Assignment 6.1: Ransomware Simulator

Joshua A. Wortz

University of San Diego

CSOL-560

Dr Varma

11/30/2025

Name of Ransomware	Brief Description & Capabilities	Order of Severity (Justification)	URL Reference
Archiver	**Control Scenario (False Positive):** Compresses files using standard GZip algorithms. This should *not* be blocked, as it simulates legitimate user archiving activity.	**Low / None** (Purpose is anomaly detection control)	https://support.knowbe4.com/hc/en-us/articles/229040167-RanSim-Product-Manual
BlackKingdomVariant	**Real-World Threat:** *Black Kingdom* Python-based ransomware that exploits critical infrastructure vulnerabilities like Microsoft Exchange ProxyLogon for initial access.	**High** (Exploits critical infrastructure; rapid lateral movement possible)	https://securelist.com/black-kingdom-ransomware/102873/
Collaborator	**Real-World Threat:** *Generic Multi-Process* Uses multiple distinct processes for enumeration, encryption, moving, and deletion to evade single-	**High** (Behavioral Evasion: Multi-threading complicates heuristic detection)	https://support.knowbe4.com/hc/en-us/articles/229040167-RanSim-Product-Manual

	process behavioral monitoring.		
CritroniVariant	**Real-World Threat:** *CTB-Locker (Critroni)* Simulates a variant that uses Elliptic Curve Cryptography (ECC) and communicates via the Tor network for C2 to mask traffic origin.	**High** (Strong encryption; C2 via Tor makes blocking difficult)	https://www.kaspersky.com/blog/new-version-ctb-locker/7310/
DearCryVariant	**Real-World Threat:** *DearCry* Exploits Microsoft Exchange vulnerabilities (ProxyLogon). Encrypts files by copying, then deleting originals, operating offline without active C2 contact.	**High** (Targets critical infrastructure; robust offline encryption)	https://www.cisa.gov/news-events/analysis-reports/ar21-102b
DjVuVariant	**Real-World Threat:** *STOP/DjVu*	**High** (Widespread	https://www.emsisoft.com/en/ransomware-decryption/stop-djvu/

	Widely distributed, often via software cracks. Encrypts files and deletes originals, causing permanent data loss.	consumer and small business impact; high prevalence)	
HollowInjector	**Real-World Threat:** *Process Hollowing (e.g., GandCrab)* Injects malicious code into a legitimate suspended process to hide encryption activity within the trusted application space.	**Extremely High** (Advanced Evasion: MITRE ATT&CK T1055.012 - Defense Evasion)	https://attack.mitre.org/techniques/T1055/012/
Injector	**Real-World Threat:** *DLL Injection (e.g., GandCrab)* Forces a legitimate running process to load a malicious DLL, executing encryption code within the context of a trusted process.	**Extremely High** (Advanced Evasion: MITRE ATT&CK T1055.001 - Defense Evasion)	https://attack.mitre.org/techniques/T1055/001/

InsideCryptor	**Real-World Threat:** *PClock* Encrypts files and overwrites the original file content in place, complicating recovery efforts compared to deletion.	**High** (Data destruction; utilizes a direct file-overwrite method)	https://www.emsisoft.com/en/blog/11686/new-ransomware-alert-cryptolocker-copycat-pclock-discovered/
LockyVariant	**Real-World Threat:** *Locky* Simulates the infection method used by Locky, known for being spread via macros in email attachments.	**Extremely High** (Historical precedent for rapid, massive global outbreak)	https://www.fortinet.com/blog/threat-research/a-closer-look-at-locky-ransomware-2
MazeVariant	**Real-World Threat:** *Maze* Pioneered "Double Extortion," stealing data prior to encryption. Uses sophisticated encryption and data	**Extremely High** (Data Exfiltration + Encryption; maximum integrity and confidentiality	https://www.cloudflare.com/learning/security/ransomware/maze-ransomware/

