SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

MITB 攻撃対象の傾向分析と脅威情報活用に関する考察
The trend analysis of MITB attack targets and consideration of utilizing the threat information.

高田 一樹 * 太刀川　剛 * 内田 隆徳 † 邦本 理夫 *
Kazuki Takada Tsuyoshi Tachikawa Takanori Uchida Michio Kunimoto

キーワード MITB 攻撃，金融系マルウェア，脅威情報

あらまし

インターネットバンキングなどの金融機関サービス利用者をターゲットとしたサイバー攻撃による不正送金が発生している [1]．不正送金を引き起こす攻撃方法の 1 つに金融系マルウェアを用いた MITB 攻撃が存在している．MITB 攻撃は，PC に感染したマルウェアが Web ブラウザにインジェクションすることで通信内容の盗聴や改ざんを行う．MITB 攻撃は，感染 PC 上の Web ブラウザがアクセスしている正規 Web サイトのコンテンツが改ざんされ攻撃に利用されるため Web サービス提供者による対策が難しい攻撃手法である．我々は，これまでに，MITB 攻撃を用いて不正送金などを行うマルウェア（以下，金融系マルウェア）の対策のために金融系マルウェアの長期観測手法を提案してきた [2]．この長期観測手法を用いることで，金融系マルウェアによる攻撃の動向を継続して明らかにすることを可能としている．

金融系マルウェアの長期観測では，主に金融系マルウェアが C&C サーバから取得する MITB 攻撃の指示をする攻撃設定情報の観測・分析を行う．本論文では，表 1 に示す金融系マルウェアの攻撃設定情報の分析結果から，2019 年から 2021 年における MITB 攻撃の動向について報告する．また，金融系マルウェアに攻撃対象とされた日本国内の金融機関やサービスの傾向についての分析結果もあわせて報告する．

我々は，収集した金融系マルウェア脅威情報を，総務省と一般社団法人 ICT-ISAC が連携して行っている実証事業で運営されている情報共有基盤へ投稿する実証を行っている [3]．本論文では，現在，情報共有基盤に対して投稿している脅威情報に加えて，攻撃対象の分析結果を加えることでより有効に活用する方法の検討結果を報告する．

表 1: 観測対象金融系マルウェア

マルウェア名	検体数	攻撃設定情報変更確認期間
Ramnit	1	2019.01 - 2019.12
Trickbot	5	2019.10 - 2020.09
Ursnif	7	2019.05 - 2021.09
Zloader	8	2020.04 - 2021.03

参考文献

[1] 令和 3 年上半期におけるサイバー空間をめぐる脅威の情勢等について． https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf. Accessed: 2021-11-24.

[2] 高田一樹, 岩本一樹, 遠藤基, 奥村吉生, 岡田晃市郎, 西田雅太, 吉岡克成, 松本勉. 静的解析と挙動観測を組み合わせた金融マルウェア長期観測手法の提案. 情報処理学会論文誌, Vol. 59, No. 12, dec 2018.

[3] 高田一樹, 邦本理夫, 山下知起, 寺田真敏, 吉岡克成. 金融系マルウェア脅威情報配信の実証と考察．コンピュータセキュリティシンポジウム 2021 論文集, oct 2021.

* 株式会社セキュアブレイン, 東京都千代田区紀尾井町 3-12 紀尾井町ビル 7 階, SecureBrain Corporation, Kioicho Bldg 7F, 3-12 Kioicho, Chiyoda-ku, Tokyo
† ジェノアテクノロジーズ株式会社, 東京都港区虎ノ門 4 丁目 3 番 1 号城山トラストタワー, JnoahTechnologies, Shiroyama Trust Tower, 4-3-1 Tranomon, Minato-ku, Tokyo