MWS2009発表資料　2009/10/28

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

マルウェア解析の効率化手法の検討

情報セキュリティ大学院大学
博士前期課程 2年
山口和晃

研究背景

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

従来のマルウェア解析は、限られたマルウェアの解析者がおこなってきた。

問題

現在はネットワーク接続の有無、日時などの実行環境要因から処理を分岐することで、振る舞いを変化させる耐解析機能を備えたマルウェアが増えているために、解析者の負担が飛躍的に増大しており、解析精度や解析効率の低下が起きている。

研究目的

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■マルウェアの実行環境や実行方法の工夫による自動的解析の精度の向上や解析効率の向上に対する有効性の検討を行う。

目次

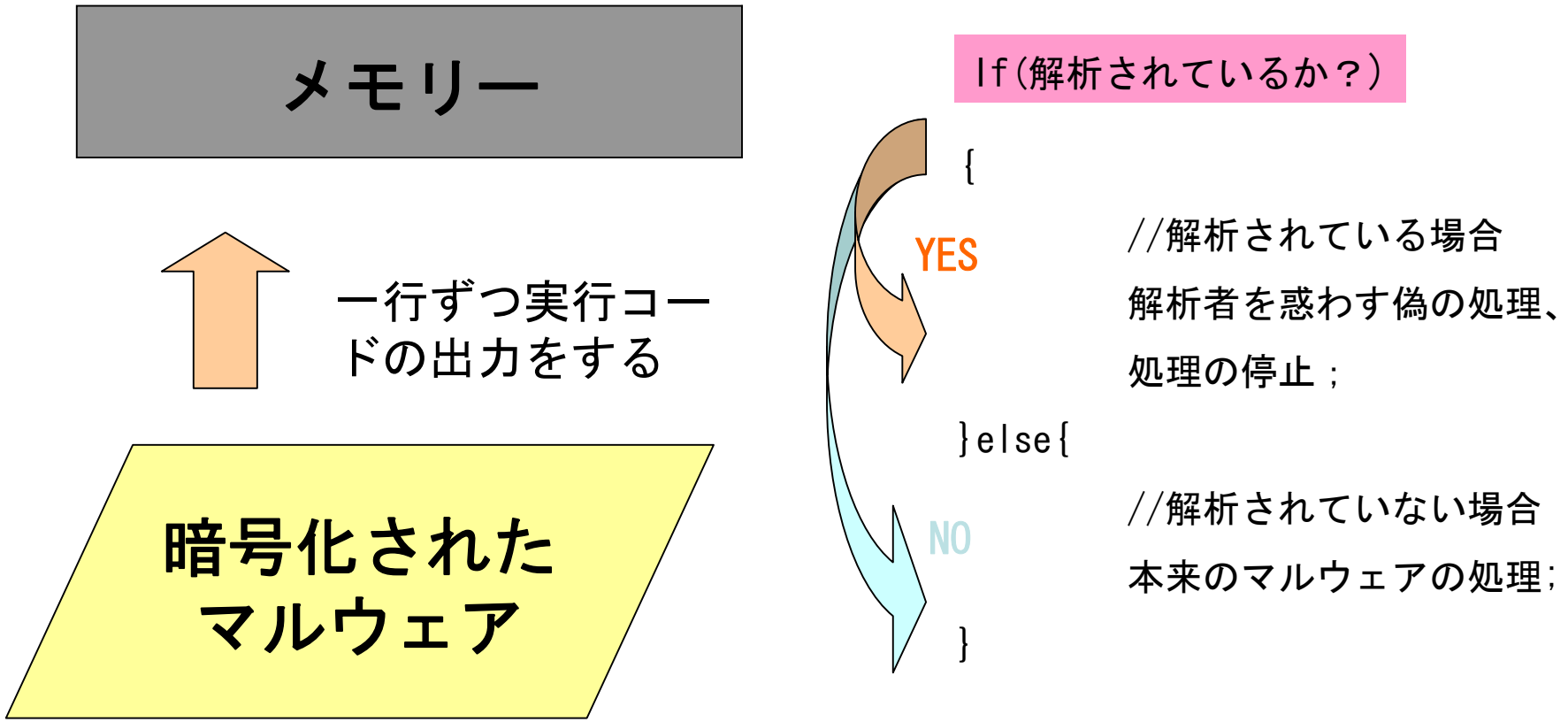
- 問題提起
- マルウェアの解析システム
- マルウェアの解析結果
- 考察
- 今後の課題

