特集
マルウェア

マルウェア観察日記 (1)
—静かに進む OS への浸食—

高倉弘喜[☆1]（京都大学）

OS やアプリケーションの自動更新やアンチウイルスソフトが普及した現在でも，マルウェアによる感染報告は後を絶たない．場合によっては，最新シグネチャとアンチウイルスソフトによる防御策ですら突破されてしまうことがある．本稿では，2009 年 10 月と 11 月に発生したバッファオーバフロー攻撃によるマルウェア感染を実例として挙げ，攻撃手法の巧妙さ，検知の難しさについて解説する．なお，本稿では，身近な OS である，Windows を例として挙げているが，他の OS でも同様の傾向にある．

長期出張前日

2009 年 10 月 7 日 16 時頃，ネットワーク・セキュリティワークショップ in 越後湯沢への出張前日．いやーな予感がする．接近中の台風 18 号のことではない．2 日後に控えたマイクロソフトセキュリティ情報の事前通知が，なぜか気になる．台風による交通機関の混乱を想定すると，今日中に越後湯沢入りすべきだ．同僚の上原先生はすでに出発済みと聞き，どうするか思案．

だが，ふと，Windows Vista や 7 のハニーポットを設置したくなった．7 はまだ納品されていなかったため，Vista を選択した．まず大丈夫だろうと，実マシン上に Vista（32bit 版）をインストール．と言いつつも，管理者権限を奪われた際に，ハニーポットと気付いてもらえるよう，管理者権限を持つユーザ honeypotter のみを設定し，PC 名を honeypotter-PC1 と名付けた．越後湯沢の後，ヨーロッパ出張と不在が十日間続き，その間に，事前通知とセキュリティ情報が公開されるので，ServicePack2（SP2）を含めすべてのパッチを適用し，毎日午前 3 時に自動更新するよう設定した．

さらに，IDS の通信遮断ルールを厳しめに，また，一定の条件を満たす通信を観測すれば，携帯電話にメールを送信するように設定した．さらに，監視用サーバとして Mac OS X マシンを設置し，ファイル共有により C ドライブの監視，Remote Desktop Connection（RDC）によるアクセスを設定した．RDC 接続時に Vista の状態がすぐに分かるよう，リソースモニタを最前面に表示させた．

予想通り，翌日の越後湯沢への移動は，困難を極めた．

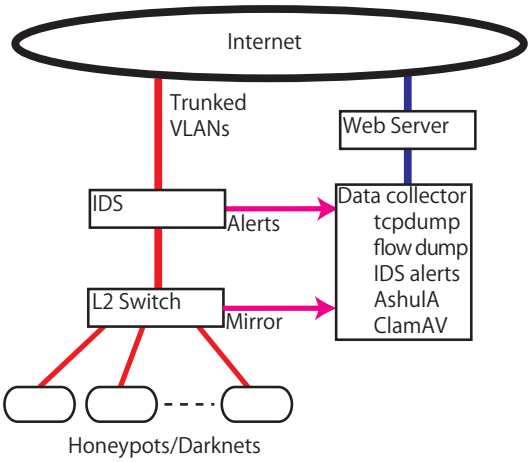


図 -1　システム構成図

[**解説**] 筆者らは，学内・学外のネットワークにさまざまな観測センサを設置している．おおよその構成は図 -1 に示す通りであり，筆者ら自身によるもの，共同研究先から預かっているものも含め，Windows 2000 Server，Windows XP（パッチ適用なし，SP2 相当，全パッチ適用），Mac OS X，各種 Linux，Solaris 8，nepenthes[☆2]，攻撃自動応答型ハニーポット[2] を設置している．また，/24 規模の darknet[1] を 2 つ設置している．

これらへのアクセスは，データ収集サーバにより pcap 形式，および，フロー単位[☆3] で記録され，DBMS（MySQL）によって管理されている．2005 年 8 月の観測開始以来，2009 年末現在，1.7 億フローを超えた．IDS（Symantec 社製 SNS7120）が発する警報，Shellcode 検知システム（AshulA[☆4]）による攻撃コード（以降，exploit

☆1 現在，名古屋大学．
☆2 http://nepenthes.carnivore.it/
☆3 TCP であれば，ヘッダ部分を削除し，ペイロードから再構成したデータ．
☆4 http://www.secure-ware.com/contents/product/ashula.html

Date	SA	DA	Proto.	Size	Exploit	Shellcode ID	IDS/AV
2009/10/10 03:09:02	86.*.*.38: 4544 2009/10/10 03:09:02 (1)	Vista: 445	tcp	854	Exist 2009/10/10 03:09:02(1)	397 2009/10/10 03:09:02(1)	CVE-2009-3103
2009/10/10 03:09:03	86.*.*.38: 4567	Vista: 445	tcp	554	No		
2009/10/10 03:09:07	86.*.*.38: 4606	Vista: 445	tcp	555	No		
2009/10/10 03:09:18	86.*.*.38: 21776	Vista: 49267	tcp	957873	No		
2009/10/10 03:26:05	86.*.*.38: 21776	Vista: 49267	tcp	1143569	No		

図-2　WebUI の検索結果(一部抜粋)

