セキュリティインシデント事例①
半導体製造企業の事例

Ver. 1.0.0

Edgecross コンソーシアム　テクニカル部会　セキュリティガイドライン策定 WG

テクニカル部会　セキュリティガイドライン策定WG
参加企業(敬称略、順不同)

株式会社立花エレテック

DMG森精機株式会社

日本電気株式会社

株式会社日立製作所

富士通株式会社

三菱電機株式会社

マカフィー株式会社

日本マイクロソフト株式会社

トレンドマイクロ株式会社

改定履歴

Ver.	改定内容	発行年月
1.0.0	初版発行	2022 年 3 月

目次

1. はじめに ····· 1

1.1 概要 ····· 1

1.2 略称 ····· 1

1.3 用語 ····· 1

1.4 関連資料 ····· 2

2. セキュリティインシデント ····· 3

2.1 概要 ····· 3

2.2 詳細 ····· 3

3. 想定されるリスク ····· 5

4. 関連する脆弱性情報 ····· 6

5. 推奨される対策 ····· 7

6. まとめ ····· 11

1. はじめに

1. 1 概要

工場におけるセキュリティインシデントは絶えることがありません。Edgecross ユーザ企業からは工場におけるセキュリティインシデント動向として具体的な事例を知りたいとの声が Edgecross コンソーシアムに寄せられています。

このような背景から、本書では、過去のセキュリティインシデントのうち代表的な事例を取り上げ、想定されるリスクや関連する脆弱性情報とともに紹介します。そして、Edgecross ユーザ向けセキュリティガイドライン[1]、Edgecross 開発者向けセキュリティガイドライン[2]を活用できるように、Edgecross を用いた FA システムがインシデント事例と同様に攻撃されることを想定して、Edgecross 向けの推奨対策を提示することが最大の特色となっています。

想定読者は、工場管理者／従事者、Edgecross 運用者、Edgecross 開発者と幅広くカバーしています。各立場に応じて本書を活用してください。

1. 2 略称

CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DLL	Dynamic Link Library
DMZ	DeMilitalized Zone
HMI	Human Machine Interface
IP	Internet Protocol
IPA	Information-technology Promotion Agency, Japan (独立行政法人 情報処理推進機構)
LAN	Local Area Network
MES	Manufacturing Execution System
OPC	OLE (Object Linking and Embedding) for Process Control
OS	Operating System
PC	Personal Computer
PLC	Programmable Logic Controller
SMB	Server Massage Block
TCP	Transmission Control Protocol
TSMC	Taiwan Semiconductor Manufacturing Company Limited
USB	Universal Serial Bus
WWW	World Wide Web

1. 3 用語

本書で用いる用語を表 1-1 に示します。

表 1-1 用語

用語	説明
セキュリティインシデント	マルウェア感染や情報窃取等、セキュリティ上の問題である事象。
脆弱性	プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥。
バッファオーバーフロー	データの一時記憶領域であるバッファに対して、想定以上の長さのデータが入力されること。
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
ワーム	自身を複製して他の機器に拡散するマルウェア。

ウイルス	他のファイルに寄生して増殖するマルウェア。
ランサムウェア	身代金の要求を目的としたマルウェア。
バックドア	秘密裏に仕込まれた、遠隔操作のための接続口。
スキャン	機器の各ポートに対して外部からパケットを送信し、その応答によって稼働中のサービスや空きポート、OS 種別・バージョン等を調査する手口。
エクスプロイト	脆弱性を攻撃するプログラム。
クラッキング	悪意のあるセキュリティ犯罪行為。
ファイルレス攻撃	ディスクには痕跡を残さず、メモリ上にのみ存在するマルウェアによる攻撃。
ネットワークセグメンテーション	複数のサブネットワークに分割して、サブネットワーク毎にポリシーを定めて運用するセキュリティ対策。
ファイアウォール	ネットワーク間の通信可否を制御して不正アクセスを防ぐセキュリティ対策。
振る舞い検知	プログラムの振る舞いからマルウェアか否かを検知するセキュリティ対策。
セキュリティパッチ	アプリケーションの脆弱性を解消するための修正プログラム。
パターンファイル	既知のウイルスの特徴を定義したファイルであり、ウイルス対策ソフトが用いる。
データコレクタ	各ネットワークを介し、生産現場のデータを収集するソフトウェアコンポーネントで、各種ネットワークおよび接続対象機器向けに各ベンダが提供。