	exfiltration tactics.	impact)	
Mover	**Real-World Threat:** *Alpha* Encrypts files and then moves the files to a subfolder of the original folder to evade basic directory monitoring tools.	**High** (Evasion relies on moving files after encryption)	https://www.broadcom.com/support/security-center/protection-bulletin/alpha-ransomware
PaymerVariant	**Real-World Threat:** *DoppelPaymer* Enterprise-targeting RaaS that terminates security processes/services before encryption. Uses threaded file encryption for speed.	**Extremely High** (Targets critical infrastructure; focused on disabling defenses)	https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html
PhobosVariant	**Real-World Threat:** *Phobos* Ransomware-as-a-Service (RaaS)	**High** (Focuses on disabling recovery and	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

	often targeting RDP ports. Deletes shadow copies and attempts to disable Windows firewall.	persistence mechanisms)	
ReflectiveInjector	**Real-World Threat:** *Reflective DLL Injection (e.g., Chimera)* Loads a DLL from memory directly into a process without the DLL ever touching the disk, bypassing file-based AV scanning.	**Extremely High** (Fileless Malware technique; difficult to signature-detect)	https://attack.mitre.org/techniques/T1055/001/
Remover	**Control Scenario (False Positive):** Simple file deletion simulation. Mimics legitimate file cleanup activity.	**Low / None** (Purpose is false positive testing)	https://support.knowbe4.com/hc/en-us/articles/229040167-RanSim-Product-Manual
Replacer	**Real-World Threat:** *DirCrypt* Overwrites file content while keeping the original file extension (e.g.,	**High** (Deception mechanism targets user trust and automated simple	https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Dircrypt

	overwrites a PDF but keeps the .pdf extension).	scanners)	
RigSimulator	**Real-World Threat:** *XMRig (Crypto-mining)* Uses CPU resources to mine Monero. Degrades system performance and hardware life, but does not compromise data integrity or confidentiality.	**Moderate** (Impacts Availability, not core data integrity)	https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a
RIPlacer	**Real-World Threat:** *Thanos (RIPlace Technique)* Exploits a Windows design flaw (Rename/Replace) to bypass built-in security features like Controlled Folder Access.	**Extremely High** (Direct bypass of core OS security controls)	https://www.sentinelone.com/labs/thanos-ransomware-riplace-bootlocker-and-more-added-to-feature-set/
SlowCryptor	**Real-World Threat:** *FCrypt Variant /*	**High**	https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-

	Intermittent Encryption Encrypts files slowly or intermittently to stay below the threshold of behavioral alerts designed to catch rapid mass file modification.	(Behavioral Evasion focused on persistence and stealth)	encryption-to-evade-detection/
Streamer	**Real-World Threat:** *Bart* Encrypts multiple files and writes the data to a single encrypted file stream. Does not rely on C2 during the encryption phase.	**High** (Bypasses network blocks; fast, direct archive method)	https://www.malwarebytes.com/blog/news/2017/01/locky-bart-ransomware-and-backend-server-analysis
StrongCryptor	**Real-World Threat:** *CryptoLocker (Offline)* Standard strong encryption: Creates	**High** (Robust encryption and effective anti-recovery method)	https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections

	new encrypted file, overwrites original, and safely deletes the original (safe wipe).		
StrongCryptorFast	**Real-World Threat:** *CryptoLocker (Fast)* Optimized for speed: Creates new encrypted file and immediately deletes the original, minimizing the time window for detection.	**High** (Focus on speed increases damage potential)	https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections
StrongCryptorNet	**Real-World Threat:** *CryptoLocker (Network)* Simulates C2 communication (sending keys to 127.0.0.1) before encryption, signaling a network indicator of compromise (IoC) presence.	**High** (Tests network behavioral detection capabilities)	https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections

ThorVariant	**Real-World Threat:** *Thor* Sophisticated Locky variant that uses file obfuscation and unique naming conventions (e.g., the .thor extension).	**Extremely High** (Advanced obfuscation complicates signature detection)	https://www.tripwire.com/state-of-security/thor-variant-locky-virus
VirlockVariant	**Real-World Threat:** *Virlock* Polymorphic ransomware that acts as a virus (file infector). Uses a "watchdog" process to ensure persistence and self-renewal if terminated.	**Extremely High** (Polymorphic + Persistence mechanisms for maximal resilience)	https://news.sophos.com/en-us/2016/01/11/the-current-state-of-ransomware-virlock-threatfinder-crypvault-and-powershell-based/
WeakCryptor	**Real-World Threat:** *TeleCrypt* Uses weak/simple encryption which may allow for free decryption tools, but abuses the	**Moderate** (Damage is reversible, but C2 channel is unconventional)	https://www.malwarebytes.com/blog/news/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated

	Telegram API for C2.		