コード)情報，ClamAV によるマルウェア情報も同サーバ上の DBMS によって管理されている．

IDS は inline IPS として構成されており，万一の外部攻撃を阻止する．さらに，TAP☆5 監視ではあるが，10 機種の IDS 等☆6 が大学の対外線を監視しており，その一部は TCP RST によるセッション切断機能を有している．

ハニーポットは，大まかに，仮想マシン上に OS をインストールするもの，実マシン上に OS をインストールするもの，nepenthes に代表される OS の脆弱性を模倣する専用プログラムを搭載するものに分類される．仮想マシンによるものは，システム構築，緊急対応，マルウェア感染後のディスクイメージ取得の容易さからよく使用される．しかし，最近のマルウェアはさまざまな手法で仮想マシンや sandbox 環境☆7 を調査するようになり，ごまかすのは難しくなりつつある．実マシンによるものはハニーポットと気付かれにくいが，OS の管理者権限を奪われた場合，当該マシン単体では緊急対応が取れない難点がある．専用プログラムによるものは，未知の脆弱性を事前に準備しにくく，また，使用 OS のフィンガープリントと脆弱性の組合せが不自然であるなどで，ハニーポットと特定されやすい．攻撃者はハニーポットに気付くと，ゼロデイ攻撃の探知を懸念して避けたり，攻撃の真意を隠すため，無意味な攻撃を集中させ観測機能の麻痺を試みたりする．

ゼロデイ攻撃

●事前通知

10 月 9 日，セキュリティ情報の事前通知が公開された[4]．Windows の緊急が 8 個もある！！　なぜかワクワクしてきた(不謹慎な！)．今回も，XP が狙い目か？

●ピンポイント攻撃着弾

10 月 10 日未明，03 時 10 分頃，携帯電話にメール着信．まずは，iPhone 3G を使って，DB システムの WebUI (図-2) にアクセス．攻撃は 03 時 09 分 02 秒．図-2 中の「日時()」表記は，攻撃元，exploit コード，shellcode☆8 それぞれの初回観測日と現時点の観測件数を表している．(1) ということは，新種だ！　Vista にのみ着弾？　おかしい．他の Windows では，exploit コードの送信前に，攻撃元からセッションを切っている．攻撃対象を絞り込んでいるのか？　IDS は CVE-2009-3103 を狙った攻撃と報告．9 月 7 日公開の攻撃手法[3] で，Vista がターゲットらしい．ゼロデイ攻撃☆9 か？　03 時 09 分 18 秒，攻撃元へのコネクトバック観測．957KB のフローの中身を確認，PE ヘッダ！　プログラムファイル (exe) だ！！！　その後，03 時 26 分 05 秒，二度目のコネクトバックを実行．暗号化されて読めない．かなりマズい．背筋が寒くなる．酔いも吹っ飛んでしまった．

03 時 27 分 50 秒，マイクロソフト社のダウンロードサイトへのアクセス観測．自動更新の設定時刻から 28 分遅れだ．最新状態の Vista なので，マルウェアの活動か？　挙動は通常と同じ，流量的もごくわずかで，IDS による通信遮断の条件は満たしていない．取得したファイルは，Windows6.0-KB936330-X64-wave0.exe，64bit 版 Vista のための SP1 パッチプログラムである．搭載 OS は 32bit 版の SP2 なので，sandbox 環境の検証に間違いない．

03 時 29 分 22 秒，最初の攻撃元とは別の国から，Vista の複数のポートに対し，アクセスを確認．マルウェアが作ったバックドアへ，何らかの指令を送信していると思われる．これも，IDS による通信遮断の条件は満たさず，Vista は応答中．応答は，指令への復唱＋α☆10 な内容の模様．今のところ，このほかの通信はない．

03 時 30 分 36 秒，バックドアへのアクセスが止まった．監視サーバから共有ディスクがアクセス不可に．管理権限を奪われた？　tcpdump を見ると，徐々に応答が悪く

☆5 光ファイバにハーフミラーを挟み込む等により，パケットを抜き出す装置．
☆6 Alaxala，Cisco，FireEye，Juniper，McAfee，paloalto，Secureware，Sourcefire，Symantec との共同研究機材など．
☆7 検証のためにインターネットをシミュレートした実験ネットワーク．
☆8 バッファオーバフロー時に実行される機械語プログラムである．たとえば，Windows shell を起動させるプログラム等がある．
☆9 セキュリティパッチの提供前に行われる攻撃であり，完成した攻撃プログラムが着弾すれば影響回避は不可能である．
☆10 Windows6.0-KB936330-X64-wave0.exe 内の文字列，これも sandbox 環境の検証か？

```
Tension Bandwith Measuring Tool 0.2 - \\TensionTeam 0wnage//

Using 30 threads
Transferred 33164.89 kb in 5.00 s @ 6792.17 kb/sec.
```

図-3　利用可能帯域幅の計測

```
Keylogger:
-------------------------------------------------
Put WinTrustNP.dll was successfull.
Install succesfull.
```

図-4　キーロガーのインストール

なっている．ハングアップか？　監視サーバからRDCでの接続……お，繋がった！　しかし，描画が遅い．設置時に稼働させたリソースモニタは動いている．CPU負荷は0%なのに，メモリ使用率は100%に張り付いたまま．管理権限の奪取には成功したが，メモリを食い潰してしまったようだ．とりあえず，外部への通信を遮断して，一晩放置することにした．もしかすると，近隣のハニーポットにちょっかいを出すかもしれない☆11．とにかく，眠い．

