侵入の痕跡（Indicators of Compromises、IoCs）

関連する SHA256 値と検出名は以下の通りです。

SHA256 値	検出名
3f28cace99d826b3fa6ed3030ff14ba77295d47a4b6785a190b7d8bc0f337e41	Trojan.PS1.MIMIKATZ.ADW
7c402add8feffadc6f07881d201cb21bc4b39df98709917949533f6febd53b6e	Trojan.PS1.LUDICROUZ.A
aaef385a090d83639fb924c679b2ff22e90ae9377774674d537670a975513397	TrojanSpy.Win32.BEAHNY.THCACAI
e28b7c8b4fc37b0ef91f32bd856dd71599acd2f2071fcba4984cc331827c0e13	Trojan.PS1.PCASTLE.B
fa0978b3d14458524bb235d6095358a27af9f2e9281be7cd0eb1a4d2123a8330	HackTool.Win32.Impacket.AI

関連する URL は以下の通りです。

- hxxp://down[.]beahh[.]com/c32.dat
- hxxp://down[.]beahh[.]com/new.dat?allv5
- hxxp://ii[.]ackng[.]com/t.php?ID={Computer Name}&GUID={GUID}&MAC={MAC ADDRESS}&OS={OS Version&BIT={32/64}&CARD={VIDEO CARD INFORMATION}&_T={TIME}
- hxxp://log[.]beahh[.]com/logging.php?ver=5p?src=wm&target
- hxxp://oo[.]beahh[.]com/t.php?ID={Computer Name}&GUID={GUID}&MAC={MAC ADDRESS}&OS={OS Version&BIT={32/64}&CARD={VIDEO CARD INFORMATION}&_T={TIME}
- hxxp://p[.]beahh[.]com/upgrade.php
- hxxp://pp[.]abbny[.]com/t.php?ID={Computer Name}&GUID={GUID}&MAC={MAC ADDRESS}&OS={OS Version&BIT={32/64}&CARD={VIDEO CARD INFORMATION}&_T={TIME}
- hxxp://v[.]beahh[.]com/wm?hp
- hxxp://v[.]y6h[.]net/g?h
- hxxp://v[.]y6h[.]net/g?l
- lplp1[.]abbny[.]com:443
- lplp1[.]ackng[.]com:443
- lplp1[.]beahh[.]com:443

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