

■侵入の痕跡（Indicators of Compromise、IoC）

今回の記事に関する侵入の痕跡はこちらを参照してください。

URLs

- dabmaster[.]wm01[.]to
- hxxps://213.188.152.96/recv7[.]php

SHA-256	検出名
753418831fcf215fe2d00ed33b9d2f1ed78bc92355e780c782 fb35228007318e	Backdoor.Win32.REVCODE.T HDBABO

※調査協力：Raphael Centeno、Mc Justine De Guzman、Augusto Remillano II

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