［解説］一般に，管理者権限を奪ったマルウェアは，別のマルウェアの侵入を防止するため，全パッチを適用して脆弱性を塞ぐ．もちろん，自分自身の活動のためのバックドア等は別途構築する．あるいは，自身がsandbox環境に置かれていないことを検証するため，実在する著名なサーバへのアクセスを行う．今回のダウンロード活動は後者と推定される．

解析開始

状況調査

午前の講演を聞きながら☆12，RDC接続で，ハードディスクの状況確認を試みた．しかし，メモリ使用率は100%のままのため，プログラムの起動不能．

10月10日10時35分頃，やむを得ず，Vista再起動．RDC接続．攻撃時刻以降のタイムスタンプを持つフォルダを探索．以下のフォルダのタイムスタンプが，攻撃時刻と一致．フォルダの中身を確認．

C:*Windows**Fonts* フォルダ
改ざんされたと思われるファイルはなかった．

C:*Windows**Installer* フォルダ
ファイルすらなかった．

C:*Windows**Config* フォルダ
4個のファイル，HONEYPOTTER-PC1.txt，xn_ et.exe，lookup.idf の存在を確認した．xn_et.exe のタイムスタンプは2005年2月17日03時17分，ほか2つについては2009年10月10日03時30分であった．

C:*Windows**System32* フォルダ
改ざんされたと思われるファイルはなかった．

C:*Windows**Config* の調査

HONEYPOTTER-PC1.txt を精査．当該ファイルには，

- IPアドレス☆13．
- CPU，メモリ，ハードディスク等のスペック
- Administrator権限を持つユーザ
- Winvnc，Realvncの設定
- OSのインストール日時，稼働時間，バージョン（サービスパックの適用状況）
- IEのバージョン
- 稼働中のネットワークサービス
- 稼働中のプロセス
- サービスプログラムの動作設定

を調査した記録，その次には，図-3の計測結果☆14，最後に，図-4の記録が書かれていた．帯域幅の調査は，64bit版Vista用のSP1プログラムのダウンロードで計測をしたのかもしれない☆15．最後の項目は親切すぎないか？　何かの罠かもしれない．それにしてもログ中のtypoが気になる．

xn_et.exe をstringsコマンドで確認（図-5）．何かのプロセスを起動するプログラムか？　“XNET 1.07”でGoogle様の御神託を受ける．2005年頃公開された，コマンドラインでサービスをコントロールするプログラムらしい．信仰心の薄い私は，“xnet.exe”で再度，伺ってみる．マルウェアの一部のような，OSの一部のような，なんとなく怪しいプログラムの雰囲気がする．このギャップ，なんか不自然である．

lookup.idf は意味不明な文字列の塊であった．

☆11 その後，5時台に，指令元へ1パケットを送信しようとしたところで，力尽きてしまったようだ．
☆12 ごめんなさい．あまり聞いてませんでした．
☆13 仮想マシン上のOSだと，プライベートIPアドレスの場合がある．
☆14 昨晩，サイバーディフェンス社の名和利男氏から，最近のDDoS攻撃請け負いサービスでは，DDoSの帯域幅と継続時間の品質保証を謳っている話を聞いたなぁ．品質保証のための計測か？
☆15 DoS攻撃にはなっていなかったとはいえ，迂闊だったかも．

```
Successfully modified Service info.
Request completed successfully.
Service successfully removed.
Request completed successfully.
Are you sure ? (y/n)
XNET 1.07
Usage : XNET <Start    | Stop    | Restart | Pause     | Continue | List
              Install | Remove | Modify  | Reboot    | Shutdown | Help>
Usage : XNET <Start | Pause | Continue | List> [[\\Server\]ServiceName] [/w:Wait]
```

図-5　xn_et.exe の一部抜粋

C：\Windows\System32 の調査

作業報告 HONEYPOTTER-PC1.txt の最後にキーロガーとして記載されていた，WinTrustNP.dll を捜索する．*C*：*Windows**System32* の下にあった．フォルダのタイムスタンプが攻撃時刻になったのはそのためか．しかし，OS で表示されている当該ファイルのタイムスタンプは 2009 年 4 月 11 日 15 時 27 分 36 秒．あきらかに不自然だ．タイムスタンプが改ざんされている？　当該ファイルを VirusTotal☆16 で検査．結果は，41 ソフト中，検知できるものは皆無．本物のマルウェアであれば，未知のものか？　作業報告ではキーロガーとなっているが，このファイルがキーロガー機能を持ち，かつ，指令受信機能を備えているのだろうか？　指令受信機能を持つ exe ファイルが，タイムスタンプを改ざんされて，存在するのか？　ここまでの情報を，共同研究先等に送付する☆17．

直感的に，現状の感染状況は中途段階と思われ，観測続行を決断した．IDS による通信遮断の条件を強化し，さらに，上流のルータで outbound 方向の流量制限をかけて，万が一 IDS による防御網を突破されても，DoS 攻撃にはならないようにした．

