



技術

V6.2

Main author:

Contributors:

August 5th 2016 (Updated March 19th 2017 JH)

Slavo Greminger (SWITCH-CERT)

Jeroen van der Ham, Jeffeny Hoogervorst, Serge Droz,
Daniel Roethlisberger, Patric Lichtensteiger, Silvio
Oertli, Don Stikvoort



TRANSITS

イントロダクション



© GÉANT 2017

Video duration: 2:49

2 of ...



目次

- Part I 脅威の全容
- Part II マルウェア テクニック
- Part III ハッキング
- Part IV 防御策と軽減策

取り上げるキーワード

- サイバーキルチェイン
- DDoS、DRDoS
- ボットネット
- C&Cサーバ (C2サーバ)
- RAT
- CaaS
- ペイロード、エクスプロイト
- ダークネット
- Tor
- マルウェア
- ウィルス、ワーム、トロイの木馬
- 中間者攻撃
- 防弾ホスティング
- ファイルレスマルウェア
- 脆弱性
- CVE、CVSS
- クロスサイトスクリプティング
- SQLインジェクション
- Bug Bounty
- ボットネットのティクダウン



TRANSITS

Part I 脅威の全容



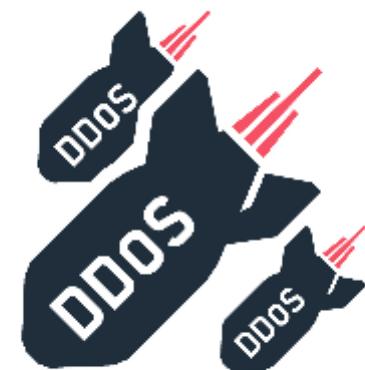
脅威の全容 – 脅威



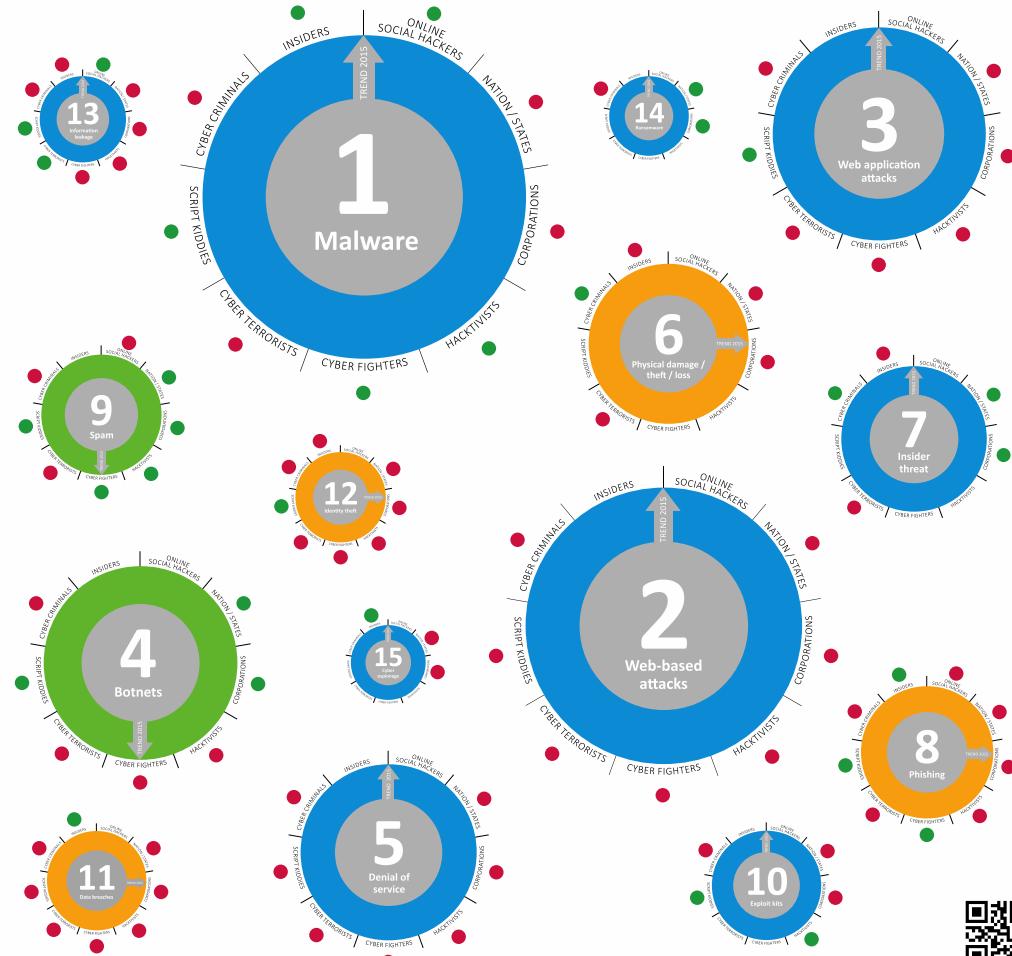
グループディスカッション

サイバーでの脅威とは？

被害者は誰か？



脅威の全容 – 脅威と攻撃者



脅威の全容 – 脅威

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	◐	1. Malware	◐	→
2. Web-based attacks	◐	2. Web based attacks	◐	→
3. Web application /Injection attacks	◐	3. Web application attacks	◐	→
4. Botnets	◐	4. Botnets	◐	→
5. Denial of service	◐	5. Denial of service	◐	→
6. Spam	◐	6. Physical damage/theft/loss	◑	↑
7. Phishing	◐	7. Insider threat (malicious, accidental)	◐	↑
8. Exploit kits	◐	8. Phishing	◑	↓
9. Data breaches	◐	9. Spam	◐	↓
10. Physical damage/theft /loss	◐	10. Exploit kits	◐	↓
11. Insider threat	◑	11. Data breaches	◑	↓
12. Information leakage	◐	12. Identity theft	◑	↑
13. Identity theft/fraud	◐	13. Information leakage	◐	↓
14. Cyber espionage	◐	14. Ransomware	◐	↑
15. Ransomware/ Rogueware/Scareware	◐	15. Cyber espionage	◐	↓

Legend: Trends: Declining, Stable, Increasing

Ranking: Going up, Same, Going down

Source: ENISA Threat Landscape 2015

情報セキュリティ10大脅威2018

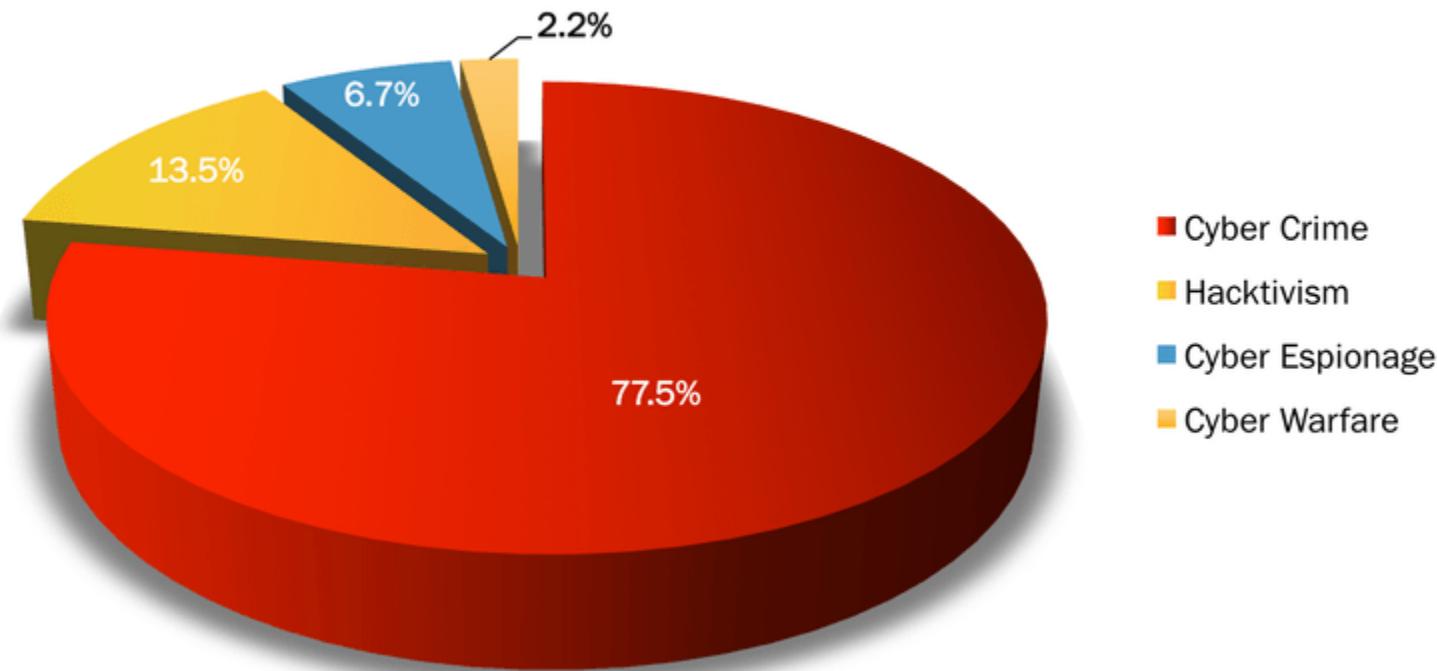
「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングやクレジットカード情報等の不正利用	1	標的型攻撃による被害
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを狙った攻撃	4	脆弱性対策情報の公開に伴う悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するためのセキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT 機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT 機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告によるインターネット詐欺	10	犯罪のビジネス化 (アンダーグラウンドサービス)

<https://www.ipa.go.jp/security/vuln/10threats2018.html>



脅威の全容 – 攻撃者

Motivations Behind Attacks
January 2017

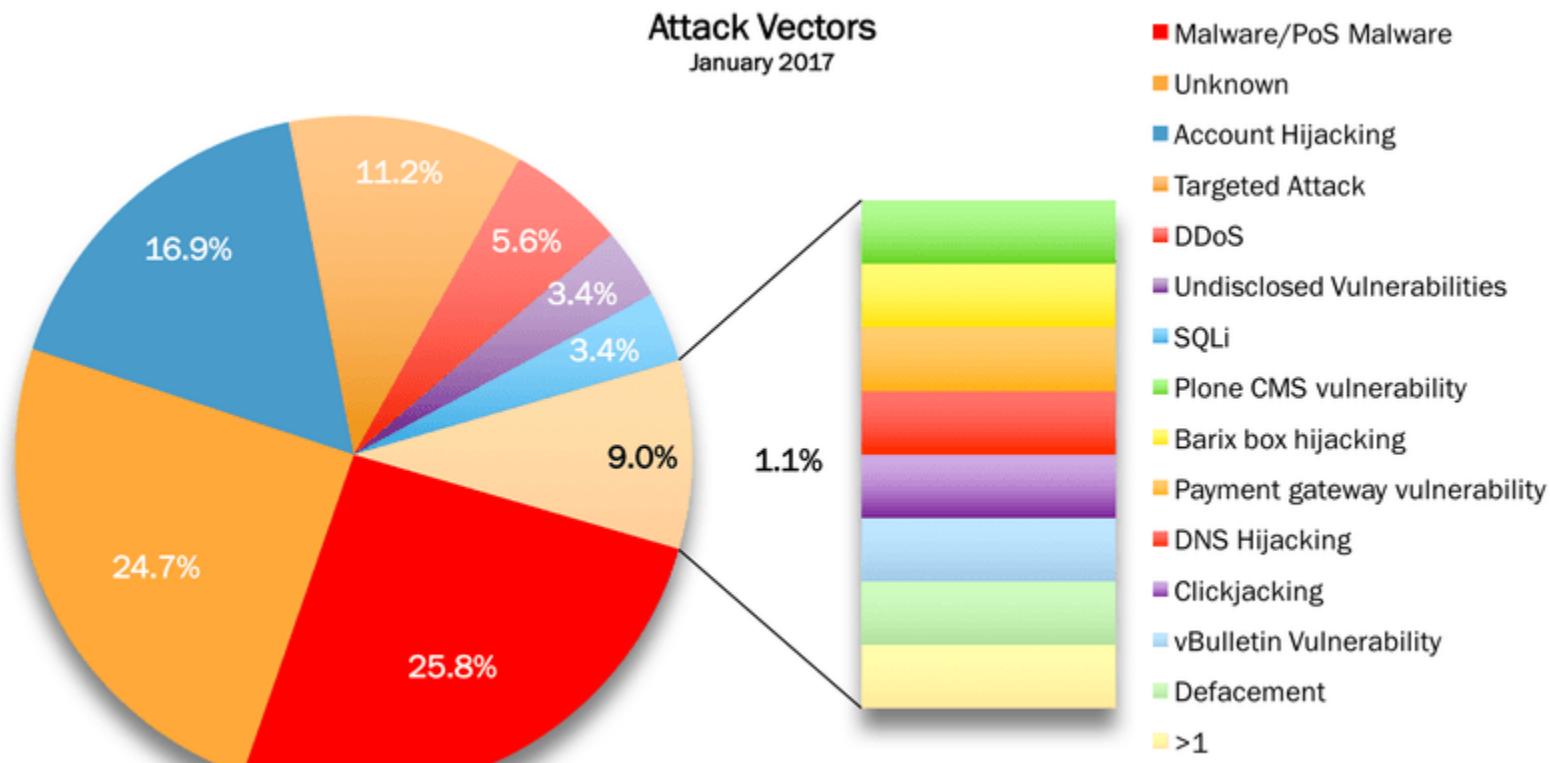


hackmageddon.c

Source: hackmageddon.com



脅威の全容 – 攻撃者

Source: hackmageddon.com



脅威の全容 – 攻撃者たち

- サイバー犯罪者
- サイバーテロリスト
- Hacktivists
- 企業
- 政府
- 従業員
- スクリプトキディ



脅威の全容 – 脅威と攻撃者



グループディスカッション

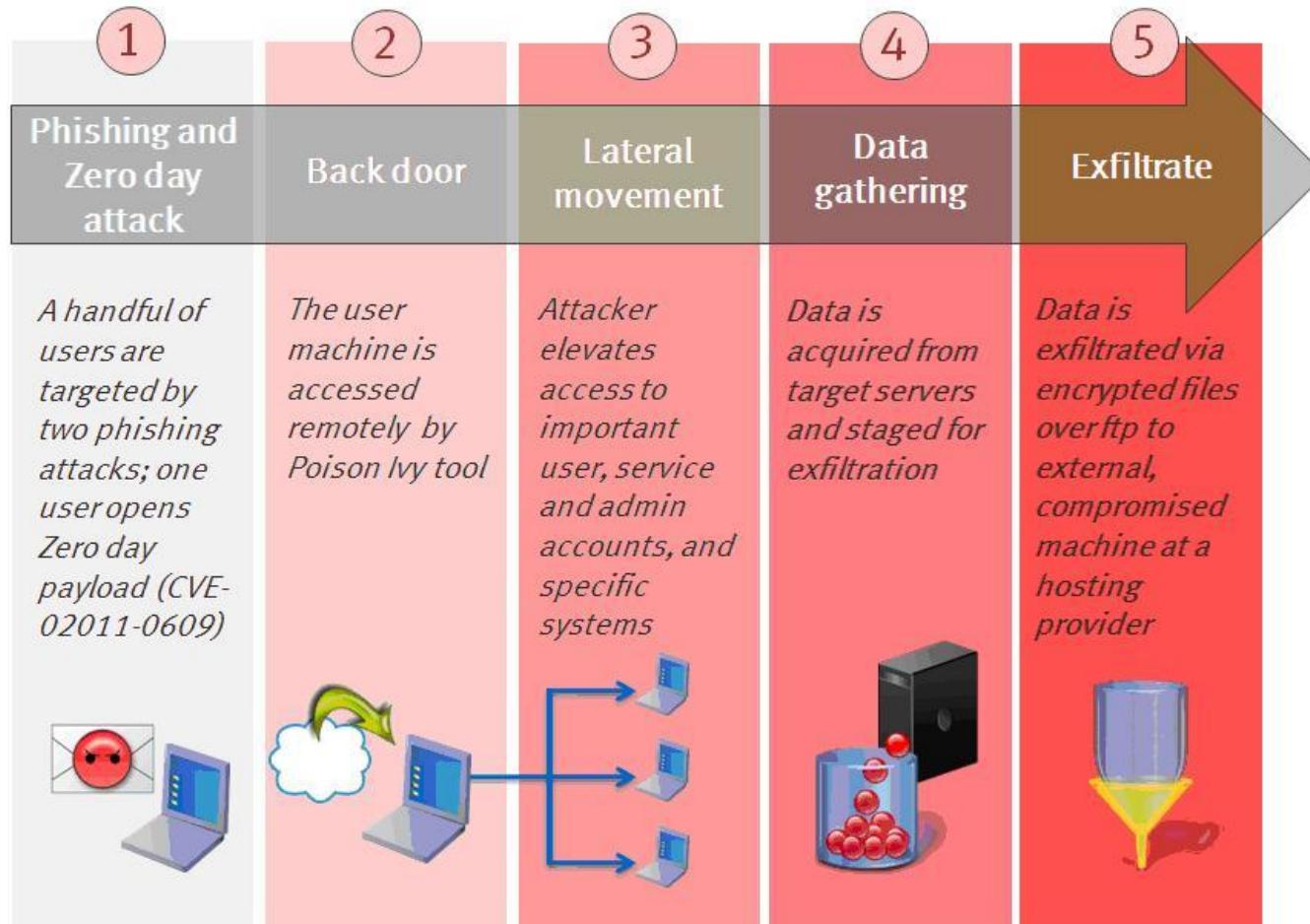
それぞれの攻撃者はどのような手段で攻撃をするか?



- Advanced
 - 特別の役割と目的を持つ
 - 機密情報の収集、通信の傍受、コンピュータへの侵入に多種多様な技術を用いる
- Persistent
 - 長期間 (数年間)
 - ‘長期間でゆっくりとした’ アプローチ
- Threat
 - 特定のターゲットに対して複雑で効果的な攻撃
 - 政府
 - 多国籍企業/ 組織
 - 攻撃の被害は甚大: 大規模な損失



脅威の全容 - ターゲットアタック(APT)



Source: RSA 2011

サイバーキルチーン

- 標的型攻撃における攻撃者の行動(攻撃の手順)を構造化したフレームワーク

	偵察	配送	攻撃	インストール	遠隔操作	侵入拡大	目的達成
攻撃例	<ul style="list-style-type: none"> 外部からの脆弱性スキャン 社員のSNSの情報収集 フィッシングメールを送信 	<ul style="list-style-type: none"> マルウェア付きメールを送信 なりすましのメールを送信 悪意のあるWebサイトのURL付きメールを送信 脆弱性を悪用した外部からのコマンド実行 	<ul style="list-style-type: none"> ユーザに添付ファイルを開かせる 悪意のあるWebサイトにアクセスさせる 悪意のあるコマンドを実行させる 	<ul style="list-style-type: none"> 添付ファイルを実行したことによるマルウェアへの感染 悪意のあるWebサイトにアクセスした事によるマルウェアのダウンロード・感染 悪意のあるコマンドを実行した事による設定の変更、さらなるマルウェアのダウンロード 	<ul style="list-style-type: none"> データの採取 さらなるマルウェアのダウンロード OSの設定変更、OS情報の送信 	<ul style="list-style-type: none"> 同じネットワークに存在する別の端末への感染拡大 	<ul style="list-style-type: none"> 目的の情報・データを外部へ送信 目的の設定・バックドア・トロイの木馬を埋め込み



A Denial of Service 攻撃
(DoS攻撃) の目的は以下の
ようなサービスの停止である

- フローディング
 - 帯域の利用
 - 大量接続
 - ...
- サービスのクラッシュ



近年はストレステストとして
知られている



脅威の全容 - [DR]DoS

- Distributed Denial of Service attack(DDoS攻撃)



Botnet Mariposa 2009: 13 Mio zombies

Source: rivalhost 2013



- Distributed Denial of Service attack
(DDoS攻撃)
 - Booterの増加
 - Booterのshell script は、効率的に大量トラフィックを送付することができるPHP/ASP/Perl scriptである。概して、それらは（無罪の）ウェブサイト上に設置される



A screenshot of a web browser window titled "DeLiRium's DoS .ASP Script". The URL bar shows "192.168.135.170/booters/asp-dos.aspx/?site=www.prolexic.com&port=80×=100". The main content area displays the text "Attack executed successfully." repeated ten times, indicating a successful denial-of-service attack.

Source: Prolexic



TRANSITS

脅威の全容 – **Anonymous DDoS Hack Tools**



- Distributed Reflection Denial of Service attack(DDoS攻撃)
 - ボットネットは必要ない。既存のUDPサービスを利用するだけでよい
 - リクエストを増加させるようなサービスを悪用する : DNS, NTP, SNMP, ...
1つの小さなクエリーから、1つの大きな返答
 - この悪用はFirewallのルールによって無効化することができる
 - 特徴的な**増加要因**
 - DNS: ~50-100
 - NTP: ~500-5000
 - SNMP: ~6-12



脅威の全容 – [DR]DoS



ケーススタディ

Spamhausに対するDRDoS – ピーク時: 300 Gbps



TRANSITS

脅威の全容 - [DR]DoS



はブロックリストの提供を実施。
CB3ROB aka Cyberbunkerとして知られるホスティング事業者のホストより、Spamhausは大量のDRDoS攻撃を受けた。
*off-sho.re*がその攻撃に利用された。

Wed Oct 31, 2012 7:46 am | PROFILE | PM | QUOTE

off-sho.re
LEVEL 2

Joined: 15 Jan 2013
Posts:
Rep:
Location: /dev/ttys0

DDoS bots are 90s.

