TrendLabs

Pop-up Ads and Over a Hundred Sites are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware

Appendix

TrendLabs Security Intelligence Blog

Joseph C. Chen

Cyber Safety Solutions Team

March 2018

Malicious Domains:

- activatetool.com
- allupdates.net
- bestofkeygen.com
- ckfile.com
- crack4k.com
- crackandkeygen.com
- crackasm.com
- crackedits.com
- crackednow.com
- crackedpc.com
- crackedpc.org
- crackedreal.com
- crackflare.com
- crackfullpc.com
- crackfullworld.com
- crackithub.com
- crackkey.net
- crackkeys.org
- cracklists.com
- crackmakes.com
- crackorigin.com
- crackprowin.com
- cracksapp.com
- cracksbeforesoft.com
- cracksbook.com
- cracksbox.com
- cracksea.com
- crackslink.com
- cracksmine.com
- cracksofthub.com
- cracksone.com
- crackstell.com
- crackswall.com
- crackswar.com

- crackswell.com
- crackswin.com
- crackswork.com
- crackszone.net
- cracktorrent.com
- crackworld.net
- crackxonly.com
- crackzee.com
- cracx.com
- cracx.net
- cracxactivator.com
- cracxfree.com
- cracxtool.com
- daily2crack.com
- fdcrack.com
- flamboyantly.info
- freeactivators.com
- freesoftsfiles.com
- fullactivators.com
- fullcrackmac.com
- fullsoftwarez.com
- haxcrack.com
- haxkeys.com
- haxri.com
- hdcrack.com
- howtocracksoft.com
- hqcrack.com
- insiderex.com
- itisfile.com
- keygensoftware.com
- keygenworld.com
- lcrack.com
- lumion8crack.com
- macactivator.com
- maccrack.net
- macinwin.com
- macupdater.com
- maqprosoft.co

- onhaxapk.me
- onhaxcrack.me
- pcactivators.com
- pccracked.com
- pcfullversion.com
- pcprocrack.com
- pcsoftnkeygen.com
- pcsoftwarespro.com
- pcwarez.org
- postapk.com
- procracks.net
- procracksoft.com
- procrackz.com
- procracx.com
- prosoftcrack.com
- racracks.com
- realcracks.net
- realcracksoft.com
- rootcracked.com
- secrack.com
- shoaibpc.com
- snapcrack.net
- softactivator.com
- softenia.com
- softnkeygen.com
- softsasm.com
- softshere.com
- softsmob.com
- softwaresa2z.com
- softwaresdaily.com
- softwaresdaily.net
- softwareshax.com
- softwarespatch.com
- softwarezcrack.com
- softwarezpro.com
- theinspiron.com
- thepcwares.com
- warezcrack.net

- warezkeys.com
- warezx.net
- winsoftmac.com
- workingkeygen.com
- www.keysfull.com
- zipsoftwares.com
- epictorrents.com
- etorrent.club

Related SHA256:

SHA256	Detection
a7a09ba7c9dc34fe28836310863f47c9f945ac3f53225c26310d0eb967888f7d	TROJ_SMOKELOADER.A
3dafda982f1775498018b660a7cb97cf42c0362362aa1124ca14534f92f097c0	PUA_ICLOADER
d6c32a028f1b49fd7e5aa2ed6abf1dc6843951be095ec0d262370238b08901c2	TROJ_SMOKELOADER.A
0e8beaf0504f3d14cf85d4362797bad98ad3fb7b36bb89b09482ae1ac8aedaff	TROJ_AZORULT.A
2137ac079e435087125529bcd96bee3021837dd87f3f0cbf69153d787bee8d83	RANSOM_GANDCRAB.TIAOBGC
a717e5991bb3a4516b2a120d219e21944428e2b7deb2ab6733849839be07e8f4	TSPY_URSNIF.TIBAIAX
d3cfa3a6b06f8468fc95a4cfb105c199923240f6a7721707a10128898ca52351	PUA_INERINO
8a13b3b6b86668c0b73e6e2a41019aad3facb7ef76ca75588f01e25eb68ddca9	COINMINER_MALXMR.TIBAFR
6b4a1ef616c2554592d12c29c30ae04f46dc4c71e8e5b52c802ba4	PUA_INERINO

f161f8cedb	
ab23bb13cda920a539dd43b72f4348be1df358f3a3a1889cbc66d1d58e989fd5	PUA_INERINO
84a3dea39e10cc4066036013219bd0faed4a453ce36012b4e51ef9a4100b6282	PUA_ICLoader
e331a165ede87506376e0d4ce3135abdb610d82001b5a8cb27ff99b62a153a78	COINMINER_MALXMR.TIBAFR
1cd1275d15a2c1f7dcfdae2f5c33a24279d1c0e8d352a039edda3d281670ac95	PUA_ICLoader
fdc5e87411376fe5b7eec1fe1bf6b3447b88b022a72ebc9b91d2ced7bc1b00ff	PUA_ICLoader
24BB36D9543CF1DE86EF442CC50C10A3A3D3A3D577226D6E9BFFBBAFD3542ECD	PUA_INERINO
600afae6b9509dda4cdf8486251cf4846effb59e585ccf31aca8e0a923a8eacc	PUA_INERINO
18ccea7115a2921234e16747555dd94e1cfdc79b8081aeafac0061691cdb4b87	COINMINER_MALXMR.TIBAFR
d85abae0348bb6c7fd793c88dd7d7b5196bbc08b4ffc479198805ce231ed87ee	TROJ_SMOKELOADER.A
bf4b944d01a39c5c426315310671f5f309d7348fbc5113110cb3b6a9bb063644	RANSOM_GANDCRAB.TIAOBGC
b1b5e89c3c60281730264f968213427ea127d885ce8a008b83943883afa2bd29	TROJ_SMOKELOADER.A
83aeeea83e2a727abb18b1a7b13da7b0e4961668bb40ee98aa046200c6908d5e	TROJ_AZORULT.A
35a5ad36c0d441c51fb331590233870a7195041b09b52c18bb43b444ed5de944	TROJ_NEUTRINO.B

4b766e422d3bc2121a3ecdd20d7ca18eedf6fa3b55b4628782af7cae643db883	PUA_ICLoader

Command and Control Domains:

inerino[.]ru	iNerino C&C Domain
chlen[.]bit	SmokeLoader C&C Domain
d3s1[.]me	SmokeLoader C&C Domain
godz[.]bit	SmokeLoader C&C Domain
ram1[.]bit	SmokeLoader C&C Domain
tretiuybbd[.]top	SmokeLoader C&C Domain
boorgen[.]pw	SmokeLoader C&C Domain
advstat5[.]win	SmokeLoader C&C Domain
advstat70[.]host	SmokeLoader C&C Domain
readybit7[.]win	SmokeLoader C&C Domain
spaceclub30[.]win	SmokeLoader C&C Domain
needyoulove[.]pw	AZORult C&C Domain
gidrobon[.]pw	AZORult C&C Domain
watermaker10[.]bit	NeutrinoBot C&C Domain
gdcb[.]bit	GandCrab Ransomware C&C Domain
malwarehunterteam[.]bit	GandCrab Ransomware C&C Domain

politiaromana[.]bit	GandCrab Ransomware C&C Domain

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO