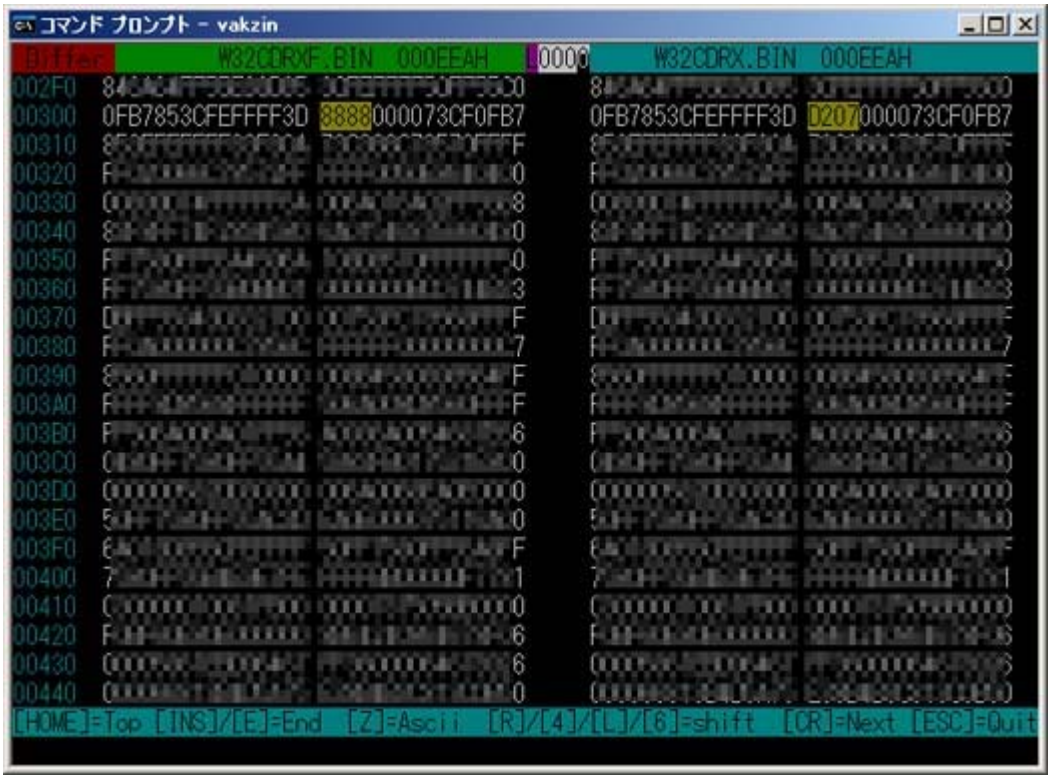
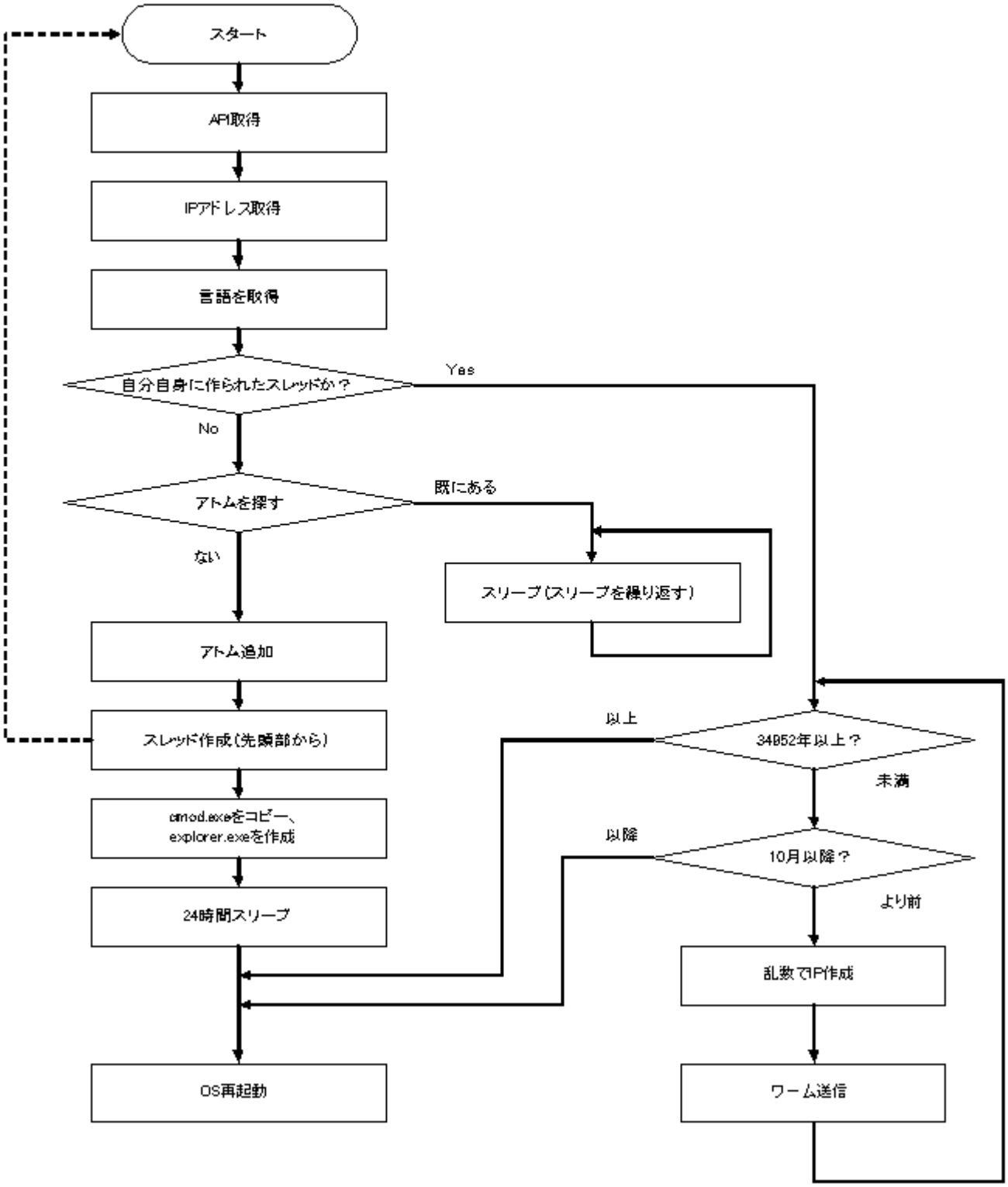
ウィルス解析報告書

