(TLP:CLEAR)

Encryption-less Ransomware

DISTRICT OF COLUMBIA FUSION CENTER
INTELLIGENCE ASSESSMENT

2024-07-017
14 August 2024

(TLP:CLEAR) Ransomware attacks that do not encrypt victim systems or data as part of the attack represent a notable change in cyber threat actor tactics. This approach provides threat actors with the ability to:

- Launch high-impact campaigns with less effort and fewer tools,
- Increase efficiency of their operations, and
- Make their attacks harder for victims to counter.

(TLP:CLEAR) For public safety officials and Chief Information Security Officers (CISOs), this shift presents new challenges, including:

- Faster attack execution,
- Potentially quicker data exfiltration, and
- Need for enhanced data protection and access monitoring.

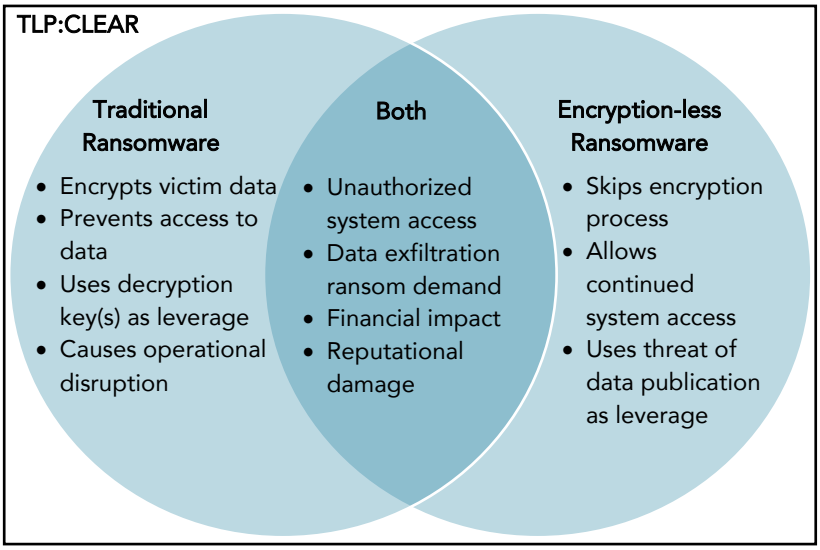
(TLP:CLEAR) What is encryption-less ransomware?

(TLP:CLEAR) Also known as "extortion-only ransomware," encryption-less ransomware represents a significant shift in cyber threat tactics. Similar to traditional ransomware, encryption-less ransomware operates by gaining unauthorized access to a company's systems. Exfiltrating sensitive data and threatening to publish that data unless a ransom is paid.

(TLP:CLEAR) The key difference is that encryption-less ransomware skips the encryption process, allowing victims to maintain access to their systems and continue business operations.[i]

(TLP:CLEAR) Encryption-less ransomware tactics may be preferred over encryption-based tactics for faster extortion schemes. The DC Fusion Center assess that cyber threat actors likely will increase their use of encryption-less ransomware tactics over the coming years, as encryption-less ransomware strategies provide adversaries with high-impact ransomware campaigns that achieve greater financial impact while simultaneously using fewer resources.

- (TLP:CLEAR) Cyber threat actors shifted from a double-extortion model, in which they encrypted victims' systems after exfiltrating the data, to encryption-less ransomware in January 2023. A May 2023 CISA advisory detailed an identified ransomware group's shift to encryption-less ransomware as a primary ransom tactic.[ii]



(TLP:CLEAR) Venn diagram depicting differences and similarities between Traditional and Encryption-less Ransomware

(TLP:CLEAR) Cyber threat actors likely will target critical infrastructure within the United States using encryption-less ransomware tactics. Cyber threat actors with profit motives benefit from compromising critical infrastructure systems and tend to reuse successful tactics. Therefore, we assess that cyber threat actors will continue to target critical infrastructure.

- (TLP:CLEAR) According to cybersecurity researchers, cyber threat actors shifted their focus to targets that possess sensitive data and have the financial capability to meet substantial ransom demands, which proved successful against government, healthcare, manufacturing, professional and legal services, education, and ecommerce organizations in North America and Europe.[iii,iv]

(TLP:CLEAR) Perspective

(TLP:CLEAR) For the District, this observed shift to encryption-less ransomware may reflect an increased risk to the following critical infrastructure sectors and subsectors:

- Communications,
- Education Facilities,
- Energy,
- Government Services,
- Healthcare and Public Health, and
- Water and Wastewater.

