マルウェア通信活動抑制のための ネットワーク制御

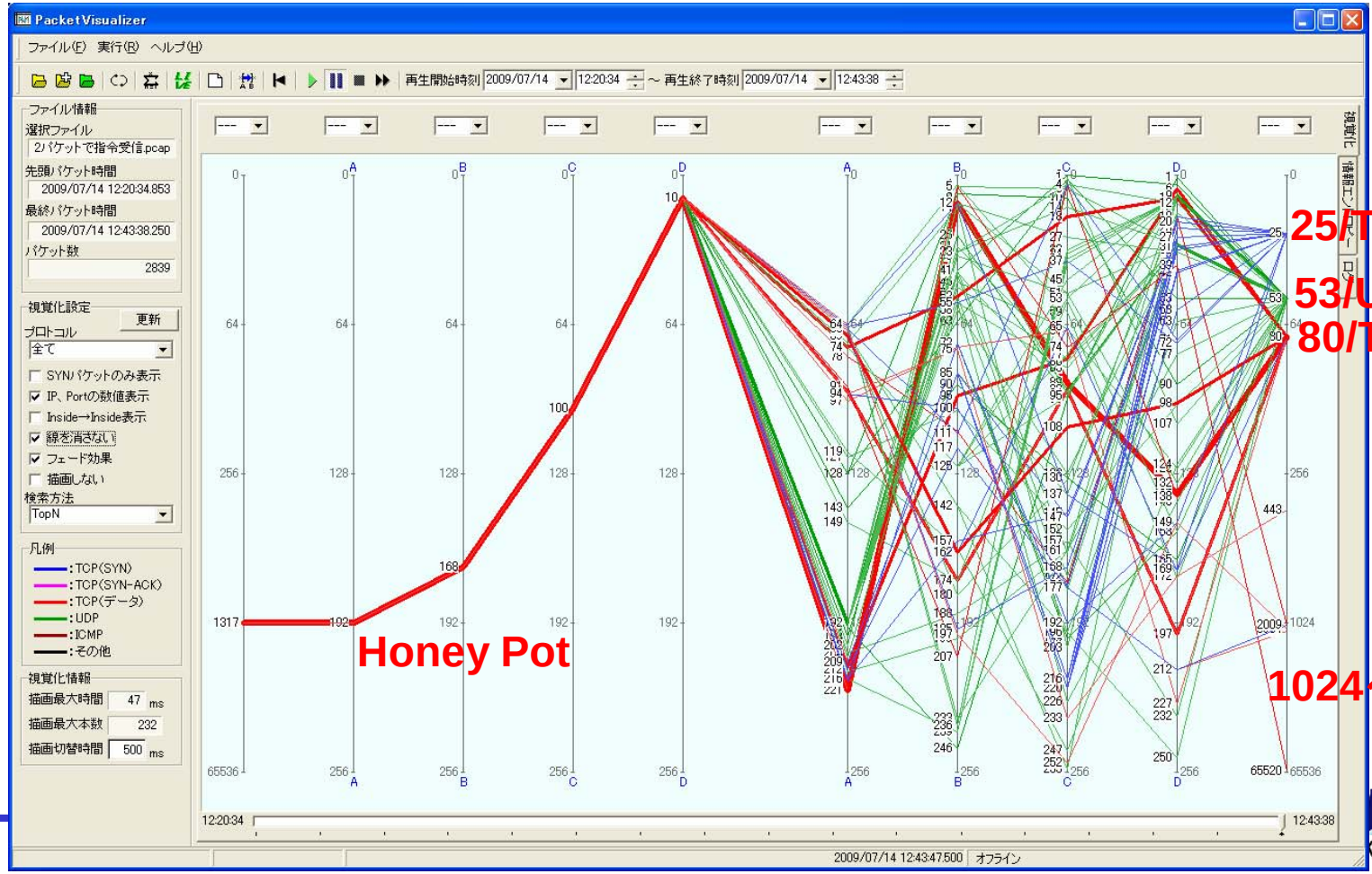
KDDI研究所　静岡大学　NICT
竹森敬祐　酒井崇弘　西垣正勝　安藤類央　三宅優

はじめに
定義: マルウェア通信
調査: CCC DATAset 2009 攻撃通信データ
提案: 通信活動の抑制手法
評価: CCC DATAset 2009 マルウェア検体
おわりに

