macnica networks

標的型攻撃対策
世界に通じるセキュリティ

インテリジェンスを活用して攻撃者を特定せよ！

～Dissecting the Tactics, Techniques, and Procedures～

マクニカネットワークス株式会社
セキュリティ研究センター
政本 憲蔵

マクニカネットワークス　会社概要

会社名	マクニカネットワークス株式会社 （株式会社マクニカ　100%出資）
設　立	2004年3月1日
本　社	横浜市港北区新横浜1-5-5
代表者	代表取締役社長　宮袋 正啓
資本金	3億円
社員数	296名　(2013年4月1日時点)
事業内容	企業向けネットワーク、コンピュータ及び情報通信システム関連ハードウェア・ソフトウェアの輸出入、開発、販売コンサルティング/保守・サービスにわたるITソリューションの提供

取扱い製品（セキュリティ関連）

FireEye
標的型サイバー攻撃対策

CROWDSTRIKE
攻撃者に着目した標的型攻撃対策サービス
次世代エンドポイント・セキュリティ

iMPERVA
WAF / DBF

BLUE COAT
セキュアWebゲートウェイ / SSL可視化
ネットワーク・フォレンジック

McAfee
An Intel Company
IPS / SIEM

radware
DDoS攻撃対策

splunk>
インシデント調査・相関分析

Infoblox
DNSファイアウォール

CITRIX
WAF / アプリケーション・デリバリ・コントローラ

ARXAN
Protecting the App Economy
ソフトウェア・クラッキング対策

DELL SonicWALL
ハイパフォーマンスUTM

Barracuda
スパムメール対策

MobileIron
MDM / MAM / MCM

Kill Chain

偵察	企業サイト、SNSなどのオープンな情報からターゲットの情報（組織、取引先など）を収集。マルウェア配布やC2で使えそうな正規サーバを探すことも。
武器化	攻撃コード（エクスプロイト）とマルウェア（実行ファイル）の作成。
配送	取引先などになりすましたメール（攻撃コード/マルウェアを添付）を送付。またはマルウェアを事前に仕込んだWebサイトへアクセスさせ、ドライブバイダウンロード。
攻撃	ユーザに添付ファイル（PDF、Office）を開かせる、もしくは悪性Webサイトへアクセスさせ、脆弱性を利用した攻撃コード（エクスプロイト）を実行する。
インストール	攻撃コードの実行された結果としてマルウェア（実行ファイル）がインストールされる。もしくはメールに添付した実行ファイルを開かせることでインストール。
遠隔操作（C2）	C&Cサーバへ接続させ、端末を遠隔操作する。必要に応じて、追加のマルウェアやツールをダウンロードする。
侵入拡大	Pass-the-Hash攻撃等で他のコンピュータに足掛かりを作りながら、ネットワークを動き回る。必要に応じて、追加のマルウェアをダウンロードする。
目的実行	目的の情報を探し、暗号化および細分化してから外部へ持ち出す。

APT攻撃の多発地域

図 1 の赤い丸印が示すように、APT 攻撃の標的となった国は世界中に分散しています。色が濃い国ほど、多くの攻撃が発生しています。

以下は、2013 年の FireEye のデータが示す、APT 攻撃の標的になった国トップ 10 です。

1. アメリカ
2. 韓国
3. カナダ
4. 日本
5. イギリス
6. ドイツ
7. スイス
8. 台湾
9. サウジアラビア
10. イスラエル

図 1: APT 攻撃の発生件数（国別）

FireEye 高度な攻撃に関する脅威レポート: 2013年版

http://www2.fireeye.com/advanced-threat-report-2013-ja.html?x=FE_WEB_IC

2013年度　日本を攻撃した攻撃者グループ

Aurora Panda (Hidden Lynx)

- Operation Aurora（2010年1月）の実行グループ。
- Bit9社を攻撃しコードサイニング証明書を盗む。（2013年2月）
- 米国、ドイツ、イタリア、日本など、ターゲットは広範囲に渡る。
- 製造業、メディア、防衛産業などを狙い攻撃。
- スキルが高い。例えば、Comment Panda（Comment Crew/APT1）よりもスキルが高い。

Dagger Panda (Icefog)

- 狙われた産業は、メディア、重工業、造船と多岐にわたる。
- CVE-2012-0158の脆弱性を利用。（Officeの脆弱性）
- 以前に使ったC2サーバ名（icefog.8.100911.com）から、カスペルスキー社ではicefogと呼んでいる。C2サーバ上のアプリケーションが「尖刀三号（Dagger Three）」という名称。

Deep Panda

- 米国の金融、法律、防衛、テレコム関連の産業を狙った攻撃キャンペーンを確認。
- 米国労働省のWebサイトにマルウェアを仕掛ける。（水飲み場攻撃）
- 日本でもDeep Pandaによると思われる攻撃を確認。（水飲み場攻撃）

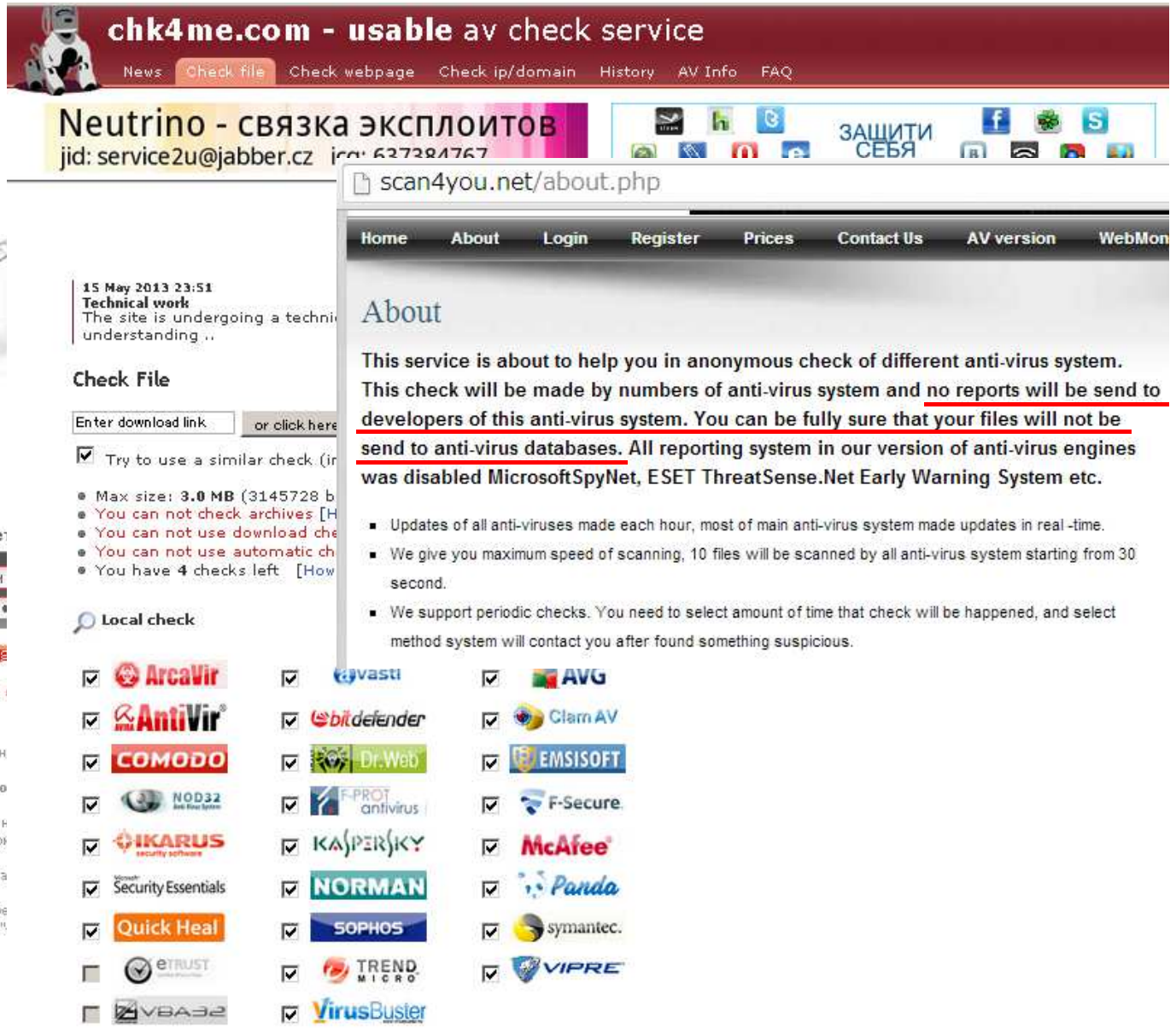
Energetic Bear

- 正規サイトを改ざん（WordPressの脆弱性を利用）して、C2サーバとして使用。
- エネルギー産業関連などをターゲットにしている模様。（昨今のロシア政府によるエネルギー外交との関連が疑われる。）

