VALKYRIE COMODO

Summary

File Name: None

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

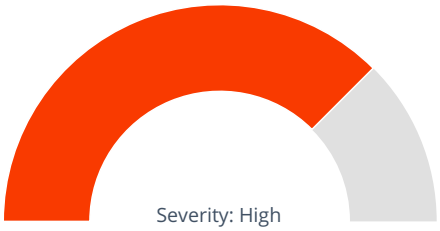
SHA1: 39d3eb36c34e98586ee540b26e4177e441e43e43

MD5: None

MALWARE

Valkyrie Final Verdict

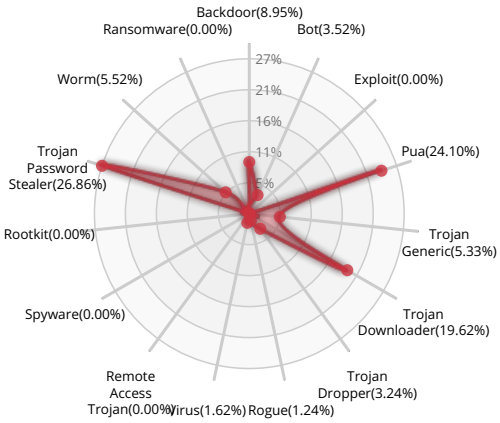
DETECTION SECTION



Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION

ACTIVITY OVERVIEW

Networking 2 (100.00%)

VALKYRIE COMODO

Activity Details

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic — Show sources

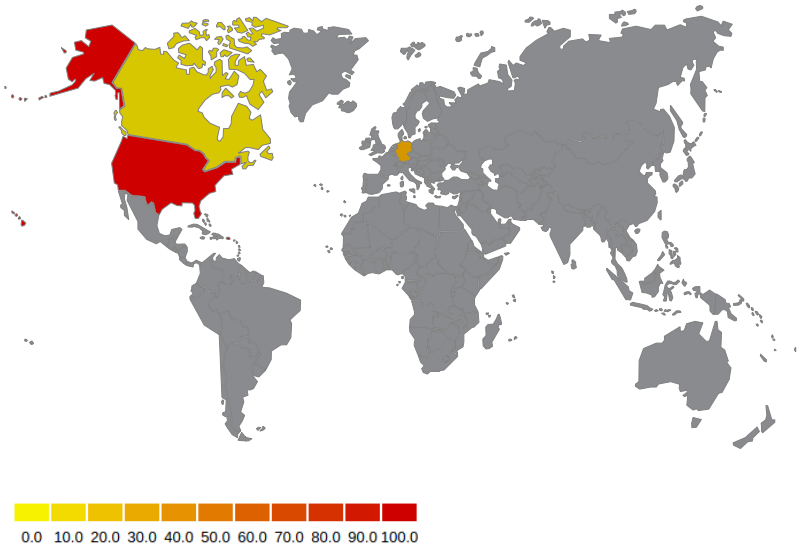
Performs some HTTP requests — Show sources

Behavior Graph

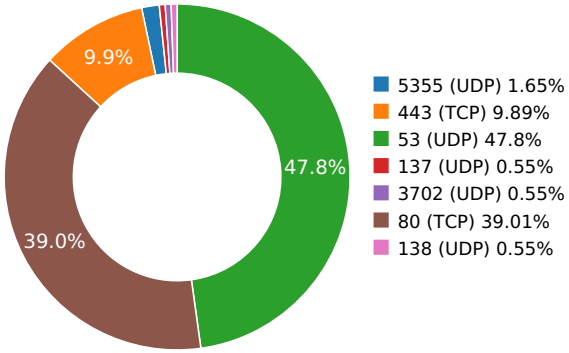
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	209.85.232.154	United States	15169	Google LLC	Malware Process
	23.63.226.179	United States	20940	Akamai Technologies, Inc.	Malware Process
	52.85.89.100	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.89.141	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.89.51	United States	16509	Amazon Technologies Inc.	Malware Process
	54.191.46.28	United States	16509	Amazon.com, Inc.	Malware Process
	54.69.184.117	United States	16509	Amazon Technologies Inc.	Malware Process
	69.164.0.0	United States	22822	Limelight Networks, Inc.	Malware Process
	69.164.0.128	United States	22822	Limelight Networks, Inc.	Malware Process
	69.195.158.198	United States	19969	Joe's Datacenter, LLC	Malware Process
	192.241.99.194	Canada	55286	B2 Net Solutions Inc.	Malware Process
	178.255.83.1		35838		OS Process
	50.112.201.212		16509	Amazon.com, Inc.	Malware Process
	184.173.21.164		36351	SoftLayer Technologies Inc.	Malware Process
	52.73.5.197		14618	Amazon Technologies Inc.	Malware Process
	172.217.7.14		15169	Google LLC	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc....	Malware Process
	69.195.158.197		19969	Joe's Datacenter, LLC	Malware Process
	94.130.73.101		24940		Malware Process
	184.26.44.105		20940	Akamai Technologies, Inc.	Malware Process
	52.85.89.64		16509	Amazon Technologies Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	52.85.89.92		16509	Amazon Technologies Inc.	Malware Process
	35.166.234.151		16509	Amazon Technologies Inc.	Malware Process
	208.111.178.129		22822	Limelight Networks, Inc.	Malware Process
	172.217.7.14		15169	Google LLC	Malware Process
	52.10.153.199		16509	Amazon Technologies Inc.	Malware Process
	52.85.89.64		16509	Amazon Technologies Inc.	Malware Process
	54.148.10.185		16509	Amazon Technologies Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	54.69.224.218		16509	Amazon Technologies Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	208.111.178.129		22822	Limelight Networks, Inc.	Malware Process
	52.85.89.56		16509	Amazon Technologies Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	172.217.10.234		15169	Google LLC	Malware Process
	54.148.143.136		16509	Amazon Technologies Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	209.85.232.157		15169	Google LLC	Malware Process
	208.111.171.129		22822	Limelight Networks, Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	52.85.89.37		16509	Amazon Technologies Inc.	Malware Process
	216.245.208.194		46475	Limestone Networks, Inc.	Malware Process
	52.34.194.250		16509	Amazon Technologies Inc.	Malware Process
	208.111.178.129		22822	Limelight Networks, Inc.	Malware Process
	209.85.232.156		15169	Google LLC	Malware Process
	52.40.133.43		16509	Amazon Technologies Inc.	Malware Process
	184.173.21.164		36351	SoftLayer Technologies Inc.	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	172.217.10.234		15169	Google LLC	Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc....	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	35.164.80.164		16509	Amazon Technologies Inc.	Malware Process
	52.85.89.37		16509	Amazon Technologies Inc.	Malware Process
	184.173.21.164		36351	SoftLayer Technologies Inc.	Malware Process
	208.111.171.129		22822	Limelight Networks, Inc.	Malware Process
	172.217.10.227		15169	Google LLC	Malware Process
	184.173.21.164		36351	SoftLayer Technologies Inc.	Malware Process
	184.26.44.105		20940	Akamai Technologies, Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	52.27.206.225		16509	Amazon Technologies Inc.	Malware Process
	172.217.10.227		15169	Google LLC	Malware Process
	94.130.73.104		24940		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
cc.ppacti.com	80	GET	1.1		1	12.028373003
Path: /productprice.svc/getcountrycode **URI:** http://cc.ppacti.com/productprice.svc/getcountrycode						
www.pcbooster.biz	80	GET	1.1		1	12.202256918
Path: /getIpAddress.asp **URI:** http://www.pcbooster.biz/getIpAddress.asp						
www.advancedpctools.com	80	GET	1.1		1	12.3437108994
Path: //getIpAddress.asp **URI:** http://www.advancedpctools.com//getIpAddress.asp						
trkr.pcbooster.biz	80	GET	1.1		1	12.4696989059
Path: /ipfiles/192_241_99_194.txt **URI:** http://trkr.pcbooster.biz/ipfiles/192_241_99_194.txt						
www.pcbooster.biz	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	15.4447779655
Path: /asc/afterinstall/?x-context=&utm_source=ascsite&utm_campaign=ascsite&utm_medium=ascdefault&utm_pubid=&x-at=&pxl=&x-ip=192_241_99_194&x-datetime=&x-fetch=0&LangID=en&x-ccode=us **URI:** http://www.pcbooster.biz/asc/afterinstall/?x-context=&utm_source=ascsite&utm_campaign=ascsite&utm_medium=ascdefault&utm_pubid=&x-at=&pxl=&x-ip=192_241_99_194&x-datetime=&x-fetch=0&LangID=en&x-ccode=us						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	15.7993049622
Path: //asc/afterinstall/?x-context=&utm_source=ascsite&utm_campaign=ascsite&utm_medium=ascdefault&utm_pubid=&x-at=&pxl=&x-ip=192_241_99_194&x-datetime=&x-fetch=0&LangID=en&x-ccode=us **URI:** http://www.advancedpctools.com//asc/afterinstall/?x-context=&utm_source=ascsite&utm_campaign=ascsite&utm_medium=ascdefault&utm_pubid=&x-at=&pxl=&x-ip=192_241_99_194&x-datetime=&x-fetch=0&LangID=en&x-ccode=us						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	15.889729023
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.int-x3.letsencrypt.org	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	15.948168993
Path: / **URI:** http://ocsp.int-x3.letsencrypt.org/						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.3825359344
Path: /js/jquery.min.js **URI:** http://www.advancedpctools.com/js/jquery.min.js						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4120948315
Path: / **URI:** http://ocsp.digicert.com/						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4430289268

