

Codered3 ワームの感染先探索特性の検討 Rev.1

寺田真敏

terada@doi.ics.keio.ac.jp

慶應義塾大学 大学院 理工学研究科

〒223-8522 神奈川県横浜市港北区日吉 3-14-1

1. はじめに

本メモは、「Sasser.C ワームの感染先探索特性の検討」の追加検討であり、CodeRed3 ワームを対象に実機での感染先探索特性の検証をおこなった。

CodeRed3 ワームは、2003 年 3 月に発見されたネットワーク型ワームであり、コードそのものはオリジナルの CodeRed II と 2 バイトしか異なる。この 2 バイトは、CodeRed II に設定されていた稼働期限 2001 年 9 月末が、CodeRed3 では稼働期限 34952 年 9 月末まで動作するよう変更されたことによる。したがって、CodeRed II と CodeRed3 の感染探索特性は同一であり、本メモでの検証は CodeRed II にも当てはまる。

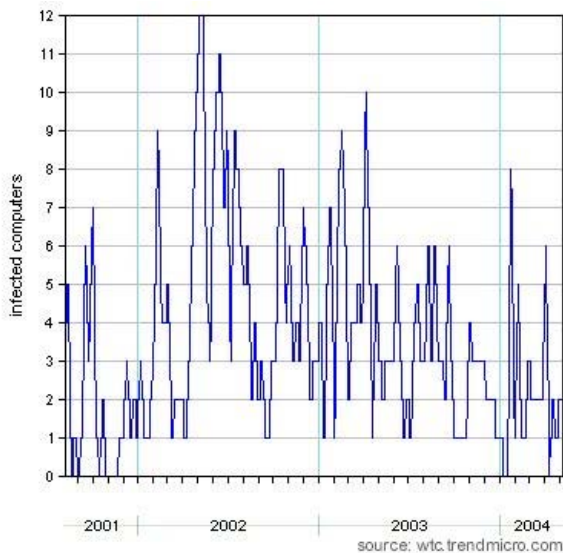


図 1.1 CodeRed II のコンピュータ感染状況
出典:トレンドマイクロ

CodeRed3 ワームのコード解析に基づく感染先探索特性はいくつかのベンダから提供されている(表 1.1)。このコード解析によれば、感染先 IP アドレスの生成は次の通りである。

- 感染PCのIPアドレスブロック以外でランダム(異.異.異.異) : 12.5%
- 下位 3 オクテットがランダム(同.異.異.異) : 50%
- 下位 2 オクテットがランダム(同.同.異.異) : 37.5%

表 1.1 CodeRed3 ワームの感染先探索特性

情報提供元	探索特性の情報(抜粋)
ネットワークアソシエーツ	W32/CodeRed.f.worm The worm tends to probe nearby systems with probability 50% (4/8) - same Class A net (255.0.0.0) 37.5% (3/8) - same Class B subnet (255.255.0.0) 12.5% (1/8) - random
シマンテック	CodeRed.F 言語設定が中国語(台湾あるいはPRC)の場合はスレッドを 600 個作成し、それ以外の場合はスレッドを 300 個作成します。これらのスレッドはランダムな IP アドレスを生成します。生成された IP アドレスは次の感染対象となる Web サーバーを探すために使用されます。
トレンドマイクロ	CODERED.F 各スレッドはそれぞれランダムな IP アドレスを作成し、セキュリティホールを狙った HTTP アクセスでワームのコードを送信します。ワームがアクセスした IP アドレスにセキュリティホールを持った IIS サーバーが存在した場合、ワームに侵入されてしまいます。
eEye Digital Security	CodeRedII Worm Analysis the worm will 1/8th of the time generate a random IP not within any ranges of the local IP Address. 1/2th of the time, it will stay within the same class A range of the local IP Address 3/8th of the time, it will stay within the same class B range of the local IP Address finally, use this last byte to gen a 1st octet.

