

# 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

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



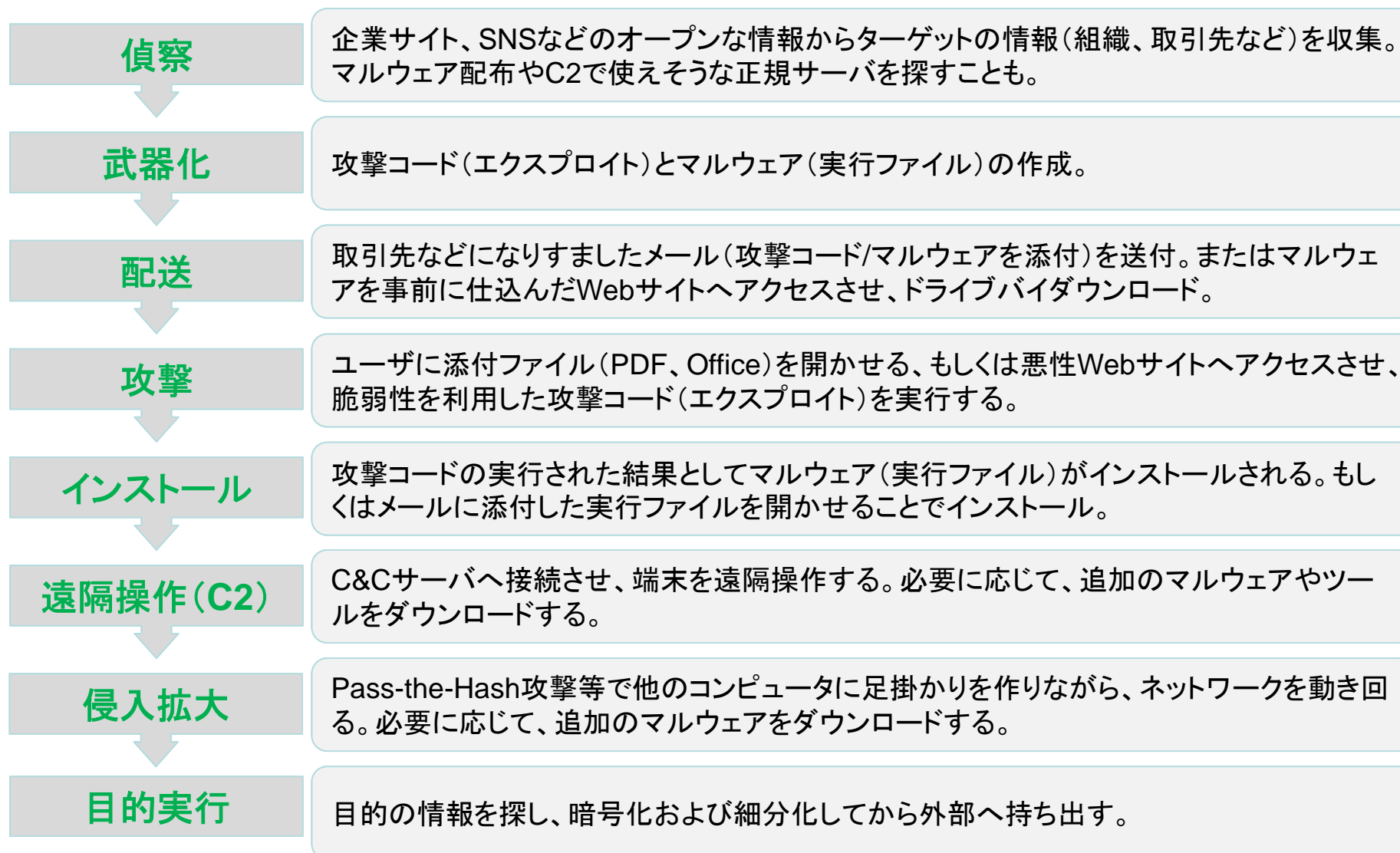
マクニカ新横浜本社



西日本支社

# 取扱い製品(セキュリティ関連)





# 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



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

## ■ 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ン証明書を盗む。(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



## CHINA

- Comment Panda:** Commercial, Government, Non-profit
- Deep Panda:** Financial, Technology, Non-profit
- Foxy Panda:** Technology & Communications
- Anchor Panda:** Government organizations, Defense & Aerospace, Industrial Engineering, NGOs
- Impersonating Panda:** Financial Sector
- Karma Panda:** Dissident groups
- Keyhole Panda:** Electronics & Communications
- Poisonous Panda:** Energy Technology, G20, NGOs, Dissident Groups
- Putter Panda:** Governmental & Military
- Toxic Panda:** Dissident Groups
- Union Panda:** Industrial companies
- Vixen Panda:** Government

## IRAN

**Clever Kitten:** Energy Companies

## INDIA

**Viceroy Tiger:** Government, Legal, Financial, Media, Telecom

## RUSSIA

**Energetic Bear:** Oil and Gas Companies

# 攻撃者向けAVスキャンサービス

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

Virtest.com

Support:  
ICQ: 570352881  
GTalk: virtest@gmail.com  
Jabber: virtest@jabber.ru



Кабинет:

Логин

Site

Наибольшее количество антивирусных движков среди ан  
не производится выборочно на любое количество ав-движко  
куда не утекает и не отсылается в ав-конторы - проверяемые файлы н  
их файлов с антивирусной конторой (если таковые имеются и были до  
альная функция сканирования выдачич связок. Подробно описа  
ежных папок/архивов (с любой вложенностью подпапок), причем ре  
файл в нем!"



# 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	.....@.....
00000020	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	..;.!.^!;.L^!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 54	ode....\$......T
00000080	7D 6C 42 10 1C 02 11 10 1C 02 11 10 1C 02 11 6B	}IB.....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 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	.....
00000030	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	..;.!.^!;.L^!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	mode....\$......
00000080	54 7D 6C 42 10 1C 02 11 10 1C 02 11 10 1C 02 11	T}IB.....


