

ウイルス解析報告書

ウイルス名	W32/Lovegate.C-mm
プログラム名及び容量 (添付ファイル名)	WinRpcsrv.exe, sysshelp.exe, winrpc.exe, WinGate.exe, rpcsrv.exe 78,848バイト (fun.exe, humor.exe, docs.exe, s3msong.exe, midsong.exe, billgt.exe, Card.EXE, SETUP.EXE, searchURL.exe, tamagotxi.exe, hamster.exe, news_doc.exe, PsPGame.exe, joke.exe, images.exe, pics.exe)
種別	32ビットWindows環境用ワーム
プログラム言語:	Visual C++
発症環境	Windows 95/98/ME/NT/2000/XP
発見日時	2003年2月24日
発見場所(発信地)	不詳
危険性	高い(5段階で4)
発症条件	即時
ウイルスの活動、影響	<p>このワームはWindows 95/98/ME/NT/2000/XPで動作する。</p> <p>このワームはサービスプロセスとして実行されるのでタスクの一覧に表示されない。</p> <p>ワームはLSASS.EXEが実行されているときには、このプロセスにワームのコードをコピーし、システムファイルであるLSASS.EXEの一部としてワームコードを動作させる。このため、ファイアーウォールソフトによるポート監視によってセキュリティ違反の通信を発見できない可能性がある。</p> <p>ワームはシステムフォルダにWinRpcsrv.exe, sysshelp.exe, winrpc.exe, WinGate.exe, rpcsrv.exe, ily.dll, Task.dll, reg.dll, 1.dllを作成する。 さらにレジストリを改ざんし、パソコンの起動時にこれらのワームファイルが実行されるようにする。</p> <p>テキストファイルの拡張子の関連付けが変更され、テキストファイルを開くときにワームが起動するようになる。</p> <p>Windowsフォルダのwin.iniのWINDOWSセクションのrun部分が設定され、パソコンの起動時にワームが実行されるようになる。</p> <p>ワームはネットワーク上の他のPCにログインを試みて、成功したときにはウイルスをコピーして実行する。 また、ネットワークで共有されているフォルダに自身をコピーする。</p> <p>ワームはMAPIを利用して、受信トレイにあるメッセージにワームを添付して返信する。 メールが送信された場合にはメーラーの送信済みトレイに送信されたメールが残る。</p> <p>ワームはファイルを検索してメールアドレスを収集し、自身を添付したメールを送信する。この場合、独自にSMTP接続してメールを送信するのでメーラーの送信済みトレイに送信されたメールは残らない。</p> <p>ワームは特定のメールアドレスにメールを送信する。この内容は感染パソコンのユーザー名とホスト名である。</p> <p>ワームはバックドア機能を有しており、このための通信ポート10168と1192に設定する。 外部からコマンドの実行とファイルのUpload、Downloadが可能となる。</p>
被害の規模	日本国内を含む世界各地で、かなり流行している。(2003年2月26日)
亜種、変種の有無	A型からC型までが確認されている。機能的にはあまり大きな差異はない。
	<p>ワームは起動すると表示されないウインドウを開く。 ワームはウインドウが作られたときに次の動作を行う。</p> <p>ワームはワーム自身をシステムフォルダにWinRpcsrv.exeという名前でコピーする。 ワームはコピーしたワームを-start_serverという引数をつけてサービスとして実行する。</p> <p>ワームは引数にinstallを含むならば、上記のコピーと実行を行う。</p>

ワームは引数にremoveを含むならばサービスを終了させる。
ワームは引数にstart_serverを含むならば、メインスレッドをサービス制御ディスパッチャスレッドにする。

ワームはレジストリの
HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥syshelp にシステムフォルダのsyshelp.exeへのパスを設定する。
ワームはワーム自身をシステムフォルダにsyshelp.exeという名前でコピーする。
ワームはワーム自身をシステムフォルダにwinrpc.exeという名前でコピーする。
ワームはレジストリのHKEY_CLASSES_ROOT¥txtfile¥shell¥open¥commandにシステムフォルダのwinrpc.exeへのパスを設定する。

ワームはワーム自身をシステムフォルダにWinGate.exeという名前でコピーする。
ワームはレジストリの
HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥WinGate initialize にシステムフォルダのwinrpc.exeへのパスを引数に-remoteshellをつけて設定する。

ワームは引数にremoteshellを含むならば、LSASS.EXEというプロセスを探す。
プロセスがあるならば、ワームのコードをそのプロセスにコピーしてリモートスレッドとして実行する。

ワームは引数がありremoteshellを含まないならば、その引数で示されているファイルをメモ帳で開く。

ワームはワーム自身をサービスプロセスにする。

ワームはワーム自身をシステムフォルダにrpcsrv.exeという名前でコピーする。
ワームはWindowsフォルダのwin.iniのWINDOWSセクションのrunにシステムフォルダのrpcsrv.exeへのパスを設定する。

ワームは「My I-WORM-and-IPC-20168 running!」という名前のイベントを作る。既に存在しているため作れないときには終了する。

ワームはスレッドを作る。ワームはネットワーク上の他のPCにAdministratorとしてログインを試みる。
パスワードは無しまたはabc123、12345678、abcdefg、abcdef、abc、888888、666666、111111、admin、administrator、guest、654321、123456、321、123を試みる。ワームはログインできたときには、ワーム自身を¥admin¥system32にstg.exeという名前でコピーする。

ワームはコピーしたファイルをそのマシンで「Microsoft NetWork Services FireWall」という名前でサービスとして実行する。

ワームはスレッドを作る。ワームはシステムフォルダにily.dll、Task.dll、reg.dllを作る。これらは同じ内容。
ワームはily.dllを実行する。

ワームはスレッドを作る。ワームはsmtp.163.comのポート25に接続してhello_dll@163.comにメールを送信する。
件名は「!@#%&*()_+」、送信者と受信者はhello_dll@163.comになる。ユーザー名とホスト名が送信される。