DNS amplification attacks can bring upto 140Gbps to a single resource from a single controller. the beauty of it that the "bots" are just open DNS resolvers in the world.

Some BP hosters were lately united, check our latest prank :

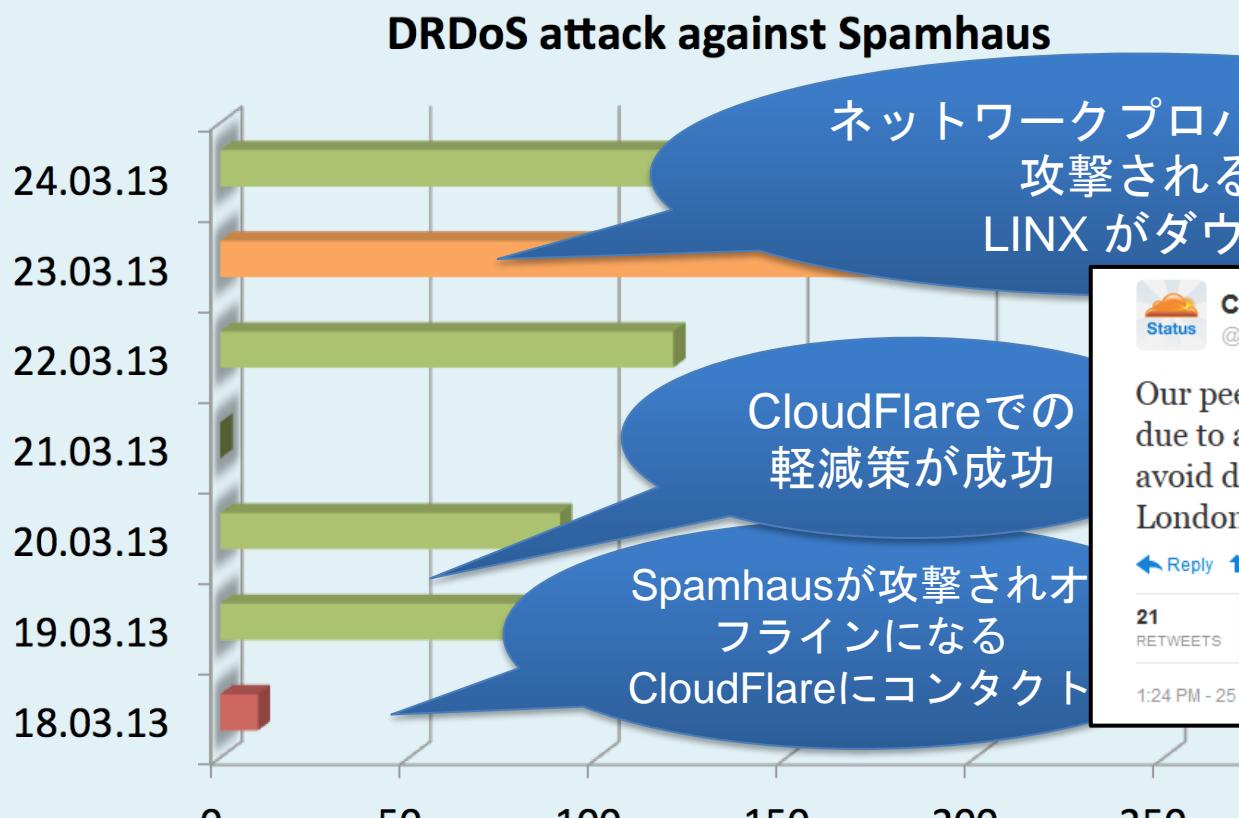
<http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho>

Dirty hoster. Recommended by Spamhaus.
<http://www.spamhaus.org/sbl/query/SBL182932>

Wed Mar 20, 2013 10:36 pm | PROFILE | PM | EMAIL | ICQ |

Display posts from previous: All Posts Oldest First Go

- 利用されたテクニック: DNS Amplification Attack





TRANSITS

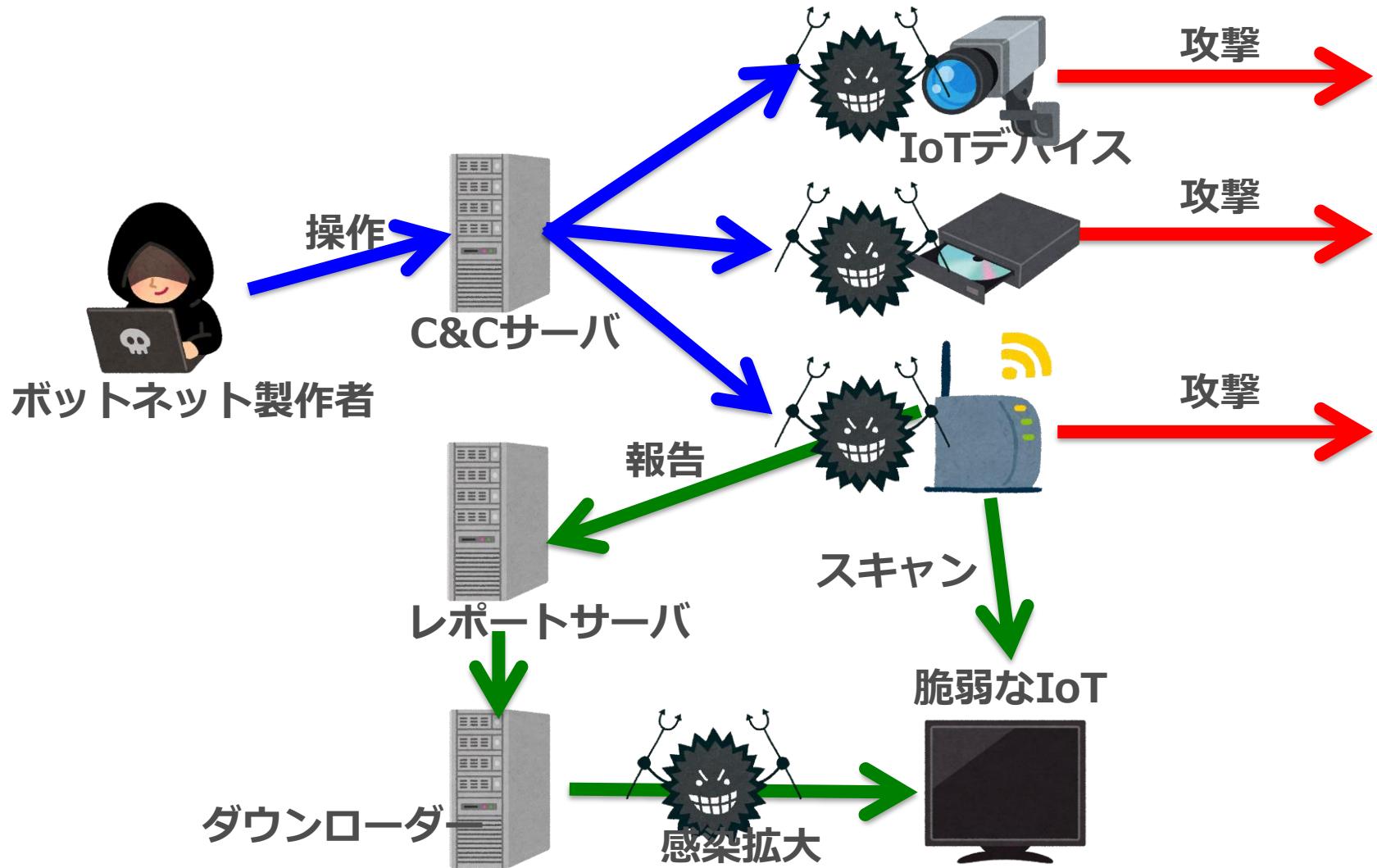
Threat Landscape – [DR]DoS



Mirai概要

- 監視カメラ、DVR、ホームネットワーク機器、ルータなどのIoT機器をターゲットとするマルウェア
- Telnetで接続し、簡単な辞書攻撃で突破できるデバイスに感染する
- ボットネットを構築し、大規模なDDoS攻撃を行う
- Miraiのソースコードが公開されている
 - C&Cサーバ機能
 - ボット機能
 - ボットプログラムを頒布するためのダウローダー機能
- Miraiから派生して登場したマルウェア
 - HAJIME:Miraiが侵入で使うポートを残らず塞ぐ
 - BrickerBot:デフォルトのパスワードを使っているIoT端末をネットで検出すると、そのストレージを破壊し、ネットから完全シャットアウト
「Miraiの拡散を抑えるために考案した」とマルウェア作者は主張している。
※ **PDoS攻撃** = Permanent Denial of Service攻撃
 - PERSIRAI : ネットワークカメラを対象

Mirai動作概要



DDoS被害

- Krebs on Securityへの攻撃 665Gbps
- フランスのウェブホスト OVHへの攻撃 1.5Tbps
- DNSプロバイダサービス「Dyn」への攻撃 1.2Tbps
 - Twitter、Spotify、Reddit、Netflix、Wall Street Journalなど多くのサービスが、主に米国で約6時間にわたって利用できなくなっていた

Mirai DDoSの種類

攻撃の種類	攻撃概要
UDPフラッド	UDPパケットを大量に送り付ける攻撃
VSEフラッド	ゲームエンジン「Source Engine」に対するUDPフラッド攻撃
DNSリゾルバフラッド	DNSに存在しないドメインの名前解決要求を送り付ける攻撃
SYNフラッド	SYNパケットを大量に送り付ける攻撃
ACKフラッド	ACKパケットを大量に送り付ける攻撃
TCP STOMPフラッド	PSHパケットとACKパケットを大量に送り付ける攻撃
GRE IPフラッド	GREプロトコルでカプセル化されたパケットを大量に送り付ける攻撃
GRE イーサネットフラッド	イーサネットとGREプロトコルでカプセル化されたパケットを大量に送り付ける攻撃
プレーンUDPフラッド	ヘッダなどを省略して高速化したUDPフラッド攻撃
HTTPフラッド	HTTPリクエストを大量に送り付ける攻撃

Mirai botnet as a Service

- 2016年10月1日にソースコードをリリースし、そのわずか4日後にはMiraiに感染した機器をDDoS攻撃のプラットフォームとして貸し出す「Mirai botnet as a Service」がアンダーグラウンドで売買され始めていることが確認される。
- MiraiのC&Cサーバのデータベースのusersテーブルには、usernameやpasswordの他に、max_botsやlast_paid、cooldown、duration_limitなどのカラムがあり、それらのカラムが攻撃コマンドの作成時の処理に利用されている。ユーザーごとに利用できるボットの数の上限や、攻撃間隔の制限、アカウントの有効期限などが存在するようです。加えて、ユーザーがボットネットの所有者に最後に金銭を支払った時間などもC&Cサーバのデータベース上に保持されていると考えられる。



DDOS ATTACK with my Botnet: 24 hours ddos on your website target

USD 30.12 (including 2.35 transaction fee)

฿ 0.0118

In stock

Shipping options

Please select an option...

Quantity: 1

 Buy Now

Vendor

amelia75 [+6|0] Level 1 (7)

Class

Digital

 Question

 Report

 Details

 Feedback

Listing Details

DDOS ATTACK: I will point my botnet on your website target DURING 24 HOURS.

If your target is DDOS protected by Cloudflare, Incapsula, Akami or any other kind of protection, please order my offer twice.

No Guarantee of downtime as the target can mitigate the attack in some ways but I will do my best to provide the maximum downtime possible during these 24 hours.

99% SATISFACTION on AB, please check following link: alphabaywyjrktqn.onion/listing.php?id=199254&tab=3

Another advantage of the DDOS attack that you probably don't know is the loss of Google Organic Ranking. Google really don't like unreachable URLs or slow website. As soon as they find a decrease of availability or speed, your target will be temporary removed from results and then it will lose his Google ranking. Two weeks after a four days DDOS attack, I have seen a website going from first page to third page.

DoS攻撃の脅迫

DoS攻撃の脅迫をするハッカーグループ（2017年）

- Almada Collective
- Phantom Squad

件名： Ransom request: DDoS Attack!!!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [REDACTED] will be DDoS-ed starting [REDACTED]. if you don't pay 10 Bitcoins @ [REDACTED]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([REDACTED]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [REDACTED], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

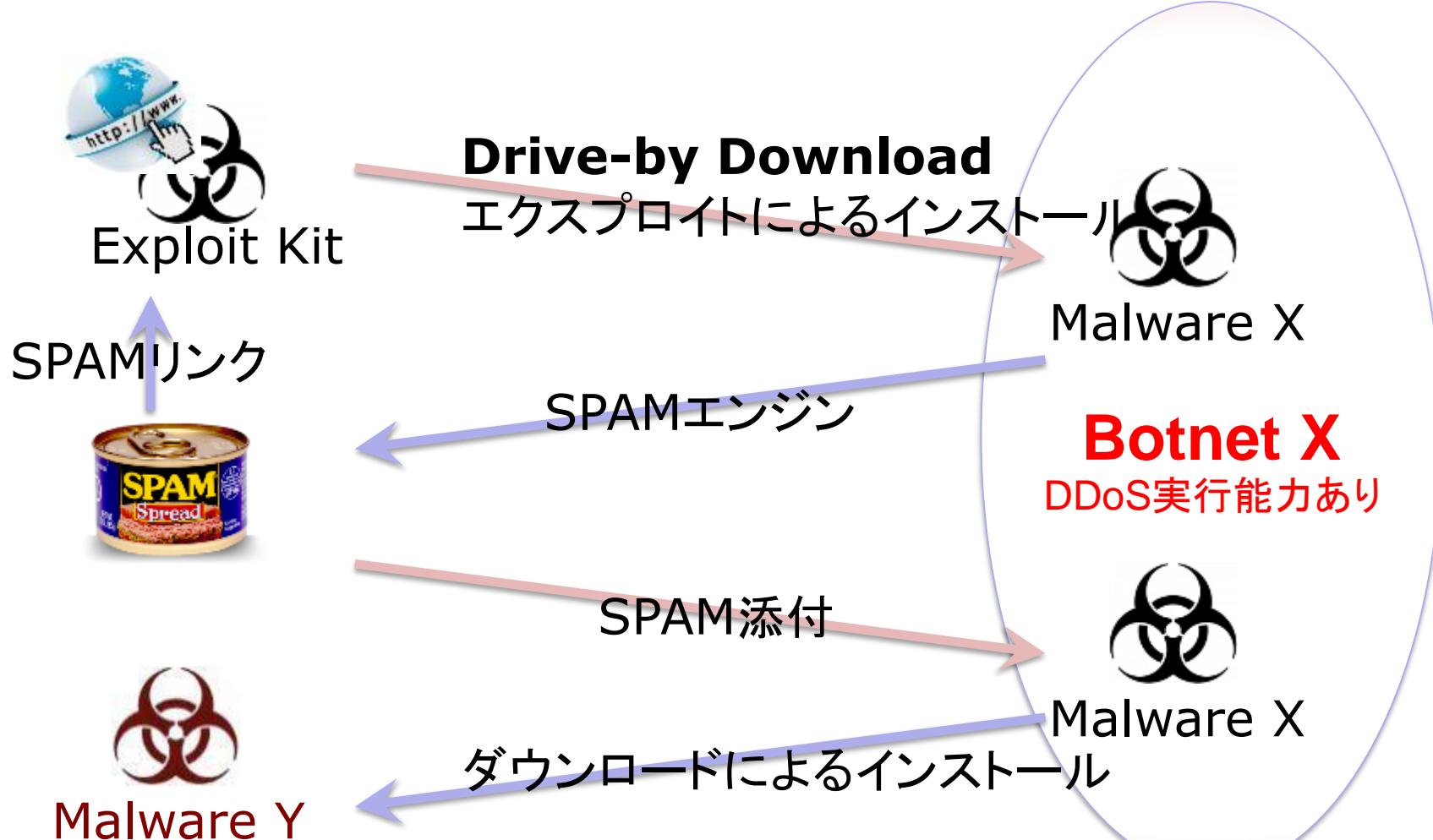
Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [REDACTED]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

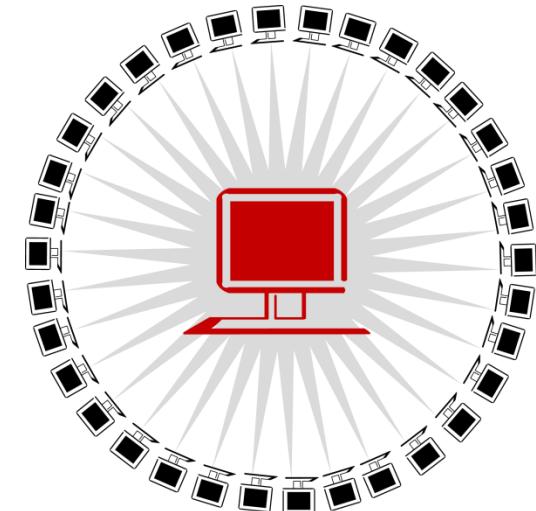
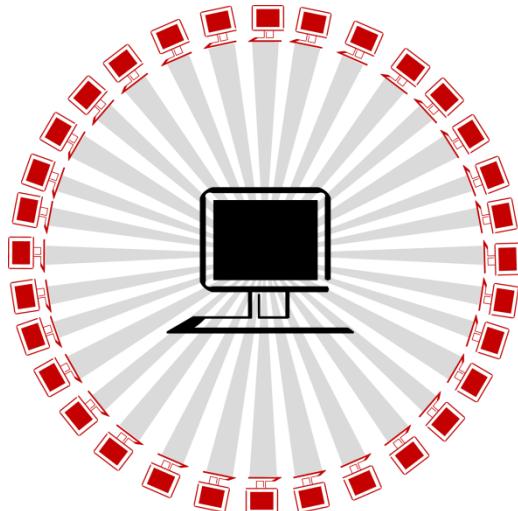
<https://www.jpcert.or.jp/newsflash/2017062901.html>





脅威の全容 – ボットネット

- ボットネット: さまざまな脅威の根幹
 - 感染したマシン、ボット/ドローン/ゾンビと呼ばれる
 - エンティティと呼ばれるボットハーダーより外部から操作可能
 - 中央集中型 (IRC,HTTP) 分散型(P2P)





- ボットネット: さまざまな脅威の根幹 – なぜ?
...たくさん の 利益を 生む こ と が で き る た め
 - クリック・フラウド
 - スパム / フィッシング
 - マルウェア配布
 - 個人情報の収集
(生年月日, 認証情報,
クレジットカード)
 - APT 踏み台サーバ
 - プロクシ
 - DDoS





- ボットハーダーの稼ぎ方
 - 動作主体
 - e.g. bitcoinマイニング
 - サービスプロバイダー
 - e.g. マルウェア配布 1\$/インストール
 - e.g. ボットネットのレンタル
 - e.g. スパム業者のスパムメール配信代行
- スパム業者の稼ぎ方
 - サービスプロバイダー
 - e.g. 広告や詐欺内容の送信
 - e.g. マルウェアの送信
 - e.g. drive-byサイト / フィッシングサイトのリンクの送信



- アンダーグラウンドの定義

“アンダーグラウンドやブラックマーケットは、商品またはサービスが違法に取引されている市場である。より正確には、取引 자체が違法であり、商品やサービスは問わない。”

- さまざまなタイプの人々が関与している:

マネーミュール, 翻訳者, ホットラインオペレータ, ビデオクリエーター(gwapoなど) etc.



犯罪と闘うために、攻撃者の視点から考える必要がある…

Crime as a Service

ビジネスモデル:
世界最大のスパ事業者

- 広告や詐欺
- マルウェア
- drive-byサイトへのリンク / フィッシングサイト



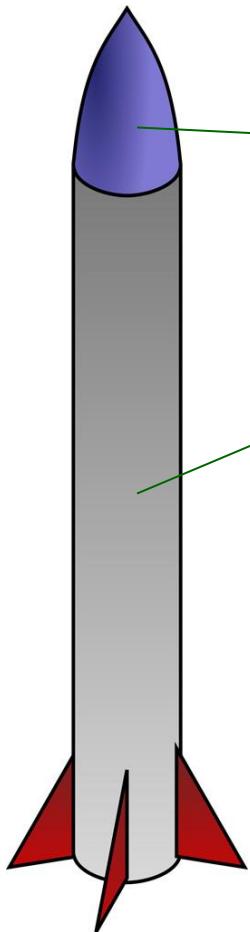


脅威の全容 – CaaS



Source: Wikipedia (Tom-b)

エクスプロイトとペイロード



- **ペイロード (Payload)** : 脆弱性を突いた後に実行されるコード。トロイの木馬、ランサムウェア、バックドアなど
- **エクスプロイト (Exploit)** : 脆弱性を突いてペイロードを攻撃対象に届ける
エクスプロイトキットの例
 - **EternalBlue** (NSAツール Fuzzbunch)
 - **EternalRomance** (NSAツール Fuzzbunch)
 - **Angler Exploit Kit**
 - etc.



Step-by-stepガイド:

1. ペイロード購入 (e.g. スパムエンジン)



Step-by-step guide:

1. ペイロード購入 (e.g. スパムエンジン)
2. exploit kit (EK)のレンタル
 - Angler
 - FlashPack
 - Infinity aka RedKit aka Goon
 - Niteris aka CottonCastle
 - Nuclear Pack
 - Rig
 - ...



Source: Kahu Security



Step-by-step guide:

1. ペイロード購入 (e.g. スパムエンジン)
2. exploit kit (EK)のレンタル
3. Pleskを狙ったの0dayを購入
4. ウェブサイトへの訪問者へのウイルス感染拡大のためウェブサイトへの侵入
5. 大量のマシンへの感染 – どのように?