Adversary Groups

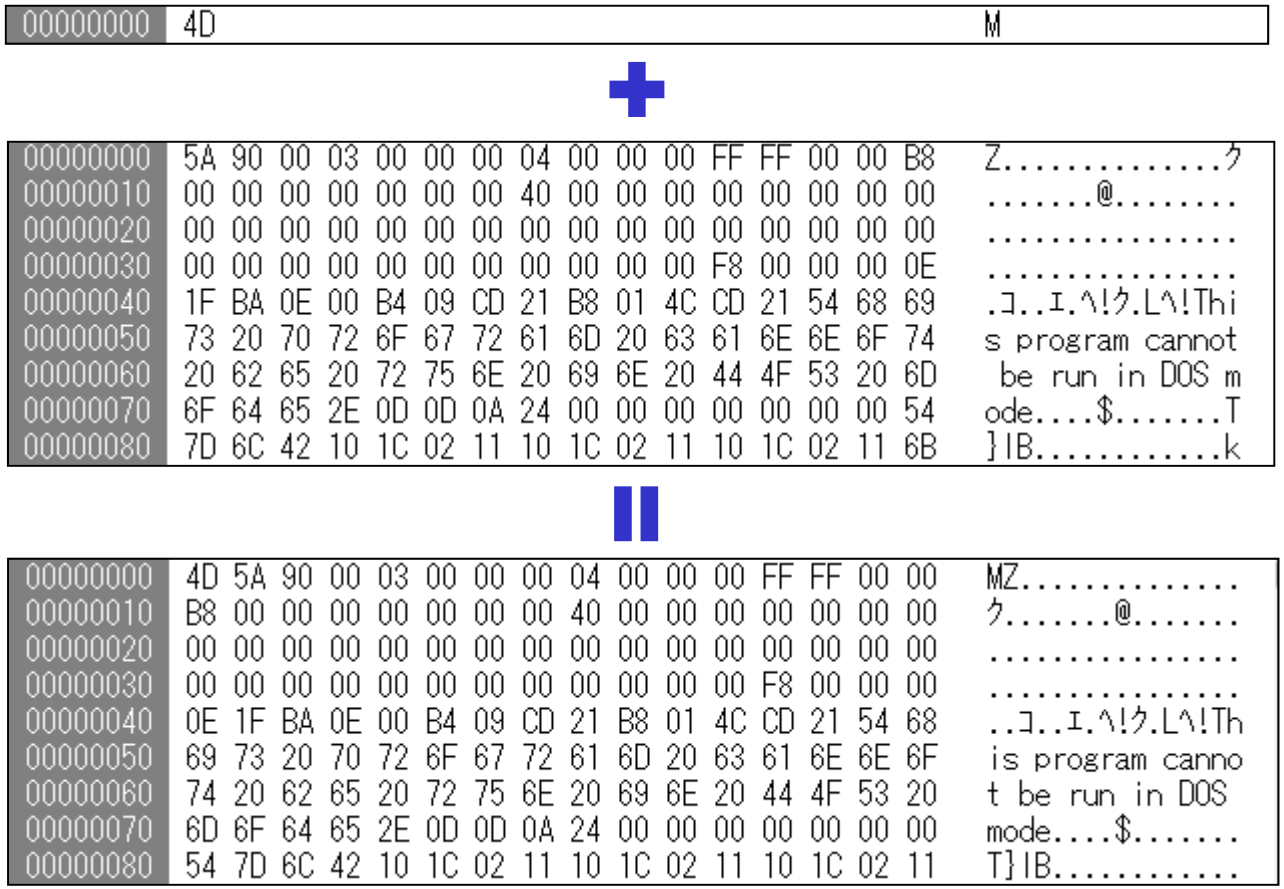
攻撃者向けAVスキャンサービス

- http://www.virtest.com/
- http://chk4me.com/
- http://scan4you.net/



マルウェアの分割

- マルウェアを分割して配送することで、途中経路にあるセキュリティ製品の検知を回避できる。



```
00000000  4D                                                M
```

＋

```
00000000  5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8   Z.............ｸ
00000010  00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00   .......@........
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030  00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00 0E   ................
00000040  1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69   .ｺ..ｴ.ﾍ!ｸ.Lﾍ!Thi
00000050  73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74   s program cannot
00000060  20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D    be run in DOS m
00000070  6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 54   ode....$.......T
00000080  7D 6C 42 10 1C 02 11 10 1C 02 11 10 1C 02 11 6B   }lB............k
```

＝

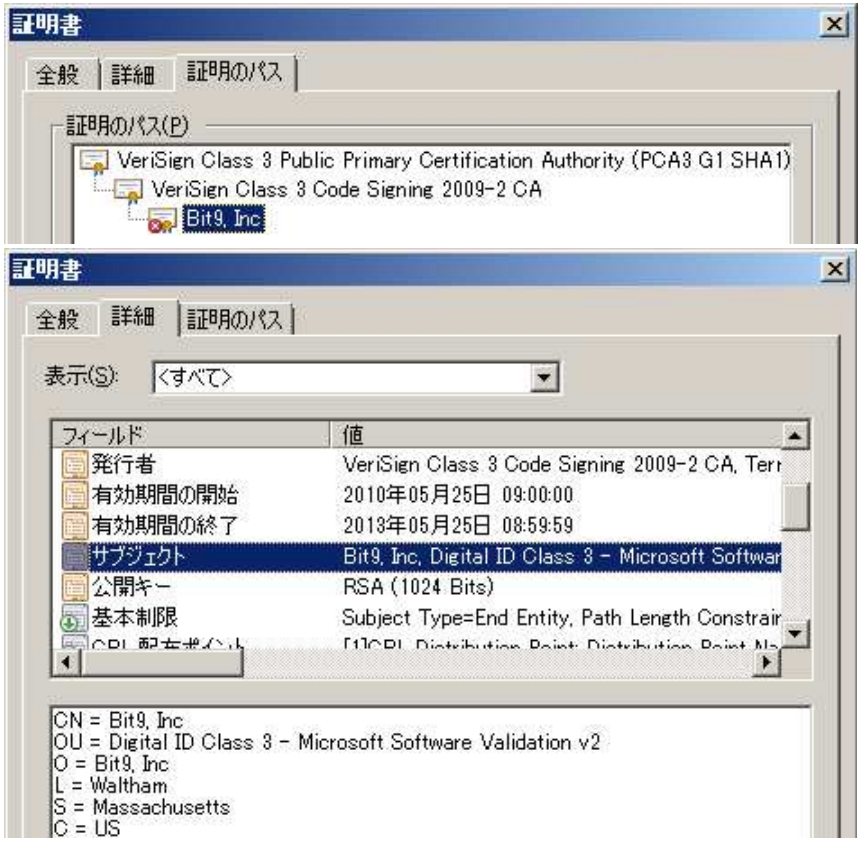
```
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..............
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ｸ.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00   ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..ｺ..ｴ.ﾍ!ｸ.Lﾍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
00000080  54 7D 6C 42 10 1C 02 11 10 1C 02 11 10 1C 02 11   T}lB............
```

- ドライブバイキャッシュと合わせ技で使われたことを確認。

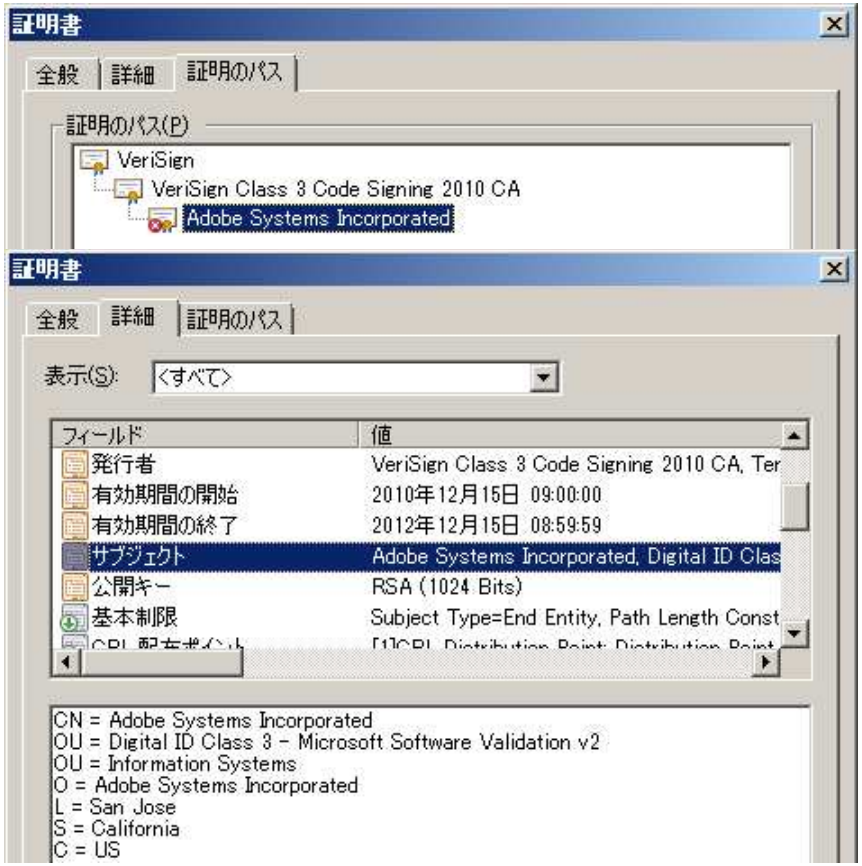
デジタル署名が付いたマルウェア

- **Adobe （2012年10月）**
- **Bit9 （2013年2月）**
- **Opera （2013年6月）**

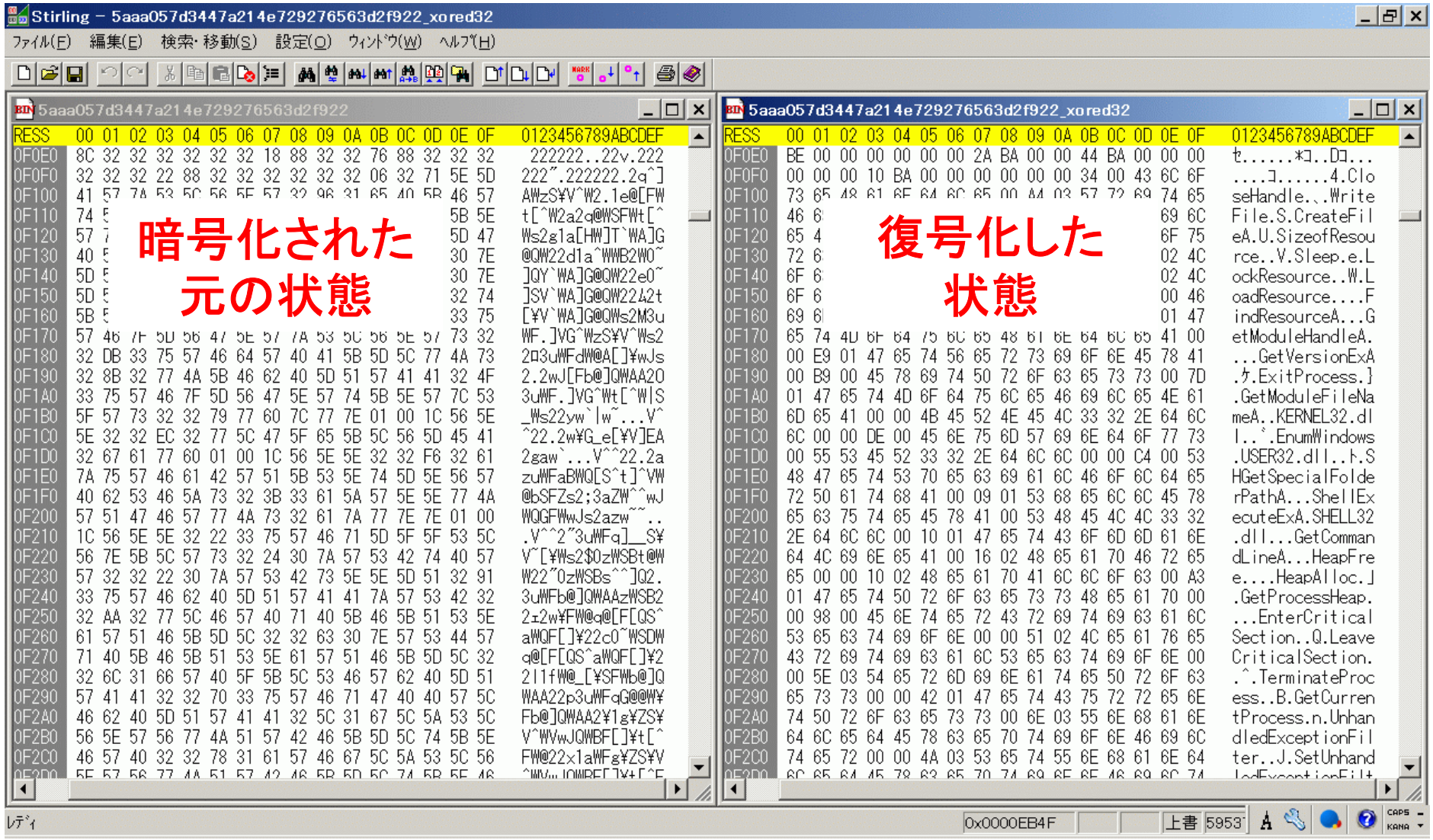
Aurora Pandaのドロッパー
MD5 Hash: 918f76b341b40af346ae7a1358548799



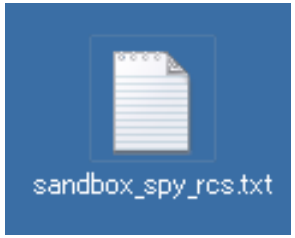
Deep PandaのRAT
MD5 Hash: 46db73375f05f09ac78ec3d940f3e61a



XOR暗号されたマルウェア



デモ： サンドボックスを見破るためのIndicator



[17/May/2014:02:33:58 +0900] "GET /?User=XXXXX&IP=X.X.X.X&ComputerName=X.X.X.X&MousePresent=XXX&MouseButtons=X&PrimaryMonitorSize=XXXXXXX&UserDomainName=XXXXX&OsVer=XXXXX HTTP/1.1" 200

サンドボックスとリアル環境との違いをもっと知りたい方は、こちらをお読みください。
http://www.atmarkit.co.jp/ait/articles/1404/18/news004.html

執筆者：
マクニカネットワークス
セキュリティ研究センター
主任研究員　凌　翔太

Attack Campaign by Aurora Panda?

- Operation Aurora / 2009
  - https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/67000/KB67957/en_US/Combating%20Threats%20-%20Operation%20Aurora.pdf
- Operation Ephemeral Hydra / 2011
  - http://www.fireeye.com/blog/technical/cyber-exploits/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
- VOHO Campaign / 2011
  - http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf
- Bit9 Incident
  - https://blog.bit9.com/2013/02/25/bit9-security-incident-update/
- Japanese Organization X / 2012
  - Attributed by CrowdStrike.
- Operation DeputyDog / 2013
  - http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
- Monju Incident / 2013
  - http://www.contextis.com/files/TA10009_20140127_-_CTI_Threat_Advisory_-_The_Monju_Incident.pdf
- Japanese Organization Y / 2014
  - Under Investigation.

Bit9 Incident

https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

The "netddesrv.exe" file is a backdoor / remote access tool containing an embedded rootkit component. This file was dropped on the compromised virtual system containing the Bit9 code-signing certificate. This backdoor is customized for each victim and creates a corresponding "netddrsrv.conf" configuration file which we believe contains the target name and the beacon address to use.

Filename	netddesrv.exe
File size	73216 bytes
MD5	fc99fa2d9872eab586478b98c33beca5
SHA1	57f2d86de4de82627ab6ada51be6903f37a0d583
Version metadata	Child Type: StringFileInfo Language/Code Page: 1033/1200 Comments: CompanyName: FileDescription: NetDDESrv FileVersion: 1, 0, 0, 1 InternalName: NetDDESrv LegalCopyright: Copyrigh LegalTrademarks: OriginalFilename: msrv.exe PrivateBuild: ProductName: NetDDESrv ProductVersion: 1, 0, 0, 1 SpecialBuild: Child Type: VarFileInfo Translation: 1033/1200

https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

The first beacon contains fifty-two (52) bytes of encoded data. When decoded with a four (4) byte XOR key, the following string is revealed: "**matrix_passwor**".

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	97	85	DD	C0	8E	87	CF	E0	92	85	DD	C0	9E	81	DD	C0
00000010	22	84	DD	C0	8B	85	DD	C0	FA	85	BC	C0	E3	85	AF	C0
00000020	FE	85	A5	C0	C8	85	AD	C0	F6	85	AE	C0	E4	85	AA	C0
00000030	F8	85	AF	C0												

Raw HEX view of the NetDDESrv beacon data

デコード後に見られる特徴的なString

XOR

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	00	00	00	00	19	02	12	20	05	00	00	00	09	04	00	00
00000010	B5	01	00	00	1C	00	00	00	6D	00	61	00	74	00	72	00
00000020	69	00	78	00	5F	00	70	00	61	00	73	00	73	00	77	00
00000030	6F	00	72	00												

Decoded HEX view of the NetDDESrv beacon data

DMZの公開サーバに対するSQLインジェクションがキッカケ。

コードサイニング証明書を盗まれる。

XOR暗号化されたペイロード（Japanese Organization X）

```
⊞ Frame 14: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: [redacted], Dst Port: https (443), Seq: 1, Ack: 1, Len: 54
  Secure Sockets Layer
```

```
0000  [redacted]
0010  [redacted]                                        54 bytes
0020  [redacted] 01 bb fe 09 e3 b1 00 00 02 0[redacted]  ....... ......P.
0030  fa f0 eb 19 00 00 55 f3 b3 52 64 f0 a1 72 50 f3  ......U. .Rd..rP.
0040  b3 52 5c f7 b3 52 e0 f2 b3 52 4b f3 b3 52 38 f3  .R\..R.. .RK..R8.
0050  d2 52 21 f3 c1 52 3c f3 cb 52 0a f3 c3 52 34 f3  .R!..R<. .R...R4.
0060  c0 52 26 f3 c4 52 3a f3 c1 52 31 f3              .R&..R:. .R1.
```

XOR

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   00 00 00 00 31 03 12 20 05 00 00 00 09 04 00 00   ....1.. ........
00000010   B5 01 00 00 1E 00 00 00 6D 00 61 00 74 00 72 00   µ.......m.a.t.r.
00000020   69 00 78 00 5F 00 70 00 61 00 73 00 73 00 77 00   i.x._.p.a.s.s.w.
00000030   6F 00 72 00 64 00                                 o.r.d.
```

日本国内の大学にある正規サーバがC2に利用されていた。

XOR暗号鍵がコネクション毎に変化。

XOR暗号化されたペイロード（Japanese Organization Y）

```
⊞ Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: [redacted], Dst Port: https (443), Seq: 1, Ack: 1, Len: 54
  Secure Sockets Layer
```

