資料５－３

巧妙化するmalwareの現状

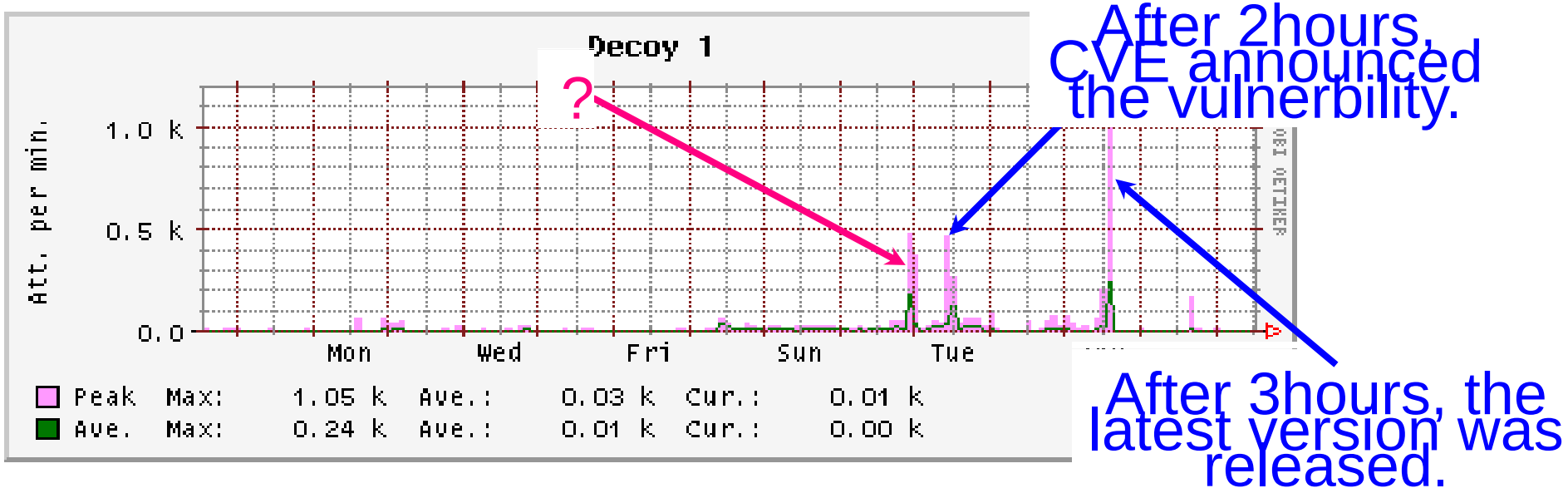
高倉 弘喜
京都大学

Malicious codeの開発は継続している

- Security adibisory、実証コード(PoC)、パッチ公開直後
  - 水面下で開発中のコードを検知するのは困難
  - ターゲット型攻撃はさらに見つけ難い
- ☑それでも、ユーザを守らねばならない？
  - 未知の悪意ある(ありそうな？)活動を観測
    - 活動の追跡と解析による攻撃者の目的を特定
      - 数日、数週間...数年？
    - 新たな検知パターンの作成(IDS, AV)

攻撃活動の変化例

- 観測: 2004年12月
- 対象: samba (Symantec Decoy Server)
  - ✓ 最新版公開直後、有効な攻撃を観測
  - ✓ CVE情報公開直後、ほぼ完成に近い攻撃を観測
  - ✓ 情報公開前から、不審な活動を観測



悪意あるプログラムの開発活動

- 完璧なプログラムのためには...
  - 実環境での実証実験による評価
  - 実験に伴う大量の誤検知
- Example (MS06-040)
  - パッチ公開 (8/9)
  - 初回攻撃検知(8/13)
  - IDSのパターン提供(8/16)
  - 30以上の悪意あるコード観測
    - 3プログラムのみバックドア開設に成功...まだ不完全