KDDI R&D LABS

はじめに

- インターネット上のホストと連携したマルウェア活動
  - 脆弱性を突く「侵入フェーズ」
  - 指令や新たなマルウェアを受け取る「指令・配布フェーズ」
  - 外部への感染拡大パケットや迷惑メールを送信する「攻撃フェーズ」



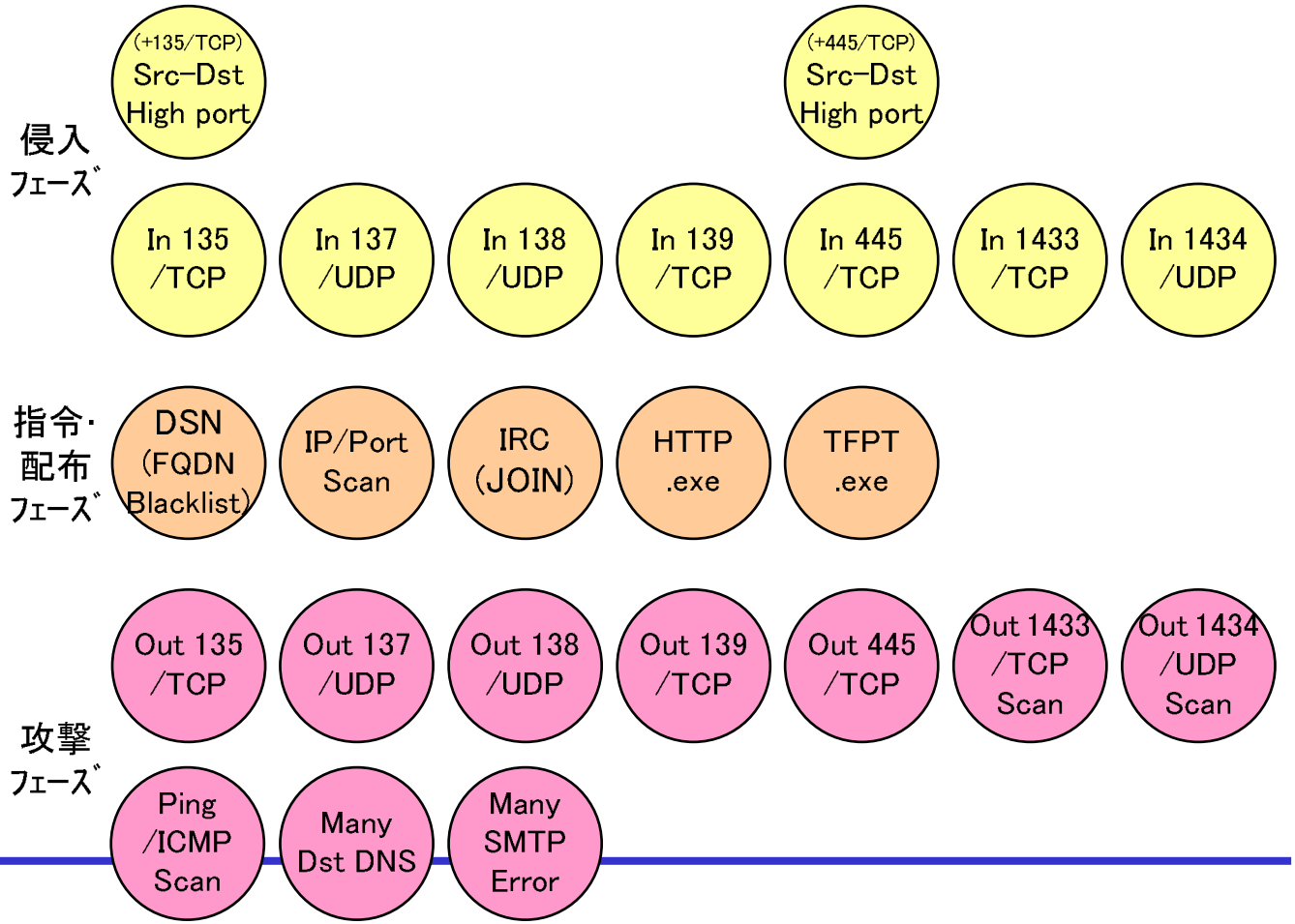
KDDI R&D LABS

はじめに

- 気付き
  - 一部の通信シナリオを阻止することで、外部ホストとの連携が損なわれ、ネットワーク上での通信活動を抑制できるのでは？！
- 従来技術: ボット検知
  - 指令を受け取るIRC通信や攻撃パケットなどの通信要素に着目した検知手法
  - 通信要素(Port番号)が組み合わされた通信シナリオに着目した検知手法
- 従来技術: 攻撃抑制
  - 不要な通信Portを閉じるルータやファイヤウォールにおけるPortフィルタ
  - スパムメールの送信規制に利用されるOut Bound Port 25 Block（OP25B）
  - スパムメールの送信規制に利用されるDNS Blacklist（DNS-BL）
  - フィッシングサイトへの誘導を阻止するOpenDNS
- しかし
  - 個々の通信要素を防ぐ技術であり、通信シナリオ全体への抑制効果は不明
- 本研究
  - 通信シナリオの進展を阻止する技術の選定と、その抑制効果について評価する。
  - 既存の通信設備での抑制を目指す　⇒ パケットヘッダのみに注目

マルウェアの通信要素

- 通信要素の抽出
  - CCC攻撃通信データについてヒューリスティックな調査を繰り返し、ハニーポットへの侵入フェーズ、感染後の指令･配布フェーズ、外部への攻撃フェーズに含まれる、特徴的な通信要素について調査した。



KDDI R&D LABS

調査：CCC DATAset 2009 攻撃通信データ

- 2009年3月13, 14日のCCC攻撃通信データ
