侵入の痕跡（Indicators of Compromise, IoC）

SHA256 値	Trend Micro 検出名	ファイル名	概要
7f505a1064ea09daba577aa553efbf3385c890ab5aac2ace6ef3e927f480fb87	Trojan.VBS.CVE20188174.AMT	vbs.vbs	BottleEK に利用される CVE-2018-8174
96e91a1f656fb70339f8f4e383e7f967d25c1a414f436ddffc692518ace579ad	Trojan.SWF.CVE201815982.AK	swf.swf	BottleEK に利用される CVE-2018-15982
01bf58c650b6ba30733c14026fcff4ecfc24becdd05637a84ef2a7e86aff3fe0	TrojanSpy.Win32.CONNIP.SM	EVSSL.exe	Cinobi V1 のハッシュ
ed7b5c16cb5c4f56b3ded279688b693ec52389cacc0b81e940b0591b7f68aa84	Trojan.Win32.SYSTELEK.A	N/A	Cinobi V2 のハッシュ
914eb64b93cbb631c710ef6cbd0f9cedf93415be421ccc6e285b288b87f3a246	TrojanSpy.Win32.CONNIP.SM	N/A	
c1b67a30119107365c4a311479794e07afb631980a649749501cb9f511fb0ab4	TrojanSpy.Win32.CONNIP.SM	N/A	
a9ea7e952ce38bf8bc14114325ca2a1bfed16f63798028565a669808b8b728dc	TrojanSpy.Win32.CONNIP.SM	N/A	
14842334ac730f417f2730dec9898491575341da3721584a49d44fbf02f1fa6a	TrojanSpy.Win32.CONNIP.SM	foepcyof.dll	Cinobi V2 のハッシュ (Stage 2 DLL)
b1d30ee17a4d1fae263ea0ca696765d2f48b727c9953009c079ed2cb3ee15ab9	TrojanSpy.Win32.CONNIP.SM		Cinobi V2 のハッシュ (Stage 3 DLL)

db1e379c66c41debf58062e0865527a8a5bd7b37b5f43e06c80540a47ac7f5a4	TrojanSpy.Win32.CONNIP.SM		Cinobi V2 のハッシュ (Stage 4 DLL)

ドメイン	説明
shop[.]inteleksys[.]com	Bottle エクスプロイトキットのドメイン
view[.]inteleksys[.]com	
priv[.]inteleksys[.]com	
sales[.]inteleksys[.]com	
xizr[.]inteleksys[.]com	
byte[.]inteleksys[.]com	
cionx[.]inteleksys[.]com	Cinobi V1 C&C ドメイン
5frjkvw2w3wv6dnv[.]onion	Cinobi V2 C&C Tor ドメイン
4w6ylniamu6x7e3a[.]onion	
bank-japanpostpo[.]jp	Cinobi V1 を拡散するフィッシングドメイン
bank-japanpost[.]com	
bank-japanposst[.]jp	
bank-japanpostjp[.]com	
jp-bank-japanossts[.]jp	
jp-bamk[.]jp	
japanp0st[.]jp	
ts3cardd[.]com	

security-amazon[.]jp	Operation Overtrap に繋がるフィッシングドメイン
safety-amazon[.]jp	
safetb-amazon[.]jp	

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