Date	DA	Code ID	IDS
08/13	winxp-fp	87	
08/14	winxp-fp	82	
08/14	winxp-fp	70	
08/15	winxp-fp	82	
08/15	winxp-np	88	
08/16	winxp-np	90	MS05-027
08/16	winxp-np	91	MS05-027
08/16	winxp-np	92	MS05-027
08/16	winxp-np	93	MS05-027
08/16	winxp-fp	94	MS06-040
08/17	winxp-fp	87	MS06-040
08/19	winxp-np	95	MS06-040, MS05-027, Backdoor
08/20	winxp-fp	96	MS06-040, MS05-027
08/20	winxp-np	97	MS06-040, MS05-027, Backdoor
08/24	winxp-fp	98	MS06-040, MS05-027
08/24	winxp-np	99	MS06-040, MS05-027
08/24	winxp-fp	100	MS06-040
08/24	winxp-np	101	MS06-040, MS05-027
08/24	winxp-fp	101	MS06-040, MS05-027
08/24	winxp-np	101	MS06-040, MS05-027, Backdoor
08/24	winxp-np	101	MS05-027, Backdoor
08/24	winxp-np	101	MS06-040, MS05-027, Backdoor
08/24	winxp-np	101	MS06-040, MS05-027, Backdoor

括弧書き: exploit codeの種別
BO: Buffer Overflow として検知

予備調査活動の探知

検知できない攻撃コード

20秒の時間差

約2分の時間差

全て異なる攻撃コード

DATE	DA	Size	Payload's MD5	Buffer Overflow	IDS
2005/08/04 19:35:55	cp***.nl: 2848	fbsd: 443	290	6f22dd356c97068ba41d27c4425839c6	N	BO
2005/08/04 19:36:14	cp***.nl: 2863	fbsd: 443	525	dead4b69594419589d8aac12c692923d	Malicious (1)	
2005/08/04 19:36:14	cp***.nl: 2862	fbsd: 443	525	1e13ac9e4840ae9a5f8ab8b9af4b8fa9	Malicious (1)	
2005/08/04 19:36:15	cp***.nl: 2878	fbsd: 443	525	9adbcd798074b2edc022509138f81e76	Malicious (3)	
2005/08/04 19:36:15	cp***.nl: 2877	fbsd: 443	525	9cce54cd78eee1cee9232b1056613bbe	Malicious (2)	
2005/08/04 19:36:16	cp***.nl: 2880	fbsd: 443	525	4b5375af9c4a4d3555d104e99746bae5	Malicious (5)	
2005/08/04 19:36:16	cp***.nl: 2871	fbsd: 443	525	09fde55f52375c8bc1a701b07c17723e	Malicious (4)	BO
2005/08/04 19:38:10	cp***.nl: 2879	fbsd: 443	660	58e89da6b6c87c4d553c8d7c549ac559	Malicious (6)	
2005/08/04 19:38:37	cp***.nl: 2868	fbsd: 443	660	764f1c5b6e2fda0b100c5203af36968e	Malicious (1)	
2005/08/04 19:38:37	cp***.nl: 2867	fbsd: 443	660	5728ee7b2ba2f5ecfe572567e3d1210f	Malicious (1)	
2005/08/04 19:38:40	cp***.nl: 2869	fbsd: 443	660	13c2f69[illegible]5594d86c	Malicious (1)	
2005/08/04 19:38:41	cp***.nl: 2864	fbsd: 443	660	fec2d7e[illegible]b2fea36b	Malicious (7)	
2005/08/04 19:38:50	cp***.nl: 2875	fbsd: 443	525	78e553c[illegible]da1e8060	Malicious (9)	
2005/08/04 19:38:50	cp***.nl: 2874	fbsd: 443	525	04c9d8e53b4053bec691cc2df22a421e	Malicious (8)	
2005/08/04 19:38:52	cp***.nl: 2873	fbsd: 443	525	02cc9ac04eb003efff18cadf1bddac18	Malicious (10)	
2005/08/04 19:38:52	cp***.nl: 2872	fbsd: 443	525	add5141d76867404f0ee483ffbb8fd00	Malicious (10)	
2005/08/04 19:39:15	cp***.nl: 2861	fbsd: 443	660	acfbe3c4922d5a511ec38648ccd12bae	Malicious (7)	
2005/08/04 19:39:19	cp***.nl: 2860	fbsd: 443	660	9804f2069d70d146d901f7acce2aa807	Malicious (7)	
2005/08/04 19:39:20	cp***.nl: 2859	fbsd: 443	660	1ba84e2dafe48ffa6913e2dde3f14ea4	Malicious (7)	
2005/08/04 19:39:23	cp***.nl: 2858	fbsd: 443	660	1cd58a58d357f63b6a6137e41cb29062	Malicious (7)	
2005/08/04 19:39:41	cp***.nl: 2881	fbsd: 443	525	cac1045d59ac629874134cb2345f38a3	Malicious (10)	
2005/08/04 19:39:47	cp***.nl: 2857	fbsd: 443	660	cfdb1198f72d7c8e076a823fd42319a0	Malicious (11)	BO