- 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PPER

MD5 Hash: 918f76b341b40af346ae7a1358548799



証明書

全般 | 詳細 | 証明のパス

証明のパス(P)

- VeriSign Class 3 Public Primary Certification Authority (PCA3 G1 SHA1)
- VeriSign Class 3 Code Signing 2009-2 CA
- Bit9, Inc

証明書

全般 | 詳細 | 証明のパス

表示(S): <すべて>

フィールド	値
発行者	VeriSign Class 3 Code Signing 2009-2 CA, Terr...
有効期間の開始	2010年05月25日 09:00:00
有効期間の終了	2013年05月25日 08:59:59
サブジェクト	Bit9, Inc, Digital ID Class 3 - Microsoft Softwar
公開キー	RSA (1024 Bits)
基本制限	Subject Type=End Entity, Path Length Constrai
CRL 配布ポイント	[1]CRL Distribution Point: Distribution Point No...

CN = Bit9, Inc  
OU = Digital ID Class 3 - Microsoft Software Validation v2  
O = Bit9, Inc  
L = Waltham  
S = Massachusetts  
C = US

Deep PandaのRAT

MD5 Hash: 46db73375f05f09ac78ec3d940f3e61a



証明書

全般 | 詳細 | 証明のパス

証明のパス(P)

- VeriSign
- VeriSign Class 3 Code Signing 2010 CA
- Adobe Systems Incorporated

証明書

全般 | 詳細 | 証明のパス

表示(S): <すべて>

フィールド	値
発行者	VeriSign Class 3 Code Signing 2010 CA, Ter
有効期間の開始	2010年12月15日 09:00:00
有効期間の終了	2012年12月15日 08:59:59
サブジェクト	Adobe Systems Incorporated, Digital ID Clas
公開キー	RSA (1024 Bits)
基本制限	Subject Type=End Entity, Path Length Const
CRL 配布ポイント	[1]CRL Distribution Point: Distribution Point

CN = Adobe Systems Incorporated  
OU = Digital ID Class 3 - Microsoft Software Validation v2  
OU = Information Systems  
O = Adobe Systems Incorporated  
L = San Jose  
S = California  
C = US

# XOR暗号されたマルウェア

Stirling - 5aaa057d3447a214e729276563d2f922\_xored32

ファイル(E) 編集(E) 検索・移動(S) 設定(O) ウィンドウ(W) ヘルプ(H)

5aaa057d3447a214e729276563d2f922

RESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0F0E0	8C	32	32	32	32	32	32	18	88	32	32	76	88	32	32	32	222222..22v.222
0F0F0	32	32	32	22	88	32	32	32	32	32	06	32	71	5E	5D	5D	222".222222.2q^]
0F100	41	57	7A	53	5C	56	5F	57	29	96	31	65	40	5F	46	57	AWzSYV^W2.1e@[FW
0F110	74	5													5B	5E	t[~W2a2q@WSFWt[^
0F120	57	7													5D	47	Ws2g1a[HW]T^WA]G
0F130	40	5													30	7E	@QW22d1a^WwB2W0^
0F140	5D	5													30	7E	]QY^WA]G@QW22e0~
0F150	5D	5													32	74	]SV^WA]G@QW2242t
0F160	5B	5													33	75	[YV^WA]G@QW22M3u
0F170	57	46	7F	5D	56	47	5E	57	7A	53	5C	56	5E	57	73	32	WF. ]VG^WzSYV^W2
0F180	32	DB	33	75	57	46	64	57	40	41	5B	5D	5C	77	4A	73	2p3uWFdW0A[ ]#wJs
0F190	32	8B	32	77	4A	5B	46	62	40	5D	51	57	41	41	32	4F	2.2wJ[Fb@]QWAA20
0F1A0	33	75	57	46	7F	5D	56	47	5E	57	7A	5B	5E	57	7C	53	3uWF. ]VG^Wt[ ^W]S
0F1B0	5F	57	73	32	32	79	77	60	7C	77	7E	01	00	1C	56	5E	_Ws22yw`lw...V^
0F1C0	5E	32	32	EC	32	77	5C	47	5F	65	5B	5C	56	5D	45	41	^22.2wYGe[ YV]EA
0F1D0	32	67	61	77	60	01	00	1C	56	5E	5E	32	32	F6	32	61	2gaw`...V^22.2a
0F1E0	7A	75	57	46	61	42	57	51	5B	53	5E	74	5D	5E	56	57	zuWfFaBWQ[S^t]^VW
0F1F0	40	62	53	46	5A	73	32	3B	33	61	5A	57	5E	5E	77	4A	@bSFZs2:3aZW^wJ
0F200	57	51	47	46	57	77	4A	73	32	61	7A	77	7E	7E	01	00	WQGFwWJs2azw~..
0F210	1C	56	5E	5E	32	22	33	75	57	46	71	5D	5F	5F	53	5C	.V^2~3uWFq]_S\$Y
0F220	56	7E	5B	5C	57	73	32	24	30	7A	57	53	42	74	40	57	V^[YWs2\$0zWSBt@W
0F230	57	32	32	22	30	7A	57	53	42	73	5E	5E	5D	51	32	91	W22~0zWSBs^~]Q2.
0F240	33	75	57	46	62	40	5D	51	57	41	41	7A	57	53	42	32	3uWfFb@]QWAAzWSB2
0F250	32	AA	32	77	5C	46	57	40	71	40	5B	46	5B	51	53	5E	2z2wYFW@q@[F]QS^
0F260	61	57	51	46	5B	5D	5C	32	32	63	30	7E	57	53	44	57	aWQF[ ]Y22c0^WSDW
0F270	71	40	5B	46	5B	51	53	5E	61	57	51	46	5B	5D	5C	32	q@[F]QS^aWQF[ ]Y2
0F280	32	6C	31	66	57	40	5F	5B	5C	53	46	57	62	40	5D	51	211fW@_ [YSFw@]Q
0F290	57	41	41	32	32	70	33	75	57	46	71	47	40	40	57	5C	WAA22p3uWfFqG@WY
0F2A0	46	62	40	5D	51	57	41	41	32	5C	31	67	5C	5A	53	5C	Fb@]QWAA2Y1gYZSY
0F2B0	56	5E	57	56	77	4A	51	57	42	46	5B	5D	5C	74	5B	5E	V^WwJQWBF[ ]Yt[^
0F2C0	46	57	40	32	32	78	31	61	57	46	67	5C	5A	53	5C	56	FW@22x1aWfFgYZSYV
0F2D0	5E	57	56	77	4A	51	57	42	46	5B	5D	5C	74	5B	5E	46	^WwJQWBF[ ]Yt[^