1. 4 関連資料

本書の関連資料を表 1-2 に示します。

表 1-2 関連資料

No.	資料名称	資料 No	入手方法
1	Edgecross ユーザ向けセキュリティガイドライン詳細版	ECD-TE4-0006-01-JA	https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0006-01-JA.pdf
2	Edgecross 開発者向けセキュリティガイドライン	ECD-TE4-0008-01-JA	Edgecross コンソーシアム会員用ホームページ
3	台湾 TSMC、半導体工場がウイルス感染 生産一時停止 2018 年 8 月 6 日 日本経済新聞	-	https://www.nikkei.com/article/DGXMZO33846620W8A800C1FFE000/
4	制御システムのインシデント事例 6 ～2018 年 半導体製造企業のランサムウェアによる操業停止～ 2020 年 9 月 IPA	-	https://www.ipa.go.jp/files/000085317.pdf

2. セキュリティインシデント

本章では、WannaCry マルウェアによるセキュリティインシデントについて順を追って説明します。

2. 1 概要

2018 年 8 月、台湾の半導体製造企業 TSMC (Taiwan Semiconductor Manufacturing Company Limited)は、工場が WannaCry マルウェアに感染し、生産が 3 日間にわたって停止した結果、最大 190 億円の損害を被りました[3]。

本マルウェアに感染した端末が工場のネットワークに接続されることで、同ネットワークにつながる他の機器にも感染が拡大しました。そして、生産に関わる複数の機器が感染後に内部のデータを暗号化されることで機能不全となり、工場の生産が停止しました。

2. 2 詳細

生産停止に至るまでのサイバー攻撃は、下記(1)～(5)のような流れで行われたとされています[4]。

(1) WannaCry マルウェアに感染した端末を持ち込み、工場内の制御ネットワークに接続。

(2) 端末内のマルウェアが、ネットワーク上の他の機器をスキャンして、利用可能なポートを持つ攻撃対象の機器を探索。

具体的には、端末内のマルウェアがローカルネットワーク内のスキャンを行うとともに、パブリック IP アドレスをランダムにスキャンし、SMBv1 サービスの脆弱性（MS17-010）が存在する攻撃対象の機器を探索。

(3) 端末内のマルウェアが、利用可能なポートを通して攻撃対象の機器と通信し、同機器内の脆弱性を悪用して自分自身をコピーすることで、本機器を新たに感染。

具体的には、端末内のマルウェアが、SMBv1 サービスの脆弱性が存在する攻撃対象の機器に、攻撃コード（通称：EternalBlue）を用いて攻撃を実行。バッファオーバーフローによるデータ書き換えを起点に、シェルコードを配置・実行し、SMB の正規の関数をフックしてバックドア（通称：DoublePulsar）を設置。

さらに、バックドアを利用して、攻撃対象の機器にマルウェア本体を内包した不正 DLL(launcher.dll)を正規プロセス(lsass.exe)に注入。そして、不正 DLL がマルウェアファイルを作成し、不正サービス（mssecsvc2.0：“Microsoft Security Center (2.0) Service”）を開始。

