2017 年 5 月 17 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、世界規模で感染が拡大するランサムウェア「WannaCry」に対するフォレンジクス分析と亜種にも有効なキルスイッチ・ドメインを公開

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社（本社：東京都、代表取締役社長：ピーター・ハレット、以下チェック・ポイント）は、チェック・ポイントの Incident Response チームがランサムウェア「WannaCry」の広範囲にわたる感染拡大の追跡調査を行い、詳細なフォレンジクス分析結果を含む WannaCry の活動分析、一般的な対策、チェック・ポイントによる保護機能の適用、および亜種にも有効なキルスイッチ・ドメインの登録を公開しました。現在、WannaCry を利用した複数の攻撃キャンペーンが同時発生しており、国内においても複数の被害が確認され SMB（Microsoft Server Message Block）経由でネットワーク内部に感染被害が広がっています。

WannaCry が使用する複数の攻撃経路

1 **SMB（Microsoft Server Message Block）を利用した直接的な感染拡大**：同じ攻撃経路を使用する亜種や模倣版など複数のサンプルの存在が確認されています。チェック・ポイントが検証したすべてのサンプルは、SandBlast のアンチランサムウェアまたは Threat Emulation で検出およびブロック可能です。

2 **電子メール内の不正なリンク**

3 **不正な PDF ファイルの添付**：不正なリンクを含む PDF ファイル

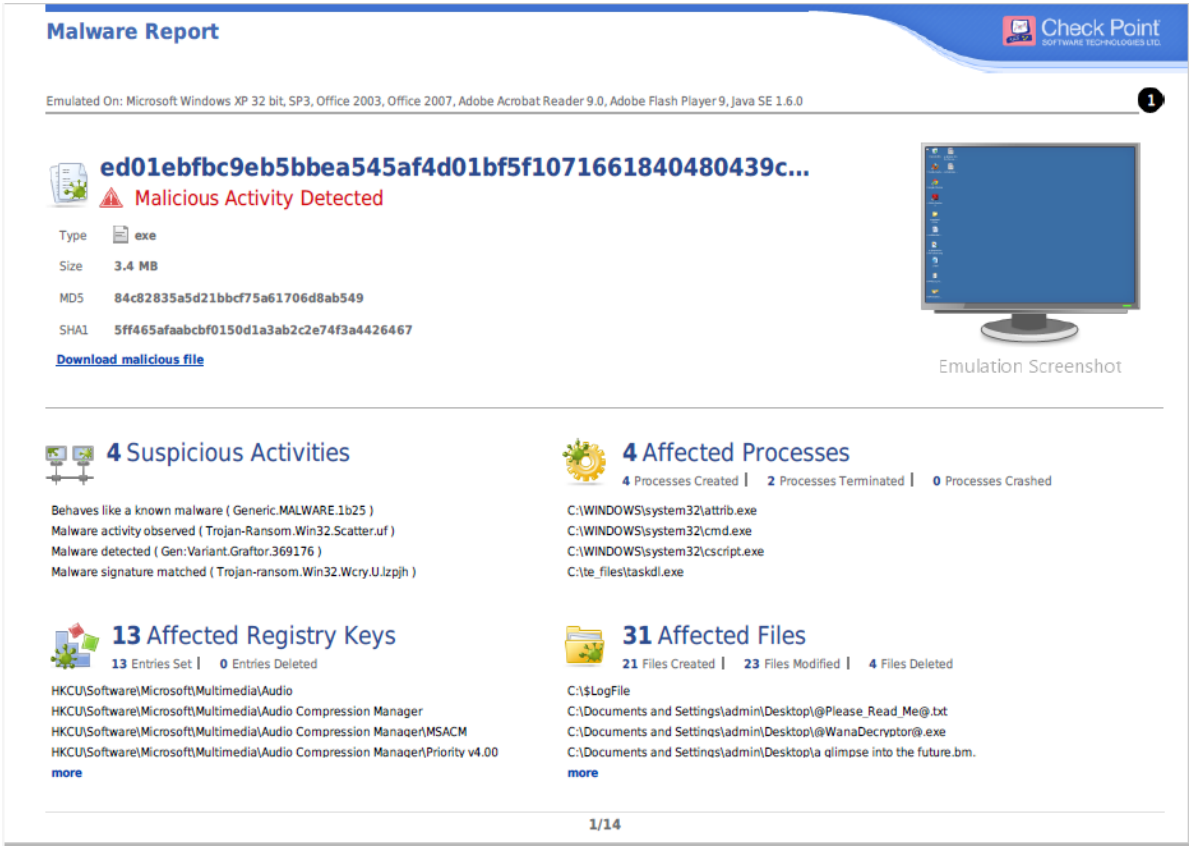
4 **不正な Zip ファイルの添付**：パスワードで保護された Zip ファイル。一連の感染活動を開始する PDF ファイルが格納されています。

