■ 侵入の痕跡（Indicators of Compromise、IoC）

SHA-256	検出名
f7d270ca0f2b4d21830787431f881cd004b2eb102cc3048c6b4d69cb775511c8	Ransom.MSIL.CRYNG.A
e687308cd4184e17c33fa9e44686e7d6a4d73adf65f7fb3cac9c4ad765b4ffdf	Ransom.Win32.CRING.C
771a680f9a09a7a73ac2678f31f4d82fce49c046cc5f4c415cea5310b833911f	Trojan.BAT.DISABLER.AA
71821ddb0b49f5b91fc520ca3de1c5ea7cee3bf166ddebd625859966fc5221a2	Trojan.BAT.CRING.A
a999e096a9fb6a994f4d58b04001c61bb2d1fd0d4f0fa87a5be0b61b23591f24	Trojan.PS1.COBEACON.FAIN

MITRE ATT&CK が公開している「戦術（Tactics）」および「手法（Techniques）」

戦術（Tactics）	手法（Technique）
初期アクセス（Initial Access）	T1078: Valid Accounts T1190: Exploit Public-Facing Application
実行（Execution）	T1059: Command and Scripting Interpreter
持続性（Persistence）	T1546.012: Event Triggered Execution: Image File Execution Options Injection

特権の昇格（Privilege Escalation）	T1078.002: Valid Accounts: Domain Accounts
セキュリティ回避（Defense Evasion）	T1562.001: Impair Defenses: Disable or Modify Tools T1070.004: Indicator Removal on Host: File Deletion
認証情報へのアクセス（Credential Access）	T1003: OS Credential Dumping T1552: Unsecured Credentials
探索（Discovery）	T1083: File and Directory Discovery
ラテラルムーブメント/横展開（Lateral Movement）	T1570: Lateral Tool Transfer T1105: Remote File Copy T1021: Remote Services
コマンド＆コントロール（Command and Control）	T1090: Proxy T1105: Ingress Tool Transfer T1043: Commonly Used Port T1188: Multi-hop Proxy T1094: Custom Command and Control Protocol
情報送出（Exfiltration）	T1041: Exfiltration Over C2 Channel
影響（Impact）	T1486: Data Encrypted for Impact T1489: Service Stop T1485: Data Destruction T1490: Inhibit System Recovery

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 thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com