

## Cisco Security Agent および Win32.Rinbot.H エクスプロイト

### 概要

W32.Rinbot.H は、特定の脆弱性を悪用し、ネットワーク共有を介して拡散するワームです。また、感染したコンピュータ上にバックドアを開きます。このエクスプロイトは Windows 2000、Windows 95、Windows 98、Windows Me、Windows NT、Windows XP の各オペレーティング システムを攻撃の対象とします。このワームは 2007 年 2 月 26 日に初めて確認されました。

この脆弱性を悪用したさまざまな攻撃がすでに出回っています。シスコではエクスプロイト ファイルを入手し、Cisco Security Agent の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。現在サポートされている Cisco Security Agent 4.5.x、5.0.x、5.1.x の各バージョンはすべて、現在までに確認されているエクスプロイトに対して有効に機能します。

### 脆弱性の詳細情報

W32.Rinbot.H は Windows プラットフォームに感染するワームです。このワームにはバックドアを開く機能もあり、感染したコンピュータでは、IRC チャネルを利用して悪意あるユーザがバックグラウンドでリモート アクセスすることが可能になります。

ワームは、実行されると次の場所に自身のコピーを作成します。

```
%System%\mstsc.exe
```

次に、以下のレジストリ エントリを作成して Windows の起動とともに実行されるようにします。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ "Terminal Services" = %System%\mstsc.exe"
```

このワームは次の脆弱性を悪用することにより、弱いパスワードで保護されているネットワーク共有を介して拡散します。

Symantec Client Security および Symantec Antivirus の特権昇格の脆弱性 (CID 18107)

Microsoft Windows Server サービスのリモート バッファ オーバーフローの脆弱性 (CID 19409)

UDP ポート 1434 を利用した Microsoft SQL Server ユーザ認証のリモート バッファ オーバーフローの脆弱性 (CID 5411)<sup>1</sup>

### 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することができます。こうした保護を実行するために Cisco Security Agent のポリシーを更新したり、デフォルト設定を変更する必要はありません。

<sup>1</sup> Symantec : [http://www.symantec.com/en/ca/smb/security\\_response/writeup.jsp?docid=2007-022615-1754-99&tabid=1](http://www.symantec.com/en/ca/smb/security_response/writeup.jsp?docid=2007-022615-1754-99&tabid=1)