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /css/bootstrap.min.css **URI:** http://www.advancedpctools.com/css/bootstrap.min.css						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4471609592
Path: /css/designer.css **URI:** http://www.advancedpctools.com/css/designer.css						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4473919868
Path: /css/flags.css **URI:** http://www.advancedpctools.com/css/flags.css						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4510228634
Path: /css/styleResponsive.css **URI:** http://www.advancedpctools.com/css/styleResponsive.css						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.4541239738
Path: /js/bootstrap.min.js **URI:** http://www.advancedpctools.com/js/bootstrap.min.js						
www.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.5026819706
Path: /js/jquery.flagstrap.js **URI:** http://www.advancedpctools.com/js/jquery.flagstrap.js						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.595042944
Path: /asc/website/images/fav_icon.ico **URI:** http://cdn.advancedpctools.com/asc/website/images/fav_icon.ico						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.7510390282
Path: /asc/website/images/logo.png **URI:** http://cdn.advancedpctools.com/asc/website/images/logo.png						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.751157999
Path: /asc/website/images/Contact_divider.png **URI:** http://cdn.advancedpctools.com/asc/website/images/Contact_divider.png						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.7792258263
Path: /asc/website/images/Award.png **URI:** http://cdn.advancedpctools.com/asc/website/images/Award.png						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.7804260254
Path: /asc/website/images/compatible.jpg **URI:** http://cdn.advancedpctools.com/asc/website/images/compatible.jpg						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.7806518078
Path: /asc/website/images/email.png **URI:** http://cdn.advancedpctools.com/asc/website/images/email.png						
cdn.advancedpctools.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.7807879448
Path: /asc/website/images/afterinstall.gif **URI:** http://cdn.advancedpctools.com/asc/website/images/afterinstall.gif						
www.google-analytics.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.8192448616
Path: /ga.js **URI:** http://www.google-analytics.com/ga.js						
www.google-analytics.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.8200829029

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /analytics.js **URI:** http://www.google-analytics.com/analytics.js						
ocsp.pki.goog	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	16.8318829536
Path: /GTSGIAG3 **URI:** http://ocsp.pki.goog/GTSGIAG3						
ocsp.pki.goog	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	16.9474408627
Path: /GTSGIAG3 **URI:** http://ocsp.pki.goog/GTSGIAG3						
www.google-analytics.com	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	16.9887909889
Path: /r/__utm.gif?utmwv=5.7.1&utms=1&utmn=1739016911&utmhn=www.advancedpctools.com&utmcs=UTF-8&utmsr=800x600&utmvp=800x463&utmsc=24-bit&utmul=en-us&utmje=1&utmfl=20.0%20r0&utmdt=THANK%20YOU%20FOR%20INSTALLING%20-%20Advance%20System%20Care&utmhid=2002771210&utmr=-&utmp=%2F%2Fasc%2Fafterinstall%2F%3Fx-context%3D%26utm_source%3Dascsite%26utm_campaign%3Dascsite%26utm_medium%3Dascdefault%26utm_pubid%3D%26x-at%3D%26pxl%3D%26x-ip%3D192_241_99_194%26x-datetime%3D%26x-fetch%3D0%26LangID%3Den%26x-ccode%3Dus&utmht=1520539238398&utmac=UA-82355406-1&utmcc=__utma%3D62558844.1238354791.1520539238.1520539238.1520539238.1%3B%2B__utmz%3D62558844.1520539238.1.1.utmcsr%3Dascsite%7Cutmccn Dascsite%7Cutmcmd%3Dascdefault%3B&utmjid=1523496691&utmredir=1&utmu=qAAAAAAAAAAAAAAAAAAAAAE~ **URI:** http://www.google-analytics.com/r/__utm.gif?utmwv=5.7.1&utms=1&utmn=1739016911&utmhn=www.advancedpctools.com&utmcs=UTF-8&utmsr=800x600&utmvp=800x463&utmsc=24-bit&utmul=en-us&utmje=1&utmfl=20.0%20r0&utmdt=THANK%20YOU%20FOR%20INSTALLING%20-%20Advance%20System%20Care&utmhid=2002771210&utmr=-&utmp=%2F%2Fasc%2Fafterinstall%2F%3Fx-context%3D%26utm_source%3Dascsite%26utm_campaign%3Dascsite%26utm_medium%3Dascdefault%26utm_pubid%3D%26x-at%3D%26pxl%3D%26x-ip%3D192_241_99_194%26x-datetime%3D%26x-fetch%3D0%26LangID%3Den%26x-ccode%3Dus&utmht=1520539238398&utmac=UA-82355406-1&utmcc=__utma%3D62558844.1238354791.1520539238.1520539238.1520539238.1%3B%2B__utmz%3D62558844.1520539238.1.1.utmcsr%3Dascsite%7Cutmccn Dascsite%7Cutmcmd%3Dascdefault%3B&utmjid=1523496691&utmredir=1&utmu=qAAAAAAAAAAAAAAAAAAAAAE~						
cdn.ywxi.net	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	17.5418000221
Path: /js/host-loader.js?h=www.advancedpctools.com **URI:** http://cdn.ywxi.net/js/host-loader.js?h=www.advancedpctools.com						
clients1.google.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	2	17.593173027
Path: /ocsp **URI:** http://clients1.google.com/ocsp						
cdn.ywxi.net	80	GET	1.1	Mozilla/5.0 (Windows NT 6...	1	17.7195749283
Path: /js/host.js?v=20180302043822708657&h=advancedpctools.com **URI:** http://cdn.ywxi.net/js/host.js?v=20180302043822708657&h=advancedpctools.com						
ocsp.comodoca.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	17.7876768112
Path: / **URI:** http://ocsp.comodoca.com/						
ocsp.pki.goog	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	17.8437628746
Path: /GTSGIAG3 **URI:** http://ocsp.pki.goog/GTSGIAG3						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	20.9462618828
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	20.9843928814
Path: / **URI:** http://ocsp.digicert.com/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	24.6877508163
Path: / **URI:** http://ocsp.digicert.com/						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
cdn.pcbooster.biz	80	GET	1.1		1	32.9940078259
Path: /asc/asc_upgrades/upgrade_en_us.xml **URI:** http://cdn.pcbooster.biz/asc/asc_upgrades/upgrade_en_us.xml						
ocsp.comodoca.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	2	72.3998959064
Path: / **URI:** http://ocsp.comodoca.com/						
ocsp.comodoca.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	2	72.4434499741
Path: / **URI:** http://ocsp.comodoca.com/						
ocsp.digicert.com	80	POST	1.1	Mozilla/5.0 (Windows NT 6...	1	75.6709148884
Path: / **URI:** http://ocsp.digicert.com/						

