侵入の痕跡（Indicators of Compromises、IoCs）

SHA256	検出名
649675baef92381ffcdfa42e8959015e83c1ab1c7bbfd64635ce5f6f65efd651	BKDR_WATERBEAR.ZTGF
3909e837f3a96736947e387a84bb57e57974db9b77fb1d8fa5d808a89f9a401b	TROJ_WATERBEAR.ZTGD
fcfdd079b5861c0192e559c80e8f393b16ba419186066a21aab0294327ea9e58	TROJ_WATERBEAR.ZTGJ
3f26a971e393d7f6ce7bf4416abdbfa1def843a0cf74d8b7bb841ca90f5c9ed9	TROJ_WATERBEAR.ZTGH
abb91dfd95d11a232375d6b5cdf94b0f7afb9683fb7af3e50bcecdb2bd6cb035	TROJ_WATERBEAR.ZTGH
bda6812c3bbba3c885584d234be353b0a2d1b1cbd29161deab0ef8814ac1e8e1	TROJ_WATERBEAR.ZTGI
53402b662679f0bfd08de3abb064930af40ff6c9ec95469ce8489f65796e36c3	TROJ_WATERBEAR.ZTGH
f9f6bc637f59ef843bc939cb6be5000da5b9277b972904bf84586ea0a17a6000	TROJ_WATERBEAR.ZTGI
3442c076c8824d5da065616063a6520ee1d9385d327779b5465292ac978dec26	BKDR_WATERBEAR.ZTGD
7858171120792e5c98cfa75ccde7cba49e62a2aeb32ed62322aae0a80a50f1ea	TROJ64_WATERBEAR.ZTGI
acb2abc7fb44c2fdea0b65706d1e8b4c0bfb20e4bd4dcee5b95b346a60c6bd31	BKDR_WATERBEARENC.ZTGF
b9f3a3b9452a396c3ba0ce4a644dd2b7f494905e820e7b1c6dca2fdcce069361	BKDR64_WATERBEAR.ZTGD
7c0d2782a33debb65b488893705e71a001ea06c4eb4fe88571639ed71ac85cdd	BKDR_WATERBEARENC.ZTGH
c7c7b2270767aaa2d66018894a7425ba6192730b4fe2130d290cd46af5cc0b7b	BKDR_WATERBEARENC.ZTGI
7532fe7a16ba1db4d5e8d47de04b292d94882920cb672e89a48d07e77ddd0138	BKDR_WATERBEARENC.ZTGI
dea5c564c9d961ccf2ed535139fbfca4f1727373504f2972ac92acfaf21da831	BKDR_WATERBEARENC.ZTGI

05d0ab2fbeb7e0ba7547afb013d307d32588704daac9c12002a690e5c1cde3a4	BKDR64_WATERBEARENC.ZTGJ
39668008deb49a9b9a033fd01e0ea7c5243ad958afd82f79c1665fb73c7cfadf	BKDR_WATERBEARENC.ZTGD

この脅威についての「MITRE ATT&CK」による攻撃手法分類

Tactic	Technique	ID	Description
Execution	Execution through Module Load	T1129	Dynamically loads the DLLs through the shellcode
	Execution through API	T1106	Dynamically loads the APIs through the shellcode
Persistence	Hooking	T1179	Hooks security product's commonly used APIs
Privilege Escalation	Process Injection	T1055	Injects the decrypts payload into *svchost.exe* process
	Hooking	T1179	Hooks security products' commonly used APIs
Defense Evasion	Binary Padding	T1009	Adds junk data to evade anti-virus scan
	Disabling Security Tools	T1089	Targets a specific security product's process for injection purposes

	Deobfuscate/Decode Files or Information	T1140	Uses TROJ_WATERBEAR to decrypt encrypted payload
	Execution Guardrails	T1480	Targets specific software in the victim's environment
	DLL Side-Loading	T1073	Uses modified legitimate DLL to load the malicious DLL
	Process Injection	T1055	Injects the decrypted payload into svchost.exe process
Exfiltration	Exfiltration Over Command and Control Channel	T1041	Possibly sends collected data to attackers via C&C channe

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