ウイルス名	W32/CodeRed.F (Codered.F, W32/Codered2.F)
プログラム名及び容量 (添付ファイル名)	ファイルとして存在しないため不定　(3,818バイト)
種別	Windows環境ワーム
プログラム言語:	アセンブラ
発症環境	WindownNT/2000 IIS(「Index Server ISAPI エクステンションの未チェックのバッファにより Web サーバーが攻撃される (MS01-033)」セキュリティーホールがあること)
発見日時	2003年3月12日
発見場所 (発信地)	不詳
危険性	中程度 (5段階で3から4の間)
発症条件	セキュリティホールのあるWindownNT/2000 IISがインターネット接続されている場合
ウイルスの活動、影響	このウイルスはWindowsNT/2000でセキュリティーホールのあるIISで動作する32ビットのワームである。 2001年8月に流行したCodeRed2ワームの西暦2001年9月末であった稼働期限が、西暦34952年9月末まで動作するように変更されていることが唯一の相違点であり、これによって内容が2バイトのみ異なる。  ワームに感染するとワームはバックドアを作成する。バックドアが作成されるとネットワークを通じて誰でも感染したマシンを操作したり、マシン内のファイルの取得などができるようになる。 ワームに感染したマシンは他のサーバを攻撃し、感染を広める。
被害の規模	不明
亜種、変種の有無	CodeRed, CodeRed2, CodeBlue, CodeGreen と呼ばれる亜種が確認されている。
	ワームはポート80に接続する。セキュリティホールがあるIISならばワームはプログラムとして実行される。 ワームは78000000hまたはBFF00000hにKERNEL32.DLLがロードされているとみなして、このアドレスを調べる。MZシグネチャ、PEシグネチャをチェックし、エクスポートテーブルを参照する。エクスポートテーブル

