NetStable 検出シグネチャのご説明

検出概要

2019 年 4 月 1 日から 5 月 21 日までの検出より、特に注意を頂きたいシグネチャについて抜粋し、その内容と対処についてご説明致します。

【今回取り上げるシグネチャ】

シグネチャ ID	シグネチャ名	検出割合
2000381	Windows Live Mail SMTP	39.8%
2000479	BaiduIME Block SSL	25.4%
2000432	FTP Server unencrypted login	16.1%

2000381 Windows(ウインドウズ) Live(ライブ) Mail(メール) SMTP(エスエムティーピー) について

【シグネチャの内容】

このシグネチャは、サポートが終了しているソフト「Windows Live メール」を用いたメールの送信を検知するシグネチャです。

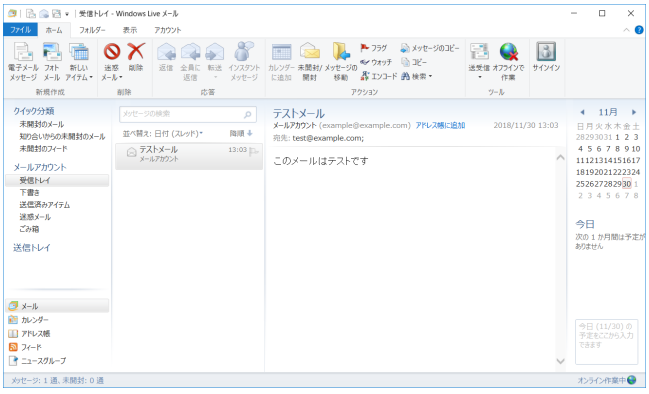
このシグネチャが検知された場合は、社内で「Windows Live メール」を利用しメール送信が行われていることを示します。

【検出時の対処】

検出ログの送信元 IP アドレスのパソコンに「Windows Live メール」がインストールされており、メール送信が行われています。

サポートが終了しているソフトは、今後機能追加やセキュリティの更新が行われないため、マルウェア感染のリスクが高くなります。

他のメールソフトの「Outlook(アウトルック)」や「Thunderbird(サンダーバード)」などへ移行される事をお勧めします。



Windows Live メールの外観

2000479 BaiduIME Block SSL について

【シグネチャの内容】
日本語入力ソフト「BaiduIME」の「クラウド変換機能」が有効である場合に発生する、Baidu 社サーバへの通信を検知するシグネチャです。

また、社内の Wi-Fi に接続されているスマートフォン上に、日本語入力アプリ「Simeji」がインストールされており、クラウド変換機能が有効の場合にも検出されます。

【検出時の対処】
検出ログの送信元 IP アドレスのパソコンやスマートフォンに「BaiduIME」や「Simeji」がインストールされています。

BaiduIME は、顔文字や今話題のワードなどの変換に長けているという特徴があるとされています。
また、クラウド変換機能は、入力中の文字情報を Baidu 社のサーバに送信し、変換精度を高める機能です。
業務用のパソコンにおいて「クラウド変換機能」の必要の有無や、「BaiduIME」の利用可否を検討されることをお勧めします。

2000432 FTP Server unencrypted login について

【シグネチャの内容】
ホームページ更新等に利用される「FTP」の通信において、暗号化せずにログインの接続が行われた事を検知するシグネチャです。

FTP 標準では通信内容が暗号化されず、セキュリティリスクがあります。
近年では暗号化された FTP 通信である「FTPS」等に対応したサービスも多くなっていますので、利用している FTP サーバでセキュリティが高い方式が利用可能である場合、設定を変更されることをお勧めします。

【検出時の対処】
検出ログの送信元 IP アドレスのパソコンが、受信先 IP アドレスのサーバと暗号化されていない FTP 通信を行っています。

FTP 通信の設定を確認し、暗号化された FTP 通信や、セキュリティの高い方式に変更されることをお勧めします。