DNS QUERIES

Request	Type
cc.ppacti.com	A
Answers - 216.245.208.194 (A)	
www.pcbooster.biz	A
Answers - 184.173.21.164 (A) - pcbooster.biz (CNAME)	
www.advancedpctools.com	A
Answers - advancedpctools.com (CNAME)	
trkr.pcbooster.biz	A
Answers - 69.164.0.0 (A) - 69.164.0.128 (A) - pcvark.vo.llnwd.net (CNAME)	
pcbooster.biz	A
pcbooster.biz	AAAA
search.services.mozilla.com	A
Answers - 54.148.10.185 (A) - 34.211.20.200 (A) - 35.164.80.164 (A) - search.r53-2.services.mozilla.com (CNAME)	
search.r53-2.services.mozilla.com	A
search.r53-2.services.mozilla.com	AAAA
advancedpctools.com	A
advancedpctools.com	AAAA

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)	
secure.informaction.com	AAAA
tiles.services.mozilla.com	A
Answers - 52.39.131.77 (A) - 34.210.37.21 (A) - 54.148.143.136 (A) - 52.43.35.239 (A) - 54.70.252.70 (A) - 52.41.78.152 (A) - 52.40.133.43 (A) - tiles.r53-2.services.mozilla.com (CNAME) - 54.148.131.146 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
tiles.r53-2.services.mozilla.com	A
tiles.r53-2.services.mozilla.com	AAAA
cs9.wac.phicdn.net	A
ocsp.int-x3.letsencrypt.org	A
Answers - a771.dscq.akamai.net (CNAME) - 23.63.226.179 (A) - ocsp.int-x3.letsencrypt.org.edgesuite.net (CNAME) - 23.63.226.144 (A)	
cs9.wac.phicdn.net	AAAA
a771.dscq.akamai.net	A
Answers - 184.26.44.105 (A) - 184.26.44.103 (A)	
a771.dscq.akamai.net	AAAA
Answers - 2600:140a::48f6:2b38 (AAAA) - 2600:140a::48f6:2b2b (AAAA)	
fonts.googleapis.com	A
Answers - googleadapis.l.google.com (CNAME) - 172.217.10.234 (A)	
cdn.advancedpctools.com	A
cdn.ywxi.net	A

Request	Type
Answers - 52.85.89.37 (A) - 52.85.89.100 (A) - 52.85.89.227 (A) - 52.85.89.138 (A) - dtx9pzf7ji0d9.cloudfront.net (CNAME) - 52.85.89.105 (A) - 52.85.89.212 (A) - 52.85.89.156 (A) - 52.85.89.203 (A)	
googleadapis.l.google.com	A
googleadapis.l.google.com	AAAA
Answers - 2607:f8b0:4006:813::200a (AAAA)	
tiles-cloudfront.cdn.mozilla.net	A
Answers - 52.85.89.252 (A) - 52.85.89.61 (A) - 52.85.89.92 (A) - 52.85.89.204 (A) - 52.85.89.19 (A) - 52.85.89.141 (A) - dcky6u1m8u6el.cloudfront.net (CNAME) - 52.85.89.56 (A) - 52.85.89.182 (A)	
pcvark.vo.llnwd.net	A
pcvark.vo.llnwd.net	AAAA
dtx9pzf7ji0d9.cloudfront.net	A
dcky6u1m8u6el.cloudfront.net	A
dtx9pzf7ji0d9.cloudfront.net	AAAA
Answers - 2600:9000:201c:f200:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:600:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:4c00:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:1800:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:e000:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:c00:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:a800:14:6bfc:5740:93a1 (AAAA) - 2600:9000:201c:2600:14:6bfc:5740:93a1 (AAAA)	
www.google-analytics.com	A
Answers - www-google-analytics.l.google.com (CNAME) - 172.217.10.238 (A)	
dcky6u1m8u6el.cloudfront.net	AAAA
www-google-analytics.l.google.com	A
www-google-analytics.l.google.com	AAAA
Answers - 2607:f8b0:4006:813::200e (AAAA)	
ocsp.pki.goog	A

Request	Type
Answers - www3.l.google.com (CNAME)	
www3.l.google.com	A
www3.l.google.com	AAAA
fonts.gstatic.com	A
Answers - 172.217.10.227 (A) - gstaticadssl.l.google.com (CNAME)	
gstaticadssl.l.google.com	A
gstaticadssl.l.google.com	AAAA
Answers - 2607:f8b0:4006:813::2003 (AAAA)	
pcvarkr.hs.llnwd.net	A
pcvarkr.hs.llnwd.net	AAAA
safebrowsing.google.com	A
Answers - sb.l.google.com (CNAME)	
clients1.google.com	A
Answers - clients.l.google.com (CNAME)	
sb.l.google.com	A
clients.l.google.com	A
stats.g.doubleclick.net	A
Answers - stats.l.doubleclick.net (CNAME) - 209.85.232.156 (A) - 209.85.232.154 (A) - 209.85.232.157 (A) - 209.85.232.155 (A)	
clients.l.google.com	AAAA
sb.l.google.com	AAAA
stats.l.doubleclick.net	A
stats.l.doubleclick.net	AAAA
Answers - 2607:f8b0:400d:c0d::9c (AAAA)	
ocsp.comodoca.com	A
Answers - 178.255.83.1 (A)	
ocsp.comodoca.com	AAAA
Answers - 2a02:1788:2fd::b2ff:5301 (AAAA)	
sites.fastspring.com	A