ワームはスレッドを作る。ワームはポート10168で待機する。
接続があると、

User Access Verification

Your PassWord:

と送信する。誤ったパスワードを受信するとSorry, Your PassWord Not Right.と送信する。
パスワードとしてxyz123を受信した場合、OK! Please Enter:を送信する。
ワームは受信した内容に応じて、コマンドの実行およびファイルのupload、downloadを行う。

ワームはスレッドを作る。ワームはネットワークで共有されているリソースを再帰的に列挙し、共有されているフォルダを再帰的に検索する。
検索して見つけたすべてのフォルダにワームはワーム自身をコピーする。
そのときのファイル名はfun.exe、humor.exe、docs.exe、s3msong.exe、midsong.exe、billgt.exe、Card.EXE、SETUP.EXE、searchURL.exe、tamagotxi.exe、hamster.exe、news_doc.exe、PsPGame.exe、joke.exe、images.exe、pics.exeの中から乱数で選ばれる。

ワームはカレントフォルダとカレントフォルダのwinpath、レジストリの
HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell

Folders\Personalで示されるパスを「*.ht*」で検索して見つけたファイルを開く。
ファイルの中からmailto:を探し、その後ろをメールアドレスとみなして、ワームを添付したメールを送信する。

ワームはsmtp.163.comのポート25に接続してメールを送信する。送信者はhello_dll@163.comとなる。
件名と本文、添付ファイルは下記の中から選ばれる。

件名:Cracks!
本文:Check our list and mail your requests!
添付:CrkList.exe

件名:The patch
本文:I think all will work fine.
添付:Patch.exe

件名:Last Update
本文:This is the last cumulative update.
添付:LUPdate.exe

件名:Do not release
本文:This is the pack ;)
添付:Pack.exe

件名:Beta
本文:Send reply if you want to be official beta tester.
添付:_SetupB.exe

件名:Help
本文:I'm going crazy... please try to find the bug!
添付:Source.exe

件名:Evaluation copy
本文:Test it 30 days for free.
添付:Setup.exe

件名:Pr0n!
本文:Adult content!!! Use with parental advisory.
添付:Sex.exe

件名:Roms
本文:Test this ROM! IT ROCKS!.
添付:Roms.exe

件名:Documents
本文:Send me your comments...
添付:Docs.exe

ワームはスレッドを作る。ワームはMAPIを取得する。ワームはMAPIを利用して受信トレイの中にあるメールを列挙する。そしてそれらに返信する。
そのメールは下記ようになる。

件名
Re: %元の件名%

本文
%ユーザー名% wrote:
====
%元の本文%
> =====

%s auto-reply:
' I'll try to reply as soon as possible.
Take a look to the attachment and send me your opinion! '
> Get your FREE %s now! <

%sはYAHOO.COM Mailになるか、%s account(%sはメールアドレスの@より右側)になる。

ウイルス動作概要

	<p>DLLについて</p> <p>ワームが作るily.dll、Task.dll、reg.dllのコードの大半はワーム本体と同じである。 ワームはレジストリの HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥Module Call initialize に RUNDLL32.EXE reg.dll ondll.regを設定する。 またワームを1.dllとしてシステムフォルダにコピーする。</p> <p>ワームは上記のポート10168のバックドアを含んでいる。しかしポートは1192を使用し、パスワードは abc123となる。</p> <p>ワームはRundll32.exe Task.dll ondll_serverをサービスとして実行する。</p> <p>ワームは上記の特定のアカウントへのメール送信機能を含んでいる。メールが 送信されるアカウントはhacker117@163.comになっている。</p> <p>ワームは上記のLSASS.EXEというプロセスを探してワームのコードをプロセスにコピーしてリモートスレ ッドとして実行する機能を含んでいる。</p>
感染・発症防止方 法	<p>安全性の確認されていないメール添付ファイルは実行しない。 不必要なフォルダ共有はできる限り避け、必要時のみ共有を行う。</p>
ウイルスの駆除方 法	<p>< 確認 > システムフォルダにWinRpcsrv.exe、syshelp.exe、winrpc.exe、WinGate.exe、rpcsrv.exe、ily.dll、Task.dll、 reg.dll、1.dllのいずれかがあれば感染している。 レジストリのHKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run以下に syshelp、WinGate initialize、Module Call initializeのいずれかがあれば感染している。</p> <p>< 駆除 > システムフォルダにあるWinRpcsrv.exe、syshelp.exe、winrpc.exe、WinGate.exe、rpcsrv.exe、ily.dll、 Task.dll、reg.dll、1.dllを削除する。 またレジストリのHKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run以下の syshelp、WinGate initialize、Module Call initializeを削除する。 Windowsフォルダのwin.iniのWINDOWSセクションのrunにrpcsrv.exeへのパスが設定されているときに は、それを削除する。 テキストファイルの拡張子の関連付けは、元情報が失われているため再度設定しなおすこと。</p> <p>感染パソコンとネットワーク接続されているすべてのWindowsパソコンは、いったんLAN接続を解除す る。 fun.exe、humor.exe、docs.exe、s3msong.exe、midsong.exe、billgt.exe、Card.EXE、SETUP.EXE、 searchURL.exe、tamagotxi.exe、hamster.exe、news_doc.exe、PsPGame.exe、joke.exe、images.exe、 pics.exeというファイル名でサイズが78,848バイトのものはワームなので削除する。</p>
その他	<p>報告書作成：2003年2月27日現在</p>



