THREAT ALERT: Inside the Redeemer 2.0 Ransomware

cybereason.com/blog/threat-alert-inside-the-redeemer-2.0-ransomware

The Cybereason Global Security Operations Center (SOC) Team issues Cybereason Threat Alerts to inform customers of emerging impacting threats. The Alerts summarize these threats and provide practical recommendations for protecting against them. In this article, the Cybereason Research team exposes Redeemer 2.0, an updated version of the original ransomware.

What's Happening?

The malware dubbed Redeemer 2.0 is an updated variant of the Redeemer ransomware. This version differs from its older variants as it:

- Infects machines running the Windows 11 Operating Systems (OS).
- Keeps the OS safe from unintended damage (outside of the file encryption).
- Changes the icons of encrypted files

In this article, Cybereason Security Research Team analyzed the new release of this ransomware and how to defend against it through the Cybereason Defense Platform.

Key Observations

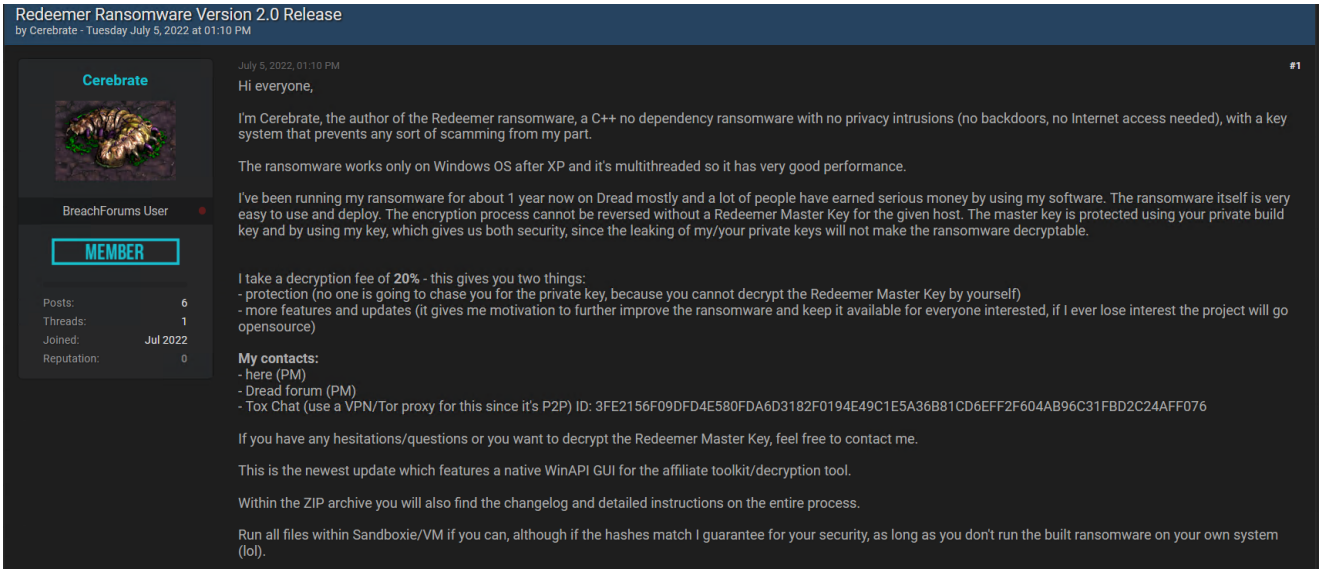
- In July 2022, a new version of Redeemer (v2.0) was released on an underground forum

- The new variant is advertised as “easy-to-use” and supports Windows 11
- The Cybereason Defense Platform includes Anti-Ransomware and Anti-Malware capabilities that detects and prevents the ransomware payload execution.

Analysis

Redeemer 2.0 Toolkit Release

A new and improved Redeemer 2.0 ransomware version was released on an underground forum. The author, calling himself “Cerebrate”, describes the new version as a “C++ no dependency ransomware with no privacy intrusions”, targeting the Windows OS:



Underground forum screenshot

Redeemer Toolkit and Build

The Redeemer 2.0 ransomware build can be generated using the toolkit as shown in this video:

Redeemer 2.0 Ransomware Builder

The build of the ransomware copies itself into the Windows directory with legitimate file names and executes itself as a new process, for example *sqlserver1.exe, svchost.exe*, etc.