暗号化された元の状態

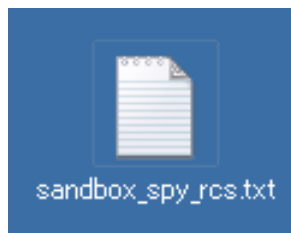
5aaa057d3447a214e729276563d2f922\_xored32

RESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0F0E0	BE	00	00	00	00	00	00	2A	BA	00	00	44	BA	00	00	00	t.....*..D3...
0F0F0	00	00	00	10	BA	00	00	00	00	00	00	34	00	43	6C	6F	....3.....4.Clo
0F100	73	65	48	61	6F	6A	6C	65	00	AA	03	57	72	69	74	65	seHandle...Write
0F110	46	6													69	6C	File.S.CreateFil
0F120	65	4													6F	75	eA.U.SizeofResou
0F130	72	6													02	4C	rce..V.Sleep.eL
0F140	6F	6													02	4C	ockResource...W.L
0F150	6F	6													00	46	oadResource....F
0F160	69	6													01	47	indResourceA...G
0F170	65	74	4D	6F	64	75	6C	65	48	61	6E	64	6C	65	41	00	etModuleHandleA.
0F180	00	E9	01	47	65	74	56	65	72	73	69	6F	6E	45	78	41	...GetVersionExA
0F190	00	B9	00	45	78	69	74	50	72	6F	63	65	73	00	7D	00	.f.ExitProcess.]
0F1A0	01	47	65	74	4D	6F	64	75	6C	65	46	69	6C	65	4E	61	.GetModuleFileNa
0F1B0	6D	65	41	00	00	4B	45	52	4E	45	4C	33	32	2E	64	6C	meA..KERNEL32.dl
0F1C0	6C	00	00	DE	00	45	6E	75	6D	57	69	6E	64	6F	77	73	l...EnumWindows
0F1D0	00	55	53	45	52	33	32	2E	64	6C	6C	00	00	C4	00	53	.USER32.dll...t.S
0F1E0	48	47	65	74	53	70	65	63	69	61	6C	46	6F	6C	64	65	HGetSpecialFolde
0F1F0	72	50	61	74	68	41	00	09	01	53	68	65	6C	6C	45	78	rPathA...ShellEx
0F200	65	63	75	74	65	45	78	41	00	53	48	45	4C	4C	33	32	ecuteExA.SHELL32
0F210	2E	64	6C	6C	00	10	01	47	65	74	43	6F	6D	6D	61	6E	.dll...GetComman
0F220	64	4C	69	6E	65	41	00	16	02	48	65	61	70	46	72	65	dLineA...HeapFre
0F230	65	00	00	10	02	48	65	61	70	41	6C	6C	6F	63	00	A3	e...HeapAlloc.]
0F240	01	47	65	74	50	72	6F	63	65	73	73	48	65	61	70	00	...GetProcessHeap.
0F250	00	98	00	45	6E	74	65	72	43	72	69	74	69	63	61	6C	...EnterCritical
0F260	53	65	63	74	69	6F	6E	00	00	51	02	4C	65	61	76	65	Section..Q.Leave
0F270	43	72	69	74	69	63	61	6C	53	65	63	74	69	6F	6E	00	CriticalSection.
0F280	00	5E	03	54	65	72	6D	69	6E	61	74	65	50	72	6F	63	.^.TerminateProc
0F290	65	73	73	00	42	01	47	65	74	43	75	72	72	65	6E	00	ess...B.GetCurrent
0F2A0	74	50	72	6F	63	65	73	73	00	6E	03	55	6E	68	61	6E	tProcess.n.Unhan
0F2B0	64	6C	65	64	45	78	63	65	70	74	69	6F	6E	46	69	6C	dledExceptionFil
0F2C0	74	65	72	00	00	4A	03	53	65	74	55	6E	68	61	6E	64	ter...J.SetUnhand
0F2D0	6C	65	64	45	78	63	65	70	74	69	6F	6E	46	69	6C	74	ledExceptionFil

復号化した状態

0x0000EB4F | 上書 5953 | CAPS KANA

# 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=X  
XX&MouseButtons=X&PrimaryMonitorSize=XXXXXXX&UserDomainNam  
e=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>



atmarkit  
ITエキスパートのための問題解決メディア

開発 運用構築 設計

注目のテーマ ▾ IaaS選定 **Now** DB統合 ECM データ分析 統合インフラ Hybrid Cloud DevOps タブレット

@IT > Security & Trust > マルウェアの視点で見るサンドボックス: 合法マルウェアで実感...

2014年04月18日 18時00分 更新

### マルウェアの視点で見るサンドボックス:

## 合法マルウェアで実感「リアルとサンドボックスの違い」(1/3)

標的型攻撃対策の手法として、「サンドボックス」が注目を集めています。しかし攻撃者もすでに「サンドボックス対策」を進めています。合法的に作成したマルウェアのアプリ「ShinoBOT」を通じて分かったサンドボックス対策のヒントを、制作者本人が解説します。

[凌 翔太 (マクニカネットワークス), @IT]

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](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](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](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 "netddesrv.conf" configuration file which we believe contains the target name and the beacon address to use.