Request	Type
Answers - 52.86.92.18 (A) - 52.73.5.197 (A)	
safebrowsing-cache.google.com	A
Answers - safebrowsing.cache.l.google.com (CNAME) - 172.217.7.14 (A)	
safebrowsing.cache.l.google.com	A
safebrowsing.cache.l.google.com	AAAA
Answers - 2607:f8b0:4006:800::200e (AAAA)	
sites.fastspring.com	AAAA
self-repair.mozilla.org	A
Answers - shield-normandy-elb-prod-2099053585.us-west-2.elb.amazonaws.com (CNAME) - 54.69.184.117 (A) - self-repair.r53-2.services.mozilla.com (CNAME) - 35.166.234.151 (A) - 52.10.153.199 (A)	
shield-normandy-elb-prod-2099053585.us-west-2.elb.amazonaws.com	A
shield-normandy-elb-prod-2099053585.us-west-2.elb.amazonaws.com	AAAA
shavar.services.mozilla.com	A
Answers - 50.112.201.212 (A) - 54.69.100.200 (A) - shavar.prod.mozaws.net (CNAME) - 52.34.194.250 (A) - 54.191.46.28 (A) - 34.214.15.91 (A) - 52.42.20.106 (A)	
shavar.prod.mozaws.net	A
shavar.prod.mozaws.net	AAAA
tracking-protection.cdn.mozilla.net	A
Answers - 52.85.89.168 (A) - 52.85.89.205 (A) - 52.85.89.184 (A) - 52.85.89.106 (A) - d1zkz3k4cclnv6.cloudfront.net (CNAME) - 52.85.89.71 (A) - 52.85.89.64 (A) - 52.85.89.51 (A) - 52.85.89.83 (A)	
d1zkz3k4cclnv6.cloudfront.net	A
d1zkz3k4cclnv6.cloudfront.net	AAAA
cdn.pcbooster.biz	A
easylist-downloads.adblockplus.org	A

Request	Type
Answers - 136.243.88.49 (A) - 148.251.66.238 (A) - 176.9.26.105 (A) - 144.76.116.39 (A) - 94.130.73.101 (A) - 144.76.219.20 (A) - 178.63.70.146 (A) - 78.46.93.235 (A) - 88.99.186.158 (A) - 46.4.115.44 (A) - 144.76.137.234 (A) - 144.76.20.58 (A) - 88.198.17.12 (A) - 178.63.13.4 (A) - 94.130.73.103 (A) - 148.251.12.230 (A) - 46.4.7.165 (A) - 94.130.73.112 (A) - 88.99.186.151 (A) - 94.130.76.59 (A) - 78.46.66.108 (A) - 88.99.186.149 (A)	
notification.adblockplus.org	A
Answers - 148.251.238.203 (A) - easylist-downloads.adblockplus.org (CNAME) - 144.76.153.101 (A) - 85.10.210.166 (A) - 176.9.146.200 (A) - 5.9.15.86 (A) - 213.239.192.206 (A) - 94.130.104.87 (A) - 136.243.22.80 (A) - 88.99.186.159 (A)	
easylist-downloads.adblockplus.org	AAAA
Answers - 2a01:4f8:202:30ed::2 (AAAA) - 2a01:4f8:202:81c8::2 (AAAA) - 2a01:4f8:110:4168::2 (AAAA) - 2a01:4f8:c0c:2d11::2 (AAAA) - 2a01:4f8:130:11ee::2 (AAAA) - 2a01:4f8:c0c:3842::2 (AAAA) - 2a01:4f8:c0c:3843::2 (AAAA) - 2a01:4f8:200:7348::2 (AAAA)	
aus5.mozilla.org	A
Answers - 34.210.48.174 (A) - 34.208.7.8 (A) - 52.24.21.9 (A) - balrog-aus5.r53-2.services.mozilla.com (CNAME) - 54.148.132.67 (A) - 52.27.206.225 (A) - 35.162.46.217 (A) - 34.208.65.55 (A) - 52.88.57.64 (A)	
balrog-aus5.r53-2.services.mozilla.com	A

