RAZR Ransomware

Archived: 2026-04-05 18:27:33 UTC

RAZR is a recently identified ransomware variant that abuses web hosting service called PythonAnywhere for hosting the malicious binaries. The malware uses AES-256 algorithm for encryption and appends .raz extension to the filenames. The ransom note is dropped in form of a text file README.txt in which the attackers also threaten that the confidential files have not only been encrypted but also exfiltrated.

Symantec protects you from this threat, identified by the following:

Adaptive-based

- ACM.Untrst-Bcdedit!g1

Behavior-based

- SONAR.ProcHijack!g45
- SONAR.Ransomware!g34
- SONAR.SuspLaunch!g195
- SONAR.TCP!gen1

Carbon Black-based

- Associated malicious indicators are blocked and detected by existing policies within VMware Carbon Black products. The recommended policy at a minimum is to block all types of malwares from executing (Known, Suspect, and PUP) as well as delay execution for cloud scan to get maximum benefit from VMware Carbon Black Cloud reputation service.

File-based

- Downloader
- Ransom.Raz
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

Machine Learning-based

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

Network-based

- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 721
- Web Attack: Webpulse Bad Reputation Domain Request

Web-based

- Observed domains/IPs are covered under security categories in all WebPulse enabled products

---