```
0000  [redacted]                                        [redacted]
0010  [redacted]                                        [redacted]
0020  [redacted] 01 bb 19 bc  d4 d1 df 92 4b 9a [redacted]  [redacted]....K.P.
0030  01 00 e1 95 00 00 bc a8  5a 23 8d ab 48 03 b9 a8  ........ Z#..H...
0040  5a 23 ad ac 5a 23 18 ab  5a 23 a2 a8 5a 23 d1 a8  Z#..Z#.. Z#..Z#..
0050  3b 23 c8 a8 28 23 d5 a8  22 23 e3 a8 2a 23 dd a8  ;#..(#.. "#..*#..
0060  29 23 cf a8 2d 23 d3 a8  28 23 d8 a8              )#..-#.. (#..
```

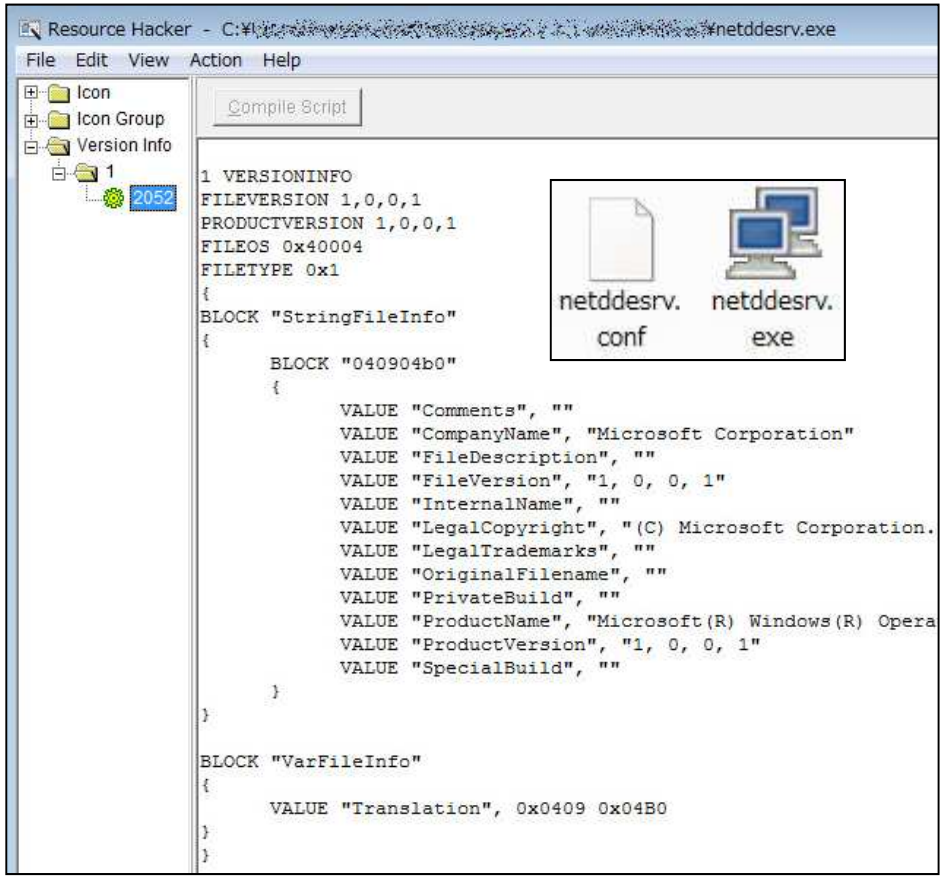
54 bytes

XOR

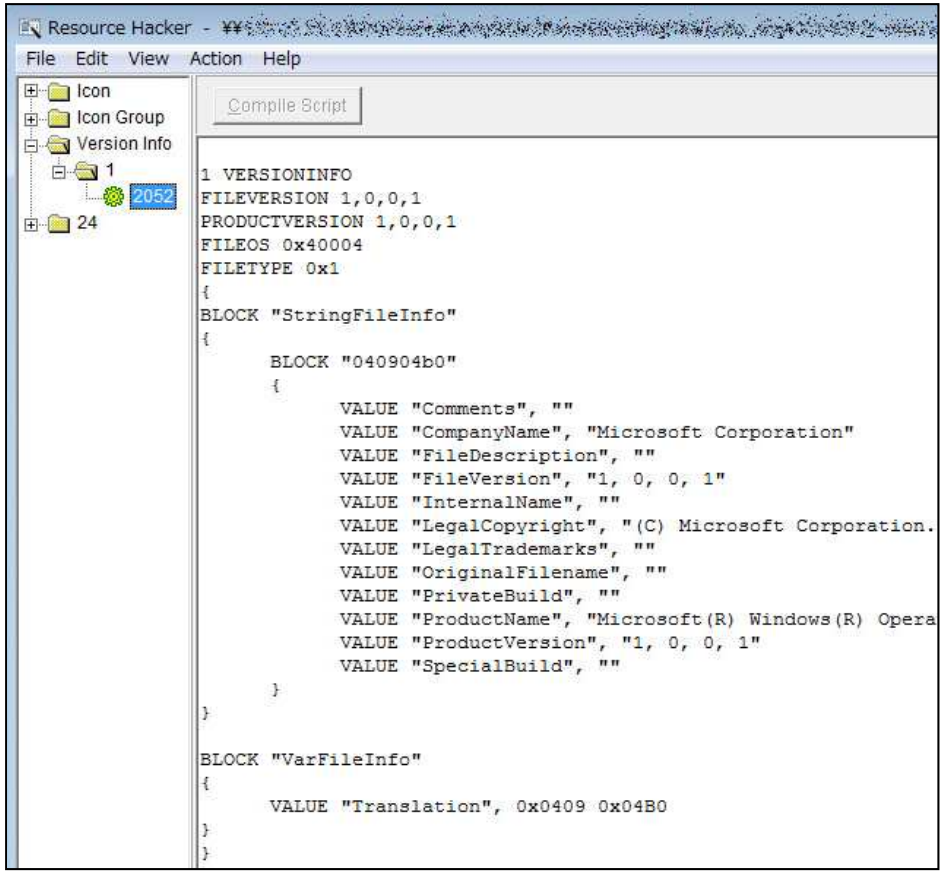
```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   00 00 00 00 31 03 12 20 05 00 00 00 11 04 00 00   ....1.. ........
00000010   A4 03 00 00 1E 00 00 00 6D 00 61 00 74 00 72 00   ¤.......m.a.t.r.
00000020   69 00 78 00 5F 00 70 00 61 00 73 00 73 00 77 00   i.x._.p.a.s.s.w.
00000030   6F 00 72 00 64 00                                 o.r.d.
```

韓国にあるサーバがC2で利用されていた。（攻撃者が所有しているドメイン/IPアドレスかは不明）

検体の類似性



Japanese Organization X



Japanese Organization Y

Gh0st RAT variant

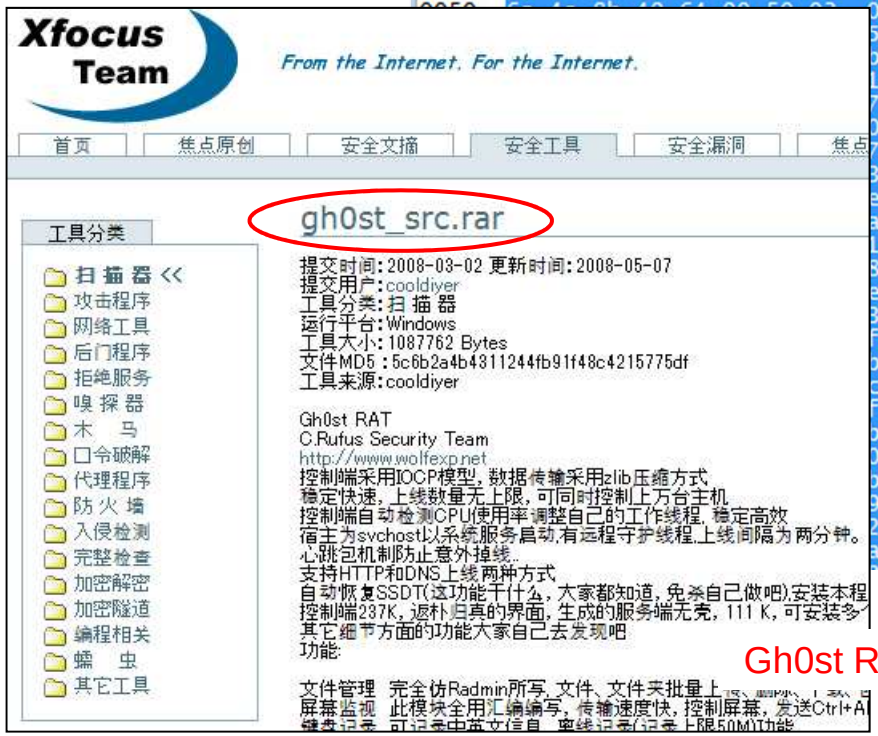
VOHOキャンペーンとGOM Playerアップデート時に仕込まれたマルウェアは、Gh0st RATの亜種だった。

No.	Time	Source	Destination	Protocol	Length	Info
34	15.912568	10.0.2.15	198.199.78.132	TCP	62	td-postman > https [SYN] Seq=0
35	15.987211	198.199.78.132	10.0.2.15	TCP	58	https > td-postman [SYN, ACK] S
36	15.987378	10.0.2.15	198.199.78.132	TCP	60	td-postman > https [ACK] Seq=1
37	15.993719	10.0.2.15	198.199.78.132	SSL	573	Continuation Data
38	15.993791	198.199.78.132	10.0.2.15	TCP	54	https > td-postman [ACK] Seq=1

```
Frame 37: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits)
Ethernet II, Src: CadmusCo_29:78:cd (08:00:27:29:78:cd), Dst: RealtekU_12:35:02 (52:54:00:12:35:02
Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 198.199.78.132 (198.199.78.132)
Transmission Control Protocol, Src Port: td-postman (1049), Dst Port: https (443), Seq: 1, Ack: 1,
Secure Sockets Layer
```

```
0000  52 54 00 12 35 02 08 00  27 29 78 cd 08 00 45 00   RT..5... ')x...E.
0010  02 2f 00 52 40 00 80 06  d7 1c 0a 00 02 0f c6 c7   ./.R@... ........
0020  4e 84 04 19 01 bb 96 4c  04 26 00 00 00 fa 02 50   N......L .&.....P.
0030  fa f0 5f a9 00 00 48 54  54 50 53 07 02 00 00 80   .._...HT TPS.....
0040  03 00 00 78 9c ad 52 4b  68 13 51 14 3d 6f a4 52   ...x..RK h.Q.=o.R
```

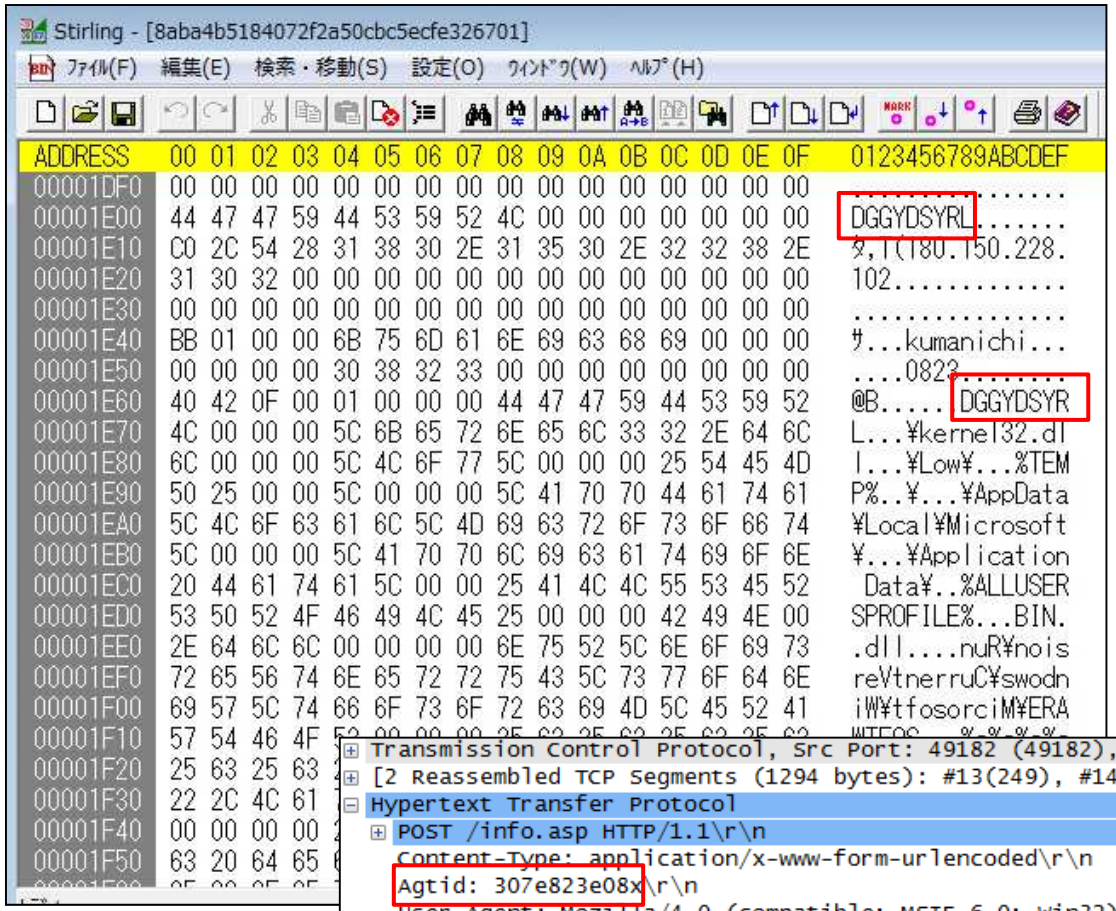
本家のGh0st RATでは、”Gh0st”という5 bytesが入る。

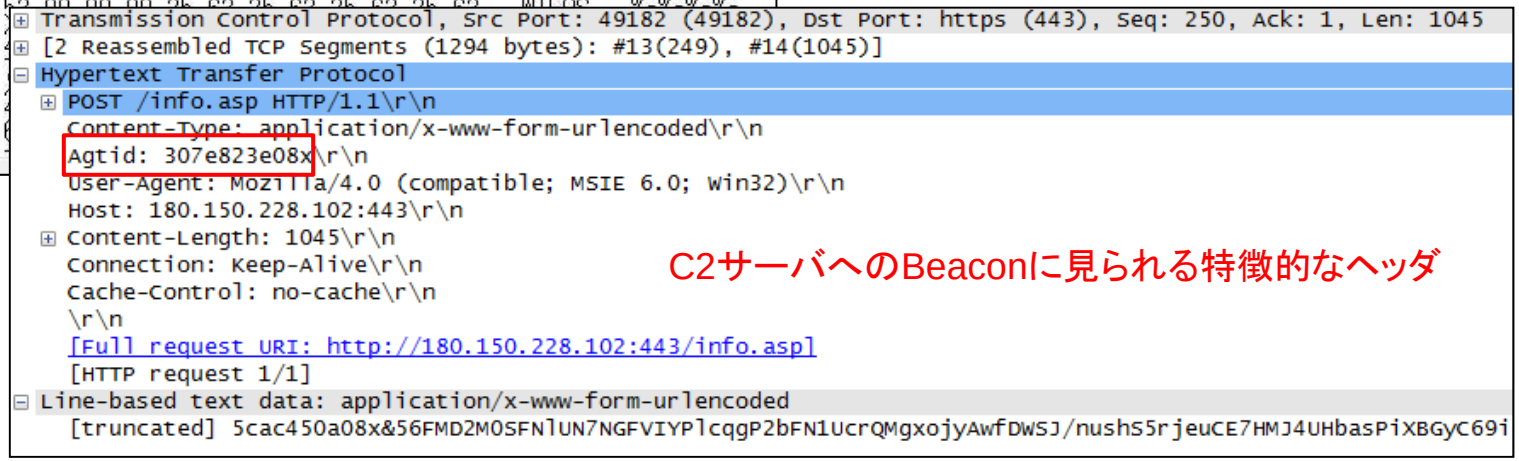