(TLP:CLEAR) The threat from cyber threat actors using encryption-less ransomware is not exclusive to the above sectors and subsectors; partners, regardless of critical infrastructure sector, are encouraged to employ cybersecurity best practices to mitigate vulnerabilities and reduce their overall risk of ransomware attacks.

(TLP:CLEAR) Alternative Analysis

(TLP:CLEAR) Although we assess it to be unlikely, cyber threat groups' shifts to encryption-less ransomware could be driven by efforts to advance new malware and to employ more advanced encryption, requiring a reallocation of existing resources away from active ransomware campaigns. This is unlikely, because cyber threat groups traditionally modify existing tools, as opposed to creating new, sophisticated tools. Incident reporting on new malware with upgraded encryption would prompt us to reassess this alternative.

(U) Sources

---

[i] (TLP:CLEAR) SharedSecure | Encryption-less-Ransomware | https://shardsecure.com/blog/encryption-less-ransomware | Accessed June 6, 2024 | Source Classification: Unclassified.

[ii] (TLP:CLEAR) CISA | #StopRansomware: BianLian Ransomware Group | https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a | Accessed June 7, 2024 | Source Classification: Unclassified.

[iii] (TLP:CLEAR) Cyberint | BianLian Ransomware: Victimology and TTPs | https://cyberint.com/blog/research/bianlian-ransomware-victimology-and-ttps/ | Accessed June 7, 2024 | Source Classification: Unclassified.

[iv] (TLP:CLEAR) PaloAlto | Threat Assessment: BianLian | Published January 23, 2024 | https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/ | Accessed June 7, 2024 | Source Classification: Unclassified.

Collection, Reporting, Dissemination, and Feedback Information

Collection Requirements

(U) This product addresses the following District of Columbia Fusion Center (DCFC) Standing Information Needs (SINs) and Homeland Security (HSEC) SINs:

- (U) DCFC SIN(s): 1.5, 1.6, 1.7
- (U) HSEC SIN(s): 1.8

Reporting Suspicious Activity

(U) The DC Fusion Center encourages its partners to report any urgent or imminent threats to life or property to local law enforcement by calling 911.

(U) Suspicious activity can be submitted to the DC Fusion Center via the iWATCH website at iWATCHDC.org or via telephone to (202) 727-9099.

Intended Audience

(U) Federal, state, local, tribal, and territorial homeland security personnel, law enforcement, first responders, and private sector partners.

Dissemination and Privacy Notice

(U) Distribution: This document is TLP:CLEAR. Recipients may use TLP:CLEAR information without restriction; however, this information remains subject to standard copyright rules.

(U) Electronic Privacy Notice: This document contains information that is, or may be, covered by electronic communications privacy laws, including but not limited to the Electronic Communications Privacy Act of 1986 (ECPA 18 U.S.C. §§ 2510-2523) and the Privacy Act of 1974 (5 U.S.C. § 552a). It is intended for the exclusive use of the addressee(s) and may contain confidential or privileged information. If you are not the intended recipient, please notify the sender immediately and destroy all copies of this message and any attachments.

Expressions of Likelihood

(U) Phrases such as "the DC Fusion Center judges" and "we assess," and terms such as "likely" and "probably," convey analytical judgments and assessments. The chart below approximates how expressions of likelihood and probability correlate with percentages of chance.

Terms of Likelihood	Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain(ly)
Terms of Probability	Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
Percentages of Chance	1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

(U) DC Fusion Center reporting relies on terms of likelihood; however, this chart includes terms of probability and percentages of chance for comparison, as such terms may appear in other reporting.

Feedback

(U) Please take a few moments to complete a survey to help us evaluate the relevance, timeliness, and value of this product.

(U) Our product satisfaction survey is available via Microsoft Forms by scanning the QR code at right or by clicking on the following link: DC Fusion Center Product Satisfaction Survey (https://forms.office.com/g/BsvF6qYjkd).