博士後期課程

博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目 ： Identification of Encrypted C2 Communication Used by Malware
申請者 ： 神田 敦
審査委員会 ： 主査　教授　大久保 隆夫
副査　教授　後藤 厚宏
副査　教授　有田 正剛
副査　教授　橋本 正樹

Ⅰ. 論文内容の要旨

本論文は、暗号化された C2 通信の識別に関する研究である。

第 1 章では、序論として本研究の概要を述べている。暗号化通信（HTTPS/TLS）がインターネットの標準となる一方で、マルウェアも TLS を用いて C2 通信を秘匿化しており、従来のペイロード解析型検知は有効性を失いつつある。本論文は、TLS ハンドシェイク情報を用いた識別の限界として「Parameter variation」と「Parameter spoofing」という二つの課題を定義し、それぞれに対する新たな識別技術を提案している。

第 2 章では、研究の背景について説明している。暗号化通信を利用する脅威の増加、TLS インスペクションの性能・プライバシ・互換性上の限界、そして自動検知を補完するアクティブディフェンス／スレットハンティングの重要性を整理し、復号に依らない識別技術の必要性を明確化する。

第 3 章では、論文理解の前提となる内容について説明している。TLS/SSL の歴史と TLS 1.3 の特徴を整理し、TLS 1.3 では ClientHello/ServerHello 以外が暗号化されるため、識別に使える情報が限定される点を説明する。加えて、暗号データのランダム性評価としてシャノンエントロピーおよび NIST SP800-22（Monobit Test、Runs Test 等）の基礎を解説している。

第 4 章では、先行研究について説明している。先行研究を、TLS フィンガープリンティングなどのシグネチャベース手法と、機械学習ベース手法に分類して整理する。加えて、JA3/JA4 等の既存手法は、微小なパラメータ差異や衝突、更新による変化に弱い点を指摘している。

第 5 章では、第 1 章で挙げた 2 つの課題のうち、「Parameter variation(パラメータ変動)」について説明している。変動は、約 11.5 年分の Malware Traffic Analysis データセットを用い、同一マルウェア内でも TLS パラメータが短期的に揺らぐ「Parameter Fluctuation」と、長期的に変化する「Parameter Drift」が実在することを実証する。これに対し、TLS 構造を CBOR で表現する Compacted Protocol Representation（CPR）と、構造差分を定量化する Structural Edit Distance（SED）を提案する。さらに、揺らぎやすいパラメータを除去してから一致判定する Exact Match after De-fluctuation（EM-D）戦略が、未知のフィンガープリントが多い環境で最も高い識別性能を示すことを実験で示している。

された。

第 6 章では、第 1 章で挙げた 2 つの課題のうち、「Parameter spoofing(パラメータ偽装)」について説明している。攻撃者が TLS を偽装する FakeTLS（ハンドシェイクを信用できない、あるいは存在しない通信）に対し、ハンドシェイクに依らず暗号化ペイロードの統計的ランダム性から検知する枠組みを提案している。ま

た、Monobit Test と Runs Test 由来の特徴量を用いた TLS Lie Detector により、特に弱い暗号（XOR 等）を用いた FakeTLS を高精度に検出できることを示している。

第 7 章では、2 つの課題に対する第 5 章、第 6 章の提案について総合的に考察している。パラメータ変動対策（構造的フィンガープリント）とパラメータ偽装対策（ペイロードの新規性検知）は補完関係にあり、SIEM/IDS やスレットハンティングでの多層的活用が有効であると議論する。一方で、長期運用時の性能維持や実運用データでの検証が課題として残る。

第 8 章では、結論と今後の課題について述べている。

Ⅱ. 論文審査結果の要旨

本論文は、暗号化 C2 通信識別における二大課題を体系化し、構造的手法とランダム性解析という新たな方向性を提示した。また、通信パラメータの変動が短期的変動と長期的変動に分かれることを発見し、その詳細を明らかにした。この成果は、企業、組織のセキュリティ対策担当者にとって、暗号化通信が主流となる将来のネットワーク防御において、復号に依らない、C2 通信の識別、特定のための実践的基盤となる可能性を示している。また、既存のフィンガープリントにとる通信識別手法はパラメータの変動に弱いことが指摘されており、本論文で提案する CPR/SED は、C2 通信に限らず、暗号化通信の特定を可能とし、社会に大きく貢献するものであると評価できる。

以上の理由から、本論文は、博士（情報学）の論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、2026 年 1 月 22 日に論文内容とこれに関連する事項について口述試問を行った。審査に当たっては、博士学位のディプロマ・ポリシーに基づいて総合的に評価し、申請者が学位取得にふさわしい知見を持つものと判断した。