The Cybereason Defense Platform Anti-Malware capability detects and prevents the ransomware execution:

MalOp Management screen as seen in the Cybereason Defense Platform

The new process executed by the Redeemer build was detected and prevented by Anti-Ransomware:

MalOp Management screen as seen in the Cybereason Defense Platform

Analysis with Cybereason Defense Platform

When Anti-Ransomware is set to "Detect" mode (which means that the ransomware is detected but not prevented on purpose), it is possible to analyze the Redeemer actions on the victim machine:

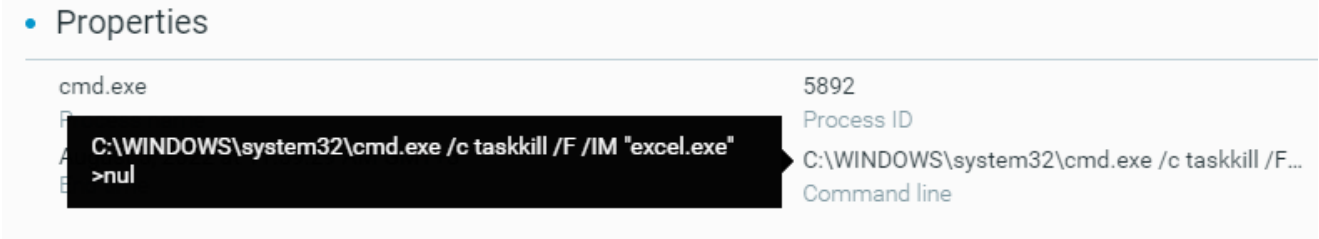
MalOp process as seen in the Cybereason Defense Platform

Redeemer ransomware 2.0 tries to:

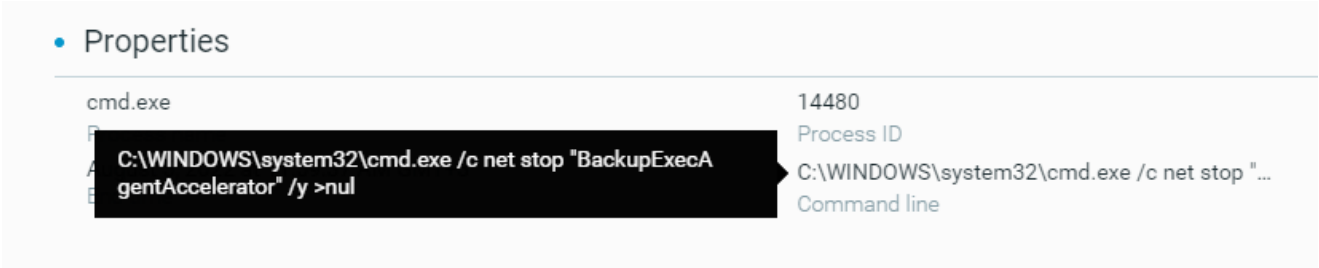
- Clear the Windows event logs

- Stop services
- Kill processes

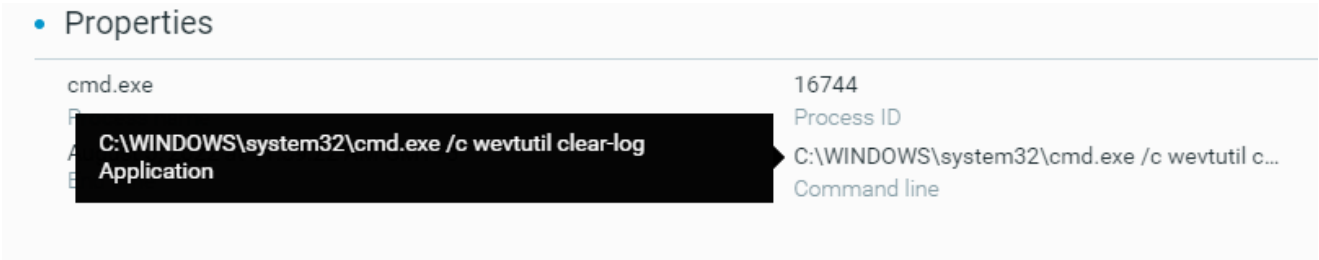
These actions can be observed from in the MalOp details for the process, as shown below:



Example of a command line to kill processes before encryption



Example of a command line to stop services before encryption



Example of a command line to clear the windows event log before encryption

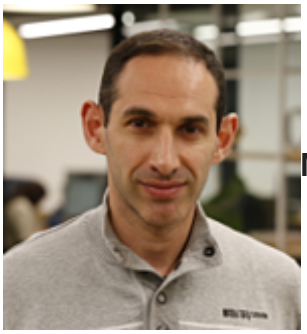
Example of a command line to delete shadow copies

Cybereason Recommendations

The Cybereason Defense Platform detects and prevents Redeemer 2.0 infections through the Anti-ransomware feature. Cybereason recommends the following:

- Enable Anti-Malware and set the Anti-Malware > Signatures mode to Prevent, Quarantine, or Disinfect
- Enable Anti-Ransomware, set Anti-Ransomware to Prevent mode and enable canary files (with default settings)
- Enable Application Control
- Keep systems fully patched: Make sure your systems are patched in order to mitigate vulnerabilities
- Regularly backup files and create a backup process and policy : Restoring your files from a backup is the fastest way to regain access to your data

About the Researcher



Mark Tsipershtein, Security Operations Analyst at Cybereason

Mark Tsipershtein, a cyber security analyst at the Cybereason Security Research Team, focuses on analysis automation and infrastructure. Mark has more than 20 years of experience in SQA, automation, and security testing.

About the Author

Cybereason Global SOC Team

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

All Posts by Cybereason Global SOC Team