5 **RDP サーバに対するブルート・フォース・アタックでのログイン**：ログイン後、同サーバにランサムウェアが仕掛けられます。

WannaCry の活動分析

以降では、WannaCry に対する攻撃の分析、レポートを紹介します。また、ランサムウェア全般の詳細については、こちらをご覧ください。

SandBlast Threat Emulation サンドボックスの検査レポートによる活動分析



Malware Report

Check Point SOFTWARE TECHNOLOGIES LTD.

Emulated On: Microsoft Windows XP 32 bit, SP3, Office 2003, Office 2007, Adobe Acrobat Reader 9.0, Adobe Flash Player 9, Java SE 1.6.0

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c...

Malicious Activity Detected

Type	exe
Size	3.4 MB
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467

Download malicious file

Emulation Screenshot

4 Suspicious Activities

Behaves like a known malware (Generic.MALWARE.1b25)
Malware activity observed (Trojan-Ransom.Win32.Scatter.uf)
Malware detected (Gen:Variant.Graftor.369176)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.lzpjh)

4 Affected Processes

4 Processes Created | 2 Processes Terminated | 0 Processes Crashed

C:\WINDOWS\system32\attrib.exe
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\cscript.exe
C:\te_files\taskdl.exe

13 Affected Registry Keys

13 Entries Set | 0 Entries Deleted

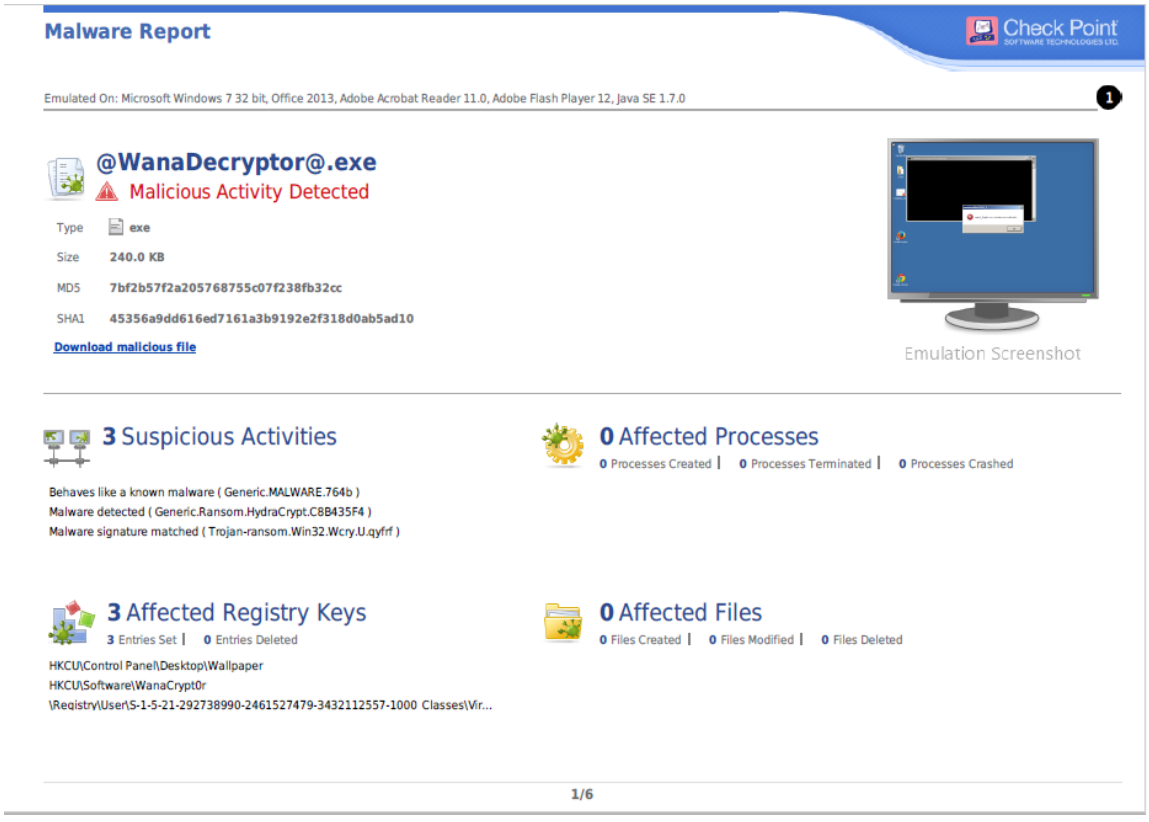
HKCU\Software\Microsoft\Multimedia\Audio
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00
more

