侵入の痕跡（Indicators of Compromise, IoC）

スクリプト名	Sha256	検出名
supermicro_cr	d0d3743384e400568587d1bd4b768f7555cc13ad163f5b0c3ed66fdc2d29b810	Ransom.SH.DARKRADIATION.A
supermicro_bt	652ee7b470c393c1de1dfdcd8cb834ff0dd23c93646739f1f475f71a6c138edd	Trojan.SH.DARKRADIATION.A
supermicro_cr_third (obfuscated)	9f99cf2bdf2e5dbd2ccc3c09ddcc2b4cba11a860b7e74c17a1cdea6910737b11	Ransom.SH.DARKRADIATION.A
supermicro_cr_third (deobfuscated)	654d19620d48ff1f00a4d91566e705912d515c17d7615d0625f6b4ace80f8e3a	Ransom.SH.DARKRADIATION.D
test.sh	79aee7a4459d49dc6dfebf1a45d32ccc3769a1e5c1f231777ced3769607ba9c1	Trojan.SH.DARKRADIATION.A
downloader.sh.save	da68dc9d5571ef4729adda86f5a21d3f4478ddbae2de937f34f57f450d8a3c76	Trojan.SH.DARKRADIATION.A
downloader.sh	3bab2947305c00df66cb4d6aaef006f10aca348c17aa2fd28e53363a08b7ec68	Trojan.SH.DARKRADIATION.A
crypt3.sh	0243ac9f6148098de0b5f215c6e9802663284432492d29f7443a5dc36cb9aab5	Trojan.SH.DARKRADIATION.A
crypt2_first.sh	e380c4b48cec730db1e32cc6a5bea752549bf0b1fb5e7d4a20776ef4f39a8842	Ransom.SH.DARKRADIATION.A
bt_install.sh	fdd8c27495fbaa855603df4f774fe86bbc21743f59fd039f734feb07704805bd	Trojan.SH.DARKRADIATION.A
binaryinject1.so	7a15e51e5dc6a9bfe0104f731e7def854abca5154317198dad73f32e1aead740	Trojan.Linux.PROCHIDER.AA
exploit4.py	c869261902a1364dd3decb2f8dce54b81621f20abd7204a427a3365c8dcc9d78	Trojan.SH.EXPLOADER.AA
exploit3.py	503276929ce5c56c626eaa5c3aca0e0160743bf3c8d415042dc3f9bb8c8b44a2	Trojan.SH.EXPLOADER.AA
exploit1.py	847d0057ade1d6ca0fedc5f48e76dd076fa4611deb77c490899f49701e87b6dd	Trojan.SH.EXPLOADER.AA
pwd.c	14584a716c5378405cba188dd60cec03571965329f52cfbd8c54116fa2d59377	Invalid

C&C サーバ IOCs

- **Malware command and control server: 185[.]141[.]25[.]168**
- **Hack tools directory: hxxps[://]u2wgg22a111ssy[.]space**
- **Hack tools directory: hxxps[://]www[.]0zr33n33fo[.]space**
- **Hack tools directory: hxxp[://]vk-o2vox-n[.]pp[.]ua**
- **Hack tools directory: hxxps[://]m0troppm[.]site**
- **Hack tools directory: hxxps[://]apooow4[.]space**
- **Hack tools directory: hxxps[://]ga345ss34u[.]space**

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