Busting the ghost in the machine

機械の中のお化け退治

Kirk P. Arnett, Mark B. Schmidt

この記事ではWindows XP SP2をOSとして持つ2台の新品のDell製PC(Grease とGrime と呼ぶ)へのスパイウェアの感染実験を行い，その結果を述べる．どちらのPCにもSymantec Antivirus 8.1.0.125, Spyware Doctor 3.1(以下Docとする), Spybot Search and Destroy 1.3(以下SSDとする)， Sandra 2005 software をインストールしている．ただし，免疫オプションは感染と実験のプロセスにおいては作動させていない．表1にベンチマークSandra2005を用いて，感染させる前の測定結果を示した．なおSandra2005はSISoftware, www.sisoftware.net/から入手できる．

ステージ1感染．まず，Webメールクライアントを用い，GreaseとGrime上で同一の電子メールを同一のアカウントを用いて読んだ．使用した電子メールは7通であり，それらは典型的なスパムメールを分野別に網羅している．具体的にはRolex Watches, Canadian Pharmacy, Obtain a Diploma, CIALIS Softabs および, 3通の異なるアダルトメールである．

これらの電子メールを同時にそれぞれのPC上で開き, 電子メールにハイパーリンクが含まれていれば，そのハイパーリンクをたどりWebページを表示する．また，リンクが切れていなければ，購買ページにたどり着くまでリンクをたどる．メンバーログインまたは登録が必要な場合はアクセスのために適当なユーザIDとパスワードを作成する. 電子メールアドレスが必要ならば偽装したアドレスを用いる．クレジットカード情報と個人情報は入力しない．しかし，他の指示の場合には購入または登録の直前のステップまでは進む．

例えば，「Order Rolex Online」というタイトルの電子メールに対してはBuyボタンまではリンクをたどっていき，このページで（ここでは名前，住所，クレジット情報が必要であった）ブラウザのバックボタンを使用し，サイト外に出た．

7通のスパムメッセージを一度読んだ後にDocとSSDをスキャンモードで実行し, 以下がスパイウェアとして確認された．

Doc 3.1	SSD 1.3
Mediaplex.com	MediaPlex.com
Pointroll.com 5	entries for
Imrworldwide.com	DSO Exploit
Doubleclick.net	DoubleClick.net
2o7.net	Tribalfusion.com

ステージ2感染．2回目のSandra2005ベンチマークテストの実行によって，感染前後でパフォーマンスに実質的な違いが無いことが分かった．というのも，2%以上の差が表れたテストは無く，しかもいくつかのテストは感染前より良いパフォーマンスを示していたからである．そこで，さらに多くのスパイウェアを得るためにswitchboard.comにアクセスし2台のPC上で同一の街の電話番号を検索した．加えて，いくつかのバナー広告とポップアップ広告にアクセスするという試行を何度か繰り返した．これにより例として，有名な追跡会社のGAIN社から，金魚鉢のスクリーンセーバがスパイウェアと共にインストールされた．

このステージ中では適切な郵便番号を入力したが，他の情報や電子メールアドレスは入力しなかった．ただし，このステージはステージ1ほど2台のPC上での作業が同一であ

表 1　Sandra2005 ベンチマークの一部

		Grease	Grime	
CPU演算ベンチマーク	ドライストーンALU	8162	8168	MIPS
	ウェットストーンFPU	3346	3351	MFLOPS
	ウェットストーンiSSE2	5747	5796	MFLOPS
	モデル		Intel P4 2.8GHz	
	スピード		2.79	
	パフォーマンスレーティング		PR3715 (est.)	
CPUマルチメディアベンチマーク	Integer x8 iSSE2	19704	19691	it/s
	Float x4 iSSE2	26449	26244	it/s
ファイルシステムベンチマーク	ドライブインデックス	47	47	MB/s
	平均アクセス時間	8	8	Ms
	バッファードリード	39	40	MB/s
	シーケンシャルリード	54	54	MB/s
	ランダムリード	38	37	MB/s
	バッファードライト	39	40	MB/s
	シーケンシャルライト	52	54	MB/s
	ランダムライト	37	36	MB/s
	ドライブサイズ	37	37	GB
	フリースペース	15	15	GB
キャッシュ・メモリベンチマーク	複合インデックス	7886	7956	MB/s
	スピードファクタ	11.3	11.2	
	8KB ブロック	24656	24729	MB/s
インターネット接続ベンチマーク	データバンド幅	1294	1432	kB/s
	データレイテンシ	16	15	Ms
	パケットロス	20%	40%	
	平均レイテンシ	16	15	Ms
	最小レイテンシ	15	14	
	最大レイテンシ	16	15	

ったわけではない．なぜなら毎回異なった広告が表示されるため，正確なアクセスの順序やアクセスしたサイトは 2 台の PC の間で異なっているからである．全体で 6 分以内の時間で switchboard.com からリンクされているサイトへのアクセスを行った．

