4ZC-02

マルウェアのネットワーク通信の特徴調査及びSSLインスペクションの評価

諸　鷹大†　　吉浦　紀晃†
埼玉大学理工学研究科†

1.はじめに

近年ではリモートワークも増え、マルウェアなどサイバー攻撃に対するセキュリティの重要性が高まっている。マルウェアはネットワーク通信を利用し、外部への機密情報を漏洩、外部からの新たなマルウェアのダウンロードなどを行う。そのためマルウェアの行うネットワーク通信の詳細について知ることは不正な通信を検出することに役に立てられると考える。

マルウェアが行う不正なネットワーク通信を検出するためにプロキシサーバを用いてネットワーク通信を監視する手法[1]がある。しかしプロキシサーバで通信内容を監視するためには通信内容が暗号化されていないことが必要である。

そこで本研究では明示型のプロキシサーバを開発し、マルウェアの行うネットワーク通信について調査を行う。

調査の対象となるマルウェアサンプルとして MalwareBazaar[2]に 2021 年 11 月の間の実験当日にアップロードされた EXE ファイルのマルウェアを用いた。マルウェアがアップロードされた時間が実験当日の UTC 時間で早いものから選んだ。ネットワーク通信を行う 1000 サンプルのマルウェアを対象に調査を行った。

2. 実験

マルウェアは Windows 10 Pro の Hyper-V を用いて FlareVM[3]を構築し仮想環境上で実行する。開発した明示型プロキシサーバとのみ通信を行う。実験において 1 サンプルにつきマルウェアは 5 分間実行し調査を行う。

2.1　プロキシサーバの開発

実験ではマルウェアに外部への通信を許可しない。そのため、本研究では適当なレスポンスを返すようなプロキシサーバが必要になる。そのため OpenSSL ライブラリを利用し、C 言語を用いてリクエストに HTTP/1.1 200 OK を返す明示型プロキシサーバを開発した。暗号化された通信を復号するために、SSL インスペクションを行う。

A survey on malware from the viewpoint of network communication and SSL inspection
Takahiro Moro†, Noriaki Yoshiura†
Graduate School of Science and Engineering, Saitama University†

2.2 調査する特徴

本研究では、マルウェアの行うネットワーク通信の特徴として、プロキシサーバを経由するマルウェアの割合、通信先のポート番号、通信先ドメイン、通信先のサーバが用いるサーバ証明書、通信先へのリクエストメソッド、通信先への HTTP リクエスト時のファイル拡張子、SSL インスペクションへの耐性を調査する。

3. 実験結果

ネットワーク通信を行うマルウェア 1000 サンプルのうち、プロキシサーバを経由せず通信を行おうとするマルウェアは 436 サンプル存在した。また、プロキシサーバを経由するマルウェアは HTTPS 通信を行うマルウェアが 315 サンプル、HTTP 通信を行うマルウェアが 324 サンプル存在した。サンプルのなかには HTTP 通信や HTTPS 通信の両方を利用するような場合がある。なお、プロキシサーバを経由しないマルウェアについては宛先ポート番号のみ調べる。宛先ポート番号以外の特徴についてはプロキシサーバを経由するマルウェアについてのみ調査を行う。

3.1 宛先ポート番号

HTTP 通信や HTTPS 通信を行うウェブサーバなどでは HTTP 通信では 80 番のポート番号、HTTPS 通信では 443 番を利用していることが多い。マルウェアがネットワーク通信を行う際にはどのポート番号と通信を行うのか調査を行った。

プロキシサーバを経由しないマルウェアは 161 サンプルがポート番号 80 番、33 サンプルがポート番号 443 番を利用したリモートサーバと通信を行った。プロキシサーバを経由するマルウェアについては HTTP 通信を行うマルウェアでは 12 サンプルが 80 番ではない 1234 番、2222 番, 8000 番, 8080 番, 58888 番とのポート番号と通信を行った。また、HTTPS 通信を行うマルウェアについては 2 サンプルがそれぞれ 443 番ではない 58899 番、61443 番のポート番号と通信を行っている。

