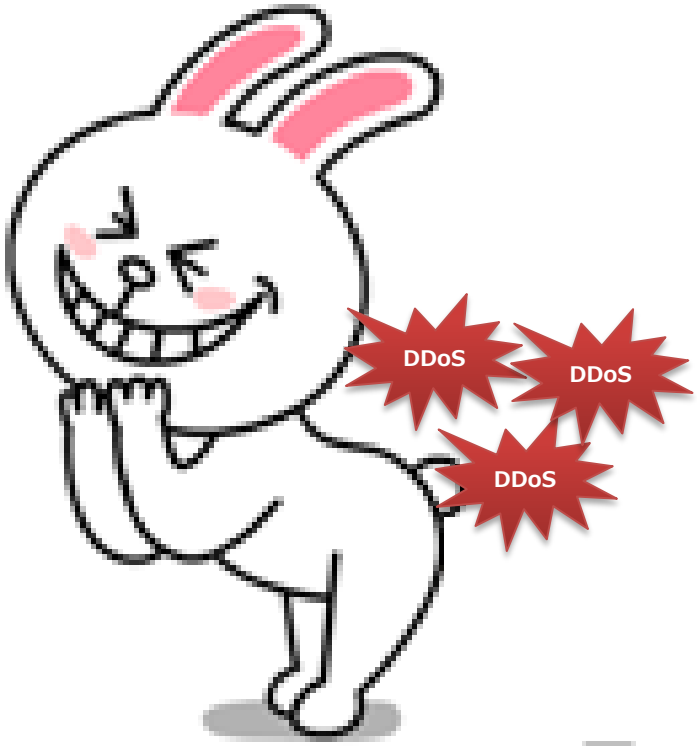
韓国の DDoS 攻撃と対応
～「7.7 大乱」と「3.4 DDoS」～

2012.7.6
株式会社アンラボ
愼 麻由美



JANOG

今日は韓国の DDoS のお話です

AhnLab

～2009年7月7日

—

2009年7月5日~ 7.7 大乱

AhnLab

02:00
~14:00　**1次DDoS攻撃 (米：3サイト)**

22:00
~6日 18時　**2次DDoS攻撃 (米：21サイト)**

7月5日(日)　7月6日(月)　7月7日(火)　7月8日(水)

18:00　**3次DDoS攻撃　(韓：11サイト/米：13サイト)**

18:44　インターネット振興院(KISA)の侵害センター(KISC)のDDoS対応システムで大統領府、韓国国会などのWebサイトに対するDDoS攻撃検知

19:00頃　KISC、上記を関連機関に通知

19:05　放送通信委員会(KCC)及びKISA担当者、非常待機を開始

19:50　KISA、攻撃IPアドレス検知および位置確認

19:50
~1:00　KISA、E/U 同意得て、リモートでゾンビパソコン分析実施

21:00　KCCネットワーク政策局、DDoS攻撃緊急対応チーム構成。運営開始

21:30　KISA、状況レポート送信 (8つのISPにモニタリング強化要請)

