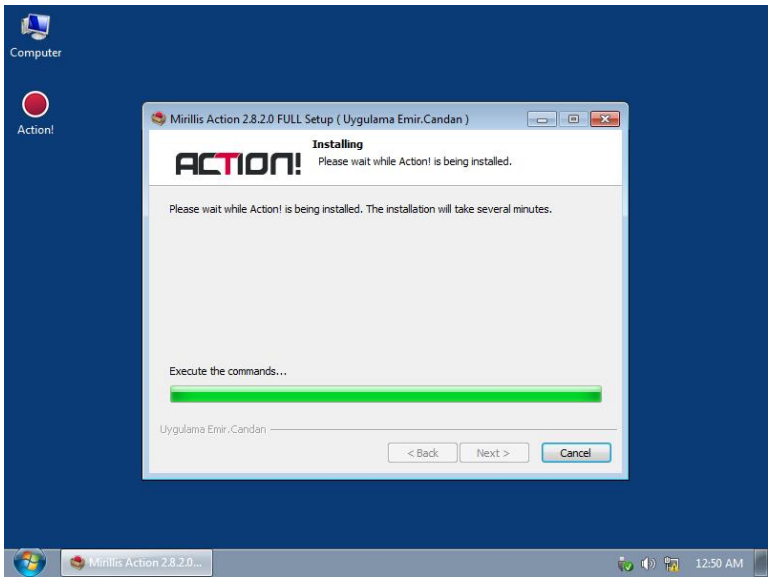

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
https://www.facebook.com
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:52 AM


Computer
Action!
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
Completing the Action! Setup Wizard
Action! has been installed on your computer.
Click Finish to close this wizard.
ACTION!
THE ULTIMATE
SCREEN & GAME
RECORDER
www.mirillis.com
Finish
Cancel
Mirillis Action 2.8.2.0...
12:50 AM


Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
Welcome to the Action! Setup Wizard
This wizard will guide you through the installation of Action!.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
ACTION!
THE ULTIMATE
SCREEN & GAME
RECORDER
www.mirillis.com
Next >
Cancel
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
Read staticxx.facebook.com
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:51 AM

