侵入の痕跡（Indicators of Compromise, IoC）

ファイル名	SHA-256	検出名
happy.jpg 20200209122021_qifxyren.jpg	F28876A7F162FF9CDD608F07EE45F8E9211DA4304B3602152D0386CEEAC82442	TrojanSpy.Win32.DNESPY.A
sad.jpg 20200209122021_abjeuitk.jpg	15D80E616B6B5FEC3CFA0EEED5AC9037F34C4547AE27F5DFCAA5475501DE4B95	TrojanSpy.Win32.AGFSPY.A
20200209122021_abjeuitk.jpg	8304FCCCAF18546CAF94851C63DC8293EAF8DE575AB442D4419AA9ED29EA8614	TrojanSpy.Win32.AGFSPY.A

URLs

whoami2[.]ddns[.]net	dneSpy が利用する C&C サーバのドメイン
whoamimaster[.]ddns[.]net	dneSpy が利用する C&C サーバのドメイン
selectorioi[.]ddns[.]net	agfSpy が利用する C&C サーバのドメイン
agf[.]zapto[.]org	agfSpy が利用する C&C サーバのドメイン
rs[.]myftp[.]biz	シェルコードが利用する C&C サーバのドメイン

TrendMicro™DeepSecurity™および User Protection ソリューションは、以下のルールによって、本ブログ記事で解説した Operation EarthKitsune における脆弱性を利用した攻撃を検知します。

- 1010544 - GNUBoard SQL Injection Vulnerability （EDB-ID-7927）
- 1005613 - Generic SQL Injection Prevention – 2

- 1005933 - Identified Directory Traversal Sequence In Uri Query Parameter
- 1010542 - GNUBoard 'tb.php' SQL Injection Vulnerability （CVE-2011-4066）
- 1010543 - GNUBoard 'ajax.autosave.php' SQL Injection Vulnerability （CVE-2014-2339）
- 1010545 - GNUBoard Local File Inclusion Vulnerability （EDB-ID-7927）
- 1010546 - GNUBoard Local/Remote File Include Vulnerability （CVE-2009-0290）
- 1010547 - GNUBoard Remote Code Execution Vulnerability （KVE-2018-0449 and KVE-2018-0441）

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