uVALUE

MS05-039の脆弱性を悪用した侵害活動の再考

MS05-039と**既知脆弱性**（MS03-026, MS04-011）**の悪用について比較してみよう**

2005/10/24

株式会社日立製作所
Hitachi Incident Response Team
寺田真敏

http://www.hitachi.co.jp/hirt/

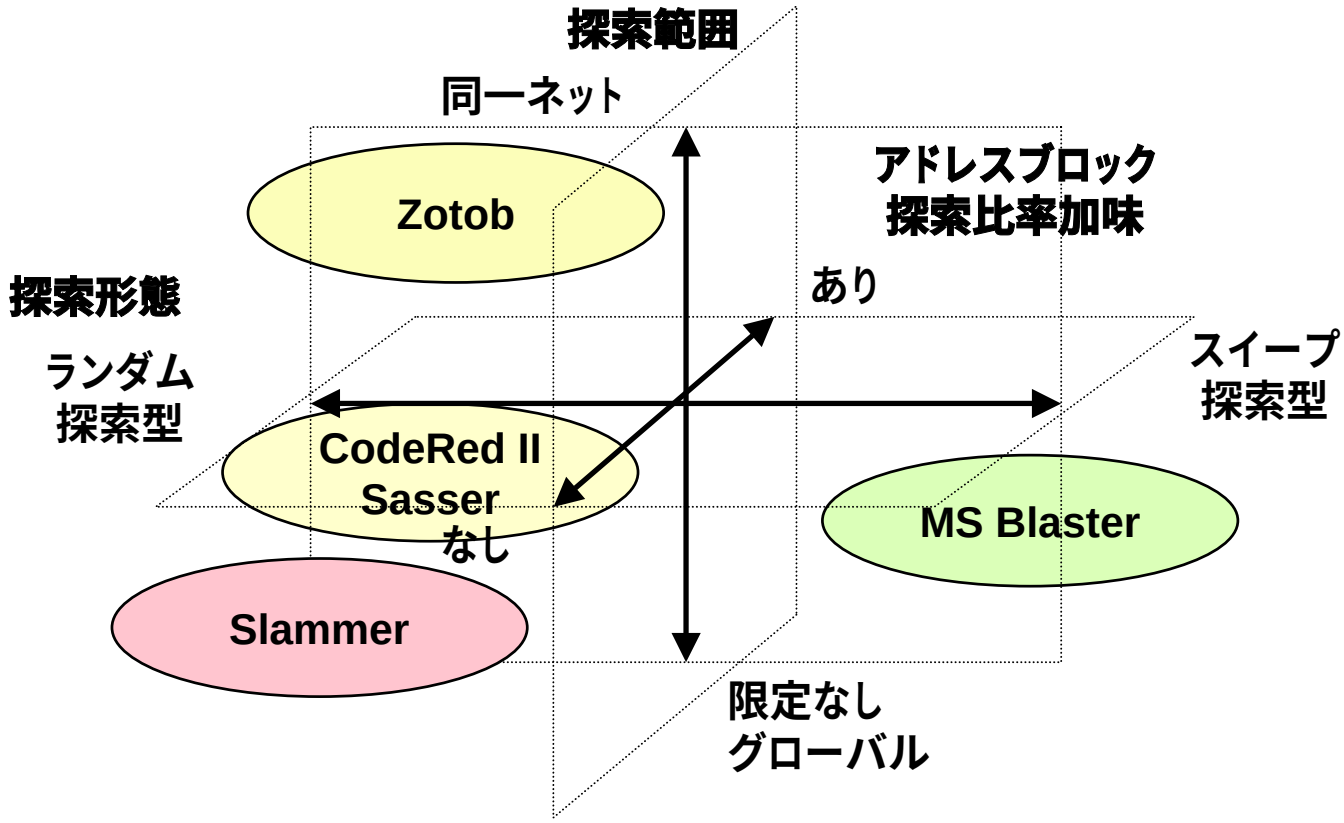
HITACHI
Inspire the Next

1. MS Blaster、Sasser、Zotobの感染活動の比較

	MS Blaster	Sasser.A	Zotob.A
悪用する脆弱性 (公表日)	MS03-026 2003-07-17	MS04-011 2004-04-14	MS05-039 2005-08-10
ベース POC (公表日)	dcom.c 2003-07-27	HOD-ms04011-lsasrv-expl.c 2004-04-29	HOD-ms05039-pnp-expl.c 2005-08-12
ベースワーム	ー	ー	Mytob
発生日	2003-08-11	2004-04-30	2005-08-14
探査方法: 探索比率加味	アドレスブロック 探索比率加味型	アドレスブロック 探索比率加味型	アドレスブロック 探索比率加味型
探査方法: 探索形態	スイープ探索型	ランダム探索型	ランダム探索型
探査方法: 探索範囲	限定なし(グローバル)	限定なし(グローバル)	同一ネット
バックドア活動	・DoS 攻撃 日付がある条件の 場合、”windowsupdate.com” に対して DoS 攻撃を開始	ー	・プロセスの終了 ・DoS 攻撃 ・特定の IRC サーバに接続 ・インターネットからファイルの ダウンロード ・特定の Web サイトを訪問 ・自身のコピーの アンインストール ・システム情報の収集(CPU 速度、メモリ容量) ・自身のアップデートファイルの ダウンロード ・ポート 8888 番を介して リモートコマンドシェルを作成

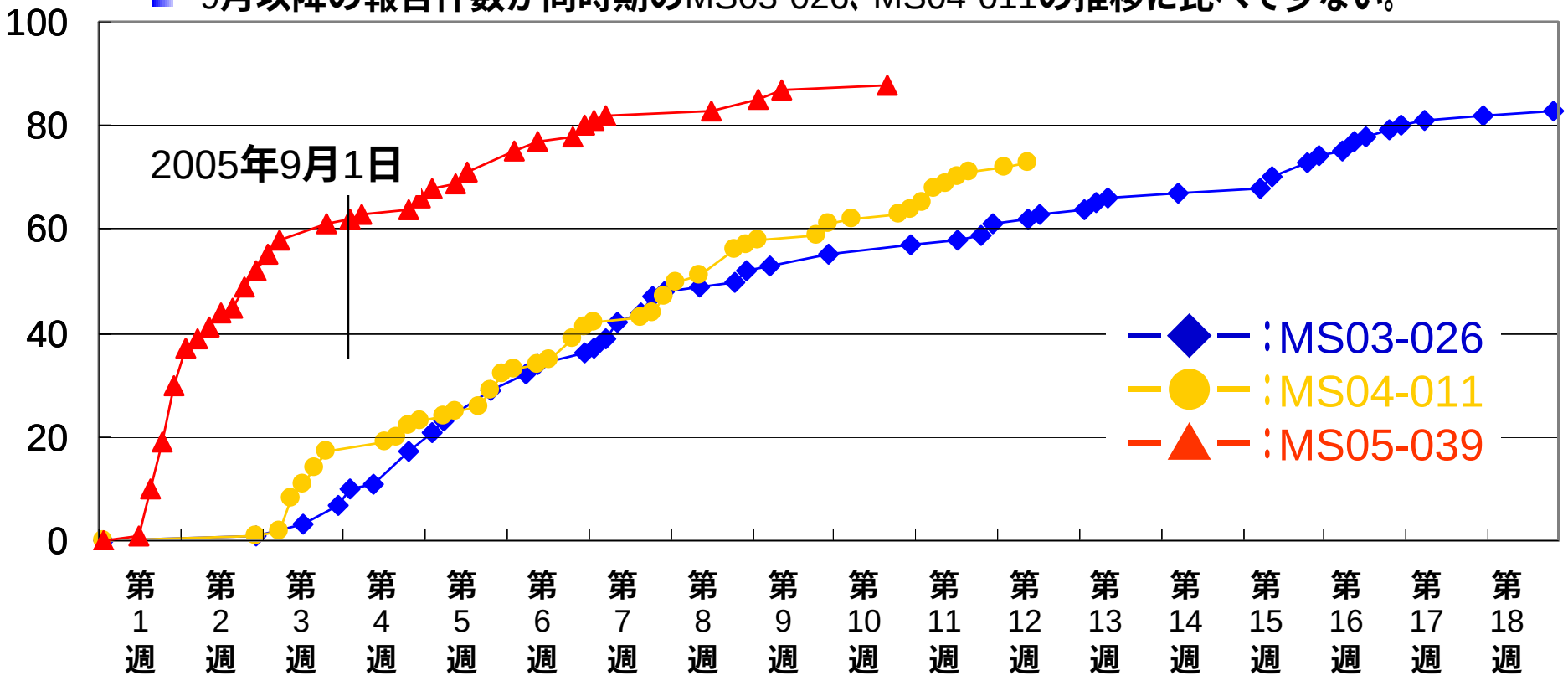
2. MS Blaster、Sasser、Zotobの探索方法の比較

- Zotobの感染活動に伴う探索範囲は、同一ネット(上位2オクテットが同一)に限定されており、このような動作は探索範囲に制限を設けずに流布する既存ネットワークワームCodeRed、Slammer、MS Blaster、Sasserとの大きな違いとなっている。



3. MS03-026、MS04-011、MS05-039を悪用するマルウェアの発生状況

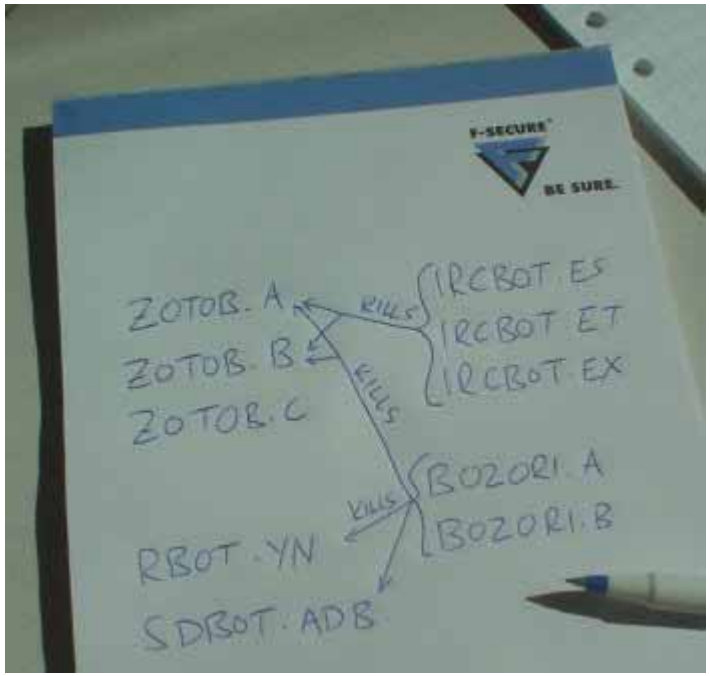
- MS03-026とMS04-011を悪用するマルウェア発生状況は、ほぼ類似した推移をたどっているが、MS05-039については下記の点で推移形態が異なっている。
  - Zotobとその亜種との争いにより、初期段階におけるマルウェア種類数の報告件数がMS03-026、MS04-011に比べて多い。
  - 9月以降の報告件数が同時期のMS03-026、MS04-011の推移に比べて少ない。



グラフの出典
マイクロソフトの脆弱性を悪用するワームやボットの発生度合い
http://www.doi.ics.keio.ac.jp/%7Eterada/fdin/TA05-221A.htm

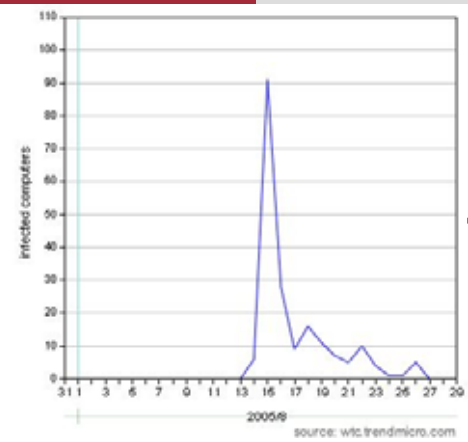
5. MS05-039とネットワークワームの捕食関係

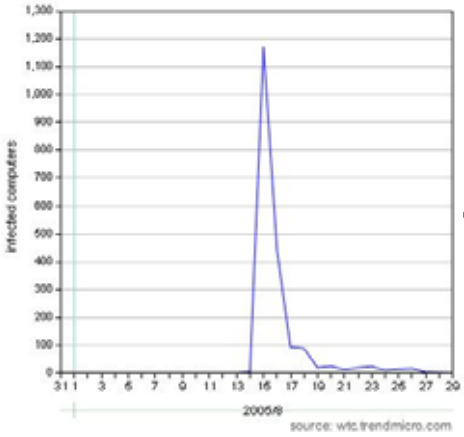
- IRCBOT(Esbot.A, Esbot.B, Esbot.C, Zotob.D)とBOZORI(Zotob.E, Zotob.F)系のボット(捕食者)が、Zotob、RBOT、SDBOTなどの競合相手であるボット(被食者)を削除する(これを捕食と呼ぶこととする)。
  - 被食者の感染報告数は、捕食者の感染報告数増加と共に激減している。
  - 捕食者は、ネットワークワームを攻撃対象としている。すなわち、ネットワークワームを競合相手としている。
  - 捕食者は、マスメール送信型ワームZotob.Cを攻撃対象としていない。
    このため、Zotob.Cの感染報告数は、捕食者の感染報告数変動に影響を受けていない。

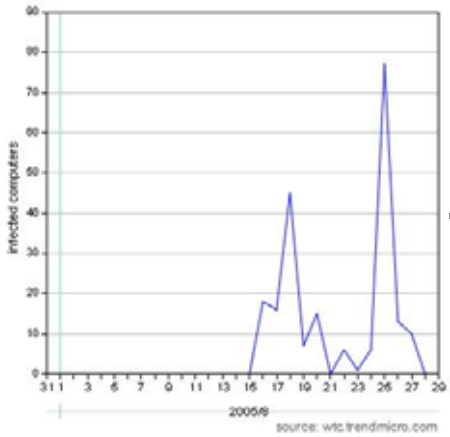


写真の出典
F-Secure: This is not a viruswar, this is a botwar!
http://www.f-secure.com/weblog/archives/archive-082005.html#00000631

MS05-039とネットワークワームの捕食関係







Zotob.A
W32/Zotob.worm
Zotob.A
WORM_ZOTOB.A

Zotob.B
W32/Zotob.worm.b
Zotob.B
WORM_ZOTOB.B

Zotob.C
W32/Zotob.worm.c
W32.Zotob.C@mm
WORM_ZOTOB.C

RBOT.YN

SDBOT.ADB

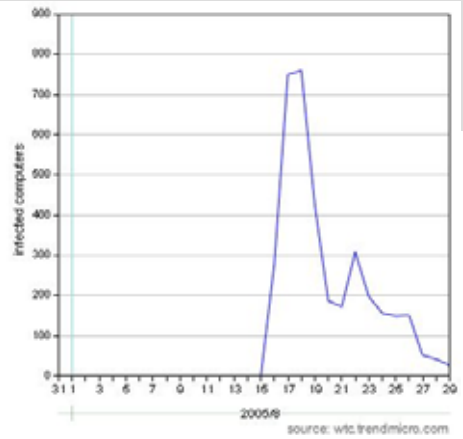
IRCBOT.ES
W32.Esbot.A
WORM_ESBOT.A

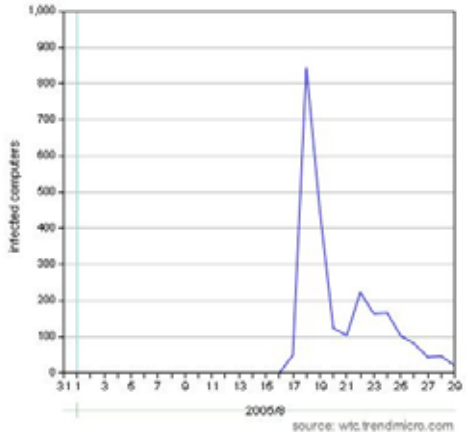
IRCBOT.ET
W32.Zotob.D
WORM_ZOTOB.D

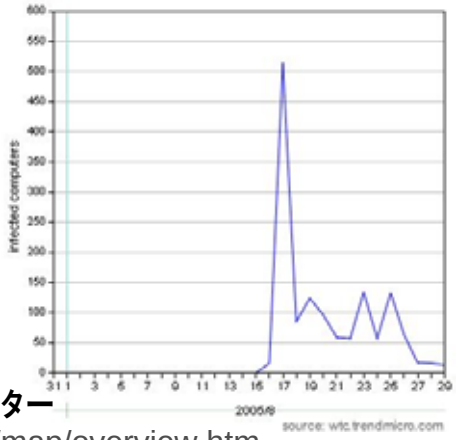
IRCBOT.EX
W32.Esbot.B
W32.Esbot.C
WORM_ESBOT.C