問題提起

耐解析手法について①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

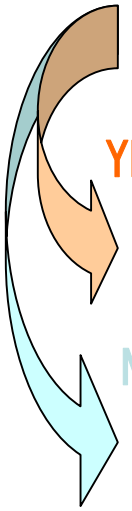
■ 挙動の分岐と暗号化をあわせた技術



耐解析手法について②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

主に自動的なマルウェアの解析は容易性から仮想マシンやデバッガで行われているが、侵入したホストが解析されていることを検出して活動を停止するマルウェアが多くなっている。




```
If(仮想マシン上でマルウェアが実行されているか？){
        //実行されている場合
        解析者を惑わす偽の処理;
}else{
        //実行されていない場合
        本来のマルウェアの処理;
}
```

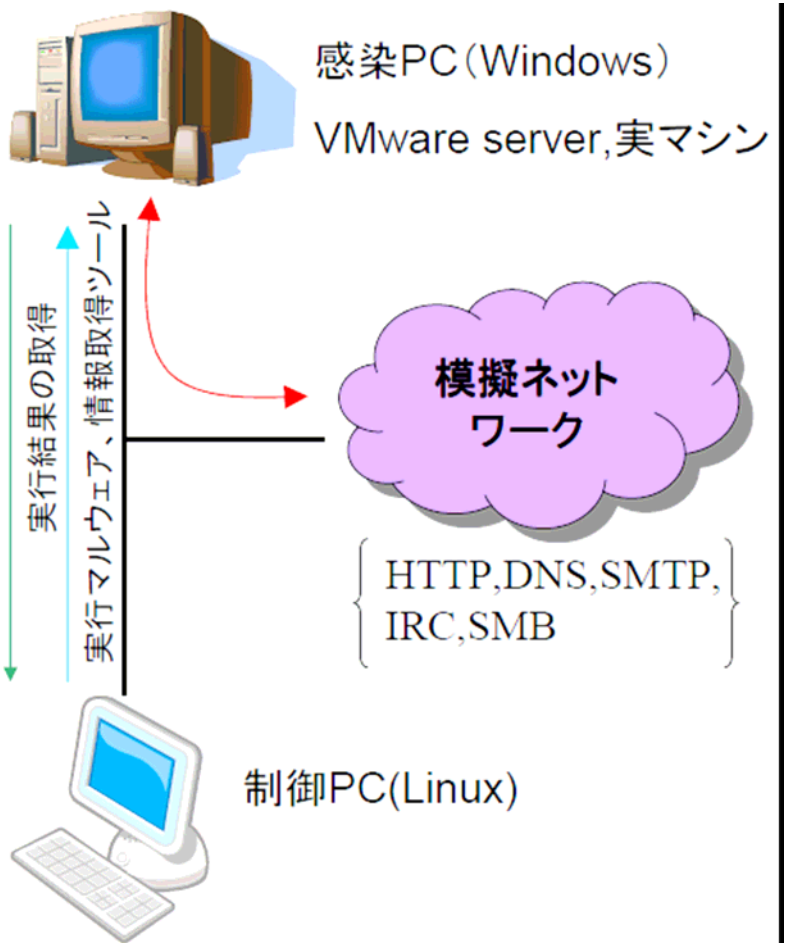
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

