侵入の痕跡（Indicators of Compromise, IoC）

今回の攻撃キャンペーンに関連する以下のハッシュは、トレンドマイクロ製品で検出されます。

SHA256	SHA1	Trend Micro Detection
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2f1a5a7411d015d01aaee4535835400191645023	Backdoor.MSIL.SUNBURST.A
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	75af292f34789a1c782ea36c7127bf6106f595e8	Trojan.MSIL.SUPERNOVA.A
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	d130bd75645c2433f88ac03e73395fba172ef676	Backdoor.MSIL.SUNBURST.A
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	76640508b1e7759e548771a5359eaed353bf1eec	Backdoor.MSIL.SUNBURST.A
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	1b476f58ca366b54f34d714ffce3fd73cc30db1a	Backdoor.MSIL.SUNBURST.A

今回の攻撃キャンペーンに関連する以下のドメイン名もブロックされています。

- avsvmcloud[.]com
- databasegalore[.]com
- deftsecurity[.]com
- highdatabase[.]com
- incomeupdate[.]com
- panhardware[.]com
- thedoccloud[.]com
- zupertech[.]com
- seobundlekit[.]com
- solartrackingsystem[.]net
- freescanonline[.]com
- kubecloud[.]com
- globalnetworkissues[.]com
- digitalcollege[.]org
- lcomputers[.]com
- webcodez[.]com
- virtualwebdata[.]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