なぜ誤検知が発生するのか？

- 完全な(検知されない)攻撃コードの作成は困難
  - セキュリティ製品のどれかが検知していまう
- 攻撃者は外部からセキュリティ製品を制御できる
  - ほとんど製品は同じような仕組みを採用
    - ...つまり、パターンマッチ
  - 意図的に誤検知を発生させるのは容易
    - 監視者に無害な攻撃と判断させる
  - 膨大な誤報(IDSならいつものこと)による監視機能麻痺
    - 数千個の誤報に隠されるたった1個の未知コード

観測事例: Allaple (Win XP fully patched)

- 時間を遡って狙われる脆弱性
  - src port番号は順次増加
  - MS04-007を除くと使用されたコードは毎回違う
    - この頻度でのpolymorphism化は難しい
    - しかも、大半が効果のないコード
  - 100-300回の辞書攻撃
    - ID/passwordの奪取には不十分

Date&Time	src	dst	payload size	# of the same code was obs.	vulnerability
2007/06/20 08:43:28	*.or.jp : 2053	winxp-fp : 139	2786	1	MS06-040 MS05-027
2007/06/20 08:43:28	*.or.jp : 2065	winxp-fp : 139	3245	1	MS05-039
2007/06/20 08:43:29	*.or.jp : 2188	winxp-fp : 139	2647	1	MS04-012

観測事例: Allaple (Win XP SP2)

- 時間を遡って狙われる脆弱性
  - source port番号が不規則に変化
  - MS04-007を除くと使用されたコードは毎回違う
  - TCP 9988番に開かれるバックドア
- 極めて少数回の辞書攻撃(0-5)
- バックドアを通じてMalware (Allaple)を注入

Date&Time	src	dst	payload size	# of the same code was obs.	vulnerability
2007/06/20 08:40:23	*.or.jp : 4002	winxp-pp : 139	2733	1	MS06-040
2007/06/20 08:40:23	*.or.jp : 1759	winxp-pp : 139	3192	1	MS05-039
2007/06/20 08:40:25	*.or.jp : 1760	winxp-pp : 139	2593	1	MS04-012

観測事例: Allaple (Win XP with no patch)

- 攻撃パターンが大きく変化
  - MS06-040を狙った攻撃が大きく遅延(1st. v.s. last)
  - MS04-007を狙った攻撃コードが巨大化(x2)
    - このときだけコードが別物
  - お約束の辞書攻撃(100-300回) times
- そもそも、バックドアが何故開かない？

Date&Time	src	dst	payload size	# of the same code was obs.	vulnerability
2007/06/20 08:41:21	*.or.jp : 3914	winxp-np : 139	3192	1	MS05-039
2007/06/20 08:41:22	*.or.jp : 4190	winxp-np : 139	2593	1	MS04-012
2007/06/20 08:41:23	*.or.jp : 1733	winxp-np : 139	4197	1	MS04-011
2007/06/20 08:41:23	*.or.jp : 1831	winxp-np : 139	7285	1	MS04-007

観測事例: Allaple (Win 2000)

