SOFTCAMP

WannaCryランサムウェア
SHIELDEX 無害化処理結果

2017. 06. 02

SoftCamp Co., Ltd.

SOFTCAMP

WannaCryランサムウェア分析概要

2017年5月12日、世界的にWannaCryランサムウェアを利用した大規模サイバー攻撃が発生して多くの企業が被害を受けました。

WannaCryはマイクロソフトWindowsのファイル共有に使われるサーバーメッセージブロック(SMB)遠隔コードの弱点を悪用したもので、Eメール添付ファイルを通じて流布する一般的なランサムウェアとは違い、インターネットネットワークに接続しただけでも感染します。MSではこの弱点を補完するパッチを3月から提供していました。

しかし、WannaCryの流布初期にはドライブバイダウンロード(Drive-by download)方式でもEメール添付を通した古典的な方式で流布したので、いくらパッチを適用したとしても、WannaCryに感染しないと確信することはできません。

このため、ソフトキャンプでは
WannaCryに含まれていた文書ファイルを抽出した後、
シールデックス(SHIELDEX) 無害化技術を通じて
悪性コードの遮断可否を模擬テストしました。

WannaCryランサムウェア文書ファイル分析および無害化結果

❑ 文書ファイル分析

SHA256 ハッシュリスト	
全体	596
収集されたサンプル件数	568
Non-PEファイル	78
.rtfファイル	28

ソフトキャンプはWannaCryファイルで公開されたSHA256ハッシュリスト596件のうち
568件の原本ファイルを収集しました。(95%収集)

収集された原本ファイル568件から78件のNon-PEファイルをスキャンした結果
文書形式で作られた.rtfファイル28件を抽出しました。
.rtfファイルのうち任意で1件を選択して無害化前後の結果を比較してみました。

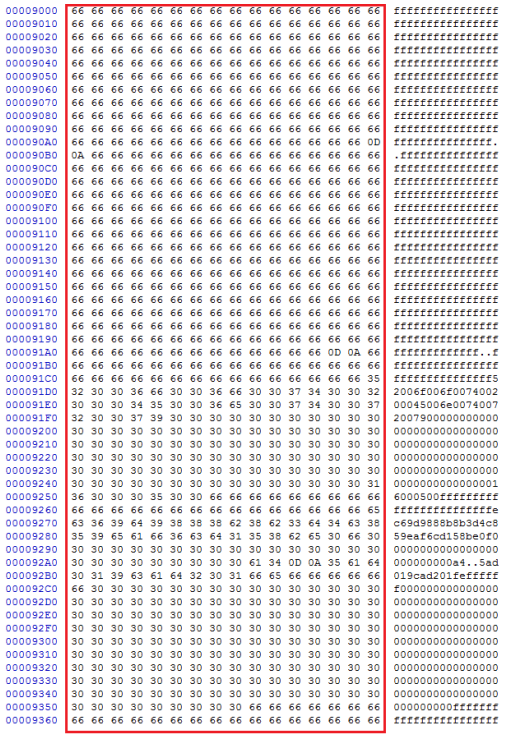
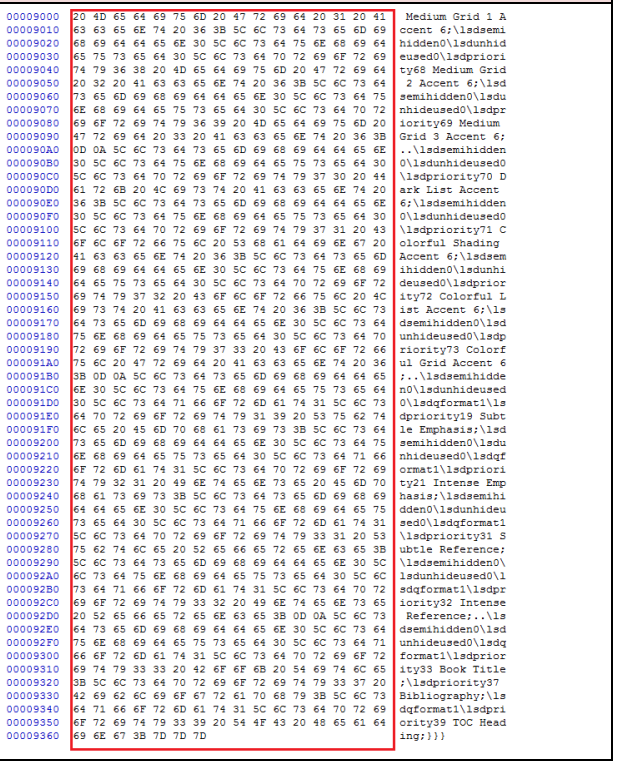
ファイル名	m_vietnamese.rtf
ファイルサイズ	38,377
SHA256	1adfee058b98206cb4fbe1a46d3ed62a11e1dee2c7ff521c1eef7c706e6a700e
機能	WannyCryで使う各国の言語で準備された.rtfファイル28件の中の一つ