(4) 新たに感染した機器が(2)(3)を実行してマルウェアを再拡散。

(5) 新たに感染した機器内のマルウェアが、同機器内のデータを暗号化。

具体的には、不正サービスがランサム機能のファイルを展開して実行。ファイル暗号化や脅迫文の表示等のクラッキング活動を実施。

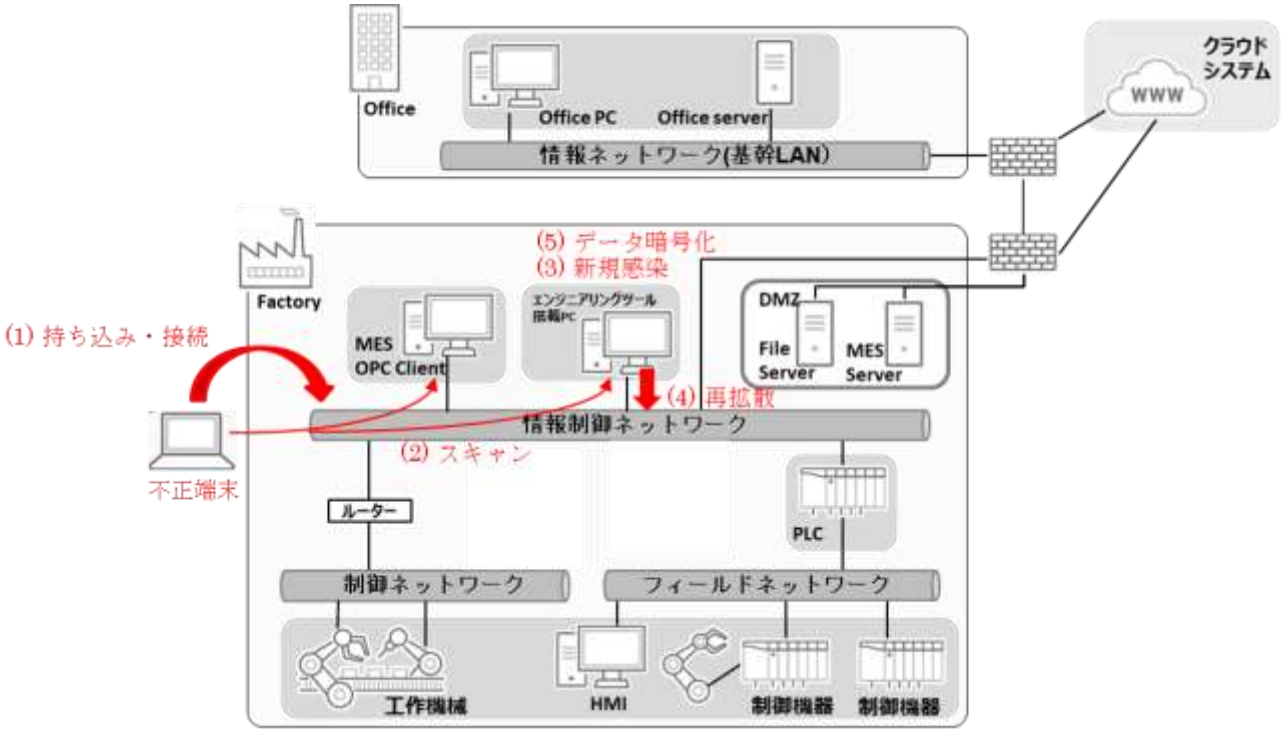

表 2-1 攻撃の流れ※

※システム構成は、実態が定かでないため、推測となります。

3. 想定されるリスク

本章では、セキュリティインシデントにより想定されるリスクについて説明します。

セキュリティインシデントが発生した場合に想定されるリスクとして、以下のものが考えられます。

(1) 製品事業の伸張・継続、納期遵守・遅延防止、コスト低減が妨げられる
FAシステムは、製品事業の伸張・継続を実現するために、生産性をより高め、コスト低減を図るとともに、安定的かつ継続的に製品を生産するためのシステムであり、その安定・連続稼働(可用性)が求められます。これは、納期遵守・遅延防止のためにも必要です。セキュリティインシデントの発生により、FA システムの可用性が損なわれると、製品事業の伸張・継続、納期遵守・遅延防止、コスト低減が妨げられるリスクがあります。

(2) 工場の安全確保、製品の品質確保が妨げられる
工場の安全確保や製品の品質確保を実現するために、FA システム及び機器が正常に動作する状態を保つことが求められます。セキュリティインシデントの発生により、機能・制御の完全性が損なわれると、工場の安全確保や製品の品質確保が妨げられるリスクがあります。

(3) FA システム及び機器の正常動作確保や、適正なフィードバック制御の実現を妨げられる
FA システム及び機器が正常に動作する状態を保つためには、システム及び機器の機能・制御の仕方を設定・指示(命令)するデータが正しいこと、すなわちデータが壊れたり改ざんされたりしていないことが求められます。また、FA システム及び機器の制御・稼働・運用の最適化・自動化(自律化)を図る目的で、システム及び機器の稼働状態に応じたフィードバック制御を実現するために、システム及び機器の稼働状態にかかわるデータを収集・分析・監視し、その時点の状態に基づき、システム及び機器の機能・制御の仕方にかかわる設定・指示(命令)を変更していく運用の実現が必要になってきています。セキュリティインシデントの発生により、データの完全性が損なわれると、FA システム及び機器の正常動作確保や、適正なフィードバック制御の実現が妨げられるリスクがあります。