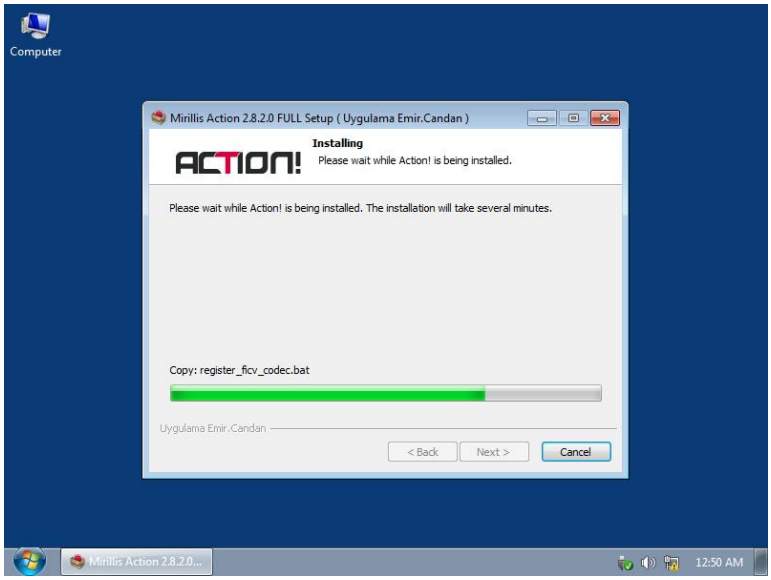

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:53 AM

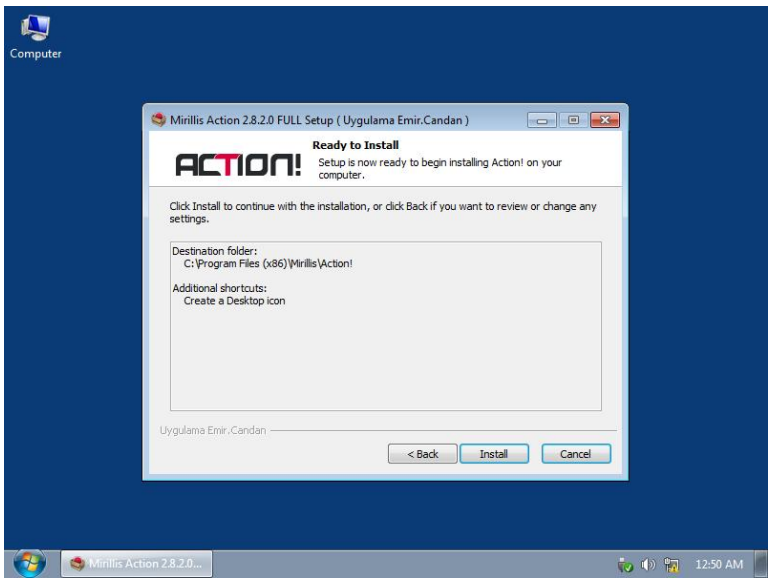

Computer
Action!
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Execute the commands...
Uygulama Emir.Candan
< Back
Next >
Cancel
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Mark facebook.com as Untrusted
Mark fbcdn.net as Untrusted
Forbid Scripts Globally (advised)
Options...
About NoScript 2.9.0.3...
facebook
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Emir Candan
Waiting for cx.atdmt.com...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:51 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
Looking up googleads.g.doubleclick.net...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:51 AM

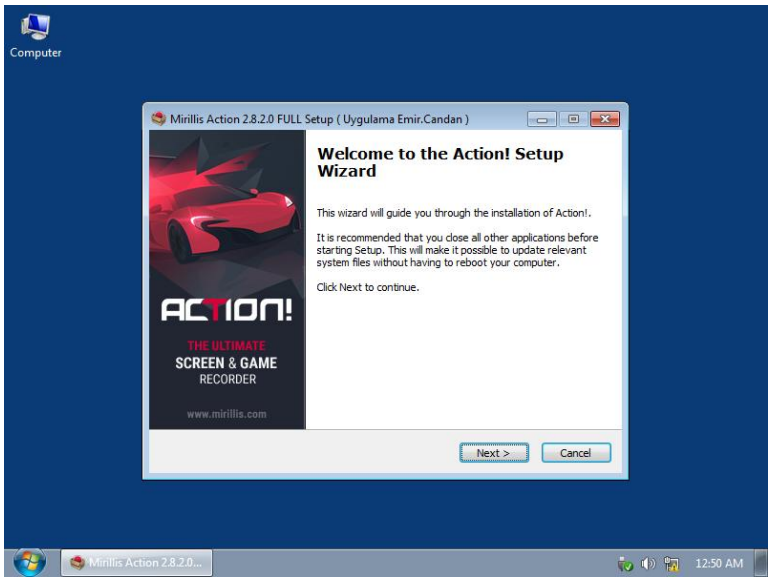

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: register_ficv_codec.bat
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM


Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Ready to Install
Setup is now ready to begin installing Action! on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination folder:
C:\Program Files (x86)\Mirillis\Action!
Additional shortcuts:
Create a Desktop icon
Uygulama Emir.Candan
< Back
Install
Cancel
Mirillis Action 2.8.2.0...
12:50 AM

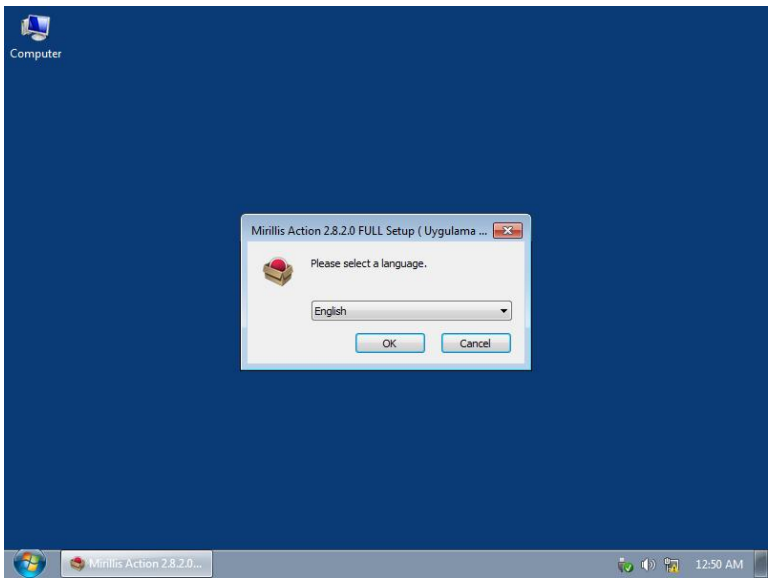

New Tab
Search or enter address


Mozilla Firefox
12:51 AM
Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:52 AM