Request	Type
balrog-aus5.r53-2.services.mozilla.com	AAAA

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.028373003	Sandbox	216.245.208.194	80
12.202256918	Sandbox	184.173.21.164	80
12.3437108994	Sandbox	184.173.21.164	80
12.4696989059	Sandbox	69.164.0.128	80
15.4447779655	Sandbox	184.173.21.164	80
15.694494009	Sandbox	35.164.80.164	443
15.7993049622	Sandbox	184.173.21.164	80
15.8290748596	Sandbox	69.195.158.198	443
15.889729023	Sandbox	72.21.91.29	80
15.9353039265	Sandbox	54.148.143.136	443
15.948168993	Sandbox	23.63.226.179	80
16.4430289268	Sandbox	184.173.21.164	80
16.4471609592	Sandbox	184.173.21.164	80
16.4473919868	Sandbox	184.173.21.164	80
16.4510228634	Sandbox	184.173.21.164	80
16.4541239738	Sandbox	184.173.21.164	80
16.5325348377	Sandbox	172.217.10.234	443
16.595042944	Sandbox	69.164.0.0	80
16.6377878189	Sandbox	52.85.89.141	443
16.751157999	Sandbox	69.164.0.0	80
16.7776658535	Sandbox	52.85.89.100	443
16.7792258263	Sandbox	69.164.0.0	80
16.7804260254	Sandbox	69.164.0.0	80
16.7806518078	Sandbox	69.164.0.0	80
16.7807879448	Sandbox	69.164.0.0	80
16.8192448616	Sandbox	172.217.10.238	80
16.8195428848	Sandbox	172.217.10.238	443
16.8200829029	Sandbox	172.217.10.238	80
16.8318829536	Sandbox	172.217.10.238	80
17.4191999435	Sandbox	172.217.10.227	443
17.5418000221	Sandbox	52.85.89.100	80
17.576032877	Sandbox	172.217.10.238	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
17.593173027	Sandbox	172.217.10.238	80
17.6219010353	Sandbox	172.217.10.238	80
17.6350779533	Sandbox	69.164.0.128	443
17.7876768112	Sandbox	178.255.83.1	80
17.798197031	Sandbox	209.85.232.154	443
18.0033249855	Sandbox	172.217.7.14	443
20.7417700291	Sandbox	54.69.184.117	443
24.5650959015	Sandbox	54.191.46.28	443
24.9070780277	Sandbox	52.85.89.51	443
32.9940078259	Sandbox	69.164.0.128	80
72.0920939445	Sandbox	176.9.26.105	443
72.1390078068	Sandbox	85.10.210.166	443
72.3998959064	Sandbox	178.255.83.1	80
72.4001808167	Sandbox	178.255.83.1	80
72.4434499741	Sandbox	178.255.83.1	80
72.4583899975	Sandbox	178.255.83.1	80
73.5053329468	Sandbox	52.27.206.225	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.19502592087	Sandbox	224.0.0.252	5355
3.27008581161	Sandbox	192.168.56.255	137
3.27325582504	Sandbox	224.0.0.252	5355
3.31202197075	Sandbox	239.255.255.250	3702
5.82968187332	Sandbox	224.0.0.252	5355
9.26469492912	Sandbox	192.168.56.255	138
11.9486169815	Sandbox	8.8.4.4	53
12.1104369164	Sandbox	8.8.4.4	53
12.2586119175	Sandbox	8.8.4.4	53
12.4080238342	Sandbox	8.8.4.4	53
15.3859019279	Sandbox	8.8.4.4	53
15.4682848454	Sandbox	8.8.4.4	53
15.5121488571	Sandbox	8.8.4.4	53
15.5627849102	Sandbox	8.8.4.4	53
15.6555700302	Sandbox	8.8.4.4	53
15.7160799503	Sandbox	8.8.4.4	53
15.7614510059	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
15.7617788315	Sandbox	8.8.4.4	53
15.793006897	Sandbox	8.8.4.4	53
15.8171339035	Sandbox	8.8.4.4	53
15.8285679817	Sandbox	8.8.4.4	53
15.8312809467	Sandbox	8.8.4.4	53
15.8400409222	Sandbox	8.8.4.4	53
15.8578119278	Sandbox	8.8.4.4	53
15.8643670082	Sandbox	8.8.4.4	53
15.8954918385	Sandbox	8.8.4.4	53
15.8965499401	Sandbox	8.8.4.4	53
15.9337408543	Sandbox	8.8.4.4	53
16.0788419247	Sandbox	8.8.4.4	53
16.4901659489	Sandbox	8.8.4.4	53
16.4904270172	Sandbox	8.8.4.4	53
16.4906318188	Sandbox	8.8.4.4	53
16.5163578987	Sandbox	8.8.4.4	53
16.579654932	Sandbox	8.8.4.4	53
16.5800068378	Sandbox	8.8.4.4	53
16.580755949	Sandbox	8.8.4.4	53
16.6306769848	Sandbox	8.8.4.4	53
16.6313669682	Sandbox	8.8.4.4	53
16.6315829754	Sandbox	8.8.4.4	53
16.6749169827	Sandbox	8.8.4.4	53
16.6878008842	Sandbox	8.8.4.4	53
16.6946268082	Sandbox	8.8.4.4	53
16.7140350342	Sandbox	8.8.4.4	53
16.7398338318	Sandbox	8.8.4.4	53
16.7905290127	Sandbox	8.8.4.4	53
16.8214409351	Sandbox	8.8.4.4	53
16.8530550003	Sandbox	8.8.4.4	53
17.287321806	Sandbox	8.8.4.4	53
17.3155579567	Sandbox	8.8.4.4	53
17.3409919739	Sandbox	8.8.4.4	53
17.4055738449	Sandbox	8.8.4.4	53
17.4622309208	Sandbox	8.8.4.4	53
17.4954819679	Sandbox	8.8.4.4	53
17.5382678509	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
17.5398290157	Sandbox	8.8.4.4	53
17.5811040401	Sandbox	8.8.4.4	53
17.5818359852	Sandbox	8.8.4.4	53
17.585901022	Sandbox	8.8.4.4	53
17.6125910282	Sandbox	8.8.4.4	53
17.6128809452	Sandbox	8.8.4.4	53
17.6187639236	Sandbox	8.8.4.4	53
17.6453478336	Sandbox	8.8.4.4	53
17.768362999	Sandbox	8.8.4.4	53
17.779460907	Sandbox	8.8.4.4	53
17.7910788059	Sandbox	8.8.4.4	53
17.9661319256	Sandbox	8.8.4.4	53
17.9664378166	Sandbox	8.8.4.4	53
17.9932208061	Sandbox	8.8.4.4	53
18.0145258904	Sandbox	8.8.4.4	53
18.0185818672	Sandbox	8.8.4.4	53
18.0541880131	Sandbox	8.8.4.4	53
20.5506930351	Sandbox	8.8.4.4	53
20.7391009331	Sandbox	8.8.4.4	53
20.7624628544	Sandbox	8.8.4.4	53
24.4608700275	Sandbox	8.8.4.4	53
24.4718270302	Sandbox	8.8.4.4	53
24.4961400032	Sandbox	8.8.4.4	53
24.8279960155	Sandbox	8.8.4.4	53
24.8962030411	Sandbox	8.8.4.4	53
24.9454689026	Sandbox	8.8.4.4	53
32.9170398712	Sandbox	8.8.4.4	53
71.9838728905	Sandbox	8.8.4.4	53
72.0307598114	Sandbox	8.8.4.4	53
72.0313458443	Sandbox	8.8.4.4	53
72.0418748856	Sandbox	8.8.4.4	53
72.0428569317	Sandbox	8.8.4.4	53
72.3711078167	Sandbox	8.8.4.4	53
72.3717548847	Sandbox	8.8.4.4	53
72.3856480122	Sandbox	8.8.4.4	53
72.4009928703	Sandbox	8.8.4.4	53
73.4075269699	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.4191408157	Sandbox	8.8.4.4	53
73.4298398495	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	39d3eb36c34e98586ee540b26e4177e441e43e43
MD5:	None
First Seen Date:	2017-11-06 21:39:26.685264 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-11-06 21:39:26.685264 (2 years ago)
Human Expert Analysis Date:	2017-11-07 17:10:42.672273 (2 years ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	8
Compilation Time Stamp	0x5698AC5A [Fri Jan 15 08:22:50 2016 UTC]
LegalCopyright	
FileVersion	1.0.0.2502
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Advance -System Care
ProductVersion	1.0.0.2502
FileDescription	Advance -System Care Setup
Translation	0x0000 0x04b0
Entry Point	0x4113bc (.itext)
Machine Type	Intel 386 or later - 32Bit
File Size	5013480
Sha256	2f5858e0cabd4600649440ae358c5cff05687e484f71b86f67d9e642556bab00
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xf134	0xf200	6.39169445915	1a600bbd86f701d3e6b2978b57906082
.itext	0x11000	0xb44	0xc00	5.7430519764	0b6f227afa44fd825f60bccacb9073bf
.data	0x12000	0xc88	0xe00	2.24753305436	da9cb156b6104ba552cb70804b8a50a3
.bss	0x13000	0x56b8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x19000	0xdd0	0xe00	4.97188203377	93d91a2b90e60bd758fc0c4908856ae1
.tls	0x1a000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x1b000	0x18	0x200	0.20448815744	3dffc444ccc131c9dcee18db49ee6403
.rsrc	0x1c000	0x179c8	0x17a00	5.11444157397	8fa633f323281672d5794a324a362d4e

PE Imports

- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- advapi32.dll

    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
- user32.dll
    - GetKeyboardType
    - LoadStringW
    - MessageBoxA
    - CharNextW
- kernel32.dll
    - GetACP
    - Sleep
    - VirtualFree
    - VirtualAlloc
    - GetSystemInfo
    - GetTickCount
    - QueryPerformanceCounter
    - GetVersion
    - GetCurrentThreadId
    - VirtualQuery
    - WideCharToMultiByte
    - MultiByteToWideChar
    - lstrlenW
    - lstrcpynW
    - LoadLibraryExW
    - GetThreadLocale
    - GetStartupInfoA
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetCommandLineW
    - FreeLibrary
    - FindFirstFileW
    - FindClose
    - ExitProcess
    - WriteFile
    - UnhandledExceptionFilter
    - RtlUnwind
    - RaiseException
    - GetStdHandle
    - CloseHandle
- kernel32.dll
    - TlsSetValue
    - TlsGetValue
    - LocalAlloc
    - GetModuleHandleW
- user32.dll
    - CreateWindowExW
    - TranslateMessage
    - SetWindowLongW
    - PeekMessageW
    - MsgWaitForMultipleObjects
    - MessageBoxW
    - LoadStringW
    - GetSystemMetrics
    - ExitWindowsEx
    - DispatchMessageW
    - DestroyWindow
    - CharUpperBuffW
    - CallWindowProcW
- kernel32.dll
    - WriteFile
    - WideCharToMultiByte
    - WaitForSingleObject
    - VirtualQuery
    - VirtualProtect
    - VirtualFree
    - VirtualAlloc
    - SizeofResource
    - SignalObjectAndWait
    - SetLastError
    - SetFilePointer
    - SetEvent
    - SetErrorMode
    - SetEndOfFile