(4) 製品や生産(ノウハウ)にかかわる情報やデータの外部漏えい
製品事業にとって、競合他社による自社製品の優位点の模倣を防ぎ、差異及び競争優位性を確保することは重要であり、製品や生産(ノウハウ)にかかわる情報やデータが外部に漏えいしないようにすることが求められます。セキュリティインシデントの発生により、データの機密性が損なわれると、製品や生産(ノウハウ)にかかわる情報やデータの外部漏えいが起こるリスクがあります。

(5) 製品の部品に内包されたセキュリティ脅威により、製品の製造責任を問われる
工場における製品の生産過程で、製品の部品として用いられるハードウェアやソフトウェア(プログラム)の中に、セキュリティ脅威を内包する不正なものが意図せず含まれてしまうことがあり、製品出荷後に製品内包セキュリティ脅威により、製品が外部から不正に利用・制御されたり、製品の稼働を妨害されたり、製品利用者の情報を外部へ漏えいさせたりする問題を引き起こすことが発生しています。セキュリティインシデントの発生により、製品が外部から不正に利用・制御されたり、製品の稼働を妨害されたり、製品利用者の情報を外部へ漏えいされたりすることで、製品の製造責任を問われるリスクがあります。

上記のリスクを防止/抑止するために、セキュリティインシデントを対象としたセキュリティ対策を検討する必要があります。

特に、工場が WannaCry に感染した場合には、データが暗号化されることで、FA システムや機器の正常動作に支障がでるだけでなく、復旧までに多大な時間を要するというリスクがあります。

4. 関連する脆弱性情報

WannaCry 関連の脆弱性は、マイクロソフトのセキュリティ情報「MS17-010」で公開された内容に該当します。MS17-010 では該当する脆弱性は 6 つあります。

CVE 番号	概要	CVSS v3
CVE-2017-0143	Windows SMB のリモートでコードが実行される脆弱性	8.1
CVE-2017-0144	Windows SMB のリモートでコードが実行される脆弱性	8.1
CVE-2017-0145	Windows SMB のリモートでコードが実行される脆弱性	8.1
CVE-2017-0146	Windows SMB のリモートでコードが実行される脆弱性	8.1
CVE-2017-0148	Windows SMB のリモートでコードが実行される脆弱性	8.1
CVE-2017-0147	Windows SMB の情報漏えいの脆弱性	5.9

概要:

WannaCry の感染に利用された脆弱性は、Windows OS のファイル共有やプリンター共有等で利用される SMB(Server Massage Block)プロトコルに対する脆弱性です。SMB の中でも古い v1 が該当します。

リモートから任意のコードが実行される脆弱性であるため、マイクロソフトでは WannaCry の被害拡大前の 2017 年 3 月には修正プログラムを公開していましたが、この修正が適用されていない環境下において被害が拡大しました。

背景の一つには、WannaCry そのものはランサムウェアとして広く認識されていますが、感染手法が自己増殖を繰り返すワーム活動と同等のものであったため、急激な広がりを見せました。

EternalBlue について:

WannaCry の感染には攻撃ツール「EternalBlue」が利用されています。EternalBlue は MS17-010 の脆弱性を利用しています。WannaCry ではこのツールを利用し、自身の感染を広げるワーム活動に利用しています。

より技術的な詳細は以下のサイトでご確認ください。

https://blog.trendmicro.co.jp/archives/15154

SMBv1 について:

SMBv1 (1.0)は Windows XP および Windows Server 2003 R2 以前の OS が利用します。Windows Vista 以降の OS では互換性のために SMB1.0 がサポートされています。

ファイル共有、プリンター共有が不要な場合は、通信ポート(TCP445)を閉じることで対処ができます。通信ポートを閉じることができない場合は、OS 上での SMB1.0 の無効化が推奨されます。

5. 推奨される対策

本章では、分類した脅威と、それぞれの対策・緩和策について記述します。
表 5-1 に、本インシデント事例に関連した 8 種類の脅威と、それぞれの脅威に対しての対策・緩和策の概要を示しています。また、それぞれの対策・緩和策の対応を、Edgecross を活用する工場組織における、どの立場の人が行うべきかをマトリクスで示します。チェックマーク「✔」がついている立場の人が、対象者となります。