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
Transferring data from static.xx.fbcdn.net...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:51 AM

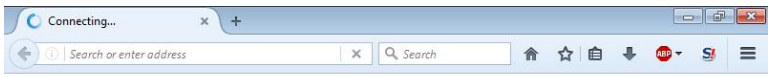

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
Welcome to the Action! Setup Wizard
This wizard will guide you through the installation of Action!.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
ACTION!
THE ULTIMATE
SCREEN & GAME
RECORDER
www.mirillis.com
Next >
Cancel
12:50 AM

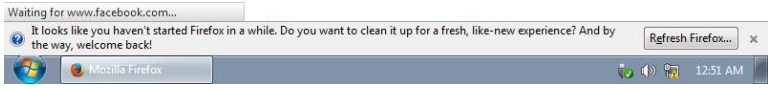

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz
İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM

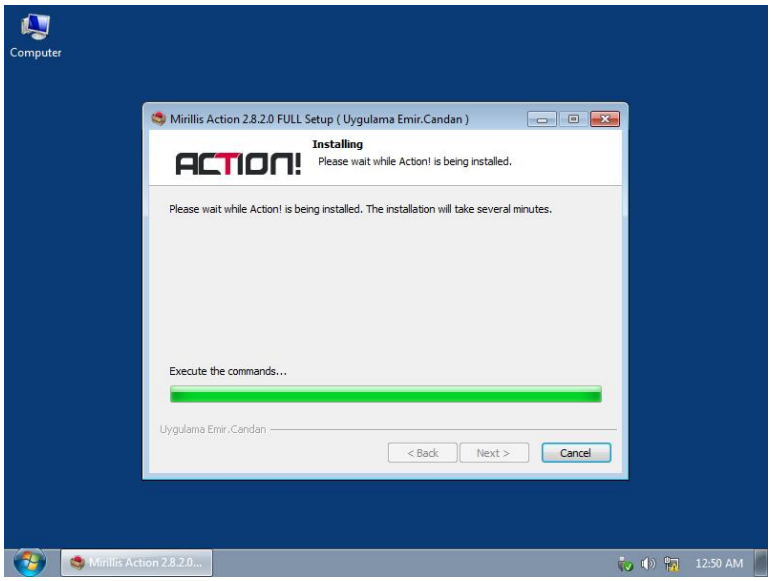

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama ...
Please select a language.
English
OK
Cancel
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:53 AM


Connecting...
Search or enter address
Search


Waiting for www.facebook.com...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Mozilla Firefox
12:51 AM

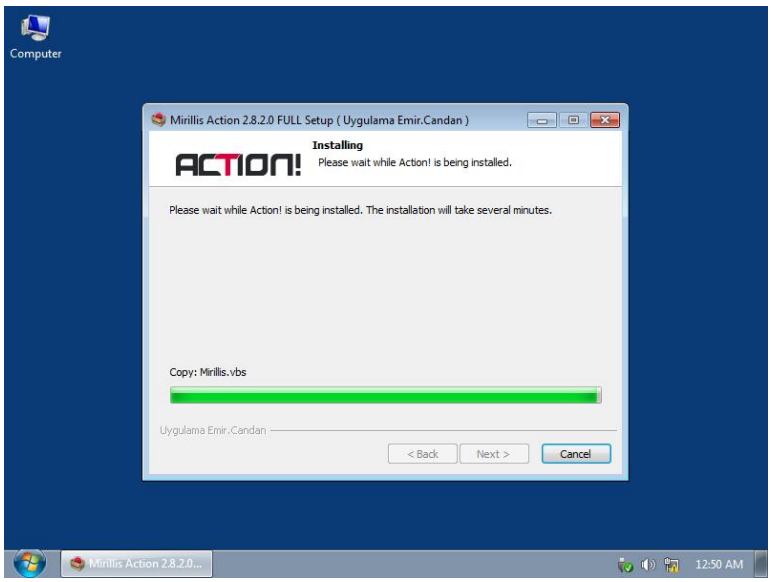

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Execute the commands...
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM

