5F-02

Event Logを用いたMS17-010の脆弱性を悪用する攻撃の検知

藤本 万里子[1]　松田 亘[1]　満永 拓邦[1]

概要：Windows の脆弱性を悪用する攻撃により，多くの組織がサイバー攻撃による被害を受けている．特に 2017 年に公開された MS17-010 の脆弱性は，Wannacry ランサムウエアや標的型攻撃の感染拡大活動に悪用された．本脆弱性を悪用する Eternalblue Doublepulsar などの攻撃ツールはインターネットに公開されており，攻撃者は容易に MS17-010 を悪用した攻撃を行える．更に本ツールは WIndows の正規のプロセスを悪用するため，攻撃を受けたことに気づくのが難しい．本研究では，WIndows の Event Log から MS17-010 の脆弱性を悪用する攻撃の痕跡を調査する方法を紹介する．

1. MS17-010の脆弱性とそれを悪用する攻撃

1.1 MS17-010の脆弱性

MS17-010[1] は，Server Message Block (SMB) version 1[*1]のリクエストの処理に存在するバッファオーバフロー[*2]の脆弱性である．攻撃者が脆弱性の悪用に成功した場合，ターゲットシステム上で任意のコードを実行することが可能になる場合がある．MS17-010 の脆弱性は，カーネルの一部の機能に存在するため，脆弱性の悪用に成功した場合，特権 (管理者権限) で悪意あるコードが実行される．さらに，SMB のサービスがインターネットに公開されている場合，攻撃者は遠隔から任意のコードを実行できるため，大きな脅威となる．

1.2 Eternalblue Doublepulsar

Eternalblue は MS17-010 の脆弱性を悪用する攻撃ツールで，Wannacry ランサムウエアや標的型攻撃の感染拡大活動に悪用された．攻撃者は本ツールを用いて，ターゲットシステムに Doublepulsar と呼ばれるバックドアを設置し，遠隔からターゲットをコントロールする．これらのツールはインターネットに公開され，フリーのペネトレーションテストツールである Metasploit Framework[2] にも組み込まれているため，専門知識を有していなくとも，比較的容易に攻撃を行うことができる．さらに，Doublepulsar は Windows の正規のプロセスを悪用するため，攻撃を受けたことに気づくのが難しい．攻撃の流れを以下に示す．

(1) ターゲットシステムに SMB リクエストを送信し，レスポンスから Doublepulsar が設置されているかを調査する
(2) 設置されていない場合，再度 SMB リクエストを送信し，正規の Windows プロセスに Doublepulsar のペイロードを注入する
(3) Doublepulsar を設置後，Doublepulsar を使用して遠隔からターゲットシステムをコントロールする

2. 既存研究

M.Satheesh Kumar ら，Paraskevi Dinaki らは SMB の通信パケットから Eternalblue Doublepulsar による攻撃を検知するための IDS[*3]のルールを提案している [3],[4]．また，Da-Yu Kao らは通信パケットやプロセス等の情報から Eternalblue Doublepulsar による攻撃を検知する手法を提案している [5]．しかし，Windows 標準のログから攻撃を検知する手法については紹介されていないため，本研究では Event Log を用いた検知手法について紹介する．

3. 提案手法

本研究では，WIndows の Event Log から Eternalblue Doublepulsar による MS17-010 の脆弱性を悪用する攻撃の痕跡を検知する方法を紹介する．

[1] 東京大学 (The Uniersity of Tokyo)

[*1] 全バージョンの Windows で利用できるファイル共有サービスなどで使用されるプロトコル．

[*2] 入力データを検証せずにコピーなどを行っている処理に対して，悪意あるデータを入力されることにより，メモリ領域が意図せず上書きされる脆弱性．攻撃者は脆弱性を悪用し，悪意あるコードをロードして実行する事ができる．

[*3] ネットワークを監視し，侵入やその兆候を検出するシステム．

表 1　検知に用いる Event Log
Table 1　Event logs for detection.

Event ID	イベントの概要
5140	ネットワーク共有オブジェクトにアクセスされた
4688	新しいプロセスが作成された
4763	特権を持つサービスが呼び出された

表 2　検知に用いる指標
Table 2　Signatures for detection.