［解説］一般に，インシデント対応のための解析では，インシデント発生直後のハードディスクイメージ，メモリイメージ，CPU の状態を保全することが望ましい．しかし，大学に戻るのは 1 週間以上先で，しかも，次の出張先はヨーロッパ．観測を継続すると，万一の携帯電話通知が間に合わない☆18．ゼロデイ攻撃の可能性が濃厚になったが，ハニーポットを停止して証拠保全すべきか，今後の挙動を追跡するため観察を続行するか悩んだ．

共同研究先からの報告

10 月 11 日以降，共同研究先から報告．産業技術総合研究所の森彰氏☆19 によると，xn_et.exe はサービスプログラムの制御を行うための汎用的なプログラムとのこと．セキュアウェア社の齋藤和典氏によると，攻撃プログラムは 9 月 9 日に Metasploit で公開された攻撃プログラム[7]に含まれる shellcode をそのまま使用しているとのこと．さらに，Windows のバッファオーバフロー対策の 1 つ，DEP（Data Execution Prevention）機能を停止するコードも含まれていると連絡があった．

JPCERT/CC からは，WinTrustNP.dll は確かにキーロガーの機能を持っていると報告があった．

［解説］Windows Vista からはユーザアカウント制御（UAC）により，管理者権限でのプログラム実行が制御されている．しかし，UAC の対象は exe のようなプログラムであり，dll のようなライブラリは含まれていない．何らかのプログラムが WinTrustNP.dll のキーロガー機能を呼び出しても，UAC はユーザに権限昇格の確認を行わない．一方，ライブラリ内の 1 関数を，どのプログラムがどのタイミングで呼び出すのかを特定するのは非常に困難である．そもそも，このキーロガー機能が使われるのかすら特定しにくい．

経過観察

10 月 14 日から，研究打ち合わせのためニースに滞在．

まずは答え合わせ

10 月 14 日，10 月のセキュリティ情報公開．CVE-2009-3103 に該当するのは，MS09-050[5] と判明．MS09-050 は Vista および 2008 Server のみが緊急☆20 に該当し，XP や 7 は対象外．やはり，対象 OS を絞り込んだピンポイント攻撃で，パッチ公開が間に合わなかったゼロデイ攻撃．

☆16 http://www.virustotal.com/ は一般的な 41 のアンチウイルスソフトの対応状況を調査してくれるサービスである．
☆17 セキュアウェア社の野川裕紀氏から「いつの間に Vista を設置したん？」と聞かれたので，「こんなこともあろうかと思って，一昨日ね」と回答した．
☆18 事故の際の責任の所在を明確にするため，学生に監視をしてもらうわけにはいかない．
☆19 総務省・戦略的情報通信研究開発推進制度 (091603006) を共同実施．
☆20 遠隔の第三者による任意のコード実行の可能性がある．

謎の「自動」更新

10月10日以降，Conficker といった以前からの攻撃を観測するが，それ以外に変わった動きはない．嵐の前の静けさか？　それとも，マルウェアプログラムはメモリ上にのみ存在していて，再起動で消滅したか？

現地時間10月16日03時37分（日本時間，同日10時37分），状況が急変，携帯電話にメール着信．ただちに，WebUI で状況を確認．msecn.net の Web サーバに毎秒1回のペースでアクセス．やばい，DoS 攻撃か？

ただちにフローデータ確認．よかった，Vista の更新のためのダウンロードだ．

え？待て，不自然じゃないか！　自動更新の設定は，日本時間の「毎日午前3時」のはず．過去のアクセス履歴を確認したが，更新ダウンロードは確認されなかった[☆21]．自動更新が解除されていた？　ダウンロード開始前に，指令が送られた記録はない．10月10日10時35分頃の再起動，それからほぼ7日後……潜伏期間を経て，マルウェアの活動開始か？　マルウェアが行っているダウンロードだとしても，正規の手順に従っている限り，阻止しない方が良い．これにより，Vista は最新の状態になったが，変だぞ，再起動しない？

［解説］この更新により，Vista のハードディスクの状態は大きく変わった．多くのファイルの更新時刻が変わることは，後日の解析で，大きな支障となる．一方で，更新を阻止すれば，攻撃者にハニーポットと気付かれることになりかねない．

ファイル消滅

現地時間10月16日23時10分（日本時間，翌日06時10分），監視サーバから RDC により接続．*C*:*Windows\Config* フォルダの配下にあったはずのファイルがすべて消滅．ファイル削除？　しかし Config フォルダ自体のタイムスタンプは変化なし．ファイル削除後，タイムスタンプの改ざんか？　それとも rootkit[☆22] が仕込まれたか？　指令の受信，または，マルウェアの追加インストールを疑い，Vista に関する通信をすべて調査．しかし，conficker 等の無害なものを除けば，不審な活動の記録なし．何が起きたのか，皆目見当がつかない．深刻な事態を懸念し，観測継続を断念．Vista をシャットダウン．

フォレンジック解析

ハードディスクイメージ取得

帰国後，まずは，PC を KNOPPIX で起動．USB 外付けハードディスクを接続後，内蔵ハードディスクのイメージ採取．このとき，細かいことではあるが，ミスに気がついた．ハニーポットに使用するハードディスクは，イメージ採取，および，解析の時間短縮のため，必要最小限の容量が望ましい．しかし，出張直前で慌てていたため，60GB のハードディスクを1パーティション構成でフォーマットしてしまっていた．このため，20GB もあれば十分なのに，60GB をまるまるダンプせねばならなくなった．