  - ハニーポットの再起動がほぼ定時刻に完了して、前周期の通信要素が残っていない延べ182周期(=台)のハニーポットを調査

通信要素が観測されたハニーポットの延べ台数と出現確率

侵入フェーズ	100%（182台）	指令･配布フェーズ	73%（133台）	攻撃フェーズ	29%（53台）
In135/TCP	87%(159)	DNS(FQDN BL)	27%(49)	Out135/TCP	16%(28)
S/D HighPort	19%(35)	IP/Port Scan	69%(126)	Out137/UDP	0%(0)
In137/UDP	2%(3)	IRC(JOIN)	17%(31)	Out138/UDP	0%(0)
In138/UDP	2%(4)	HTTP.exe	21%(39)	Out139/TCP	0%(0)
In139/TCP	41%(75)	TFTP.exe	6%(11)	Out445/TCP	0%(0)
In445/TCP	66%(121)			Out1433/TCP	0%(0)
S/D HighPort	23%(41)			Out1434/UDP	0%(0)
In1433/TCP	15%(27)			Ping/ICMP	16%(30)
In1434/UDP	14%(25)			Many DNS	0%(0)
				Many SMTP	0%(0)

提案:通信活動の抑制手法

- 脆弱性Portのブロック
  - 侵入フェーズを阻止することで、感染ホストの増加を抑えられる。

- 必須
  - 135/TCP, 445/TCP, 139/TCP, 138/UDP, 137/UDPは、LANに限られたサービスであるため、WANルータやLAN-Gateway(GW)で、Inbound/Outboundブロックが有効である。

必須　IP/OP135, 137-139, 445B

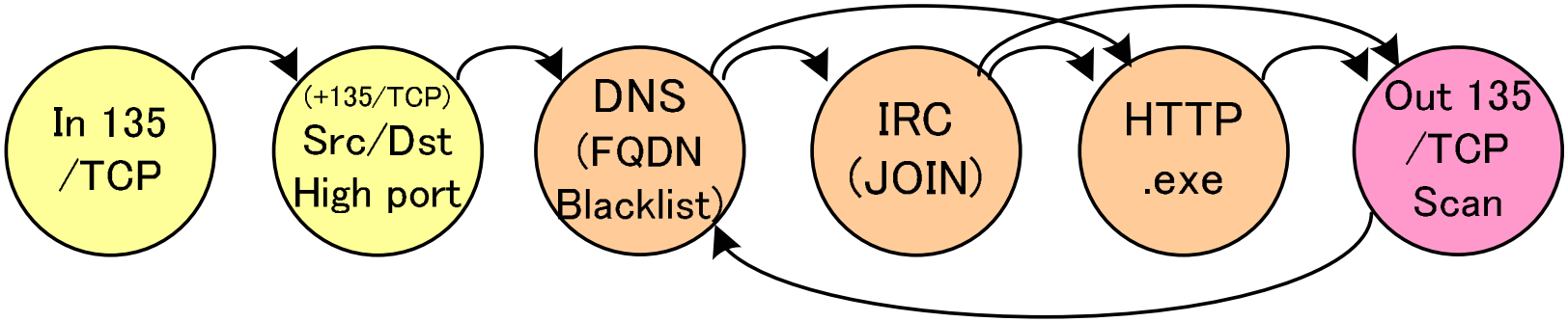
- 推奨
  - 1433/TCPや1434/UDPもブロックすべきであるが、WANにはこれらのサービスを提供するWebサーバもある。