21:35　KISA、マルウェアサンプル入手・分析

ソース：2009 韓国電子新聞、2009 KCC「7.7 DDoS事件概要」、Byoung Tak Kang「7.7大乱DDoS攻撃実態と現況」ほか

2009年7月8日~ 7.7 大乱

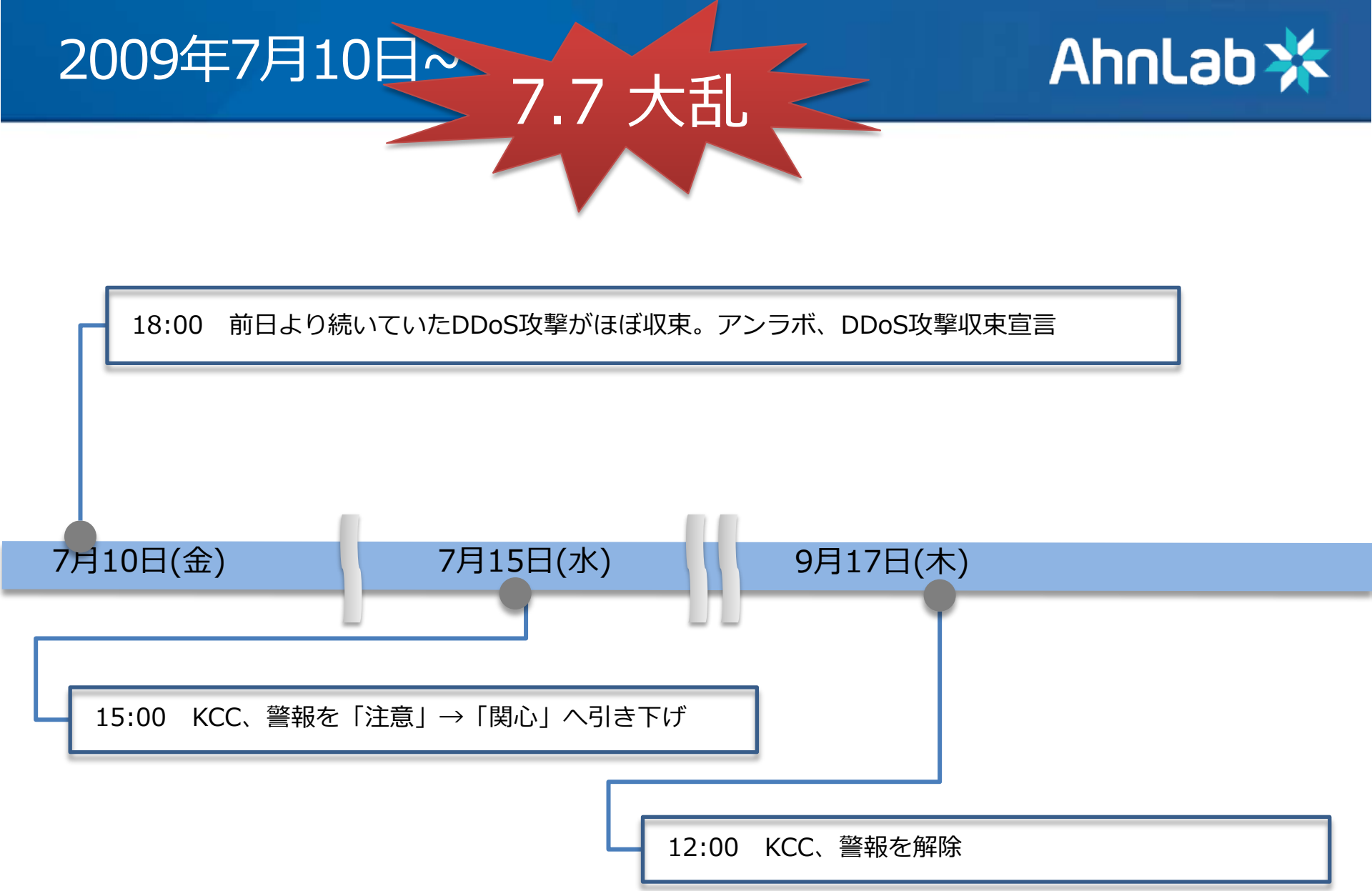
AhnLab

00:00　KISA、「DDoS攻撃で主要サイト接続障害」ニュースリリース配布
00:39　KISA、1次マルウェア分析内容結果抽出 (攻撃対象リスト抽出)
02:40　KCC、対国民へ「注意」警報発令
(早朝)　アンラボ、 4次DDoS攻撃用無料駆除ツール配布開始
18:00　**4次DDoS攻撃 (韓：15サイト)**
(全日)　KCC、マルウェア配布サイトが疑われる529サイトを遮断