解析開始

Autopsy[☆23] を使用して，ハードディスクの調査開始．まずは，10月10日の調査で確認された不審な4フォルダを調査．

(1) *C*:*Windows\Fonts* および *C*:*Windows\Installer* フォルダ

ファイルの改ざん，削除の痕跡はなかった．

(2) *C*:*Windows\Config* フォルダ

図-6 によれば，10月10日の調査で発見された4個のファイルは残っており，さらに，

1行目：xn_et.exe ファイルは削除され，復元不能に

2行目：xnet.exe ファイルも削除され，復元不能に

6行目：xnet.exe ファイルが03時29分48秒（CREATED）に新たに作成され，03時30分14秒（CHANGED）に削除された．ただし，META データ[☆24] が5行目と同じで，状態が realloc であることから，xn_et.exe（赤枠）に名前が変わったと推定．

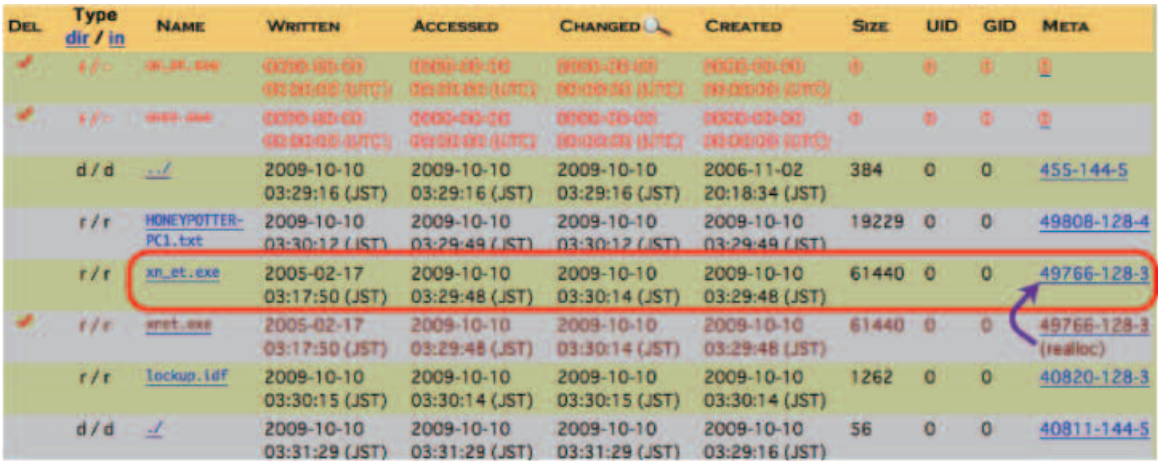
を確認．5行目の xn_et.exe は，OS で表示されるタイムスタンプ（WRITTEN）が改ざんされており，10月10日の調査で見えていた通り表示されるようになっている．

(3) *C*:*Windows\System32* フォルダ

図-7 によれば，redirex.exe，rasstr.dll，msagent.dll，WinTrustNP.dll の4ファイルの変更時刻（青枠）は攻撃時刻であるが，OS で表示されるタイムスタンプ（赤枠）は改ざんされたことを確認．

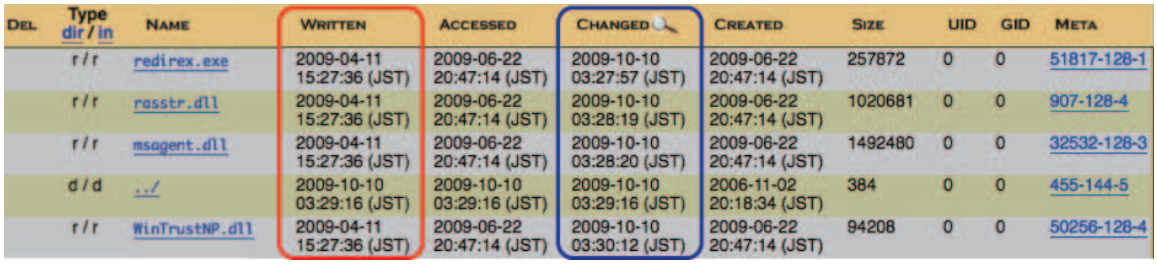
また，「自動」更新により *System32* フォルダに28ファイルが置かれたことも確認．図-8 に示すように，ファイルが置かれた時刻（CREATED）はダウンロードを観測した時間帯に合致する．そのうち，23ファイルは，変更時刻（青枠）が2009年10月17日03時08分とな

☆21 当然，更新データが公開された10月14日も．
☆22 OS の管理権限掌握後にインストールされるプログラムで，プロセス表示でボットプログラムを隠す，フォルダ表示でマルウェアの存在を遮蔽する，更新日時やファイルサイズを偽情報にすり替える等の機能を持つ．
☆23 http://www.sleuthkit.org/autopsy/
☆24 ハードディスク内の位置情報等．