なお、本表の対象者は一例であり、対象となる組織等の構成を考慮して、対応する対象者に読み替えてください。

表 5-1 脅威の種別と対策・緩和策の概要

#	脅威	対策・緩和策	対象者			
			Edgecross 運用者	Edgecross 開発者	工場 従事者	工場 管理者
(1)	不正接続	・入退出管理 ・持ち込み機器の検疫			✔	✔
(2)	マルウェア拡散	・ネットワークセグメンテーション ・ファイアウォール最適化				✔
(3)	脆弱性の存在	・セキュリティパッチ導入 ・脆弱性作りこみ防止	✔	✔		
(4)	侵入攻撃	・脆弱性の解消 ・通信制限	✔			
(5)	バックドア設置	・侵入経路遮断 ・アクセス制限	✔			
(6)	マルウェア感染	・マルウェア対策ソフト導入	✔			
(7)	情報暗号化	・情報バックアップ ・リストア体制構築	✔			✔
(8)	亜種/新型マルウェアの出現	・マルウェア対策ソフト導入 ・最新のセキュリティ対策の実施	✔			✔

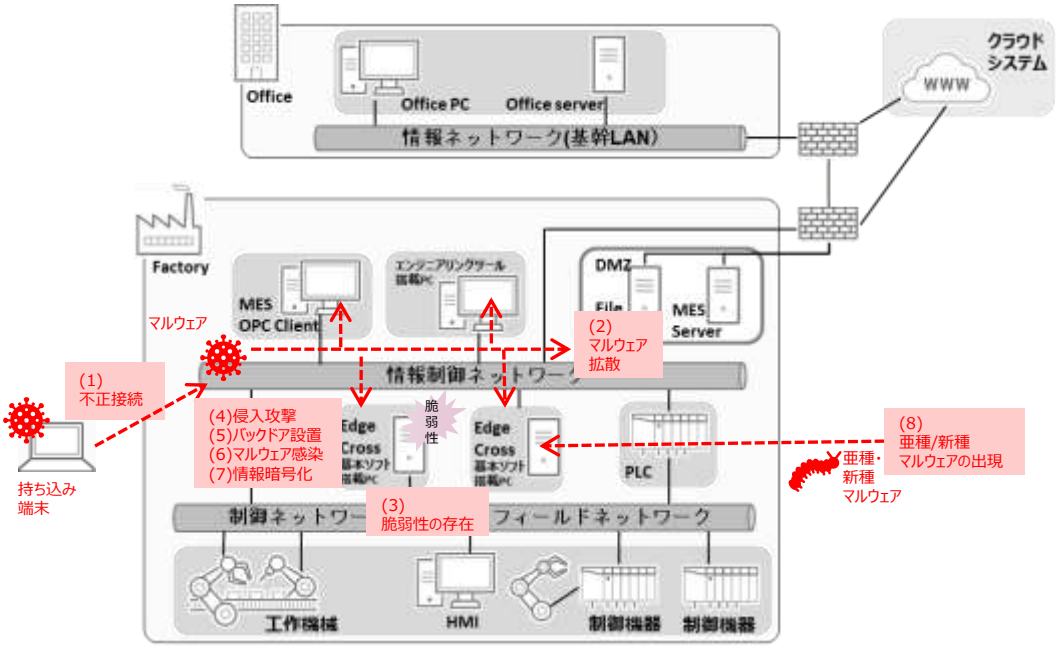

図 5-1 脅威の種別

以降に、8 種類のそれぞれの脅威に対して、どのような対策・緩和策を行うべきかの詳細を示します。

5.1 不正接続

WannaCry マルウェアはその感染した PC が接続したネットワークをスキャンして、感染拡大を図ります。そのため感染した PC や USB メモリを工場ネットワーク内に接続させないことが重要です。

感染した PC や USB メモリを接続させないためには、外部からそれらを持ち込む際に、持ち込み物の点検や、持ち込む際にウイルス対策ソフトでスキャンすることでリスクを低減することが可能です。

また工場ネットワークでの対策として、許可された PC や USB メモリのみが通信・動作するようなセキュリティ対策をすることが効果的です。

5.2 マルウェア拡散

WannaCry マルウェアは、感染 PC が接続されたネットワーク内をスキャンして攻撃対象（脆弱性の存在する PC）を探索し、マルウェアの拡散を試みます。

マルウェア拡散の防止・抑制には、各々の PC で脆弱性の対処を行うとともに、システム動作に必要な範囲にネットワークの通信を制限することが重要です。

制御ネットワークのように独立性の高いネットワークにおいても、適切なネットワークセグメンテーションを行い、セグメント間にファイアウォールを設置し、セグメント間の通信は必要最小限に制限する必要があります。

