研究用データセット「動的活動観測 2017」

寺田真敏[†1]　佐藤隆行[†1]　青木　翔[†1]
亀川　慧[†2]　清水　努[†2]　萩原健太[†2]

概要：マルウェア検体の解析では，指令サーバ接続，情報窃取，バックドアなどの機能の存在や挙動把握に重点が置かれ，攻撃者の行動という視点で把握や解析することはなかった．しかし，組織内ネットワークへの侵害活動においては，攻撃者の存在，攻撃者のアトリビューションを意識する必要がある．本稿では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測とその研究用データセット「動的活動観測 2017 (BOS_2017)」について報告する．

キーワード：動的活動観測，マルウェア，指令サーバ

Overview of Research Data Set "Behavior Observable System 2017"

Masato Terada[†1], Takayuki Sato[†1], Sho Aoki[†1],
Satoshi Kamekawa[†2] , Tsutomu Shimizu[†2] and Kenta Hagihara[†2]

Abstract: Under the analysis of malware, mainly it focuses on the functions and behaviors of malware itself such as C&C server connection, information leak, backdoor and etc. The analysis of malware does not include the viewpoint of actions of threat actors. But under the targeted attack such as APT, we should focus on the actions of threat actor and attribution, too. In this paper, firstly we will describe the overview of our research data set "BOS_2017" for the countermeasures of targeted attack age. Secondly, we will introduce the typical case of targeted attack in BOS_2017.

Keywords: Behavior Observable System, Malware, C2 server

1. はじめに

マルウェアを用いたサイバー攻撃は技術を継承しつつ，活動形態を大きく変化させながら進化している(図 1)．1990 年代中盤，数多くのパケットレベルの DoS 攻撃を可能とする脆弱性が発見された(発見の世代)．1999 年の後半に入ると，パケットレベルの DoS 攻撃は，DoS 攻撃用エージェントを分散配置し，それらのエージェントを制御しながら，攻撃を仕掛ける DDoS 攻撃へと進化した(ツール世代)．その後，2000 年代の『電子メール型ワーム』『ネットワーク型ワーム』という自己を複製しながら伝播する技術は，DoS 攻撃用エージェントの配備機能となり(ワーム世代)，マルウェアの革新技術である『ボットネット』につながっている(ボット世代)．標的型世代では，ボット世代の技術をベースに，遠隔操作ツール(RAT: Remote Access Trojan/Remote Administration Tool)を主体とした組織内ネットワークへの侵害活動が，APT(Advanced Persistent Threat)という名称で広く知れ渡るようになった(標的型世代)．2010 年代中盤以降は，IoT を対象としたボットの台頭(IoT ボット世代)，電子メールで流布し始めたファイル暗号型のランサムウェアは，2017 年 5 月にワーム機能を搭載した WannaCry として登場したことで(ランサムウェア世代)，「特定組織を対象とし(標的型攻撃)，組織内ネットワークを活動基点とする(潜伏型手法の)侵害活動」の総称である APT においても，ランサムウェアを組み合わせた攻撃活動が予見される．

本研究の目的は，多様化と巧妙化するサイバー攻撃に対抗するため，攻撃者の行動観測を通してサイバー攻撃活動を分析すると共に，攻撃者のアトリビューションに着目した動的活動観測を進めることにある[1][2][3]．本稿では，2016 年に実施した電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS(Behavior Observable System)とその研究用データセット「動的活動観測 2017(BOS_2017)」について報告する．

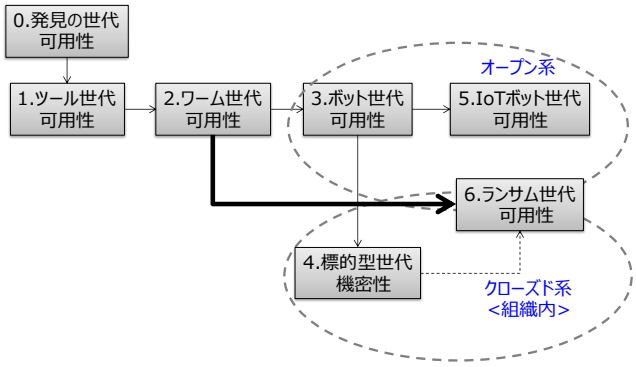

図 1：攻撃活動の変遷

†1 (株)日立製作所, Hitachi Ltd.
†2 トレンドマイクロ(株), Trend Micro Incorporated.