- 攻撃者の眼中に無い?
  - 狙われたのはたった二つの脆弱性
    - (MS06-040 and MS04-007)
  - お約束の辞書攻撃はある(100-300回)

Date&Time	src	dst	payload size	# of the same code was obs.	vulnerability
2007/06/20 08:40:46	*.or.jp : 3704	win2k : 139	2725	1	MS06-040

Date&Time	src	dst	payload size	# of the same code was obs.	vulnerability
2007/06/20 08:40:23	*.or.jp : 4002	winxp-pp : 139	2733	1	MS06-040
2007/06/20 08:40:23	*.or.jp : 1759	winxp-pp : 139	3192	1	MS05-039
2007/06/20 08:40:25	*.or.jp : 1769	winxp-pp : 139	2593	1	MS04-012

TCP 9988から注入されたmalware

- 2006/12/09 01:38〜2007/12/25 16:30
- Rbotは別の攻撃による
- Tenga, Virut.xはAllaple型攻撃による
  - そのような挙動をもつAllapleは見つかっていない
  - そもそも、観測数に大きな差が存在

Name	Count
Backdoor.Win32.Rbot.bni	1157
Net-Worm.Win32.Allaple.a	301
Net-Worm.Win32.Allaple.b	1657
Net-Worm.Win32.Allaple.d	628
Net-Worm.Win32.Allaple.e	879
Virus.Win32.Cheburgen.a	6
Virus.Win32.Tenga.a	1
Virus.Win32.Virut.a	6
Virus.Win32.Virut.ao	1
Virus.Win32.Virut.b	6
Virus.Win32.Virut.d	11
Virus.Win32.Virut.e	7
Virus.Win32.Virut.n	2
Virus.Win32.Virut.q	2

Allaple自身の注入時の挙動

- Allaple.eの注入は879回観測
- a,b,e,d全体で3465回観測

Date	SA	DA	Size	Overflow	Sig. ID	Old Sig. ID	IDS/AV
2007/12/24 22:35:23	92.81.202.115: 2020	winxp-pp-y3: 139	2733	Malicious (1)	128 (11635) 128 (11635)	157 (11634) 157 (11634)	IDS Evasion IDS Evasion MS06-040 MS05-027
2007/12/24 22:35:30	92.81.202.115: 2098	winxp-pp-y3: 139	3192	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	IDS Evasion MS05-039
2007/12/24 22:35:37	92.81.202.115: 2149	winxp-pp-y3: 139	2593	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	MS04-012 IDS Evasion MS05-027
2007/12/24 22:35:45	92.81.202.115: 2209	winxp-pp-y3: 139	4197	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	MS04-011 MS04-011 IDS Evasion MS05-027
2007/12/24 22:35:47	92.81.202.115: 2256	winxp-pp-y3: 139	4493	Malicious (12861)	129 (48768) 130 (48765) 131 (48765)	159 (48760)	MS04-007

Virus.Win32.Viurt.q注入時の挙動

- 観測は僅か2回 (2007/9/22, 2007/11/21)
- Viurt系: IRC bot http://canon-sol.jp/product/nd/virusinfo/vr_win32_virut_e.html
  - 42回観測 (大半はSP2で発生)

Date	SA	DA	Size	Overflow	Sig.ID	Old Sig.ID	IDS/AV
2007/11/21 13:11:25	211.186.205.76: 3862	winxp-pp-y3: 139	2733	Malicious (1)	128 (11635) 128 (11635)	157 (11634) 157 (11634)	IDS Evasion IDS Evasion MS06-040 MS06-040
2007/11/21 13:11:29	211.186.205.76: 3938	winxp-pp-y3: 139	3192	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	IDS EvasionIDS Evasion MS05-039 MS05-039
2007/11/21 13:11:35	211.186.205.76: 3953	winxp-pp-y3: 139	2593	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	MS04-012 MS04-012 IDS Evasion IDS Evasion
2007/11/21 13:11:41	211.186.205.76: 4045	winxp-pp-y3: 139	4197	Malicious (1)	129 (48768) 130 (48765) 131 (48765)	158 (33204) 159 (48760)	MS04-011 MS04-011 MS04-011 MS04-011 IDS Evasion IDS Evasion
2007/11/21	211.186.205.76:	winxp-pp-y3:		Malicious	129 (48768)		MS04-007

二つの挙動は良く似ているが...