    - ResetEvent
    - RemoveDirectoryW
    - ReadFile
    - MultiByteToWideChar
    - LockResource
    - LoadResource
    - LoadLibraryW
    - GetWindowsDirectoryW
    - GetVersionExW
    - GetUserDefaultLangID
    - GetThreadLocale
    - GetSystemInfo
    - GetStdHandle
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetLastError
    - GetFullPathNameW
    - GetFileSize
    - GetFileAttributesW
    - GetExitCodeProcess
    - GetEnvironmentVariableW
    - GetDiskFreeSpaceW
    - GetCurrentProcess
    - GetCommandLineW
    - GetCPInfo
    - InterlockedExchange
    - InterlockedCompareExchange
    - FreeLibrary
    - FormatMessageW
    - FindResourceW
    - EnumCalendarInfoW
    - DeleteFileW
    - CreateProcessW
    - CreateFileW
    - CreateEventW
    - CreateDirectoryW
    - CloseHandle
- advapi32.dll
    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
    - OpenProcessToken
    - LookupPrivilegeValueW
- comctl32.dll
    - InitCommonControls
- kernel32.dll
    - Sleep
- advapi32.dll
    - AdjustTokenPrivileges

PE Resources

RT_ICON
RT_STRING
RT_RCDATA
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Success ✔

[+] Syscare Logics Inc	
Status	NoError ✔
Start Date	2017-06-01 00:00:00+00:00
End Date	2018-06-01 23:59:59+00:00
Sha256	eee1e6bb93a1f1483c1b115a13cc80ff03fe34cc39d0e10734104b0c3347edfb
Serial	00C215EFBBA0144FF0ADD34E172C59B2F3
Subject Key Identifier	1e 0e 93 b0 78 cc 3b 54 3d a6 1e 87 3c 59 3a 5b 04 37 54 97
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

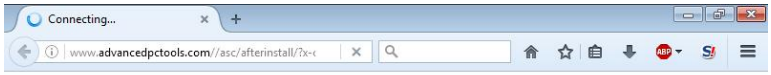
[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

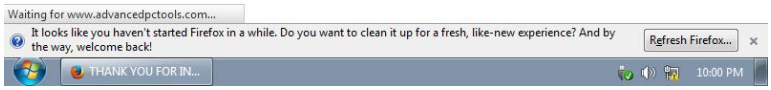
[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

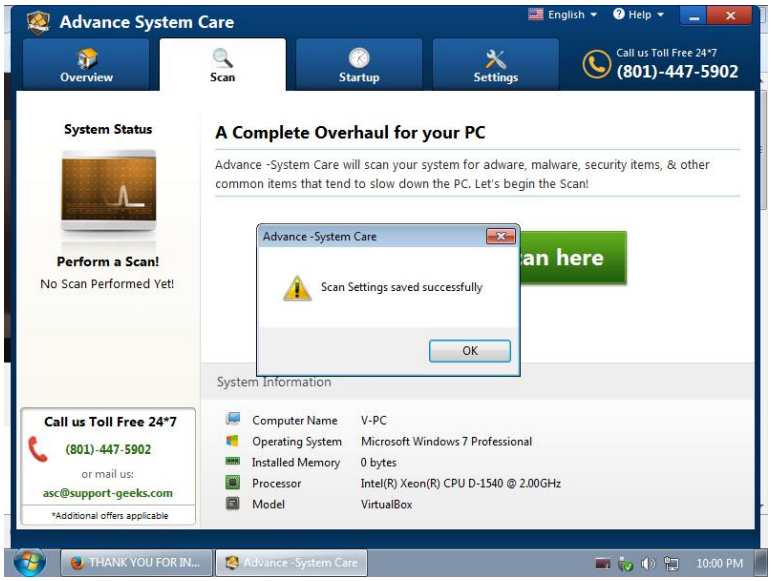
[+] GlobalSign Timestamping CA - G2	
Status	NoError ✔
Start Date	2011-04-13 10:00:00+00:00
End Date	2028-01-28 12:00:00+00:00
Sha256	0f870989c6b1f8082f91361833e8a61864a760c50594398911ffe34531cd1065
Serial	0400000000012F4EE152D7
Subject Key Identifier	46 d8 3e ff dc e3 be ff 83 e6 f4 85 9b b0 dd 6a d6 14 a9 c1
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Crl link	http://crl.globalsign.net/root.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

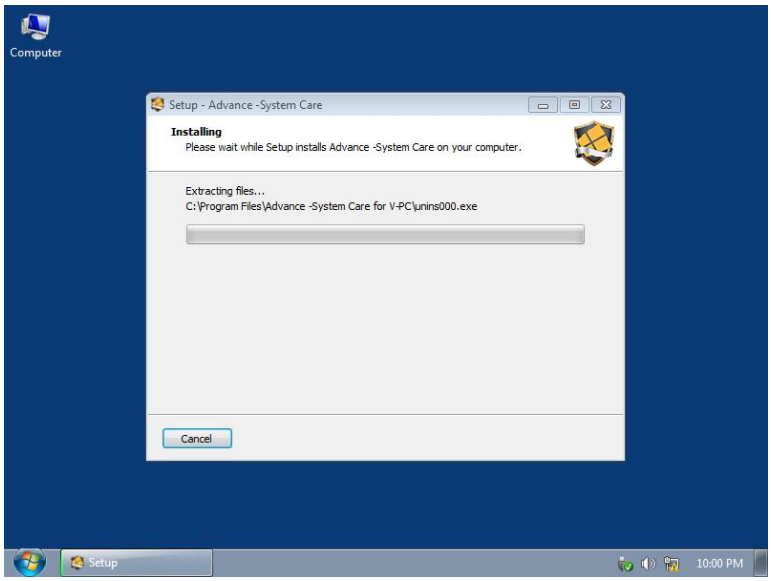
[+] GlobalSign Root CA	
Status	NoError ✔
Start Date	1998-09-01 12:00:00+00:00
End Date	2028-01-28 12:00:00+00:00
Sha256	8890262a3cd37c0b6c37c0239b9533f33244fb4ec82b6d846f6bd379ed2184b7
Serial	040000000001154B5AC394
Subject Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