⇒ 昨今の被害状況からすると、Webサイト内のみで1433/TCP, 1434/UDPを使うべきであり、Webサイトの設計が悪いとも考えられる。

推奨　IP/OP1433, 1434B

マルウェアの通信シナリオ

- 通信要素の組み合せである通信シナリオの抽出
  - ◆状態遷移モデル：検出された通信要素とその遷移の関係を○と→で表現
    - ⇒ しかし、→の関係が複雑化する
  - ◆ 通信シナリオ：状態遷移モデルの→を排除して簡易化
    - ⇒ 通信要素を出現順に並べたモデル



(a) 通信要素の状態遷移モデル

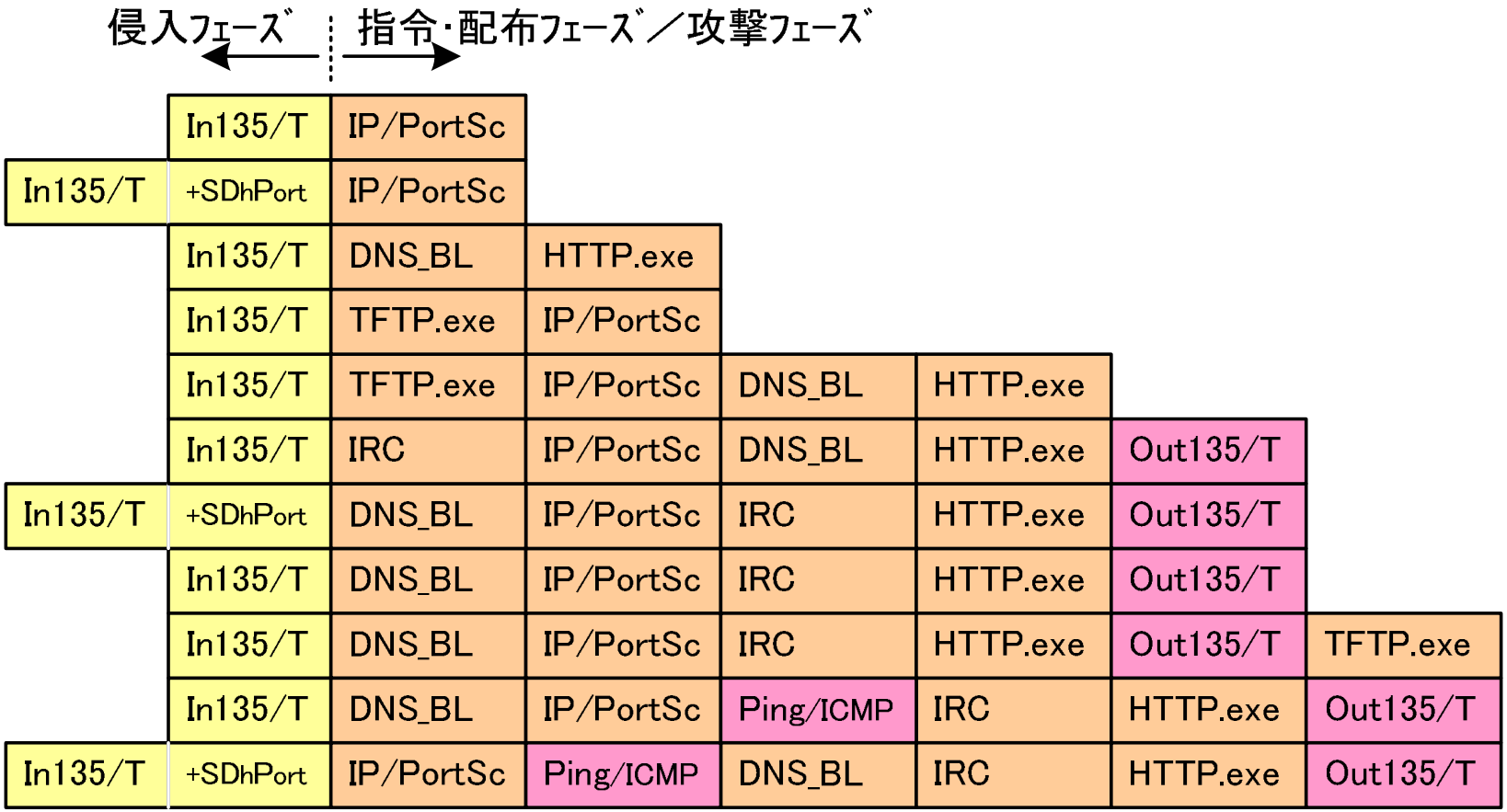
In 135 /TCP	(+135/TCP) Src/Dst High Port	DNS (FQDN Blacklist)	IRC (JOIN)	HTTP . exe	Out135 /TCP