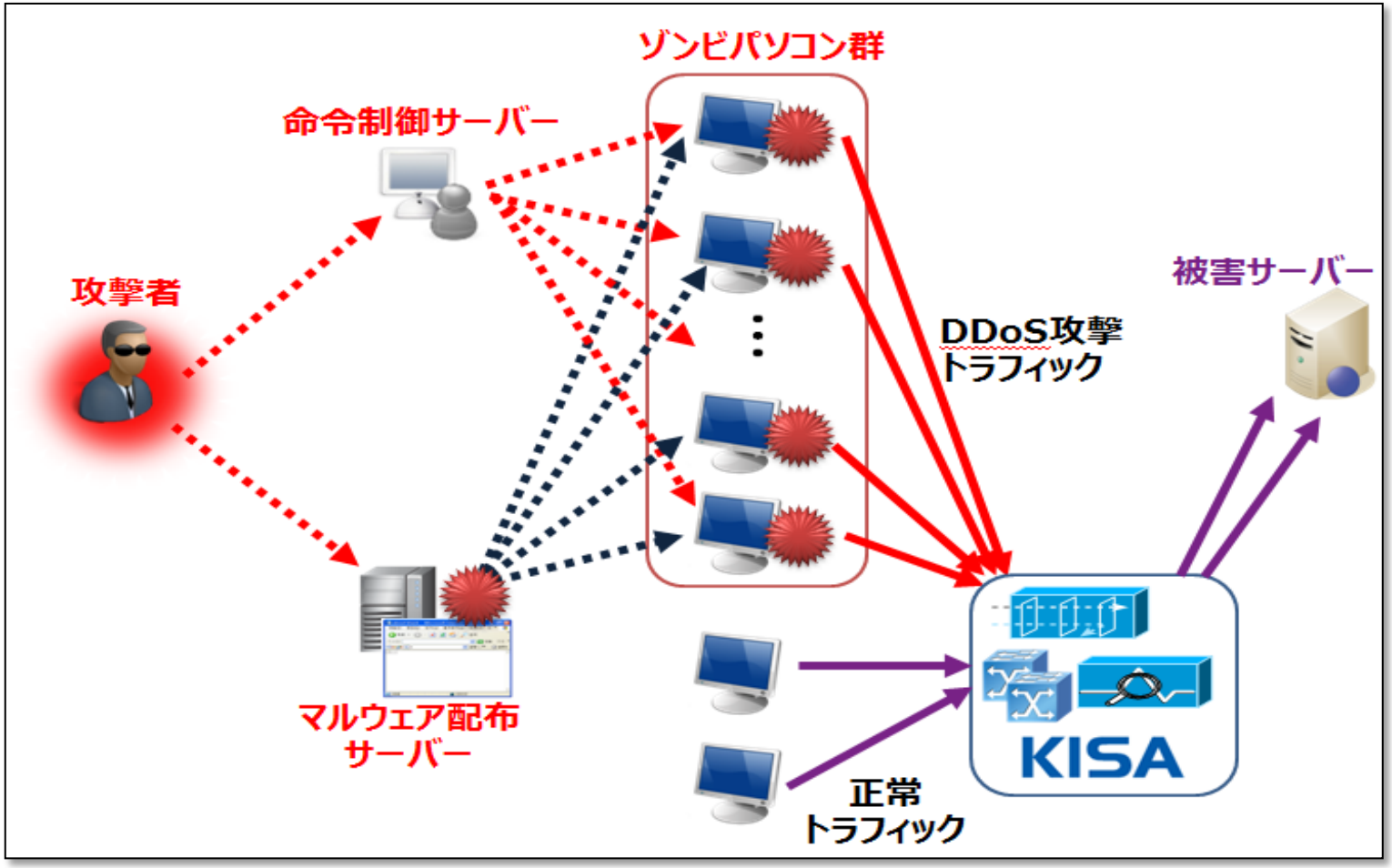
7月8日(水)　7月9日(木)　7月10日(金)　7月11日(土)

02:00　アンラボ、5次DDoS攻撃用無料駆除ツール配布開始
14:30 ~17時　KCC、ISP社長団緊急会議、事務次官級会議、国政課題戦略協議会など開催
18:00　**5次DDoS攻撃 (韓：7サイト)**
23:30　3大ポータルサイトおよび地上波TV3者、ニュース専門放送局への緊急字幕実施
→ハードディスク破壊するマルウェア駆除ツール使用を推奨

2009年7月10日~ 7.7 大乱



「D-DOSサイバー待避所」



「DDoS対応システムテスト構築事業」

IXで、DDoS攻撃を自動的に検知・遮断できるシステムを設けるもので、SKテレコム、SKブロードバンド、ドリームライン、セジョンテレコム、HCN、Tブロード、CJハローヴィジョンの各社のインターネット網の一部IXに構築され運営された