Net-Worm.Win32.Allaple.e	Virus.Win32.Virut.q
IDS Evasion IDS Evasion MS06-040 MS05-027	IDS Evasion IDS Evasion MS06-040 MS06-040
IDS Evasion MS05-039	IDS Evasion IDS Evasion MS05-039 MS05-039
IDS Evasion MS04-012 MS05-027	IDS Evasion IDS Evasion MS04-012 MS04-012
IDS Evasion MS04-011 MS04-011 MS05-027	IDS Evasion IDS Evasion MS04-011 MS04-011 MS04-011 MS04-011
MS04-007	MS04-007 MS04-007

やはり
微妙に違う

これはもはやAllapleの挙動とは言えない...

Date	SA	DA	Size	Sig.ID	IDS/AV
2008/01/30 20:28:26	***.it: 22309	winxp-pp-y3: 139	2786	128 (12342) 128 (12342)	IDS Evasion MS06-040
2008/01/30 20:28:43	***.it: 22955	winxp-pp-y3: 139	3245	129 (51134) 130 (51131) 131 (51131)	IDS Evasion MS05-039
2008/01/30 20:28:49	***.it: 24142	winxp-pp-y3: 139	2647	129 (51134) 130 (51131) 131 (51131)	MS04-012 IDS Evasion
2008/01/30 20:29:07	***.it: 24575	winxp-pp-y3: 139	4251	129 (51134) 130 (51131) 131 (51131)	MS04-011 MS04-011 IDS Evasion
2008/01/30 20:29:08	***.it: 25782	winxp-pp-y3: 139	4493	129 (51134) 130 (51131) 131 (51131)	MS04-007
2008/01/30 20:29:26	***.it: 26001	winxp-pp-y3: 9988	94890		Net-Worm.Win32.Allaple.e
2008/01/30 20:29:37	***.it: 27791	dc2-y1: 80	1640	254 2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:15	***.it: 30198	Solaris: 80	1647	254 2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:18	***.it: 30172	Solaris: 80	66421	254 2008/01/30 20:29:37(16)	MS01-016 MS03-007
2008/01/30 20:30:56	***.it: 32660	Solaris: 80	1647	254 2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:58	***.it: 32658	Solaris: 80	66421	254 2008/01/30 20:29:37(16)	MS01-016 MS03-007

イレギュラーな活動

- このコードの初回観測日: 2008/1/30
  - 不正コード収集システム 2005/8月から稼働
  - 狙われている脆弱性が余りにも古過ぎる
  - すごーく不自然なので....
    - Custom signatureをIDSに投入

Date	SA	DA	Size	Sig.ID	IDS/AV
2008/01/30 20:29:37	***.it: 27791	dc2-y1: 80	1640254	2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:15	***.it: 30198	Solaris: 80	1647254	2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:18	***.it: 30172	Solaris: 80	66421254	2008/01/30 20:29:37(16)	MS01-016 MS03-007
2008/01/30 20:30:56	***.it: 32660	Solaris: 80	1647254	2008/01/30 20:29:37(16)	CVE-2005-2088, CVE-2005-2090 MS99-019
2008/01/30 20:30:58	***.it: 32658	Solaris: 80	66421254	2008/01/30 20:29:37(16)	MS01-016 MS03-007

IDSによる防御

- IDSによるTCP RST送信(sourceとdestination)
  - Honeypotへの着弾観測されず
  - 誤検知による通信遮断は無い(今のところ)
- TCP RSTに対する攻撃者の反応
  - 一般的なsignatureによる検知と判断
  - 検知回避に注力したコード改良(4時間程)