(b) 通信要素の出現順位に注目した通信シナリオ

KDDI R&D LABS

調査：CCC DATAset 2009 攻撃通信データ

- 通信シナリオの調査
  - 2009年3月13-14日の延べ182周期(=台)のハニーポットの通信シナリオを調査
  - 1～10の通信要素までを持つ延べ101種類の通信シナリオを抽出



CCC攻撃通信データの通信シナリオの一例

KDDI R&D LABS

提案:通信活動の抑制手法

- 戦略(予想)
  - 可能な限り初期段階(左側)で出現する通信要素を阻止することで、その後の通信シナリオの抑制を効果的に行えるはず？！
  - ここでは、指令･配布フェーズ以後の通信要素について、侵入フェーズを除いた通信要素の平均出現順位と出現確率を調査した。

指令･配布, 攻撃フェーズにおける通信要素の出現順位と出現確率

通信要素	出現順位	出現確率
DNS(FQDN Blacklist)	1.69	37%
Ping/ICMP	2.17	23%
IRC(JOIN)	3.03	23%
HTTP.exe/TFTP.exe	3.28	38%
Out135/TCP	5.18	21%

提案：通信活動の抑制手法

- DNSの名前解決でブロック（DNS-Block）
  - スパムメール受信抑止のDNS-BLや、フィッシングサイト誘導阻止のOpenDNSのように、指令サーバや配布サーバ等の名前解決をブロックする。
  - 指令・配布サーバのFQDNやIPアドレスを、網羅性と信頼性を持って管理する。

Reputation DB

（明確な基準で悪性サイトを評価したDB）

- IRCサーバ通信ブロック（IRC-Block）
  - Reputation DBで、指令サーバのIPアドレスを管理して、通信をブロックする。

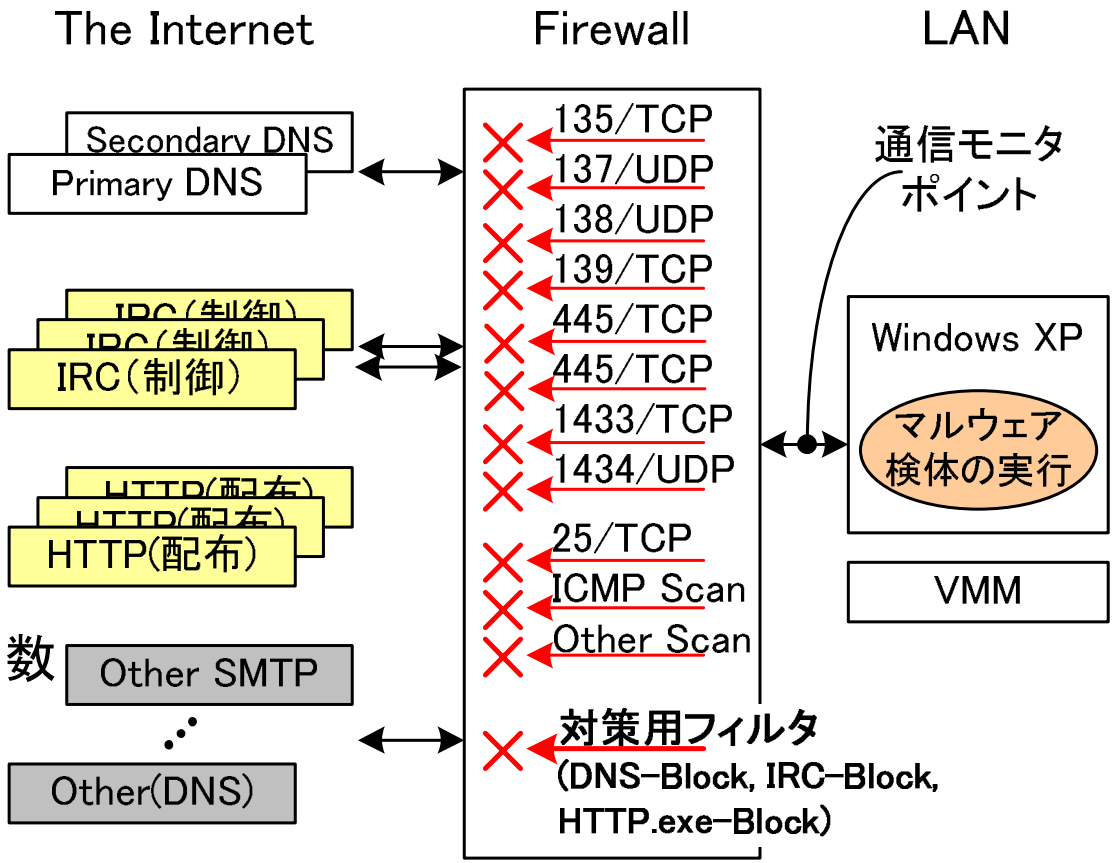
- 配布サーバ通信ブロック（HTTP.exe-Block）
  - Reputation DBで、指令サーバのIPアドレスを管理して、通信をブロックする。

