

## Cisco Security Agent および Microsoft Win32/Nuwar.N (Storm Trojan) エクスプロイト

### 概要

Win32/Nuwar.N@MM!CME-711 は、E メール経由でトロイの木馬を送信する大量メール送信型のワームです。このエクスプロイトは、Windows 2000、Windows 95、Windows 98、Windows Me、Windows NT、および Windows XP オペレーティング システムに影響を与えます。このワームがはじめて検出されたのは、2007 年 1 月 19 日 です。このエクスプロイトを表す名前は、アンチウイルスベンダーによって異なります。CME-711、W32/Downloader.AYDY (F-Secure 社)、Troj/DwnLdr-FYD (Sophos 社)、Trojan.Peacomm (Symantec 社)、Win32/Pecoan、Win32/Pecoan.B、Win32/Pecoan.E、Win32/Pecoan.F、Win32/Pecoan.G、および Downloader-BAI.sys!M711 (McAfee 社)

この脆弱性を悪用したさまざまな攻撃がすでに回っています。シスコシステムズはエクスプロイト ファイルを入手し、Cisco Security Agent でデフォルトのセキュリティ ポリシー設定を使用することで、これらのエクスプロイトを阻止する効果があることを確認しました。現在サポート中のバージョンである Cisco Security Agent 4.0.3.x、4.5.1.x、5.0.0.x、および 5.1.0.x は、今までに確認されているエクスプロイトを防ぐうえで効果的です。

### 脆弱性の詳細情報

トロイの木馬が添付されているファイルを開くと、Eメールのワーム コンポーネントのコピーがダウンロードされます。この Eメール コンポーネントは、暗号化されています。Eメール コンポーネントは wincom32.sys を投下し、インストールします。wincom32.sys は、ロードされて dll に感染し、services.exe のメモリ プロセスを検索します。dll には、さまざまな UDP ポートをスキャンして、感染したほかのコンピュータとの Peer-to-Peer (P2P) ネットワークを構築し、ダウンロードおよびアップデートを実現する機能が含まれます。この P2P ネットワークは、その後悪意のあるユーザによって使用され、ダウンロードおよび実行するファイルの情報が抽出されます。また、追加ピアの情報を抽出し、収集した情報で独自のピア リスト ファイルをアップデートします。ダウンロードされたほかの既知のコンポーネントは、Win32/Nuwar の変種です<sup>1</sup>。

Win32/Nuwar.N@MM!CME-711 で構成される Eメールには、次の特徴があります。

- 件名 (次のいずれか 1 つ)
  - 230 dead as storm batters Europe.
  - A killer at 11, he's free at 21 and kills again!
  - British Muslims Genocide
  - Naked teens attack home director.
  - Re: Your text
  - Russian missile shot down USA satellite
  - U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel.

<sup>1</sup> 参考

Microsoft: <http://www.microsoft.com/security/encyclopedia/details.aspx?Name=Win32/Nuwar.N@mm>

- 本文
  - 空白
- 添付ファイルの名前
  - FullClip.exe
  - Full Story.exe
  - FullVideo.exe
  - Read More.exe
  - Video.exe

### Cisco Security Agent によるエクスプロイトの阻止

Cisco Security Agent のデフォルト ポリシーには複数のルールが含まれており、エクスプロイトによる被害を回避できます。こうした保護を実行するために、Cisco Security Agent のバイナリを更新したり、デフォルト設定を変更する必要はありません。

デフォルトのセキュリティ ポリシーを適用した Cisco Security Agent では、以下のアクションがブロックされることが確認されています。

- 最近ダウンロードされたアプリケーションによるシステム ファイルのアクセス
- 信頼できないリモート アプリケーションによるシステム ファイルの修正
- バッファ オーバーフローによる、バッファからのシステム機能の実行
- カーネル機能の変更
- さまざまな UDP ポート (UDP ポート 137、53、6121、18559、2581、3620) 上でのクライアントアクセスの開始

