ネットワークセキュリティ脅威レポート2013と2014年の脅威予測

Dell™ SonicWALL™ 脅威調査チーム

目次

要約

- 脅威調査チームは、1 兆 600 億件以上の IPS 関連インシデントを検出および予防し、17 億 8,000 万件以上のマルウェアのダウンロードをブロックしました。

- CVE から報告される新たな脆弱性は 4,429 件あり、3,644 件はネットワーク攻撃に関連するものでした。ブラウザまたはアプリケーションなどの Web に関連する脆弱性が上位を占める状況に変化はありませんでした。

- 2013 年に Dell SonicWALL は、5 件の帯域外ゼロデイ通知を含めて、Microsoft セキュリティ速報を対象とした 19 件のセキュリティアドバイザリを公表しました。

- 2013 年、Dell の感染後マルウェアの活動検出では 780 億件がヒットしました。

- 2013 年に公表された既知のゼロデイ脆弱性は 14 件であり、Dell SonicWALL はそれぞれをブログで報告しました。

- 2013 年にはアプリケーションコントロールの利用が劇的に増加しました。Dell が確認したアプリケーショントラフィックコントロールのヒット数は、2012 年にわずか 240 兆件であったのに対して、2013 年には 770 兆件でした。

- インストールされているファイアウォールあたりに検出されたエクスプロイトおよびマルウェアダウンロードの比率が最も高かったのは、韓国、エルサルバドルおよびエジプトでした。

- サーバが IPS ブロック攻撃の最大のターゲットであると確認されました。

- 2012 年の 1,600 万種に対して、2013 年には 2,010 万種以上の固有なマルウェアのサンプルが収集されました。

- 全体として、Web ベースのエクスプロイトキットの使用は 2013 年に減少しました。しかし、Microsoft Silverlight の脆弱性を取り込む Angler Exploit Kit など、より巧妙な機能が初めて確認されました。

2013 年の注目すべきセキュリティ関連の出来事

- 標的となった小売店 POS のデータ漏洩、4,000 万人以上に影響
  （2013 年 12 月）

- Adobe 社のデータ漏洩、3,800 万人以上のユーザに影響
  （2013 年 10 月）

- Blackhole Exploit Kit の作成者を逮捕、Blackhole Exploit Kit と Cool Exploit Kit は消滅
  （2013 年 10 月）

- Web サイト php.net、マルウェアに感染し悪用される
  （2013 年 10 月）

- スノーデン氏、170 万件の NSA（米国家安全保障局）機密文書を暴露
  （2013 年 6 月）

- 有名なオープンソースのコンテンツ管理システム（CMS）Drupal.org のデータ漏洩、100 万人以上のユーザに影響
  （2013 年 5 月）

- 複数の水飲み場型攻撃、米国労働省を含む政府系 Web サイトを標的に
  （2013 年 5 月）

- Living Social のデータ漏洩、5,000 万人以上のユーザに影響
  （2013 年 4 月）

- 過去最大の DDoS 攻撃、300 ギガビット / 秒相当のトラフィックが発生
  （2013 年 3 月）

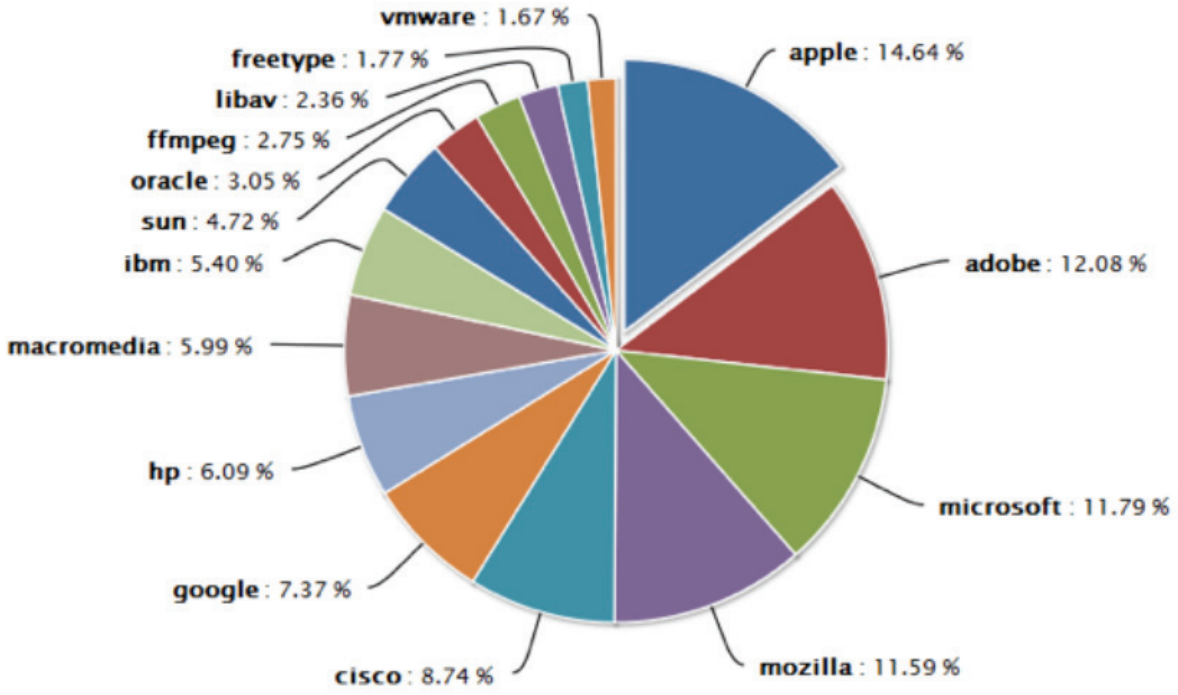
- 米連邦準備銀行サイトのデータ漏洩、4,600 名以上の銀行幹部の信用情報が流出
  （2013 年 2 月）