❑ 文書ファイル分析結果

▲ バイナリ比較

.rtfファイルの16進数バイナリを無害化前後で比較してみました。/比較アドレス00009000～00009360

無害化前のバイナリでは使用者に不必要なHiddenAttachmentが発見され、
無害化後のバイナリでは悪性コードが挿入されるおそれがあるHidden Attachmentが削除され、使用者に必要なVisible Content(テキスト、イメージ、テンプレート、スタイル、スライドなど)でのみ再構成され、きれいな文書で作られるのを確認することができます。

無害化前のバイナリ結果	無害化後のバイナリ結果
	

▲ VirusTotal比較

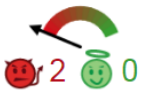
無害化前後のファイルを悪性コード分析サービスであるVirusTotalで比較してみました。

無害化前のファイルをVirusTotalで分析した結果、16件のワクチンから悪性コードが探知されましたが、
無害化後のファイルでは悪性コードが全く発見されないという結果を確認することができました。

無害化前の悪性コード結果

virustotal

SHA256: 1f21838b244c80f8bed6f6977aa8a557b419cf22ba35b1fd4bf0f98989c5bdf8
파일 이름: m_vietnamese.rtf
탐지 비율: 16 / 56
분석 날짜: 2017-05-19 15:23:01 UTC (4일, 17시간 전)



분석 | File detail | 추가 정보 | 댓글 1 | 투표

안티바이러스	결과	업데이트
ESET-NOD32	Win32/Filecoder.WannaCryptor.D	20170519
Tencent	Win32.Trojan.Filecoder.Dxmn	20170519
Ikarus	Trojan.Win32.Filecoder	20170519
Emsisoft	Trojan.GenericKD.5085944 (B)	20170519
Ad-Aware	Trojan.GenericKD.5085944	20170519
BitDefender	Trojan.GenericKD.5085944	20170519
F-Secure	Trojan.GenericKD.5085944	20170519
eScan	Trojan.GenericKD.5085944	20170519
Arcabit	Trojan.Generic.D4D9AF8	20170519
Symantec	Trojan.Gen.7	20170518
TrendMicro	TROJ_RANSOMNOTE.RTF	20170519
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF	20170519
AegisLab	Troj.Ransomnote.Rtf!c	20170519
GData	Script.Trojan.Agent.54KIMR	20170519
Microsoft	Ransom:Win32/WannaCrypt.A!rsm	20170519
Fortinet	Malware_Generic.P0	20170519