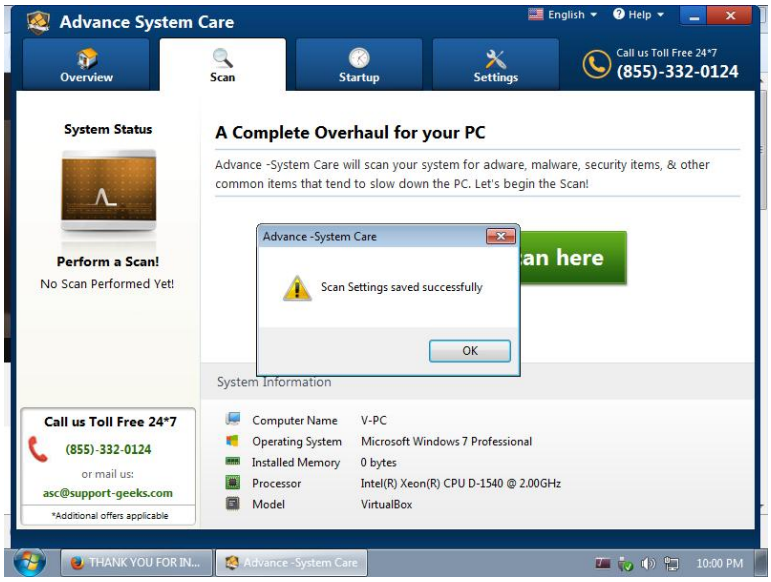
SCREENSHOTS

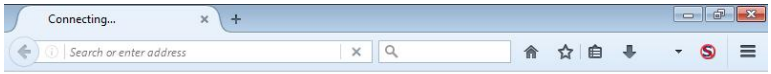

Connecting...
www.advancedpctools.com//asc/afterinstall/?x=


Waiting for www.advancedpctools.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...
THANK YOU FOR IN...
10:00 PM

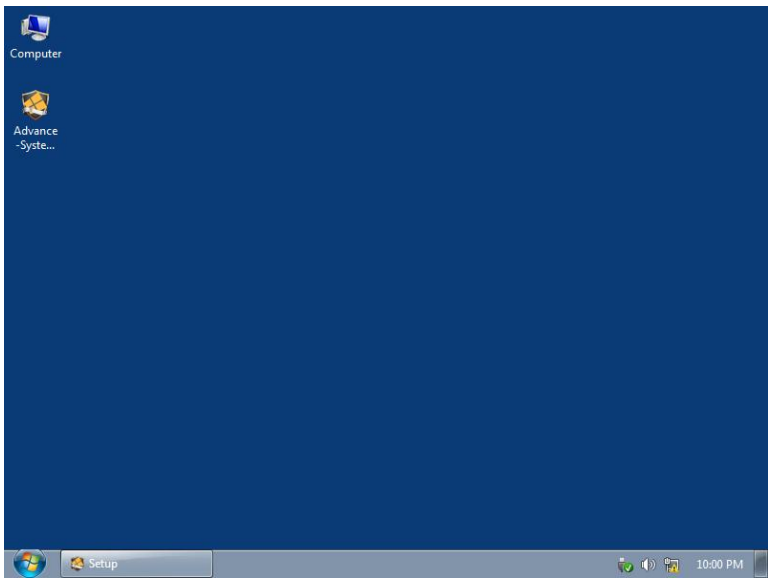

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(801)-447-5902
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Advance -System Care
Scan Settings saved successfully
OK
an here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(801)-447-5902
or mail us:
asc@support-geeks.com
*Additional offers applicable
THANK YOU FOR IN...
Advance -System Care
10:00 PM


Computer
Setup - Advance -System Care
Installing
Please wait while Setup installs Advance -System Care on your computer.
Extracting files...
C:\Program Files\Advance -System Care for V-PC\unins000.exe
Cancel
Setup
10:00 PM

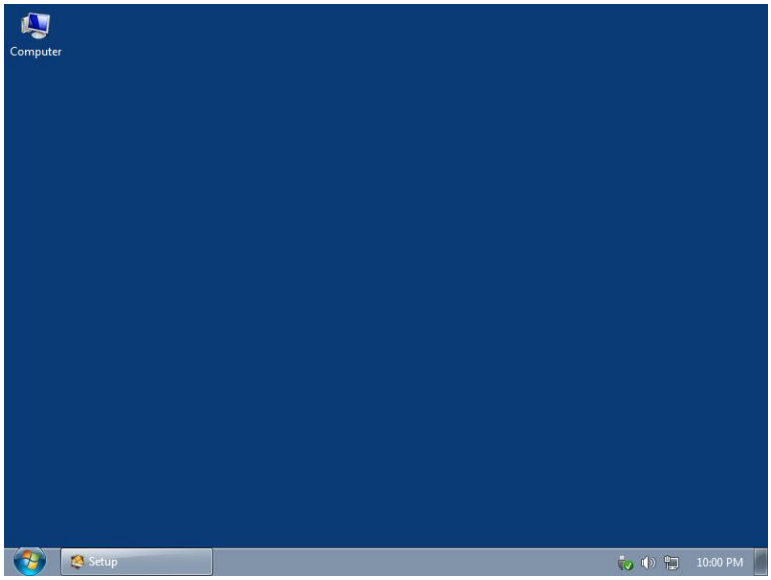

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(855)-332-0124
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Advance -System Care
Scan Settings saved successfully
OK
an here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(855)-332-0124
or mail us:
asc@support-geeks.com
*Additional offers applicable
THANK YOU FOR IN...
Advance -System Care
10:00 PM