3.2 マルウェアの宛先ドメイン

プロキシサーバを経由するマルウェアは HTTP に従いプロキシサーバに宛先を伝える。宛先を I

P アドレスにて指定したマルウェアは HTTPS 通信を行うマルウェアでは 16 サンプル、HTTP 通信を行うマルウェアでは 91 サンプル存在した。

マルウェアの通信先のサーバのトップレベルドメインのなかで比較的多い com,org,top についてアクセスするマルウェアの数を表 1 に示す。

マルウェアの宛先として多かったのは cdn.discordapp.com:443 及び onedrive.live.com:443 であった。cdn.discordapp.com:443 にアクセスするマルウェアは 111 サンプル、onedrive.live.com:443 にアクセスするマルウェアは 37 サンプルであった。

表 1　トップレベルドメイン

	HTTPS	HTTP	合計
com	247	147	394
org	58	38	96
top	0	40	40

3.3 マルウェアが要求するファイル拡張子

通信先に拡張子がついたファイルを要求しているマルウェアについて調査を行ったところ HTTPS 通信では exe, jpg, txt, php, sre, jpeg, dll, png, bin, xml, json, crw, ini の 13 種類の拡張子が確認された。また HTTP 通信では exe, jpg, txt, php, upt, asmx, jpeg, bin, png, crl, dll, crw の 12 種類の拡張子が確認された。多かった拡張子について表 2 に示す。

表 2　拡張子

	HTTPS	HTTP	合計
exe	38	28	66
jpg	54	6	60
txt	12	3	15
php	9	76	85

3.4 マルウェアの利用するサーバ証明書

HTTPS 通信を行うマルウェアがアクセスしようとしたサーバは 114 個存在した。これらのサーバにサーバ証明書を要求した結果、証明書を返してくるサーバで自己署名証明書を利用しているサーバは 10 個であった。また自己署名証明書を使用しているサーバと通信を行うマルウェアはすべて IP アドレスで宛先を指定していた。
なお、29 個のサーバはすでに DNS 上で存在しないサーバのホスト名を利用しているなどの原因で証明書を確認できていない。

3.5 マルウェアのリクエストメソッド

リクエストメソッドには 3 種類が確認できた。表 3 に詳細を示す。

表 3　リクエストメソッド

	HTTPS	HTTP	合計
GET	310	216	526
POST	5	126	131
HEAD	0	17	17

3.6 SSL インスペクションへの有効性

本研究ではマルウェアが偽装されたサーバ証明書に気づいた場合にはリクエストメソッドを送らないと想定した。調査の結果、リクエストメソッドを送信しないマルウェアは存在しなかった。

4.　考察

HTTP 通信と HTTPS 通信を行うマルウェアで違った特徴を確認できた。プロキシサーバを経由し HTTPS 通信を行うマルウェアでは HTTP 通信を行うマルウェアと比較し、宛先に IP アドレスを指定することが少なく、サーバへのリクエストでは POST メソッドと HEAD メソッドが用いることが少なく、また PHP ファイルを要求していることが少ないことなどがわかる。またマルウェアは有名なクラウドサービスを行うサーバと通信を行っていた。有名なサービスを行うサーバとの通信であることは安心できる理由にならないことを示している。以上の調査を行うにあたり HTTPS 通信を行うマルウェアでは現時点では SSL インスペクションに対し検証プロセスを持っていなかった。多くのマルウェアでは、通信内容を監視することができると考えられる。

5. 今後の課題とまとめ

ネットワーク通信を行うマルウェアの特徴の調査を行った。マルウェアの特徴を知ることは、機械学習においての特徴として用いるなど不正な通信を検出することに役に立てられると考える。

今後の課題としては、良性の通信の特徴を調べ悪意のある通信と比較し、マルウェア特有の特徴を調査することである。

参考文献

[1] Ahmed, M. B., Shoikot, M., Hossain, J., & Rahman,A. Keylogger Detection using Memory Forensic and Network Monitoring.International Journal of Computer Applications, Volume 177. pp. 17-21(2019).
[2]MalwareBazaar, https://bazaar.abuse.ch/
[3]FlareVM,https://www.fireeye.com/services/freeware/flare-vm.html