IIJ Technical Week 2016 - Day 3 (2016/11/11) Windowsにおけるマルウェアの 痕跡確認と防護手法のご紹介



株式会社インターネットイニシアティブ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター アナリスト 六田 佳祐

Ongoing Innovation



Internet Initiative Japan

© 2016 Internet Initiative Japan Inc.

本日の内容



1. はじめに 本セッションの概要をお話しします

- 2. 攻撃の例 どのようにしてマルウェア感染が発生するか、お話しします
- マルウェアの痕跡確認
 実行されたマルウェアが端末上に残す記録を確認する方法をお話しします
- 防護手法の例
 感染が発生し辛くなるよう、護る方法をお話しします
- 5. まとめ

1. はじめに

© 2016 Internet Initiative Japan Inc.

自己紹介



名前

- 六田 佳祐 (むだ けいすけ)

所属

- セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター

• **<u>IIJ C-SOCサービス</u>はじめます**

• アナリスト

- セキュリティデバイスが検知したイベントの真偽確認・通知
- セキュリティ関係のトレンド調査

IIJ C-SOCサービス



- 10月31日発表、2017年3月提供開始
 - IIJ運用機器・お客様運用機器から送信されるログを収集・分析
 - 機器単体のセキュリティログでは検知出来ない、 セキュリティインシデントを検知
 - アナリストがインシデントの重大度を判断し、 適切な通知や対処を実施
 - レピュテーションデータや独自シグネチャを適用し、
 脅威からの迅速な防御を実施

- セキュリティオペレーションセンター
 2017年3月 見学ツアー開始予定
- 詳しくは担当営業へお問い合わせ頂くか、 IIJ Webサイトをご覧ください

 http://www.iij.ad.jp/wizsafe/





- IIJには、お客様から検体をお預かりして調査するサービスは、 現時点ではご提供しておりません
- 一方で、観測情報やサービスに関連する情報から、マルウェアを調査する ことはあります
 - 調査の結果は、IIJサービスにフィードバックされることがあります
 - 調査で見つかった事象は、一般公開することがあります
 - Internet Infrastructure Review (IIR) http://www.iij.ad.jp/company/development/report/iir/
 - IIJ-SECT https://sect.iij.ad.jp/
- このセッションでは、感染時における調査に役立つ設定をいくつか紹介 すると共に、感染する確率を下げる手法を紹介します





- セキュリティに「絶対」はありません
 - 本セッションの内容を実施したからと言って、マルウェアに感染しなくなったり、
 確実に証拠を保全出来るものではありません
- 本セッションの内容は、2016年11月11日時点のものです
 - トレンドは常時変化します
 - 最新の情報を追いかけるように心掛けてください
- 本セッションは、Windows 10 Pro環境(x86/x86-64)を想定しています
 - バージョンやエディションが異なると、一部設定方法が異なる場合があります
 - Windows 10 (無印) では、グループポリシーが使用出来ません
 - Linux、Unix、Mac OS、他スマートデバイス(Windows 10 Mobile・IoTを含む)
 などは、本セッションでは触れません
 - 同様の機能が存在する項目もありますので、探してみてください

2. 攻撃の例

© 2016 Internet Initiative Japan Inc.





コンピュータ上で動作する不正(malicious)なソフトウェア
最近の攻撃・マルウェア例

挙動	事例	ツール例
特定のタイミングに、特定のサイト に対して大量のトラフィックを送信	米セキュリティ情報サイトに対する、 1TbpsのDDoS攻撃 (2016/9)	Mirai (bot)
特定のホストを踏み台とし、他のホ ストに通信させる	JTB社の情報流出 (2016/5)	PlugX(RAT: Remote Access Tool)
ファイルを開けないようにし、金銭 を要求する	米ロサンゼルスの病院における、 電子カルテなどの暗号化 (2016/2)	Locky (ランサムウェア)
Alexa a general contract of a general contex of a general contract on general contract on general contrac	(■・ DemoUser + マイビクチャ Superator S	ンサムウェア)の感染例





- 前項に記載の、RATを使用した例
 - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
 - それを開いたクライアント端末が感染し、RATが実行される
 - RAT経由で端末を操作し、他のホスト上にある情報を奪取する







- 前項に記載の、RATを使用した例
 - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
 - それを開いたクライアント端末が感染し、RATが実行される
 - RAT経由で端末を操作し、他のホスト上にある情報を奪取する







- 前項に記載の、RATを使用した例
 - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
 - それを開いたクライアント端末が感染し、RATが実行される
 - RAT経由で端末を操作し、他のホスト上にある情報を奪取する







- 前項に記載の、RATを使用した例
 - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
 - それを開いたクライアント端末が感染し、RATが実行される
 - RAT経由で端末を操作し、他のホスト上にある情報を奪取する







- 送信者が<u>正しく見えた</u>
 - メールの送信元(From)アドレスは、簡単に<u>偽装が可能</u>
 - 本文も**本物のよう**に見えた
 - 片言の日本語ではなく、社内メールに見える
- 添付ファイルも一見すると、正しいファイルに見える
 実は見え辛い位置に本当の拡張子があった



- ファイルサーバにアクセスしたのは、社内の正規アカウント
 - 攻撃者の存在は、ファイルサーバ側には見えない
 - ファイルサーバのアクセスログがあっても、「日時」「ファイ
 ル」「端末」は割り出せるが、具体的な攻撃元は分からない







- ウイルス対策ソフト
- パーソナルファイアウォール
- ソフトウェアの更新
- いずれも、現在でも一定の効果がある
- しかし・・・

証跡の取得

 \bullet



- 残念ながら、マルウェアに<u>絶対に</u>感染しない、ということはあり得ない
 - ウイルスの亜種
 - 挙動やシグネチャが異なり、パターンファイルでは検出不可
 - ヒューリスティック機能で検知出来る場合もあるが、完全ではない
 - ファイアウォールとしては正常に見える通信:ポリシ上は通信を許可
 - 443/tcp (HTTPS) を用いたトンネル通信
 - 53/udp (DNS) を用いたリモート制御
 - 未発見の脆弱性
 - 感染した場合に、「何が起こったのか」を把握出来るようにしたい
 - 影響範囲を知り、復旧作業の内容を策定
 - 関係者への説明時に、経緯や影響を明確に説明
 - 同様の事象が発生しないように対策

3. マルウェアの痕跡確認





- マルウェアに限らず、アプリケーションを実行すると<u>痕跡</u>が残る
 - アクセスログ
 - ファイル
 - ・ レジストリ
 - ネットワーク実行ログ
 - etc...
- Windowsの標準機能でも、ある程度は確認可能
 - しかし、初期設定のままでは確認出来ないことが多い
 - 予め、確認出来るように設定しておくことが必要
 - 設定には、Administrator権限が必要

痕跡の取得例



- マルウェアが参照したファイル・レジストリ
- ネットワークアクセスの痕跡
- マルウェアの実行
- これらをWindowsのイベントログを用いて記録する方法をご紹介
 殆どは追加のソフトウェアを必要とせず、設定すれば利用可能

4-7-1	日付と時刻			イベントロ	タスクのカテゴリ	^	操作
0、成功の起来	2016/11/11 14:17:03		Microsoft Windows security audi-	4589	プロセス終了	10	セキュリティ
9. 成功の監察	3016/11/11 14:17:0	l.	Microsoft Windows security audi-	4583	- プロセス作成		() 供存されたログを集
冬点初の監査	2016/11/11 14:17:01	1	Microsoft Windows security audi	4688	プロセス作成	~	7 1796 Ka-011
イベト 4588, Microsoft	Windows security auditme.					×	カスタムビューのイン
2.82 1518							口グの消去
						- 5	▼ 液布の07€248
1042148						^	TO/TRA
新しいプロ	27. ID 0x 1550						(0) mm
新しいプロ	27.名 Ol/UsersVOwnerVino/epade						D anna main
トークン集合	MORE BAX1937						H AVCOANTIE
(1成元70	也2.1D Bad8	ringh Handalory Lev					200919298
1ERDETDETAS CHWIndowsWojstend3Wondew						表示	
70122.00	マンドライン: "OWUsersWOwne	r¥notepad.exe*					@ 最新の情報に更
トーの人格の理論の	ニューザー アカウント制度ポリシーには	って新しいプロセスに事	即っるてられたトークンの種類を示します。				NJ.7
1655 1 (2. 15 Balla)	「ほされていない、またはグループが展分	CARTINES 76 F	トーケッデオ、フルトーケンは、フーザー アカケットを回転が開始の場合、また	17-H-NHA33.3.04	日本教 アナイア・トネトはサードス アナイア・トである		(R)1-4688, Micros
場合にのみ使用され	tt.						E 46060000
5688 1/7 15 89 100	READ TO DO LABOR DO LABORA	CONTRACTOR AND ADDRESS	TALLA OF BRIDEL M/1 3-4- DWY LEINNESS	780 1-H-M2384			1 104KUN-92
る場合に使用されます	。鼻垢されたトーウンは、アプリケーショ	が常に管理者特権を	を要求するか、または常に最高の特徴を要求するように構成され、ユーザー	が管理者ブループのよいパ	ーである場合にも使用されます。	-	Bo Wa
							ET also succes
05032000	1140-110-						tel anochore
V-205	Microsoft Windows securit	< n50E(00)	2016/11/11 14:12:03				B MROWACE
15/1 100	4581	42/08/19/09	2 70/2/085				2 ∧1k7
L-SALD	1885	#-7-500	\$13/04EW				
7-9-(0)	N/A	T-P1-b-(R)	DESKTOP-MEPHLSE				
#/C3-15(0)	1846						
Triesallyn	(AC de DATION BY						

ファイルアクセスのログ



- マルウェアが参照したり、作業フォルダに書き込んだりしたファイルを 記録すれば、使用されたツールや狙われた情報が分かるかもしれない
- NTFSには、ファイルアクセスに対する<u>監査</u>機能がある
 NTFS: Windows標準で使用されているファイルシステム
- 2か所を設定する

 ファイルのSACL
 Everyoneに 対して設定
 監査ポリシー



監査ポリシーの有効化



SACLを有効化した状態で「オブジェクトアクセスの監査」を設定すると、 イベントログの「セキュリティ」ログにアクセスログが記録



設定すると、他にWindowsフィルタリングプラットフォーム(Windows ファイアウォール)やファイル共有なども監査されるようになる
 – ファイルアクセスのみに絞りたい場合は、「詳細な構成」から





B レジストリ エディター

× - JYK2-9-

ファイル(F) 編集(E) 表示(V) お気に入り(A) ヘルプ(H)

展開する

新規(N)

検索(F)...

名前の変更(R) エクスポート(E)

アクセス許可(P). キー名のコピー(C)

HKEY_CLASSES_ROOT

HKEY CURRENIT LICED

HKEY_LOCAL

HKEY_USERS

HKEY CURRE

名前

ab)(既定)

レジストリエディタでSACLを設定し、「オブジェクトアクセスの監査」 を設定することで、監査が可能

- 詳細構成で「レジストリの監査」を設定しても良い

オブジェクト: オブジェクト名: オブジェクト値名: ハンドル ID: 操作の種類:	¥REQISTRY¥USER¥S-1-5-21- rundII92.exe 0x8cc 既存のレジストリの値が変更されました	- 100 1¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
プロセス情報 プロセス ID: プロセス名:	0x1018 C¥Windows¥regeditexe	
変更情報: 古い値の種類: 古い値: 新しい値の種類: 新しい値:	REG_SZ REG_SZ C#Windows¥System32¥rundIll32 <i>ex</i> e	

レジストリのキーを右クリックし、「アクセス許可」 から設定

- 予めレジストリの構造や、作業時のリスクを理解すること
- ファイルアクセスと同様に、読み取りに対して設定すると、

 膨大な量のログが記録されるため、注意が必要

監査対象の選定



- 「<u>読み取り</u>」を監査すると、<u>ログ量が膨大</u>になる
 - アプリケーションのDLL呼び出しが監査される場合も
 一方で、欲しい監査ログは「読み取り」である場合も多い
- 「読み取られた」ことを知りたければ、「<u>成功</u>」を監査すれば良い
 一方で、全てのアクティビティを記録したい場合は、「成功および失敗」
 - 「何でも取る」は<u>必ずしも良いとは</u> <u>限らない</u>

高度なアクセス許可: □ フル コントロール	
 フォルダーのスキャン/ファイルの実行 フォルダーの一覧/データの読み取り 属性の読み取り 拡張属性の読み取り ファイルの作成/データの書き込み フォルダーの作成/データの追加 	 □ 属性の書き込み □ 拡張属性の書き込み □ サブフォルダーとファイルの削除 □ 削除 ☑ アクセス許可の読み取り □ アクセス許可の変更
and the second	□所有権の取得

ネットワークアクセスのログ



- 「オブジェクトアクセスの監査」(一括設定時)又は「Windowsフィル タリングプラットフォームの監査」(詳細な構成時)を設定
 - Windowsフィルタリングプラットフォーム: Windowsファイアウォールなどで使用されて いる、パケットフィルタのAPI
 - Windowsフィルタリングプラットフォーム
 を使用しない場合は効果無し
 - パーソナルファイアウォールソフトウェア のログで代替
 - 追加ユーティリティの使用(後述)

イベント 5156, Microsoft Windows security auditing.						
全般 詳細						
アプリケーション情報						
7027 ID:	4					
アフリケーション名: System						
ネットワーク情報:						
方向:	送信					
送信元アドレス:	10.0.2.15					
ソース ポート:	8					
宛先アドレス:	10.0.2.2					
宛先ポート	0					
1 לעבאסל						
フィルター情報:						
フィルターの実行時 ID:	81493					
レイヤー名:	接続					
レイヤーの実行時 ID:	48					

プロセスの監査



- 実行ファイル (exe) が起動・終了したことを記録
 - 通常はインストールしていない実行ファイルが起動されると、端末上で不正な
 処理がされた可能性がある
- 「プロセス追跡の監査」を有効化することで、イベントログに記録される ようになる

へいト 41	Microsoft Windows security auditing.
全般	
プロセ	編 振しパクロセス ID: 0.xaf8 新しいプロセス名: C-¥Windows¥System32¥notepad.exe トークン昇格の種類 XX1938 必須ラベル: Mandatory Label¥Medium Mandatory Level 客成元プロセス ID: 0.xa60 客成元プロセスA: C-¥Windows¥System32¥cmd.exe ガルセスのロマンドライン:
トーク	各の種類類は、ユーザー アカウント制御ボリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。
種類 使用約	特権が削除されていない、またはグループが無効にされていない、フル トーケンです。フル トーケンは、ユーザー アカウント制御が無効の場合、またはユーザーが組み込みの管理者アカウントまたはサービス アカウントである場合にのみ す。
種類使用的	特権が所順なれていない、またはグループが無効にされていない、昇格されたトークンです。昇格されたトークンは、ユーザー アカウント制御が有効であり、ユーザーが管理者として実行してプログラムを起動することを選択する場合に す。昇格されたトークンは、アプリケーションが常に管理者特権を要求するか、または常に最高の特権を要求するように構成され、ユーザーが管理者グループのメンバーである場合にも使用されます。
種類	管理者特権が可能なれ、管理グループが無効にされた、制限されたトークンです。制限されたトークンは、ユーザーアカウント制御が有効で、アプリケーションが管理者特権を要求せず、ユーザーが管理者として実行してプログラムを

プロセス監査から分かること



- 日時 •
- 実行ユーザ
- プロセスID
- プロセス名

権限 \bullet

新しいプロセス ID: 0xaf8 新しいプロセス名: C:¥Windows¥System32¥notepad.exe トークン昇格の種類:%%1938 必須ラベル Mandatory Label¥Medium Mandatory Level 作成元プロセス ID: 0xa60 作成元プロセス名: C:¥Windows¥System32¥cmd.exe プロセスのコマンド ライン:

- UAC有効環境では、「管理者権限が必要」 な場合に「昇格」する
 - トークン昇格
 - 必須ラベル
- 呼び出し元プロセス \bullet







• 単に「プロセス追跡の監査」を設定するだけでは、実行されたexe ファイルと、付随情報が分かるのみ

C:¥Windows¥PSEXEC.EXE





単に「プロセス追跡の監査」を設定するだけでは、実行されたexe
ファイルと、付随情報が分かるのみ

C: ¥Windows ¥PSEXEC. EXE



• 実行内容を知りたい

C:¥Windows¥PSEXEC.EXE **¥¥target_host net use ¥¥fileserver¥share**

コマンドラインを記録



• グループポリシ

- 「コンピューターの構成」→「管理用テンプレート」
 →「システム」→「プロセス作成の監査」
 - →「プロセス作成イベントにコマンドラインを含める」
 - Windows 8.1 · Windows Server 2012 R2以降で有効
 - KB3004375 をインストールすると、Windows 7・8、Windows Server 2008R2・2012でも設定可能

プロセス情報:

新しいプロセス ID: 0x11d4 新しいプロセス名: C:¥Windows¥System32¥notepad.exe トークン昇格の種類:%%1938 必須ラベル: Mandatory Label¥Medium Mandatory Level 作成元プロセス ID: 0xa60 作成元プロセス名: C:¥Windows¥System32¥cmd.exe プロセスのコマンド ライン: notepad foo.txt

追加ツールを使う



- Sysmon (SYStem MONitor)
 - Windows Sysinternals
 - https://technet.microsoft.com/en-us/sysinternals/sysmon
 - Windows 7・Windows Server 2012以降で利用可能
- 記録可能な情報
 - レジストリは、Sysmonでは記録不可

イベント ID	項目		イベント ID	項目
1	プロセス作成	8	7	イメージ呼び出し
2	ファイル作成日時の変更	2	8	リモートスレッドの実行
3	ネットワーク接続		9	ディスクのRAW読み出し
4	Sysmonサービスの状態変更	3	10	プロセスアクセス
5	プロセス終了	Ē	255	Sysmonのエラー
6	ドライバ読み込み			

監査ログから見つけられる事象の例(注:いずれも可能性)



- ファイルサーバ上のファイルが、ローカルディスクにコピーされていた
 攻撃者が当該端末でファイルをまとめ、一括してアップロードする可能性
- 他端末や、インターネット上のホストへの通信が記録されていた
 クライアント同士の通信の場合、攻撃者が他ホストにも侵入した可能性
 インターネット上のホストである場合、それが攻撃者のホストである可能性
- インストールしていない実行ファイルが起動した
 攻撃に使用された実行ファイルである可能性
- 自動起動の設定
 - 何度でも侵入可能とするよう、RATを常時起動するよう設定した可能性

ログの消去

•



- ログ容量には上限がある 金段 フルネーム(F) - クライアントOSの初期設定は20MB こちのパス(し): ログのサイズ: 在成日時: - 超過すると、古い方から上書きされる 更新日時: アクセス日時 ログを有効にする(E) • 攻撃者はログを消去する キーワード 日付と時刻 ソース イベント ... タスクのカテゴリ 🔍 成功の監査 2016/11/07 13:11:12 1102 ログの消去 Eventlog
 - 取得する設定をしても、消去されると意味が無い
- ログのプロパティ・セキュリティ(憧晰: 管理) Security %SystemRoot%#System32#Winevt#Logs#Security.evb 20.00 MB(20,975,616 /C+F 2016年8月3日 8:38:25 2016年11月9日 8:57:42 2016年8月3日 8:38:25 最大ログ サイズ (KR)(X) 20480 -イベント ログ サイズが最大価に達したとき 必要に応じてイベントを上書きする(最も古いイベントから)(W) ○ イベントを上書きしないでログをアーカイブする (A) ○ イベントを上書きしない (ログは手動で消去)(N) ログの過去(P

OK

キャンセル

- ログを外部転送するなど、消去されないように対策することを推奨 - 転送しておくと、ホスト上で消去されてもログが残る
 - 当然、ログ収集ホストの権限を奪取されないことが前提
 - 例: https://technet.microsoft.com/ja-jp/library/cc748890(v=ws.11).aspx

調査とアンチウイルスソフトウェア



- とりあえずウイルススキャン?
 - 感染が発見された際によく聞くフレーズ
 - 「とにかく消去したい」場合は有効

調査とアンチウイルスソフトウェア



- とりあえずウイルススキャン?
 - 感染が発見された際によく聞くフレーズ
 - 「**とにかく消去したい**」場合は有効
- 調査を目的としている場合、適切でない場合もある
 - ウイルススキャナがファイルシステムにアクセスし、「読み取り」のログで
 <u>監査ログが埋まってしまった</u>
 - 調査したいファイルが、<u>検疫により削除</u>されてしまった
- 調査をしたい場合、<u>電源は起動したままネットワークケーブルを抜く</u>
 調査する場合も、他端末に対する感染のリスクは避けるべき
- 状況に合わせて<u>適切に判断</u>すること
 - 「調査するより止めることが先決」という状況もあるかもしれない

4. 防護手法の例

よくある感染例



- スクリプトを実行した
- 正規アプリケーションから不正な呼び出しが発生した
- こういったものを実行しないようにすると、リスクを低減出来る

注意

- 下記に示すような一般的な対策は、既に実施していることを前提とする
 - アンチウイルスの使用
 - パーソナルファイアウォールの使用
 - ソフトウェアの更新を実施
 - バックアップの取得
 - 不要アカウント・不要アプリケーションの削除

Windows Script Host

- Windowsで古くから使用されているスクリプティング手法
 - VBScript: Visual Basic記法
 - Jscript: JavaScript記法



wizSafe

- 使用しない場合は、レジストリで無効化出来る
 <u>- コンピュータ上の全ユーザ</u>
 - HKLM¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled
 現在のユーザのみ
 - HKCU¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled
 それぞれ上記のDWORD値を作成し、"0"を設定
- ログオン・ログオフスクリプトで使用している場合、動かなくなるため注意

Windows Script Host

Windows Script Host へのアクセスがこのコンピュータ上で無効にされています。 詳細については、管理者に連絡してください。

OK

 \times

PowerShell



- 比較的新しいWindowsのコマンド操作機構
 - Windowsの様々な情報を取得・設定可能



 Windows PowerShell

 Windows PowerShell

 Copyright (C) 2018 Microsoft Corporation. All rights reserved.

 PS C:#Users#Dwner> Get=WmiObject -Class Win32_UserAccount

 AccountType : 512

 Caption : DESKTOP-M4PML55#Administrator

 Domain : DESKTOP-M4PML55

 SID : S-1-5-21

 FullName : Administrator

 Name : Administrator

 AccountType : 512

初期設定では、スクリプト実行が許可されていない
 しかし、レジストリ値を1つ変更すると実行可能

Windows PowerShell	~
copyright (c) 2016 Microsoft Corporation. All rights reserved.	
PS C:¥Users¥Owner〉Desktop¥test.ps1 Desktop¥test.ps1 : このシステムではスクリプトの実行が無効になっているため、ファイル C:¥Users¥Owner¥Desktop¥test.ps1 ? 活み込むことができません。詳細こついては、「about_Execution_Policies」(http://go.microsoft.com/fwlink/?LinkID=195170) 発生場所 行:1 文字:1	

PowerShellの監査



- PowerShell v5では、実行したコマンドと出力の記録が可能
 - Windows Management Framework 5.0 に含まれる
 - Windows 10では標準搭載
 - Windows 8.1・7やServer 2012/R2・2008R2では個別にインストールが必要 https://www.microsoft.com/en-us/download/details.aspx?id=50395

• グループポリシー

- (コンピューター|ユーザー)の構成¥管理用テンプレート¥Windowsコンポー ネント¥Windows PowerShell¥PowerShellトランスクリプションを有効にす る
- 既定では「ドキュメント」フォルダに作成される
 - 攻撃者により削除される可能性はあるが・・・

特定のexeファイルを実行しない



• グループポリシ

- 「ユーザーの構成」→「管理用テンプレート」→「システム
 →「指定されたWindowsアプリケーションを実行しない」
 - 実行すると、下記ダイアログが表示される



「指定されたWindowsアプリケーションだけを実行する」というポリシもあるが、以下のような場合は回避が可能

- コマンドプロンプトから実行
- 正規のファイル名と同じ名前に変更(パスを含めた場合はこの限りではない)

攻撃を知る(管理者向け)



- 全ての攻撃手法を把握することは不可能だが、一定数を知っておくことは可能
- よく使用されるツールの例
 - PSEXEC (Sysinternals)
 - Windowsリモートシェル(WinRS)
 - リモートデスクトップ
 - 特徴的なログが記録される
 - PSEXEC: <u>システムサービス</u>(PSEXESVC) <u>のインストール・削除</u>
 - WinRS: Windows Management Instrument (WMI)の実行
 - リモートデスクトップ: **専用のログ**が存在
 - PSEXEC・WinRSはコマンドラインオプションに実行プログラムを指定するため、 コマンドラインを含めたログを取得していれば記録可能
- 上記は全て、<u>ツール自体は正規</u>のもの
 - 「システム上で使用しているかどうか」が判断基準の1つ
- システムの「定常」を知っておくことが必要

攻撃を知る(一般利用者向け)



- 機械的に制御することと併せて、ユーザにも一定の知識が必要
- 例えば・・・
 - メールのFromは**詐称可能**
 - UACで、<u>意図しない権限昇格</u>を許可しない
 - 手動で実行したなら意図したもののはず
 - ユーザが何も実行していないのに表示された場合、
 不正な処理を目的したものである可能性がある
 - 何も考えずに「はい」とは言わない
 - アイコン・ファイル名と中身が一致するとは限らない
 - Wordファイルのアイコンを用いた実行ファイル
 - ファイル名の偽装 (RLOなど)
 - グループポリシで制限可

Authentication-Results: mx.example.jp; spf=fail smtp.mailfrom=notreal@example.jp; dkim=none; dkim-adsp=unknown header.from=notreal@example.jp; dmarc=fail header.from=notreal@example.jp; x-country-code=JP

ユーザーアカウンド制度 このアプリがデバイスに言 か?	× で更を加えることを許可します	
Windows コマン 確認済みの発行元 Microso 詳細を表示 出い	くプロセッサ ft Windows しいえ	
i dummy₁テパロ	プのexe.docx	×
全般 互換性	セキュリティ 詳細 以前のバージョン	
w	dummyexe.docx	
ファ <mark>イル</mark> の種類:	アプリケーション (.exe)	

他にも



- Internet Infrastructure Review (IIR) では、他の対策も • 紹介しています http://www.iij.ad.jp/company/development/report/iir/ Vol.31 第1.4.2節 Vol.32 第1.4.2節 マルウェアに感染しないため Windowsクライアント専業 加速するトラフィック増加 アプリケーションホワイトリスティング • EMET ソフトウェア駆動型 • AppLocker (Enterprise向け) UACの厳格化 • ソフトウェアの制限ポリシー(SRP) WSHの 無効化 • 制限回避の脆弱性 rundll32.exe、regsvr32.exeの通信の禁止 • WinSxSフォルダ PowerShellの禁止 • 管理者権限の制限 HTAの禁止 Webブラウザのプラグインを自動実行させない マッシュアップコンテンツを制限 ストアアプリの禁止
 - 他にも、技術トレンドなどを掲載しております

5. まとめ

© 2016 Internet Initiative Japan Inc.





- 最近の攻撃は身近な場所で、気付かない形で発生する
 「一見正しく見える」ことが特徴
- マルウェアの実行を追跡出来るようにしておくことで、万一感染があって も経緯を追いかけることが可能
 - 感染しないことが一番だが、感染した場合の情報源となる
- 標準設定のWindowsには、強化出来る点が沢山ある
 対策可能な項目を知り、業務影響の無い範囲で強化することが必要
- セキュリティに<u>絶対は無い</u>
 - トレンドを追いかけることが必要





ご清聴ありがとうございました

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及 び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標また は登録商標です。本文中では™、®マークは表示しておりません。©2016 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及 び本書に記載されている事柄は、将来予告なしに変更することがあります。