Swichiboard.com とその提携サイトによる第 2 ラウンドの感染の後，SSD と Doc の実行によって Grease と Grime 両方で以下の感染が明らかになった．

Doc 3.1	SSD 1.3
1 Valueclick	102 infections,
2 Advertising.com	including the
1 Avenue A Inc.	tracking cookies
1 Core metrics	
1 DoubleClick	
5 DSO exploits	
11 GAIN.dashbar	
19 GAIN.Gator	
3 HitBox	
1 MediaPlex	

ステージ 3　感染と治療．再度の Sandra2005 ベンチマークテストによって，最初のベンチマークテストと実質的な違いが無いことが分かったため，追加のスパイウェアを入手した．我々はスパイウェア界の「大物」を使用することを決断し，Kazaa と Skype をダウンロードした．これらの製品は有料版ではスパイウェアが無いことを宣伝しているが，我々は無料版からのスパイウェア攻撃に興味がある．これらの無料版はスパイウェアに対して十二分な警告をしているが，いくつかの警告は意図的に隠されていて，ユーザにとって実際よりも利益があるように見えるようになっている．Kazaa や Skype は，それらが持つソフトウェアの機能を使わなくても、ネットワークの帯域を勝手に使う．

最後の SSD と Doc の実行は驚くべき結果を示した．Doc は前回の 3 倍の 384 個の感染を発見し，SSD は動作しなかった．それどころか，SSD は以下のエラーメッセージを表示した．

‘ Error during check: Winpub32 (“Ungultiger Datentyp fur”)’.

ステージ 3 感染のあと，両 PC のウィルスをスキャンし，感染の治療を行った．Symantec Antivirus は 24 分強の間に 125,000 個以上のファイルをそれぞれの PC でスキャンし，ウィルスの感染が 0 であることを確認した. Doc は 384 個の感染の治療（再起動後）を宣言した．その後 SSD もエラーなしで実行できるようになった. SSD は Claria, Kazaa Promotional Items, Joltid P2P Networking, Altnet Software, MyWay を含む 9 つの感染を発見した．SSD はこの後、8 つのスパイウェアの消去を報告した. ただし，5 個の DSO レジストリ変更は再起動後も存在した．

最終ベンチマーク結果

Sandra2005 を用い，Grease と Grim の両方に対して 7 回のベンチマークテストを行った．表 2 は実験前後のディスクアクセスタイムをまとめたものである．感染前は両 PC のファイルシステムベンチマークの平均アクセスタイムは 8 ミリ秒であった．最後の治療プロセスの直前では Grease のファイルアクセスタイムは 20%急上昇し，Grim のファイルアクセスタイムも 11%上昇した．Norton Antivirus と SSD, Doc による治療のあと，アクセスタイムは最初の 8 ミリ秒に戻った．ただし，中間のベンチマーク実行では驚くべきことに，矛盾する結果を示した．

表 2　ベンチマーク比較結果の要約
（ハードディスクアクセス時間）

ファイルシステムベンチマーク 平均アクセス時間	Grease	Grime	感染前と各ステージ間の変化率（%）	
感染前	8	8	–	–
ステージ2感染後	9	8	12.50%	0.00%
ステージ3感染後	10	9	20.00%	11.11%
治療後	8	8	0.00%	0.00%

ベンチマーク測定が信頼できると仮定すると，4 日にわたる感染と実験、そして治療のプロセスにより，以下に示すことがわかった．

- スパイウェアは大きな束になって現れる．これにより，ほんのいくつかのサイトにアクセスしただけで 100 を超える感染が Doc によって発見される結果となった．
- スパイウェアは感染の発見方法や除去方法に違いがある．よって 2 つ以上のスパイウェア除去ソフトが必要である．またインターネットで検索を行えば十分な数の無料･安価なスパイウェア除去パッケージが手に入ることが分かる．
- PC がスパイウェアによって即座に遅くなるとは限らない．実際，スパイウェアは時間をかけて PC を遅くしていき，度重なる活動の後，時間がたてばたつほど PC のパフォーマンスを低下させていく．例えば，同僚の PC が Web 上で非常に遅くなっていることが分かり，しかも彼女の PC ではポップアップが氾濫していたことがあった．そして，その後 700 例を超えるスパイウェアが彼女の PC から発見された．
- あるソフトウェアによって提供されているサービスを使用することで，スパイウェアを追加してしまうことがある．ただし，ソフトウェアの使用がスパイウェアにとって必須の条件ではない．一つの Web サイトにアクセスするだけで複数のスパイウェアに感染してしまうことがある．
- 未来に向けて希望はある！

Kirk P. Arnett
(karnett@cobilan.msstate.edu)
はミシシッピ州立大学経営情報システム学部ビジネス産業校の情報システム学の教授である．
Mark B. Schemidt
(mbschmidt@acm.org)
はミネソタ州セントクラウド大学 G.R.ハーバーガーカレッジオブビジネス，経営コンピュータ情報学部の情報システム学の助手である．

訳：糟谷勇児（早稲田大学大学院・理工学研究科）