BOZORI.A
W32.Zotob.E
WORM_RBOT.CBQ

BOZORI.B
W32/Bozori.worm.b
W32.Zotob.F
WORM_ZOTOB.F



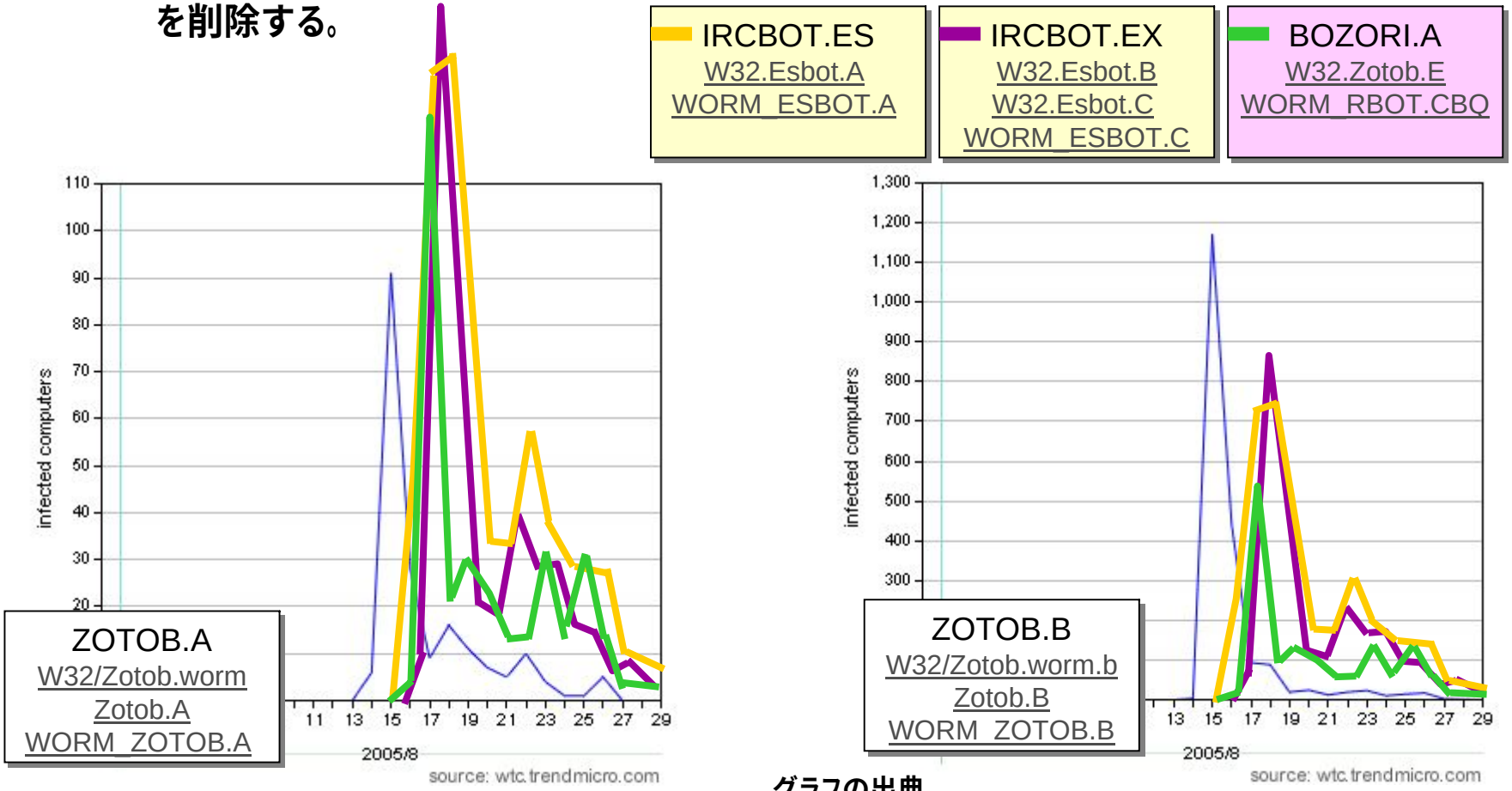




グラフの出典
トレンドマイクロウイルストラッキングセンター
http://www.trendmicro.com/jp/security/map/overview.htm

5. MS05-039とネットワークワームの捕食関係（一部拡大）

- **被食者の感染報告数は、捕食者の感染報告数増加と共に激減している。**
  - IRCBOT(Esbot.A, Esbot.B, Esbot.C, Zotob.D)とBOZORI(Zotob.E, Zotob.F)系のボット(捕食者)が、Zotob.A、Zotob.B、RBOT、SDBOTなどの競合相手であるボット(被食者)を削除する。



グラフの出典
トレンドマイクロウイルストラッキングセンター
http://www.trendmicro.com/jp/security/map/overview.htm

6. まとめ

- バックドア活動
  - バックドア活動の主体が、DDoS攻撃ではなく、侵害活動のインフラ構築、すなわち、ボットネット構築に移行している。
- 感染先探索活動
  - 感染活動は、探索範囲に制限を設けずに流布する形態ではなく、探索範囲を限定して流布する傾向にある。これは、US-CERTから報告されているTargeted Trojan Email AttacksやスピアフィッシングとΜ様であり、侵害活動がより見えにくくなって行くことが予想される。また、MS05-039を悪用するマルウェア種類数の報告件数が9月以降あまり増加していないことと合致している。
- 攻略コードの取り込み期間の短縮化
  - SasserとZotobのいずれも、攻略コードが公開されてから取り込まれるまでの期間は2日間ほどであり、マルウェアの作成が手順化ならびにモジュール化されつつあると類推される。
- 活動エリアの確保
  - 代表的な捕食活動としては、NetskyとBeagleがあるが、表立って報告されたものはあまり多くはない。今回の捕食活動は、侵害活動のインフラ構築、すなわち、ボットネット構築など活動エリアの確保とも関係していると考えられる。

uVALUE

END

MS05-039の脆弱性を
悪用した侵害活動の再考

2005/10/24

株式会社日立製作所
Hitachi Incident Response Team
寺田真敏

HITACHI
Inspire the Next