- 米国の主要メディア支局に対する標的型攻撃およびデータ漏洩
  （2013 年 1 月）

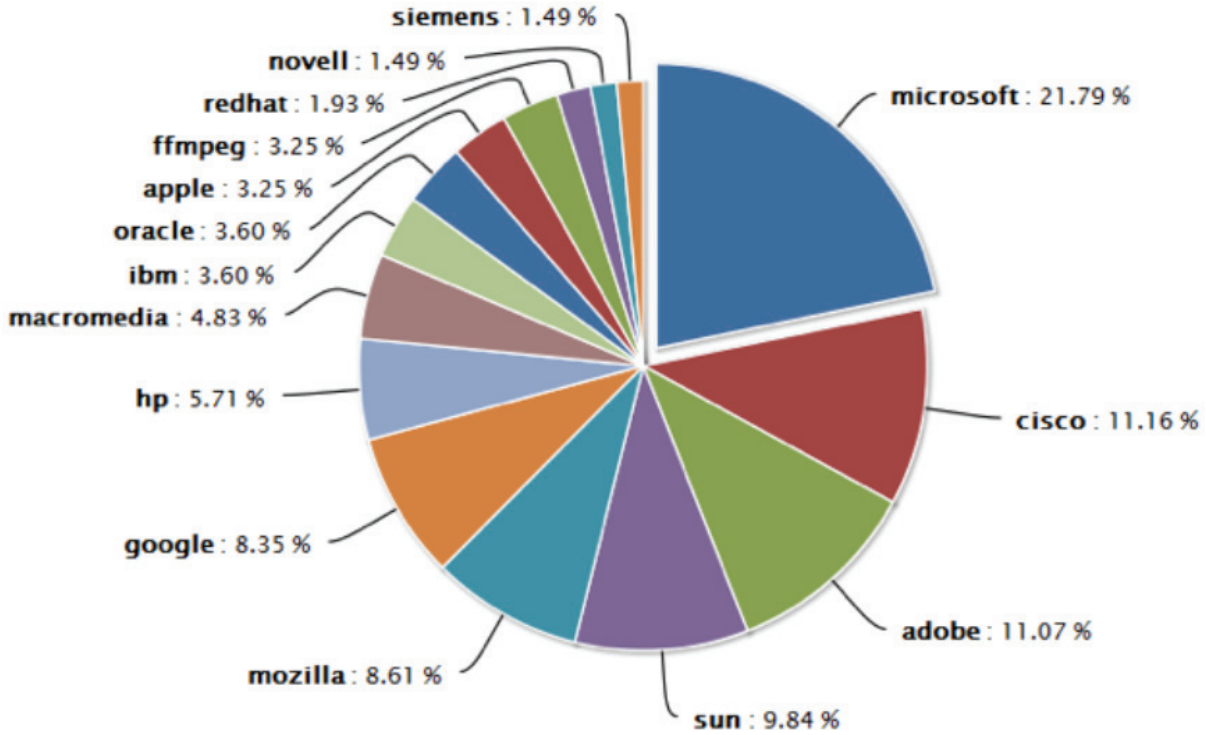
ソフトウェアベンダーごとの脅威：2012 年と 2013 年の比較

Apple 社は製品のセキュリティを向上させて成功しましたが、Microsoft 社には多くの攻撃が集中しました。

重大な脆弱性に被害を受けた上位ベンダー：2012 年



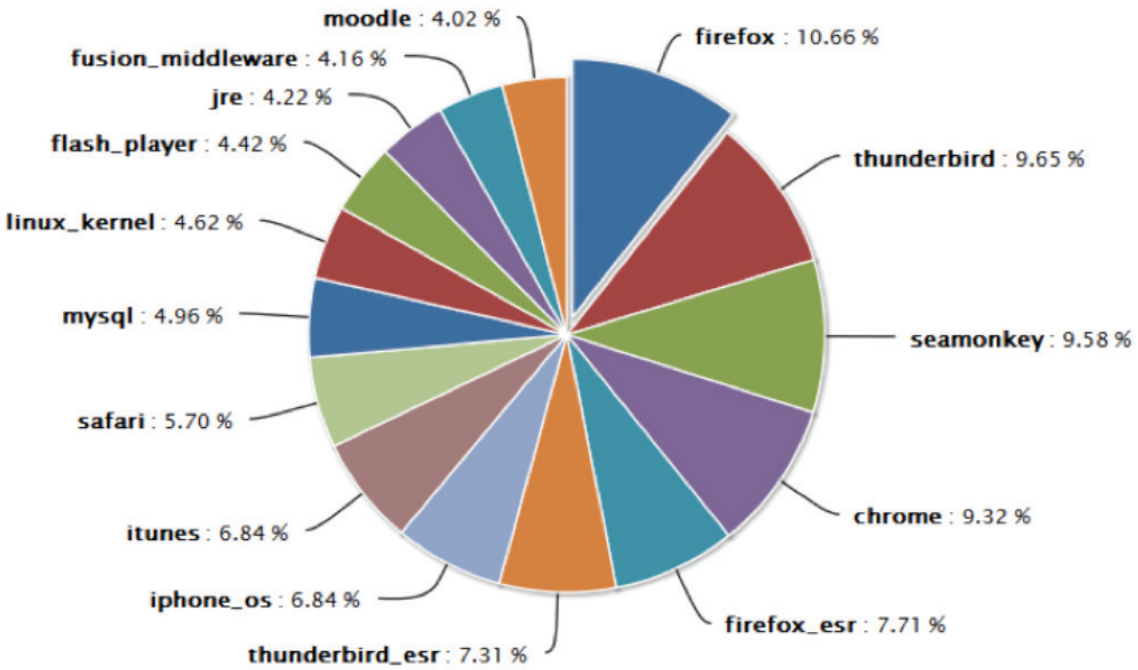
重大な脆弱性に被害を受けた上位ベンダー：2013 年



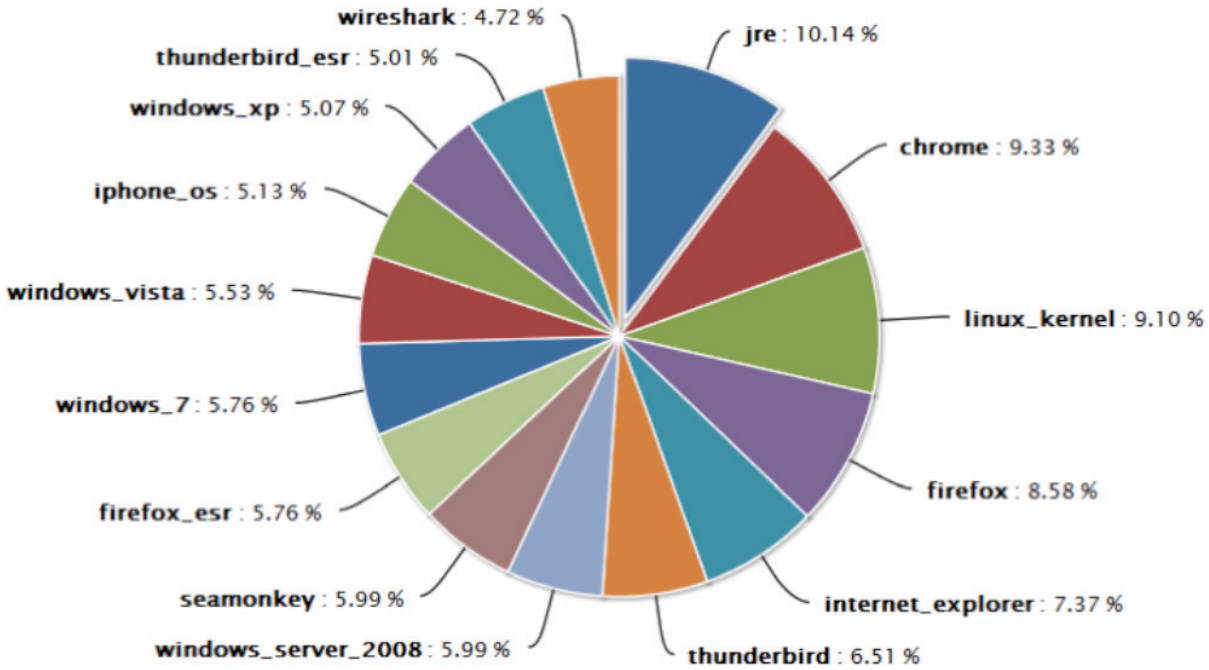
ソフトウェアアプリケーションへの攻撃：2012 年と 2013 年の比較

Apple 社は製品のセキュリティを向上させて成功しましたが、Microsoft 社には多くの攻撃が集中しました。

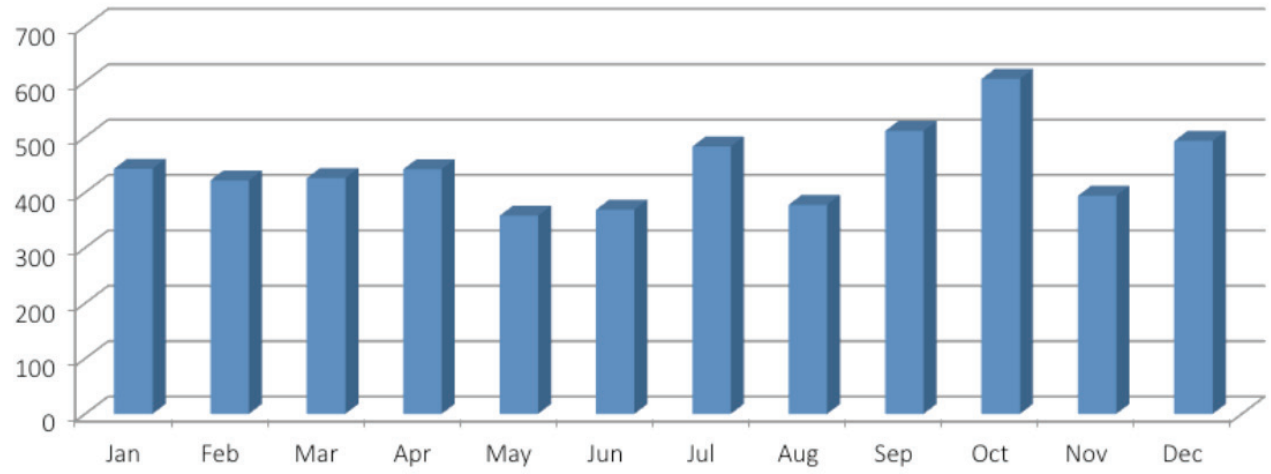
2012 年に最も被害を受けた製品のトップ 15



2013 年に最も被害を受けた製品のトップ 15



2013 年に新たに発見された共通脆弱性識別子（CVE）

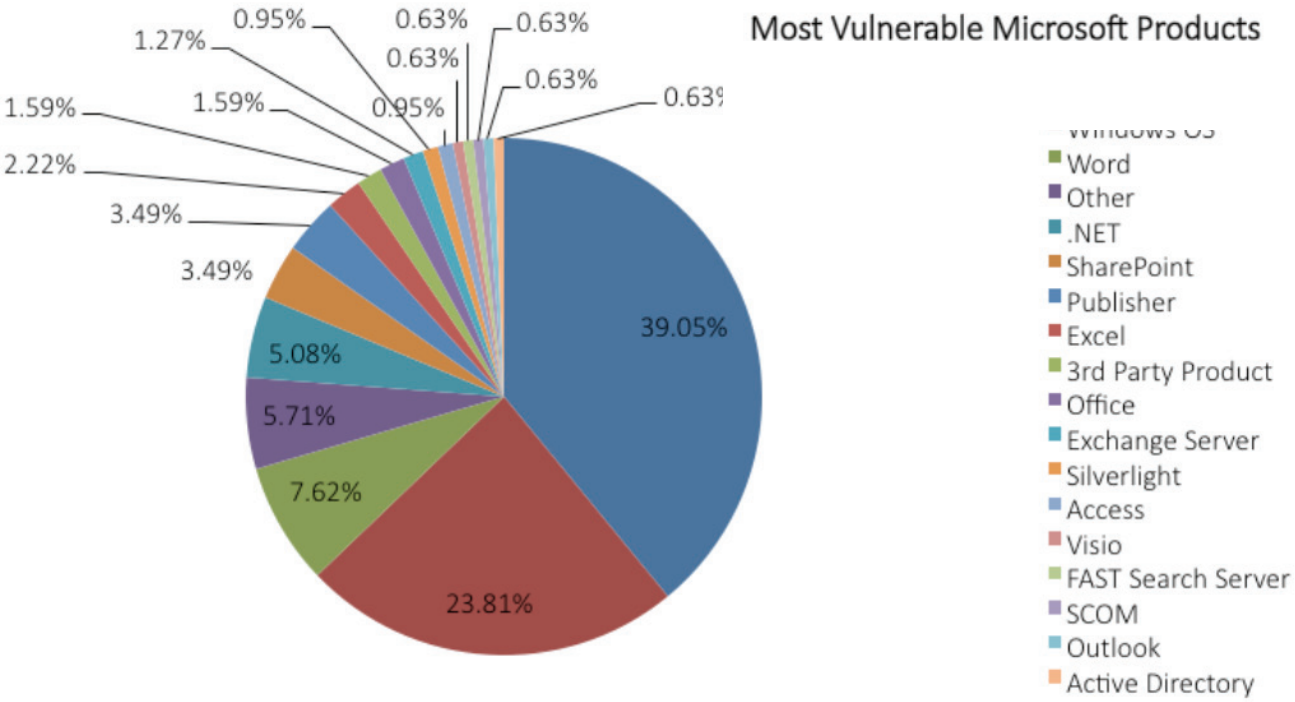


2013 年の Microsoft 製品の脆弱性

Microsoft MAPP プログラムへの継続的な参加によって、Dell は公表されたセキュリティアドバイザリの 48 時間以内に保護を提供する一貫性のある実績を維持することが可能です。
http://technet.microsoft.com/en-us/security/advisorymapp
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=380

下のグラフは、Microsoft 製品ごとの脆弱性の件数を示しています。

最も脆弱な Microsoft 製品



2013 年の Microsoft 製品の脆弱性（続き）

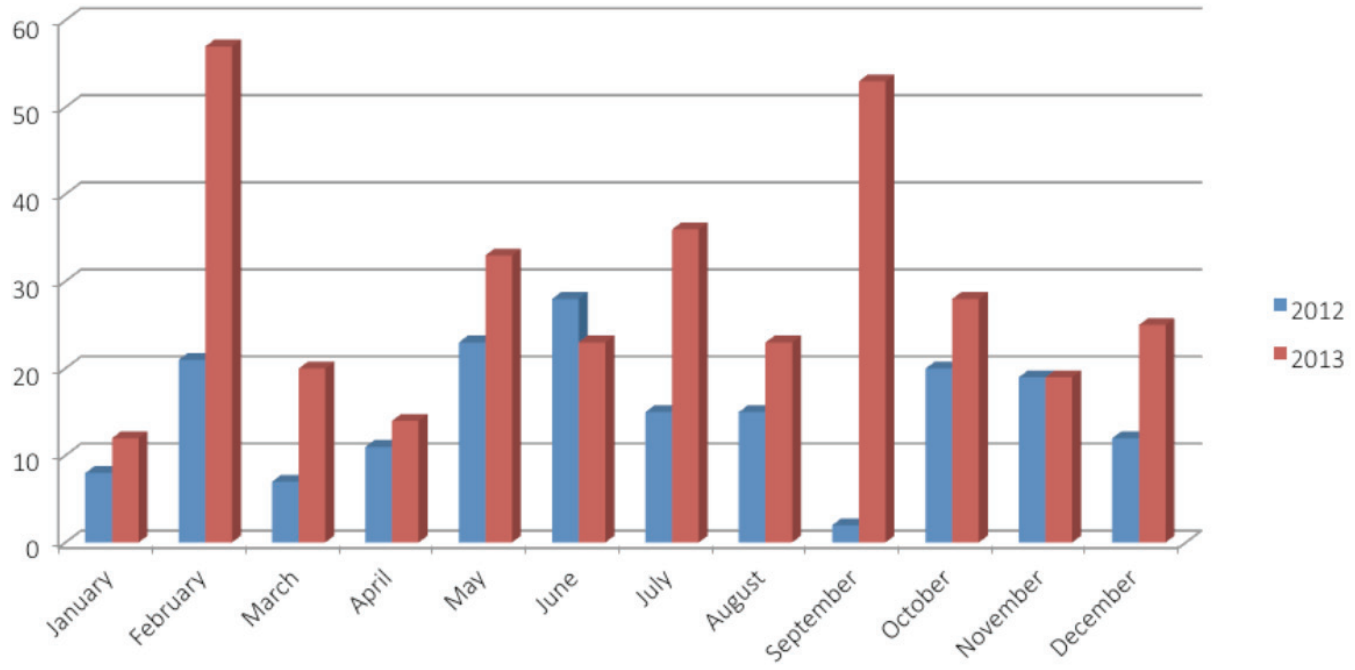
2013 年の Microsoft 社の帯域外セキュリティアドバイザリでは、以下の脆弱性が取り上げられました。