WannaCry のスキャンアルゴリズムでは、ローカルネットワーク内のスキャンを行うとともに、パブリック IP アドレスをランダムにスキャンします。つまり、制御ネットワークから情報ネットワークへスキャン（即ちマルウェア拡散の脅威）もあり得ます。

IP アドレスをランダムにスキャンするため、実際に攻撃対象となる確率は低いですが、今後スキャンアルゴリズムの違う亜種が出現する可能性もあります。

制御ネットワークから情報ネットワークへの拡散を対処するために、境界間のファイアウォールで、可能な限り不要な通信を除外する必要があります。通常、情報ネットワークから制御ネットワークへ向かう通信は厳しく制限されますが、逆方向（制御ネットワークから情報ネットワークへ向かう通信）の制限が不十分なケースがあるので注意が必要です。

5.3 脆弱性の存在

WannaCry マルウェアは、SMBv1 サービスの脆弱性（MS17-010）を利用しますが、MS17-010 のセキュリティパッチは、2017 年 3 月に公開されていました。対して、WannaCry マルウェアが猛威を振るったのはパッチ公開から 2 か月後の 2017 年 5 月であり、本インシデント事例は 1 年以上も後の 2018 年 8 月に発生しています。

この事実は、次の状況を示しています。

① 公開されているセキュリティパッチを適用しなかった機器が多数あることが、WannaCry マルウェアの世界的な拡散に繋がった。

② 上記①の事例が公になっているにも関わらず、1 年以上もセキュリティパッチを適用せずに、本インシデント事例が発生した。

システムに最新のセキュリティパッチを適用して脆弱性対策を実施することが、重要なセキュリティ対策であることが広く認知されている一方で、本インシデントが発生した事は、全ての機器にセキュリティパッチの適用を徹底することの困難さを示唆しているとも言えます。企業や工場においては、従業員個人レベルではなく、経営レベルでのトップダウンによるセキュリティ対策の徹底が望まれます。

Edgecross 開発者は、脆弱性を生み出さないように注意が必要です。SMBv1 サービスの脆弱性（MS17-010）は、バッファオーバーフローのバグが起点になっています。MS17-010 は、データサイズの演算ミスに起因するものですが、この種のバグは SMB 以外でも発生しうる危険な脆弱性になります。特に、Edgecross データコレクタ開発者は、制御装置側のネットワーク側からのバッファオーバーフロー攻撃を許さない慎重な実装が求められます。

5.4 侵入攻撃

WannaCry マルウェアの攻撃は、EternalBlue エクスプロイトにより、SMBv1 サービスの脆弱性を利用してバックドア(DoublePulsar)を設置することから始まります。この攻撃フェーズに対する最も重要な対策は、セキュリティパッチを適用し、脆弱性の芽を摘むことにあります。

翻って、攻撃者にとっては、SMB の脆弱性はバックドア設置の 1 つの手段に過ぎません。SMB の脆弱性以外の手段を用いてバックドア設置を試みるマルウェアが存在することにも留意する必要があります。

Edgecross 運用者は、侵入攻撃を緩和するために Edgecross 搭載 PC への通信は必要最小限に制限してください。

5.5 バックドア設置

DoublePulsar バックドアは、攻撃対象 PC のメモリ上にのみ存在するファイルレスマルウェアです。この種のマルウェアはファイルを持たないため、通常のマルウェア対策ソフトのファイル監視機能では検知できません。WannaCry マルウェアの攻撃シナリオにおいて、EternalBlue エクスプロイトによる SMBv1 サービスの脆弱性への攻撃、DoublePulsar の設置、不正 DLL の注入までが全てファイルレスの攻撃であり、隠密性が高い手段をとっています。(不正 DLL がファイルを生成する段階になって、ようやくファイル監視機能で検知できます。)

基本的に、一旦バックドアが設置されてしまうと被害を抑えることが困難になります。対策としては、前段階の侵入攻撃を防止することが重要です。

また、Edgecross 搭載 PC に直接ログインしてバックドアをインストールしたり、USB 接続で侵入する等、物理的な侵入経路もあったりしますので、適切なアクセス制限を行うことも重要です。

5.6 マルウェア感染

WannaCry マルウェアは、不正 DLL の注入まではファイルレスですが、破壊活動であるランサム機能は不正 DLL が生成した実行ファイルが担います。従って、マルウェア対策ソフトウェアがランサム機能の実行ファイルを検知・検疫できれば、ランサム活動の防止が可能になります。

