侵入の痕跡（Indicators of Compromise, IoC）

指標	説明	検出名
mail2000tw[.]com	Earth Wendigo によって運営されるドメイン	
bf[.]mail2000tw[.]com	Earth Wendigo によって運営されるドメイン	
admin[.]mail2000tw[.]com	Earth Wendigo によって運営されるドメイン	
googletwtw[.]com	Earth Wendigo によって運営されるドメイン	
bf[.]googletwtw[.]com	Earth Wendigo によって運	

	営されるドメイン	
ws[.]googletwtw[.]com	Earth Wendigo によって運営されるドメイン	
admin[.]googletwtw[.]com	Earth Wendigo によって運営されるドメイン	
anybodyopenfind[.]com	Earth Wendigo によって運営されるドメイン	
support[.]anybodyopenfind[.]com	Earth Wendigo によって運営されるドメイン	
supports[.]anybodyopenfind[.]com	Earth Wendigo によって運営されるドメイン	

supportss[.]anybodyopenfind[.]com	Earth Wendigo によって運営されるドメイン	
a61e84ac9b9d3009415c7982887dd7834ba2e7c8ea9098f33280d82b9a81f923	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
66cf12bb9b013c30f9db6484caa5d5d0a94683887cded2758886aae1cb5c1c65	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
4cdaca6b01f52092a1dd30fc68ee8f6d679ea6f7a21974e4a3eb8d14be6f5d74	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
f50a589f3b3ebcc326bab55d1ef271dcec372c25d65f381a409ea85929a34b49	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A

e047aa878f9e7a55a80cc1b70d0ac9840251691e91ab6454562afbff427b0879	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
a1a6dc2a6c795fc315085d00aa7fdabd1f043b28c68d4f98d4152fe539f026f1	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
10d2158828b953ff1140376ceb79182486525fd14b98f743dafa317110c1b289	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
0e04a03afa5b66014457136fb4d437d51da9067dc88452f9ebd098d10c97c5b8	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
75f3f724a2bfda1e74e0de36ff6a12d3f2ea599a594845d7e6bc7c76429e0fa4	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A

c3bc364409bb0c4453f6d80351477ff8a13a1acdc5735a9dff4ea4b3f5ad201c	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
5251087bb2a0c87ac60c13f2edb7c39fb1ea26984fcc07e4cf8b39db31ce2b08	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
7fa9a58163dd233065a86f9ed6857ed698fc6e454e6b428ea93f4f711279fb61	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
f568f823959be80a707e05791718c1c3c377da1b0db1865821c1cf7bc53b6084	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
a54d58d5a5812abaede3e2012ae757d378fb51c7d3974eaa3a3f34511161c1db	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A

77c3d62cce21c2c348f825948042f7d36999e3be80db32ac98950e88db4140b1	Earth Wendigo による XSS 攻撃のスクリプト	Trojan.JS.WENDIGOE.A
c0dabb52c73173ea0b597ae4ad90d67c23c85110b06aa3c9e110a852ebe04420	Earth Wendigo による Service Worker スクリプト	Trojan.JS.WENDIGOE.A
efe541889f3da7672398d7ad00b8243e94d13cc3254ed59cd547ad172c1aa4be	Earth Wendigo による WebSocket JavaScript バックドア	Backdoor.JS.WENDIGOE.A
2411b7b9ada83f6586278e0ad36b42a98513c9047a272a5dcb4a2754ba8e6f1d	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.A
1de54855b15fc55b4a865723224119029e51b381a11fda5d05159c74f50cb7de	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.A

d935c9fe8e229f1dabcc0ceb02a9ce7130ae313dd18de0b1aca69741321a7d1b	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.B
50f23b6f4dff77ce4101242ebc3f12ea40156a409a7417ecf6564af344747b76	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.C
fab0c4e0992afe35c5e99bf9286db94313ffedc77d138e96af940423b2ca1cf2	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.C
4d9c63127befad0b65078ccd821a9cd6c1dccec3e204a253751e7213a2d39e39	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.C
25258044c838c6fc14a447573a4a94662170a7b83f08a8d76f96fbbec3ab08e2	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.C
13952e13d310fb5102fd4a90e4eafe6291bc97e09eba50fedbc2f8900c80165f	Earth Wendigo によるシェルコードローダ	Trojan.Win32.WENDIGOE.C
ccb7be5a5a73104106c669d7c58b13a55eb9db3b3b5a6d3097ac8b68f2555d39	Earth Wendigo	Trojan.Win64.WENDIGOE.A

	によるシェルコードローダ	
40a251184bb680edadfa9778a37135227e4191163882ccf170835e0658b1e0ed	Earth Wendigo によるシェルコードローダ	Trojan.Win64.WENDIGOE.B
0d6c3cc46be2c2c951c24c695558be1e2338635176fa34e8b36b3e751ccdb0de	Cobalt Strike	Trojan.Win32.COBALT.SM

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