Filename	<u>netddesrv.exe</u>
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: Copyright LegalTrademarks: OriginalFilename: <b>msrv.exe</b> PrivateBuild: ProductName: NetDDESrv ProductVersion: 1, 0, 0, 1 SpecialBuild: Child Type: VarFileInfo Translation: 1033/1200

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。

コードサイン証明書を盗まれる。

← → ↻ <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	...YAZ+Ya'...YAZDYA
00000010	22	84	DD	C0	8B	85	DD	C0	FA	85	BC	C0	E3	85	AF	C0	"..YA<...YAG...AA...A
00000020	FE	85	A5	C0	C8	85	AD	C0	F6	85	AE	C0	E4	85	AA	C0	p...YAE...-Aö...AA...*A
00000030	F8	85	AF	C0													ø...A

Raw HEX view of the

NetDDESrv beacon data

デコード後に見られる特徴的なString

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	µ
00000020	69	00	78	00	5F	00	70	00	61	00	73	00	73	00	77	00	ix
00000030	6F	00	72	00													or

Decoded HEX view of the NetDDESrv beacon data

XOR

# 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]
0020  [redacted]
0030  [redacted]
0040  [redacted]
0050  [redacted]
0060  [redacted]
```

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	09	04	00	00	....1.. .....
00000010	B5	01	00	00	1E	00	00	00	6D	00	61	00	74	00	72	00	<u>μ.....m.a.t.r.</u>
00000020	69	00	78	00	5F	00	70	00	61	00	73	00	73	00	77	00	<u>i.x. .p.a.s.s.w.</u>
00000030	6F	00	72	00	64	00											<u>o.r.d.</u>

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
```

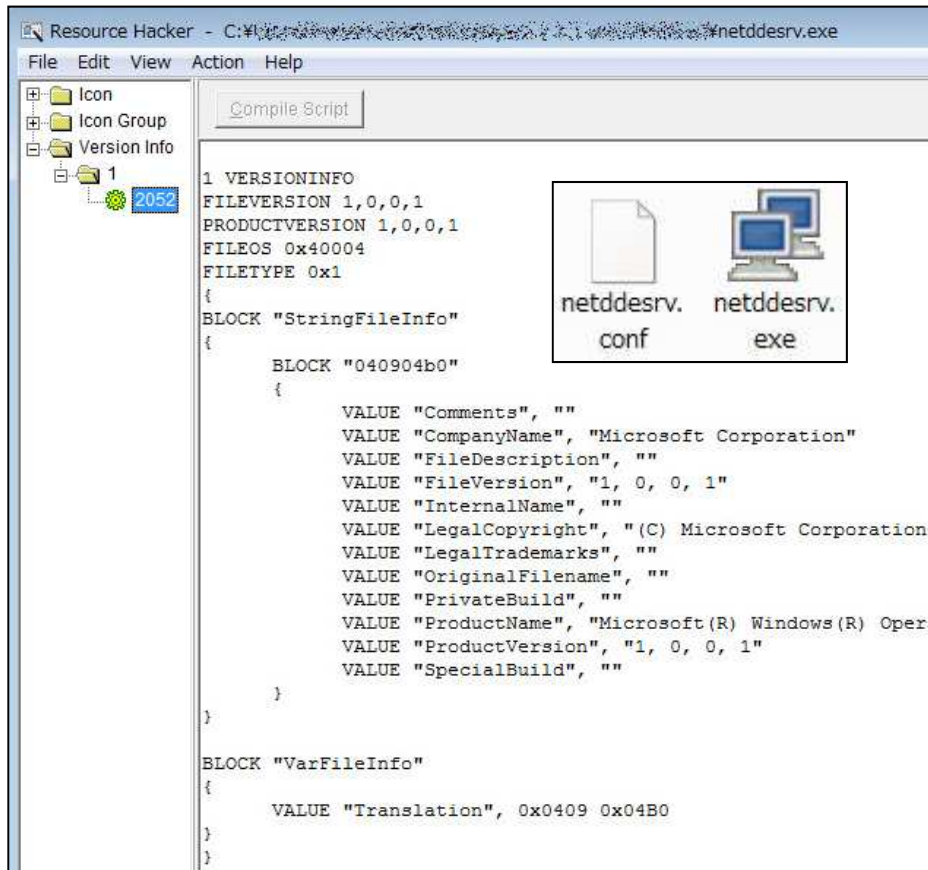
```
0000
0010
0020 01 bb 19 bc d4 d1 df 92 4b 9a 00 10 54 bytes
0030 01 00 e1 95 00 00 bc a8 5a 23 8d ab 48 03 b9 a8
0040 5a 23 ad ac 5a 23 18 ab 5a 23 a2 a8 5a 23 d1 a8
0050 3b 23 c8 a8 28 23 d5 a8 22 23 e3 a8 2a 23 dd a8
0060 29 23 cf a8 2d 23 d3 a8 28 23 d8 a8
```