DATE	SA	DA	IDS
2008-01-30 22:24:42	***.it :40361	130.54.***.137 :80	MS03-007
2008-01-30 22:24:43	***.it :40378	130.54.***.137 :80	CVE-2005-2088, CVE-2005-2090
2008-01-30 22:24:43	***.it :40378	130.54.***.137 :80	SNS_GEN_TCP-80-254N
2008-01-30 22:24:43	***.it :40378	130.54.***.137 :80	MS99-019
2008-01-30 22:24:43	***.it :40378	130.54.***.137 :80	Terminating Connection
2008-01-30 22:24:44	***.it :40361	130.54.***.137 :80	MS01-016

Botの活動(2007年6月)

- 典型的なIRC botは死滅
  - 手口が巧妙化
  - 自然な挙動
    - IRCサーバへ接続
    - 5分に1回PONG送信
    - IRCクライアントと同じ挙動
      - IDSでの識別困難
  - /16, /24を基本にした感染活動
    - 組織内感染に勤める
      - IDSでの検知回避
  - 感染成功報告はIRCで
    - 感染済みホストリストの作成？
- 同種のマルウェアインストール
  - Anti-virusの検知漏れが狙い？
  - 実際に、4社のAVでも検知漏れ

file name	type
C:¥-2066584973	unknown(ok?)
C:¥aungboya.exe	Downloader
C:¥iaxcbv.exe	Trojan Clicker
C:¥rxxkvre.exe	Downloader
C:¥xxgl.exe	PolyCrypt
C:¥system32¥awtsqqo.dll	Duntek
C:¥system32¥awvvw.dll	unknown
C:¥system32¥cwrx.exe	Ranky
C:¥system32¥ddcyx.exe	unknown
C:¥system32¥firewall.exe	IRCBot
C:¥system32¥gebyvur.dll	Duntek
C:¥system32¥hggfcaw.dll	AdWare
C:¥system32¥ipmon.exe	Trojan Clicker
C:¥system32¥jkklm.exe	unknown
C:¥system32¥khfcded.dll	AdWare
C:¥system32¥lsass6.exe	PolyCrypt
C:¥system32¥max1d1641.exe	Porn-Dialer
C:¥system32¥sumdsf.exe	Ranky
C:¥system32¥winamp.exe	IRCBot
C:¥system32¥xpdx.sys	Trojan Clicker

IRCの使用は最低限に...

- 最新プログラムのダウンロード
  - ファイルを直に指定
    - GET /xxx.exe
      - インストール時にはファイル名を変更
  - スクリプト実行系
    - GET /dl/xx.exe?rov=77&c=84d26a73+948469f3-e033-4c24-ac62-b277ac2ada93&u=91ab741a15d711dcad7e0015c55d2e2d&Aff=67370
    - GET /progs/xxxxx/xxxxxxx.php
      - “PONG”を打っていないPCからのアクセス
        - “File not found”
      - “PONG”はホスト管理に使用されている？
- 活動隠蔽？
  - 有名どころのWebブラウジング
    - yahoo, google, cnn, weather news....
  - 個人のブログを読みふけっているような挙動

感染済みホストの検証

- 有名どころのメールサーバ(G社、H社、M社)
  - 3-way handshake を実行後、直ちにFINパケット送信
    - SMTPサーバのバナーによるハニーポット環境検証？
    - Open relayデータベスへの登録の有無を確認
      - 登録済みなら、先方からRST or 受信拒否メッセージ

- 検証完了後、次のようなメールを送信

- From: "Diane Gutierrez" <cmoorecatsoqeyg@+++++.net>
- To: "vivien reed" <o.briones@*****.com>
- Cc: "merrie carter" <elisaelisa.dabove@*****.com>, ...,
- "crystal hamilton" <elisabetta.fanfani@*****.com>,
- "rosann owens" <mtldocs@*****.com>
- Subject: Get ready for the party