評価：CCC DATAset 2009マルウェア検体

- 挙動解析
  - CCC DATAset 2009マルウエア検体（10個）を、安全な挙動解析用PC上で実行したときの、通信シナリオの抑制の様子を調査した。

- 3種類の検体
  - 2009年9月4日の時点で、有効動作した5個（3種類）の検体の挙動に注目

- 通信の特徴
  - 指令（IRC）サーバは数個
  - 配布（HTTP.exe）サーバは多数



KDDI R&D LABS

評価：CCC DATAset 2009マルウェア検体

■ 考察

- DNS-Blockを適用すると、その後の通信シナリオを効果的に抑制できる。
- IRC-Blockも、効果が高い。
- HTTP.exe-Blockは、重要検体の取得を阻止できた場合には、効果が高い。

(a) マルウェア検体A

	DNS BL	IRC (指令)	HTTP (exe)	SMTP (ｽﾊﾟﾑ)	Other Scan	Total
対策無	372	71	2862	156	1164	4625
DNS-Block	170	0	0	0	0	170
IRC-Block	46	270	0	0	0	316
HTTP.exe 100% Block	8	79	24	0	0	111
HTTP.exe 50% Block (1)	4	74	12	0	0	90
HTTP.exe 50% Block (2)	361	79	1001	158	803	2402

評価：CCC DATAset 2009マルウェア検体

■ 考察

- DNS-Blockを適用すると、その後の通信シナリオを効果的に抑制できる。
- IRC-Blockも、効果が高い。
- HTTP.exe-Blockは、初期の検体が攻撃コードを含んでいた為、効果は無し。

(b) マルウェア検体B

	DNS BL	IRC (指令)	HTTP (exe)	445/TCP Scan	Total
対策無	6	58	10	1376	1450
DNS-Block	154	0	0	0	154
IRC-Block	8	318	7	0	333
HTTP.exe 100% Block	6	44	11	1936	1997
HTTP.exe 50% Block (1)	6	49	11	1776	1842
HTTP.exe 50% Block (2)	6	50	10	1738	1804

評価：CCC DATAset 2009マルウェア検体

■ 考察

- DNS-Blockを適用すると、その後の通信シナリオを効果的に抑制できる。
- IRC-Blockは、指令が検体内にハードコーディングされていた為、効果は無し。
- HTTP.exe-Blockは、重要検体の取得を阻止できた場合には、効果が高い。

(c) マルウェア検体C

	DNS BL	HTTP (exe)	445/TCP Scan	Total
対策無	24	599	1705	2328
DNS-Block	30	0	0	30
IRC-Block	26	471	1982	2469
HTTP.exe 100% Block	12	48	0	60
HTTP.exe 50% Block (1)	6	36	0	42
HTTP.exe 50% Block (2)	6	178	1738	1922

おわりに

- 本論文では
  - CCC攻撃通信データから、マルウェアの通信要素と通信シナリオに関する調査
  - 通信シナリオを進展させないネットワーク側での対策を提案
  - CCCマルウェア検体を安全な環境で実行させたときの通信抑制の効果を評価

効果

HTTP.exe-Block < IRC-Block ＜ DNS-Block

- 上記を支援する手段

IP/OP135, 137-139, 445, 1433, 1434B

Reputation DB

- 未認定Mail, DNSサーバへのブロック

OP25B　　3rd DNS-B