侵入の痕跡（Indicators of Compromise, IoC）

ファイル名	検出名	用途	SHA256
sys64.dll	Backdoor.Win64.COBEACON.SMA	Wave 1	Unable to retrieve (from SPN data)
tup2.bat	Trojan.BAT.COBALSTART.A	creates scheduled task for s.bat	4cfb525902490909512d065a59ae820c99ec6129f7ea785d89bc20e7f7384509
tup3.bat	Trojan.BAT.COBALSTART.A	creates scheduled task for vd.exe	0043aa3c5236d901333db1a4c9e0fd6e40a27b3f5330bca8a59de78e30758334
s.bat	Trojan.BAT.CONTISTART.A	Executes xx.dll	52c851fc784e175cd2a029abfad62d3bf0408bed85d77d4f94d363e892bc4d60
xx.dll	Ransom.Win64.CONTI.A	For ransomware file encryption	cb6eac0222102b6dcb72386aea373e89640f7c3a335591b561e56f35633f2bda
sys64.dll	Backdoor.Win64.COBALT.AG	Communicate with C&C	105d2eef1c6802e2ba3da84afe5ed91e986b55e77fefe1b6a203d3131ead6269

vd.exe/v.exe	Backdoor.Win64.COBALT.AH	Communicate with C&C	c27875b0053bdddbfd121d21dc3cdb8bbf41091c8a8a0614c666aec8b4d3b612
rclone32.exe	N/A	Exfiltration tool	eb03aba46e818640013bfe6b94367cae216a9ad02dabe69f241e3ace3f1a9f37
at.dll	Trojan.Win64.ROZENA.AJ	Wave 3 – Cobalt Strike beacon	1c947639ec826b462e6c36416c873d26c11b081de707d9b5d963e30b59d9234d
up.dll	Trojan.Win64.ROZENA.AJ	Wave 3 – Cobalt Strike beacon	246907de4674c7a327a1a0b7ce92e50edd7cd02f56d6a008acc134f5fb5bb71c
up.dll	Trojan.Win64.ROZENA.AJ	Wave 3 – Cobalt Strike beacon	d1c1e7edc840a0623e0fdc9f2689133339e3ce58da1e24bce513a4673b9ce054

C&C サーバ:

IP Address: 23[.]82[.]128[.]116

Domain Name: secost[.]com

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