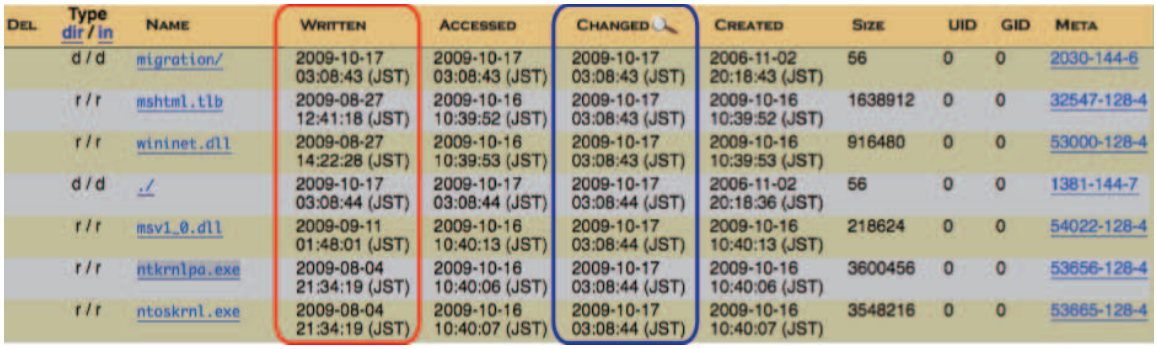
Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	d / d	../	2009-10-10 03:29:16 (JST)	2009-10-10 03:29:16 (JST)	2009-10-10 03:29:16 (JST)	2006-11-02 20:18:34 (JST)	384	0	0	455-144-5
	r / r	HONEYPOTTER-PC1.txt	2009-10-10 03:30:12 (JST)	2009-10-10 03:29:49 (JST)	2009-10-10 03:30:12 (JST)	2009-10-10 03:29:49 (JST)	19229	0	0	49808-128-4
	r / r	xn_et.exe	2005-02-17 03:17:50 (JST)	2009-10-10 03:29:48 (JST)	2009-10-10 03:30:14 (JST)	2009-10-10 03:29:48 (JST)	61440	0	0	49766-128-3
	r / r	xnet.exe	2005-02-17 03:17:50 (JST)	2009-10-10 03:29:48 (JST)	2009-10-10 03:30:14 (JST)	2009-10-10 03:29:48 (JST)	61440	0	0	49766-128-3 (realloc)
	r / r	lockup.idf	2009-10-10 03:30:15 (JST)	2009-10-10 03:30:14 (JST)	2009-10-10 03:30:15 (JST)	2009-10-10 03:30:14 (JST)	1262	0	0	40820-128-3
	d / d	./	2009-10-10 03:31:29 (JST)	2009-10-10 03:31:29 (JST)	2009-10-10 03:31:29 (JST)	2009-10-10 03:29:16 (JST)	56	0	0	40811-144-5

図-6　*Config* フォルダの状況



Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	r / r	redirex.exe	2009-04-11 15:27:36 (JST)	2009-06-22 20:47:14 (JST)	2009-10-10 03:27:57 (JST)	2009-06-22 20:47:14 (JST)	257872	0	0	51817-128-1
	r / r	rasstr.dll	2009-04-11 15:27:36 (JST)	2009-06-22 20:47:14 (JST)	2009-10-10 03:28:19 (JST)	2009-06-22 20:47:14 (JST)	1020681	0	0	907-128-4
	r / r	msagent.dll	2009-04-11 15:27:36 (JST)	2009-06-22 20:47:14 (JST)	2009-10-10 03:28:20 (JST)	2009-06-22 20:47:14 (JST)	1492480	0	0	32532-128-3
	d / d	../	2009-10-10 03:29:16 (JST)	2009-10-10 03:29:16 (JST)	2009-10-10 03:29:16 (JST)	2006-11-02 20:18:34 (JST)	384	0	0	455-144-5
	r / r	WinTrustNP.dll	2009-04-11 15:27:36 (JST)	2009-06-22 20:47:14 (JST)	2009-10-10 03:30:12 (JST)	2009-06-22 20:47:14 (JST)	94208	0	0	50256-128-4

図-7　*System32* フォルダの状況(一部抜粋)



Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	d / d	migration/	2009-10-17 03:08:43 (JST)	2009-10-17 03:08:43 (JST)	2009-10-17 03:08:43 (JST)	2006-11-02 20:18:43 (JST)	56	0	0	2030-144-6
	r / r	mshtml.tlb	2009-08-27 12:41:18 (JST)	2009-10-16 10:39:52 (JST)	2009-10-17 03:08:43 (JST)	2009-10-16 10:39:52 (JST)	1638912	0	0	32547-128-4
	r / r	wininet.dll	2009-08-27 14:22:28 (JST)	2009-10-16 10:39:53 (JST)	2009-10-17 03:08:43 (JST)	2009-10-16 10:39:53 (JST)	916480	0	0	53000-128-4
	d / d	./	2009-10-17 03:08:44 (JST)	2009-10-17 03:08:44 (JST)	2009-10-17 03:08:44 (JST)	2006-11-02 20:18:36 (JST)	56	0	0	1381-144-7
	r / r	msv1_0.dll	2009-09-11 01:48:01 (JST)	2009-10-16 10:40:13 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:13 (JST)	218624	0	0	54022-128-4
	r / r	ntkrnlpa.exe	2009-08-04 21:34:19 (JST)	2009-10-16 10:40:06 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:06 (JST)	3600456	0	0	53656-128-4
	r / r	ntoskrnl.exe	2009-08-04 21:34:19 (JST)	2009-10-16 10:40:07 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:07 (JST)	3548216	0	0	53665-128-4