TRANSITS

脅威の全容 – Malvertisement

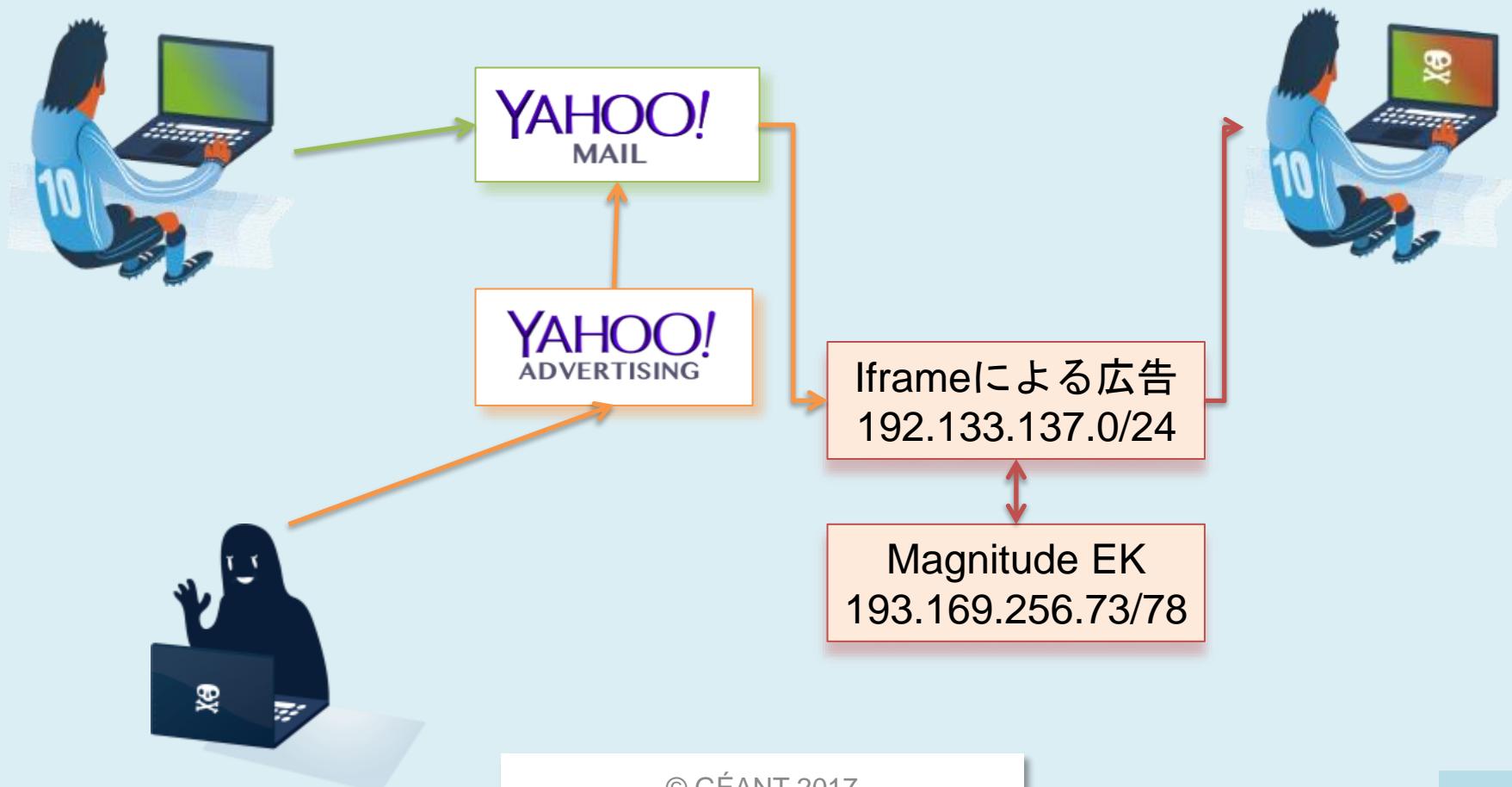


Case Study

Yahoo! Malvertisement – 27,000台感染/時間



脅威の全容 – Malvertisement





脅威の全容 – Malvertisement

- 2013-12-29 19:14 UTC → 2014-01-03 17:15 UTC
ブルーコートより
- Yahoo! Mailに300,000 hits/h → 27,000 感染/h
9%の感染率

~ 3,000,000台の感染 (5日間)

- Magnitude Exploit Kit → 9% の感染率
 - CVE-2012-0507 (Java, 2012/2に修正パッチリリース)
*Java Atomic, Java 6u30, 7u2*より以前のバージョンで動作
 - CVE-2012-4681 (Java, 2012/8に修正パッチリリース)
*Java Gondvv / Gondzz, Java 7u6*より以前のバージョンで動作

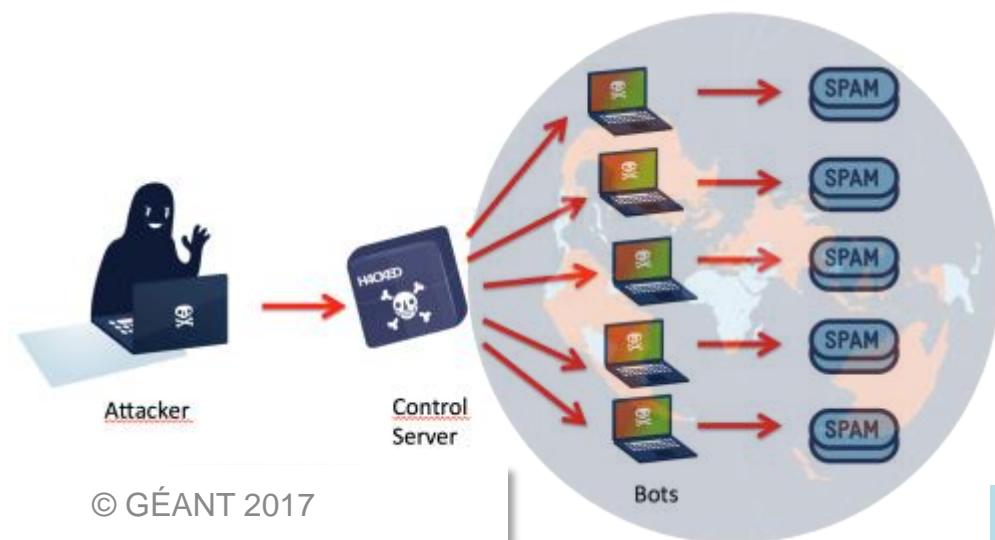


Step-by-step guide:

5. 大量のマシンへの感染

- Malvertisement
- トラフィック分配システム: Traffic Distribution System (TDS)
- ペイロードつきスパム
- マルウェアダウンロードリンクつきスパム

おめでとうございます...





TRANSITS

脅威の全容 – Paunch



Case Study

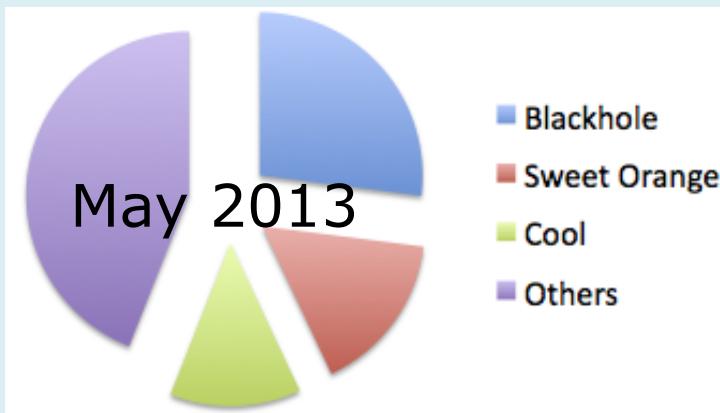
Paunchの逮捕



脅威の全容 – Arrest of Paunch

- Who is Paunch?

- BlackHole Exploit Kitの作成者
BlackHole Exploit Kit は500\$ /月で利用可能
- Cool Exploit Kitの作成者。Cool Exploit Kit は非公式であるが10,000\$ /月で利用可能。
非公開のzero-daysを含む
- Crypt.Amの作者。FUD filesを作成

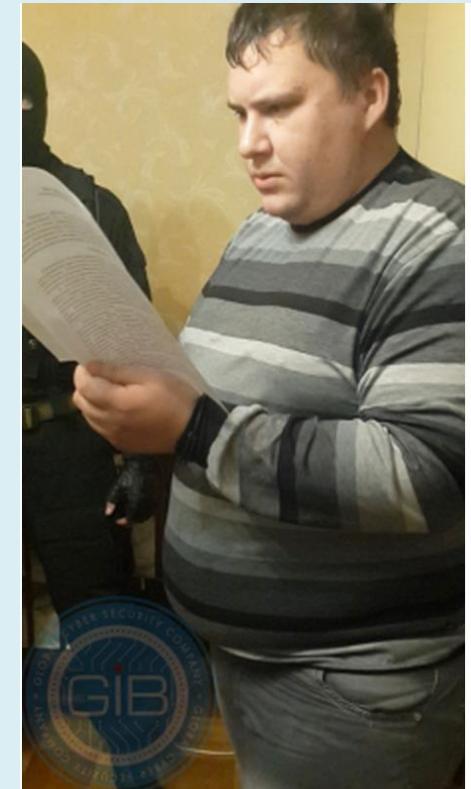


収入: 50,000\$ /月
車: ポルシェ カイエン

Source: GROUP-IB

脅威の全容 – Arrest of Paunch

- 2013/10/4
 - Dmitry E. Fedotovがロシア警察により逮捕される
 - ロシア連邦の刑法第210条を適用: 犯罪者コミュニティの作成と参加/ 1つまたはいくつかの重大もしくは特に深刻なアンダーグラウンドフォーラム
- 興味深い事象: *Torpig* ボットネットが逮捕後に消滅した



Source: GROUP-IB



TRANSITS

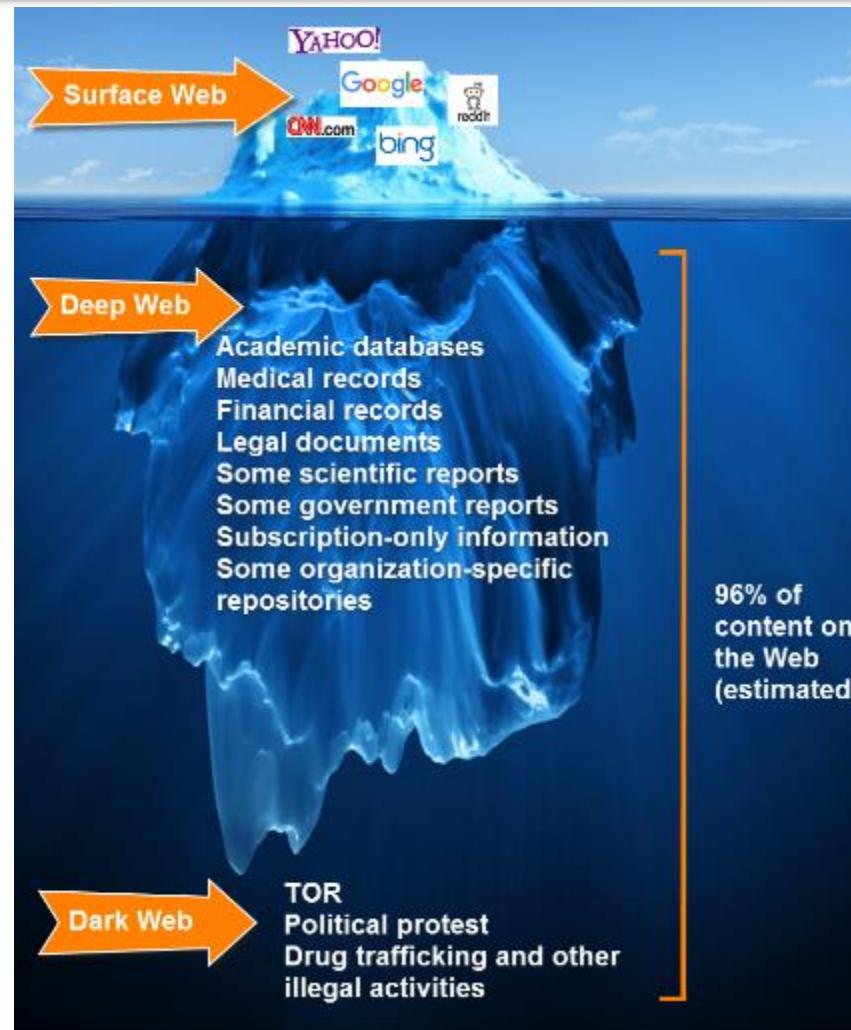
脅威の全容 – Money

HOSTED ON





脅威の全容 – Deepweb and Darkweb





TRANSITS

脅威の全容 – Deepweb and Darkweb



Shop by Category

- Drugs 8,670
 - Cannabis 2,066
 - Dissociatives 165
 - Ecstasy 660
 - Opioids 591
 - Other 455
 - Precursors 50
 - Prescription 2,146
 - Psychedelics 981
 - Stimulants 1,102
- Apparel 264
- Art 127
- Biotic materials 1
- Books 861
- Collectibles 5
- Computer equipment 32
- Custom Orders 68
- Digital goods 509
- Drug paraphernalia 305
- Electronics 77
- Frotica 540

messages 0 | orders 0 | account \$0.00

Search

Go



1g MDMA 82%+ High Quality -Made in Germany-\$1.30



50 gr. Crystal MDMA Rocks-\$23.33



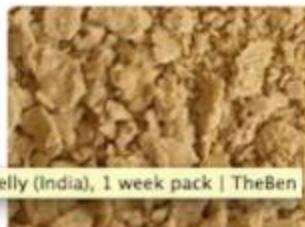
Valium 10mg/ Diazepam (100 Pills)-\$2.32



3g XxX AAA QUALITY WEED,AMAZING-\$0.98



Kamagra jelly (India), 1 week pack-\$0.98



Honeycomb Wax (85% THC) Fully Purged-\$1.45



1 gram ✪ Moroccan Hash ✪ DUTCH QUALITY-\$0.27



Citalopram 10x 20mg tab-\$0.10



TRANSITS

脅威の全容 – Deepweb and Darkweb

Active at Dark Markets? You have our attention.

The Police and the Judicial Authorities of the Netherlands are not only active in the real world, but also in all corners of the Internet. Here we trace people who are active at Dark Markets and who offer illicit goods or services there. Are you one of them? Then you have our attention.



ACTIVE

VENDORS

- DutchCandyShop
- FrankMatthews
- Etos
- DutchFarmerNL
- DutchMagic
- DutchDelights
- FromAmsterdam
- DUTCHRABBIT2
- Partyflockcrew
- DCDutchConnectionGroup
- PartySquadNL
- DrugsFromAmsterdam
- QualityWhite

ARRESTED

VENDORS

- HighQualityTrips
- RuudNL
- XTCExpress
- TheHeineken
- AmsterdamUnited
- HollandOnline
- LowLands
- AlbertHeijn
- The Flying Dutchmen
- HellsGate
- VitaminStore
- Chiquita
- SaltnPepper
- Supertrips

IDENTIFIED

BUYERS

purp*****	from	Hippolytushoef
Stra*****	from	Groningen
unex***	from	Voorburg
pink*****	from	Amsterdam
your*****	from	Nijmegen
xyli****	from	Delft
troj**	from	's-Gravenhage
Piet*****	from	Gendringen
Sera***	from	Groningen
soda*****	from	Bovenkarspel

More info? [Read the FAQ](#)



POLITIE OPENBAAR MINISTERIE

National Police and Public Prosecution Service of the Netherlands

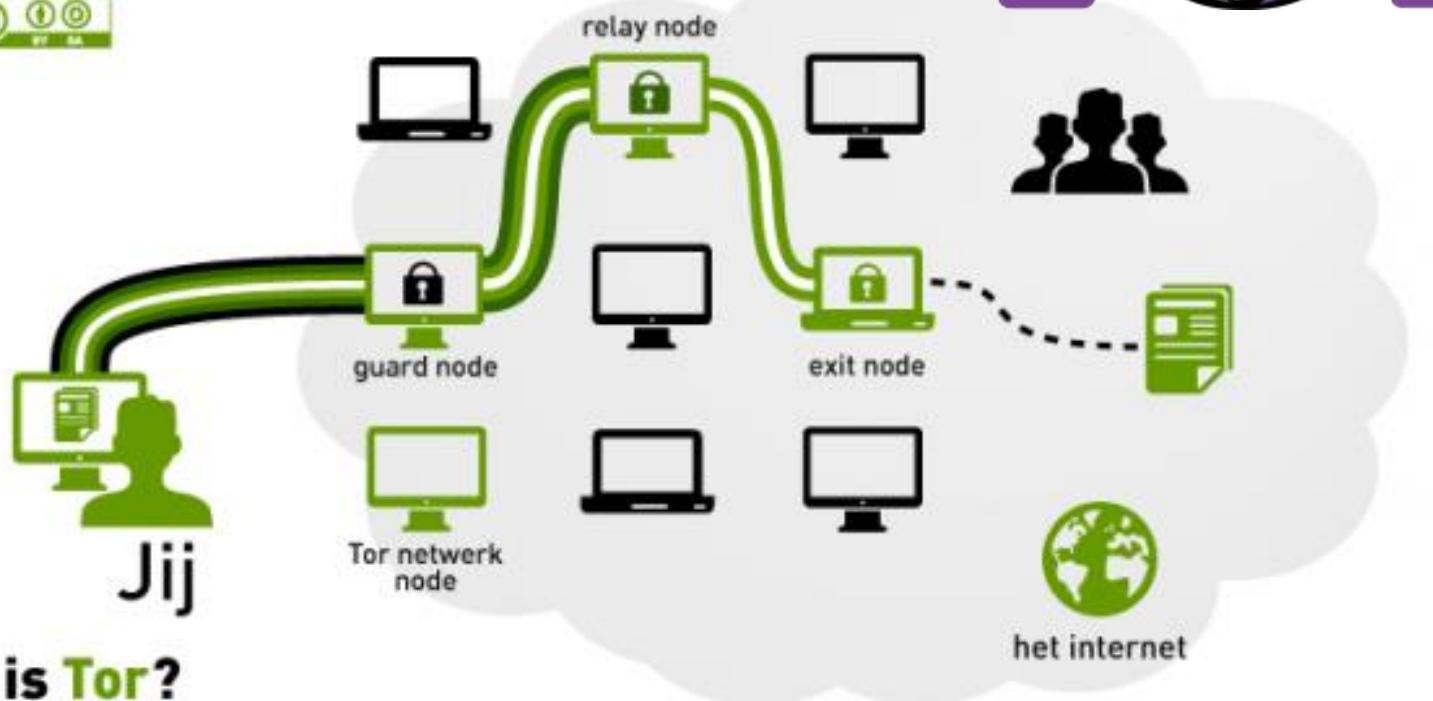
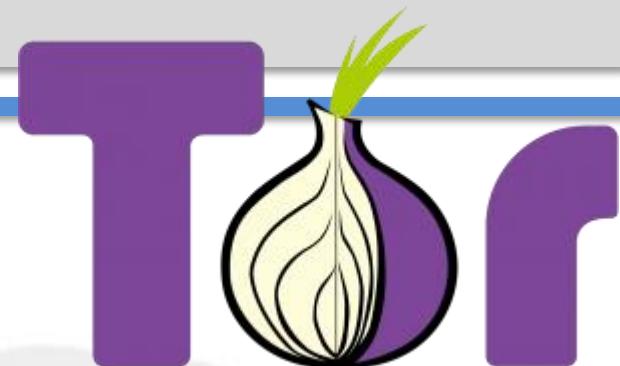


TRANSITS

脅威の全容 – Tor



BITS OF FREEDOM

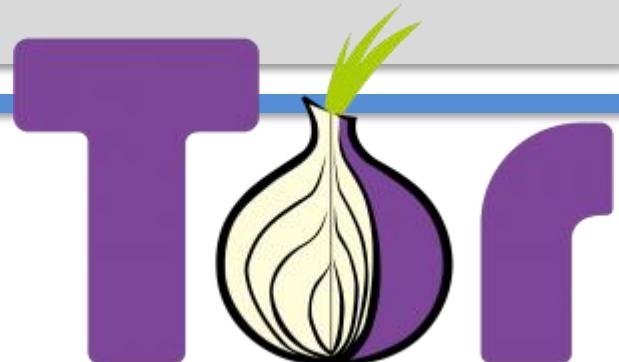


wat is **Tor**?