無害化後の悪性コード結果

virustotal

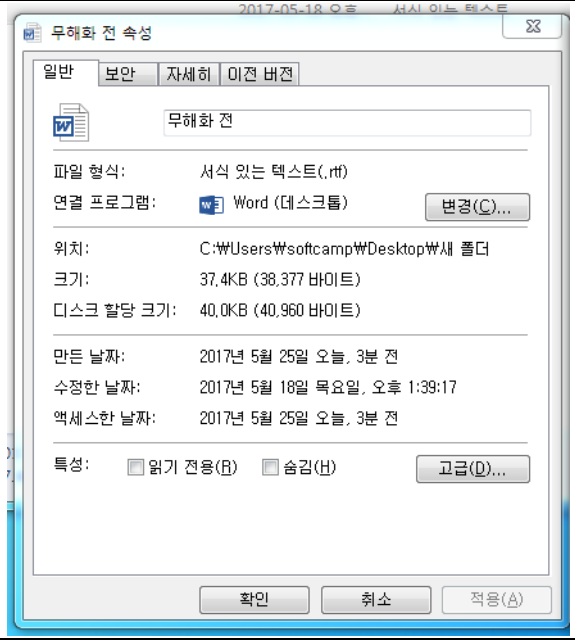
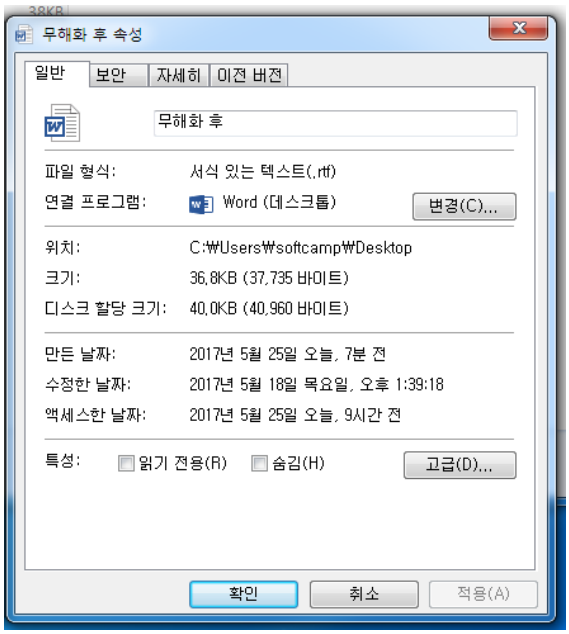
SHA256: 067d50b5bd2c783b8be865f86775199d7bcd34d50e441470ae778cde4c622b2f
파일 이름: 1adfee058b98206cb4fbe1a46d3ed62a11e1dee2c7ff521c1eef7c706e6a700e.rtf
탐지 비율: 0 / 56
분석 날짜: 2017-05-25 00:46:06 UTC (0분 전)

SOFTCAMP

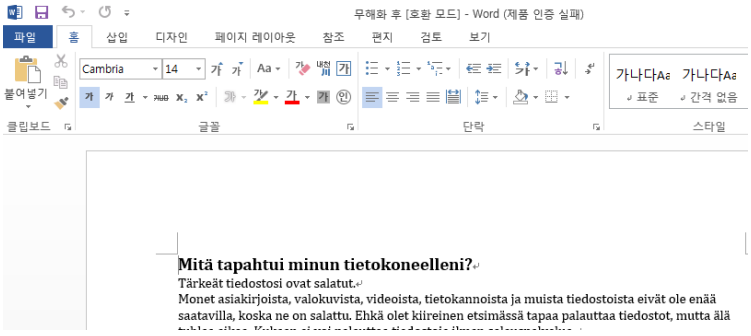
▲ ファイル属性および出力物の比較

無害化前後のファイル属性と出力物の結果を比較してみました。

無害化前、ファイル属性のファイルサイズは37.4KBでしたが、
無害化後、ファイルサイズは36.8KBで0.6KB容量が減りました。
これは、無害化技術を通じて使用者に悪影響を及ぼすおそれがある不必要なコードを除去したからです。

無害化前のファイル属性	無害化後のファイル属性
	

無害化技術で不必要なコードを除去しましたが、出力結果は無害化前と同じように不便なく確認することができます。

無害化前後の同じ出力結果


SOFTCAMP

WannaCryランサムウェア対応ソリューションSHIELDEX

ソフトキャンプ 無害化ソリューションシールデックス(SIHELDEX)は
無害化技術を基盤として外部から流入する文書ファイルによるランサムウェアの攻撃に対応できるソリューションです。

シールデックスは網が分離した環境でインターネット、Eメール、USB、網間の資料転送など
多様な外部経路を通じて流入するすべての文書ファイルを無害化技術で無害化した後、再構成する方式で
安全なコンテンツだけ内部に送るので、悪性コードを含めた外部流入ファイルが
システムの重要領域にアクセスできないように基本的に遮断します。

