Opinion writing

Cyber Crime and Digital Evidence

Submitted by

Name: Sidhant Kumar Chaurasiya

Student ID:10487

Cyber Security and digital forensics

Kathmandu, Nepal

the forensics investigation of the "Hunter XP" disk image reveals substantial evidence of criminal activities, including ransomware operation, extortion, data tempering, stalking, and conspiracy. These activities violate multiple UK laws designed to safeguard individuals and digital systems. Below is a detailed explanation of the offensive, evidence, and relevant legal framework:

1. **Ransomware and extortion**
    - **Evidence**: Recovered email communications explicitly discuss ransom demands and negotiations, involving large sums of money. The presence of encryption and data-wiping tools, such as BCWipe and BestCrypt, further corroborates the intent to extort victims through ransomware schemes
    - **Applicable Law**:
        - Theft Act 1968, Section 21 defines blackmail as making unwarranted demands with menaces, to cause loss or gain financially. The "menaces" can include threats of reputation, financial, and digital harm, not necessarily physical violence.
        - Relevance of the case: communication recovered from the disk shows deliberate coordination to demand payment under duress, fitting the legal definition of blackmail under this act.
2. **Data Tempering and concealment**:
    - **Evidence**: altered file extensions, deleted files, and tempered records were identified. Tools like BCWipe were used to erase incrimination data, indicating an effort to destroy evidence of illicit activities.
    - **Applicable Laws**:
        - Computer Misuse Act 1990, Section 3: this law criminalizes unauthorized acts that impair the operation of any computer or the data it holds. It covers the intentional destruction or modification of digital information.
        - Relevance of the case: By tempering with files and using wiping tools to delete data, the suspect engaged in activity aimed at obstructing justice and concealing criminal behavior. This fits the criteria of prosecuting under section 3 of the Act.
3. **Unauthorized data exfiltration**:
    - **Evidence**: Network and external device logs show an attempt to exfiltrate sensitive data. This includes evidence of USB drives being used and connection to unauthorized networks.
    - **Applicable Law:**
        - Data Protection Act 2018**:** This act incorporates the principles of of General Data Protection Regulation (GDPR) into UK law, ensuring strict control over the processing, storage, and transfer of personal data. Unauthorized access to personal data. Unauthorized access or exfiltration of such data constitutes a violation.
        - Relevance of the Case: Any attempt to extract personal or sensitive information from a system without authorization breaches the Data Protection Act. The logs recovered substantiate this offense.

4. **Stalking and surveillance**:
    - **Evidence:** Files recovered from the disk included materials related to stalking techniques and surveillance of the individuals. These indicate a deliberate intent to intimidate or track victims.
    - **Applicable Laws:**
        - Protection from Harassment Act 1997, Section 2: This section makes it an offense to engage in conduct that amounts to harassment, including stalking. Harassment is an action that causes alarm or distress, whether physical, digital, or physiological.
        - Relevance of the Case: the recovered files suggest predatory behavior, likely to intimidate victims, which constitutes a breach of this act.
5. **Conspiracy and collaboration**:
    - **Evidence**: Email threads show discussions between multiple parties to coordinate ransomware attacks and extortion plans. This evidence indicates premeditation and collaboration
    - **Applicable Law:**
        - Criminal Law Act 1977, section 1: this act defines conspiracy as an agreement between two or more parties to commit a criminal act. The crime need not be completed for prosecution, the agreement alone suffices.
        - Relevance to the Case: The email discussion clearly shows the planning and intent to commit ransomware and extortion, meeting the criteria for conspiracy under this law
6. **Conclusion and Recommendations**:
   The investigation provides irrefutable evidence of Bob Hunter's involvement in these activities. The comprehensive finding leaves no doubt about this culpability. It is strongly recommended that legal proceedings be initiated under the aforementioned laws, as the evidence meets the requirements for prosecution beyond a reasonable doubt.

References

CPS (2023) Blackmail: Legal Guidance. Available at: https://www.cps.gov.uk/legal-guidance/blackmail

Legislation.gov.uk (2023) Computer Misuse Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/18

ICO (2023) Guide to the UK General Data Protection Regulation (UK GDPR). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection

Legislation.gov.uk (2023) Protection from Harassment Act 1997. Available at: https://www.legislation.gov.uk/ukpga/1997/40

CPS (2023) Conspiracy: Legal Guidance. Available at: https://www.cps.gov.uk/legal-guidance/conspiracy