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

# 標的型マルウェアの通信先情報に基づく C&C サーバ監視による攻撃誘引
# Luring Cyber Attacks by Monitoring C&C Servers Based on Targeted Malware Destination Information

細見 勇介 * 津田 侑 † 鄭 俊俊 * 毛利 公一 *
Yusuke Hosomi Yu Tsuda Junjun Zheng Koichi Mouri

**キーワード** マルウェア，動的解析，C&C サーバ，死活監視

## あらまし

近年サイバー攻撃は高度化し，組織や企業を標的とした標的型攻撃が増加傾向にある．標的型攻撃は，C&C サーバと接続し遠隔操作などの攻撃活動を行うため，対策にはマルウェア感染後の挙動の解析が必要である．しかし，標的型攻撃の動的解析の時点では C&C サーバからの司令による攻撃活動を行わないことが多く，マルウェアと C&C サーバが接続した後の挙動を観測するのは困難である．攻撃活動を観測するためには攻撃者が攻撃意思を持ったタイミングで動的解析を実施する必要がある．そこで，C&C サーバの生死に着目し，死活監視を実施することで攻撃兆候の検出を行う．C&C サーバなどの不審接続先は，一度ダウンした後に復活したり，特定の期間のみ稼働したりする特徴を持つことが明らかになっており [1, 2]，攻撃を行う際に活性化することが推測される．本稿では，動的解析によるマルウェアが接続する通信先情報の収集と死活監視を行い，活性化した通信先に紐づく検体の再解析を試みた．図 1 に示すように，動的解析は STARDUST[3] を利用し，通信先情報の収集やマルウェア感染後の挙動の解析を行う．収集した通信先情報に基づいて C&C サーバの死活監視を実施し，サーバの活性化を検出した場合は再度動的解析を行う．その結果，C&C サーバの活性化が攻撃の兆候となることを確認し，実際に攻撃の誘引に成功した．

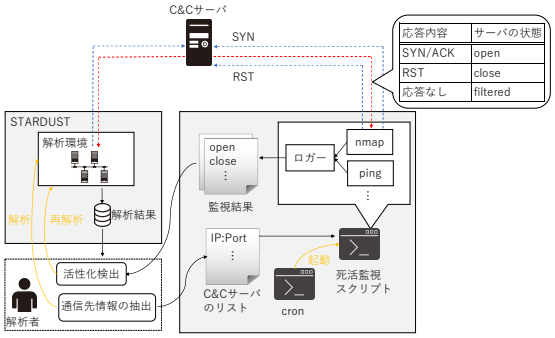


図 1: 実験の概要

## 参考文献

[1] Y. Tanaka and A. Goto, “Analysis of malware download sites by focusing on time series variation of malware”, 2016 IEEE Symposium on Computers and Communication(ISCC), pp. 173–179, 2016.

[2] ZDNet:カスペルスキー，日本を狙うサイバー攻撃を報告–米 国政府の対応にも見解，https://japan.zdnet.com/article/35111882/(2021 年 12 月 7 日閲覧).

[3] 津田侑，遠峰隆史, 金谷延幸，牧田大佑，丑丸逸人，神宮真人，高野祐輝，安田真悟，三浦良介，太田悟史，宮地利幸，神薗雅紀，衛藤将史，井上大介，中尾康二．サイバー攻撃誘引基盤 STARDUST．コンピュータセキュリティシンポジウム 2017(CSS2017) 論文集，pp. 472–479，2017.

* 立命館大学, 〒 525-8577 滋賀県草津市野路東 1-1-1, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577 Japan. mouri@asl.cs.ritsumei.ac.jp
† 情報通信研究機構, 〒 184-8795 東京都小金井市貫井北町 4-2-1, National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan.