2017年6月

McAfee
Together is power.

脅威レポート

McAfee Labs

マルウェアが利用する回避技術とその傾向

回避技術は広く利用され、より強力になっています。

回避技術の進化

1980年
Cascadeウイルス
暗号化でコンテンツを判読不能にする最初のウイルス

1990年
Chameleon ファミリー ウイルス
最初のポリモーフィック型ウイルス

1998年
メタモーフィック型マルウェア
Regswapが同じ機能に異なるレジスターを使用

1990年代
パッカー
RAM/ディスクの消費を少なくするため、パッカーで暗号化や圧縮が行われる

1999年～2003年
ルートキット
1999年に最初のWindowsルートキットのNTRootkitが出現
2003年にはHackerDefenderが出現

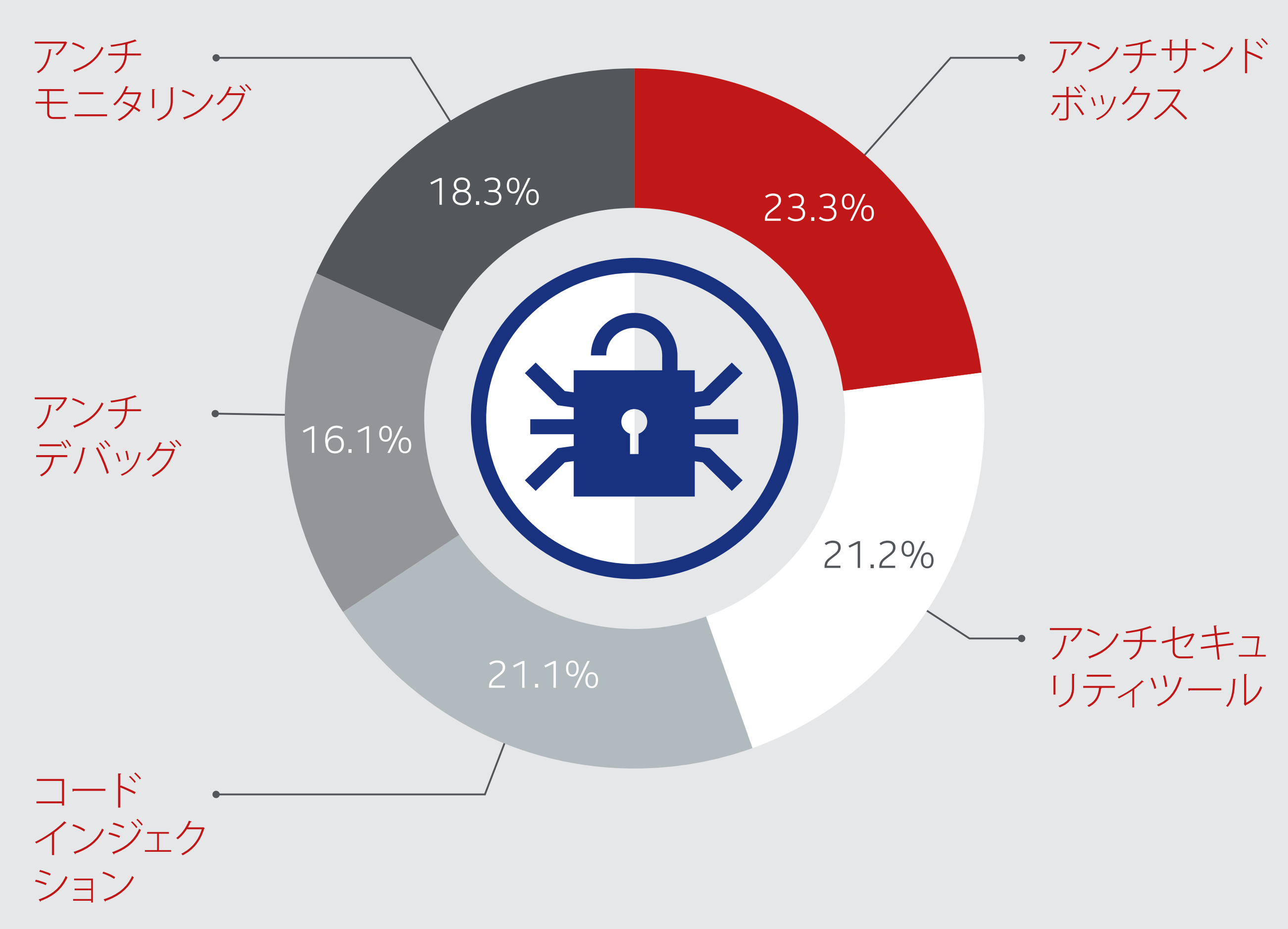
2008年
ドメイン生成アルゴリズム
ConfickerワームがDGAを使用してネットワークでの検出を回避

2011年
販売マーケット
検出回避製品/サービスを提供する最初の闇マーケット（Silkroad）が出現

2015年～2017年
Dridex、Locky
最初の大規模な難読化
PowerShellの利用
サンドボックス回避

2015年～2017年
ファームウェア マルウェア
Equation GroupとHacking Teamが検出困難なファームウェアマルウェアの存在を公開

マルウェアが利用する検出回避技術



検出回避
すぐに利用できるコードが売られている。無料のもある。

ファームウェア
回避技術としてファームウェア感染が増加している。

アンチセキュリティツール
機械学習による検知を回避するため、新しい手法が開発されている。

普通の場所が一番目立たない: ステガノグラフィーに潜む脅威

ステガノグラフィーは情報を隠すための技術です。

デジタル ステガノグラフィーのプロセス

1. カバー ファイル、隠れたメッセージ
2. 埋め込み アルゴリズム
3. ステガノグラフィー ファイル
4. 通信媒体
5. ステガノグラフィー ファイル
6. 抽出アルゴリズム
7. 隠れたメッセージ