マルウェア感染対策として、マルウェア対策ソフトウェアのパターンファイルを最新にして、既知のマルウェアから防護することが重要です。

また、未知のマルウェアから防護するため、「振る舞い検知」等の仕組みを取り入れたマルウェア対策ソフトウェアも登場しています。

5.7 情報暗号化

WannaCry マルウェアに感染すると、PC 内のデータを暗号化します。この対策としては、バックアップの取得が有効です。定期的にバックアップを取得することで、万が一 WannaCry マルウェアに暗号化されても、バックアップデータからデータを復旧することが可能です。

バックアップ取得時の注意点としては、以下 3 点です。

① バックアップ方式

常時データを同期するミラー方式のバックアップ方式は、データが暗号化されてしまった場合に、バックアップデータも暗号化されたデータになってしまうため、リストアができなくなってしまいます。必ずデータが暗号化されていないデータの静止点を見極めて、バックアップを取得することが重要となります。

② バックアップデータの格納先

バックアップデータをネットワーク上に取得することも避けるべきです。ネットワークでアクセス可能なバックアップデータは、WannaCry マルウェアの攻撃対象となりえるため、バックアップデータが暗号化されてしまう可能性があります。このためバックアップデータはネットワークから切り離し、保管することが重要となります。

③ 世代管理

WannaCry マルウェアに攻撃を受けて対象データが暗号化されたあとに取得したバックアップデータはリストアに利用できません。データの重要度に応じて、複数世代のバックアップを取得しておくことも有効です。

参考情報:ランサムウェアファイル復号ツール

バックアップからデータを復旧することができない場合、トレンドマイクロ社が提供するランサムウェアファイル復号ツールを利用することで、WannaCry をはじめとしたランサムウェアに暗号化されたファイルを復号できる可能性があります。詳細は以下サイトを参考にしてください。

トレンドマイクロ社:ランサムウェアファイル復号ツール
https://helpcenter.trendmicro.com/ja-JP/article/TMKA-19400/

5.8 亜種/新型マルウェアの出現

本インシデント事例では、WannaCry マルウェアへの対応を記載しましたが、より強力な亜種/新型マルウェアの出現も想定しておく必要もあります。

WannaCry マルウェアは、Windows10 には（SMBv1 サービスの脆弱性があったとしても）感染しないとも言われています。これには 2 つの側面があります。

1 つに、EternalBlue エクスプロイトは、ネットワークをスキャンして Windows7 以前の OS の端末のみを攻撃するため、そもそも Windows10 を攻撃対象としていないことが挙げられます。

もう1つは、Windows はバージョンが上がるにつれ、エクスプロイト保護機能（Data Execution Prevention、Address Space Layout Randomization 等）が強化され、脆弱性があっても容易に侵害されない点があります。

しかし、現在では、Windows10 を攻撃対象とするエクスプロイトや、強化されたエクスプロイト保護機能を突破するコードも出現し、攻撃と防御のいたちごっこが繰り返されています。

ユーザ側は、現状直接の脅威が無くとも、SMBv1 サービスの脆弱性のような致命的なバグは必ず対策することと、より保護機能が発達した最新 OS に更新しておくことが重要です。

WannaCry マルウェアは、バックドア(DoublePulsar)設置後にランサム行為等のクラッキング活動を行うため、感染していることが明らかです。しかし、DoublePulsar 設置および再拡散のみを行うマルウェアに感染した場合、ファイルレス攻撃が繰り返されることになり、発見が困難になります。

攻撃シナリオとして、DoublePulsar 設置と再拡散を繰り返すマルウェアを配布し、一定期間に感染拡大させた後、 一斉に DoublePulsar でクラッキング機能をインストール・実行するケースが考えられます。これは自然界のウイルスが潜伏期間を経て発症するメカニズムで拡大する様相に類似しています。

様々な亜種/新型マルウェアへの対処は難しい面もありますが、これまで記載した基本的な対策（脆弱性の解消、ネットワークセグメンテーション、通信制限、マルウェア対策ソフト導入等）が有効に働くことが期待できますので、漏らさず対策を行うことを推奨します。

6. まとめ

Edgecross を用いた FA システムの安全・安心を確保するため、本文書を活用ください。
なお、本書の記載に関する質問は、Edgecross コンソーシアムホームページのお問い合わせフォームに記入の上、問い合わせください。

Edgecross コンソーシアムお問い合わせフォーム https://www.edgecross.org/ja/contact/form/