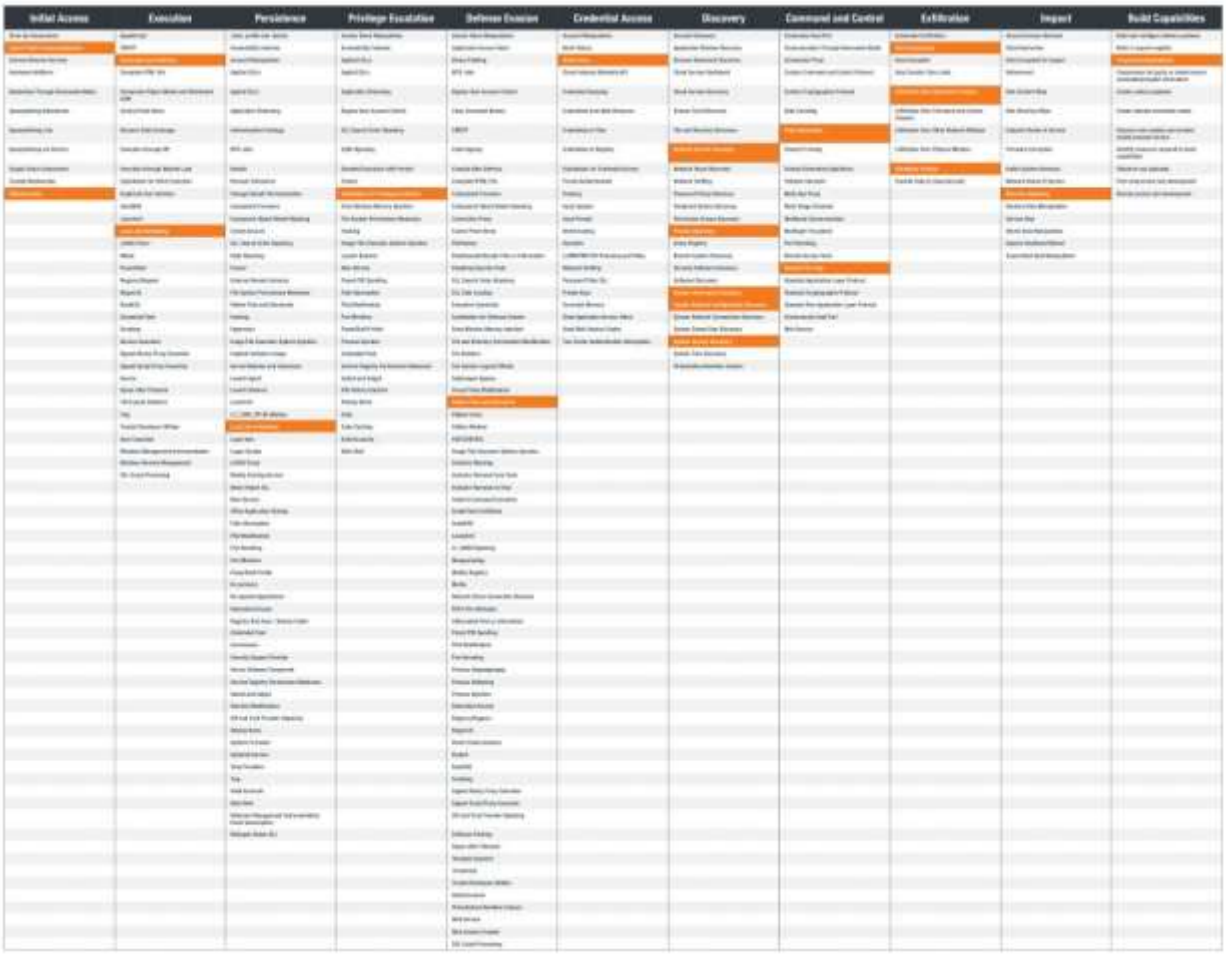
侵入の痕跡（Indicators of Compromises、IoCs）

SHA256	説明	検出名
1800de5f0fb7c5ef3c0d9787260ed61bc324d861bc92d9673d4737d1421972aa	コインマイナー	Trojan.SH.MALXMR.UWEJP
b68bd3a54622792200b931ee5eebf860acf8b24f4b338b5080193573a81c747d	Shellbot	Backdoor.SH.SHELLBOT.AA
620635aa9685249c87ead1bb0ad25b096714a0073cfd38a615c5eb63c3761976	ツール	Trojan.Linux.SSHBRUTE.B
fc57bd66c27066104cd6f8962cd463a5dfc05fa59b76b6958cddd3542dfe6a9a	コインマイナー	Coinminer.Linux.MALXMR.SMDSL32
649280bd4c5168009c1cff30e5e1628bcf300122b49d339e3ea3f3b6ff8f9a79	コインマイナー	Coinminer.Linux.MALXMR.SMDSL64

関連する URL

- 159[.]203[.]141[.]208
- 104[.]236[.]192[.]6
- 45[.]9[.]148[.]129:80　　Miner pool
- 45[.]9[.]148[.]125:80　　Miner pool
- http://www[.]minpop[.]com/sk12pack/idents.php　　Command and control
- http://www[.]minpop[.]com/sk12pack/names.php　　Command and control

MITRE ATT&CK Matrix™


Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Command and Control
Exfiltration
Impact
Build Capabilities

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

©2019 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.