マルウェアが潜むデジタル ステガノグラフィー

2010年 | 2012年 | 2014年 | 2016年

- Duqu、Shady RAT、Alureonルートキット
- Zbot、Lurk、ZeusVM、MiniDuke、CosmicDuke
- Vawtrak、Stegoloader、Sundown、AdGholas、Magento CC、DNSChanger

秘密のメッセージ
ステガノグラフィーは正規に見えるメッセージに秘密を隠す。

紀元前440年
ステガノグラフィーの起源は古く、紀元前440年まで遡る。

2011年
ステガノグラフィーを最初に使用したマルウェアは2011年に見つかったDuqu。

ネットワーク
新しいステガノグラフィーとして、ネットワークを利用する攻撃が出現した。

パスワードを盗み出すFareitの脅威が増している

ほとんどの高度な持続型攻撃では、攻撃の早い段階でパスワードを盗み出しています。2016年の民主党全国委員会の情報漏えい事件にFareitが関係している可能性があります。

Fareitの進化

2011年
- 認証情報の盗用機能とDDoS機能を搭載したFareitの最初の亜種

2012年
- BHEKがZeus、FakeAVと一緒にFareitを散布
- FareitがMedfos、Nymaimをダウンロードし、スパムで拡散

2013年
- ビットコイン マイニングを開始
- Pony Loader 1.9のソースコードが流出
- 画面をロックするランサムウェアがFareitで認証情報を窃盗

2014年
- ビットコイン ウォレットを盗み出すPony Loader 2.0
- FareitがDNSポイズニングで拡散

2015年
- Pony Loader 2.0のソースコードが流出
- Onion DukeとDNC攻撃
- Fareitの認証情報窃盗モジュールをStegoloaderが利用

2016年
- FareitがW97、PowerShell、JavaScript、MHTで拡散
- Grizzly Steppe作戦にFareitが関与

2017年
- カスタマイズされたPony Loaderの亜種が出現（Pony Loader 2.2まで）

5,599件
Fareitが最初に見つかったのは2011年で、昨年はFareitに関するインシデントが5,599件報告されている。

Fareitの機能:
- パスワードの窃盗
- 任意のマルウェアのダウンロードと実行
- DDoS攻撃の実行
- 暗号通貨のウォレットの窃盗
- FTP認証情報の窃盗

統計情報

第1四半期、1分間に出現する新しい脅威は244件で、1秒あたりに換算すると4件を超えます。

インシデント
第1四半期に公開されたセキュリティ インシデントは301件で、第4四半期よりも53%増加。医療機関、公共機関、教育機関で全体の50%を占める。第1四半期に公開されたセキュリティ インシデントの78%はアメリカ大陸で発生。

53%

マルウェア (22%)
第1四半期は新しいマルウェアのサンプルが再び増加し、3,200万件に。**マルウェア サンプルの合計数は6億7,000件で、前年よりも22%増加。**

Mac OSを狙うマルウェア (53%)
ここ3四半期で大量のアドウェアが発生し、新しいMac OSマルウェアが急増。Windowsの脅威に比べると数は少ないものの、**第1四半期に見つかった新しいMac OSマルウェアのサンプルは53%増加。**

モバイル マルウェア (79%)
アジアからのモバイル マルウェアの感染報告は第1四半期に倍増。世界の感染率が57%増加した一因に。**モバイルマルウェアの合計は1,670万件で、前年よりも79%増加。**

マクロ ウイルス (66,000)
新しいマクロ ウイルスはこの3年間の平均を下回る。**第1四半期に確認された新しいマクロ ウイルスのサンプルは66,000件。**

ランサムウェア (59%)
ランサムウェアが急増している。特に、Android OSデバイスへのCongurランサムウェア攻撃件数が増加。**ランサムウェアのサンプルの合計は9,600万件で、昨年よりも59%増加。**

McAfee Global Threat Intelligence

第1四半期にMcAfee GTIが1日に受信したクエリーは平均で550億件です。

9,500万
第1四半期にMcAfee GTIで阻止した危険度中のURLは減少。**第4四半期の1日あたり1億700万件に対し、第1四半期は9,500万件に減少。**精度の向上が要因。

5,600万
第1四半期にMcAfee GTIで阻止した不審なプログラム（PUP）は増加。**第4四半期の1日あたり3,700件に対し、第1四半期は5,600万件に増加。**

McAfee GTI

3,400万
第1四半期にMcAfee GTIで阻止した不正なファイルは減少。**第4四半期の1日あたり7,100万件に対し、第1四半期は3,400万件に減少。**マルウェアの早期検出とローカル情報が良好が要因。

5,900万
第1四半期にMcAfee GTIで阻止した危険なIPアドレスは減少。**第4四半期の1日あたり8,800万件に対し、第1四半期は5,900万件に減少。**早期検出が要因。

McAfee Labs脅威レポート: 2017年6月

レポートの完全版は、www.mcafee.com/June2017ThreatsReportをご覧ください。

McAfee
Together is power.

3181_0517_info-threat-report-malware-evasion