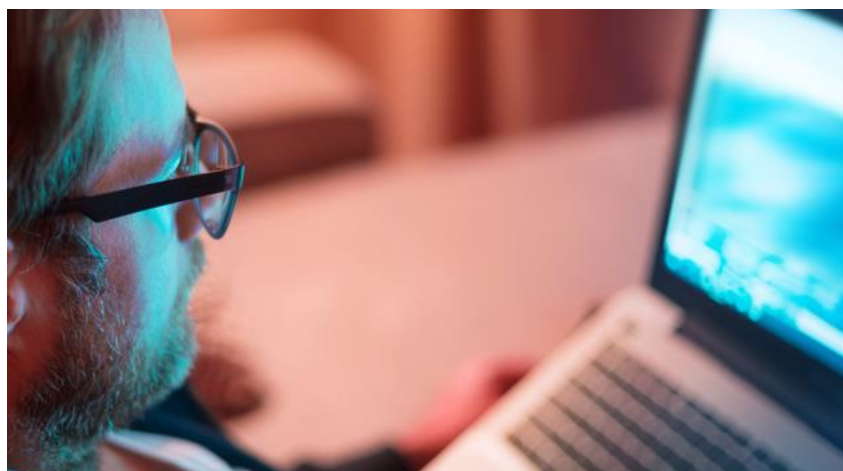


Povlsomware Ransomware Features Cobalt Strike Compatibility



What makes Povlsomware notable is not what it has already accomplished — there have been few, if any, notable incidents involving the malware at the time of writing — but how it can potentially be used. Although ostensibly advertised as an “educational” tool, its access to Cobalt Strike capabilities and its open-source nature make it a potentially dangerous malware in the hands of an experienced ransomware operator.

Ransomware attacks can come in many forms. At the simplest end of the spectrum, you have infection vectors such as phishing emails that will deploy the malware if the user accesses them. More complicated campaigns, on the other hand, might make use of complex infrastructure involving the use of tools such as Cobalt Strike or Mimikatz as part of the infection routine.

- Given the wide array of tools and techniques that ransomware operators use, organizations and individual users have to be vigilant on all fronts to protect their machines and systems from ransomware attacks. The following security best practices can help with this:
- Limiting access to shared network drives and turning off file sharing lessens the probability that a ransomware infection spreads to other devices.
- Employing authentication options that include multi-factor authentication strengthens the security of user accounts, minimizing opportunities for account theft or compromise.
- Enforcing the principle of least privilege — where users only have access to the sections of the system that they need— can help prevent attackers from running tools and software used by ransomware.
- Using application controls can help prevent attacks that leverage remote access software.
- Regular patching and updating of software and systems reduce the chance for an attacker to exploit a vulnerability that is part of the infection routine.
- Regularly backing up files, preferably [using the 3-2-1 rule](#), still remains an effective method of protecting data in the event of a successful ransomware infection.

Organizations can also take advantage of security technologies such as [Trend Micro XDR™](#), which collects and correlates data across endpoints, emails, cloud workloads, and networks to provide better context to attacks in a single console. This allows security and IT teams to respond to ransomware and other threats faster and more effectively.

SHA-256	Detection	TrendX
e05c74663775baf3ee37430d4662f7a9c89d63a752af5448c273e6b70fd9ec74	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
9effa31cbcf5e90fc0955b363871a4ef54ffd7634a0095673004b39e9036ef94	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
2aca9d08bacd2df13dd0475cc624fddec3fcc13495cbc7fc4f715764cb3c7ebe	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
c740cbdd79c5ef5fe2b9388cd57dcd76ab491cdb94bcacd525b599b12d25f88c	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
e08456212a2d597ba26456df8cbf48890a4350d9a8aba436c65afecf171ad468	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
6a61bdcdaf9b8b9dd0a5328680acee9db9d0b64166cbf1cf73046a8e0c4efec8	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE

f27b13e25bc39c222847c150488b5c404042fd526023d6ac8866e306e4975349	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
6c7485988ca145b02f564b8aae89133acf1ec6fe0db44be26cd3c8e87a6d1c6a	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
d8cb6bc96ed3c980013addb9af4f61fdfe5e3373c36e821062c2dae565dd75	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
37ca7a3b52d6cb9d9ebb9319c5f28f7b1e0ebb338bf732ace170684eb193b10e	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
cb2ef26d028621b5b438e5386daf1f06fc986d88d31c99b9833b4b906e6f0f33	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
de17f48967192dbd33ac67d752c7c4de441204d1da58b9801a90775e0265a66a	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
260950708c993ed1585a98952493bbaca92a8162439887b510ca832713898b75	Ransom.MSIL.POVLSOM.THBAOBA	N/A
3e6783288c3387437b25eb9f990cc9329acffb073baf7bb954e087c3733cfb2e	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
124e33009fc91c9964f5c44e4dc42ef7ae787bbb375305b95cbd7ee8014f080c	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
9a355fc10fe9e7906c34d8850a2efc5c93a3a1274ce3b122f5d6944b2d33f837	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE
2a6a5f6842b7f40c905ec44c43b4a9a999dadbc06f7d320ea4e96cc96e899f	Ransom.MSIL.POVLSOM.THBAOBA	N/A
78c2f745aa5ae027dad5fe67ec892cf6b05fd418f72031fb5d744b63bdf11200	Ransom.MSIL.POVLSOM.THBAOBA	Troj.Win32.TRX.XXPE