図-8　rootkit 注入？(一部抜粋)

っている．もちろん，この時刻周辺でダウンロードが行われた記録はない．ここでも，OS で表示されるタイムスタンプ(赤枠)が過去に遡っている！　さらに，*System32* フォルダの中の *migration\WininetPlugin.dll* や *catroot2\srv2.sys* も同様の状態になっていた．

カーネル等に rootkit を仕込まれて，*C*:*Windows**Config* フォルダの配下のファイルを非表示にされてしまったようだ．ここまでの検証で，筆者ら単体の解析では限界があると判断し，マイクロソフト社，NTT 情報流通プラットフォーム研究所，カスペルスキー社にハードディスクイメージを送付することとした[☆25]．その際，60GB のイメージが USB メモリに収容できず，送付に苦労することになった．

[解説](1)については，ファイルの生成・更新・削除がなかったのに，タイムスタンプが攻撃時刻になっているのは謎のままである．

(2)については，NTFS ファイルシステムではファイルやフォルダについて「最終書き込み時刻(WRITTEN)」，「最終アクセス時刻(ACCESSED)」，「MFT(Master File Table)の変更時刻(CHANGED)」，「作成時刻(CREATED)」の 4 つの時刻を記録する．このうち，ユーザが OS を通じて目にする時刻は最終書き込み時刻で

☆25 たまたま，都内某所の飲み会で話題になったのがきっかけ．

Date	SA	DA	Proto.	Size	Exploit	Shellcode ID	IDS/AV
2009/11/10 10:59:20	122.*.*.14: 2167 2009/11/10 10:59:20 (2)	XP-sp2: 445	tcp	969	Exist 2009/11/10 10:59:20(2)	445 2009/11/10 10:59:20(2)	CVE-2009-3103
2009/11/10 10:59:20	122.*.*.14: 2124 2009/11/10 10:59:20 (2)	XP-fp: 445	tcp	969	Exist 2009/11/10 10:59:20(2)	445 2009/11/10 10:59:20(2)	CVE-2009-3103
2009/11/10 10:59:25	122.*.*.14: 2207	Vista-y3:445	tcp	809	No		

図 -9　11 月 10 日の攻撃

あり，悪意あるプログラムは，その存在を察知されにくくするため，最終書き込み時刻を改ざんする．このため最終書き込み時刻と MFT の変更時刻が異なるか否かが重要なポイントとなる．

一般に，ジャーナリングファイルシステムでは新規の書き込みは末尾に追記されるため，削除ファイルを復元されてしまう可能性が高い．証拠ファイルの隠滅のために，xn_et.exe と xnet.exe と同じ名前のファイル☆26 を書き込むことで，追記ではなく，元々のディスクブロックへ上書きさせた可能性が考えられる．

(3) については，10 月 10 日の攻撃時に仕込んだファイルのタイムスタンプを改ざんすることで，マルウェア感染を確認しにくくする目的があったと推定される．また，HONEYPOTTERPC1.txt ファイルにキーローガー “WinTrustNP.dll” のインストールを記載したのは，そのほかの 3 ファイルの存在を隠蔽する囮だったのかもしれない．

なお，10 月 16 日と 10 月 17 日に操作されたファイルについては，解析が完了していない．通常の自動更新であれば，タイムスタンプを 2 カ月以上前に戻すのは不自然だし，ファイル取得後 16 時間ほどの潜伏期間も気になる．可能性として，「自動」更新により取得した最新の exe や dll ファイルに，悪意ある機能を埋め込んだと推定される．さらに，予定にない「自動」更新を行った後，しばらく様子を見ることで，PC 所有者がマルウェア感染に気付いたか様子をうかがっていたのかもしれない．指令通信が存在しないので，Vista 再起動 7 日後，最初の攻撃から 8 日後に活動を開始するよう，タイマーが仕掛けられていた可能性もある．

CVE-2009-3103 攻撃再び？

ハードディスクイメージを採取した 10 月 21 日，Vista をクリーンインストールして，ハニーポットをセットアップ．前回同様，最新パッチを適用し，自動更新も on にする．11 月も Vista に緊急が見つかると良いなどと，不謹慎なことを考えつつ……

今度は XP ？

2009 年 11 月 10 日 10 時 59 分，携帯電話に待望のメール．WebUI（図 -9）を確認．Exploit コード，shellcode ともに初観測．

ん？どういうことだ？　Exploit コードは Windows XP（sp2 : ServicePack 2 相当，fp : 全パッチ適用）にのみ着弾．しかも，IDS は CVE-2009-3103（MS09-050）への攻撃と報告．不自然だ．CVE-2009-3103 の対象は Vista だけのはず．Vista については，Vista っぽい応答を返した直後に，攻撃元から RST パケットを打ち込んでいるので，exploit コードを観測せず．そのため，セッションサイズが小さくなっている．Vista はターゲットではない？　XP に未公開の脆弱性が見つかった？

この exploit コード，攻撃成功後のコネクトバック先とマルウェア取得の手順が分かりやすく書かれている．しかし，実際にはコネクトバックしていない．この exploit コードは不完全で，発症しないようだ．