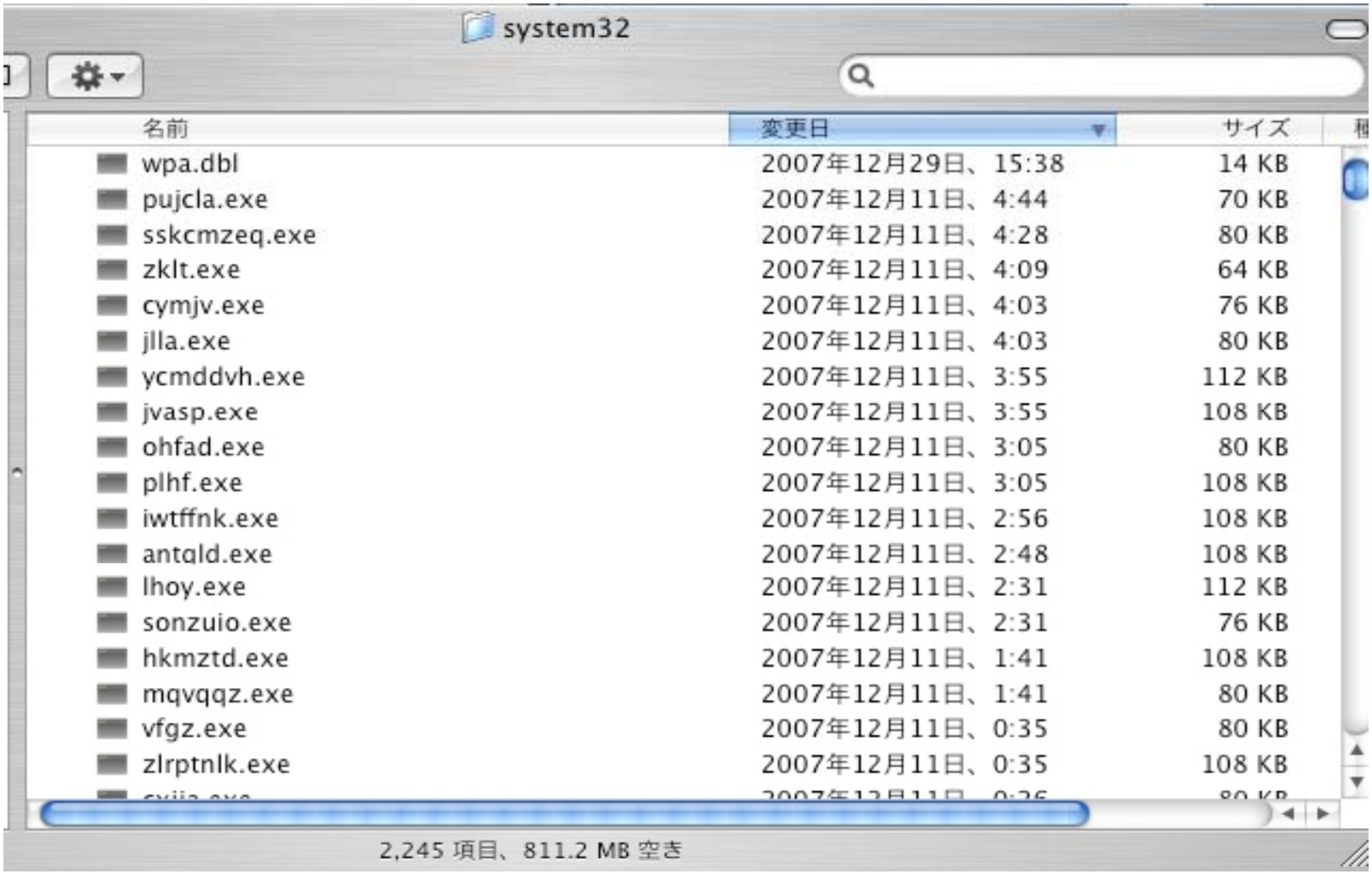
パーティ開始直後

- 感染済みPC
  - Webサーバへのアクセスで、user ID+passwordを取得
  - 定期的にWebサーバへアクセス
    - サービスの不正利用を防止
- spam発信者
  - spamメール転送の前に、user ID+passwordを含むパケットを送信
- spamが届かないと分かると...
  - IRCサーバを通じて周辺への感染活動命令