Microsoft カーネルコンポーネントの特権が昇格される脆弱性（CVE-2013-5065）
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=628

グラフィックコンポーネントのメモリ破損の脆弱性（CVE-2013-3906）
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=618

Microsoft Internet Explorer の解放済みメモリ使用の脆弱性（CVE-2013-1347）
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=557

下のグラフは、Microsoft 製品ごとの脆弱性の件数を示しています。



2013 年のゼロデイ脆弱性活動

Adobe Flash、Adobe Reader、Oracle Java および Internet Explorer の脆弱性を利用する複数のゼロデイ攻撃がユーザ環境で実際に確認されました。Dell SonicWALL 脅威調査チームは、これらの攻撃すべてについて積極的に報告し、解決策を提供しました。

- Adobe Flash Player のリモートコード実行（CVE-2013-0633）
- Adobe Flash Player のリモートコード実行（CVE-2013-0634）
- Microsoft Internet Explorer の解放済みメモリ使用の脆弱性（CVE-2013-1347）
- Microsoft Internet Explorer の解放済みメモリ使用の脆弱性（CVE-2013-3893）
- Microsoft Internet Explorer の解放済みメモリ使用の脆弱性（CVE-2013-3897）
- Microsoft Internet Explorer の解放済みメモリ使用の脆弱性（CVE-2013-3918）
- グラフィックコンポーネントのメモリ破損の脆弱性（CVE-2013-3906）
- カーネルコンポーネントの特権が昇格される脆弱性（CVE-2013-5065）
- Oracle Java のリモートコード実行（CVE-2013-0422）
- Oracle Java のリモートコード実行（CVE-2013-0809）
- Oracle Java のリモートコード実行（CVE-2013-1493）
- Oracle Java のリモートコード実行（CVE-2013-2423）
- Oracle Java のリモートコード実行（CVE-2013-2463）
- Adobe Reader のリモートコード実行（CVE-2013-0640）

2013 年の Web ベースのエクスプロイトキットの使用

BlackHole は開発者の逮捕によってほぼ消滅しました。しかし、Angler Exploit Kit などの複数のエクスプロイトキットが代わりに出現し、2013 年も脅威であり続けました。2013 年にユーザ環境で実際に確認された注目すべきエクスプロイトキットの一部を以下に示します。

- BlackHole Exploit Kit
  昨年、Blackhole Exploit Kit は活動中のマルウェアの中で最も流行したエクスプロイトキットの 1 つでした。2013 年の中頃に、作成者らによって Blackhole 2.1.0 がリリースされました。しかし、2013 年 10 月に作成者の一人である通称 Paunch が逮捕されると状況は一変しました。それ以降、エクスプロイトキットの流行は衰えました。以下は Blackhole Exploit Kit に関連する要点の一部です。
  – 攻撃ベクトル：電子メールおよび Web
  – 標的アプリケーション：Internet Explorer、Chrome、Firefox、Safari、Java、Flash および Adobe Reader

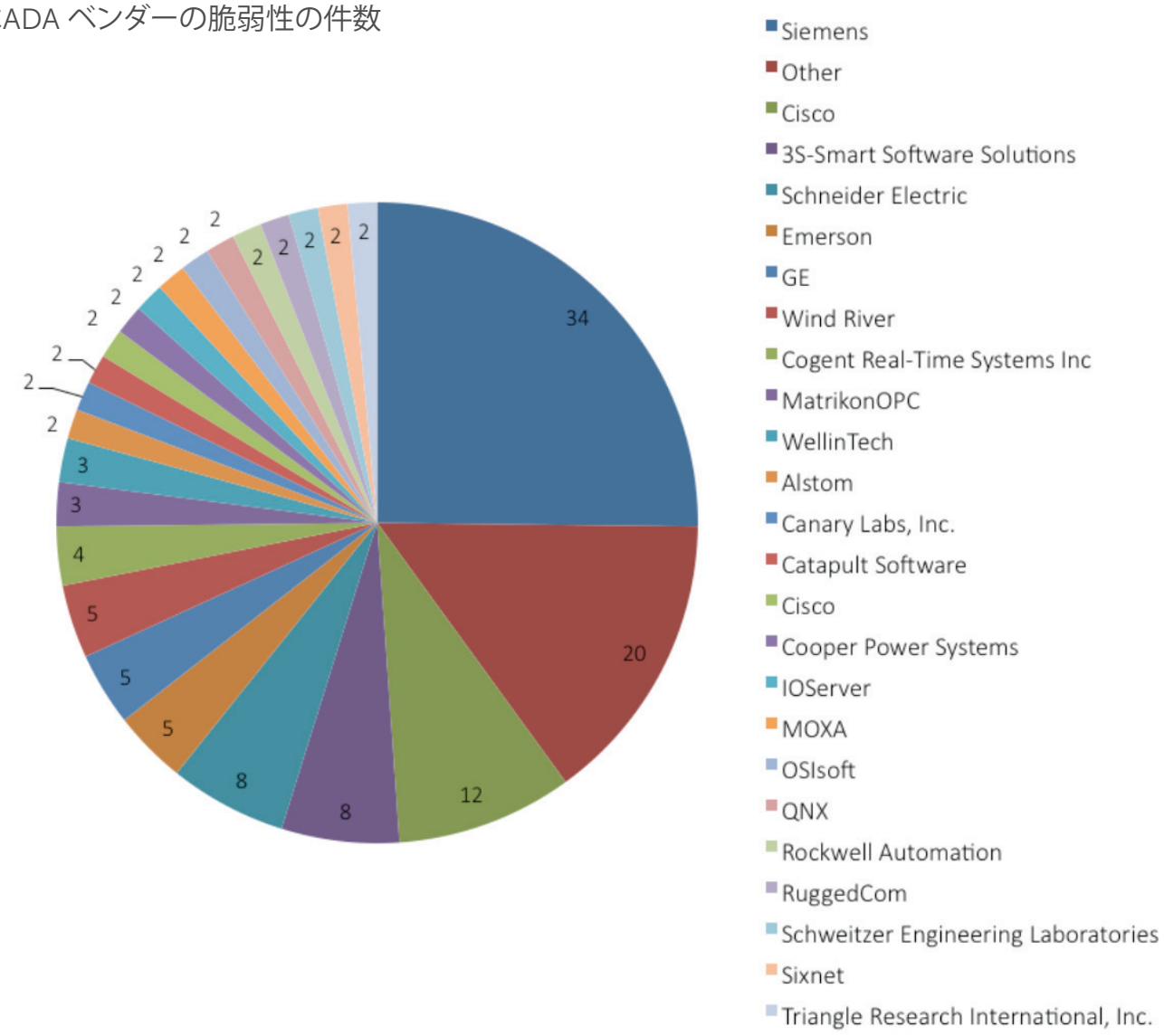
- Cool Exploit Kit
  Paunch によって作成されたとされている別のエクスプロイトキットですが、急速に消滅しつつあります。
- Whitehole Exploit Kit
- Neutrino Exploit Kit
- Angler Exploit Kit
  CVE-2013-0074/3896 を統合した最初の Angler Exploit Kit です。
- Silence Exploit Kit
- Himan Exploit Kit
- Private Exploit Kit

2013 年の SCADA の脆弱性

Stuxnet の出現と SCADA システムによって企業にもたらされるリスクによって、SCADA ベンダー各社は従来にも増して積極的に脆弱性に対応しています。下記のデータは IS-CERT から収集されたものです。

下図は 2013 年にベンダーごとに発見された脆弱性の分布を示しています。Siemens 社が 34 件で最多でした。

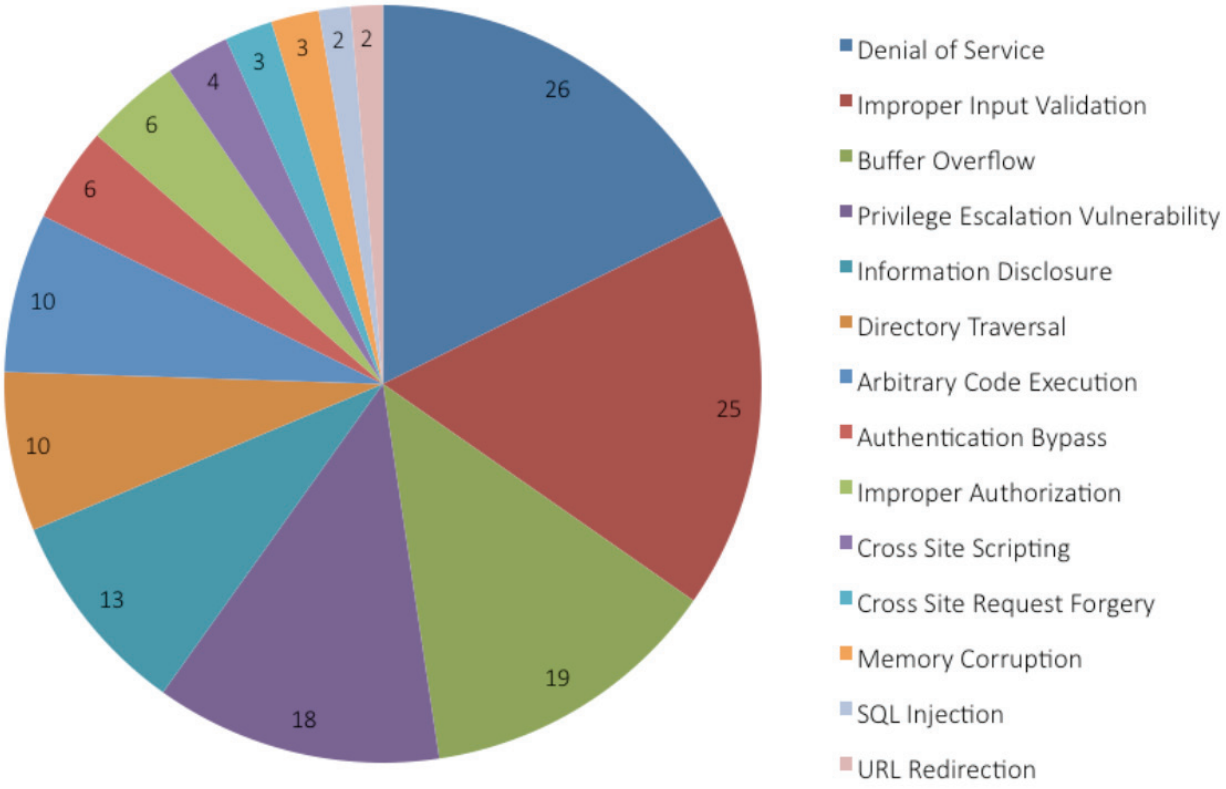
SCADA ベンダーの脆弱性の件数



2013 年の SCADA の脆弱性

下図は 2013 年に SCADA(Supervisory Control and Data Acquisition：監視制御とデータ収集) 関連製品で発見された脆弱性の種類を示しています。SCADA は社会インフラ・産業などさまざまな分野で使用されている装置や機器を監視・管理するためのプロトコルやテクノロジを指し、電気、製造、石油ガス、工作機などで利用されています。SCADA に関連するサービスがダウンすると企業だけでなく国家レベルの安全上の問題となります。2013 年はサービス妨害攻撃が最多でした。

