Threat Category: Malware ? Information Stealer

Threat Description: PennyWise Stealer is a malware targeting over 30 browsers and various cryptocurrency wallets. It is distributed through YouTube videos offering fake Bitcoin mining software. Once executed, it collects sensitive data including IP address, username, system information, and browser data, then exfiltrates it to an attacker-controlled server over TCP port 5001.

Indicators of Compromise (IoCs):

Protocol: TCP

Destination Port: 5001

Payload Content Indicators:

"*PennyWise v1."

"Worker: "

"IP: "

"Username: "

"PC: "

"System: "

"*Browsers: *"

Detection Mechanism:

The TCP connection must be established and flowing to the server.

Payload must contain the above strings.

Fast pattern matching should be used for efficient scanning.

Traffic direction: $HOME_NET ? $EXTERNAL_NET.

Reference:

Twitter disclosure: https://twitter.com/crep1x/status/1638596449226170370

Classification: Trojan-activity

Rule Metadata:

SID: 2044748

Revision: 2