図 1 および図 2 に、このテスト結果を示します。

**注:** シスコでは、エージェントをテスト モードにしてエクスプロイトをテストしました。テスト モードでは、悪意のある振る舞いに対し警告を発行します (ブロックはしません)。このテストにより、Cisco Security Agent のデフォルト ポリシーを設定した状態で、エクスプロイトを阻止するすべての方法が監視されることを確認しました。エージェントをプロテクト モード (一般的な動作設定) にすると、最初のルールによってエクスプロイトが阻止されます。エクスプロイトは悪意ある動作を実行する前に処理され、以降のイベントは発生しません。

テストは、Cisco Security Agent のデフォルト ポリシーに対して実施しました。Cisco Security Agent を有効に機能させるために、バイナリまたはポリシーの更新は必要ありませんでした。つまり、文字通りの「Day Zero」保護のテストだと言えます。シスコでは、過去のエクスプロイトおよびワームの場合と同様に、バイナリまたはポリシーの更新を実行することなく、Cisco Security Agent のデフォルト設定によってエクスプロイトを阻止できることを確認しました。表 1 に、Cisco Security Agent のデフォルトのセキュリティ ポリシー設定によって阻止された、過去のワームおよびエクスプロイトの一部を示します。

表 1

エクスプロイト	ワーム	エクスプロイト	ワーム
Bagle	E メール ワーム	SQL Snake	ネットワーク ワーム
Blaster	ネットワーク ワーム	JPEG/GDI+	マルウェア ダウンローダ
Bugbear	E メール ワーム	MyDoom	E メール ワーム
Code Red	ネットワーク ワーム	Nimda	ネットワーク ワーム
Debplot	ネットワーク ワーム	Pentagone/Gonner	E メール ワーム
Fizzer	E メール ワーム	Sasser	ネットワーク ワーム
Gator/Gain	スパイウェア	Sircam	E メール ワーム
Hotbar	スパイウェア	Sobig	E メール ワーム
SQL Slammer	ネットワーク ワーム	Zotob	ネットワーク ワーム

今回のエクスプロイトは、組織のコンピューティング環境およびネットワーク環境に深刻な打撃を与え、発生と変化を続ける攻撃の 1 つにすぎません。このような新しい攻撃を阻止するために重要なことは、デフォルト設定に変更を加えることなく攻撃を阻止できる能力、およびデフォルト ポリシー内のさまざまなルールによる多層型防御の 2 点を実現することです。

図 1 Cisco Security Agent のデフォルト設定による Storm Trojan エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)