31 Affected Files

21 Files Created | 23 Files Modified | 4 Files Deleted

C:\$LogFile
C:\Documents and Settings\admin\Desktop\@Please_Read_Me@.txt
C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe
C:\Documents and Settings\admin\Desktop\a glimpse into the future.bm.
more

1/14



Malware Report

Check Point SOFTWARE TECHNOLOGIES LTD.

Emulated On: Microsoft Windows 7 32 bit, Office 2013, Adobe Acrobat Reader 11.0, Adobe Flash Player 12, Java SE 1.7.0

@WanaDecryptor@.exe

Malicious Activity Detected

Type	exe
Size	240.0 KB
MD5	7bf2b57f2a205768755c07f238fb32cc
SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10

Download malicious file

Emulation Screenshot

3 Suspicious Activities

Behaves like a known malware (Generic.MALWARE.764b)
Malware detected (Generic.Ransom.HydraCrypt.C8B435F4)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.qyfrf)

0 Affected Processes

0 Processes Created | 0 Processes Terminated | 0 Processes Crashed

3 Affected Registry Keys

3 Entries Set | 0 Entries Deleted

HKCU\Control Panel\Desktop\Wallpaper
HKCU\Software\WanaCrypt0r
\Registry\User\S-1-5-21-292738990-2461527479-3432112557-1000 Classes\Vir...