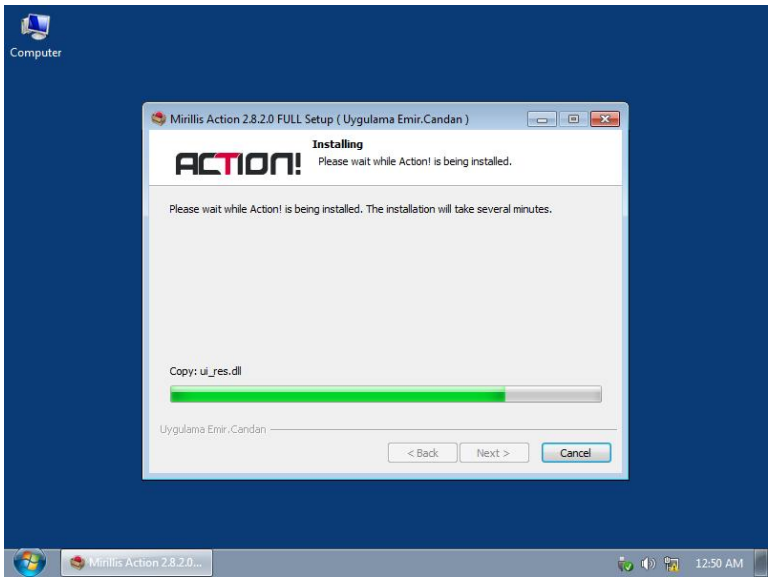

Computer
Action!
12:50 AM

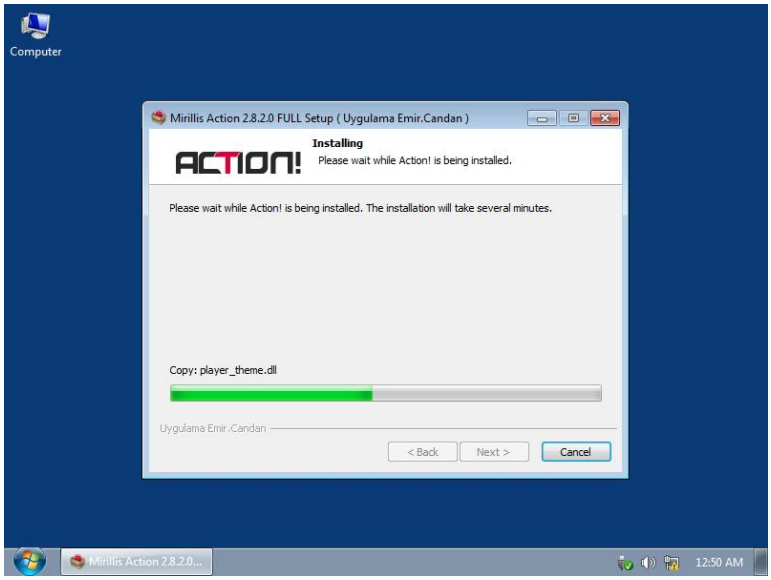

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz
İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:52 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:53 AM