TRANSITS

脅威の全容 – **Tor**



**PRIVACY
IS NOT
A CRIME**

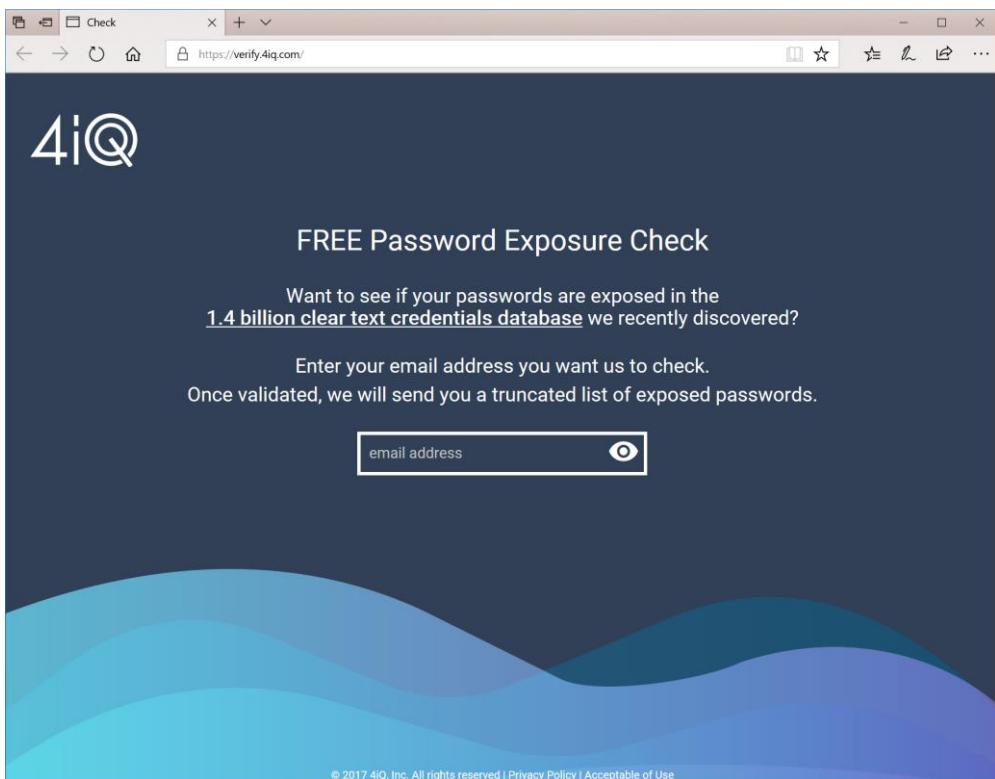
ダークウェブ上の漏洩アカウント情報

過去256件の漏洩事件から流出した平文のID/パスワード情報（ファイルとデータベース）がダークウェブ上で流通していることが分かった（2017年12月に4iQに掲載された記事）

<https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14>

	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac 
9	952446	password1 	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321
18	417878	123456a	38	227701	222222
19	398114	123321	39	226785	555555
20	371627	654321	40	220363	112233

<https://verify.4iq.com/>





TRANSITS

Part II マルウェアテクニック



マルウェアテクニック – 用語

マルウェア(**Malware**) = マリシャスソフトウェア(**Malicious Software**)

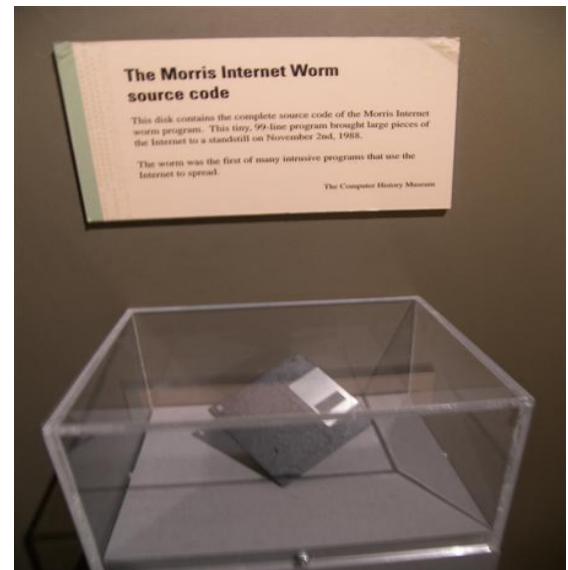
別名: 潜在的に迷惑なプログラム(Potentially Unwanted Programs (PUP))

性質・分類	ウイルス	トロイの木馬	ワーム
	1971 クリーパー	1975 Pervading Animal	1988 モ里斯
確認された年	1983	1200 BC ☺ 1972	1975
感染方法	正規プログラムの一部	正規プログラムの一部	自身のコピー
感染媒体	起動領域、プログラム、ユーザドキュメントファイル	感染端末	感染端末
拡散方法	ユーザ操作	ユーザ操作	脆弱性
拡散状況 (2014)	2.7%	62.8%	2.7%



- はじめてのワーム: Morris(モリス)
 - 1988年
 - メディア報道: <http://www.youtube.com/watch?v=fj8S6Hd-5bk&t=20s>
 - マルウェア作者の目的: インターネットサイズを計測すること
 - 約6,000台の感染
 - 拡散機能がDoS攻撃のように変貌

→この事件後、CERT/CCをはじめとする
CSIRTが各国に確立された





TRANSITS

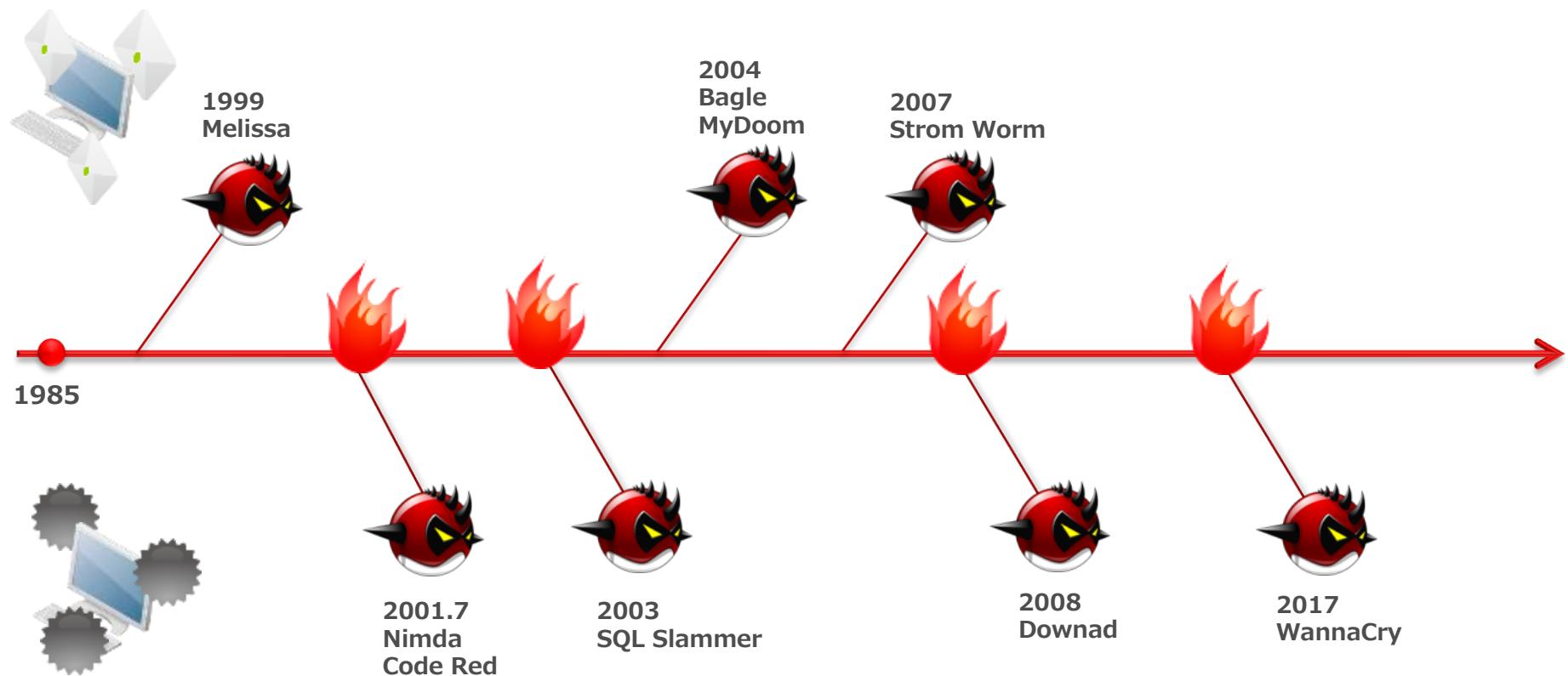
Malware Techniques – Terminology





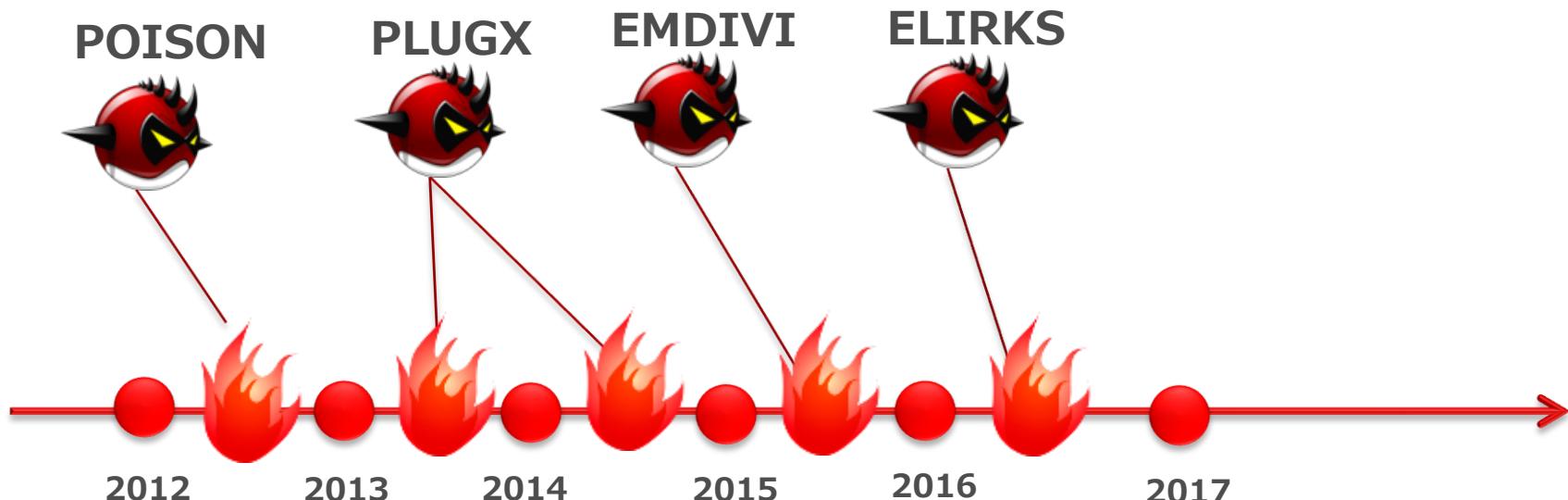
TRANSITS Workshop
NCP Japan

WORMと歴史



【※独自調べ：マルウェア名は通称で記載】

標的型攻撃の系譜



2011	2012	2013	2014	2015	2016
Sony PSN、三菱重工、外務省、衆議院など多くのセキュリティインシデントが発生。	自民党、財務省、国交省などでインシデントが継続、多くの組織でCSIRTが構築、運用が開始される	ソニーピクチャーズなどでセキュリティインシデントは継続。	多くの脆弱性が報告され、ベネッセ事件が発生し対応に、組織が疲弊する。標的型攻撃において、水飲み場攻撃の手法が観測される。	日本年金機構における情報漏えい事案が発覚。	JTBや経団連にて、状漏えい事案が発覚。

【※独自調べ：マルウェア分類は各接頭辞が有名になった年でのマッピングです。】



マルウェア (**Malware**) = マリシャスソフトウェア (**Malicious Software**)

マルウェアの基本動作:

- バックドア
- Bitcoinマイナー / スチーラー
- クリック詐欺
- DoS
- ダウンローダー / ドロッパー
- ランサムウェア
- リモートアクセスツール
- スケアウェア
- スパム・エンジン
- スパイウェア (Banker, Credential Stealer, キーロガー, スニッファ)





WannaCry感染

- IPA ランサムウェア「WannaCry」感染実演デモ
<https://www.ipa.go.jp/security/anshin/mgdayori20170515.html>





グループディスカッション

攻撃者のように考える:
どのようにして、別の銀行口座からお金を盗むのか？

マルウェアテクニック – **VM Zeus**



ケーススタディ

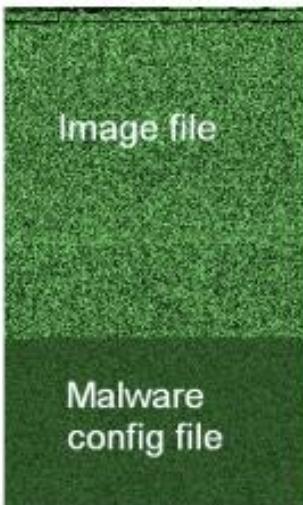
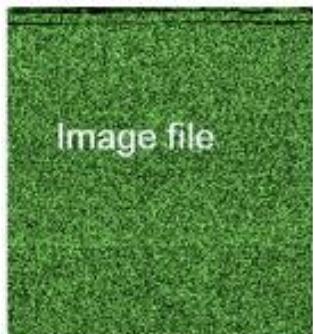
VM Zeus aka KINS aka Zberp

- VM Zeus はバンкиングトロージャン。マン・イン・ザ・ブラウザ(MITB)によって、ログイン情報を盗む





マルウェアテクニック – VM Zeus



00000	FF	D8	FF	E1	13	FE	45	78Ex
00008	69	66	00	00	49	49	2A	00	if..II*.

FF D8 = 画像ファイルのはじまり

80B98	4E	FB	9F	FF	FE	3F	10	00	N....?..
80BA0	00	F8	B7	4F	9B	C8	93	00	...0....
80BA8	00	73	70	75	31	4E	4D	4D	.spu1NMM

FF FE = JPG コメント指示
→ 設定

89F68	53	66	47	61	30	5A	57	55	SfGa0ZWU
89F70	3D	FF	D9						=..

FF D9 = 画像ファイルの終了位置



このコンフィグの場合には、簡単に発見することができる

The screenshot shows a hex editor window titled "pixel.jpg". The interface includes a toolbar with Save, Copy, Cut, Paste, Undo, and Redo buttons. Below the toolbar is a menu bar with "File", "Edit", "View", "Tools", "Help", and a "File" dropdown. The main area has tabs for "Hex", "Text search", "Go To Offset", and "Find (Text search)". The hex dump shows memory starting at address 800400. The ASCII view shows the corresponding characters. A specific section of the ASCII data is highlighted in blue, containing the bytes F FF FE 3F 10 00 followed by several characters and then the string "...\\..5....SK...o.K..N...?...". Below the editor is a status bar with "Type", "Value", "8 bit signed", "8 bit unsi...", "16 bit signed", "16 bit uns...", "Hex", "Little Endian", "Insert", "ASCII", "Offset: 0", and "Selection: 0".



概要(まとめ)

- サーバの必要性
 - 感染端末の資格情報を受け取るため
 - コンフィグファイルのアップデートのため
- 管理可能で柔軟なネットワークインフラが必要である
- 必要なメカニズム
 - アンチウイルスソフトから検出されないためのメカニズム
 - 感染したホスト上にてサーバとの接続性を確立するためのメカニズム
- より効率的なホストへの感染を必要とする



- Bulletproof Hosting
- Fastflux
- P2P

- Level 1: Bulletproof Hosting
 - 匿名化されたホスティングサービスを指す。IPアドレスの偽装、不正アクセス、迷惑メールの大量送信、機密情報の流出などコンピュータ犯罪に使われる
 - 多くの場合、ホスティング元にログは全ての状態で残っていない
 - 例: CyberBunker (オランダ)



STAY ONLINE

Product	Fee
Impenetrable Hosting Facility	€ 0.-
Concealed Location	€ 0.-
Anonymous Hosting	€ 0.-
"Mind Your Own Business" Policy	€ 0.-

If it is important to you that your servers



インターネットで最も危険な街 (Norton)

防弾ホスティング会社を実際に訪問したドキュメンタリー (2017.5.11)

<https://jp.norton.com/mostdangeroustown2>



[前作] インターネットで最も危険な街を訪ねて (2015.9.30)
- https://www.youtube.com/watch?v=F_XO2FzX5ic

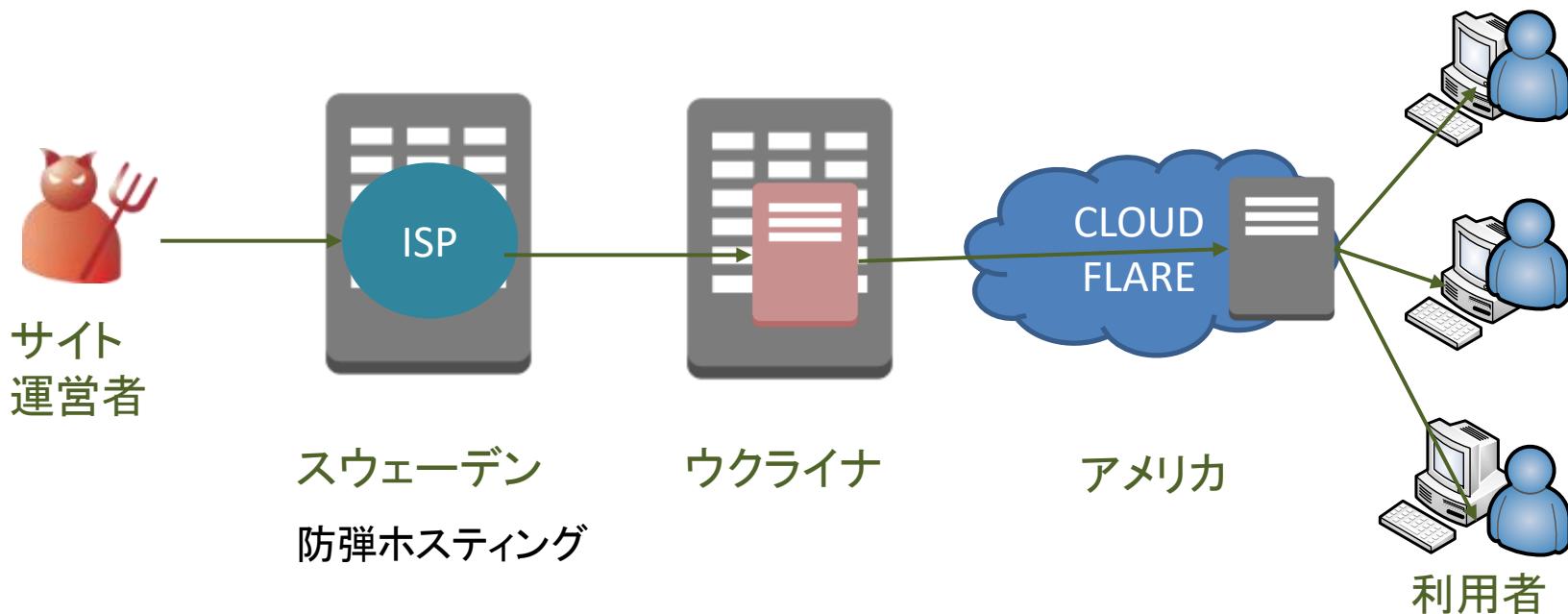
「漫画村」の追跡 (NHKクローズアップ現代)



2018年4月18日 NHKクローズアップ現代

追跡！脅威の“海賊版”漫画サイト

<https://www.nhk.or.jp/gendai/articles/4118/>

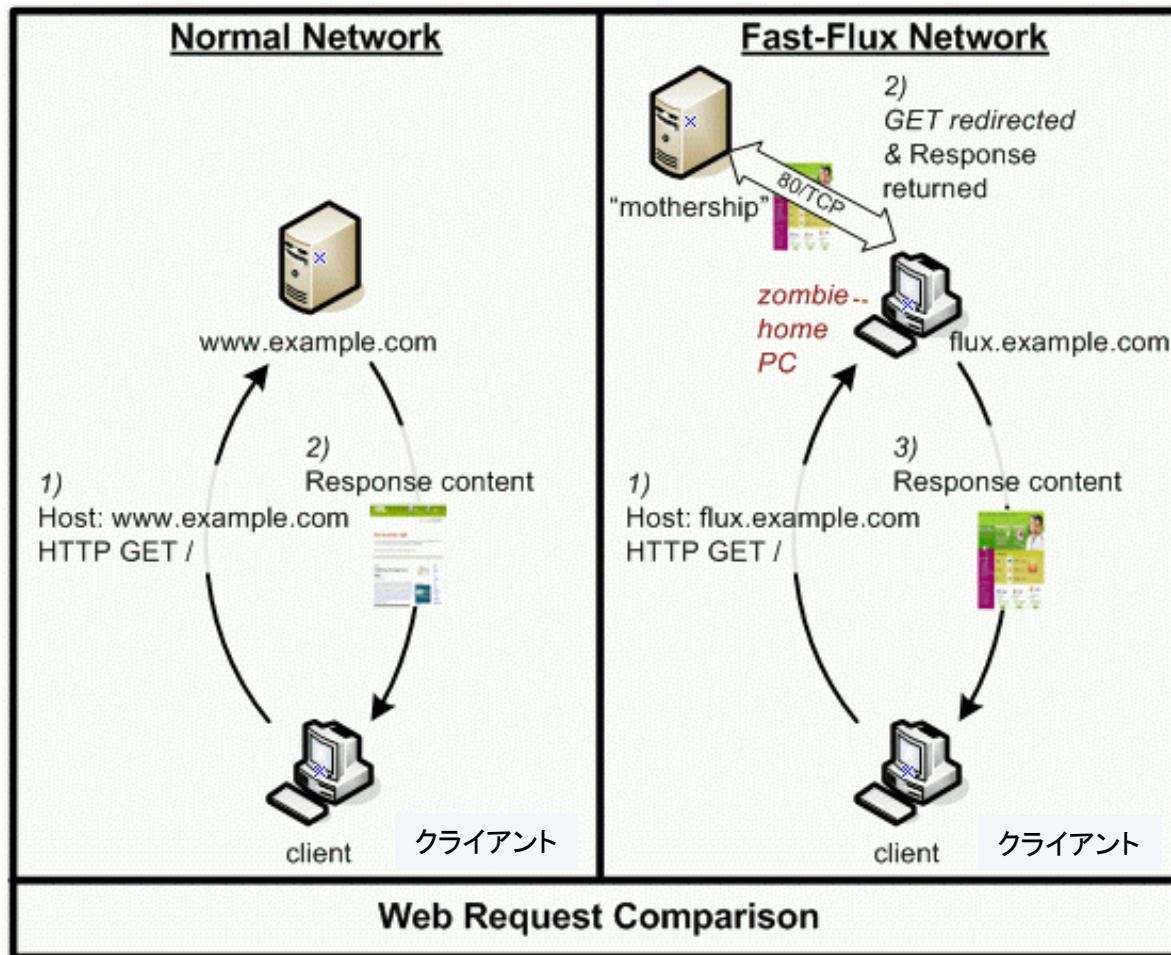




- Level 2: Fastflux
 - 課題: IPサーバーのIP範囲をブロックすることができる Cyber Bunker がブロックされることがある
 - 解決方法: Fastflux