  - 組織内でbot感染が発生すると、飛び火する可能性大
  - 発症までの潜伏期間もPC毎に変化
  - spamメールの大量送信を避ける
    - 毎時間数通といった事例も

Botが活動していたHDD(2007年12月)

- system32フォルダ内



汎用OSの普及

- 家庭用電化製品
  - テレビ、ビデオ、冷蔵庫....
  - カーナビゲーションシステム、携帯電話...
- 事務用機器
  - Fax、プリンタ、コピー機、プロジェクタ...
- その他
  - 自動車、入退出管理システム、Webカメラ...
  - 通話記録システム@韓国
- PC系OSを採用
  - Windows, Linux, FreeBSD, NetBSD, OpenBSD.....
    - 大半はembedded OSだが....
    - PC用OSをそのまま採用している機種も
  - Cabir...携帯電話(Symbian OS)
    - Bluetoothを介して感染拡大

情報家電の脆弱性問題

- 開発期間+製品寿命 >>>>> ソフトウェアの寿命
  - ex. 1998年のOSを現在も使用
  - ハードウェアであれば...
    - 10年も経てばバグが枯れる
  - ソフトウェアの場合は...
    - 10年も経てば開発チームが消滅しているかも？
      - バクが枯れたのではなく、誰も気付かなくなっただけ
- 共通プラットホーム
  - 同一メーカの製品
    - 開発チームが共通であれば、ほぼ同じ構成
      - 廉価機、普及機、高級機...違うのは追加ソフト
      - メーカ独自開発のブラウザ
        - 狙われにくい？ or 汎用ブラウザ並みの安全性？
      - 言語依存や環境依存による発症/不発症が起きにくい

組み込みシステムの脆弱性対策の難しさ

- どうやってアップデートするのか？
  - テレビなら放送波を使う手があるが...
- 迅速なアップデートを徹底できるか？
  - 極めて短い猶予期間
- アップデート失敗の場合の対策は？
  - 製造元での修理対応が受け入れられるか？
    - 洗濯機や冷蔵庫の場合は？
- 最もセキュリティレベルの低い機器に揃えざるを得ない
  - 40bit WEPのみしか使えない機器に合わせると...
    - 重要情報を盗聴により盗まれる危険性

国内のみで発生するインシデント

- 既に多数観測されている
  - 日本語版ソフトウェアでのみ発症するmalware
  - 国内のIPアドレスに絞り込んだ攻撃
- 主に国内で利用されているソフトウェア
  - 交換されるデータを改ざん
    - 想定外の動作が可能
      - 動作保証は当然ない
      - 今後問題化すると思われる

これな～んだ？

情報セキュリティ対策の課題

- 危機的な情報不足からの脱却
  - 研究機関・企業における検体不足
    - 実効性の低い情報セキュリティ研究
  - 統合的な情報解析能力の不足
    - 偽プログラムも含めた情報収集
    - 真に未知のプログラムのみ抽出、解析
- 情報収集体制の強化
  - 単独組織では収集能力に限界
  - 脆弱性の事前察知は困難
  - 初期レベルの解析までは公的組織による対応が必要？
    - 詳細な解析と対応は製造者が引き継ぐ

後追い研究に
なってないか？

観測網の整備
「P波」の検知

国内観測網の必要性

- 日本先行or独自の製品普及
  - 海外からの情報に頼れない
  - 海外ベンダーへの情報提供が必須
    - 情報がなければ対策を講じ難い
- NGN/インターネット以外からの攻撃の可能性
  - ワンセグ、Bluetooth...
    - ISP等の入り口で見張っていても察知は困難
      - 内部の不審な事象発生を察知する仕組みが必要
      - 関係者間の情報交換が重要

民間からの要請

- 過保護は却って望ましくない
  - 危機感の希薄化による、自己対策の欠如
  - 特定企業の営利活動の支援になりかねない
- 単独での情報収集能力の限界
  - 薄く広くインシデント情報を収集
  - 情報を統合解析する枠組みの構築
    - 攻撃対象の推定(特定)
    - 関係者への通知
      - Telecom ISAC Japan、他省庁、その他関係機関