```
........ .q)..kq.
.=/3mE.] x.;..{..
{....@L. .D.....1
..T....d q."o..l.
...H.... 0.x.k..{
....;Q.Y ....5..F
q..F.p.. ..e.Q-..
.P^.... .. +..X.
=..nI..! ....d...
...6..x. ..T.&N._
2~..LPw. 5z..(..I
V.....;. .Y..L...
.2.....: .ew.....
...j..|. .H......
JTp.e>.. ..LDO...
aQ...0.D ...Y)Nd.
.]..]?.. ..m.6G.H
./.g...i ..x..i..
........ ..<z/%Ev
.Q]...Z. ).'.g...
._..9.fP ..C.6..U
```

Gh0st RATのソースコードは2008年から公開されている。

Operation DeputyDog





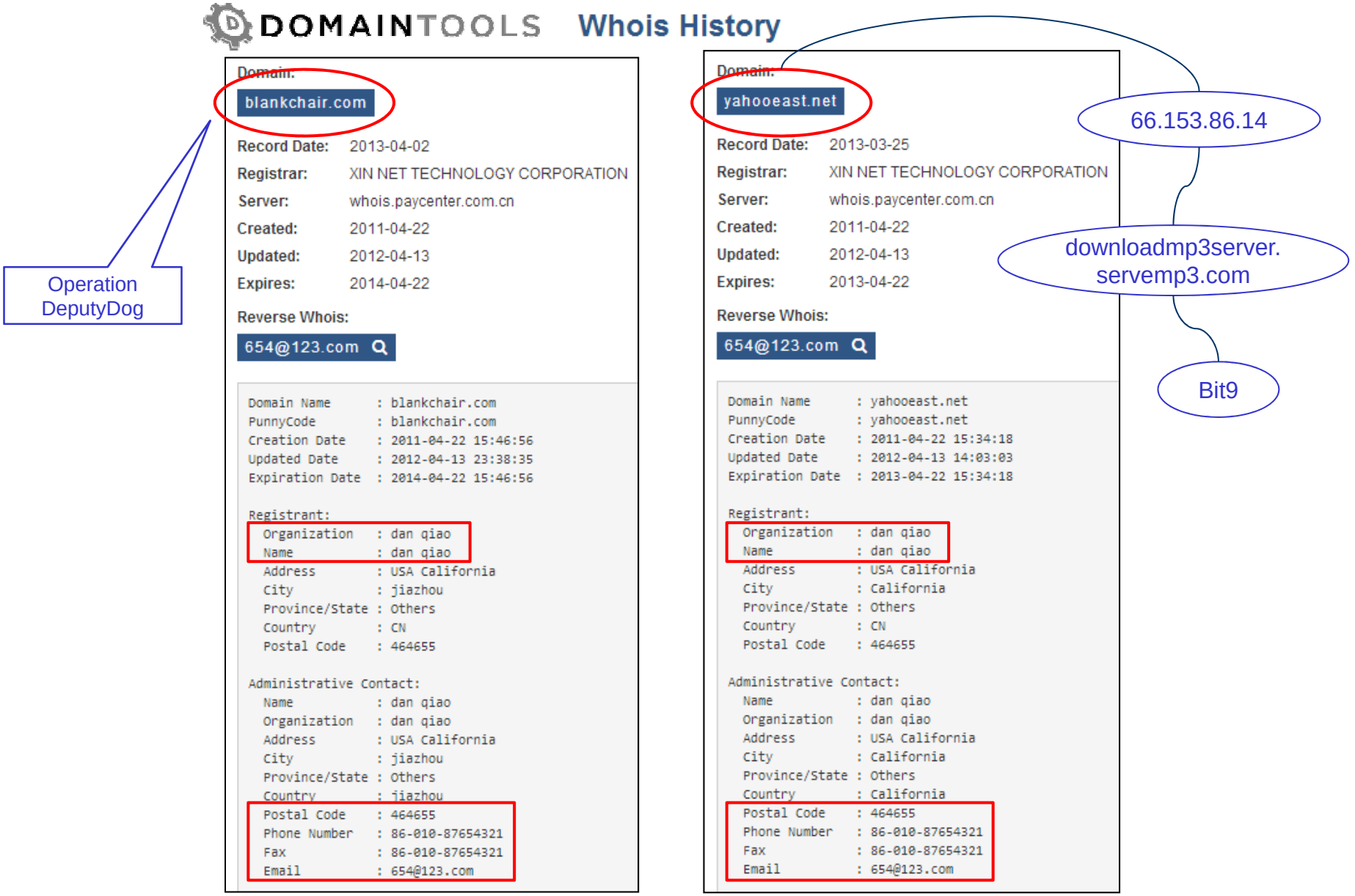
日本を狙った攻撃キャンペーン

ゼロデイの脆弱性を利用
CVE-2013-3893（IEの脆弱性）

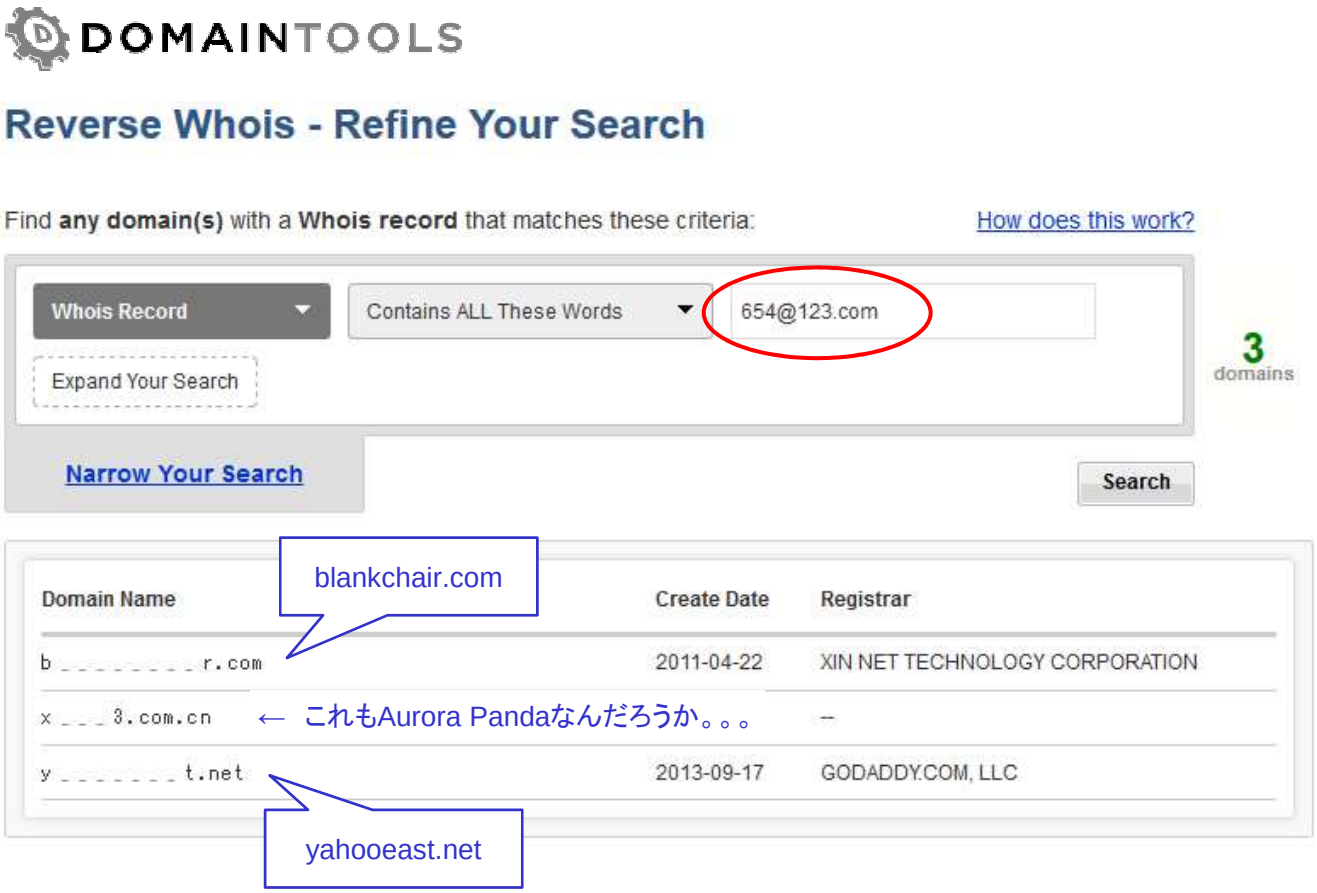
バイナリファイルに見られる特徴的なString

C2サーバへのBeaconに見られる特徴的なヘッダ

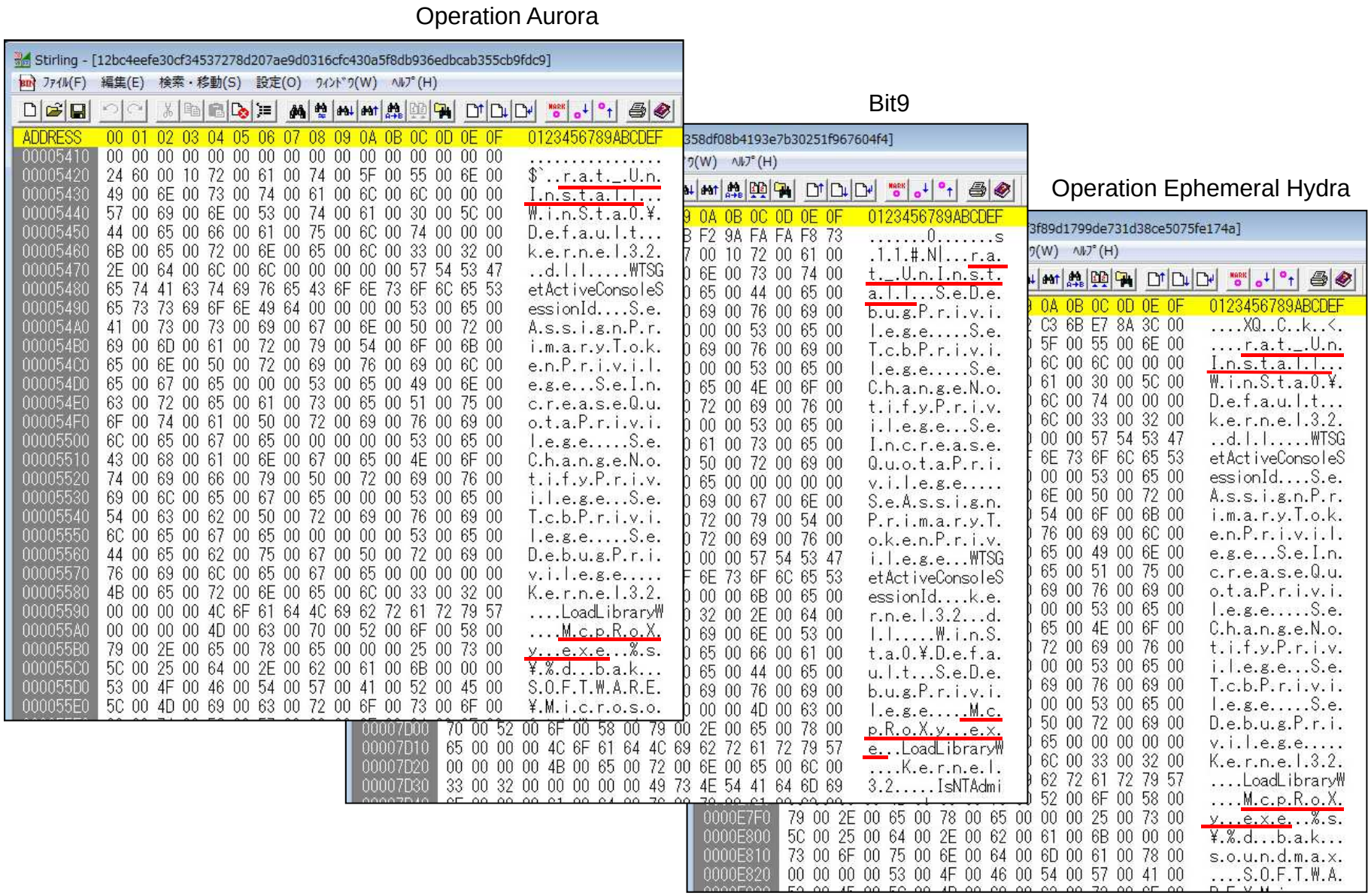
Whois History



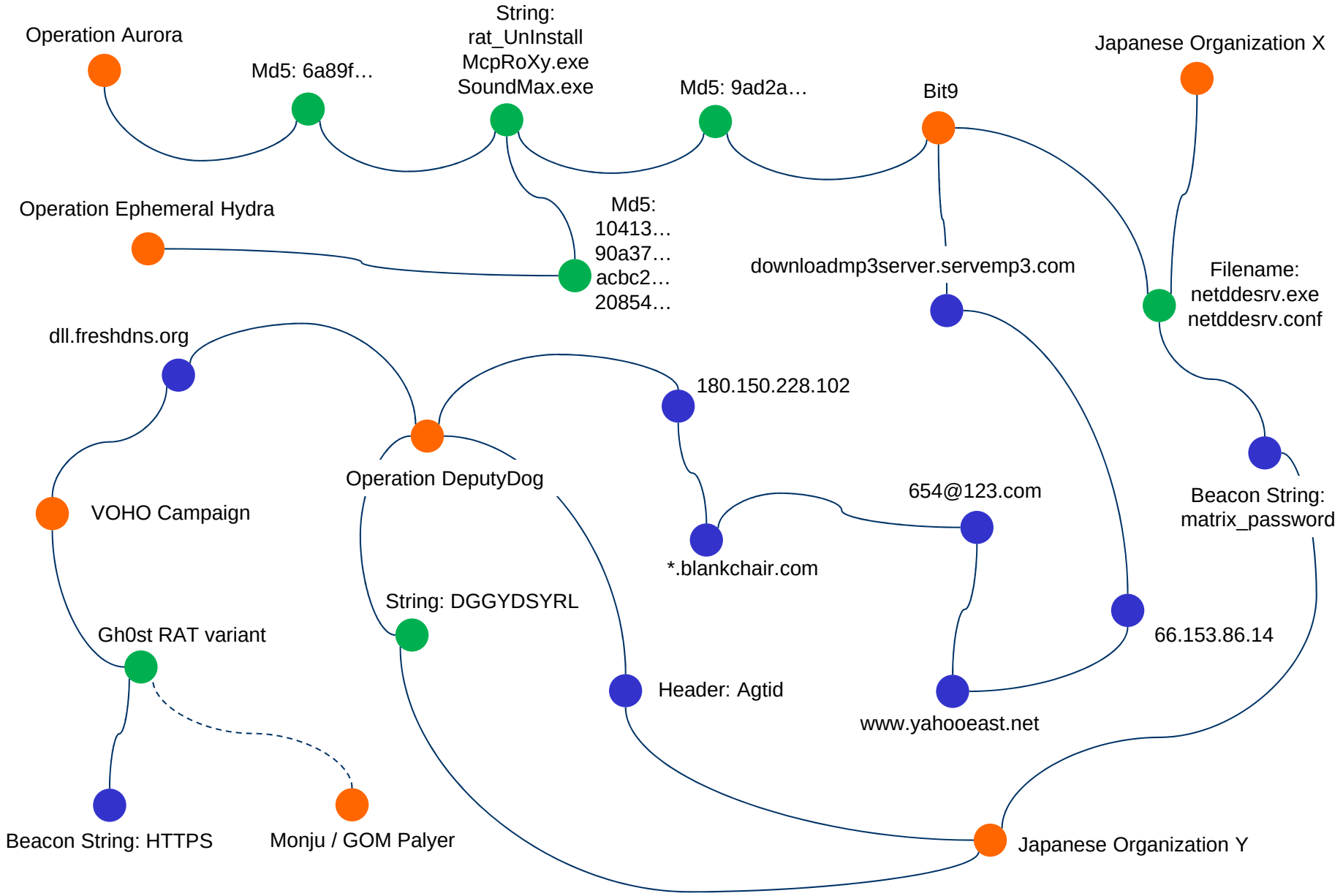
Reverse Whois



検体の類似性

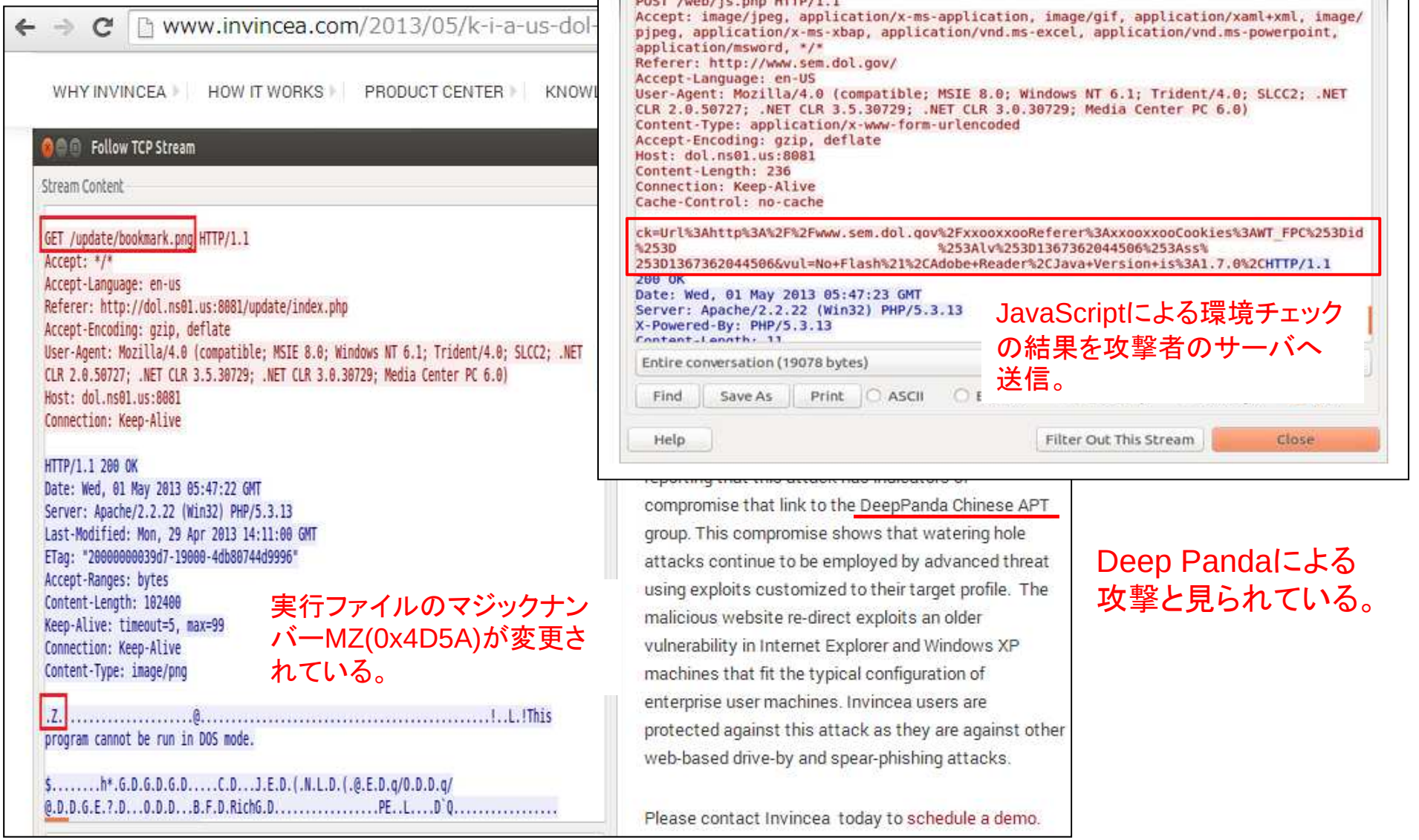


Connecting the Dots - Aurora Panda



DOLが水飲み場になった事例

Invincea社のブログによると、



http://www.invincea.com/2013/05/k-i-a-us-dol-website-pushing-poison-ivy-cve-2012-4792/

日本で確認された水飲み場攻撃 （Deep Panda？）

FireEye　FireEyeによる検知結果

Infection:	Exploit.APT.Waterhole	Communication Capture	pcap 499 bytes (text)
		IP Protocol:	TCP
Interface:	network A1 (mode tap)	Attacked Port:	80
Blocking Action:	NOT blocked	Src IP:	[redacted]
		Src MAC Address:	[redacted]
		Dst MAC Address:	[redacted]

Attempted infection communication:
Server DNS Name: [redacted] Service Port: *80* Signature Name: *Exploit.APT.Waterhole*

Direction	Command	User-Agent	Host
POST	/wp-content/uploads/2013/jQuery/201311/js.php HTTP/1.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	[redacted]

Others

Accept:
image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*

Referer:
[redacted]

Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 922
Parameters:
ck=Url%3Ahttp%3A%2F%2F[redacted]%2F1xxooxxooReferer%3AxxooxxooCookies%3A[redacted]%253D

Exploitを踏んだ直後に発生した通信
フォーマットがDOLのときと似ている。

Deep Pandaに関する詳しい情報は、

CrowdStrike Deep Panda　検索

Energetic Bearによる攻撃キャンペーン（2014年1月頃）

- [redacted].ru/wp-includes/pomo/pomo.php
- [redacted].net/wp-includes/pomo//idx.php
- [redacted].net/wp-includes/pomo/idx.php
- [redacted].com/modules/mod_search/mod_research.php
- [redacted].com/wp06/wp-includes/po.php
- [redacted].com/wp05/wp-admin/includes/tmp/tmp.php
- [redacted].ua/includes/domit/src.php
- [redacted].com/app/usr/usr_src.php
- [redacted].com/includes/phpmailer/class.pop3.php
- [redacted].ir/skin/install/default/default/source.php
- [redacted].com/wp-includes/pomo/idx.php
- [redacted].com/wordpress/wp-includes/pomo/idx.php

CROWDSTRIKE

CrowdStrike社によって、約150個のC2および水飲み場となったドメインを確認。
その全てが正規サイトであった。

改ざんされた正規サイトの多くでWordPressが使われていた。

