侵入の痕跡（Indicators of Compromise, IoC）

バックドア

SHA256	ファイル名	検出名
4070e977823d74478aec248862302063918fda16b57f2c3b561018605bfbf4fe	svchîst.exe1	Backdoor.Win32.RADMIN.CMU
57bf83837c18a75d2e7327cdf5bfdcc906ccf78d82237ec961a4f1bee85473cf	install.exe1	Trojan.Win32.ZAPIZ.A
9b6b1807f886bb9eccdc170988d6e419e4301c96817f362aca3d01df17c352fd	reg.exe1	
90728a5b2f22460e1b28e3dc350a95b993a185a6170b4aa5e45b57834b90bcee	Zoom 5.0.1 RUS, ENG.exe	Trojan.Win32.ZAPIZ.THA

Devil Shadow ボットネット

SHA256	ファイル名	検出名
a26f3981ed3784bb86f5223bf14fb0047ff3fd86b8fc94753ce5a3f1702ebb56	Zoom installer.exe	Backdoor.Win32.DEVILSHADOW.THEAABO
93bf084daddb10b3760f4e4424b1bc4d5d5590c30064045d01c8658a6fe50d3a	pyclient.cmd1	
f01da52509792a52c6def452b3ee9b0b78acaca399341926fbe4f3212c42a55e	boot-startup.vbs1	Trojan.BAT.DEVILSHADOW.THEAABO
5b7804919d437688c8811e85c54cb36efba72652bac8093833ca04b811ea87b7	cmd_shell.exe1	Trojan.Win32.DEVILSHADOW.THEAABO
628928fe61e86d3b246a7822b1d1505d3694becc4a73e373f73653851d22f1a5	new_script.txt1	Trojan.JS.DEVILSHADOW.THEAABO
65f725f380c9b90d409539b74bfbd8a57f0fa48843ee79838fa57ad28240feb5	shell.bat1	Trojan.BAT.DEVILSHADOW.THEAABO

関連する URL

hosting303[.]000webhostapp[.]com/devil_shadow	Malware accomplice
madleets[.]ddns[.]net	C&C server

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com