XOR

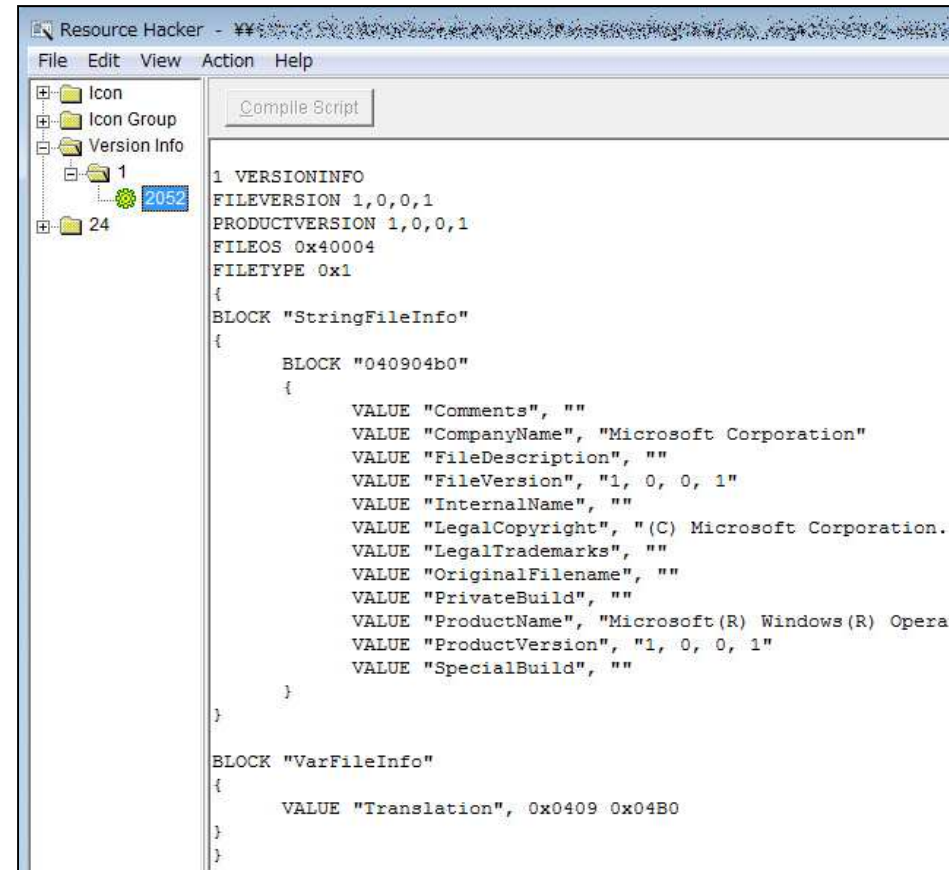
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	00	00	00	31	03	12	20	05	00	00	00	11	04	00	00	....1.. .....
00000010	A4	03	00	00	1E	00	00	00	6D	00	61	00	74	00	72	00	x..... <u>m.a.t.r.</u>
00000020	69	00	78	00	5F	00	70	00	61	00	73	00	73	00	77	00	<u>i.x. .p.a.s.s.w.</u>
00000030	6F	00	72	00	64	00											<u>o.r.d.</u>

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)

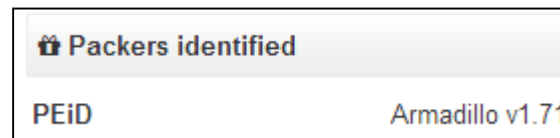
# 検体の類似性



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

Offset	Hex	ASCII
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 fa 02 50 18	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 n.Q.=O.R

本家のGh0st RATでは、"Gh0st"という5 bytesが入る。

**Xfocus Team**  
From the Internet. For the Internet.

gh0st\_src.rar

提交时间: 2008-03-02 更新时间: 2008-05-07  
提交用户: cooldiyer  
工具分类: 扫描器  
运行平台: Windows  
工具大小: 1087762 Bytes  
文件MD5: 5c6b2a4b4311244fb91f48c4215775df  
工具来源: cooldiyer

Gh0st RAT  
C.Rufus Security Team  
http://www.wolfexp.net  
控制端采用IOCP模型, 数据传输采用zlib压缩方式, 稳定快速, 上线数量无上限, 可同时控制上万台主机.  
控制端自动检测CPU使用率调整自己的工作线程, 稳定高效  
宿主为svchost以系统服务启动, 有远程守护线程, 上线间隔为两分钟.  
心跳包机制防止意外掉线.  
支持HTTP和DNS上线两种方式.  
自动恢复SSDT(这功能干什么, 大家都知道, 免杀自己做吧)安装本程序  
控制端237K, 还原逼真的界面, 生成的服务端无壳, 111 K, 可安装多  
其它细节方面的功能大家自己去发现吧  
功能:  
文件管理 完全仿Radmin所写, 文件、文件夹批量上  
屏幕监视 此模块全用汇编编写, 传输速度快, 控制屏幕, 发送Ctrl+A  
键盘记录 可记录中英文信息, 离线记录(记录上限50M)功能

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

Transmission Control Protocol, Src Port: 49182 (49182), Dst Port: https (443), Seq: 250, Ack: 1, Len: 1045  
[2 Reassembled TCP Segments (1294 bytes): #13(249), #14(1045)]  
Hypertext Transfer Protocol  
POST /info.asp HTTP/1.1\r\nContent-Type: application/x-www-form-urlencoded\r\nAgtid: 307e823e08x\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; win32)\r\nHost: 180.150.228.102:443\r\nContent-Length: 1045\r\nConnection: Keep-Alive\r\nCache-Control: no-cache\r\n\r\n[Full] request URI: http://180.150.228.102:443/info.asp  
[HTTP request 1/1]  
Line-based text data: application/x-www-form-urlencoded  
[truncated] 5cac450a08x&56FMD2M0SFN1UN7NGFVIYPlcqgP2bFN1UcrQMgxoJyAwfDWSJ/nush5rjeuce7HMJ4UHbasPiXBGyC69i

C2サーバへのBeaconに見られる特徴的なヘッダ

# Whois History

## DOMAINTOOLS Whois History

Domain: **blankchair.com**

Record Date: 2013-04-02  
Registrar: XIN NET TECHNOLOGY CORPORATION  
Server: whois.paycenter.com.cn  
Created: 2011-04-22  
Updated: 2012-04-13  
Expires: 2014-04-22

Reverse Whois:  
**654@123.com** 🔍

Domain Name : blankchair.com  
PunyCode : blankchair.com  
Creation Date : 2011-04-22 15:46:56  
Updated Date : 2012-04-13 23:38:35  
Expiration Date : 2014-04-22 15:46:56

Registrant:  
**Organization : dan qiao**  
**Name : dan qiao**  
Address : USA California  
City : jiazhou  
Province/State : Others  
Country : CN  
Postal Code : 464655

Administrative Contact:  
Name : dan qiao  
Organization : dan qiao  
Address : USA California  
City : jiazhou  
Province/State : Others  
Country : jiazhou  
**Postal Code : 464655**  
**Phone Number : 86-010-87654321**  
Fax : 86-010-87654321  
Email : 654@123.com

Operation DeputyDog

Domain: **yahooeast.net**

Record Date: 2013-03-25  
Registrar: XIN NET TECHNOLOGY CORPORATION  
Server: whois.paycenter.com.cn  
Created: 2011-04-22  
Updated: 2012-04-13  
Expires: 2013-04-22