2. 関連研究

(1) 動的活動観測

動的活動観測のうち，遠隔操作ツールを使用し組織内ネットワークへの侵害活動を想定した観測技術については，RAT サーバの画面そのものを遠隔から観測する手法[4][5]や侵害活動を長期観測するためのサイバー攻撃誘引基盤技術[6]などの研究として進められている．その一方，攻撃者の行動観測に関する研究については，数少ないという状況にある[7].

(2) アトリビューション

サイバー攻撃の分野において，アトリビューションとは，攻撃者や攻撃仲介者の同一性や場所の特定を意味する[8]. 文献 8)では，アトリビューションのための技術として，トレースバック，モニタホストの導入，ハニーポット/ハニーネットの活用などを挙げている．文献9)では，マルウェアのメタデータ，埋め込みフォント，遠隔操作ツールの設定，攻撃者の行動パターンなどが利用できるとしている．また，脅威情報構造化記述形式 STIX(Structured Threat Information eXpression)[10]では，ソフトウェアやシステムの弱点，攻撃を検知するための事象だけではなく，攻撃者の行動や手口，サイバー攻撃に関与している人／組織など，攻撃者の存在を意識したサイバー攻撃活動の構造化を試みている．

(3) 情報活用基盤

情報活用によるサイバー攻撃対策には，高度なセキュリティ人材によって情報分析する「人手を介した連携」だけではなく，即時的な対処と人の技量に左右されない「システムを介した連携」の双方を検討する必要がある(表 1). 特に，「システムを介した連携」については，サイバー攻撃活動全般を構造化し記述する脅威情報構造化記述形式 STIX，STIX などで記述した情報を交換するための検知指標情報自動交換手順 TAXII(Trusted Automated eXchange of Indicator Information)[11]を実装した情報活用基盤が普及している．米国では，サイバーセキュリティ法(Cybersecurity Act of 2015)の成立に伴い，2016 年 3 月，官民連携の一環の取り組みとして，STIX，TAXII を利用し観測事象の中から検知に有効なサイバー攻撃を特徴付ける指標を交換するための AIS(Automated Indicator Sharing)[12]が稼働し始めている．国内では，ICT-ISAC Japan が STIX，TAXII を利用した情報活用基盤の運用を試行している．

表 1：情報活用基盤の分類

	地震の場合	サイバー攻撃対策の場合
システムを介した連携(機械処理系を加味した情報網，machine readable 型)	電子メールで配信される地震速報	STIX/TAXII などを用いたシステム化(例：AIS など)
人手を介した連携(人間系の情報網，human readable 型)	関係組織が発表する会見	電子メール，SNS などを用いた連携

3. 研究用データセット BOS_2017

本章では，研究用データセット「動的活動観測 2017 (BOS_2017)」の概要について述べる．

3.1 動的活動観測

(1) 目的

動的活動観測 BOS の目的は，攻撃者のアトリビューションの一部として，マルウェアの挙動に加えて，どのような操作をしたのか，どのようなファイルにアクセスしたのかなど攻撃者の行動と組合せていくことで，攻撃者行動視点で脅威の特徴付けを試みることにある．