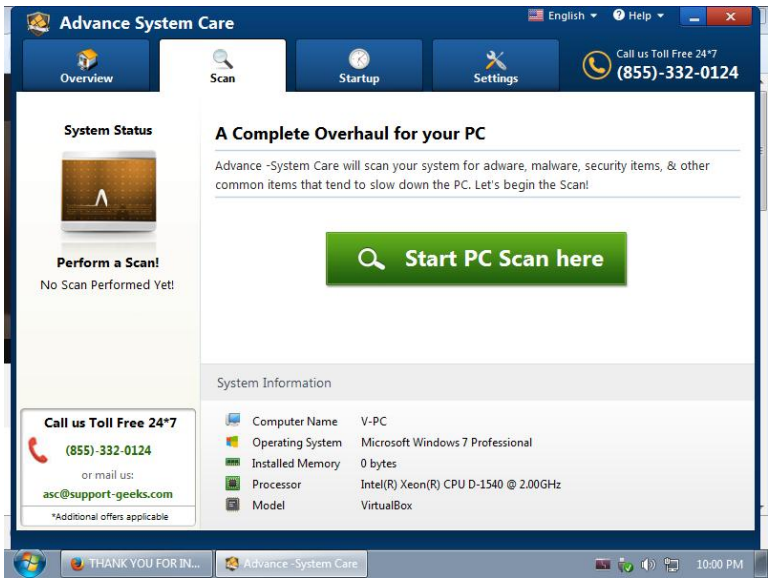

Connecting...
Search or enter address

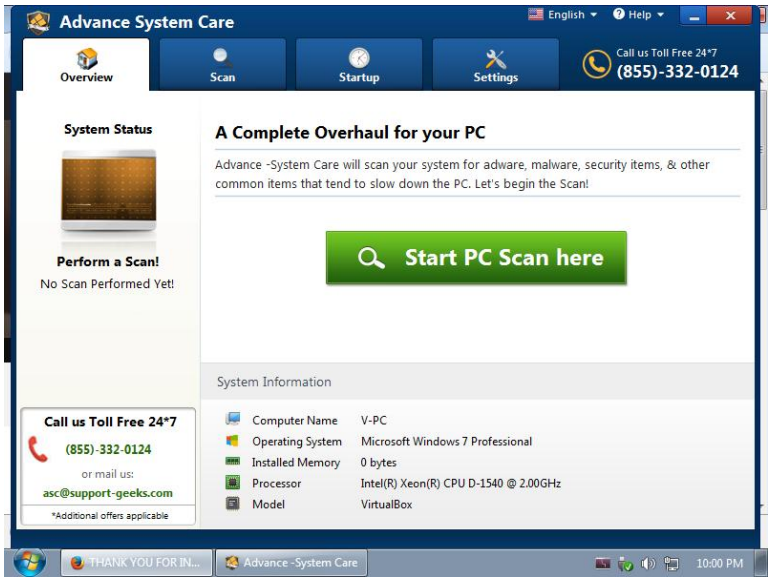

the way, welcome back!
Refresh Firefox...
Mozilla Firefox
10:00 PM

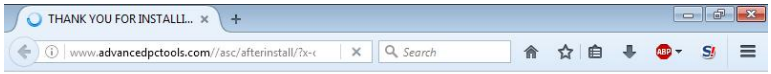

Computer
Advance -Syste...
Setup
10:00 PM

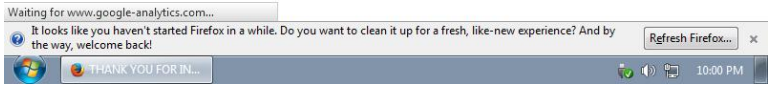

Computer
Setup - Advance -System Care
Advance System Care
Welcome to the Advance -System Care Setup Wizard
This will install Advance -System Care on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
End User License Agreement
By clicking "Next" button below you accept and agree to the End User License Agreement (EULA).
Terms of use Privacy Policy
Using Microsoft Technologies
Cancel
Next >
Setup
10:00 PM

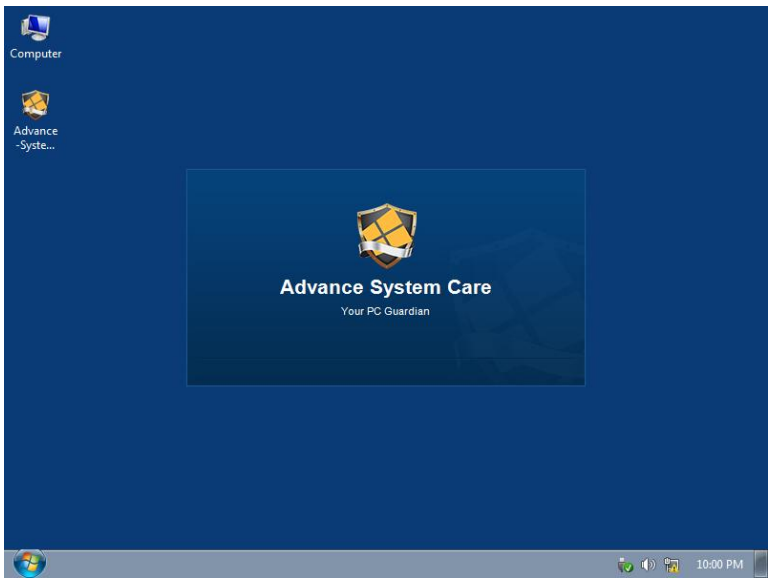

Computer
Setup
10:00 PM

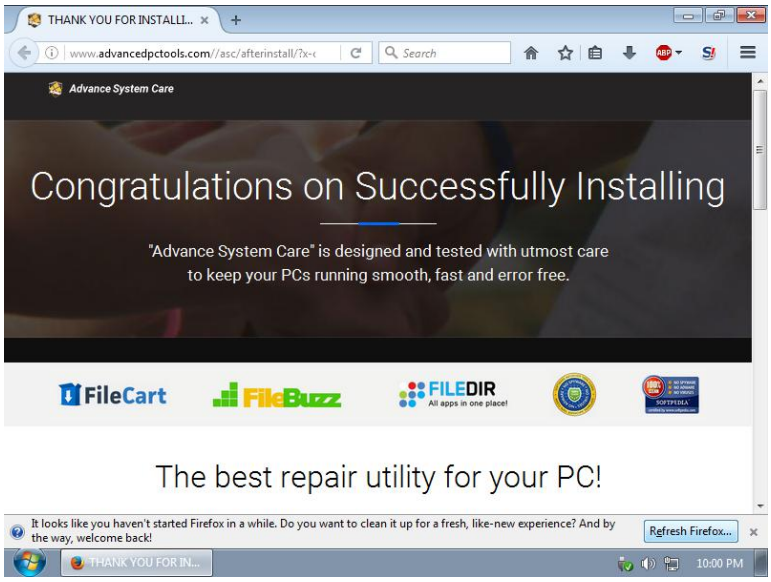

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(855)-332-0124
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Start PC Scan here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(855)-332-0124
or mail us:
asc@support-geeks.com
*Additional offers applicable
THANK YOU FOR IN...
Advance -System Care
10:00 PM

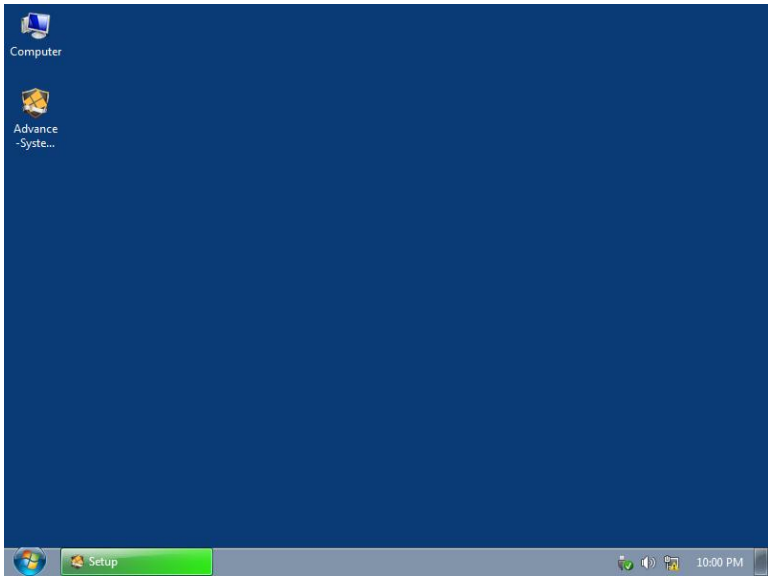

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(855)-332-0124
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Start PC Scan here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(855)-332-0124
or mail us:
asc@support-geeks.com
*Additional offers applicable
THANK YOU FOR IN...
Advance -System Care
10:00 PM


THANK YOU FOR INSTALLI...
www.advancedpctools.com//asc/afterinstall/?x=
Search


Waiting for www.google-analytics.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...
THANK YOU FOR IN...
10:00 PM


Computer
Advance -Syste...
Advance System Care
Your PC Guardian
10:00 PM


THANK YOU FOR INSTALLL...
www.advancedpctools.com//asc/afterinstall/?x=
Search
Advance System Care
Congratulations on Successfully Installing
"Advance System Care" is designed and tested with utmost care
to keep your PCs running smooth, fast and error free.
FileCart
FileBuzz
FILEDIR
All apps in one place!
The best repair utility for your PC!
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...
THANK YOU FOR IN...
10:00 PM


Computer
Advance
-Syste...
Setup
10:00 PM