Technical Report

2013年3月21日

韓国におけるサイバー攻撃の概要ならびに Sniperシリーズのシグネチャリリースについて

株式会社セキュアソフト

1. 概要

2013年03月20日午後２時ごろ、韓国の主要放送局、金融のネットワークに大規模の障害が発生したことが確認されました(放送局：3社、金融： 5 社)。本件は対象機器に対して、悪性コードを感染させ、システムのディスク破壊を行い、システムブートを不可能とするものです。

2. 本件の状況

今回の事象は各社が運用している特定セキュリティベンダーのPMS(Patch Management System：パッチ管理システム)の脆弱性が問題の基点となり、悪性コードを伝播し、サーバやPCへ被害を与えていると判断しています。
今回の悪性コードの動作内容とOSシステムごとの発生事象については下記のとおりです。

【直接被害：Windowsシステム】

Windows

- **物理ディスクの破壊**
  MBR(Master Boot Record)及びVBR(Volume Boot Record)へ任意の文字列をOverwrite.(PRINCPESまたはHASTATI)
  MBRのエラー発生後、コンピュータを再起動させようとするが、MBRが破壊されているためブート不可
- **論理ドライブの破壊**
  論理ドライブへ任意の文字列をOverwrite.(PRINCPESまたはHASTATI)

【間接被害：UNIXシステム】

UNIX

感染したWindowsシステムとSSHサービスが動作中の場合にUnixシステムが悪性コードを二次感染し、ディスクに影響を与えます。

- 論理ドライブの破壊
  論理ドライブを削除(/, /Kernel, /usr/adm, /etc, /home)

3. SNIPER IPSにおける対応シグネチャ

Sniper製品では、本攻撃に対応するため、下記シグネチャを3/22に緊急リリースします。

攻撃カテゴリ	攻撃コード	攻撃名
パターンブロック	1733	Win32/Trojan.Bootkit.24576

※今後の状況は継続的にモニタリングして追加のシグネチャがリリースされることもあります。

以上