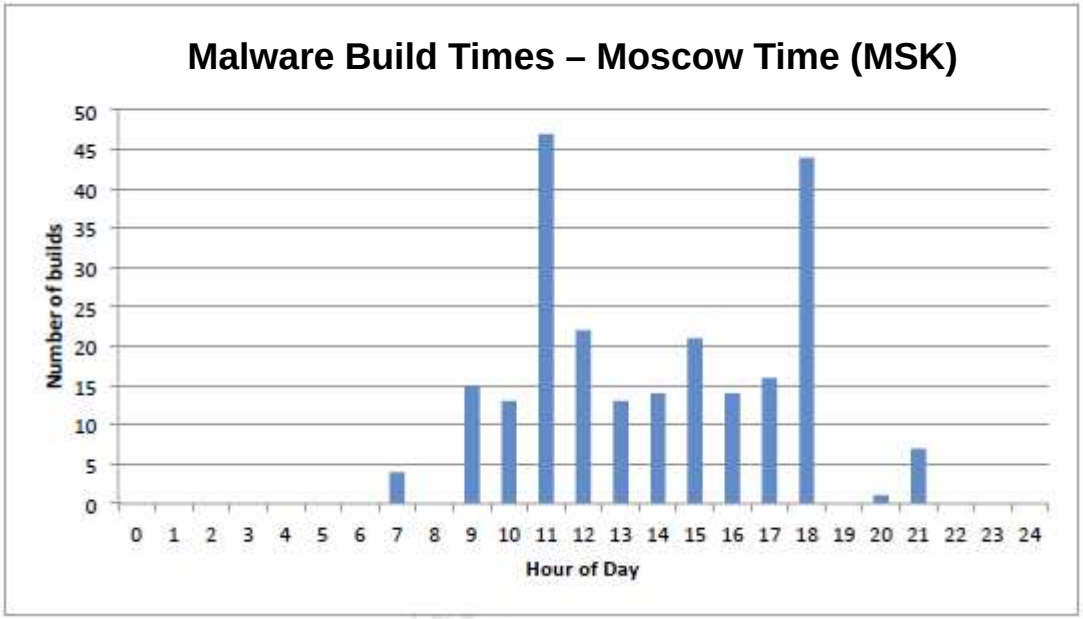
- [redacted]/wp-includes/pomo/dx.php
- [redacted].com/tareas/include/_php.php
- [redacted].ru/includes/phpmailer/source.php
- [redacted].com/catalog/install/source.php
- [redacted].com/cna/[redacted]/cna_source.php
- [redacted].ru/modules/mod_search/idx.php
- [redacted].com/res/code/res.php
- [redacted].co.jp/inc/user//mysql_s.php
- [redacted].co.jp/inc/user/mysql_s.php
- [redacted].com/chief-cooker/tiny_mce/plugins/searchreplace/edit.php
- [redacted].org/modules/mod_search/search.php

CROWDSTRIKE

Copyright 2013

Attribution Indicators （攻撃者の属性）

- C2 IP address ownership
- C2 Domain
- C2 Payload
- Whois Record
- Filename/Path
- Registry
- Mutex
- Time Zone Information
  - Build times
  - C2 check-in times
- Code Styles
- Resource Language



攻撃者のTTPs （フィクション）

	Campaign #1	Campaign #2	Campaign #3	Campaign #4
偵察	N/A	N/A	N/A	N/A
武器化	netddesrv.exe hitx.sys, https.sys Chinese-Simplified	Abc.exe String: DGGYDSYR Chinese-Simplified	netddesrv.exe https.sys Chinese-Simplified	GIUEL.exe String: DGGYDSYR Chinese-Simplified
配送	SQLi against web servers	Watering hole attack 180.150.228.x	Water hole attack 180.150.228.x	Spear Phishing aurora@xxx.yyy.com
攻撃 （エクスプロイト）	SQL Injection CVE-2011-3544(Java)	CVE-2012-1723(Java)	CVE-2013-3893(IE)	CVE-2013-3906(MS-Office)
インストール	%USERPROFILE%¥BITS.dll %TEMP%NHLGNS.DAT HKEY...Services¥NetDDESrv	%SYSTEMROOT%¥system32¥wbem¥xxx.dll	%SYSTEMROOT%¥system32¥wbem¥oci.dll %SYSTEMROOT%¥system32¥drivers¥W7fw.sys	%TEMP%¥svchost.exe %TEMP%NHLGNS.DAT HKEY...Services¥NetDDESrv
遠隔操作 （C2）	servemp3.com/66.153.86.14 String: matrix_password	blankchair.com yahooeast.net/66.153.86.14 Header: Agtid	freshdns.org 180.150.228.103 String: matrix_password	211.x.y.z String: matrix_password Header: Agtid
侵入拡大	N/A	pwdump HTran	pwdump PsExec	wce PsExec
目的実行	Code signing certificate	Intellectual property	Unknown	Intellectual property

Indicators

Atomic Indicators

IPアドレス
FQDN
URL
ファイル名
レジストリ

ヘッダ
String
Mutex
メールアドレス

Computed Indicators

MD5/SHA-1/SHA-256

Fuzzy Hashing
(ssdeep)

imphash

正規表現

Behavioral Indicators

AcroRd32.exeから
cmd.exeがキックされる

TCP80番の上で
未知のプロトコル

DNS名前解決
の失敗が頻発

SAMからNTLM
ハッシュを読み取る

%TEMP%の配下に
XXX.exeを書き込む

OpenIOC: http://www.openioc.org/
Cybox: http://cybox.mitre.org/

Yara: http://plusvic.github.io/yara/
Snort: http://www.snort.org/

Indicatorを共有するためのフォーマット

Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 53,80,443,1080 (msg:"gh0st RAT 'HTTPS' variant (aka
Backdoor.Miancha)"; flow:established,to_server; content:"HTTPS"; depth:5; rawbytes; classtype:trojan-
activity; sid:xxx; rev:1;)
```