マルウェアの解析システム

マルウェア解析システム①

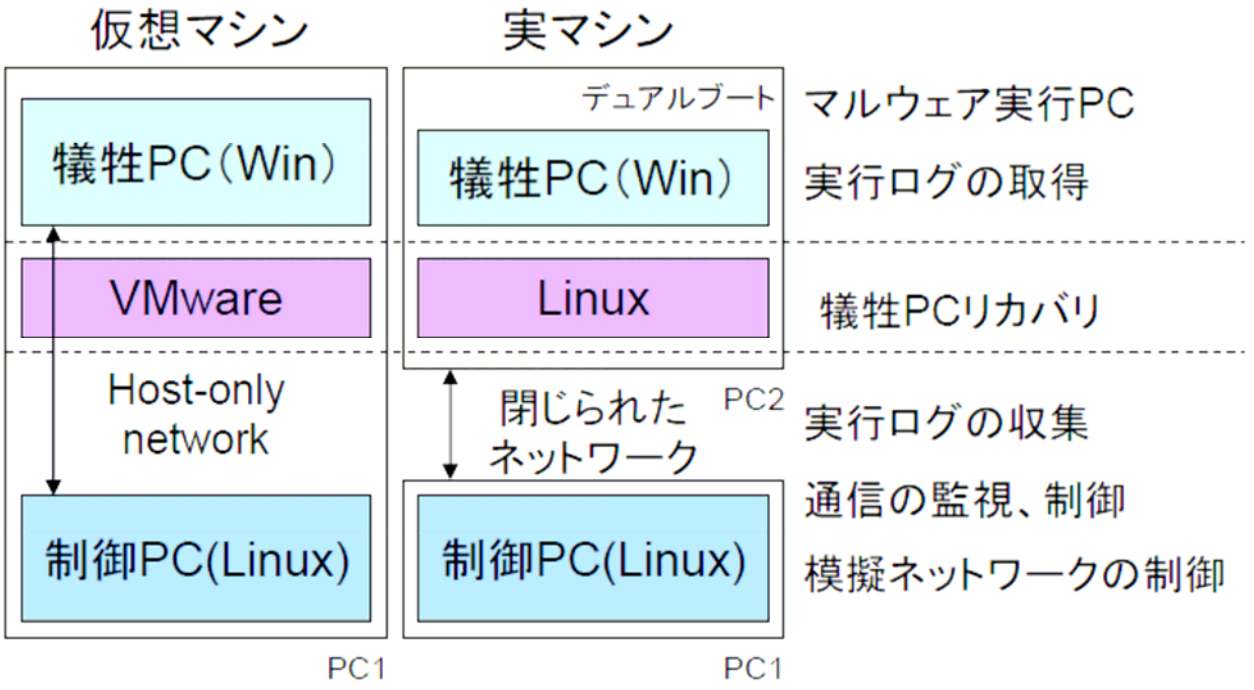
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Windows XP各サービスパックの場合の比較ができる環境を構築した。
- 模擬ネットワークには、マルウェアを実行する感染PCが接続され、模擬DNS、IRC、SMTP、SMB、HTTP の各サーバ群は、実際には制御PCの中に実装している。



マルウェア解析システム②

解析するには、実行環境、自動解析処理の全体制御や挙動の記録と分析、感染後のPC の復旧などの機能が必要となる。



マルウェア解析システム③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

環境で取得できる情報は、レジストリ改竄、システムファイルの変更、プロセスリスト、Hostファイルの改竄、ルートキットの有無、通信ログ、などの項目を文字列の情報として抽出し、これをBDB（Behavior Data Base）として蓄積する 。

BDBの一例

[HASH] マルウェアのハッシュ値の先頭6桁
f8c19c
[REGISTRY] レジストリ改ざん
c:¥windows¥u29tzwjvzhk¥command.exe
c:¥program files¥network monitor¥netmon.exe
[MD5SUM] システムファイル等の変更
Created C:¥WINDOWS¥SYSTEM32¥ATMTD.DLL.TMP
[PROCESS] Listen port プロセスリスト
628 winlogon 672 services 588 netmon
128 command 572 wuauclt
[HOSTS] HOSTSファイル改ざん
Change Found.
[ROOT KIT] ルートキットの有無
Not Detected
[TRAFFIC] 通信ログ
FQDN(13) xxx6ry3i3x3qbrkwhxhw.xxx439.com
xxxmand.xxxervs.com
PORT(13),:53(4) 80(20) 35815(3) 42613(3) 44627(3)
43327(3) 45390(3) 49830(3) 58010(3)
44645(3) 48717(3) 56840(3) 54267(3)