とりあえず，取得手順を模倣してマルウェア採取を試みた．無事採取成功！　今回の情報も NTT 情報流通プラットフォーム研究所に伝達する．

2009 年 11 月 11 日．11 月のセキュリティ情報公開．XP が緊急，Vista は重要の MS09-065[6] が出ている．これか！

とはいえ，重要も local exploit☆27 による権限昇格が可能な脆弱性であるので，危険性がまったくないわけではない．案の定，11 月 13 日から，Vista へも exploit コード着弾を観測．攻撃者側の調査が甘かったということか．

12 月 4 日．NTT 情報流通プラットフォーム研究所との合同研究会．今回の攻撃で，ダウンロードが成功した場合に実行されるはずだったマルウェアの説明を受けた．tcp.sys ファイルを改ざんし，TCP の half open な状態を 10 個に制限している機能☆28 を解除するプログラムで，

☆26 おそらく元ファイルと同じサイズ．
☆27 当該 PC にアクセスできるユーザが管理者権限を取得できる脆弱性．
☆28 tcp.sys による制限機能は，Windows XP SP2 で導入され，Vista SP2 で廃止された [8]．

ほぼすべてのバージョンの tcp.sys に対応している汎用性の高いマルウェアとのことであった．

ちょっと違和感を感じる．そこまで完成度の高いマルウェアを準備しているのであれば，exploit コードも十分に推敲されたものであるべきと思うのだが……．また，IDS が CVE-2009-3103 と誤検知するよう巧妙な偽装まで施しておきながら，このままでは発症しないことも分かっているはずなのに，なぜ撃ってきたのだろうか？パッチ公開前日までに完成できなかったので，自暴自棄になったのか？

［解説］ゼロデイ攻撃やゼロデイ攻撃前の試作コードに対して，IDS が既知の攻撃として誤報を発することがある．これは，新しい exploit コードが，誤報となったシグネチャの検知パターンと一致するためである．偶然の場合も多いが，攻撃者が意図的に誤検知させている場合もある．

まず，検知パターンそのものを「文字列」として exploit コードに含ませる☆29．実際には，exploit コードがこの「文字列」をプログラムとして使用することはなく，単なるゴミデータである．IDS は，通常，exploit コードの構文解析といった複雑な処理はせず，単に検知パターンがセッション中に含まれているかを照合するだけである．したがって，プログラムとしては意味がない「文字列」でも検知パターンと一致すれば，IDS は警報を発してしまう．

一方，IDS オペレータは，図 -9 中の exploit と shellcode のような情報は知り得ないし，Vista については警報が存在しないので，アクセスが存在し，かつ，攻撃者がこれを回避した事実を知ることすら難しい．このため，XP に関する 2 つの警報を視認しても，過去の攻撃プログラムを使って見当違いの OS を狙った素人ハッカーによる行為と判断してしまう．

結果的に，攻撃者は，exploit コードの精査を回避でき，真の目的を察知されずに済むことになる．

☆29 検知パターンは，snort 等の公開情報から簡単に取得できる．

まとめ

このように，最近のマルウェア感染は巧妙化しており，特に，PC 所有者，セキュリアナリストの心理を読んで，誤判断を誘導する手口も，感染確認，および，事後対応が遅れる要因となっている．また，攻撃者はますます用心深くなっており，攻撃から，感染，活動開始までに長時間をかけるようになった．一方，我々防御側が単独でこれらの活動を追跡・解析することは難しくなっており，研究者や各ベンダそれぞれの得意分野を連携させて，攻撃者の真意の把握や行動を予測することが重要となっている．

参考文献

1) Harrop,W. and Armitage, G. : Defining and Evaluating Greynets (Sparse Darknets) , Proc. of the The IEEE Conf. on Local Computer Networks 30th Anniversary, pp.344-350 (2005).
2) Song, J., Takakura, H. and Okabe, Y. : Cooperation of Intelligent Honeypots to Detect Unknown Malicious Codes, WOMBAT Workshop on Information Security ThreatData Exchange (WISTDE 2008), pp.21-22 (2008).
3) http://archives.neohapsis.com/archives/fulldisclosure/2009-09/0090.html
4) http://blogs.technet.Com/jpsecurity/archive/2009/10/09/3285679.aspx
5) http://www.microsoft.com/japan/technet/security/bulletin/ms09-050.mspx
6) http://www.microsoft.com/japan/technet/security/bulletin/MS09-065.mspx
7) http://www.packetstormsecurity.org/0909-exploits/smb2_negotiate_func_index.rb.txt
8) http://technet.microsoft.com/en-us/library/dd335036(WS.10).aspx

（平成 22 年 1 月 4 日受付）

高倉弘喜（正会員）
takakura@itc.nagoya-u.ac.jp
平成 2 年九大情報工学卒業．平成 4 年同大情報工学修士修了．平成 7 年京大情報工学博士修了．平成 7 年奈良先端助手．平成 9 年京大講師．平成 12 年同大助教授．平成 22 年名古屋大教授（現在に至る）．情報セキュリティ，高信頼ネットワークに関する研究に従事．博士（工学）．地理情報システム学会，システム制御情報学会，ACM 各会員．