By Context Information Security

Yara

```
rule APT_DeputyDog_Strings
{
        meta:
                author = "FireEye Labs"
                version = "1.0"
                description = "detects string seen in samples used in 2013-3893 0day attacks"
                reference = "8aba4b5184072f2a50cbc5ecfe326701"
        strings:
                $mz = {4d 5a}
                $a = "DGGYDSYRL"
        condition:
                ($mz at 0) and $a
}
```

By FireEye

Indicatorを共有するためのフォーマット

Name: CALENDAR (FAMILY)
Author: Mandiant
GUID: 6bd24113-2922-4d25-b490-f727f47ba948
Created: 2013-02-10 06:11:53Z
Modified: 2013-02-10 13:00:00Z

Type	Reference
family	CALENDAR
threatgroup	APT
family	APT1
category	Backdoor

Description:

This family of malware uses Google Calendar to retrieve commands and send results. It
event contains commands from the attacker for the malware to perform. Results are pos
using the hard coded email address and passwords. The malware uses the deprecated C
registered as a service dll as a persistence mechanism. Artifacts of this may be found i

Add: AND OR Item

```
OR
  File MD5 is cf37875adf10fb56c7c6edf86f2b3438
  File MD5 is 7bea48f1f08e2677df168e0bbe9f19ac
  File MD5 is 16c390a32f9a60bf50396fc86aea0f9d
  File Strings contains AFX_Ideas_H
  AND
    OR
      File Name is wmdmpmsn.dll
      File Name is rasautoe.dll
      File Detected Anomalies is checksum_mismatch
    OR
      File Size is 142848
    OR
      File Compile Time is 2012-02-15T13:49:01Z
  AND
    Process Handle Type is Mutant
    Process Handle Name contains AFX_Ideas_H
  AND
    File Dll Export Name is ServiceAutoRun.dll
    File Export Function contains ServiceMain
    File Export Function contains install
    File Export Function contains installservice
    File Export Function contains uninstall
    File Export Count is 4
  AND
    Registry Path contains system\currentcontrolset\services
    Registry Path contains parameters\servicedllold
```

OpenIOC

Add: AND OR Item

```
OR
  File MD5 is f0726aadcf5d66daf528f79ba8507113
  File MD5 is 5e0df5b28a349d46ac8cc7d9e5e61a96
  Service Name contains SaSaut
  Service Descriptive Name contains System Authorization Service
  Service Description contains Authorization and authentication service f
  Registry Path contains CurrentVersion\SvcHost\SaSaut
  AND
    File Detected Anomalies is checksum_is_zero
    File Detected Anomalies is contains_eof_data
    OR
      File Name is setup.dll
      File Name is spool.exe
      File Compile Time is 2010-03-30T09:00:00Z TO 2010-03-30T12:00:00Z
    OR
      File Size is 37376
      File Size is 50176
  AND
    File Dll Export Name is svc.dll
    File Export Function contains MyService
  AND
    Registry Text contains java.exe
    Registry Path contains CurrentVersion\Run\sysinfo
  AND
    Service DLL contains \setup.dll
    Service DLL Signature Verified is False
```

By Mandiant

http://www.invincea.com/2013/05/k-i-a-us-dol-website-pushing-poison-ivy-cve-2012-4792/

Indicatorを共有するためのフォーマット

Cybox

http://cybox.mitre.org/

http://www.ipa.go.jp/security/vuln/CybOX.html

Network Behavioral Indicator （マルウェアから発生する通信の特徴）

- 非標準ポートでの通信。（TCP80番以外のHTTP　など）
- 標準ポートを使った未知プロトコル。（TCP80番でHTTP以外　など）
- Content-Typeヘッダ値がコンテンツ内容と不一致。
- プロキシ認証の失敗が多い。
- DNS名前解決（No such name）の失敗が多い。
- FirewallでDenyされる通信が多い。
- 通信先のドメイン年齢が若い。
- TLDがレア。（.onion、.cn、.ru　など）
- 通信先IPアドレスの所在がレアな国。（中国、ロシア、エストニア　など）
- 通信間隔が一定な通信先IPアドレス。（標準偏差が小さい）
- 複数のUser-Agent値を使われている端末。
- User-Agentがレアな値。
- Hostヘッダ値がIPアドレス。（IPアドレス直打ち）
- TCP443番以外のCONNECTメソッド。
- POSTメソッドの比率が高い端末。
- 自己署名証明書を使ったHTTPS通信。
- 外部への転送バイト量が多い。
- 業務時間外の通信。

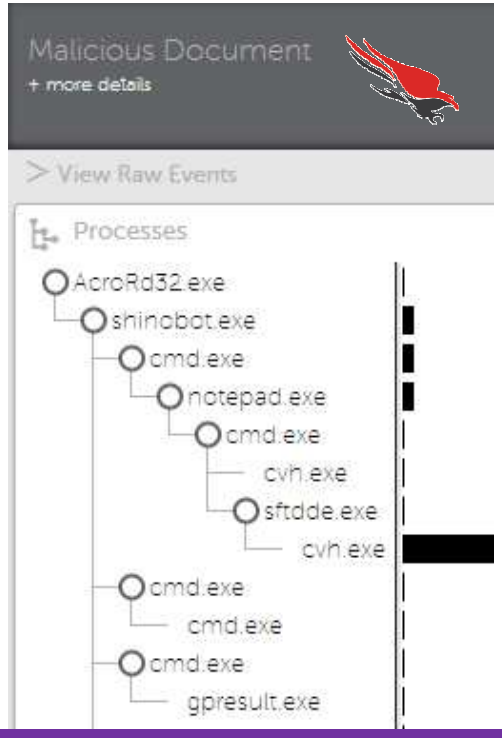
既存のフォーマットに落とし込めないIndicatorは、SIEMやSplunkなどのテクノロジーに頼るのも手段の一つ。

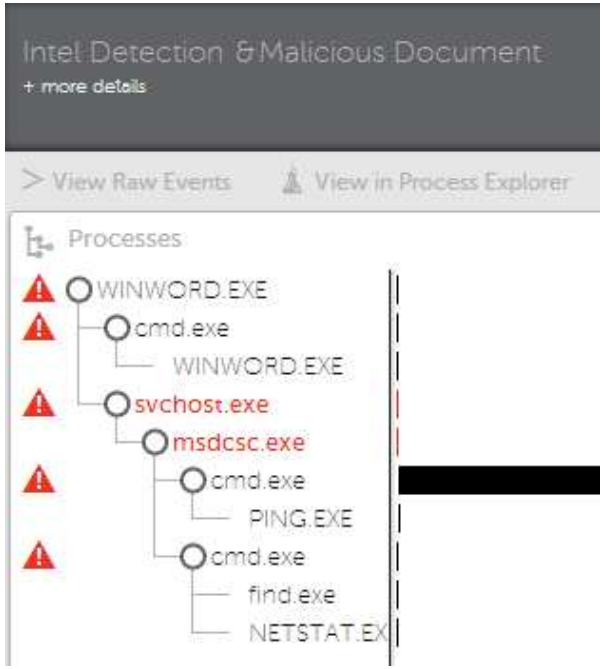
Host Behavioral Indicator（ホスト内でのマルウェアの挙動）

- AcroRd32.exeからcmd.exeがキックされた。
- Windowsのログオンパスワード・ハッシュを読み取った。
- ブラウザで記憶されているユーザ名、パスワードを読み取った。
- C:¥Users¥<ユーザ名>¥AppData¥Local¥Tempのフォルダに実行ファイルを作成。
- バイナリファイルがパッカーで圧縮されている。
- 自動起動するレジストリを変更。（ASEP）
- C:¥Windows¥System32フォルダに実行ファイルを作成した。

Strong

Weak





既存のフォーマットに
落とし込めないIndicatorは、
ホストIPSなどのテクノロジー
に頼るのも手段の一つ。

ETDR
=
Endpoint Threat Detection and
Response Tools

Indicator Hierarchy

http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

Adversary

（攻撃者＝TTPs）

エクスプロイト（攻撃コード）

IPアドレス、FQDN、URL

マルウェア・ハッシュ値

まとめ

- 攻撃者はセキュリティ製品による検知を回避するため、インテリジェンスを蓄積し、様々なテクニックを使う。
- しかし、攻撃者も人間であり組織である以上、リソースは有限である。（資金、技術、システム、時間　など）
- よって、前回の攻撃キャンペーンと同じ属性を示す場合がある。
- OSINTや商用サービスを活用することで、攻撃者の属性を知り、脅威インテリジェンスを蓄積することができる。
- 脅威インテリジェンスをIndicatorに落とし込み、それを活用することで、検知能力の向上と迅速なインシデント調査が可能となる。
- 既存のフォーマットに落とし込めないIndicatorは、ホストIPS（ETDR）やSIEM、Splunkなどのテクノロジーを使うのが良いと思う。

ご清聴ありがとうございました。

研究センターのブログを開設！

http://blog.macnica.net/

世界の最新セキュリティ技術や動向を紹介！