■ 侵入の痕跡（Indicators of Compromise、IoC）

URL

- **hxxp://185.150.117[.]186:80/asdfgsdhsdfgsdfg** （**Cobalt Strike** のダウンロード先 **URL**）

SHA256

マルウェア	SHA256	検出名
Exploit Agent	a70729b3241154d81f2fff506e5434be0a0c38135 4a84317958327970a125507	Trojan.Win64.NEKTO.YACCAT
Coroxy ドロッパ	2ef9a4f7d054b570ea6d6ae704602b57e27dee15f 47c53decb16f1ed0d949187	Trojan.Win32.COROXY.SMYXBC3A
Coroxy	c170717a69847bb7b050832c55fcd2a214e9180c 8cde5f86088bd4e5266e2fd9	Backdoor.Win64.COROXY.YACCAT
DataSpy	a290ce75c6c6b37af077b72dc9c2c347a2eede4faf a6551387fa8469539409c7	TrojanSpy.PS1.DATASPY.B
Nokoyawa	e097cde0f76df948f039584045acfa6bd7ef863141 560815d12c3c6e6452dce4	Ransom.Win64.NOKO.YACBL

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