侵入の痕跡（Indicators of Compromise, IoC）

SHA256	旧検出名	新検出名
66545fffeed4f413827f9dc51d2444aaa772adf4d44f65662356b1301e45390d	Backdoor.Linux.MIRAI.VWIUJ	IoT.Linux.MIRAI.VWISI

コマンド＆コントロール（C&C）サーバ

- methcnc[.]duckdns[.]org
- methscan[.]duckdns[.]org

「Deep Discovery ™ Inspector」は、以下のルールによって本記事で解説した脆弱性を利用する攻撃を検知します。

- 2452 – Wget Commandline Injection
- 2544 – JAWS Remote Code Execution Exploit – HTTP (Request)
- 2575 – Command Injection via UPnP SOAP Interface – HTTP (Request)
- 2692 – LINKSYS Unauthenticated Remote Code Execution Exploit – HTTP (Request)
- 2713 – AVTECH Command Injection Exploit – HTTP (Request)
- 2786 – ThinkPHP 5x Remote Code Execution – HTTP (Request)
- 2865 – CVE-2018-17173 LG Supersign Remote Code Execution – HTTP (Request)
- 4689 – Comtrend – Remote Command Execution Exploit – HTTP (REQUEST)

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