マルウェアの解析結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

実行環境変化による挙動変化

実行環境においてのマルウェアの挙動の違いを比較するため、Windows XP Professional SP0（仮想マシン）、SP2の仮想マシンと実マシンの三つの実行環境を用意し、先頭ハッシュ値６桁が68ac29のマルウェアを解析した。

実行環境OS	通信ポート（Top 5+その他+ICMP）	ファイル改ざん(Top 5+他+改竄+削除）	プロセス（Top 5+その他＋削除）
XPSP0（仮想）	0 0 0 0 0 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0
XPSP2（仮想）	0 0 0 0 0 1 0	0 0 0 0 0 0 0 0	0 1 0 0 0 0 0
XPSP2(実機)	0 0 0 0 0 1 0	0 0 0 0 0 0 0 0	0 0 1 0 0 0 0

実行環境OS	Service	RootKit	host
XPSP0（仮想）	0	0	0
XPSP2（仮想）	0	0	0
XPSP2(実機)	0	1	0

確率的な挙動の変化①

実行環境に依存せずに実行時刻などから
確率的に動作パターンを変更するマルウェア
について考察する。

- １種類の実行パターンしか持たないマルウェアに対して何度も実行していては無駄が多い。
- 複数の実行パターンを持つマルウェアにおいてはできるだけ全てのパターンを網羅したい。

確率的な挙動の変化②

大数の法則より

取りこぼし確率(単位[%])

xパターン	試行回数[回]				
	1	10	20	50	100
1	100	10	5	2	1
2		20	10	4	2
3		30	15	6	3
4		40	20	8	4
5		50	25	10	5

※これが成り立つには確率が独立であり、一様分布している必要がある。

確率的な挙動の変化③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

表１　解析の１０回試行結果

hash値	挙動パターン数	各出現回数
1d23f2	1	10
393f00	1	10
68ac29	2	5, 5
7190e4	1	10
84e9c2	1	10
cd9125	2	9, 1（１エラー含）
d49391	1	10
df7585	2	9, 1（１エラー含）
f8c19c	1	10
fdf3bbc	1	10

表２　解析の１００回試行結果

hash値	挙動パターン数	各出現回数
1d23f2	1	100
393f00	1	100
68ac29	4	69, 23, 6, 2
7190e4	1	100
84e9c2	1	100
cd9125	2	99, 1（１エラー含）
d49391	1	100
df7585	2	99, 1（１エラー含）
f8c19c	1	100
fdf3bbc	1	100

考察

考察①

実マシンのみルートキットの実行がRootkitRevealerに検出されたことがわかる。これは、仮想マシンで真の実行動作をやめてしまった可能性が高い。このことから、実マシンでの解析も併用して使用する必要があることがわかる。

ホストファイル、サービス、ルートキット有無

実行環境OS	Service	RootKit	host
XPSP0（仮想）	0	0	0
XPSP2（仮想）	0	0	0
XPSP2(実機)	0	1	0

考察②

マルウェアの挙動が実際に一様分布しているのか、検討すると、複数の挙動が確認された“68ac29”の出現回数に偏りがあることから、今回は一様分布であるとは言えないが、１０回の実行をして、複数のパターンが得られなければ、解析を停止することで、一定の効率化が可能と考えられる。

表１　解析の１０回試行結果

hash値	挙動パターン数	各出現回数
68ac29	2	5, 5
cd9125	2	9, 1（１エラー含）
df7585	2	9, 1（１エラー含）

表２　解析の１００回試行結果

hash値	挙動パターン数	各出現回数
68ac29	4	69, 23, 6, 2
cd9125	2	99, 1（１エラー含）
df7585	2	99, 1（１エラー含）

今後の課題

今後の課題

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 実マシンの解析の回数を低減する検討
- 確率的な挙動の変化の解析のための統計的なデータの取得
- より一般的な使用環境に近い実行解析環境の構築

ご清聴ありがとうございました。