ウイルス動作概要	のモジュール名がKERNEL32でないときには失敗する。エクスポートテーブルから先頭の8文字がGetProcAとなるAPIを探すことで、GetProcAddressのエントリポイントを求める。これに失敗したときにはハングアップする。 ワームはKERNEL32.DLL、WS2_32.DLL、USER32.DLLからGetProcAddressを使ってAPIを取得する。上記のアドレスをもってKERNEL32.DLLのモジュールハンドルとする。その他のDLLのモジュールハンドルの取得はLoadLibraryAを呼ぶ。 ワームはgethostnameとgethostbynameを呼び出し、マシンのIPアドレスを取得する。ワームはGetSystemDefaultLangIDの戻り値が404h(繁体字中国語、台湾)または804h(簡体字中国語、中国)ならばフラグを立てる。中国語でも香港、シンガポール、マカオではフラグが立たない。 ワームはGlobalFindAtomAを呼び出してアトム「CodeRedII」を探す。見つかったときには既にワームが起動しているとみなしてFFFFFFFFhミリ秒間のSleepを無限に呼び出すループへジャンプする。見つからなければGlobalAddAtomAで探した名前をアトムとして加える。 ワームはGetTickCountを呼ぶ。後にこの値を使ってスレッド毎に乱数の初期値を決める。ワームはフラグが立っているならば600、そうでなければ300のスレッドを作る。 ワームはGetSystemDirectoryAでシステムフォルダを取得し、システムフォルダにあるcmd.exeをc:\inetpub\scripts\root.exeとc:\progra~1\common~1\system\MSADC\root.exeにコピーする。またCドライブのルートにc:\explorer.exeを作成する。同様にDドライブに対しても行う。 ワームは24時間Sleepした後、ExitWindowsExを呼び出してログオフする。 スレッドが実行されると同様にAPIのアドレスを取得する。100ミリ秒間Sleepする。そしてGetSystemTimeを呼び出して34952年以降または10月以降ならばExitWindowsExを呼び出してログオフする。 ワームは乱数でIPアドレスを作る。IPアドレスの各桁は1から254になる。乱数で各桁がIISのIPアドレスと同じになるか、乱数で求めた値になるか決まる。この確率はアトムの名前によって異なる。最初の桁が127と224になることはない。また感染しているIISのIPアドレスになることもない。 1/8 異.異.異.異 1/2 同.異.異.異 3/8 同.同.異.異 ワームは乱数で求めたIPアドレスのポート80に接続する。接続に成功した時にはメモリ内にあるワームのコードとヘッタを送信する。 ワームはスレッドの最初のSleepの呼び出しに戻る。 CまたはDドライブのルートに作られたexplorer.exeが実行されるとウイルスはGetWindowsDirectoryAでWindowsフォルダを取得し、WindowsフォルダにあるEXPLORER.EXEを実行する。 レジストリのHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogonを開く。開くことができたときにはSFCDisableの値をFFFFFF9Dhに変更する。ウイルスはレジストリのHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Rootsを開く。開くことができたときには/Scriptの値を取得して2つのカンマの後の文字列を217に変更する。同様に/MSADCについても行う。また新たに値が「c:\,,217」で「/C」という名前のキーと、値が「d:\,,217」で「/D」という名前のキーを作る。そして10分間Sleepした後、レジストリの設定の最初に戻る。(繰り返す)
感染・発症防止方法	原因となるMS01-033セキュリティホールをふさぐために、Microsoftから供給されるパッチ、またはサービスパックを適用する。
	＜確認＞ 下記のファイルがあれば感染している可能性がある。 C:\explorer.exe C:\Inetpub\scripts\root.exe C:\Program Files\Common Files\System\Msadc\root.exe D:\explorer.exe D:\Inetpub\scripts\root.exe D:\Program Files\Common Files\System\Msadc\root.exe ＜駆除＞ レジストリの HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots

ウイルスの駆除方法	の/Scriptの値の2つのカンマの後の数字を「217」から「204」に戻す。 同様に/MSADCは「217」から「205」に戻す。 また「/C」と「/D」というキーを削除する。 CまたはDドライブのルートに作られたexplorer.exeを削除する。 下記のファイルがあれば削除する。 C:\Inetpub\scripts\root.exe C:\Program Files\Common Files\System\Msadc\root.exe D:\Inetpub\scripts\root.exe D:\Program Files\Common Files\System\Msadc\root.exe Microsoftから供給されるパッチ、またはサービスパックを適用すること。
その他	報告書作成：2003年3月13日現在

W32/Codered.F フローチャート（ワーム本体）



W32/Codered.F フローチャート (explorere.exe)