Reverse Whois:  
**654@123.com** 🔍

Domain Name : yahooeast.net  
PunyCode : yahooeast.net  
Creation Date : 2011-04-22 15:34:18  
Updated Date : 2012-04-13 14:03:03  
Expiration Date : 2013-04-22 15:34:18

Registrant:  
**Organization : dan qiao**  
**Name : dan qiao**  
Address : USA California  
City : California  
Province/State : Others  
Country : CN  
Postal Code : 464655

Administrative Contact:  
Name : dan qiao  
Organization : dan qiao  
Address : USA California  
City : California  
Province/State : Others  
Country : California  
**Postal Code : 464655**  
**Phone Number : 86-010-87654321**  
Fax : 86-010-87654321  
Email : 654@123.com

66.153.86.14  
downloadmp3server.servemp3.com  
Bit9

# Reverse Whois



## Reverse Whois - Refine Your Search

Find any domain(s) with a Whois record that matches these criteria:

[How does this work?](#)

Whois Record

[Expand Your Search](#)

[Narrow Your Search](#)

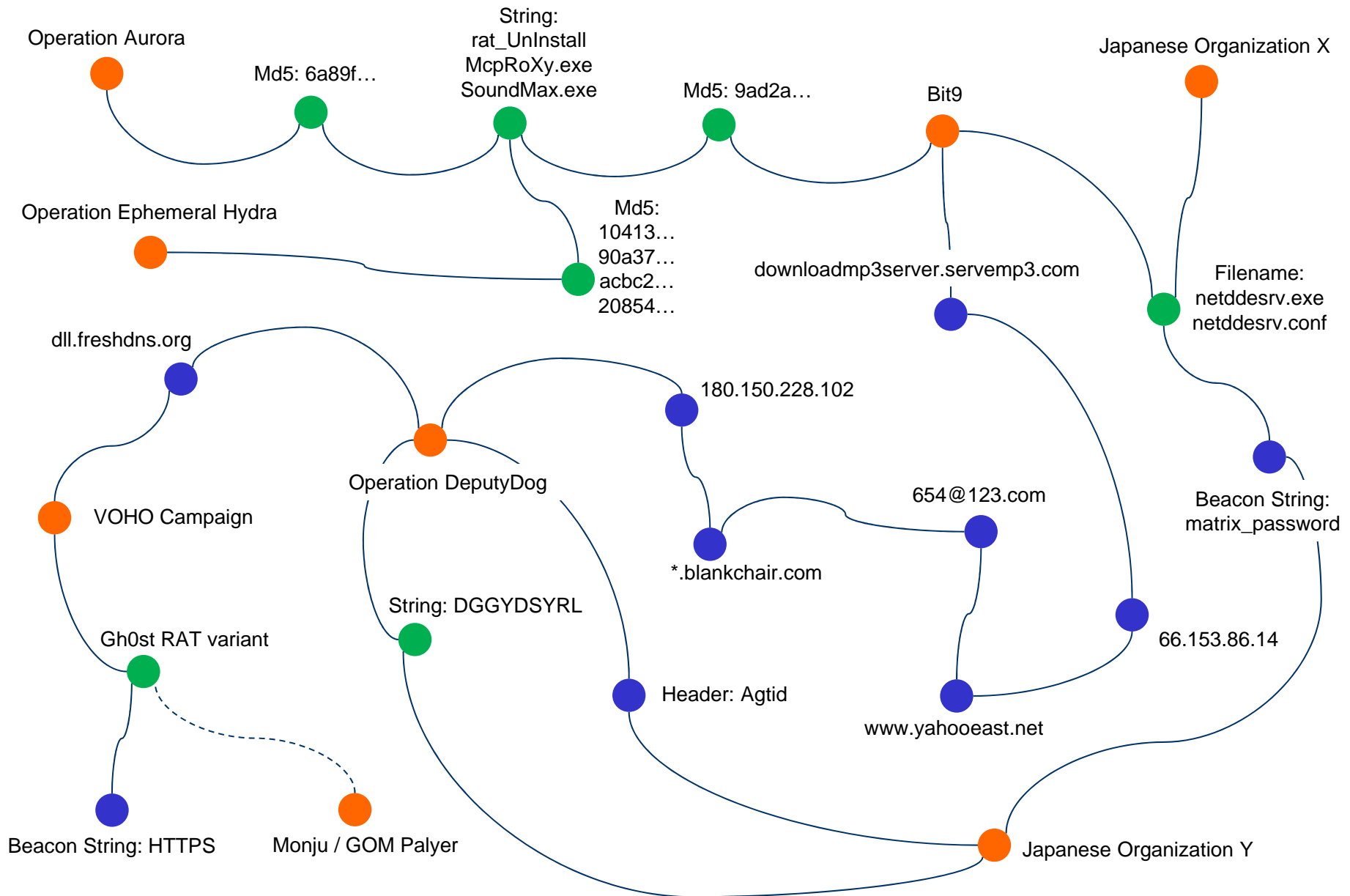
**3** domains

Domain Name	Create Date	Registrar
blankchair.com	2011-04-22	XIN NET TECHNOLOGY CORPORATION
x...8.com.cn ← これもAurora Pandaなんだろうか。。		-
yahooeast.net	2013-09-17	GODADDY.COM, LLC





# 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、

Stream Content

```
GET /update/bookmark.png HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://dol.ns01.us:8081/update/index.php
Accept-Encoding: gzip, deflate
User-Agent: 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)
Host: dol.ns01.us:8081
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 01 May 2013 05:47:22 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
Last-Modified: Mon, 29 Apr 2013 14:11:00 GMT
ETag: "2000000039d7-19000-4db80744d9996"
Accept-Ranges: bytes
Content-Length: 102400
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/png

.Z. ....@.....!..L!This
program cannot be run in DOS mode.
```

実行ファイルのマジックナンバーMZ(0x4D5A)が変更されている。

Stream Content

```
POST /web/js.php HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.sem.dol.gov/
Accept-Language: en-US
User-Agent: 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)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: dol.ns01.us:8081
Content-Length: 236
Connection: Keep-Alive
Cache-Control: no-cache

ck=Url%3Ahttp%3A%2F%2Fwww.sem.dol.gov%2FxxxooxxxooReferer%3AxxxooxxxooCookies%3AWT_FPC%253DId%253D%253D1367362044506&vul=No+Flash%21%2CAdobe+Reader%2CJava+Version+is%3A1.7.0%2CHTTP/1.1

200 OK
Date: Wed, 01 May 2013 05:47:23 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 11
```

JavaScriptによる環境チェックの結果を攻撃者のサーバへ送信。

reporting that this attack has indicators of compromise that link to the DeepPanda Chinese APT group. This compromise shows that watering hole attacks continue to be employed by advanced threat using exploits customized to their target profile. The malicious website re-direct exploits an older vulnerability in Internet Explorer and Windows XP machines that fit the typical configuration of enterprise user machines. Invincea users are protected against this attack as they are against other web-based drive-by and spear-phishing attacks.

Please contact Invincea today to schedule a demo.

Deep Pandaによる攻撃と見られている。

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



# 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

改ざんされた正規サイトの多くでWordPressが使われていた。



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。

[redacted]wp-includes/pomo/dx.php

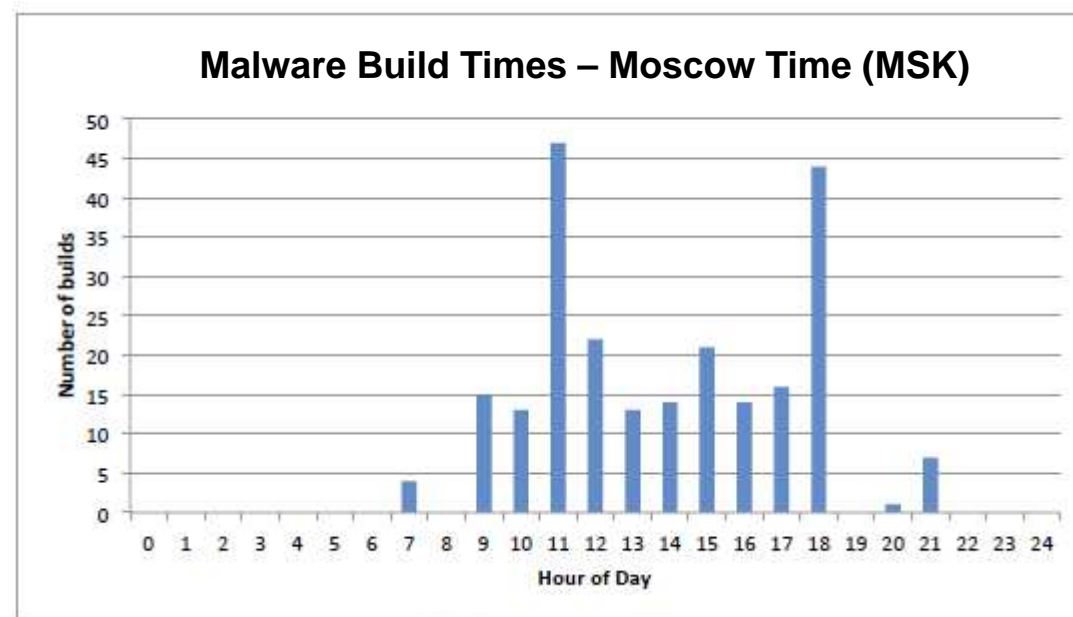
- [redacted].com/tareas/include/\_php.php
- [redacted].ru/includes/phpmailer/source.php
- [redacted].com/catalog/install/source.php
- [redacted].com/cna/[redacted]/cna\_source.php
- [redacted].ru/modules/mod\_search/idx.php
- [redacted].com/res/code/res.php
- [\[redacted\].co.jp/inc/user//mysql\\_s.php](#)
- [\[redacted\].co.jp/inc/user/mysql\\_s.php](#)
- [redacted].com/chief-cooker/tiny\_mce/plugins/searchreplace/edit.php
- [redacted].org/modules/mod\_search/search.php



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	GIJEL.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



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  
%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/>

## 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)	Type	Reference
Author: Mandiant	family	CALENDAR
GUID: 6bd24113-2922-4d25-b490-f727f47ba948	threatgroup	APT
Created: 2013-02-10 06:11:53Z	family	APT1
Modified: 2013-02-10 13:00:00Z	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

```

<!-- This collection of observables were observed as part of the widespread "Iran-Oil" (among many other names used) attack campaign in March 2012 -->
<cybox:Observable id="example:Observable-1a937ec2-90ab-4e0e-a37c-db9b2e66a58e">
  <!-- Receive "Iran-Oil" attack campaign email message -->
  <cybox:Event>
    <cybox:Type xsi:type="cyboxVocabs:EventTypeVocab-1.0.1">Email Ops</cybox:Type>
    <cybox:Description>Receive "Iran-Oil" attack campaign email message.</cybox:Description>
    <cybox:Actions>
      <cybox:Action>
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Receive</cybox:Type>
        <cybox:Associated_Objects>
          <cybox:Associated_Object id="example:Object-51359587-f201-4383-b032-5a64522fcd7d">
            <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
              <EmailMessageObj:Header>
                <EmailMessageObj:To>
                  <EmailMessageObj:Recipient category="e-mail">
                    <AddrObj:Address_Value>william.abnett@gmail.com</AddrObj:Address_Value>
                  </EmailMessageObj:Recipient>
                </EmailMessageObj:To>
                <EmailMessageObj:From category="e-mail">
                  <AddrObj:Address_Value>wmorrison89@gmail.com</AddrObj:Address_Value>
                </EmailMessageObj:From>
                <EmailMessageObj:Subject>Iran's Oil and Nuclear Situation</EmailMessageObj:Subject>
                <EmailMessageObj:Date datatype="dateTime">2012-03-02T07:42:24Z</EmailMessageObj:Date>
              </EmailMessageObj:Header>
              <EmailMessageObj:Raw_Header datatype="string">
                Return-Path: <mailto:wmorrison89@gmail.com>&#038;#038;
              </EmailMessageObj:Raw_Header>
            </cybox:Properties>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>
  
```

```

Received-SPF: pass (google.com: domain of wmorrison89@gmail.com designates 10.236.185.4 as permitted sender) client-ip=10.236.185.4;
Authentication-Results: mr.google.com; spf=pass (google.com: domain of wmorrison89@gmail.com designates 10.236.185.4 as permitted sender);
smtp.mail=wmorrison89@gmail.com; dkim=pass header.i=wmorrison89@gmail.com
Received: from mr.google.com ([10.236.185.4]) by 10.236.185.4 with SMTP id t4mr5301660yhm.129.1330692273662 (num_hops = 1);
04:44:33 -0800 (PST)
MIME-Version: 1.0
Received: by 10.236.185.4 with SMTP id t4mr4236541yhm.Fri,
02 Mar 2012 04:44:25 -0800 (PST)
Received: by 10.147.35.14 with HTTP: Fri, 2 Mar 2012
In-Reply-To:
<mailto:CADY6HTa:imaamtYvyT-nLz6reztnics-617wL4bt9YBOGu+
  
```

```

<cybox:Observable id="example:Observable-210f18f3-3874-4f9a-861d-71b328be90c6">
  <!-- Create Iran-Oil .exe Trojan file -->
  <cybox:Event>
    <cybox:Type xsi:type="cyboxVocabs:EventTypeVocab-1.0.1">File Ops (CRUD)</cybox:Type>
    <cybox:Description>Create Iran-Oil .exe Trojan file.</cybox:Description>
    <cybox:Actions>
      <cybox:Action>
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Create</cybox:Type>
        <cybox:Associated_Objects>
          <cybox:Associated_Object idref="example:Object-8b463e0d-cc16-4036-950e-5eeb09bc51aa">
            <cybox:Association_Type xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-1.0">Initiating</cybox:Association_Type>
          </cybox:Associated_Object>
          <cybox:Associated_Object id="example:Object-b7e0bc39-f519-4878-8fb0-5902554efe1c">
            <cybox:Description>
              The file (us.exe MD5: FD1BE09E499E8E380424B3835FC973A8<#038;#038;
              4861440 bytes) is created in the logged in user %Temp%<#038;#038;
              directory. The size of the embedded file is 22.5 KB (23040<#038;#038;
              bytes) and the size of the created us.exe is 4.63MB. It is an<#038;#038;
              odd discrepancy until you look at the file and it looks like the<#038;#038;
              code is repeated over and over - 211 times. The file resource<#038;#038;
              section indicates the file is meant to look like a java updater,<#038;#038;
              which is always larger than 22.5KB and that would explain all<#038;#038;
              this padding, which is done at the time when the file is being<#038;#038;
              written to the disk.
            </cybox:Description>
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:File_Name>us.exe</FileObj:File_Name>
              <FileObj:File_Path>%Temp%\FileObj:File_Path</FileObj:File_Path>
              <FileObj:Size_In_Bytes>4861440</FileObj:Size_In_Bytes>
              <FileObj:Hashes>
                <cyboxCommon:Hash>
                  <cyboxCommon:Type>MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value condition="Equals">FD1BE09E499E8E380424B3835FC973A8</cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>
  
```

<http://cybox.mitre.org/>

<http://www.ipa.go.jp/security/vuln/Cybox.html>



- 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。

Strong



Weak

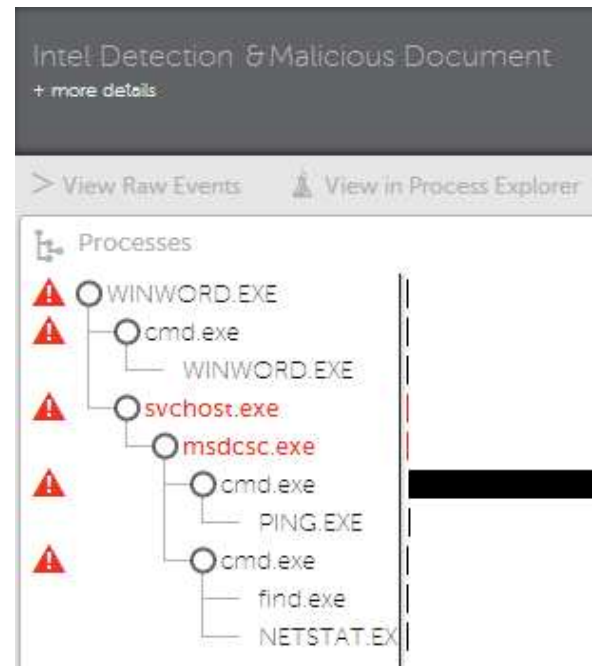
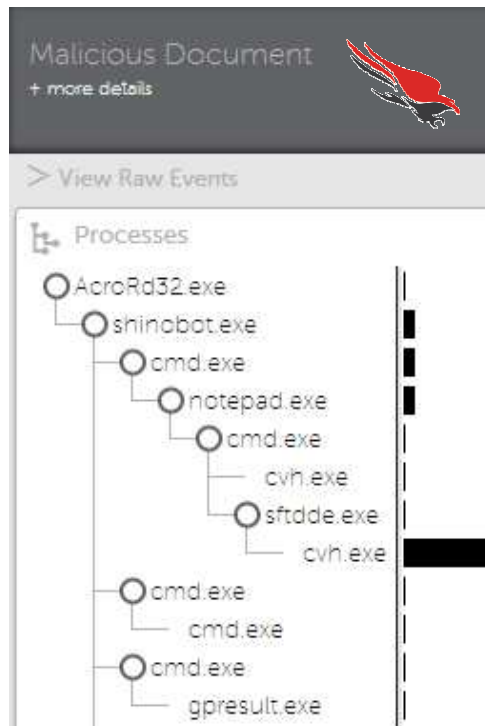
# Host Behavioral Indicator (ホスト内でのマルウェアの挙動)

- 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

<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

- 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！

