

アタックテストサービス エクスプレスご利用のお客様へ

平成 16 年 1 月 28 日  
富士通株式会社

### 新種ウィルス Mydoom ワームについて

拝啓、貴社益々ご清栄の事とお喜び申し上げます。  
平素は格別なるご高配を賜りまして、厚く御礼申し上げます。

この度、マイクロソフト社の Windows システムを攻撃対象とし、メールを仲介し拡散する Mydoom ワーム（または、Novarg、Shimg）について、1月27日付けで CERT-CC より報告されました。

つきましては、下記の方法に従って QualysGuard で本脆弱性が検出されないかをご確認ください。万が一検出された場合には、至急対処のご検討をしていただきますようお願いいたします。

敬具

### 記

#### 【Mydoom ワームの検出】

QualysID 1125 :

「Mydoom ワームの検出 (Mydoom worm detected)」

#### [脆弱性の詳細について]

Mydoom は、.zip ファイルまたは実行ファイルの形式で電子メールに添付され、送信されます。

その添付ファイルを開くと、taskmon.exe と shimgapi.dll として自分自身を直接インストールし、システムスタートアップ時に以下の3つの動作を行うようにレジストリを修正します。

- ・感染したコンピュータに登録されているアドレス帳のユーザへメールを送信します
- ・バックドアを仕掛けて、リモートからそのコンピュータへアクセスを許可します
- ・SCO.com の Web サイトへアクセスをすることにより、一種の DDos 攻撃を行います

#### [確認方法]

以下の方法にて、本脆弱性のみを選択して短時間で診断することが可能です。

- 1) QualysGuard にログインし、"Preferences"->"Options"->"Profiles"より "New Profile" を作成します。
- 2) "Selective Vulnerability Scanning"オプションの「Performing selective vulnerability scanning」を選択し、"Config"を行ないます。  
Find を「Qualys ID」、within を「All」、containing を「1125」として"Search"し、QualysID「1125」を選択して"OK"してください。
- 3) "Scanned TCP Ports"オプションの、"Partial"->"Standard"のチェックをはずし、代わりに"Additional"で、TCP ポート「139,445,3127」を選択します。  
"Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
- 4) "Profile Title"をつけ、最後に"Save"します。
- 5) "Scan"->"Launch Scan"で診断対象の IP を選択し、先程作成した"Options"を選択し、"Start Scan"します。

#### [対処について]

1. readme.txt のプロセスを停止する。
2. システムディレクトリにある taskmon.exe と shimgapi.dll を削除する。
3. レジストリから以下を削除する。  
HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run  
"TaskMon"
4. レジストリ を感染前の状態に復元する。

HKEY\_CLASSES\_ROOT¥CLSID¥{E6FB5E20-DE35-11CF-9C87-00AA005127ED}¥In  
ProcServer32  
"(Default)" の値を %SystemRoot%¥System32¥webcheck.dll にする。

#### [関連文書]

Qualys セキュリティアラート ( 英文 )  
Mydoom Email Worm (1/26)  
<http://www.qualys.com/docs/securityalerts/Qadvise-MyDoomWorm-20040126.pdf>

CERT Advisory CA-2004-02 Email-borne Viruses ( 英文 )  
<http://www.cert.org/advisories/CA-2004-02.html>

-以上-

---

#### お問い合わせ窓口)

富士通株式会社 アウトソーシング事業本部セキュリティサービス統括部  
セキュリティシステム部 アタックテストサービスエクスプレス カスタマサポート担当  
Mail : [qualys-support@support.fujitsu.com](mailto:qualys-support@support.fujitsu.com)  
電話 : 044-754-3353  
<http://segroup.fujitsu.com/secure/service/attacktest-express/index.html>