SCADA の脆弱性の件数



Dell Global Response Intelligent Defense（GRID）ネットワーク

Dell SonicWALL の GRID ネットワークは、世界中にある数百万台のセンサーから、さまざまな方向性の脅威情報を収集、分析、検討しています。2013 年には、ユーザ環境で実際にブロックされた侵入防止システムのインシデントが 2012 年から 2013 年にかけて 40% 以上増加したことが確認されました。Dell SonicWALL では、マルウェア調査に関する重要な取り組みが、最初のマルウェア感染の防止に加えて、感染後のマルウェアの活動の検出とブロックに対して重点的に行われています。このことは、感染後のマルウェア活動をブロックするためのユーザ環境で実際に記録されたヒット件数に明確に反映されています。感染後のマルウェア活動には、コマンドアンドコントロール（C2）サーバとの通信、追加のマルウェアファイルのダウンロード、マルウェア自体の更新された新種のダウンロードなどが含まれます。また、記録されたマルウェア防止インシデントも多少減少する結果になっています。

侵入防止インシデント数：
2012 年 – 7,270 億（726,906,572,333）

2013 年 – 1 兆 600 億（1,059,231,965,334）

マルウェア防止インシデント数：
2012 年 – 27.5 億（2,749,335,841）

2013 年 – 17.8 億（1,780,890,310）

感染後マルウェア活動のヒット数：
2013 年 – 780 億（78,343,886,047）

収集されたマルウェアサンプル数：
2011 年 1,350 万

2012 年 - 1,600 万

2013 年 - 2,010 万

新規クラウドシグネチャ数：
2011 年 - 316 万

2012 年 - 340 万

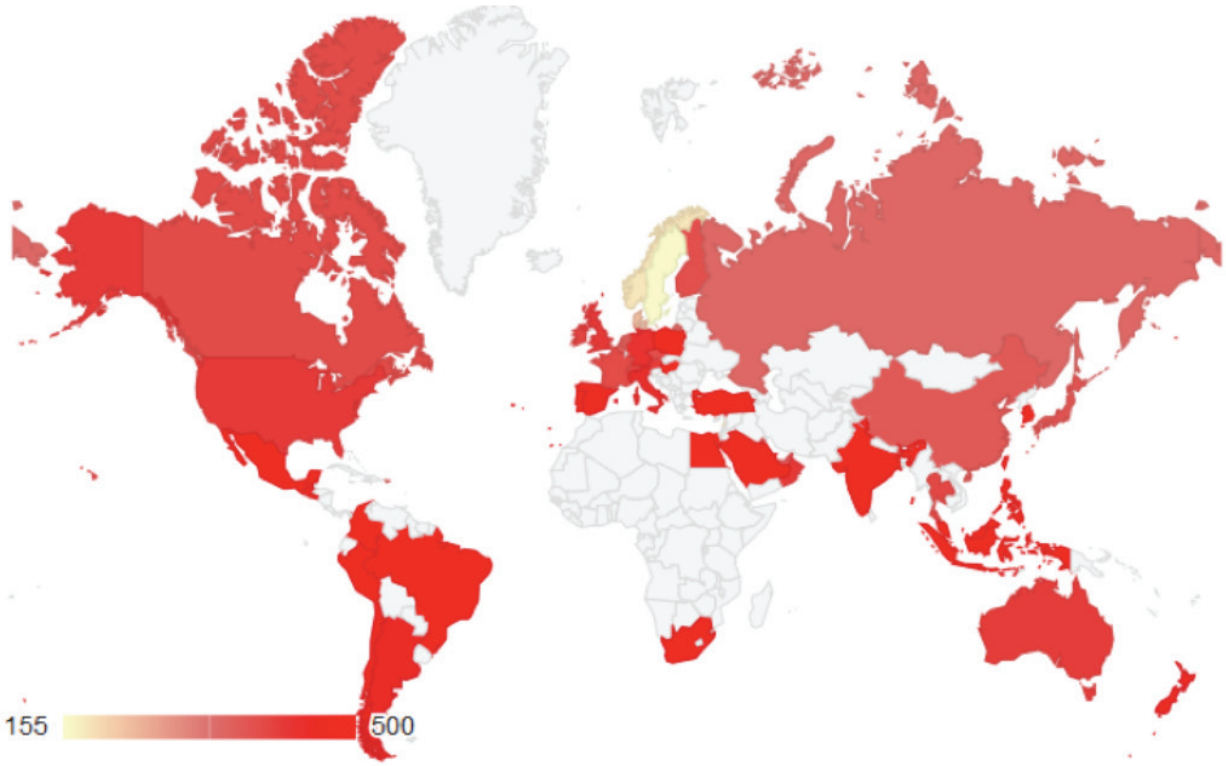
2013 年 - 400 万

アプリケーション総ヒット件数：
2012 年 – 24 兆（23,787,828,592,965）

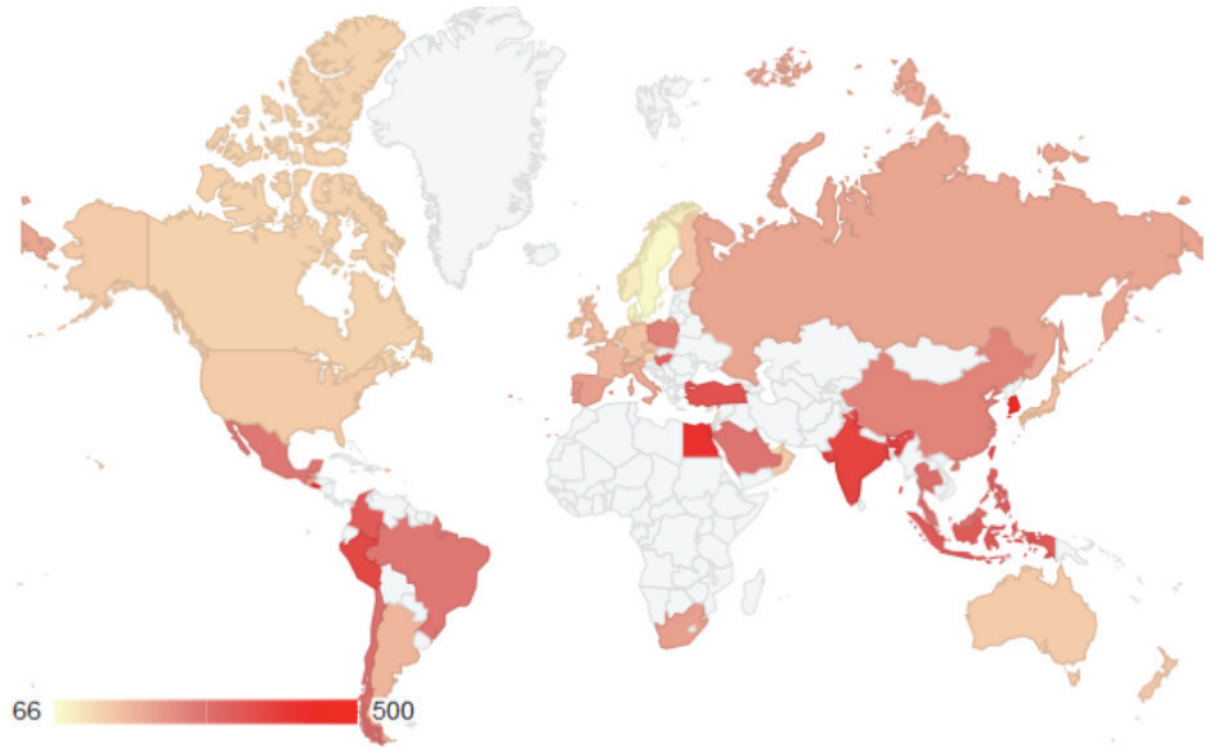
2013 年 – 77 兆（76,907,540,014,509）

攻撃の比率が最も高い国々

下図は国ごとに 1,000 ファイアウォールあたりの IPS 攻撃の件数を示しています。エルサルバドル、エジプトおよび韓国が最も攻撃を受けました。

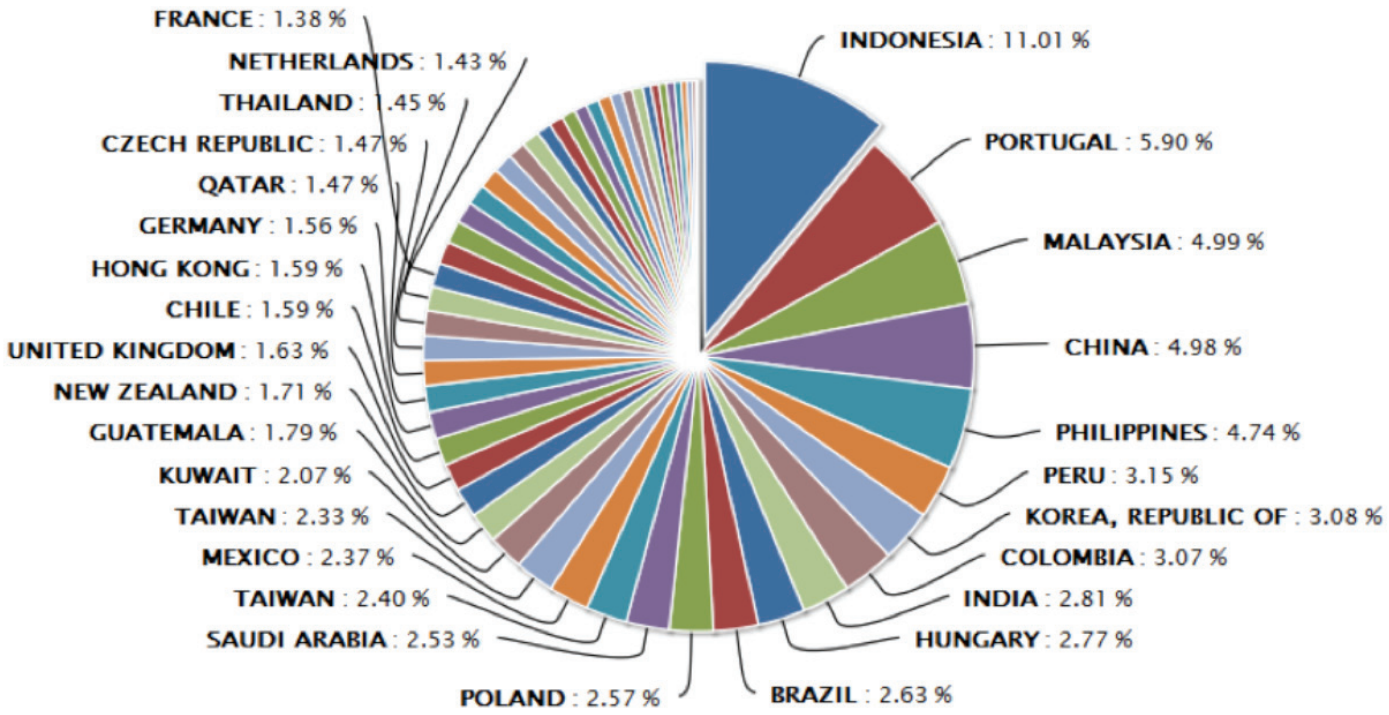


下図は国ごとに 1,000 ファイアウォールあたりのマルウェア攻撃の概要を示しています。韓国、エルサルバドルおよびエジプトが最も攻撃を受けました。

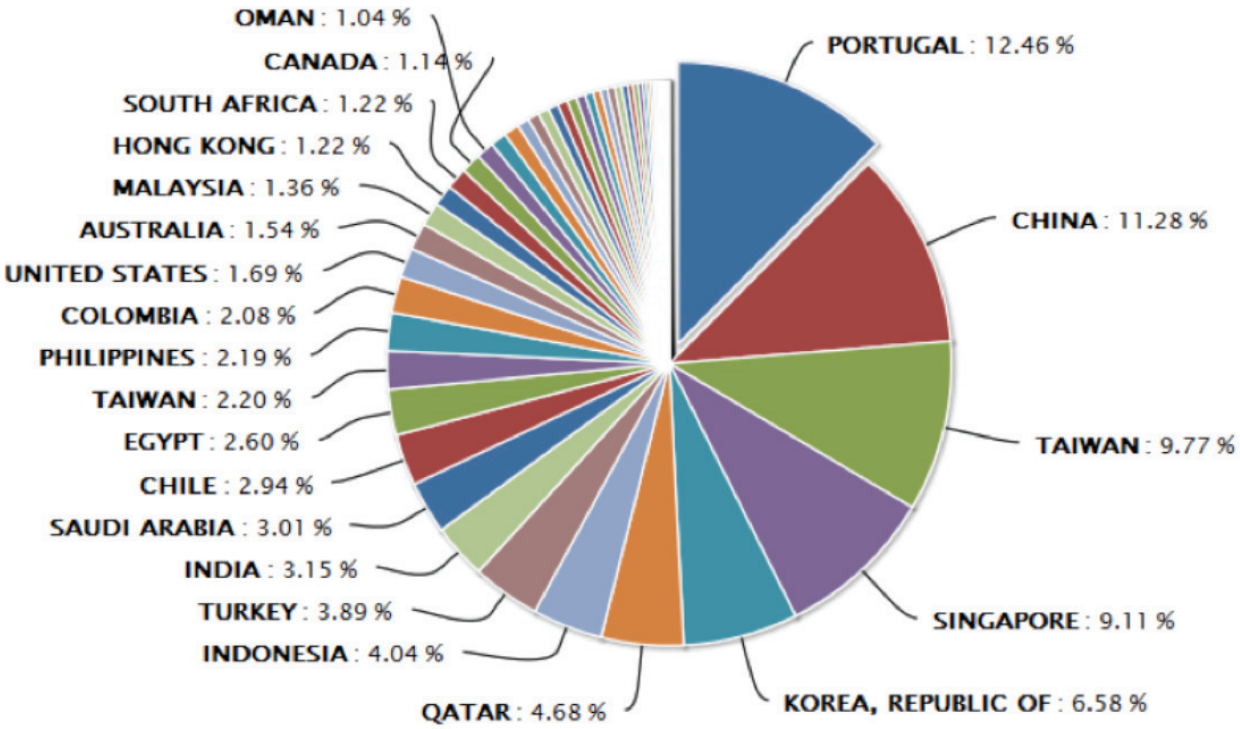


1,000 ファイアウォールあたりの国ベースの攻撃分布

下図は 1,000 ファイアウォールあたりの IPS 攻撃の分布を示しています。

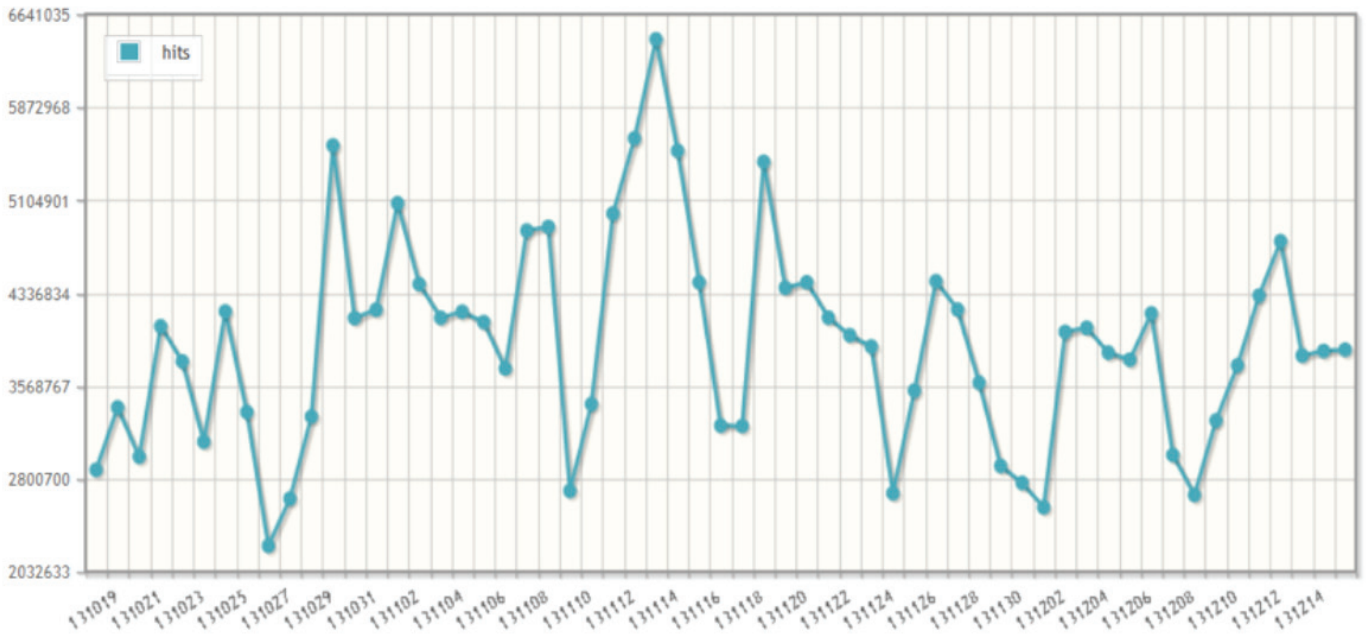


下図は 1,000 ファイアウォールあたりのマルウェア攻撃の分布を示しています。

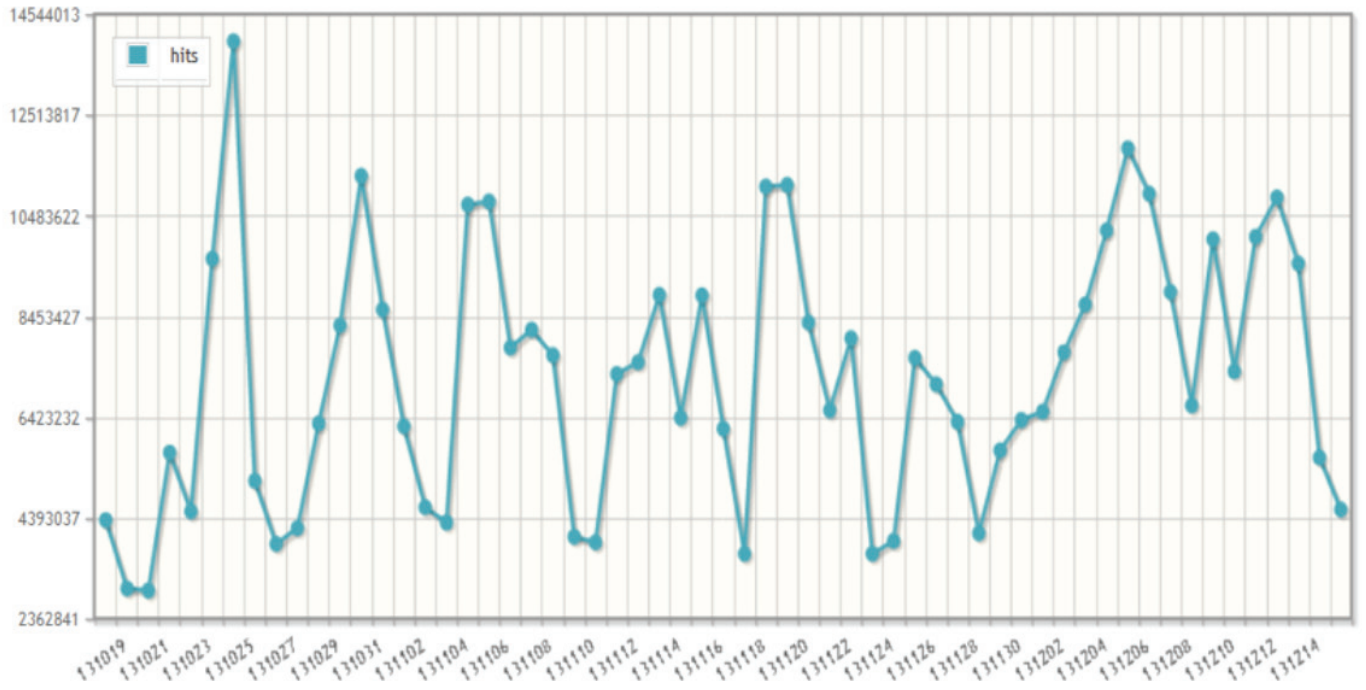


典型的な脅威の攻撃パターン

下図は 2013 年の最後の 2 ヶ月間に発生した IPS 攻撃を示しています。攻撃が週の中頃にピークになり、週末には減少することが示されています。

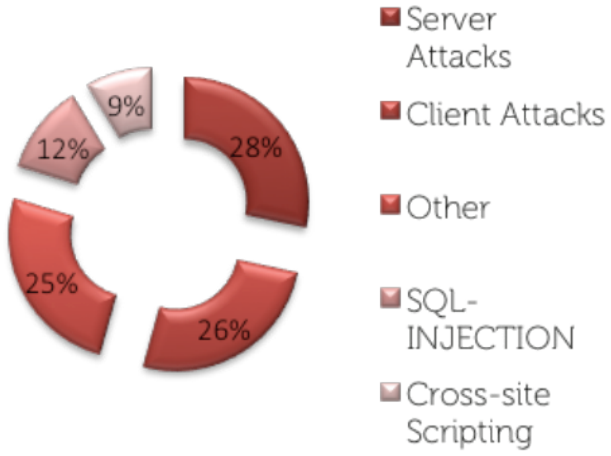


下図は同じ期間のマルウェア攻撃のパターンを示しています。

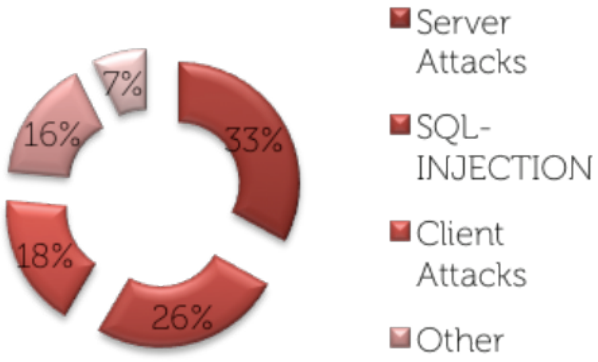


最も一般的な IPS 攻撃

2012 年



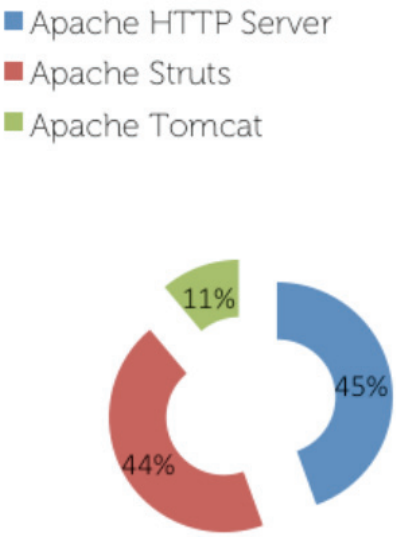
2013 年



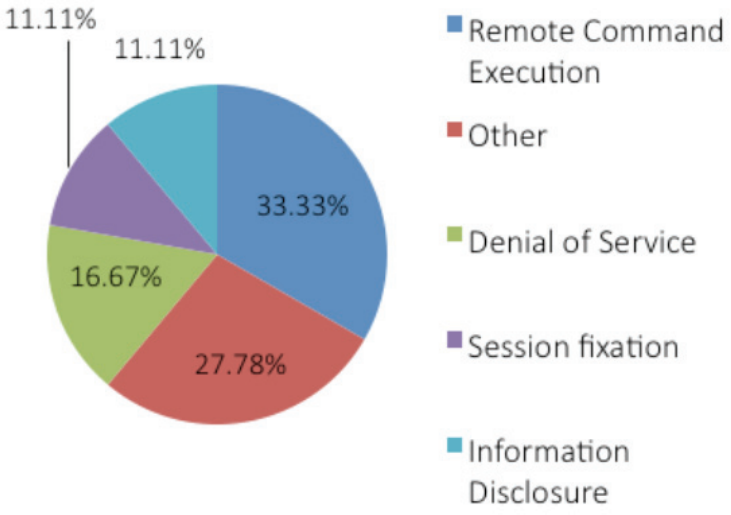
- サーバ攻撃が最も多く、昨年と比べて量が増えました。
- SQL インジェクション攻撃は 2 つ順位が上がり、2013 年には 2 位になりました。
- XSS 攻撃は 2013 年は減少しましたが、安定した攻撃ベクトルのままです。

2013 年の Apache の脆弱性

Apache の脆弱性の標的



Apache の脆弱性の種類



上のグラフは Apache HTTP Server、Struts および Tomcat に対する脆弱性の分布を示しています。Apache HTTP Server は、リモートコマンド実行による攻撃を最も受け、格好の脆弱性になっています。

2013 年の Apache の脆弱性

サーバ攻撃
ブロックされたサーバ攻撃のトップ 3：
1. 1529 – HTTP Server Directory Traversal Attack 1（HTTP サーバのディレクトリ通過アタック 1）
2. 1081 – HTTP Server Remote Code Execution 7（HTTP サーバのリモートコード実行 7）
3. 589 – Suspicious Request URI 7（疑わしい要求 URI 7）

クライアント攻撃
