侵入の痕跡（Indicators of Compromise, IoC）

SHA256	ファイル名	検出名
a99f8ef649a65ecaf2c1298f03598b4fb3f1b17939cbe58b0117d566059731b4	ExchDefender.exe	Trojan.Win32.UNDEFENDEX.YEBDV
16ae11e3ff6cd8daaa20dc3de03b05d49655278518d95c89750731539e606b0e	ChackPassAS.aspx	Trojan.ASP.CHOPPER.YPBDV
806577311a873579a07445d0d7cdb7b2847dccdb306680563659d9fca7382708	YPEvQuXw.aspx	Trojan.ASP.CVE202126855.SM
d6ec34cdc7aa8c6199e3c017798b1c0fcb9c686a3e1d2c2d90683e1d63a6ae46	App_Web_kjvc3xzm.dll	Backdoor.MSIL.CHOPPER.YABCP
fcd3639277fa46bfcb7678d849bad50954caff4823b38b144a7e7b2ceb1e4b5d	sqhost.exe	Backdoor.Win64.PROMETEI.YEBDW
f0a5b257f16c4ccff520365ebc143f09ccf233e642bf540b5b90a2bbdb43d5b4	zsvc.exe	Backdoor.Win64.PROMETEI.YEBCS
e4bd40643f64ac5e8d4093bddee0e26fcc74d2c15ba98b505098d13da22015f5	rdpclip.exe	TrojanSpy.Win32.PROMETEI.YEBDV
d811b21ac8ab643c1a1a213e52c548e6cb0bea51ca426b75a1f5739faff16cbd	m6.exe	Coinminer.Win64.TOOLXMR.SMA
6be5847c5b80be8858e1ff0ece401851886428b1f22444212250133d49b5ee30	WindowsUpdate.exe	Trojan.Win32.COBALT.AX

81a6de094b78f7d2c21eb91cd0b04f2bed53c980d8999bf889b9a268e9ee364c	conhost.exe	Coinminer_CryptoNight.SM-WIN64
fb8f100e646dec8f19cb439d4020b5f5f43afdc2414279296e13469f13a018ca	miwalk.exe	HackTool.Win64.MIMIKATZ.ENS
b9dbdf11da3630f464b8daace88e11c374a642e5082850e9f10a1b09d69ff04f	jfkzhluonvbxicy.exe	Ransom.Win64.BLACKKINGDOM.SMYXBCX
c3c786616d69c1268b6bb328e665ce1a5ecb79f6d2add819b14986f6d94031a1	mail.jsp	Trojan.PS1.LEMONDUCK.YPBD2
4ea66b41ac0e72976b42af9f0f7961f73c8eff3a1d9a3fd7e0dc7032bf4a488e	a.jsp	Trojan.PS1.LEMONDUCK.YXBCU
2eb24fb51aad7e6d556eac8276f71321a32c866225a2883e7cd4a5f22f25669b	if_mail.bin	Trojan.PS1.LEMONDUCK.YXBCU
b660aa7aca644ba880fdee75f0f98b2db3b9b55978cc47a26b3f42e7d0869fff	m6.bin	Trojan.PS1.LEMONDUCK.YXAH-A
bc3835feff6f2b3b6a8da238b87b42dad05230d2fc40aefa1749477d6e232b78	m6g.bin	Trojan.PS1.LEMONDUCK.YXBCT
42012af7555dd2f3413161474bed658cf25b730a5354255e53cfa6cc2e0f646e	kr.bin	Trojan.PS1.LEMONDUCK.YXAJH
317799c3e17b493625c600bac3e42d5f1f4c175915468400779679f0cf538bbc	if.bin	Worm.PS1.LEMONDUCK.YXBC-A

関連 URL

- **hxxp://p1[.]feefreepool[.]net/cgi-bin/prometei[.]cgi?r=8&i=LAP057RQRL1WU541**
- **hxxp://173[.]249[.]19[.]202:1337/xmr64[.]exe**
- **hxxp://t[.]netcatkit[.]com/mail[.]jsp?mail**

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

©2021 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.