

Rewterz Threat Alert - Common Raven - IOCs - Rewterz

Published: 2020-11-19 · Archived: 2026-04-05 14:31:10 UTC

Severity

High

Analysis Summary

Threat actor Common Raven have been active and methods used to perform reconnaissance activities related to financial messages are influenced by the messaging solution. This is done via SQL statements, observing files on disk, browsing the messaging interface's GUI or even as complex as hooking into legitimate software to intercept function calls. Common Raven methodology to harvest information from the client that uses AutoClient. Threat actor deploys malware to the point where it copies data from the emission and reception folders to a staging folder from where they can read or retrieve the messages.

Impact

- Information theft
- Exposure of sensitive data

Indicators of Compromise

Filename

- svschost[.]exe

MD5

- 6f5be0ae39a7acc5bce45e53a9a5a0cb
- 3e65c53da93202024480c0071104dd5f

SHA-256

- 57e6e8afb83fe29962ebd9a164d8bac6155d825897d08d94eb7cd5c71eb9d184
- 3da155bcee7727b04f3715a85e7beaa3ff55bbeed100457b2a6dcbbc3a6850fed

SHA1

- 65b7fff2d3917d0b7dc807a3430e7efc888e7240
- c9ee6ae1d15f7fb4c5e11956a7e8120d8ee8e85f

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.

Source: <https://www.rewterz.com/rewterz-news/rewterz-threat-alert-common-raven-iocs>