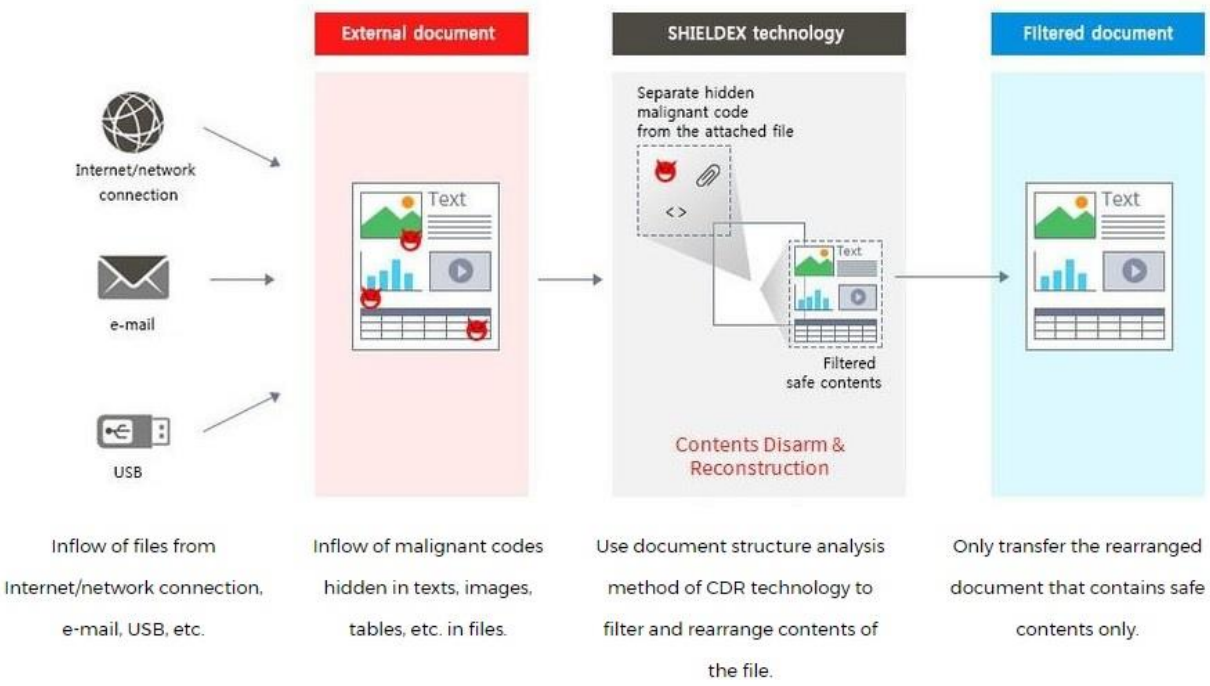
すなわち、文書ファイルに構成されたコンテンツのテキスト、図形、図、表などに対するすべての構成要素の構造を検査した後、承認された要素だけ抽出してファイルを再構成する方式です。

このように再構成されたファイルは原本ファイルそのままの形式できれいで安全なコンテンツだけで構成されたファイルに再誕生するので、ランサムウェアに徹底して対応できます。

❑ SHIELDEX情報

・SHIELDEXCDR/ファイル無害化無料体験

❑ SHIELDEXコンセプト



SOFTCAMP

❑ SHIELDEXの特徴

網分離環境に最適化され、網分離セキュリティ強化
網分離環境で主な経路を通じて流入する外部流入ファイルを無害化して
安全なファイルに再構成

既存セキュリティ方式の限界点を補完
無害化技術で文書構造分析方式を通じて既存ソリューションが探知できない
文書ファイル形態の悪性コードに対応

内部情報流出防止、ランサムウェア対応
無害化技術で悪性ファイルを防いで安全なファイルを内部に流通、
悪性コードによるセキュリティの脅威を根本的に遮断

❑ SHIELDEXの適用対象

網分離環境でファイル無害化に対するセキュリティ強化を考慮している組織

APT、ランサムウェアなどサイバー脅威に対する対応方案を考慮している組織

Zero Dayなど知られていない攻撃に対する強化されたセキュリティ対策の構築が必要な組織