Event ID	項目名	検知指標
5140	Security ID	ANONYMOUS LOGON に一致
	Share Name	IPC$を含む
4688	Security ID	SYSTEM に一致
	New Process Name	rundll32.exe を含む
4763	Security ID	SYSTEM に一致
	Privileges	SeTcbPrivilege を含む

3.1　検知に用いる Event Log

Event Log とは，システムやアプリケーションが記録する Windows 標準のログであり，当該コンピュータ上で発生した事象 (Event) が記録される．各 Event にはカテゴリ毎に Event ID と呼ばれる ID が割り当てられている．表 1 に検知に使用する Event ID，及び表 2 攻撃検知のポイントを示す．

3.2　検知アルゴリズム

攻撃を行った際に，表 1 に示す Event でが記録されるが，これらは，通常の運用時にも記録される Event であるため，Event 単独で判定を行うと，false positive[*4]が発生する．表 3 に示す複数の環境で評価を行なった結果，攻撃時にはこれらの Event 群が一連の流れで発生する事が分かったため，以下のアルゴリズムにて判定を行う．なお，Event log はそのままの形式では解析するのが難しいため，本研究では，Windows 標準の機能で CSV 形式にエクスポートしたデータに対して，アルゴリズムの適用を行う．

(1) 表 1 に示す Event ID を抽出する
(2) Event ID: 4763(攻撃時に最後に発生する Event) を境界とし，前後 3 秒 (攻撃コード実行完了に要する時間の平均から算出) 以内に発生した Event をグルーピングする
(3) グルーピングした Event 群に対して，表 2 に合致する全ての Event が含まれる場合，攻撃と判定する

4.　提案手法の評価

提案手法によって，Eternalblue Doublepulsar を用いた攻撃を検知することが可能か評価を実施する．攻撃ツールは Metasploit に組み込まれた Eternalblue Doublepulsar のモジュールを使用する．表 3 に示す環境での評価結果を示す．[5] によると，ターゲットシステムに Doublepulsar が既に設置されている場合と，そうでない場合で攻撃ツールの挙動が変わるため，Doublepulsar が設置済の場合と未設置の場合について評価を行った．また，Doublepulsar のペイロードを注入するプロセスとして，インターネットに攻撃例として紹介されている spoolsv.exe を使用した．

[*4] 攻撃でない事象を攻撃であると判定すること

表 3　評価結果
Table 3　Evaluation result.

OS	Doublepulsar 有無	検知可否
Windows Server 2008 R2	未設置	検知成功
Windows Server 2008 R2	設置済	検知成功
Windows 7(x64)	未設置	検知成功
Windows 7(x64)	設置済	検知成功

評価の結果，提案手法を用いて，Eternalblue Doublepulsar を用いた攻撃を検知することが可能であることが分かった．ただし，以下のケースは未検証である．

- spoolsv.exe 以外のプロセスが悪用された場合
- 表 3 に示す環境以外のシステムが攻撃を受けた場合

false positive が発生しないことを確認するために，攻撃を行っていない 40 台のコンピュータの Event log を入力とし，評価を行なったところ，全ログ 56,527 件中，false positive は 0 件であった．

5.　終わりに

MS17-010 のように，悪用によって遠隔から任意のコードを実行できる脆弱性の攻撃手法が公開された場合，被害が広がるリスクが高い．本研究では Event log から MS17-010 の脆弱性を悪用する攻撃を検知する手法を紹介し，提案手法を用いて攻撃活動を早期に検知することで，被害を抑制することが可能になる．今後は，通信の分析による検知や，驚異度の高い他の Windows の脆弱性の検知手法などについて，研究を継続する予定である．

参考文献

[1] Microsoft : Microsoft Security Bulletin MS17-010 - Critical，入手先 ⟨https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010⟩.
[2] Eleven Paths : Eternalblue-Doublepulsar-Metasploit，入手先 ⟨https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit⟩.
[3] M.Satheesh Kumar and Jalel Ben-Othman and K.G.Srinivasagan.: Department of Electronics and Communication Engineering National Engineering College, An Investigation on Wannacry Ransomware and its Detection.
[4] Paraskevi Dinaki.: SCHOOL OF SCIENCE & TECHNOLOGY, Deep Packet Inspection: A Comparison Study Between Ex- act Match and Regular Expres- sion Techniques.
[5] Da-Yu Kao and Shou-Ching Hsiao, Department of Information Management, Central Police University, The dynamic analysis of WannaCry ransomware.