2011年3月3日~ 3.4 DDoS

AhnLab

11:10 国家サイバー安全センター(NCSC)、アンラボにサンプル送信

15:57 ドロッパー (Dropper) 情報確認および配布サイト、sharebox.co.kr 確認
国家情報院と KISA に配布サイトへのアクセス遮断を要請、
V3 にシグネチャアップデート(ヒューリスティック検知機能含む)

16:52 KISAにマルウェアのサンプルを送信

19:44 (3月4日18:30 攻撃マルウェア診断用) 無料駆除ツール製作、サイトから配布開始

3月3日(木) 3月4日(金) 3月5日(土) 3月6日(日)

ソース：AhnLab e-Security response Emergency Center 「3.4 DDoS 分析レポート」2011年3月号およびKISA「業務現況」2011年9月号、KISA月刊誌「Internet」2011年3+4月号、「Botnet」サイト「3.4 DDoS攻撃総整理」ほか

2011年3月4日~ 3.4 DDoS

AhnLab

01:30 アンラボ、攻撃時間 (3月4日18:30) および攻撃目標 (40 サイト) を確認

02:04 追加のマルウェア配布サイトを確認- filecity.co.kr、bobofile.co.kr

08:50 亜種マルウェアの配布を確認 - superdown.co.kr

09:00 攻撃時間 (3月4日10:00) および攻撃目標 (29 サイト) を確認 (※ 40サイトから訂正)
V3 にシグネチャアップデート

09:30 攻撃目標サイトに事前対応警告

10:00 一次攻撃開始
KCC、対国民へ「注意」警報発令

3月4日(金) 3月5日(土) 3月6日(日)

13:23 緊急対応体制を全社に拡大

17:40 ネットワークシグネチャ配布完了

18:30 二次攻撃開始

(時間不明) KISA、DDoS待避所利用し、ゾンビPC群を確認
KISA、ポホナラサイトで専用駆除ツール提供開始
KISA、3大ISP加入者 1,700万名にポップアップ表示 (最終DL数：1,151万名)

2011年3月5日~ 3.4 DDoS

AhnLab

03:00 アンラボ、亜種マルウェア配布確認
ziofile.com、ondisk.co.kr、luckyworld.co.kr

21:12 アンラボ、C&C サーバーのHDD破壊モジュールの配布確認
V3にヒューリスティックシグネチャアップデート

23:04 (ハードディスク破壊対応用) 専用駆除ツール配布
23:54 (ハードディスク破壊対応用) V3エンジンをアップデート

(時間不明) KCC、対国民警報解除

3月5日(土) 3月6日(日) 3月8日(火) 3月15日(火)