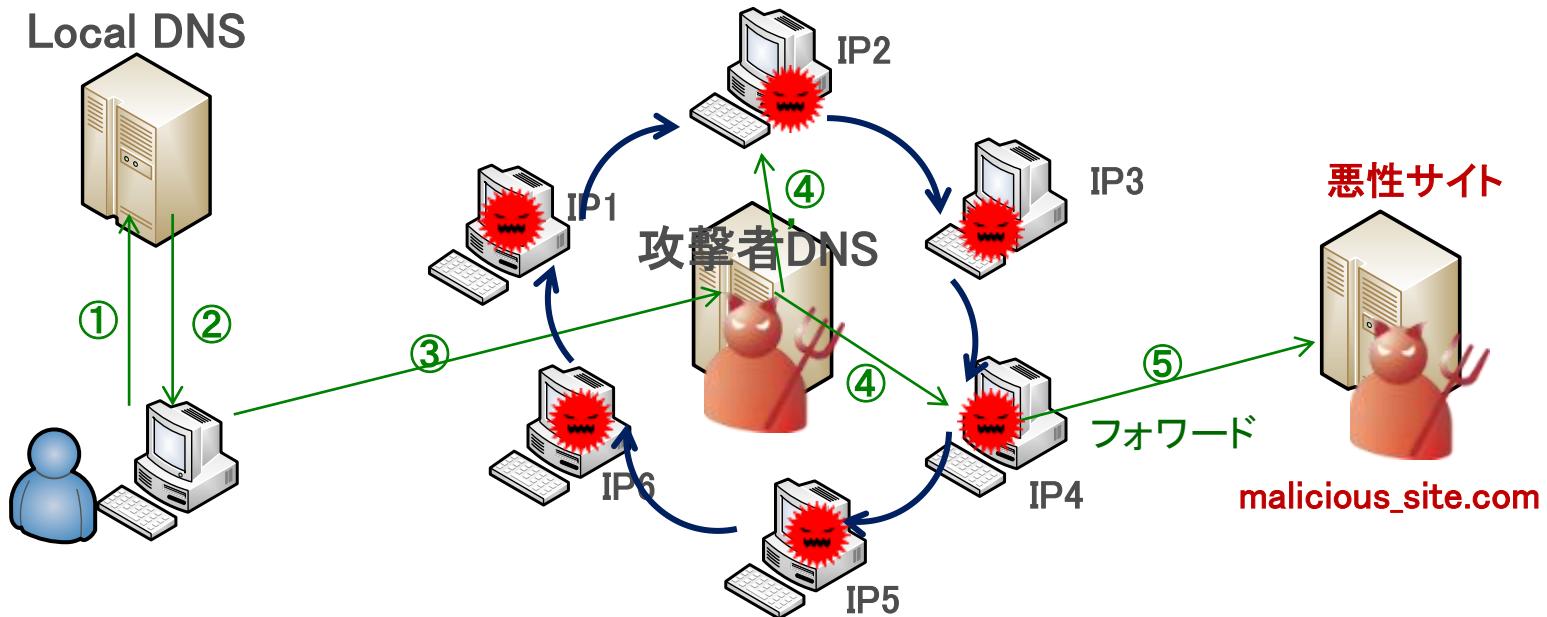
- Level 2: Fastflux - Single



Source: Honeynet

FastFlux - Single

攻撃者が管理するDNS上で、悪性サイトのサイト名に対応付けるIPアドレスを、ボット感染させたコンピュータのIPアドレスで短時間（数分）に切り替える（DNSレコードの有効期限（TTL）が極端に短く設定）ことで、悪性サイトのアドレスをカモフラージュする





- Level 2: Fastflux - Single

```
;; WHEN: Sat Feb 3 20:08:08 2007
divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 76.209.81.xxx [SBIS-AS - AT&T Internet Services]
divewithsharks.hk. 1800 IN A 85.207.74.xxx [adsl-ustixxx-74-207-85.bluetone.cz]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msjw.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

ns1.world-wr.com. 87169 IN A 66.232.119.212 [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com. 87177 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

30分後…

```
;; WHEN: Sat Feb 3 20:40:04 2007 (~30 minutes/1800 seconds later)


divewithsharks.hk. 1800 IN A 24.85.102.xxx [xxx.vs.shawcable.net] NEW


divewithsharks.hk. 1800 IN A 69.47.177.xxx [d47-69-xxx-177.try.wideopenwest.com] NEW
divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msjw.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

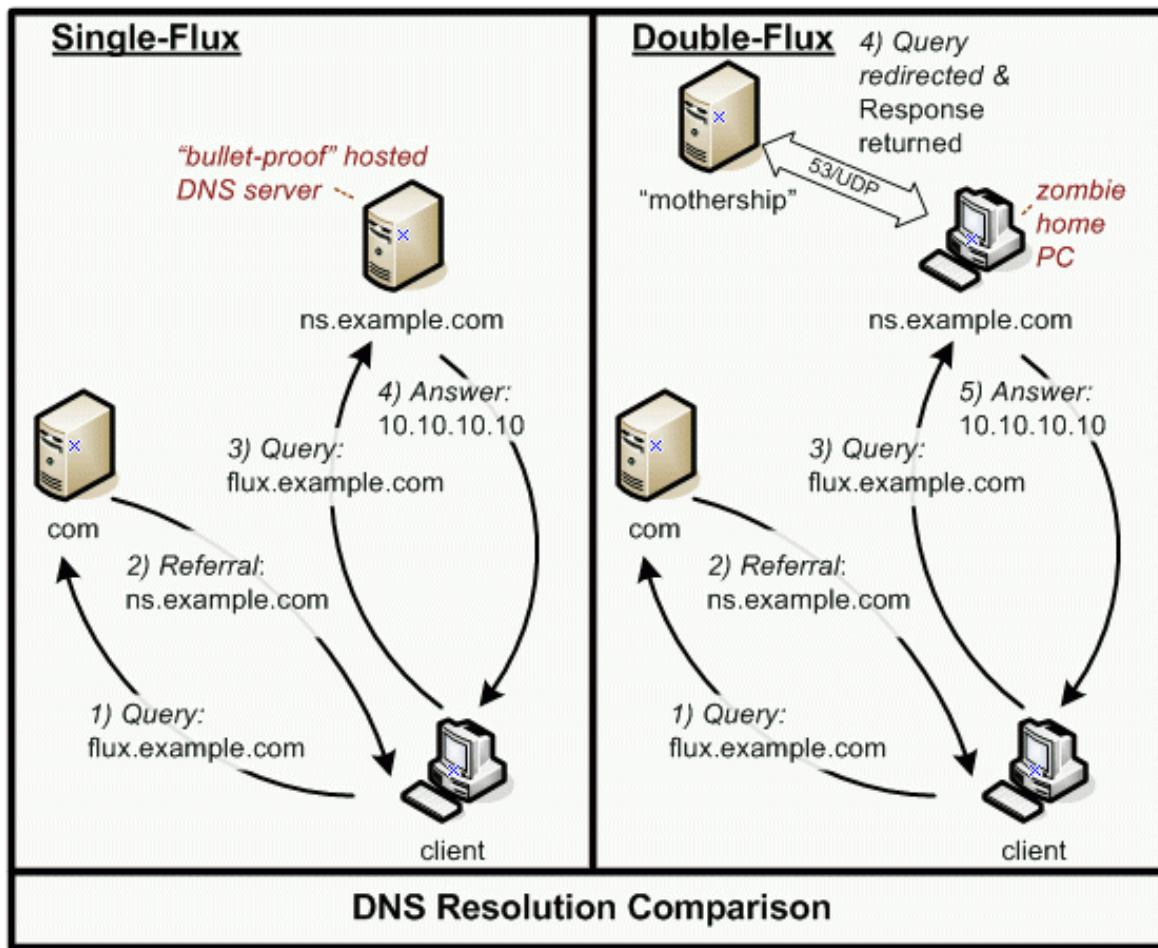
ns1.world-wr.com. 85248 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com. 82991 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]


```

Source: Honeynet



- Level 2: Fastflux - Double



Source: Honeynet



- Level 3: P2P

- 課題: 集中型のボットネットにはC&Cサーバが情報を保持するため、C&Cサーバをブロックするとボットネットなどが機能しなくなる課題がある
 - Solution: P2P



- Level 3: P2P
シンプルなインフラ (P2P) はセントラルサーバが必要である

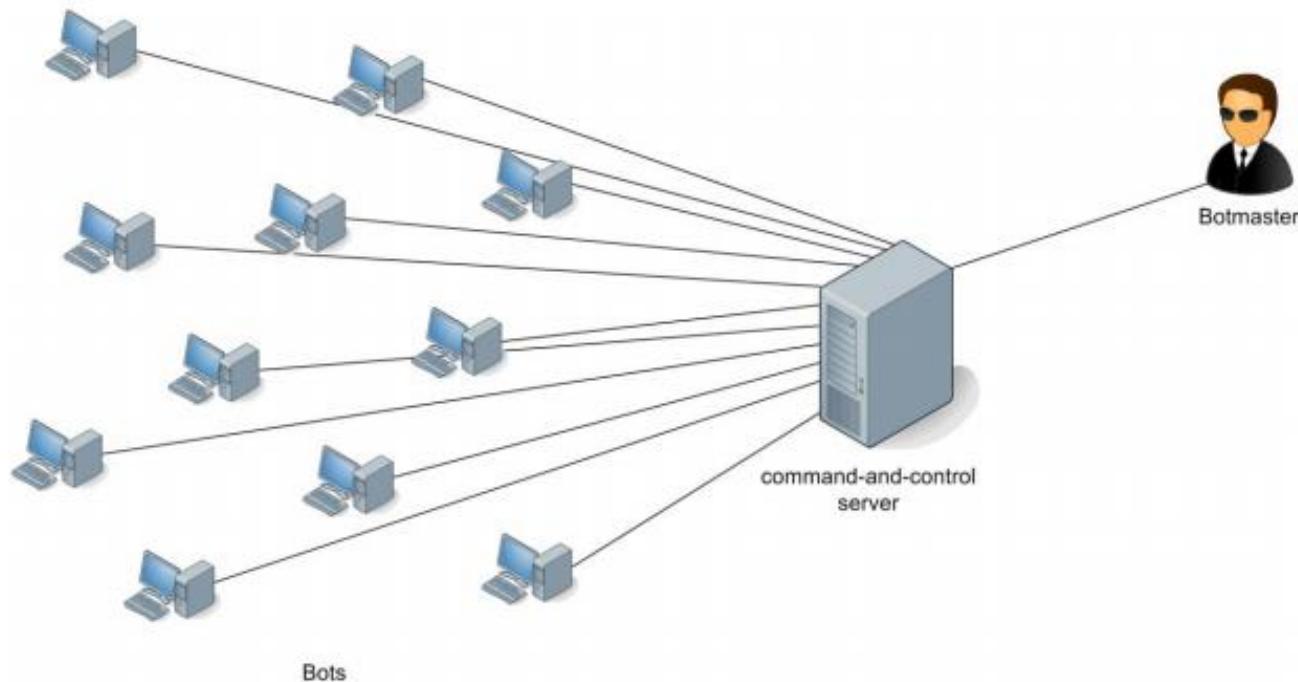


Figure 1: Centralised botnet.

Source: ENISA



- Level 3: P2P

P2Pのインフラは軽減策を取るのが難しい

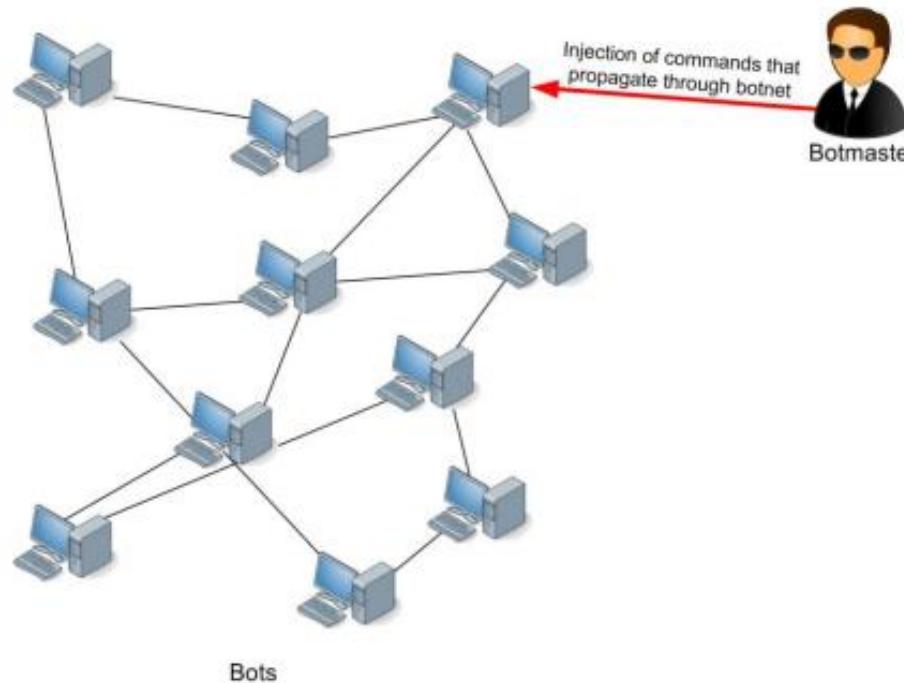
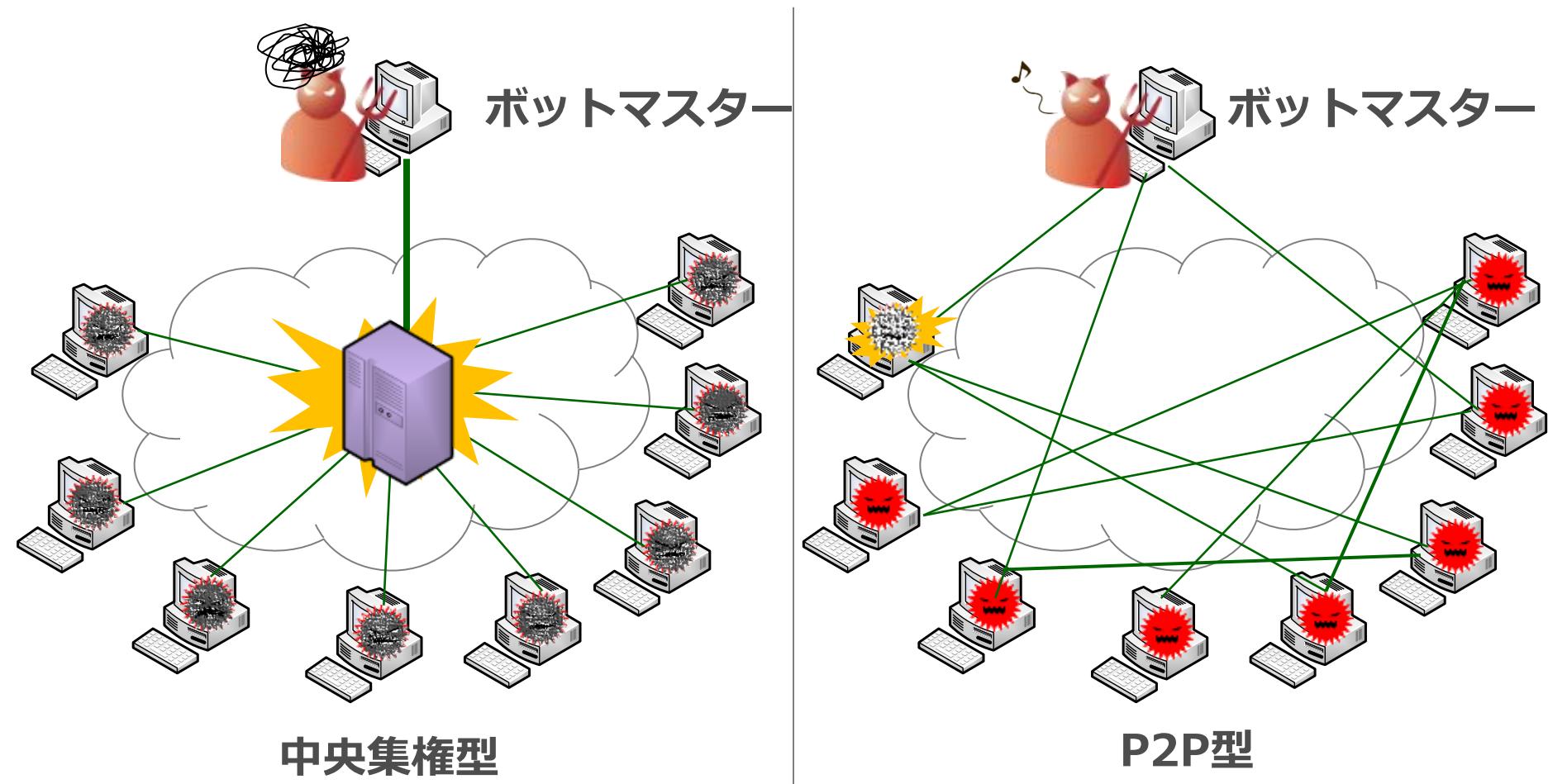


Figure 2: Peer-to-peer botnet.

Source: ENISA



中央集権型とP2P型





- Persistence
- ルートキット
- リバースエンジニアリングと、アンチリバースエンジニアリング
 - パック
 - アンチ逆アセンブラ
 - アンチデバッガ
 - アンチバーチャルマシン
 - 難読化



- Persistence

- システムが停止、再起動してもマルウェアは長期的に動作するため、再感染する必要がある
 - 一般的に:

- Windows: Registry, ...

- Tool: Autoruns

- *nix: rc.d, ...

- Tool: LKM

- Mac OS X: [launchd].plist, ...

- Tool: Knock Knock

- マルウェアは再感染の必要があるため、上記のチェックは有効である

VM ZeusにはHKCU-Run-Keyがある。しかしながら、起動後にキーは削除され、シャットダウン時に再作成される



- ルートキット
 - システム関数呼び出しの出力を操作する
 - 複雑(単純ではない)：OSの動作に矛盾が見える事がある

The screenshot shows a Windows desktop environment. In the foreground, a terminal window is open with the command `cd C:\Windows\system32\cmd.exe` entered. The terminal output shows the directory structure of the AppData\Roaming folder on the C drive, listing various application-specific folders like Adobe, InstallShield, Macromedia, Microsoft, Mozilla, and tor. The terminal window has a blue title bar and a black background for the text.

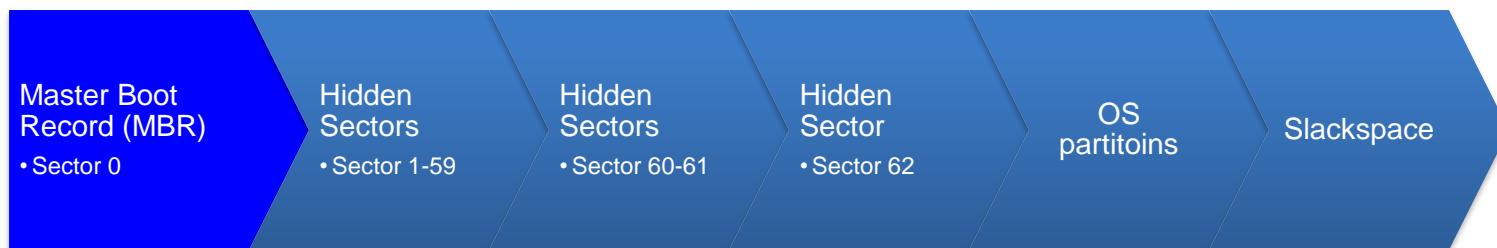
```
C:\Users\<User>\AppData\Roaming>cd <AppData>
C:\Users\<User>\AppData\Roaming>dir
Volume inlaufwerk C: hat keine Bezeichnung.
Volumenseriennummer:

Verzeichnis von C:\Users\<User>\AppData\Roaming

12.12.2013 14:42    <DIR>      .
12.12.2013 14:42    <DIR>      ..
11.11.2011 10:39    <DIR>      Adobe
12.12.2013 13:12    <DIR>      .
11.11.2011 09:58    <DIR>      identities
11.11.2011 10:11    <DIR>      InstallShield
17.01.2014 12:12    <DIR>      Izisec
11.11.2011 10:48    <DIR>      Macromedia
14.07.2009 19:18    <DIR>      Media Center Programs
12.12.2013 13:19    <DIR>      Mopa
11.11.2011 10:45    <DIR>      Mozilla
22.01.2014 07:14    <DIR>      tor
                           0 Dateien,   0 Bytes      Bytes frei
C:\Users\<User>\AppData\Roaming>=
```



- ルートキット
 - MBRの操作 → ブートキット
 - OSの開始に先立って起動
 - 悪意あるドライバをロードすることができる





- リバースエンジニアリング (RE) とアンチリバースエンジニアリング (Anti-RE)

ウイルス検出: **0 / 54**





- リバースエンジニアリング (RE) とアンチリバースエンジニアリング (Anti-RE)
 - パッキングは複雑。複数のAnti-RE技術を含む
例：
 - 仮想マシンの検出
 - デバッガの検出
 - コードの難読化
 - ...
 - コードの難読化は、人間が理解することが困難なフォームへとコードを変換する



デモンストレーション

難読化を解説

イスラエルのマルウェアドメインから悪意あるJavaScriptの埋め込み

マルウェアテクニック – 難読化



The screenshot shows the homepage of the SWITCH website (www.switch.ch). The header includes the TRANSITS logo and the title "マルウェアテクニック – 難読化". The main navigation bar features links for Home, Sitemap, News, Contact, All Services by SWITCH (with dropdown for de, fr, it, en), and a search bar. The top banner highlights the "SWITCH Journal: Security and stability". The left sidebar has a "Portrait" section with links to Studying, Education & Research, University IT, and Public Services. The central content area discusses SWITCH's mission to serve universities, mentions switchplus ag as a subsidiary, and promotes domain names and hosting services. A call-to-action button says "The direct route to your internet address". A sidebar on the right provides news about the "SWITCH Junior Web Award" and links to media releases.

SWITCH – our mission
At the service of the universities

SWITCH provides innovative, unique internet services for the Swiss universities and internet users.

» [More about SWITCH](#)

switchplus ag – our subsidiary
Domain Names and hosting

switchplus offers domain names as well as web and mail hosting for private and business customers.

The direct route to your internet address [» continue](#)

11.08.2014
SWITCH Junior Web Award: The new generation of web designers

The website competition for schools, now in its ninth year, kicks off today. SWITCH wants school students from all over Switzerland and the Principality of Liechtenstein to design their own website together with their teacher. The success story of the Junior Web Award began in 2007, when the SWITCH foundation launched the competition to mark its 20th anniversary. As the pioneer of the Swiss Internet, the foundation wants to promote the latest generation's World Wide Web know-how.

» [Read on](#)
» [Media releases](#)

マルウェアが利用する検出回避技術

セキュリティ対策を回避する技術

マルウェア対策エンジン、ファイアウォール、アプリケーション隔離等による検出を回避する

サンドボックスを回避する技術

マルウェアの挙動を観測するサンドボックス内で実行されているかどうか検知する

分析を回避する技術

Process ExplorerやWiresharkなどの監視ツール、リバースエンジニアリングを回避する

ツール名称	説明
クリプター	マルウェアの暗号化/復号によりマルウェア対策エンジンによる検出やリバースエンジニアリングを困難にする
パッカー	マルウェアを圧縮してRAM/ディスクの消費を少なくする
ポンパー	ファイルサイズを増やし、検知されにくくする
FUD	マルウェア実行前や実行中に、マルウェア対策エンジンによる検出を困難にする。 (FUD=Fully UnDetectable)

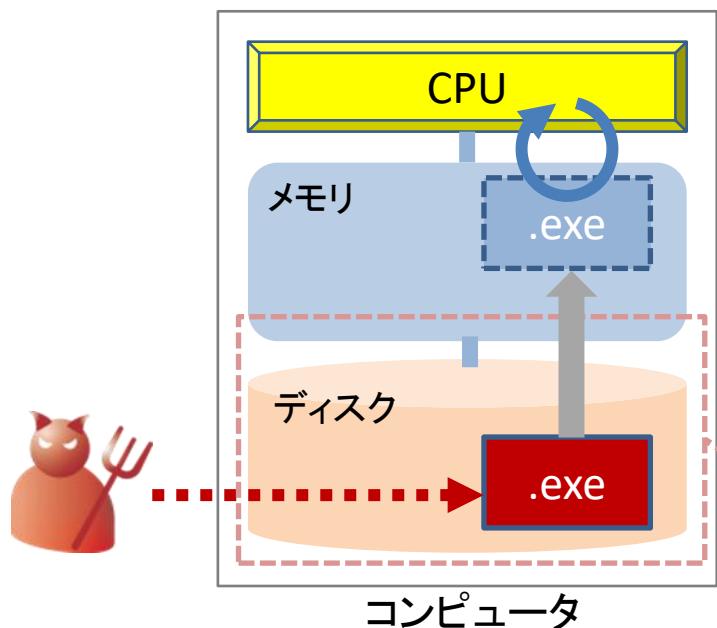
参考： McAfee脅威レポート2017年6月

<https://www.mcafee.com/jp/resources/reports/rp-quarterly-threats-jun-2017.pdf>

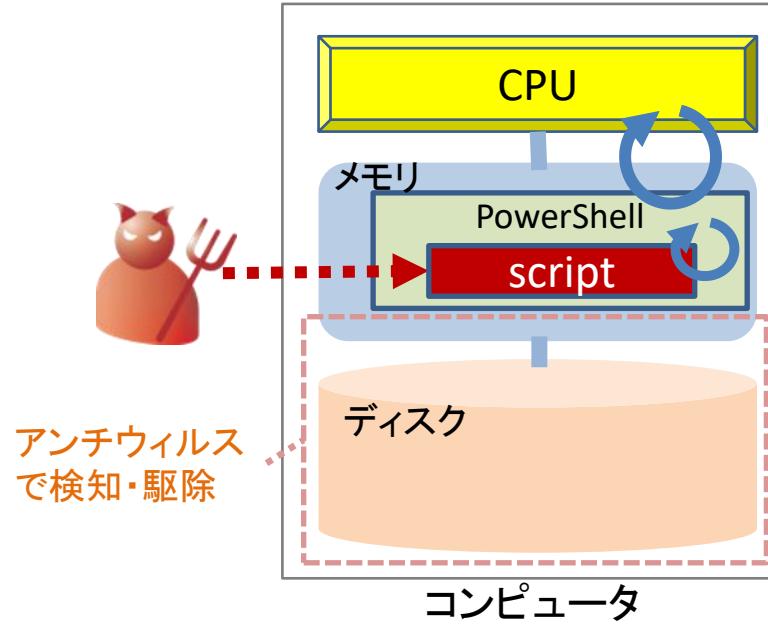
ファイルレス・マルウェア

- 実体が実行ファイル（拡張子exeのファイル）の形でディスク上に保存されず、メモリ上のみに存在して動作するマルウェア
- アンチウィルスソフトでの検知・駆除が難しい
- Windows PowerShellやWindows Management Instrumentation (WMI)などのWindowsの標準機能が悪用される

従来型のマルウェア



ファイルレス・マルウェア



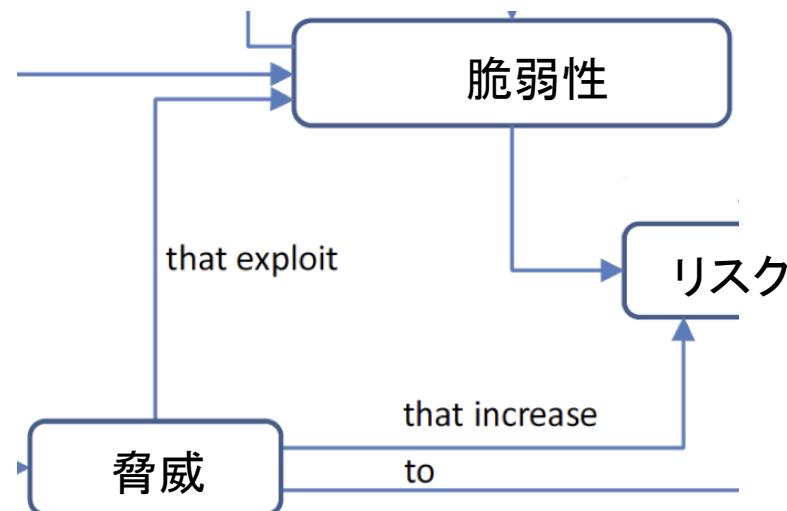


TRANSITS

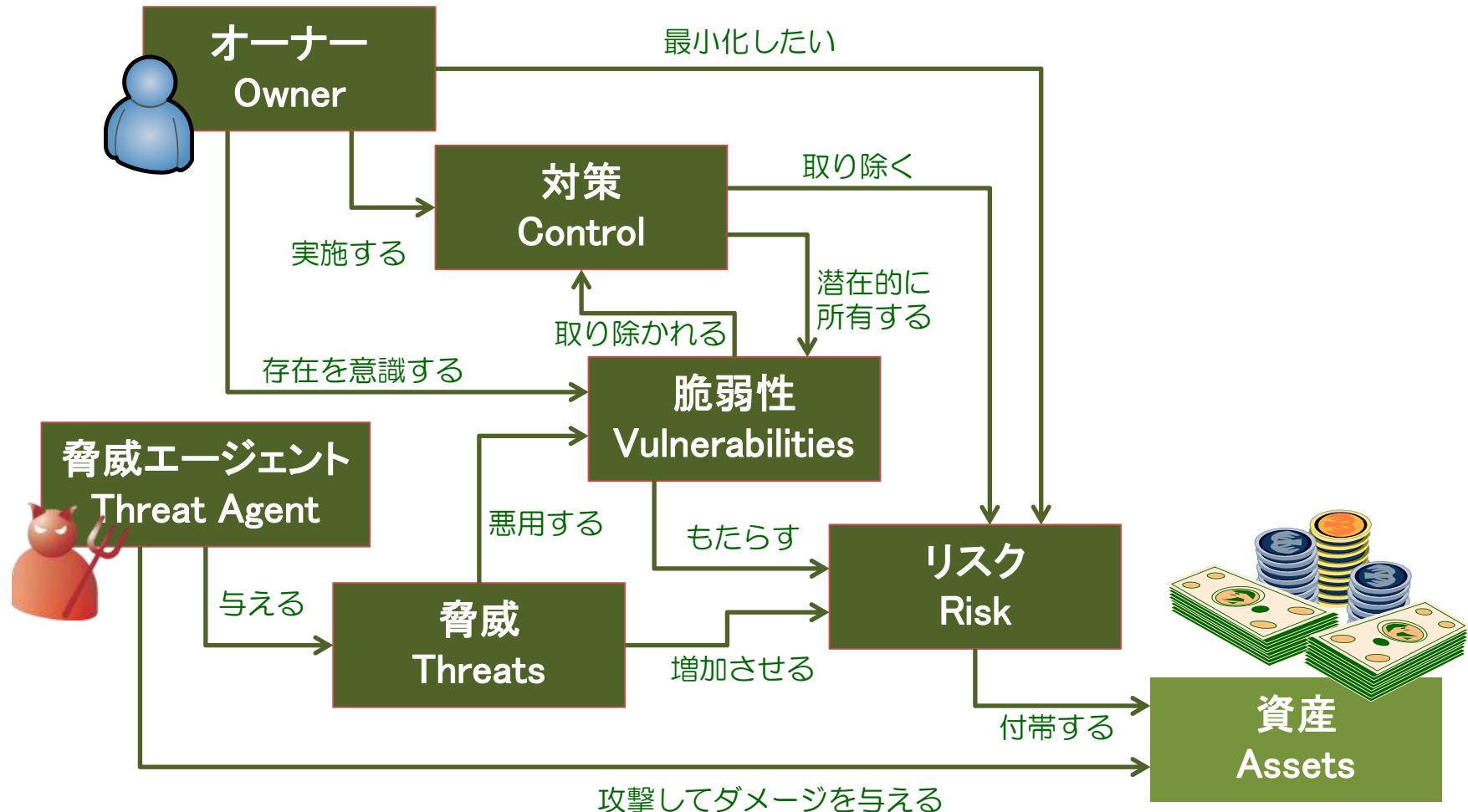
Part III ハッキング



- ハッキング: コンピュータシステム、ネットワークに侵入し、アクセス権を取得する、データを不正に取得する。そして、AICを侵害する(可用性、完全性、機密性)
- 脆弱性: 弱点を悪用される
 - ie. 結果として、ハッキングを可能にする
 - ie. 結果として、セキュリティポリシーに違反する
- 100%安全なソフトウェアはない



脅威、脆弱性、リスクの関係





ハッキング – 例 1: [DR]DoS

71783 (1) – NTP monlist Command Enabled

概要

NTP Projectが提供するntpdの一部のバージョンにはNTPサーバの状態を確認する機能(monlist)が実装されており、同機能は遠隔からサービス運用妨害(DDoS)攻撃に使用される可能性がある

説明

NTP は、通常 UDP を使用して通信するため、容易に送信元 IP アドレスを 詐称することができる。また、monlist 機能は、サーバへのリクエストに対して大きなサイズのデータを送信元 IP アドレスへ返送するため、攻撃者は攻撃対象の IP アドレスを送信元 IP アドレスに偽装した問い合わせパケットを NTP サーバに送信することで、大きなサイズのデータを攻撃対象 (Web サイトなど) に送りつけることができる

解決策

修正済みのバージョン(NTP 4.2.7-p26)へアップデートする。

または、'ntp.conf'に'disable monitor'を追加しサービスを再起動する。また必要に応じてはベンダーに問い合わせる。

NTPサービスを外部に提供する必要が無い場合は、信頼できるホスト以外からの受付は制限することも検討する



ハッキング – 例 1: [DR]DoS

71783 (1) – NTP monlist Command Enabled

概要

NTP Projectが提供するntpdの一部のバージョンにはNTPサーバの状態を確認する機能(monlist)が実装されており、同機能は遠隔からサービス運用妨害(DDoS)攻撃に使用される可能性がある

危険レベル

中

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

参照

CVE-2013-5211, CWE-20, cpe://a:ntp:ntp:4.2.7



ハッキング – 用語

- CPE: Common Platform Enumeration cpe://a:ntp:ntp:4.2.7
共通プラットフォーム一覧
情報システムを構成する、ハードウェア、ソフトウェアなどを識別するための共通の名称基準を目指している
- CWE: Common Weakness Enumeration CWE-20: Improper Input Validation
共通脆弱性タイプ一覧
ソフトウェアにおけるセキュリティ上の弱点(脆弱性)の種類を識別するための共通の基準を目指している
- CVE: Common Vulnerability and Exposure CVE-2013-5211
共通脆弱性識別子
個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子
- CVSS: Common Vulnerability Scoring System CVSS 5.0 (Medium)
共通脆弱性評価システム
情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、米国国家インフラストラクチャ諮問委員会(National Infrastructure Advisory Council: NIAC)のプロジェクトで2004年10月に原案が作成された



ハッキング – 例 2: Improper Input Validation

- CWE-20: Improper Input Validation

The screenshot shows a web browser displaying a shopping cart page from 'www.bookstore.com'. The page title is 'Welcome to A Clean Well-Lighted Place for Books'. The left sidebar contains links: Home, Events, Book Search, Autographed Books (which is circled in red), Remainders 50% off!! (also circled in red), Remainders 60% off!! (circled in red), and Booksense 76. The main content area shows a shopping cart with one item: 'Linux Security for Large-Scale Enterprise Networks' by Becker, Jamieson, Paperback, Special Order, quantity -1, price \$-59.99. Buttons for 'Save Qty Changes' and 'Check Out' are visible. A red arrow points from the 'Autographed Books' link to the quantity input field. Another red arrow points from the 'Remainders 60% off!!' link to the total price 'Total: \$ -59.99'. A green oval labeled 'Secure communications' surrounds the lock icon in the browser's status bar.

Qty	Description	Price	Remove
-1	Linux Security for Large-Scale Enterprise Networks Becker, Jamieson 1555582923 Paperback Special Order	\$-59.99	Remove

Insecure software

Secure communications



- CWE-89: SQL Injection

- 動作について

データベース駆動のアプリケーションは、多くの場合、データベースクエリを作成するにはユーザー提供の値を使用する

```
$q = sql_query("SELECT * FROM users WHERE user='$user");
```

ユーザーが指定した値 \$user:

Username:

```
$q = sql_query("SELECT * FROM users WHERE user='johndoe' OR '1='1");
```

結果: ユーザ情報の完全ダンプ



ハッキング – SQL Injection



Demonstration

オンラインバンキングのアカウント取得



ハッキング – SQL Injection

Screenshot of a simulated Altoro Mutual website demonstrating SQL injection vulnerabilities.

The page shows a navigation bar with links for "Sign In", "Contact Us", "Feedback", and "Search". A banner at the top right reads "DEMO SITE ONLY".

The main content area is divided into four sections:

- ONLINE BANKING LOGIN**: Includes links for "Deposit Product", "Checking", "Loan Products", "Cards", "Investments & Insurance", and "Other Services".
- PERSONAL**: Features a "Download AppScan Trial" button and a "Privacy and Security" section. It includes a photo of a couple standing in front of a house with a "SOLD" sign.
- SMALL BUSINESS**: Includes links for "Deposit Products", "Lending Services", "Cards", "Insurance", "Retirement", and "Other Services". It features a photo of a stack of credit cards.
- INSIDE ALTORO MUTUAL**: Includes links for "About Us", "Contact Us", "Locations", "Investor Relations", "Press Room", and "Careers". It features a photo of a large group of people.

Below the main content, there is a note about the website being a demo site for AppScan, and copyright information for IBM Corporation.



ハッキング – 例 5: Cross Site Scripting

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

- 動作概要

脆弱な Web アプリケーションに対して、攻撃者が被害者に危険なコンテンツを送信させる際に発生する。この危険なコンテンツは、被害者に返され Web ブラウザ上で実行される

The screenshot shows a web browser window. The URL bar contains the URL <https://xss-doc.appspot.com/demo/2?query=test>. A red box highlights the query parameter 'test'. The main content area displays the word 'bobazillion' in a stylized font where each letter has a different color: b (red), o (green), b (blue), a (yellow), z (dark blue), i (light blue), l (red), l (dark blue), i (light blue), o (red). Below this, a message says 'Sorry, no results were found for **test.** [Try again.](#)' A red box highlights the word 'test.' in the message. On the right side of the browser window, there is a vertical scrollbar.

Source: Google



ハッキング – 例 5: Cross Site Scripting

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

- 動作概要

脆弱な Web アプリケーションに対して、攻撃者が被害者に危険なコンテンツを送信させる際に発生します。HTMLの例：

URL <https://xss-doc.appspot.com/demo/2?query=<u>test</u>>

```
9   
10  <div>
11  Sorry, no results were found for <b><u>test</u></b>. <a href='?'>Try again</a>.
12    <script>top.postMessage(window.location.toString(), "*");</script>
13  </div>
```

Sorry, no results were found for **test.** [Try again.](#)

Source: Google



ハッキング – 例 5: Cross Site Scripting

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
 - 動作概要
脆弱な Web アプリケーションに対して、攻撃者が被害者に危険なコンテンツを送信させる際に発生する。JavaScriptの例：

The screenshot shows a web browser window with the following details:

- URL:** https://xss-doc.appspot.com/demo/2?query=<script>alert('hello')</script>
- Content Area:** Displays the following HTML code:

```
9 
10 <div>
11 Sorry, no results were found for <b><script>alert('hello')</script></b>. <a href='?'>Try again</a>.
12 <script>top.postMessage(window.location.toString(), "*");</script>
```
- Message Bar:** Shows "The page at https://xss-doc.appspot.com"
- Bottom Status:** Shows "Sorry, no results were found for . Try again."
- Source:** Google
- Page Number:** 107 of ...

A red arrow points from the URL bar to the message bar, highlighting the injected JavaScript code.



- OWASP Top Ten Weaknesses
 - Open Web Application Security Project

2013 Top 10 List

A1-Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2-Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.



ハッキング – **Injecti0n-Proxy**



Demonstration

トロイの木馬による権限昇格と、感染端末へVNC接続



TRANSITS

Hacking – Injecti0n-Proxy



Recycle Bin



NDA Spec...



Mozilla
Firefox



TCPView



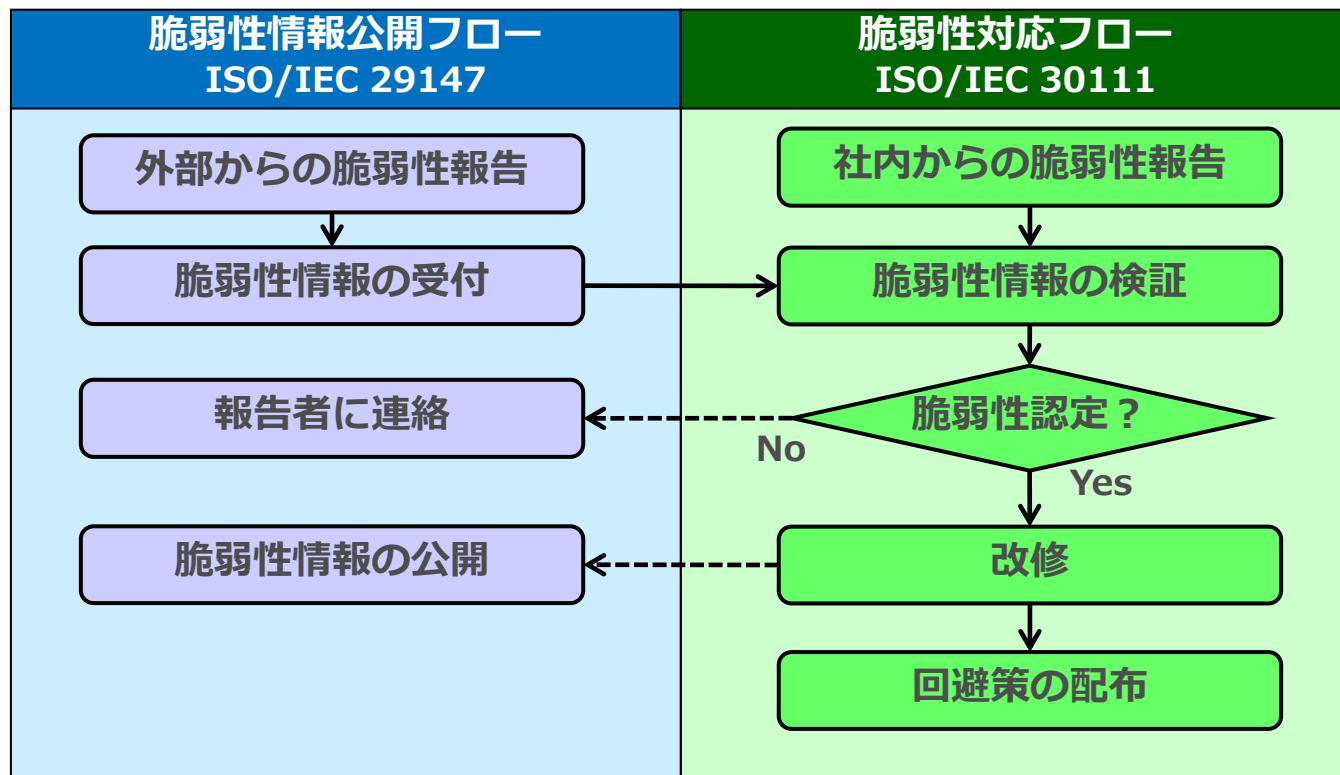
Topview -
Shortcut

SWITCH



自社ソフトウェア商品の脆弱性管理

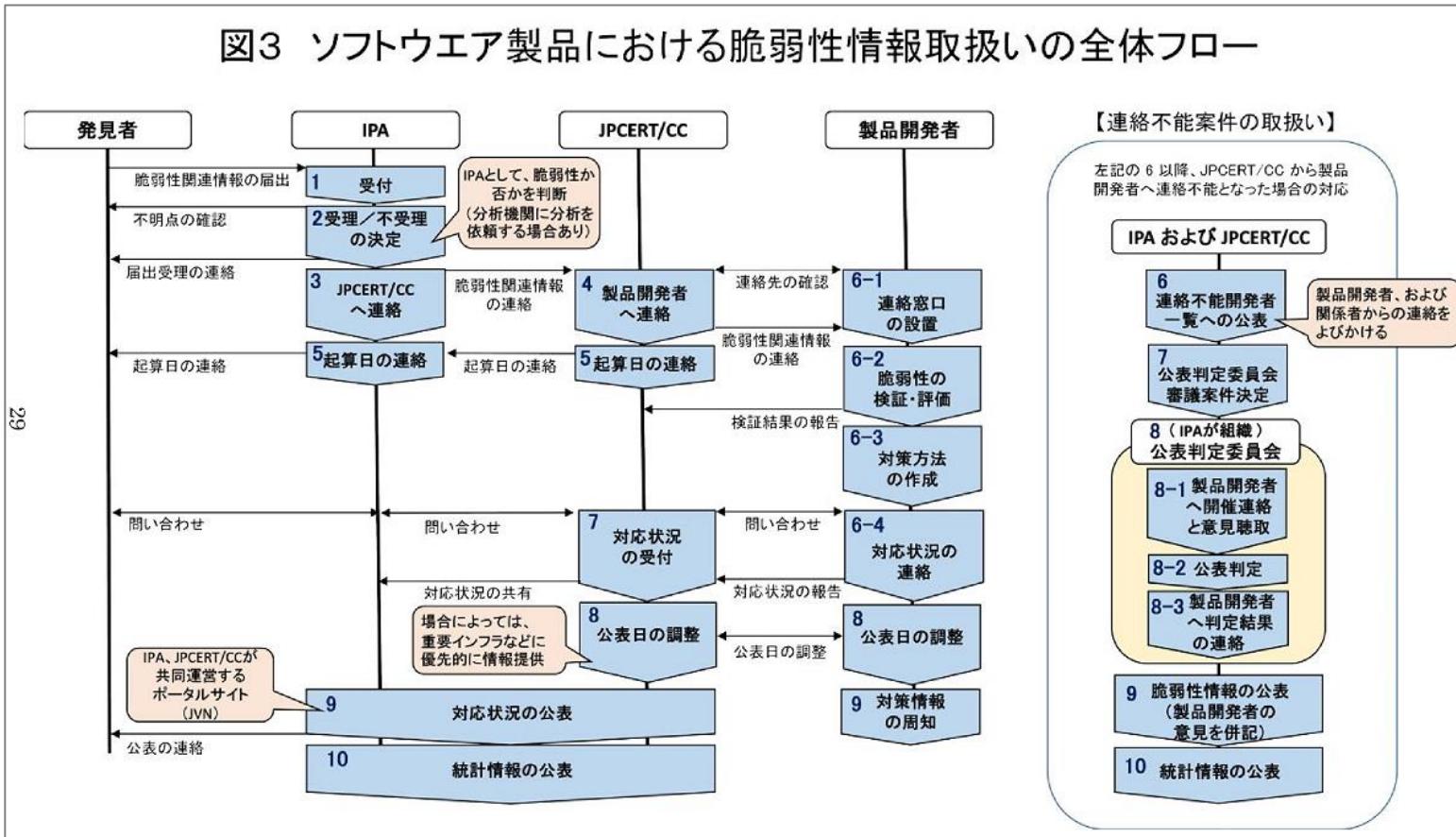
自社で開発したソフトウェアに脆弱性が発見された場合、その脆弱性を解決するためのパッチを開発し脆弱性情報を公開する



早期警戒パートナーシップ (ソフトウェア)



図3 ソフトウェア製品における脆弱性情報取扱いの全体フロー



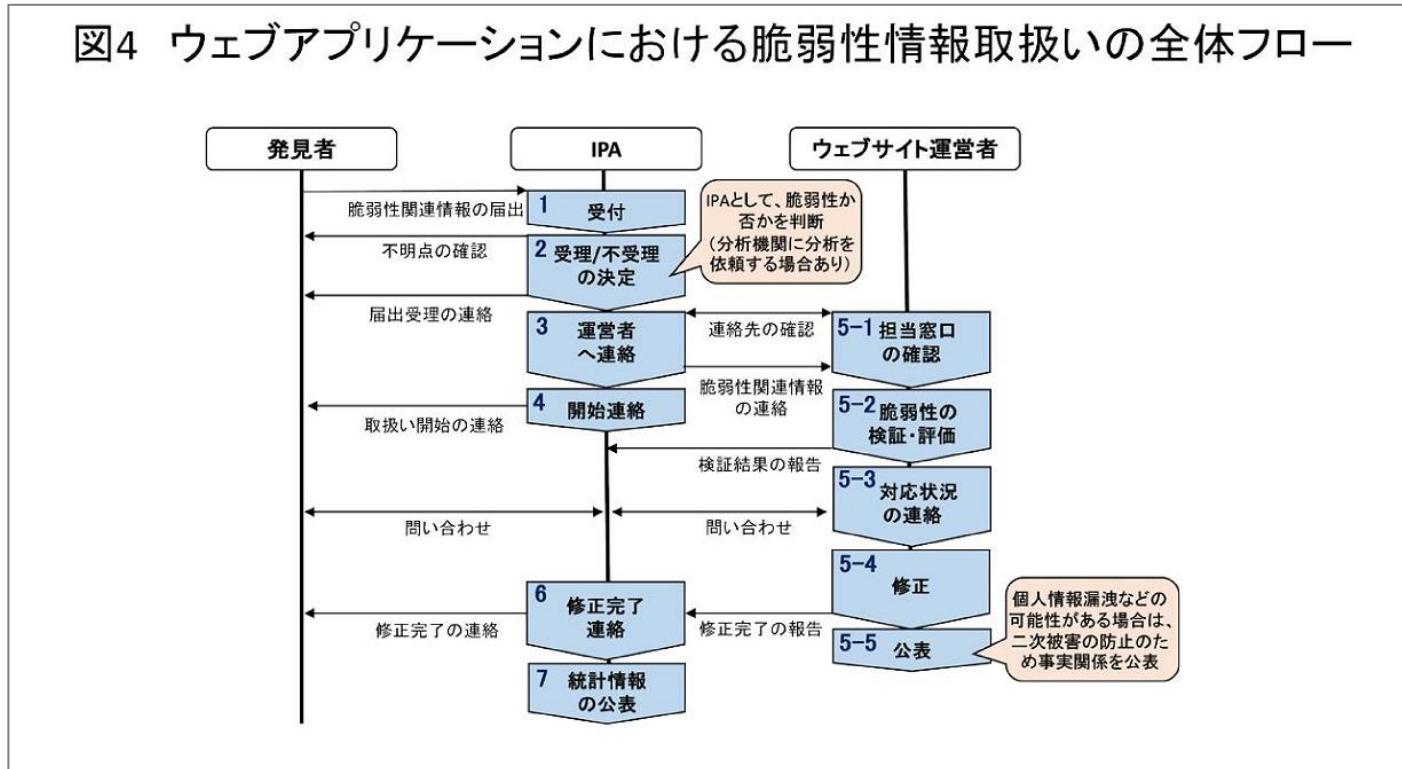
IPA 早期警戒パートナーシップ

https://www.jpcert.or.jp/vh/partnership_guideline2015.pdf

IPA 早期警戒パートナーシップ (ウェブアプリ)

ソフトウェア商品とは異なり、ウェブアプリの場合は、脆弱性情報の公開は無い

図4 ウェブアプリケーションにおける脆弱性情報取扱いの全体フロー



脆弱性情報公開ポリシー

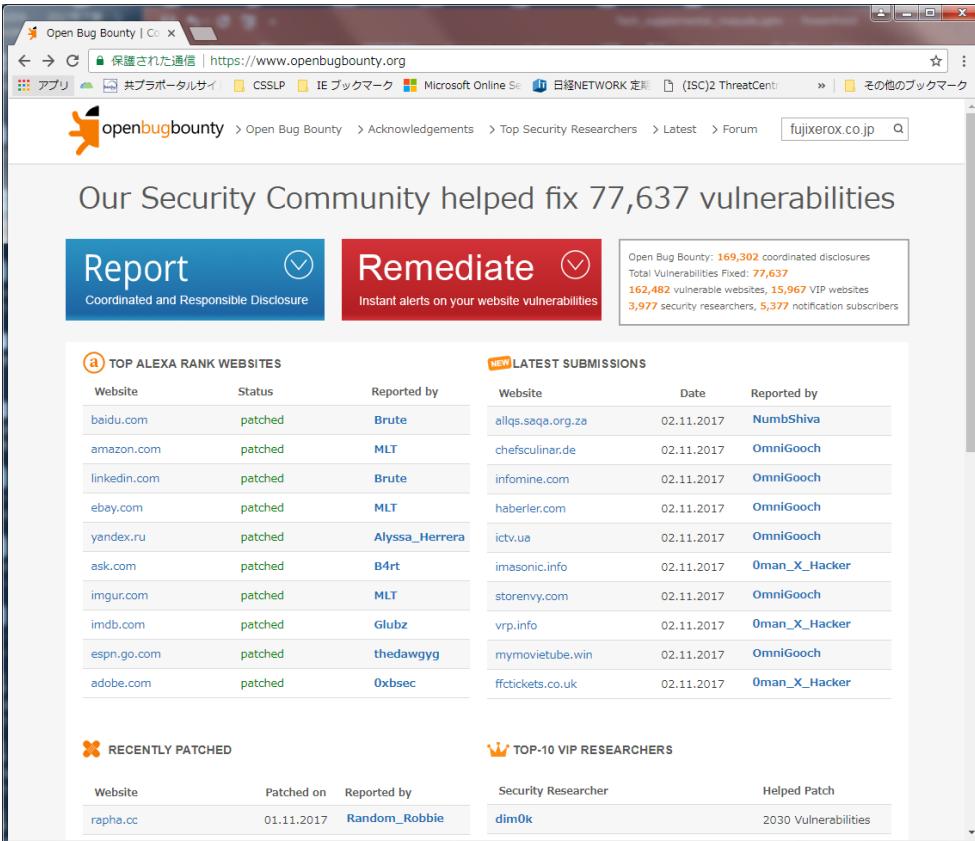
先進的な企業では、自社の脆弱性情報公開ポリシーを定め、脆弱性を報告してもらう窓口を用意している。

発見者への報奨金制度（Bounty Program）を設けている企業もある。

- Cisco “Security Vulnerability Policy”
 - IBM “Report Security Vulnerabilities”
 - Microsoft “Report a Computer Security Vulnerability”
 - Salesforce.com “Vulnerability Reporting Policy”
 - LINE “Security Bug Bounty Program”
 - サイボウズ “脆弱性情報ハンドリングポリシー”
- etc.

OpenBugBounty

脆弱性発見者への報奨金を支援するサイト



The screenshot shows the homepage of the Open Bug Bounty website. At the top, it displays the message "Our Security Community helped fix 77,637 vulnerabilities". Below this are two main buttons: "Report" (Coordinated and Responsible Disclosure) and "Remediate" (Instant alerts on your website vulnerabilities). A sidebar on the right provides key statistics: Open Bug Bounty: 169,302 coordinated disclosures, Total Vulnerabilities Fixed: 77,637, 162,482 vulnerable websites, 15,967 VIP websites, 3,977 security researchers, and 5,377 notification subscribers.

TOP ALEXA RANK WEBSITES

Website	Status	Reported by
baidu.com	patched	Brute
amazon.com	patched	MLT
linkedin.com	patched	Brute
ebay.com	patched	MLT
yandex.ru	patched	Alyssa_Herrera
ask.com	patched	B4rt
imgur.com	patched	MLT
imdb.com	patched	Glubz
espn.go.com	patched	thedawgyg
adobe.com	patched	0xbsec

LATEST SUBMISSIONS

Website	Date	Reported by
allqs.sqaq.org.za	02.11.2017	NumbShiva
chefsculinar.de	02.11.2017	OmniGooch
infomine.com	02.11.2017	OmniGooch
haberler.com	02.11.2017	OmniGooch
ictv.ua	02.11.2017	OmniGooch
imasonic.info	02.11.2017	Oman_X_Hacker
storenvy.com	02.11.2017	OmniGooch
vrp.info	02.11.2017	Oman_X_Hacker
mymovietube.win	02.11.2017	OmniGooch
ffttickets.co.uk	02.11.2017	Oman_X_Hacker

RECENTLY PATCHED

Website	Patched on	Reported by
rapha.cc	01.11.2017	Random_Robbie

TOP-10 VIP RESEARCHERS

Security Researcher	Helped Patch
dim0k	2030 Vulnerabilities

<https://www.openbugbounty.org/>



TRANSITS

Part IV

防御策と軽減策



- 防御策と軽減策における重要な確認事項
 - 何が起きているのか? どのように止めるのか? リカバリーの時間/コストをどう削減するか?
→ インシデントレスポンス が関連する
 - なぜ起きてしまったか? いつ起きたか? 被害や損失の規模は?
→ デジタルフォレンジックスが関連する

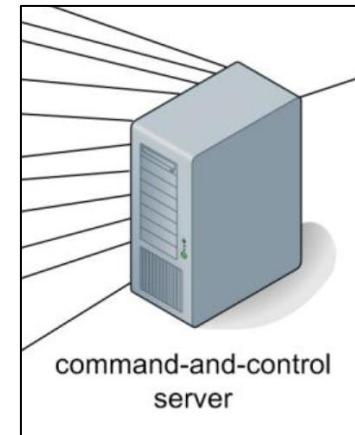
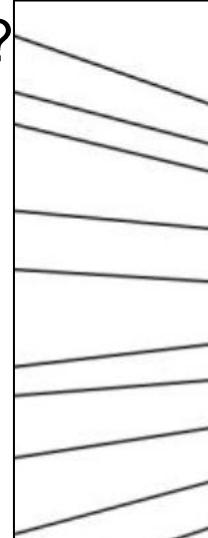
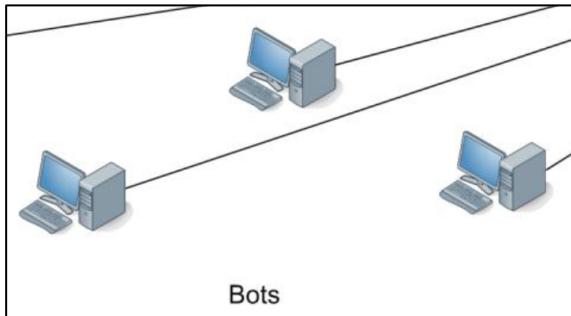


防御策と軽減策- Botnet Mitigation



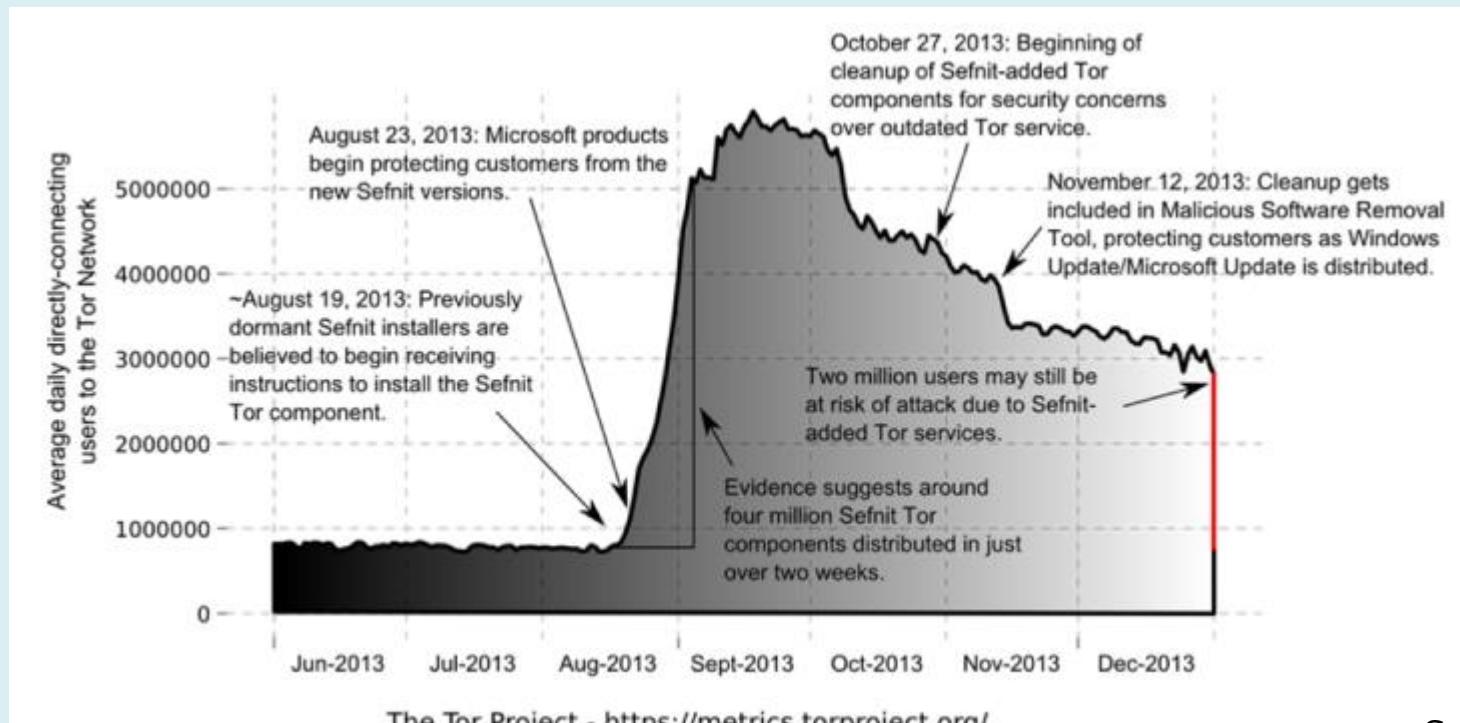
グループディスカッション

ボットネットの軽減策は?



防御策と軽減策 - Sefnit

- Win32/Sefnit が Tor v0.2.3.25 をインストール
- Win32/Sefnit の除去 → Tor v0.2.3.25 は残存 ...



The Tor Project - <https://metrics.torproject.org/>

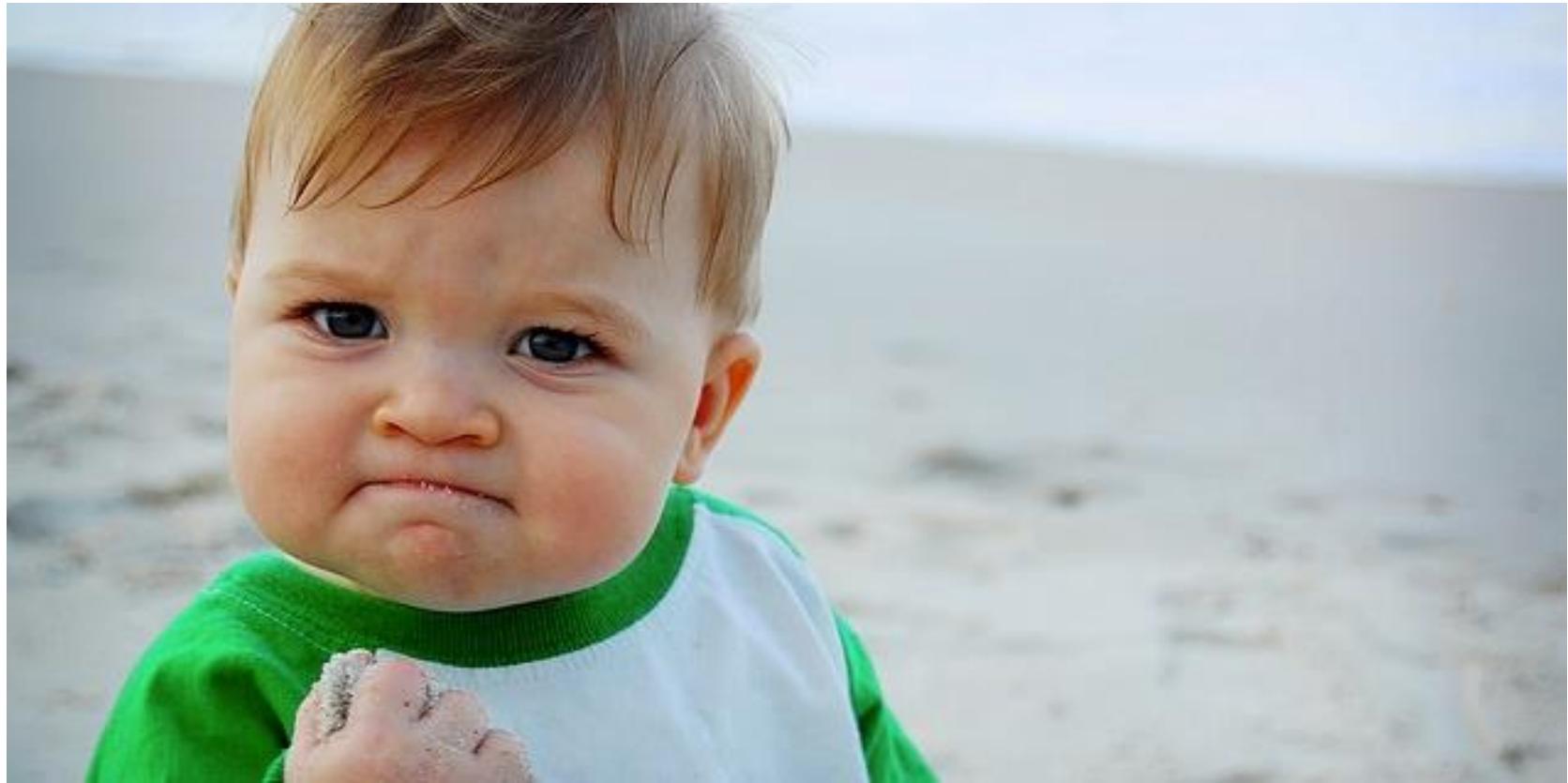
Source: Microsoft



TRANSITS

防御策と軽減策- コミュニティ

- 一人では対抗できない!





- … 幸運にも、以下のようなサービスやツールを公開している
コミュニティがある
 - *Passive DNS* by cert.at
 - *Panopticon Shared Proxy* by circl.lu et al.
 - openresolverproject.com / www.openresolver.nl
 - *n6 Reports* by cert.pl
 - *CAP Reports* by Team Cymru
 - phishtank.com, spamcop.net
 - 他組織との連携
- …ほかにも多数 – 他にどのようなものがあるか?



TRANSITS

防御策と軽減策- **Operation Tovar**



Case Study

Operation Tovar