商品名称等に関する表示
本メモに記載されている会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

情報提供元	探索特性の情報(抜粋)
@police	<p>W32/CodeRed.F 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。この確立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。</p> <p>1/8 異・異・異・異 1/2 同・異・異・異 3/8 同・同・異・異</p>

2. CodeRed3 の感染先探索特性に関する動作確認

本章では、感染先探索特性の動作知見の情報収集を目的として、実験環境下での動作確認をおこなった。

2.1 確認環境

(1) 感染 PC(wormPC)とモニタ装置(monitor)

- 感染 PC(wormPC)

VMware Workstation 4 上で稼動する Microsoft Windows 2000 Server (SP 適用なし) 環境を構成した。感染 PC に対して CodeRed3 が感染時に送出するパケットを送信した。

- モニタ装置(monitor)

Linux 上の tcpdump を使用して、CodeRed3 ワームの送出するパケット(宛先ポート番号 80/tcp)をモニタリングした。

(2) ネットワーク

Sasser.C ワームの実機検証と同様に、図 2.1 に示すネットワークを構成した。

- 一番小さなサブネットワークを構成する (Netmask=255.255.255.252)。
- 感染 PC の DefaultRoute としてモニタ装置の IP アドレスを設定する。

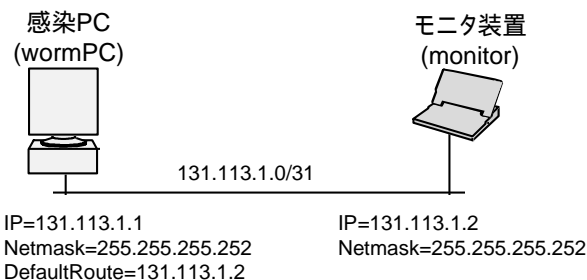


図 2.1 動作確認に使用したネットワーク構成

2.2 動作確認結果

感染 PC の IP アドレスとして、表 2.1 に示すグローバル IP アドレスを設定することで感染先探索特性を調査した。

表 2.1 IP アドレスとモニタリングパケット数

設定 IP アドレス	モニタリングパケット数(件)
プライベート=未実施	-
グローバル=131.113.1.1 DNSによる名前解決なし[b]	18895

(1) 感染 PC のパフォーマンス(CPU 使用率)

感染 PC は CodeRed3 のパケットを受信すると、そのパフォーマンス(CPU 使用率)は一時的に 100%となるが(図 2.1)、以降は数%の状態を維持する。

CodeRed3 パケット受信

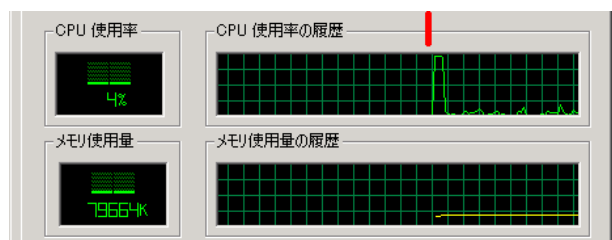


図 2.2 感染 PC のパフォーマンス(CPU 使用率)

(2) モニタリングパケット数

実機検証において、「システムのシャットダウン」を示す警告ダイアログが挙がることはなかった。モニタリングパケット数は 4 分弱で約 19000 パケットに達した。表 2.1 のモニタリングパケット数は、取得したパケット数である。

なお、本メモにおいて比較検討を行なう際にはモニタリングパケット数を観測開始から 10000 パケットに限定する。

2.2.1 経過時間毎の探索 IP アドレスの分布

経過時間毎の探索 IP アドレスの分布(図 2.3)では、横軸に CodeRed3 感染以降の経過時間、縦軸に送出されたパケットの宛先 IP アドレス範囲(0.0.0.0 ~ 255.255.255.255)を示している。

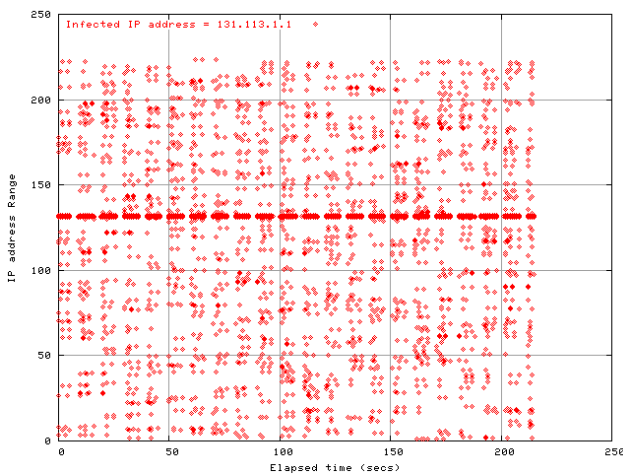
b) 感染PCのIPアドレスをDNSに登録していない。感染PCには利用可能なDNSサーバを設定していない。

- 動作確認の範囲においては、感染 PC に設定した IP アドレスの近接範囲(IP アドレスの先頭から 1~2 オクテットが同一の IP アドレスであり、131.x.x.x,131.113.x.x)に探索範囲が集中している以外には、探索の規則性は見受けられない。

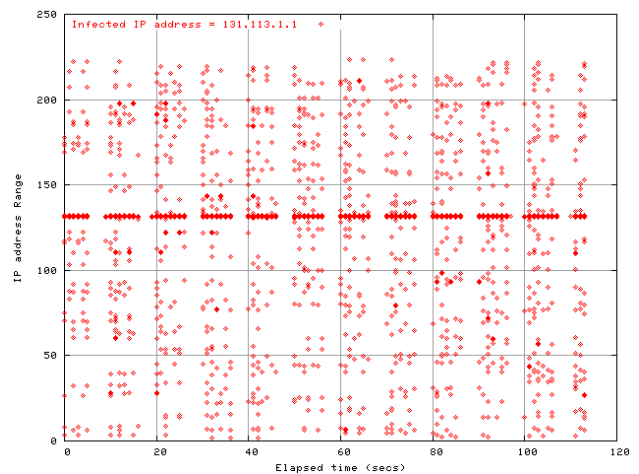
2.2.2 上位 1 オクテットを対象とした探索 IP アドレスの分布

先頭から 1 オクテットを対象とした IP アドレスの分布(図 2.3)では、横軸に探索対象となる宛先 IP アドレスの先頭から 1 オクテットの IP アドレス範囲(000 ~ 255)、縦軸に送出されたパケット数を示している。

- 動作確認の範囲においては、探索 IP アドレスとして、ループバックアドレス(127.x.x.x)、IP マルチキャストアドレス以降(224 ~)を持つパケットは送出されていない。
- 探索 IP アドレスの発生割合は、コード解析の結果に沿っている(図 2.6)。
- 上位 1 オクテットが合致しない IP アドレスに対する探索比率の平均値は、Sasser.C (平均:約 21 パケット) にくらべ約 1/4 になっている(表 2.2)。



全モニタリングパケット

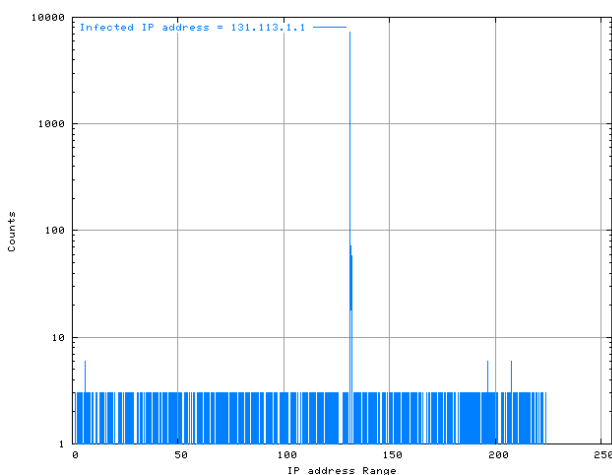


000

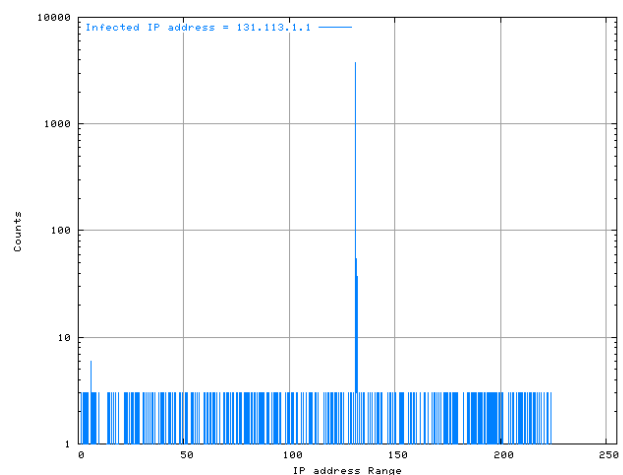
観測開始から 10000 パケット

255

図 2.3 経過時間毎の探索 IP アドレスの分布



全モニタリングパケット

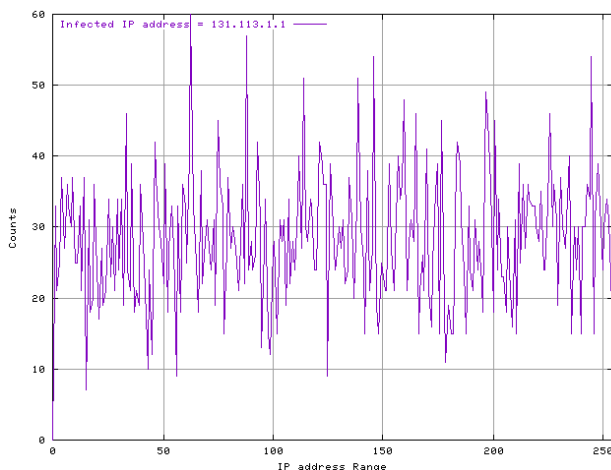


000

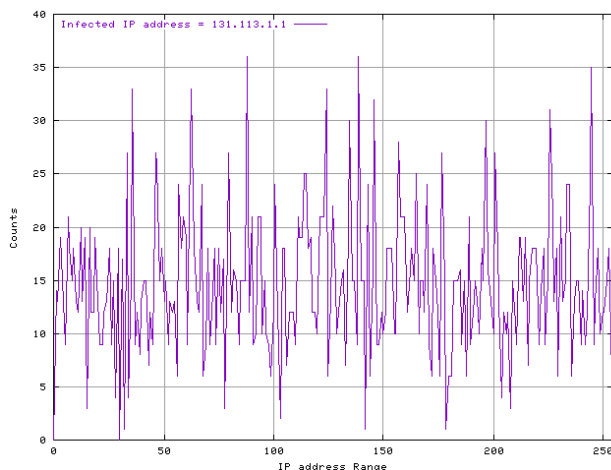
観測開始から 10000 パケット

255

図 2.4 上位 1 オクテットを対象とした探索 IP アドレスの分布

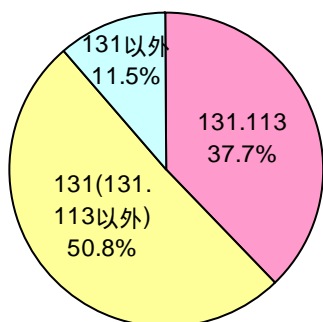


全モニタリングパケット



観測開始から 10000 パケット

図 2.5 上位 2 オクテット(131.113)を対象とした探索 IP アドレスの分布



	実機検証	コード解析
上位 2 オクテットが同一(同.同.異.異)	37.7%	37.5%
上位 1 オクテットが同一(同.異.異.異)	50.8%	50%
上記以外(異.異.異.異)	11.5%	12.5%

図 2.6 探索 IP アドレスの発生割合 (観測開始から 10000 パケットの分布)

2.2.3 上位 2 オクテットが同一の探索 IP アドレスの分布

上位 2 オクテットが同一の探索 IP アドレスの分布(図 2.5)では、横軸に探索対象となる宛先 IP アドレスの先頭から 3 オクテット目の IP アドレス範囲(131.113.000 ~ 131.113.255)、縦軸に送出されたパケット数を示している。

表 2.2 動作確認結果の基本統計量

(上位 1 オクテットの探索 IP アドレスの分布)

感染 PC の IP	IP=未実施	IP=131.113.1.1
平均(パケット数)	-	5.17
標準誤差	-	0.25
中央値	-	6
最頻値	-	3
標準偏差	-	3.83
分散	-	14.7
範囲	-	21
最小	-	0
最大	-	21
合計(パケット数)	-	1149

注 1) 観測開始から 10000 パケットを用いて算出

注 2) 基本統計量算出にあたり、以下のデータを除外している。

- IP アドレスの上位 1 オクテットが感染 PC と同一の IP アドレス範囲である 131.x.x.x
- ループバックアドレス(127.x.x.x)
- IP マルチキャストアドレス以降(224~)

表 2.3 動作確認結果の基本統計量

(上位 2 オクテットが同一の探索 IP アドレスの分布)

感染 PC の IP	IP=未実施	IP=131.113.1.1
平均(パケット数)	-	14.7
標準誤差	-	0.42
中央値	-	15
最頻値	-	15
標準偏差	-	6.76
分散	-	45.76
範囲	-	36
最小	-	0
最大	-	36
合計(パケット数)	-	3772

注 1) 観測開始から 10000 パケットを用いて算出

- 動作確認の範囲において、パケットが送出されなかったアドレスブロックは 131.113.xxx の場合に3ブロック(131.113.0, 131.113.030, 131.113.255)となっている。
- 上位2オクテットが同一のIPアドレスに対する探索比率の平均値は、Sasser.C (平均: 約10パケット) にくらべ、約1.4倍多い。

3. まとめ

本メモでは、CodeRed3 ワームの流布特性について実機での検証をおこなった。

(1) CodeRed3 ワームの感染先探索特性

- CodeRed3 ワームは、アドレスブロック探索比率を加味して常に探索 IP アドレスをランダムに選択する(アドレスブロック探索比率加味型&ランダム探索型)タイプに属する(図 3.1)。
- アドレスブロックの探索比率は、コード解析の結果に沿っている(図 2.6)。
- ループバックアドレス(127.x.x.x)、IP マルチキャストアドレス以降(224~)は、探索範囲から除外されている。

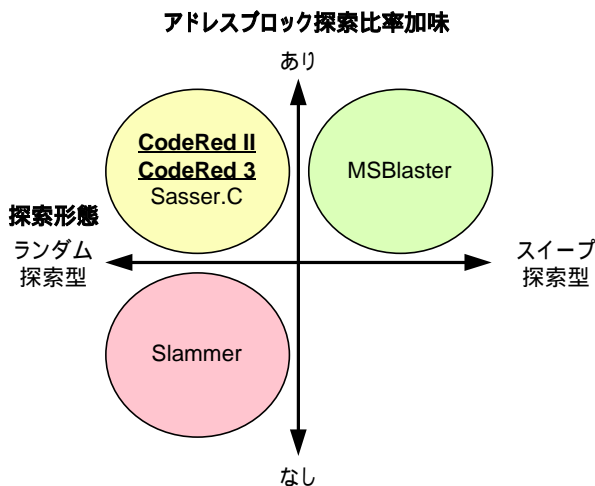


図 3.1 感染先探索特性の分類

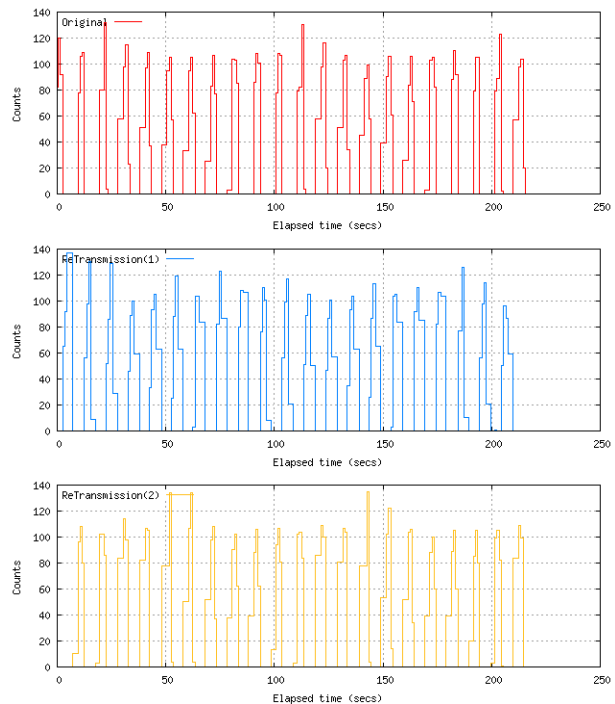
(2) TCP 再送処理に関する考察

本実験構成において、モニタ装置(monitor)は、受信したパケットを次のように処理するため、感染PCではTCPパケットの再送処理が発生することになる(図 3.2)。

- 宛先 IP アドレスがモニタ装置(monitor)の IP アドレスに一致した場合: "icmp: tcp port 80 unreachable"を感染 PC に返送する。
- 上記以外: 受信パケットを廃棄する。

図 3.2 の横軸は CodeRed3 のパケット受信以降の経過時間、縦軸は送出されたパケット数を示している。

- Sasser.C に比べると、パケット送信数の変動が規則的である。



(上段:オリジナル, 中段:1回目の再送, 下段:2回目の再送)

図 3.2 経過時間毎の TCP 再送パケットの分布

参考文献

1) CodeRed3

ネットワークアソシエーツ:

W32/CodeRed.f.worm

http://vil.nai.com/vil/content/v_100142.htm

シマンテック: CodeRed.F

<http://www.symantec.com/region/jp/sarcj/data/c/codered.f.html>

トレンドマイクロ: CODERED.F

<http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=CODERED.F>

eEye Digital Security: CodeRedII Worm Analysis

<http://www.eeye.com/html/Research/Advisories/AL20010804.html>

2004/06/04 8:37

@police : W32/CodeRed.F(W32/Codered2.F)
http://www.cyberpolice.go.jp/server/virus/pdf/W32CodeRed_F_jp_20030302.pdf

更新履歴

日付	更新内容
2004-05-14	初版
2004-05-30	ネットワーク構成を追記した。 比較対象パケット数を観測開始から 6000 パケットに変更した。
2004-06-02	Sasser.C の比較対象パケット数(観測開始 から 10000 パケット)にあわせ改訂した。 実験環境依存に関する検討項目として、 TCP 再送処理を記載した。