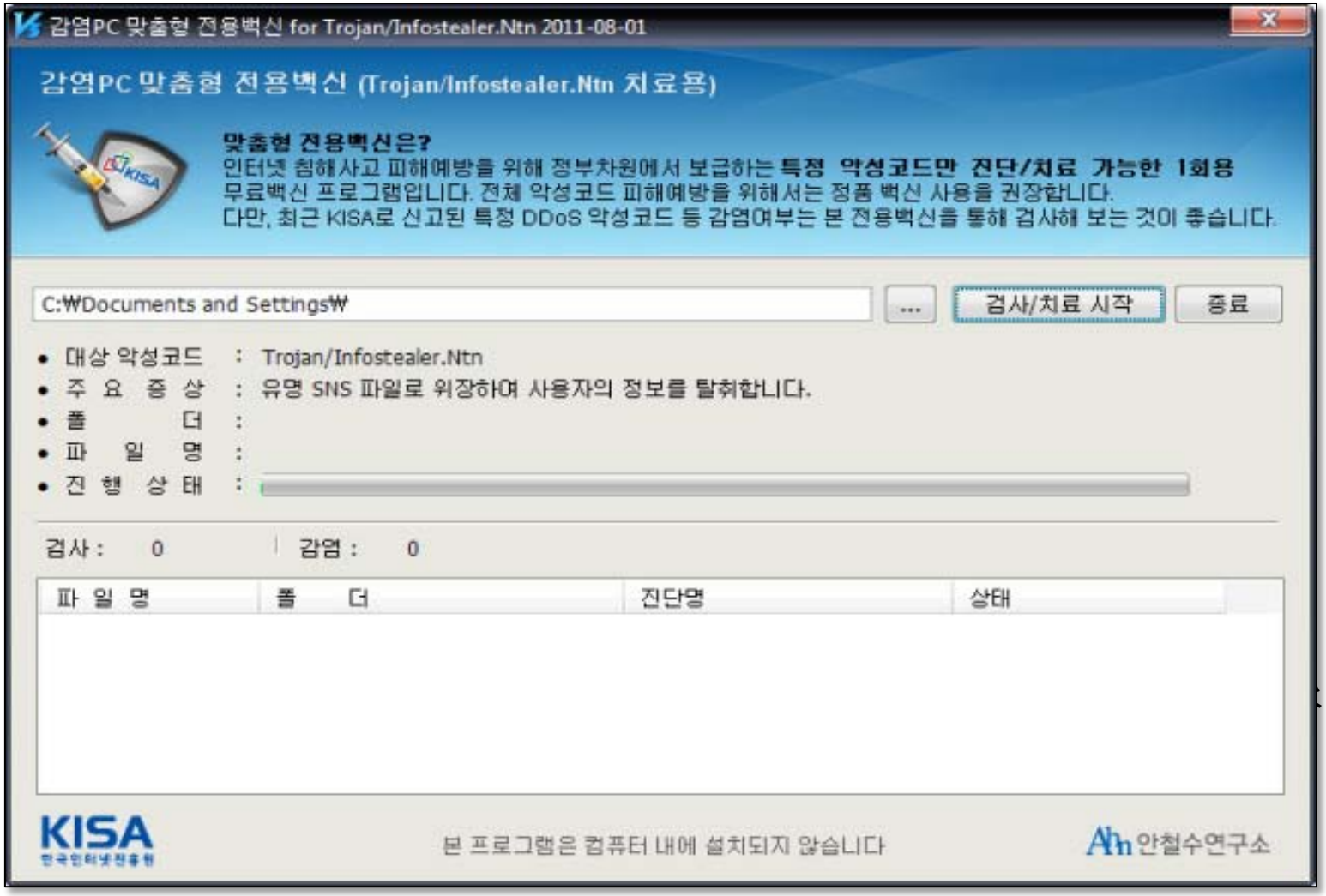
(時間不明) KCC、全国民パソコン安全手順発表
「PC起動時はセーフモードで」
01:58 アンラボ、HDDを直ちに破壊する内容確認
(時間不明) KISA、ポホナラサイト2重化
KISA、24時間無料相談センタ(118)開設
06:21 アンラボ、HDD破壊対応ﾏﾆｭｱﾙ配布
10:08 アンラボ、お客様へ情報発信 (E-mail、SMS)

18:00 アンラボ、緊急対応体制解除

<その他の動き>

KCC、P2Pｻｲﾄﾍﾞﾝﾀﾞ ﾍｾｷｭﾘﾃｨ強化措置指導
KCC、72カ国748ﾏﾙｳｪｱ配布サーバ/C&Cサーバ遮断
KCC、各ﾎﾟｰﾀﾙｻｲﾄからも専用駆除ﾂｰﾙDL措置
行政安全部、有害IP分析／遮断、各機関への通知
(P2Pサイトアクセス禁止)
警察、C&Cサーバ所在35カ国に協調要請文を送付、
捜査に着手