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、次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。

- 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
- 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 ファイルの修正
- レジストリ キーの変更
- システム メモリの改変

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、悪意のある動作に対して警告を発行します(ブロックはしません)。これにより、Cisco Security Agent のデフォルト ポリシーがエクスプロイトを阻止するあらゆる方法について確認できます。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るため、悪意のある動作を実行する前にエクスプロイトが処理され、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 ポリシーを対象に実施しました。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。次のリストは、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、過去のワームや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 Win32.Rinbot.H エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)

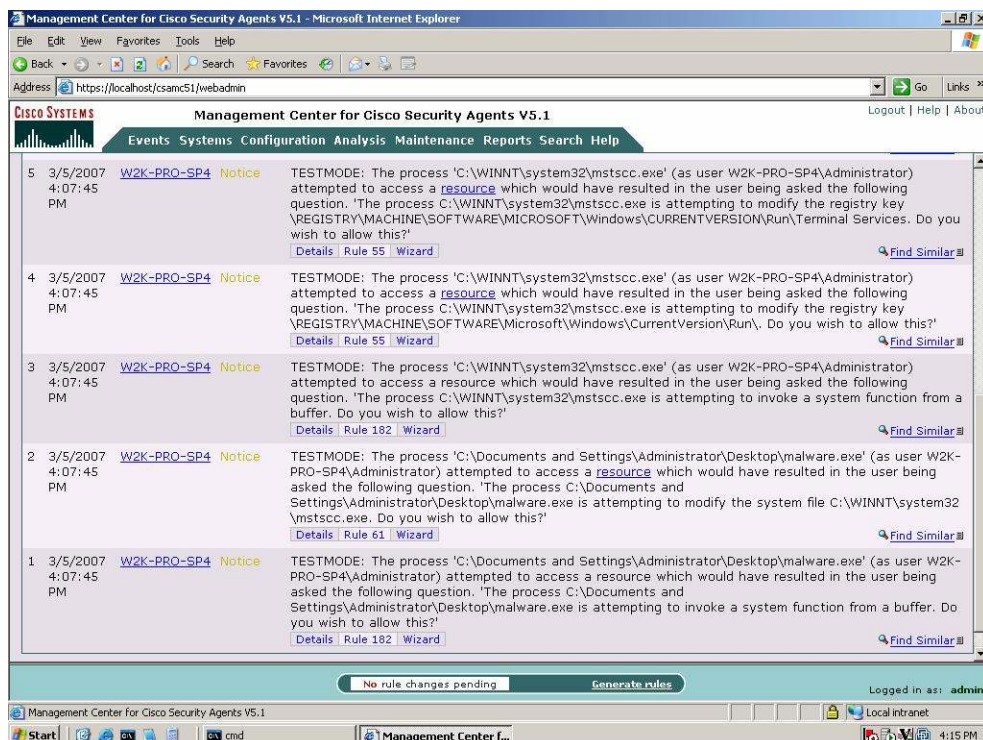
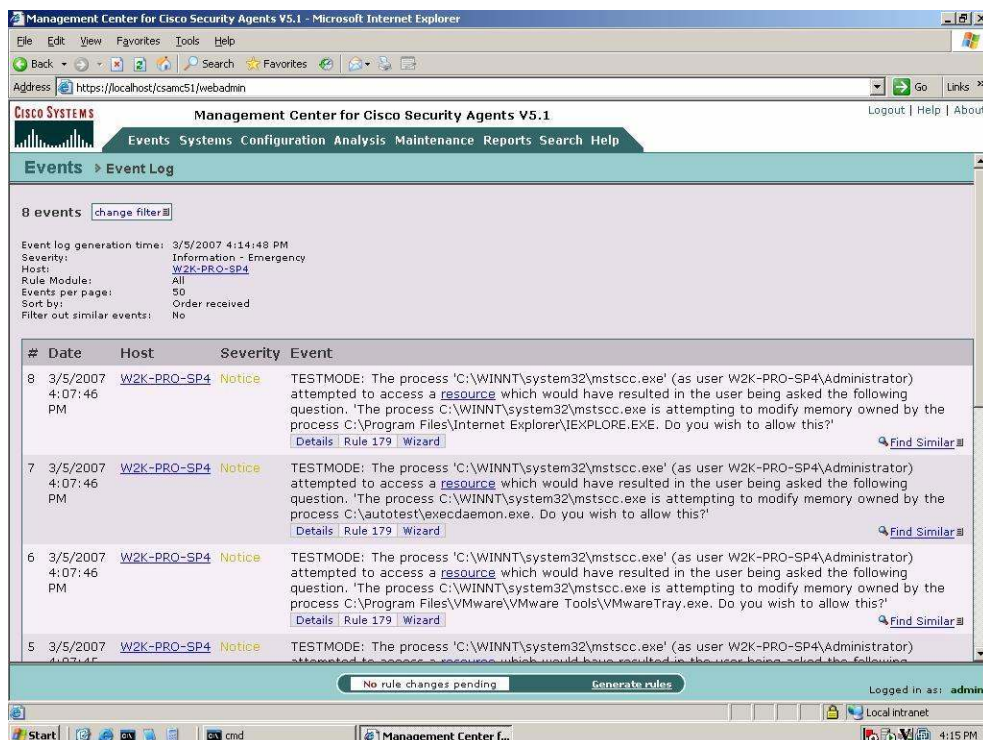


図 2 Cisco Security Agent のデフォルト設定による Win32.Rinbot.H エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)



©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。(0704R)

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**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<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**