References

Broadcom. (2016). *Alpha Ransomware*. Symantec Enterprise. https://www.broadcom.com/support/security-center/protection-bulletin/alpha-ransomware

Cloudflare. (n.d.). *What is Maze Ransomware?* https://www.cloudflare.com/learning/security/ransomware/maze-ransomware/

Cybersecurity and Infrastructure Security Agency. (2013). *Alert TA13-309A: Cryptolocker Ransomware*. https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections

Cybersecurity and Infrastructure Security Agency. (2016). *Alert AA16-059A: Locky Ransomware*. https://www.cisa.gov/news-events/alerts/2016/02/17/locky-ransomware

Cybersecurity and Infrastructure Security Agency. (2021). *Analysis Report AR21-102B: DearCry Ransomware*. https://www.cisa.gov/news-events/analysis-reports/ar21-102b

Cybersecurity and Infrastructure Security Agency. (2022). *Advisory AA22-320A: XMRig Cryptomining Malware*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a

Cybersecurity and Infrastructure Security Agency. (2024). *Advisory AA24-060A: Phobos Ransomware*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

Elastic Security. (n.d.). *PClock Ransomware Overview*. https://www.elastic.co/security/center/ransomware/pclock

Emsisoft. (2015). *New ransomware alert: CryptoLocker copycat "PClock" discovered*. https://www.emsisoft.com/en/blog/11686/new-ransomware-alert-cryptolocker-copycat-pclock-discovered/

Emsisoft. (n.d.). *STOP/DjVu Ransomware Decryption Information*. https://www.emsisoft.com/en/ransomware-decryption/stop-djvu/

Fortinet. (2016). *A Closer Look at Locky Ransomware*. Fortinet Blog. https://www.fortinet.com/blog/threat-research/a-closer-look-at-locky-ransomware-2

Kaspersky. (2015). *New version of CTB-Locker*. Kaspersky Daily. https://www.kaspersky.com/blog/new-version-ctb-locker/7310/

KnowBe4. (n.d.). *RanSim Product Manual*. https://support.knowbe4.com/hc/en-us/articles/229040167-RanSim-Product-Manual

Malwarebytes. (2016). *TeleCrypt: The ransomware abusing Telegram API defeated*. Malwarebytes Labs. https://www.malwarebytes.com/blog/news/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated

Malwarebytes. (2017). *Locky "Bart" ransomware and backend server analysis*. Malwarebytes Labs. https://www.malwarebytes.com/blog/news/2017/01/locky-bart-ransomware-and-backend-server-analysis

Microsoft. (n.d.). *Win32/Dircrypt Malware Encyclopedia*. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Dircrypt

MITRE ATT&CK. (n.d.-a). *Technique T1055.001: Process Injection: Dynamic-link Library Injection*. https://attack.mitre.org/techniques/T1055/001/

MITRE ATT&CK. (n.d.-b). *Technique T1055.012: Process Injection: Process Hollowing*. https://attack.mitre.org/techniques/T1055/012/

Securelist. (2021). *Black Kingdom ransomware: what you need to know*. Kaspersky. https://securelist.com/black-kingdom-ransomware/102873/

SentinelOne. (2020). *Thanos Ransomware: RIPlace Bootlocker and More Added to Feature Set*. https://www.sentinelone.com/labs/thanos-ransomware-riplace-bootlocker-and-more-added-to-feature-set/

SentinelOne. (2023). *Ransomware Developers Turn to Intermittent Encryption to Evade Detection*. https://www.sentinelone.com/labs/ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

Sophos. (2016). *The current state of ransomware: VirLock, ThreatFinder, CrypVault, and PowerShell-based*. Sophos News. https://news.sophos.com/en-us/2016/01/11/the-current-state-of-ransomware-virlock-threatfinder-crypvault-and-powershell-based/

Trend Micro. (2021). *An Overview of the DoppelPaymer Ransomware*. https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

Tripwire. (2016). *Thor Variant of Locky Virus: What You Need to Know*. The State of Security. https://www.tripwire.com/state-of-security/thor-variant-locky-virus