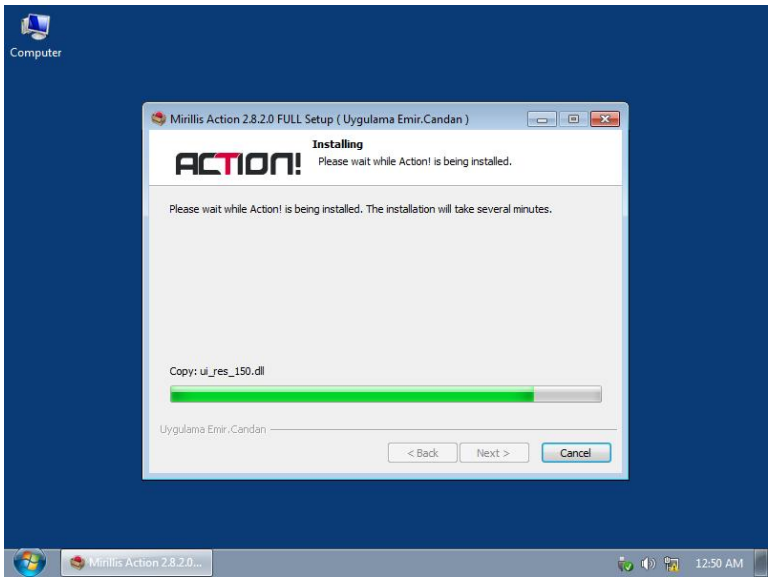

Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:52 AM

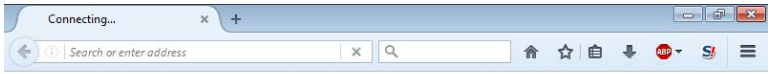

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: Mirillis.vbs
Uygulama Emir.Candan
< Back
Next >
Cancel
12:50 AM

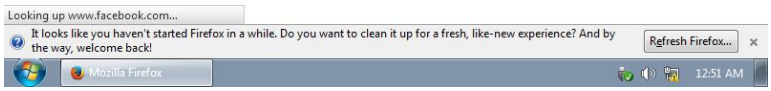

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: ui_res.dll
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM

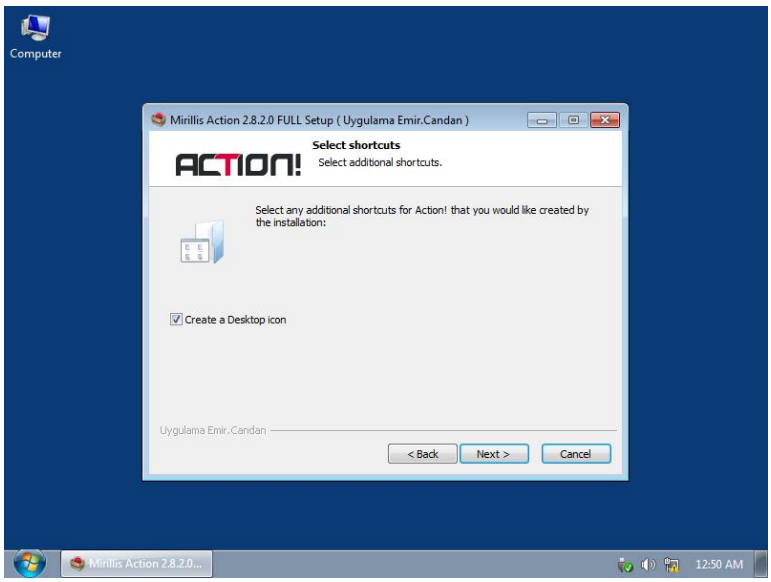

Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: player_theme.dll
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
Search
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
Waiting for cx.atdmt.com...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Emir Candan | Faceb...
12:51 AM


Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Installing
Please wait while Action! is being installed.
Please wait while Action! is being installed. The installation will take several minutes.
Copy: ui_res_150.dll
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM


Connecting...
Search or enter address


Looking up www.facebook.com...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Mozilla Firefox
12:51 AM


Computer
Mirillis Action 2.8.2.0 FULL Setup (Uygulama Emir.Candan)
ACTION!
Select shortcuts
Select additional shortcuts.
Select any additional shortcuts for Action! that you would like created by the installation:
Create a Desktop icon
Uygulama Emir.Candan
< Back
Next >
Cancel
Mirillis Action 2.8.2.0...
12:50 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:51 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
facebook
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Wednesday, March 20, 2019
12:53 AM


Emir Candan | Facebook
https://www.facebook.com/emirr.candan
For a better experience on Facebook, update your browser.
Email or Phone
Password
Forgot account?
Emir Candan is on Facebook.
To connect with Emir, sign up for Facebook today.
Log In
or
Sign Up
Ücretsiz Full Program İndir
Emir Candan
Transferring data from external-dfw5-2.xx.fbcdn.net...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
12:51 AM