ブロックされたクライアント攻撃のトップ 3：
1. 7693 – Obfuscated HTML Code 4（難読化された HTML コード 4）
2. 4733 – HTTP Client Shellcode Exploit 17a（HTTP クライアントシェルコードのエクスプロイト 17a）
3. 4816 – Client Application Shellcode Exploit 2（クライアントアプリケーションシェルコードのエクスプロイト 2）

最も標的にされたデバイス /OS：

Microsoft Windows オペレーティングシステム（特に Windows XP/7）が実行されているコンピュータと Android オペレーティングシステムが実行されているスマートフォンが 2013 年に最も標的にされたデバイスでした。

2013 年のサイバー犯罪活動

以下のカテゴリにおける脅威の数の増加が確認されています。
a) バンキング系トロイの木馬およびランサムウェアを含む標的型スパムキャンペーン

b) ゼロデイエクスプロイト攻撃に続く自動ダウンロードを含む各種の標的型攻撃で使用される主要ベクトルであり続けている Web ベースのエクスプロイトキット

c) 検出を回避するために SSL ベースのコマンドアンドコントロール通信を利用するマルウェアファミリの増加とともに、SSL ベースのボットの増加が確認されています。

d) Bitcoinminer ボットネット、ClickFraud ボットネット、ペイパ―インストールマルウェア、さらに巧妙なランサムウェアによって生じるマルウェア経済

- SSL ボット SonicAlert を含む標的型キャンペーンの記事：
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=597
- https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=623
- 巧妙なランサムウェア SonicAlert の記事：
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=601

2013 年の新種の攻撃

- SSL ボットと主要マルウェアファミリによるコマンドアンドコントロールサーバを用いた SSL ベース通信の増加
- ランサムウェアファミリ - CryptoLocker は感染したマシン上のデータを暗号化するために非対称鍵暗号化方式を使用した最初のランサムウェアです。PGP 鍵ペアがコマンドアンドコントロールサーバ上で動的に生成され、72 時間以内に支払いが受領されなかった場合、秘密鍵は破壊されます。また、コマンドアンドコントロールサーバを隠すために特別なドメイン生成アルゴリズムも使用されます。
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=601

2013 年の新種の攻撃（続き）

- 収入を上げるために感染したシステム上の CPU および CPU 処理サイクルを利用する Bitcoin マイニングマルウェアの増加 Bitcoin マイニング IRC ベースのボットネットの増加
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=621,
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=564
- Android ベースのスマートフォンユーザを標的とする巧妙なバンキング系マルウェア
- CVE-2013-3893 などの標的型攻撃の急増

  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=602
- MiniDuke のように巧妙な手法を用いたソーシャルエンジニアリングの手口
  https://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor, and ASLR/DEP bypass.
- 正規の収集した / 偽装した電子メールアドレスを利用する標的型スパムキャンペーンの増加
- スパムテーマは過去数年間で相当に進化し、より一層本物のように見えるようになったため、ユーザが URL をクリックしたり、添付ファイルを開いたりする可能性が大幅に高くなっています。確認された多くの電子メールは、社内のファクス、ボイスメールモジュール、スキャナ、および正規の問題のないベンダーの電子メールによるキャンセルされたオンライン注文から届いたと装ったものでした。
- スパムテキストメッセージに対して脆弱なモバイルデバイス
  http://threatpost.com/google-nexus-phones-vulnerable-to-sms-denial-of-service-attack/103066

2013 年の標的型攻撃

- ファクス、ボイスメール、プリンタ、スキャナなどのサービスを利用した企業の従業員に対する標的型スパム
- 特別なドメイン生成アルゴリズムと非対称暗号化を利用した CryptoLocker のような巧妙なランサムウェア
- SSL ベースのマルウェアダウンロードおよび通信
- 自動ダウンロードや標的マシン上でのインストールに至るゼロデイエクスプロイトペイロードによる Web ベースのエクスプロイトキット。以下はゼロデイエクスプロイトを利用した最近の標的型攻撃の例です。

脆弱性のトップ 3：

クロスサイトスクリプティング攻撃

- Apache HTTP Server XSS の脆弱性（2013 年 3 月 8 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=539

サービス妨害攻撃

2013 年にはサ―ビス妨害攻撃に関するいくつかの出来事がありました。

- nginx Server Denial of Service（2013 年 5 月 24 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=563
- DDoS 機能を持つ Delphi ベースのボット（2013 年 3 月 15 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=541
- Oracle MySQL サーバのジオメトリクエリの DoS（2013 年 3 月 22 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=543
- Squid の Accept-Language 値の DoS（2013 年 4 月 5 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=548
- 新種のロシア製 DDoS ボットネットの発見（2013 年 5 月 1 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=554

- DDoS およびスパイ機能を持つ C++ ベースのボット（2013 年 5 月 10 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=559
- Bitcoin マイニングおよび DDoS 機能を持つ Infostealer Trojan（トロイの木馬）（2013 年 5 月 30 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=564
- Samba の read_nttrans_ea_list 関数の DoS（2013 年 8 月 22 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=591

クライアントアプリケーションの解放済みメモリ使用の脆弱性に対する攻撃
2013 年には、複数の解放済みメモリ使用の脆弱性エクスプロイトがユーザ環境で実際に確認されました。以下は 2013 年に公表された解放済みメモリ使用の脆弱性に対する攻撃に関する SonicAlert です。

- Windows IE の解放済みメモリ使用の脆弱性 MS13-047（2013 年 6 月 21 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=572
- Firefox の onreadystatechange の解放済みメモリ使用の脆弱性（2013 年 8 月 9 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=587
- Microsoft Windows IE のメモリ破損（2013 年 9 月 18 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=600
- Microsoft Windows IE の脆弱性 CVE-2013-3893（2013 年 9 月 26 日）
  (https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=602
- Microsoft Windows IE の脆弱性 CVE-2013-3897（2013 年 10 月 8 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=607
- Microsoft Windows IE の脆弱性 CVE-2013-1347（2013 年 10 月 17 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=610

マルウェアのサンプル

2013 年には約 2,010 万種の固有マルウェアのサンプルが収集されました。これは 2012 年の 1,600 万種に対して増加しています。平均すると、1 日に約 5,5000 の新たなサンプルが出現していることになります。

2013 年の上位マルウェア

- Cryptolocker ランサムウェアファミリは、最も注目すべき厄介なマルウェアの 1 つでした。
- 正規のテーマで企業の電子メールアドレスを標的とする標的型スパムキャンペーンと連動した SSL ボットが 2013 年の新たな観測でした。
- Zeus や Cridex を含むバンキング系トロイの木馬は、自動ダウンロードおよび電子メールスパムキャンペーンによってユーザ環境で実際に流行し続けました。
- Bitcoin の価値の上昇に伴って（最高値は 1,200 米ドル）、Bitcoin マルウェアファミリと IRC ベースのボットネットの数の増加も確認されました。

2013 年の Microsoft 製品の脆弱性に関する報道

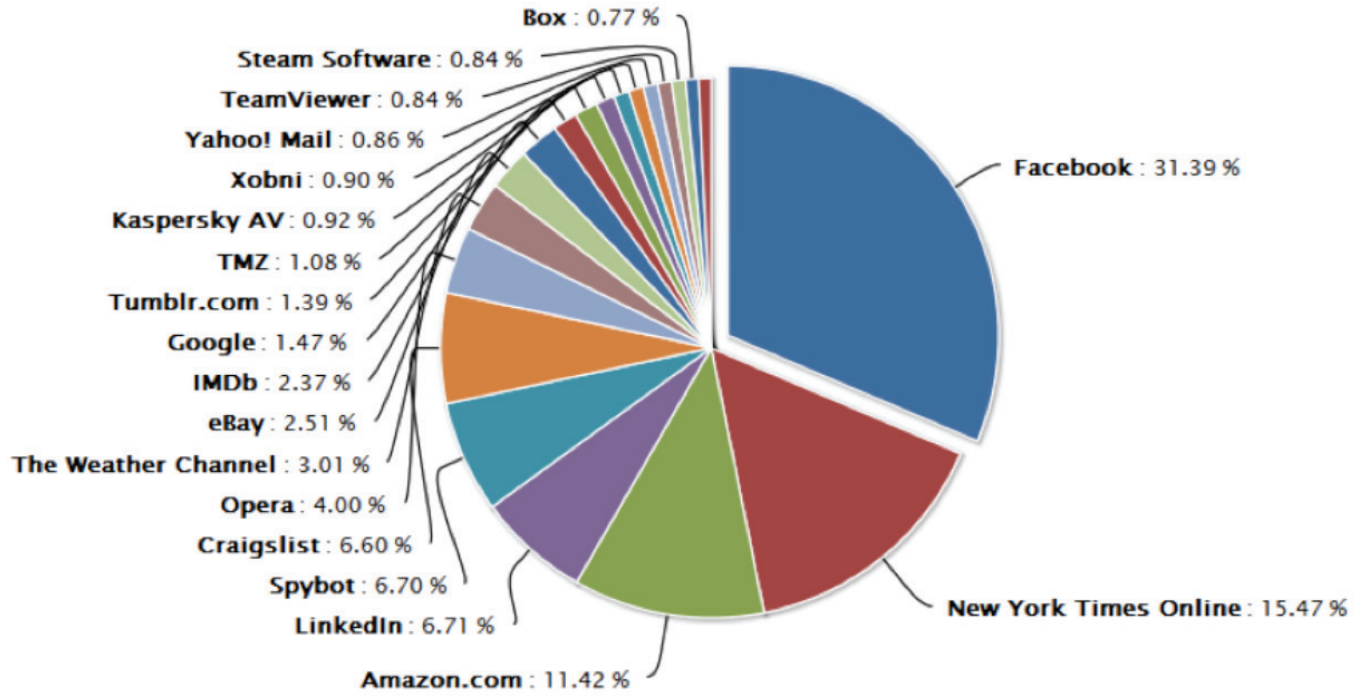
- Microsoft セキュリティ速報の報道（2013 年 12 月 10 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=631
- Windows カーネルに対する Microsoft 社の帯域外セキュリティアドバイザリ（2013 年 11 月 27 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=628
- Microsoft セキュリティ速報の報道（2013 年 11 月 12 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=498
- グラフィックコンポーネントに対する Microsoft 社の帯域外セキュリティアドバイザリ（2013 年 11 月 5 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=618
- Microsoft セキュリティ速報の報道（2013 年 10 月 8 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=608
- Microsoft セキュリティ速報の報道（2013 年 9 月 10 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=598
- Microsoft セキュリティ速報の報道（2013 年 8 月 13 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=589
- Microsoft セキュリティ速報の報道（2013 年 7 月 9 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=578
- Microsoft セキュリティ速報の報道（2013 年 6 月 12 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=568
- Microsoft セキュリティ速報の報道（2013 年 5 月 14 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=560
- IE 8 に対する Microsoft 社の帯域外セキュリティアドバイザリ（2013 年 5 月 4 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=557
- Microsoft セキュリティ速報の報道（2013 年 4 月 9 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=549
- Microsoft セキュリティ速報の報道（2013 年 3 月 12 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=540
- Microsoft セキュリティ速報の報道（2013 年 2 月 12 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=526
- Microsoft セキュリティ速報の報道（2013 年 1 月 8 日）
  https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=514

Microsoft MAPP program プログラムにおいて、Dell は当社顧客のすべてに 48 時間以内に保護を提供していると一貫して認識されました。
http://technet.microsoft.com/en-us/security/advisorymapp

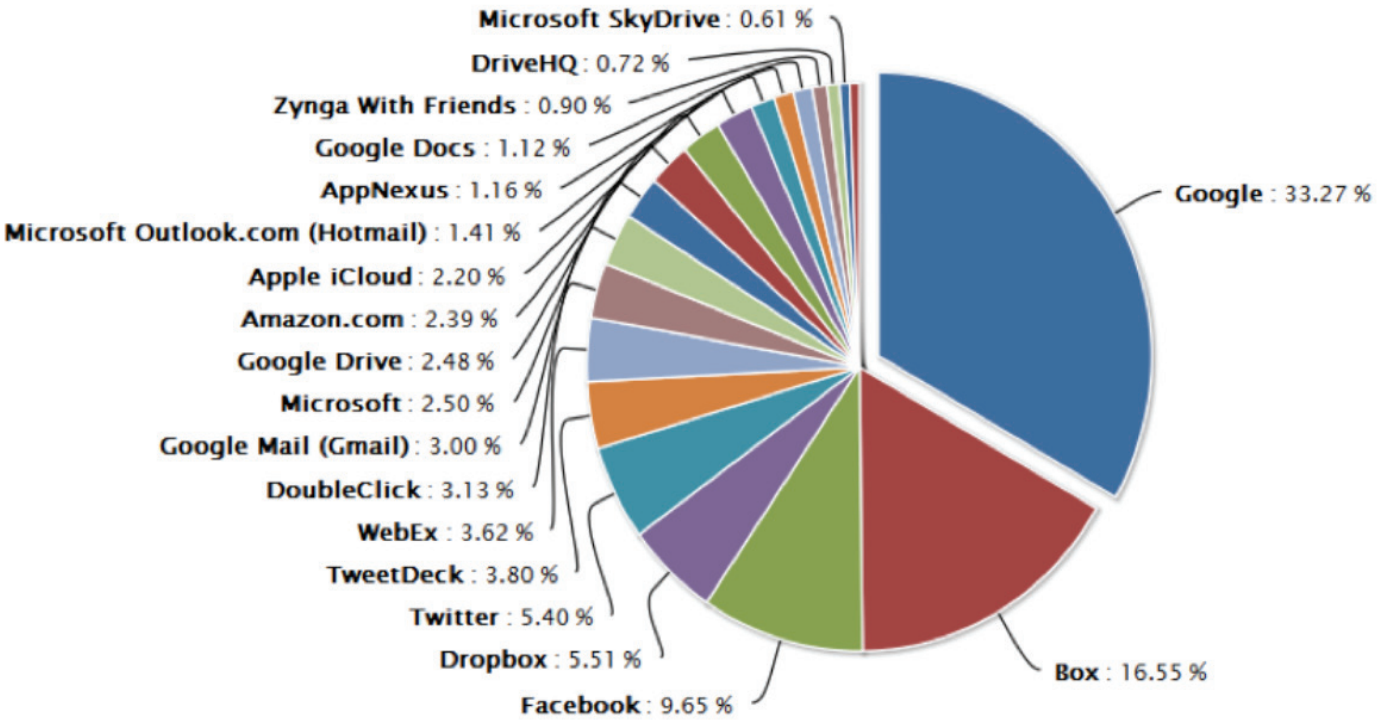
Dell SonicWALL によって取り上げられた Microsoft 社関係の脆弱性：
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=380

アプリケーショントラフィックの使用

最も多く閲覧されている Web サイトのトップ 20



最も多く閲覧されている安全なブラウジング Web サイトのトップ 16



各国のアプリケーションシグネチャのトップ 3

米国（北米）

カテゴリ	シグネチャ ID	シグネチャ名
VoIPアプリケーション	6589	RTP — G711 PCMU Audio
プロトコル	5147	HTTP — GET
プロトコル	5159	SSL — TLSv1.0 (SSLv3.1) Client Hello

英国（欧州）

カテゴリ	シグネチャ ID	シグネチャ名
プロトコル	5147	HTTP — GET
プロトコル	5159	SSL — TLSv1.0 (SSLv3.1) Client Hello
VoIPアプリケーション	6589	RTP — G711 PCMU Audio

南アフリカ（アフリカ）

カテゴリ	シグネチャ ID	シグネチャ名
プロトコル	5147	HTTP — GET
プロトコル	5159	SSL — TLSv1.0 (SSLv3.1) Client Hello
プロトコル	5148	HTTP — POST

イタリア（欧州）

カテゴリ	シグネチャ ID	シグネチャ名
プロトコル	5147	HTTP — GET
プロトコル	4413	POP — TCP 110
VoIPアプリケーション	6589	RTP — G711 PCMU Audio

インド（アジア）

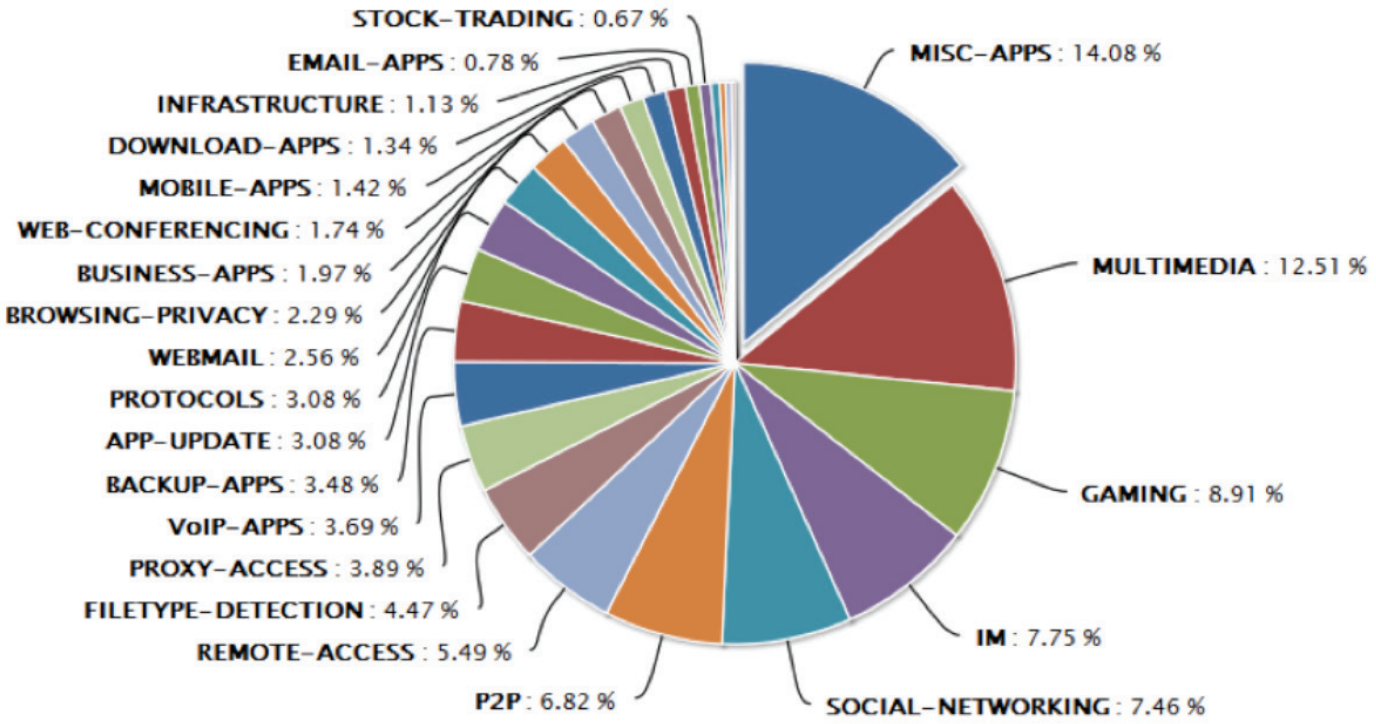
カテゴリ	シグネチャ ID	シグネチャ名
VoIPアプリケーション	6589	RTP — G711 PCMU Audio
プロトコル	5147	HTTP — GET
プロトコル	4413	POP — TCP 110

中国（アジア）

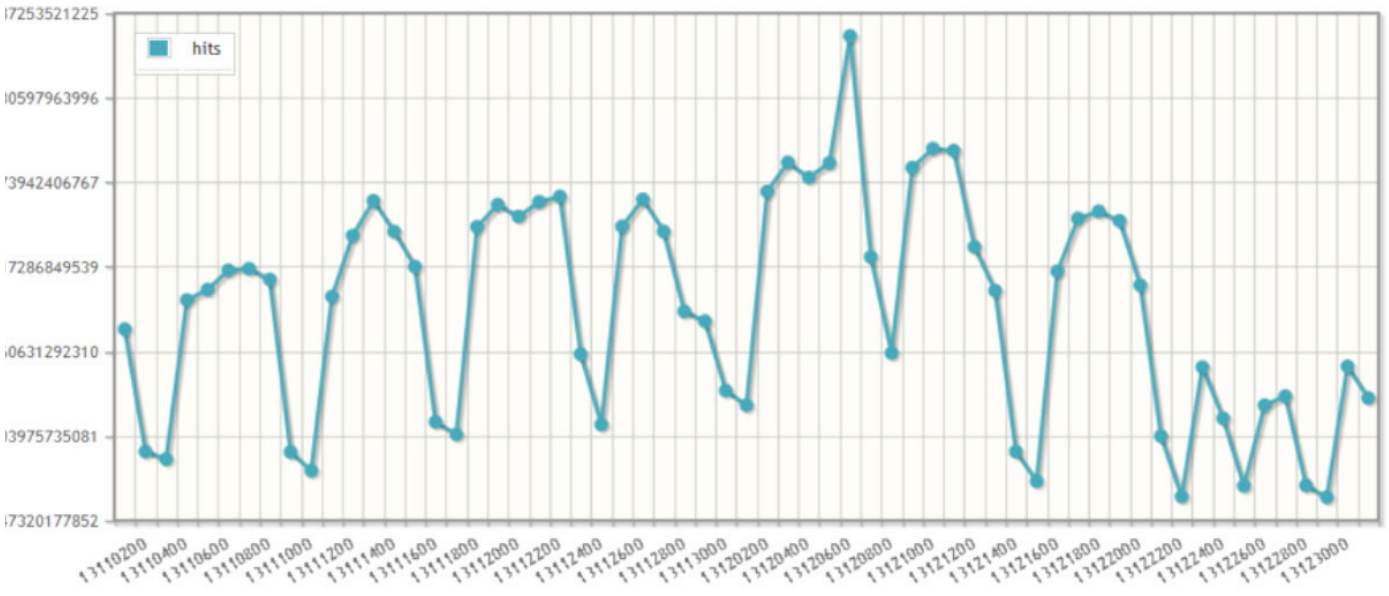
カテゴリ	シグネチャ ID	シグネチャ名
プロトコル	5147	HTTP — GET
プロトコル	4413	POP — TCP 110
プロトコル	5148	HTTP — POST

アプリケーションシグネチャのカテゴリ分布

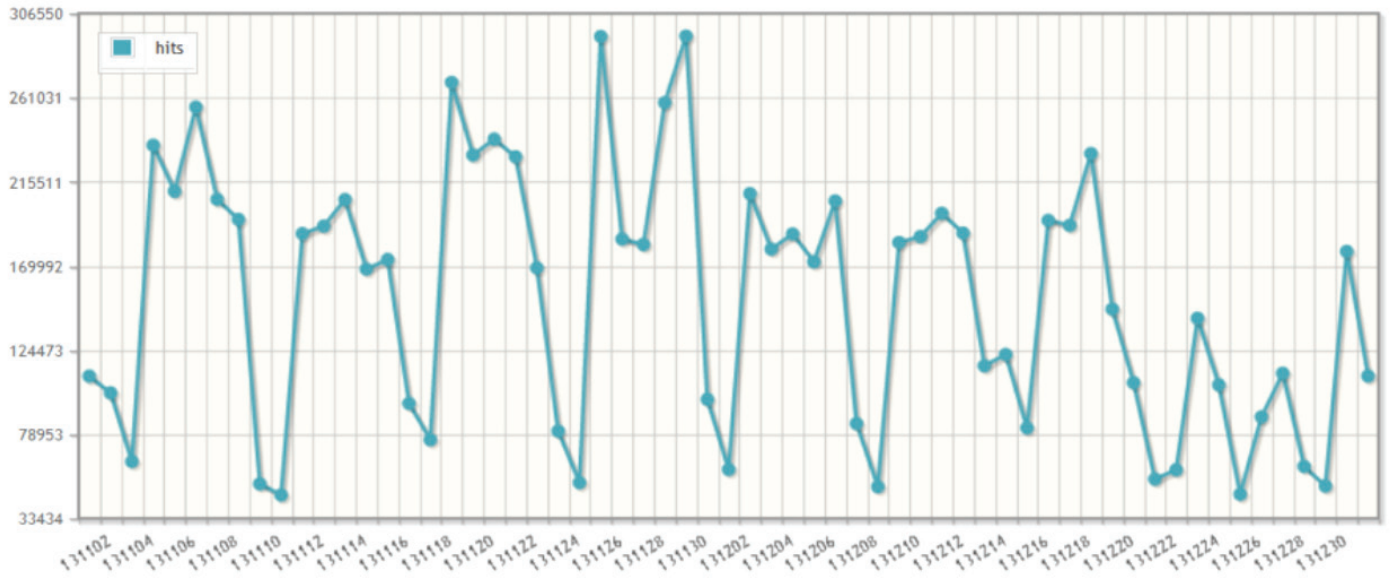
2013 年に Dell は多くの一般的なアプリケーションを網羅しました。下図は Dell SonicWALL アプリケーションシグネチャのカテゴリ分布を示しています。



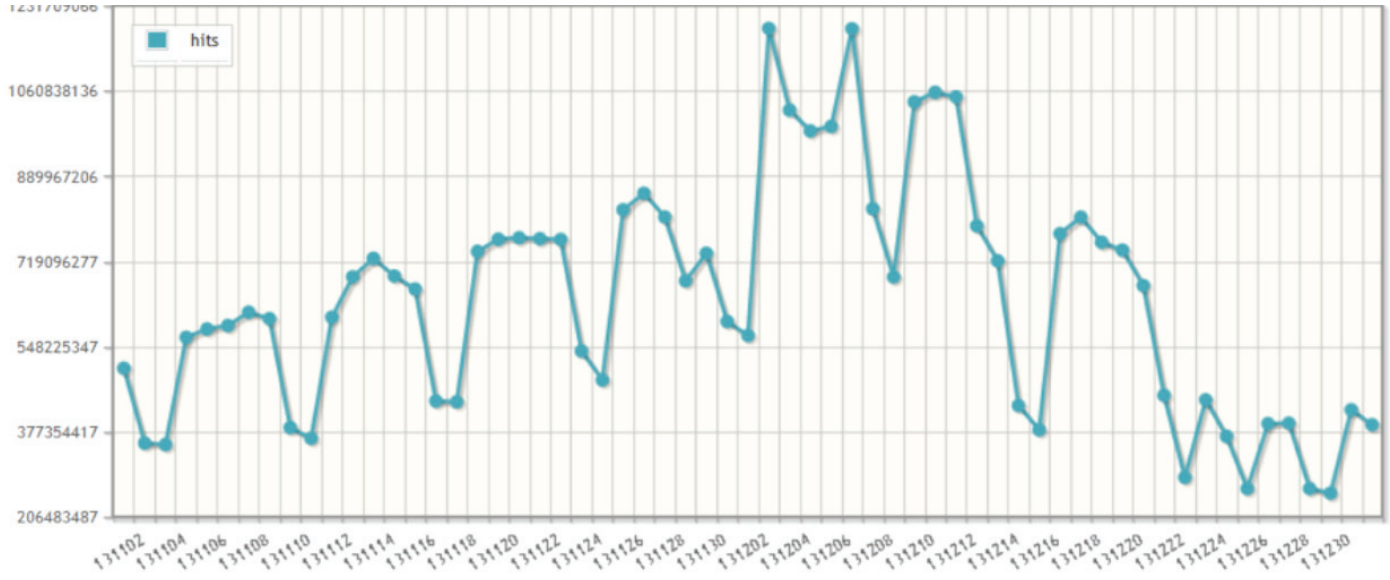
2013 年の最後の 2 ヶ月間のアプリケーショントラフィックの使用



2013 年の最後の 2 ヶ月間のソーシャルネットワークトラフィックの使用



2013 年の最後の 2 ヶ月間のオンラインショッピングトラフィックの使用



2014 年の予測

- モバイルデバイスでは、脆弱性、巧妙なマルウェア攻撃および想定されるモバイルボットネットの数の増加が予想されます。Android はモバイル攻撃の主要プラットフォームであり続けることでしょう。
- 巧妙なハイブリッドマルウェアでは、企業ネットワークに侵入して拡散するためにモバイルデバイスが利用されるでしょう。
- 水飲み場型攻撃などのソーシャルエンジニアリング攻撃は、標的型攻撃の重要なベクトルの 1 つであり続けるでしょう。
- 作成者の逮捕によって BlackHole Exploit Kit のインフラストラクチャはほぼ消滅したため、ゼロデイエクスプロイトを活用し、さまざまなプラットフォームを標的とする最新機能を備えた、新たな後継のエクスプロイトキットが出現すると予測されます。
- Windows XP は、サポートライフサイクルが 2014 年に終了しますが、依然として標的になるでしょう。
- Windows 7/8 は、Windows XP の利用が縮小するにつれて、標的になる可能性が高くなるでしょう。
- より多くのソーシャルネットワークが攻撃ベクトルとして利用されるでしょう。
- ユーザ信用証明および個人データの盗難は継続することでしょう。
- ランサムウェアは活動を継続することでしょう。
- マイニングボットネットなどの Bitcoin 関連の攻撃は増加するでしょう。

詳細は以下にお問い合わせください。

デル株式会社　ソニックウォール
〒160-0023　東京都新宿区西新宿6-10-1
日土地西新宿ビル13F
Tel. 03-6279-4030
http://www.sonicwall.com/japan/

Report-2013DellSonicWALLThreatReport-US-TD593-20140123