3.4 DDOS 施策…「ゾンビパソコン対策」

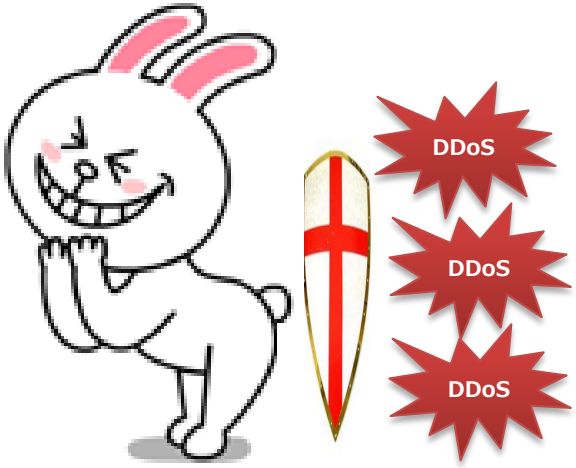


3.4 DDOS 評価~7.7大乱との違い/共通点 AhnLab

	7.7大乱 (2009年)	3.4 DDoS (2011年)
攻撃対象	(米) ホワイトハウスなど主要25サイト (韓)大統領府など韓国主要23サイト	(米)駐韓米軍など2サイト (韓)大統領府ネイバーなど国内主要38サイト
ダウンしたサイト	攻撃対象の多くのサイトが一時的にダウン	なし
攻撃持続時間	7~9の3日間、18時~翌日6時まで	4日10時、18時30分に開始、終了時点不明確
破壊OS	MS Windows 2000/XP/2003	すべてのWindows OS
ファイル構成	同一ファイル構成で複数回の攻撃	攻撃ごとにファイル構成が変化
駆除妨害	なし	ホスト改ざんでセキュリティソフトアップデートおよびホームページアクセス妨害
HDD/ファイル破壊時点	最後のDDoS攻撃日である10日正午に破壊。セキュリティソフトがない場合、システム時間をバックデートすれば防げた	システム時間を変更したり、感染時刻を記録したnoise03.datファイルを削除すると感染後7日、4日だったものが5日夜9時以降は即時破壊に変更
ゾンビパソコン数(KCC発表)	115,044台	116,299台
対応方式	備えがない状態で攻撃され、混乱を招いた	7.7大乱以降、企業/機関の備えがあり、セキュリティベンダと各機関との協調で被害最小化

類似点は、▲マルウェア配布場所がP2Pサイトであったこと、▲攻撃に個人ユーザーPCが使われたこと、▲攻撃形式が事前にすべて計画されていたこと がある

ということで、2度目の攻撃への対応はうまくいったのですが…



そのわずか一カ月後に。

韓国農協に対する攻撃 (DDoSでないAPT)

한국일보 뉴스 오피니언 | 핫이슈 | 포토 · 동영상

전체 정치 경제 사회 국제 문화·연예 스포츠 라이프 피플

사회 | 최신기사 법원·검찰·경찰 교육 노동 날씨·환경 보건복지 수도권 지역소식 사건사고

한국일보 > 뉴스 > 사회

[농협 해킹 北 소행 결론] 검찰이 밝힌 北공격 수법… 근거는

검찰 "악성코드 45자 암호 키, 2차례 디도스 공격 때와 동일"
직원 노트북 좀비PC 만든 후 프로그램 설치 등
7개월 동안 새로운 사이버 테러 치밀하게 준비
檢 "비밀번호만 자주 바꿨어도 큰 피해 막았다"

강철원기자 strong@hk.co.kr

검찰은 3일 농협 전산망 장애 사태 수사 결과를 발표하면서 그 주체로 북한을 지목한 이유와 복잡한 침투 경로를 설명하는 데 상당한 시간을 할애했다. 이번 사태가 북한 소행으로 추정된다는 언론 보도가 이미 여러 차례 나왔기 때문에 검찰이 어떤 근거로 북한을 범인으로 지목했는지가 관심사였다.

검찰은 이런 점을 의식한 듯 이번 사태를 "장기간 치밀하게 준비된 새로운 형태의 사이버 테러"로 규정하며 수사 결과를 상세하게 설명했다. 공식 보도자료 외에 해킹 경로 등을 묘사한 시각물 및 용어

2011年4月12日16:50ごろ、韓国最大の銀行である農協の電算ネットワークのデータが大量に破壊され、数日にわたりサービス利用ができなくなった事件発生

ソース：http://news.hankooki.com/lpage/society/201105/h2011050318250321950.htm#

それでも攻撃はつづく。

【本発表に関するお問合せ先】
株式会社アンラボ
企画マーケティング　愼 麻由美 (しん・まゆみ)
Twitter@AhnLab_Japan
facebook.com/AhnLabJapan
facebook.com/shinmym

Thank you

AhnLab