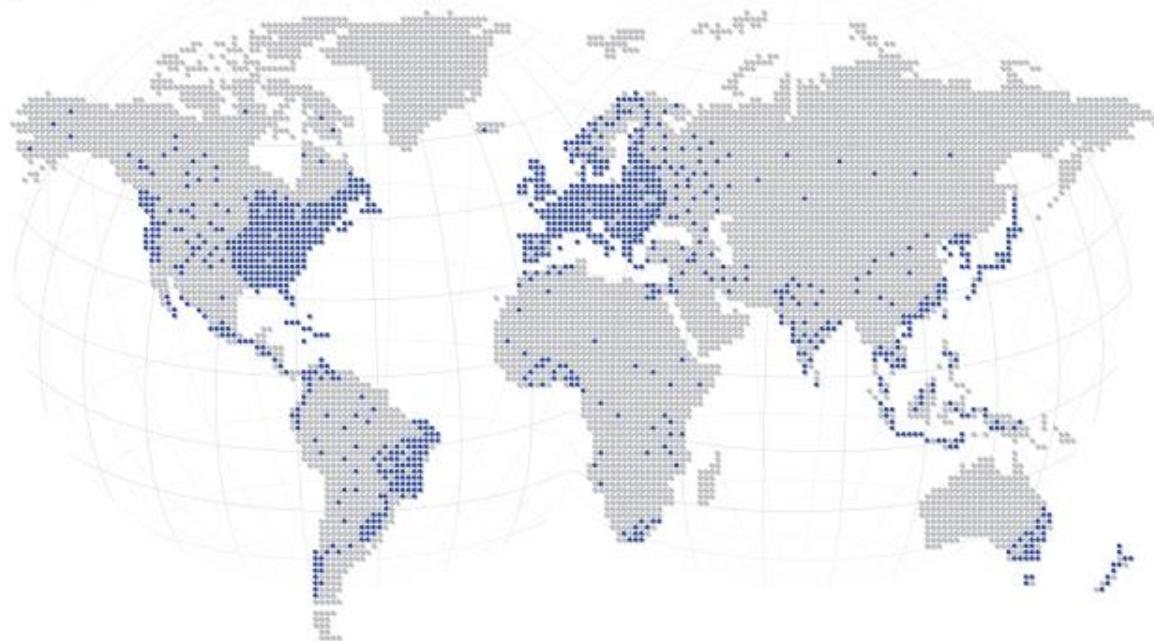
- Gameover Zeus – バンキングトロージャンであるが、他にもさまざまな活動を実施
 - 情報の取得: 金融情報と個人情報
 - 第三者へのサービス(Crime As A Service)提供基盤として利用。CryptoLocker Gang等: GOZボットネットの一部はダウンローダーとして利用される
 - Jumphost for APT campaigns!
- 1つだけのボットネット、ロシアとウクライナの小さなグループによりコントロール。
 - > 500,000 感染台数
 - > 100,000,000\$ 被害総額



防御策と軽減策- Operation Tovar

GOZ/CryptoLocker Scope

- More than 1 million GOZ infections globally
- Roughly 25% of infected computers are located in the United States
- Losses estimated globally in the hundreds of millions of dollars
- Key participation of 10 partner countries in support of takedown operation



FBI CYD 1603.0514.4.2 EXT

Source: FBI

防御策と軽減策- **Operation Tovar**

Operation Tovar

“



Gameover ZeusとCryptolockerを無効化することに成功した
(米国司法省 副検事総長・コール)

FBI, UK NCA, Europol/EC3

Australian Federal Police; National Police of the Netherlands High Tech Crime Unit;
Germany's Bundeskriminalamt; France's Police Judiciare; Italy's Polizia Postale e delle
Comunicazioni; Japan's National Police Agency ; Luxembourg's Police Grand Ducal; New
Zealand Police; the Royal Canadian Mounted Police; Ukraine's Ministry of Internal Affairs-
Division for Combating Cyber Crime



Operation Tovar

専門知識と技術支援を提供したパートナー

- Dell SecureWorks
- CrowdStrike
- Microsoft Corporation
- CSIS
- abuse.ch, Afilias, F-Secure, Level 3 Communications, McAfee, Neustar, Anubis Networks, Symantec, Heimdal Security, Sophos, Trend Micro
- VU University Amsterdam, Saarland University

調整や駆除の支援をしたパートナー

- US CERT (トリアージにおける重要な役割を実施)
- CERT UK and other CERTs
- Shadowserver (さまざまなプロバイダから情報収集、知見の提供)

防御策と軽減策- Operation Tovar

- ボットハーダーは捕まっていない...

**WANTED
BY THE FBI**

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV



Multimedia: Images

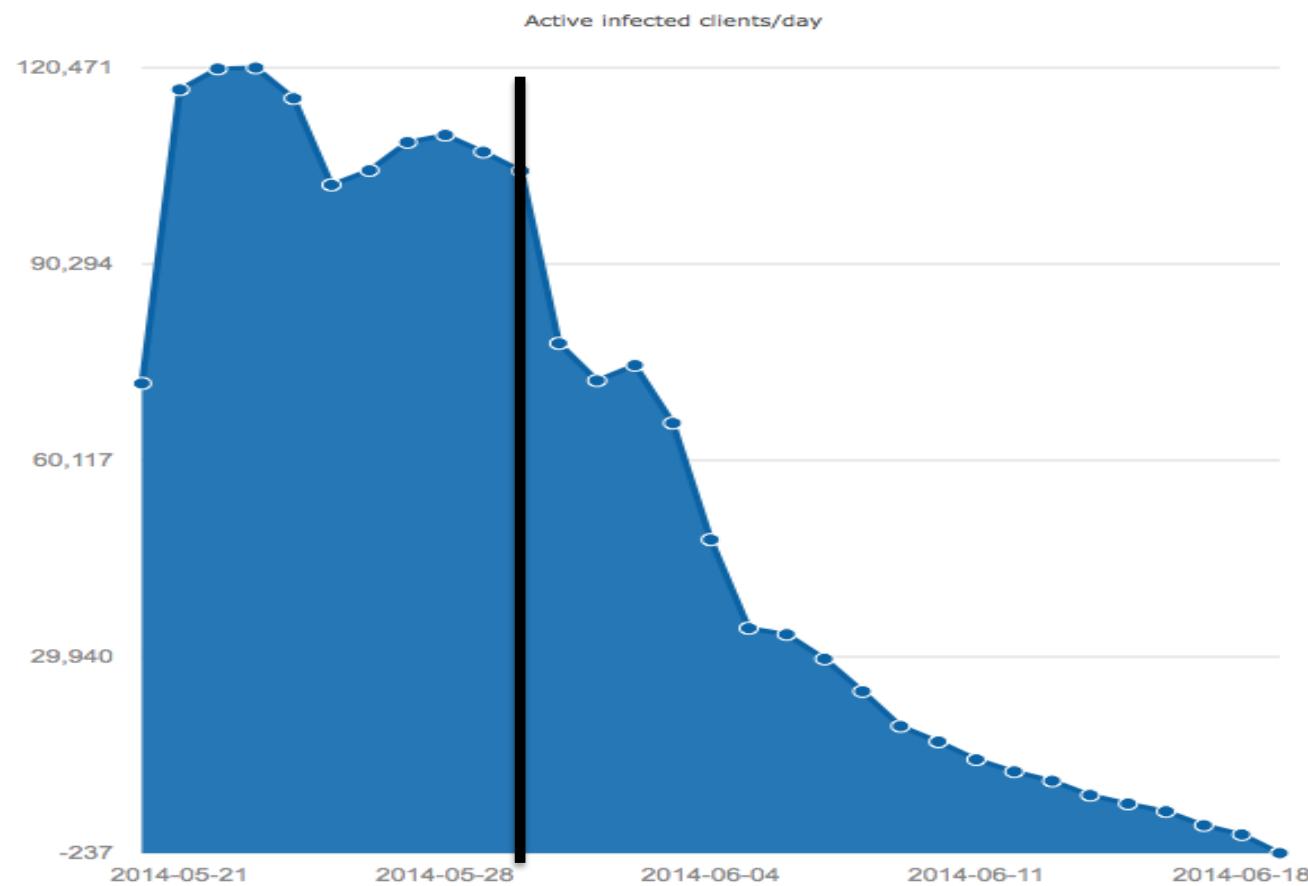
Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Source: FBI



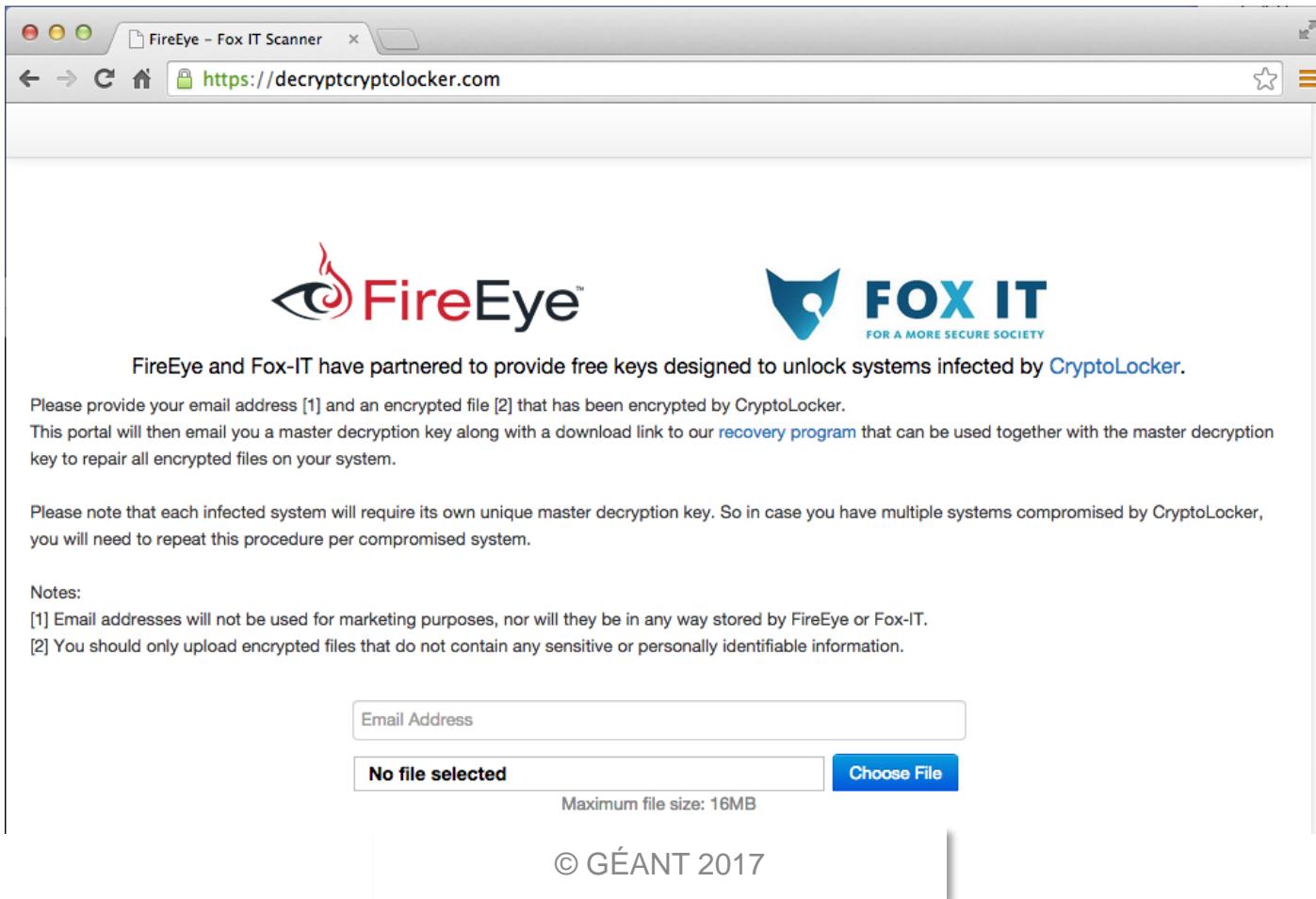
防御策と軽減策- Operation Tovar

- …しかし作戦は成功した:



防御策と軽減策- Operation Tovar

- …しかし作戦は成功した:

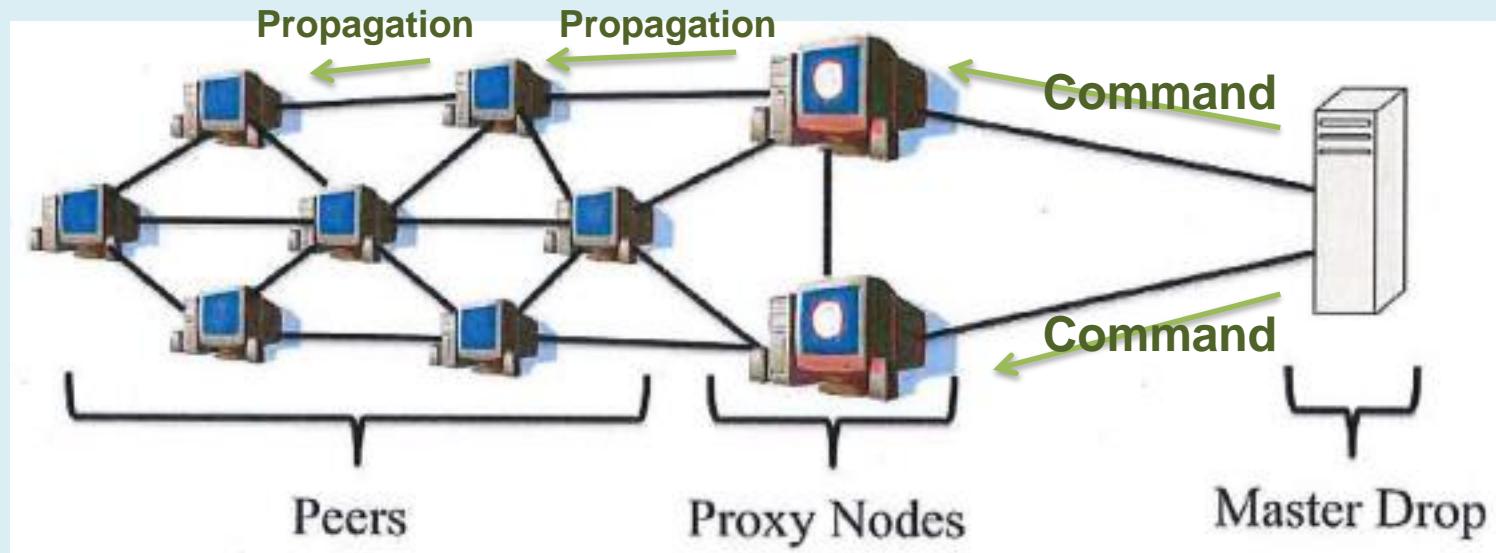


The screenshot shows a web browser window titled "FireEye - Fox IT Scanner". The URL in the address bar is <https://decryptcryptolocker.com>. The page content features the logos for FireEye (red eye icon) and FOX IT (blue fox head icon). A text block states: "FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by [CryptoLocker](#)". Below this, instructions say: "Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker. This portal will then email you a master decryption key along with a download link to our [recovery program](#) that can be used together with the master decryption key to repair all encrypted files on your system." A note follows: "Please note that each infected system will require its own unique master decryption key. So in case you have multiple systems compromised by CryptoLocker, you will need to repeat this procedure per compromised system." A "Notes:" section lists: "[1] Email addresses will not be used for marketing purposes, nor will they be in any way stored by FireEye or Fox-IT." and "[2] You should only upload encrypted files that do not contain any sensitive or personally identifiable information." At the bottom, there are input fields for "Email Address" and "Choose File" (maximum file size: 16MB), and a copyright notice: "© GÉANT 2017".



防御策と軽減策- Operation Tovar

- ボットネットによる乗っ取り: どうやって?
秘密鍵を利用した暗号化通信により情報連絡するタイプの
P2Pボットネット...

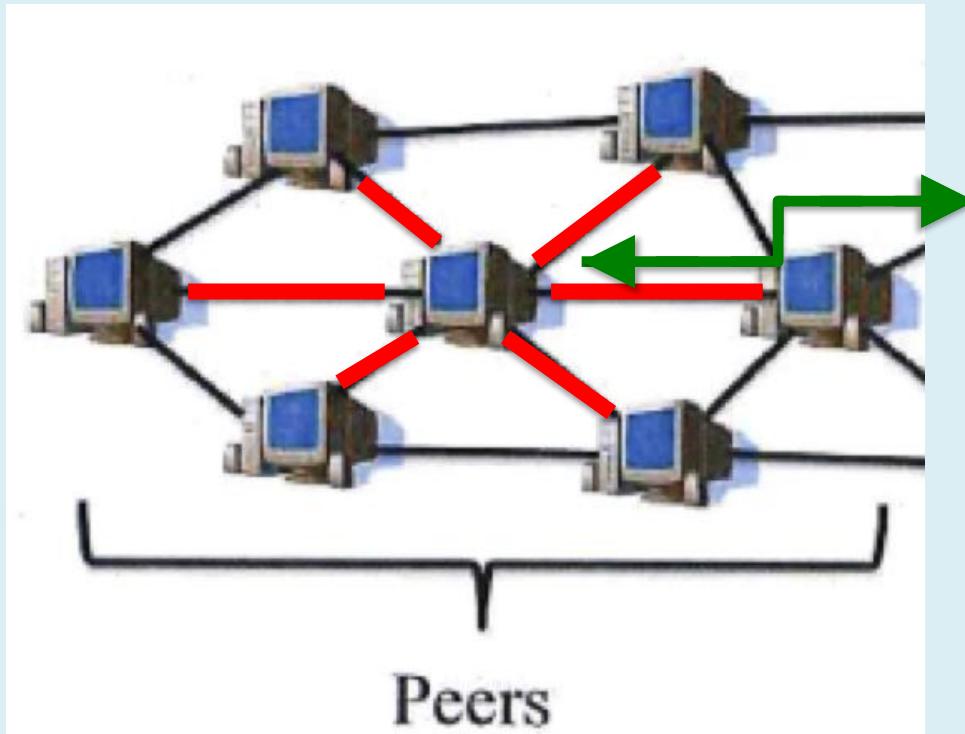


Source: FBI



防御策と軽減策- Operation Tovar

- ボットネットによる乗っ取り: どうやって?



Domain Generating Algorithm

31.5.2014 a3j4adh45.org
31.5.2014 gl134jaf34.com
31.5.2014 oejlk124nj.com
31.5.2014 afne134adf.org
31.5.2014 aglkj34nia.org
31.5.2014 jherkj2n4.net
31.5.2014 a34dm243.org
31.5.2014 gj3213n4o.net
...
thousands
...

防御策と軽減策- **Operation Tovar**

Game Over?

いや、まだである

Slavikはいまだ逮捕されていない.

GOZの新バージョンが利用可能である.

顧客ごとに秘密鍵を利用可能になった.

約10,000台の感染端末が世界中に広がっている.



Source: CSIS



TRANSITS

Defense and Mitigation



FBI

Most Wanted Hackers



Any further Questions

The End ?

取り上げたキーワード

- サイバーキルチェイン
- DDoS、DRDoS
- ボットネット
- C&Cサーバ (C2サーバ)
- RAT
- CaaS
- ペイロード、エクスプロイト
- ダークネット
- Tor
- マルウェア
- ウィルス、ワーム、トロイの木馬
- 中間者攻撃
- 防弾ホスティング
- ファイルレスマルウェア
- 脆弱性
- CVE、CVSS
- クロスサイトスクリプティング
- SQLインジェクション
- Bug Bounty
- ボットネットのティクダウン