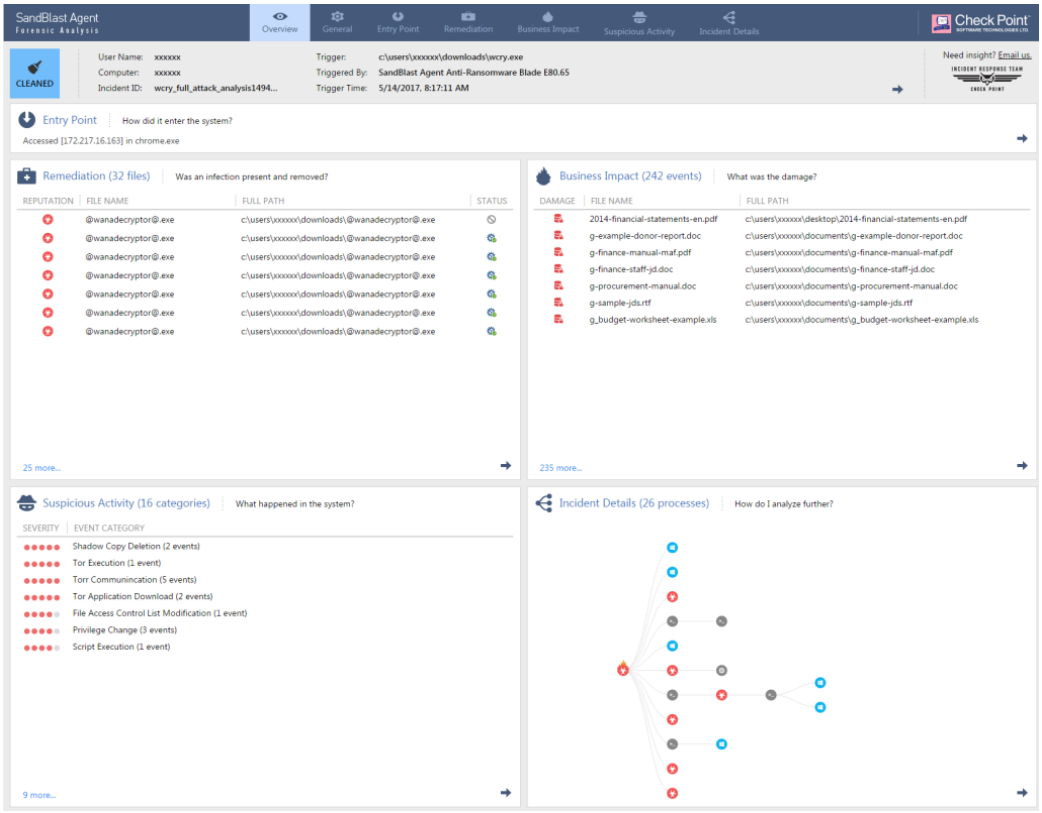
0 Affected Files

0 Files Created | 0 Files Modified | 0 Files Deleted

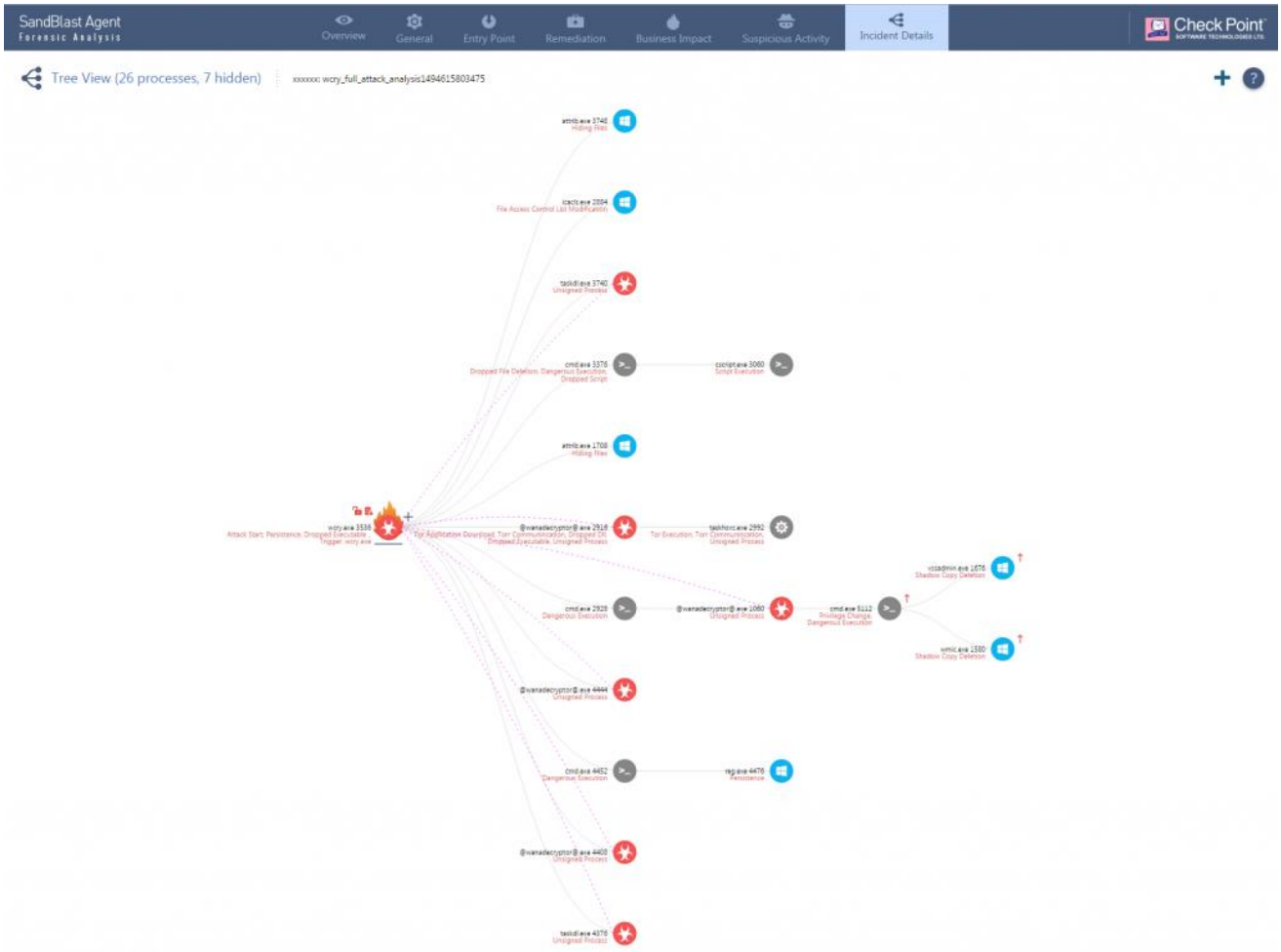
1/6

Check Point SandBlast Agent のフォレンジック機能による活動分析

詳細なオンライン・レポートは http://freports.us.checkpoint.com/wannacryptor2_1/index.html でご覧いただけます。



攻撃ツリー



Check Point Sandblast Agent のアンチランサムウェア機能に観察

ランサムウェアの暗号化とランサムウェア感染をブロックおよび復旧する Sandblast Agent 機能による復旧の動作を動画で紹介します。

推奨される一般的な対策

- Microsoft のセキュリティ情報 MS17-010「Microsoft Windows SMB サーバに対する緊急セキュリティ更新プログラム（4013389）」（https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx）で報告された脆弱性の修正パッチを Windows マシンに適用する
- ネットワークで共有されていない場所にバックアップを保存する
- パスワードで保護された添付ファイルをメール・ゲートウェイでブロックする

チェック・ポイントでは、WannaCry に対する次の保護機能を提供しています。

- **ネットワーク保護機能（SandBlast）**

  Threat Extraction および Threat Emulation

  アンチボット/アンチウイルス

- **エンドポイント保護機能（SandBlast Agent）**

  アンチランサムウェア

  Threat Extraction および Threat Emulation

  アンチボット/アンチウイルス

  アンチマルウェア

- **IPS 保護機能（フラット・ネットワークでは使用不可）**

  Microsoft Windows における、EternalBlue による SMB 経由でのリモート・コード実行
  https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0332.html

  Microsoft Windows における SMB 経由でのリモート・コード実行（MS17-010： CVE-2017-0143）
  https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0177.html

Microsoft Windows における SMB 経由でのリモート・コード実行（MS17-010： CVE-2017-0144）
https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0198.html

Microsoft Windows における SMB 経由でのリモート・コード実行（MS17-010： CVE-2017-0145）
https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0200.html

Microsoft Windows における SMB 経由でのリモート・コード実行（MS17-010： CVE-2017-0146）
https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0203.html

Microsoft Windows における SMB 経由での情報漏洩（MS17-010： CVE-2017-0147）
https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0205.html

チェック・ポイントの Incident Response チームは、WannaCry の動向を注視しつつ、お客様への支援を提供しています。

WannaCry 攻撃キャンペーンの最新情報はチェック・ポイントのブログをご確認ください。

http://www.checkpoint.co.jp/threat-cloud/

http://blog.checkpoint.com/

■チェック･ポイントについて　　WELCOME TO THE FUTURE OF CYBER SECURITY

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（ http://www.checkpoint.co.jp/ ）は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

担当　マーケティング　溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行　共同ピーアール株式会社

担当　花岡・上瀧

Tel: 03- 3571－5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp