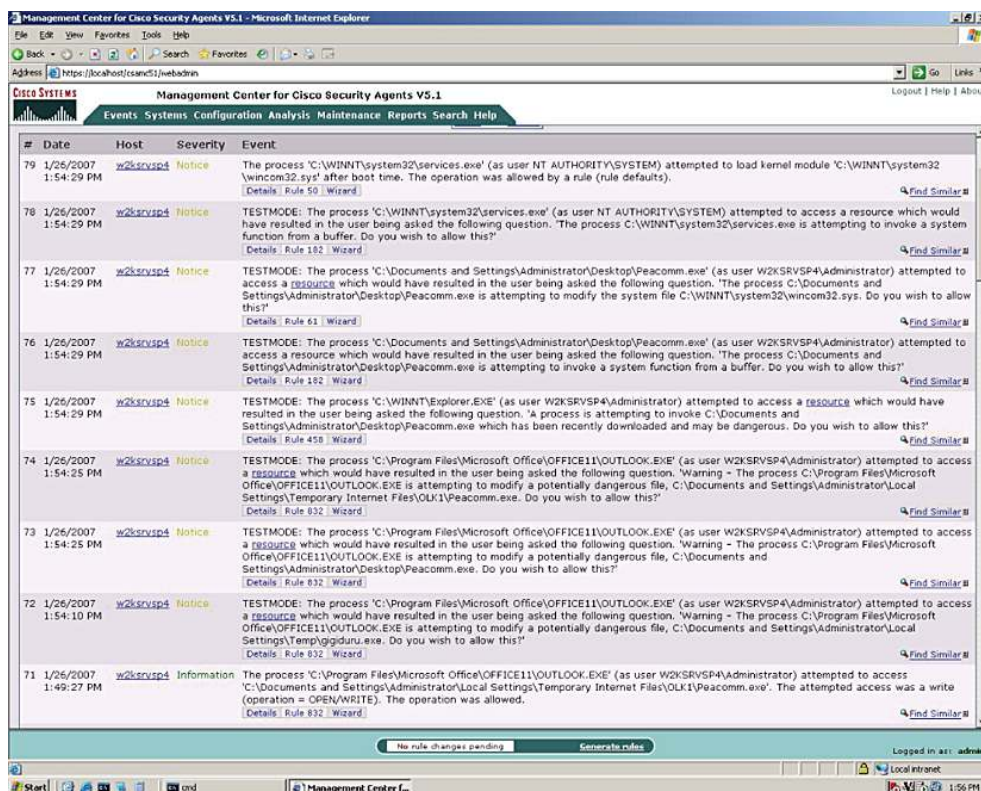
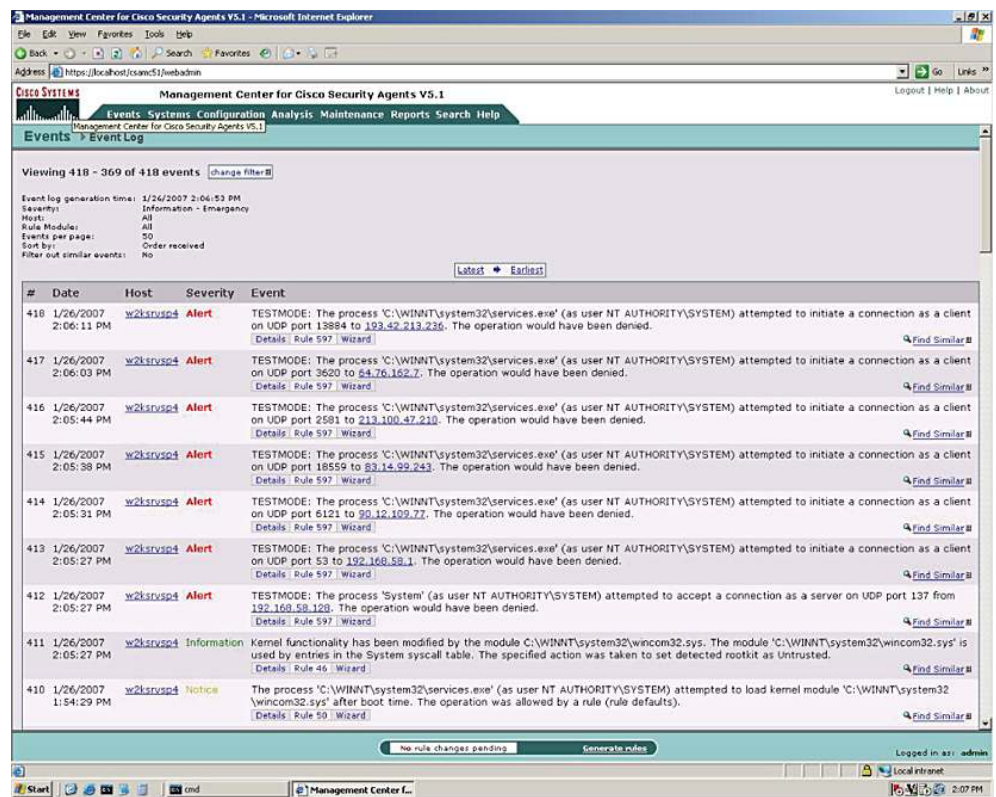


図 2 Cisco Security Agent のデフォルト設定による Storm Trojan エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)



©2007 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

http://www.cisco.com/jp

お問い合わせ先(シスコ コンタクトセンター)

http://www.cisco.com/jp/go/contactcenter

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先