(2) 観測環境

動的活動観測 BOS では，組織内ネットワーク自身を模擬した観測環境を構築している(図 2). この環境は，組織内ネットワークのパソコンにおいてマルウェア感染が発生した以降を対象に，実インターネット上の攻撃者が組織内ネットワークで試みるサイバー攻撃活動を観測するシステムとなっている．クライアントは，標的型攻撃メールに添付されたマルウェア検体を実行するパソコンであり，プロキシ経由／プロキシ経由なしのいずれかの形態で，実インターネットへのアクセスが可能である．

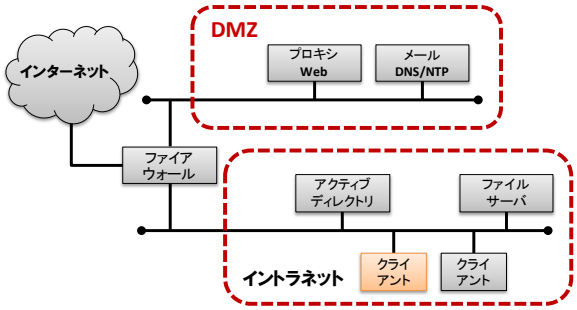

図 2：動的活動観測環境の概要図

3.2 観測事例

本節では，2016 年に実施した電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS とその研究用データセット「動的活動観測 2017 (BOS_2017)」について述べる(表 2).

BOS_2017 では，BOS_2016 と同様，表 3 に示す進行度という動的活動観測における侵害活動の進み具合の区分を設け，標的型攻撃の段階に応じた研究用データセットとなるよう工夫をしている．これにより，検体が動作し，指令サーバ(以降，C2 サーバ)との通信が発生した後，動的観測環境で攻撃者による活動を観測できた事例のみ(進行度 7 以上)を研究用データセットとしてきた BOS_2014～BOS_2015 に比べてバリエーションを増やすことができている．

表 2：動的活動観測 2017(BOS_2017)の観測事例

#	観測期間		マルウェア検体名	進行度
	開始	終了		
f01	2017/01/12	2017/01/14	BKDR_ZACOM.SM	3
f02	2017/01/13	2017/01/19	BKDR_FYNLOS.SMM	2
f03	2017/01/18	2017/02/02	BKDR_CHCHES.NAK	7
f04	2017/01/20	2017/01/20	BKDR_CHCHES.NAM	2
f05	2017/01/20	2017/01/22	TROJ_INJECTOR.AUSREKT	1
f06	2017/01/24	2017/01/24	BKDR_ChChes.SM2	2
f07	2017/01/24	2017/02/06	LNK_OTORUN.YWY	6
f08	2017/02/06	2017/02/08	BKDR_ChChes.ZLDK-B	2

表 3：動的活動観測における進行度

進行度	区分		内容
1	通信発生なし		検体の実行が不可能 or マルウェアではない
2			検体実行するも，通信発生無し
3	検体が動作し，通信が発生	C2 サーバと攻撃通信成立せず	C2 サーバの名前解決不可
4			C2 サーバへ SYN パケット送信のみ
5			C2 サーバと通信成立しない (HTTP のステータスコード =403, 404, 503 など)
6		C2 サーバと攻撃通信成立	攻撃(活動/操作)観測できず.
7			攻撃(活動/操作)観測できた.
8			攻撃(活動/操作)観測でき，継続的に観測できた.

(1) **Case f03**

検体 Chches の exe 型で, 組織内ネットワークでの一連の侵害活動を観測した事例である(表 4). 攻撃者は，検体実行後 1 時間後に動的活動観測環境を来訪し，計 0.7 時間ほどの間，環境情報の取得を実施している．インストールプログラムの確認に PowerShell を使用している点に特徴がある．

(2) **Case f07**

検体 Chches の PowerShell 型で，組織内ネットワークでマルウェアが活動を開始し，C2 サーバとの TCP コネクションを確立し，HTTP のステータスコードが 200(OK)で，C2 サーバとの攻撃通信が成立したが, 攻撃者が動的活動観測環境に来訪しなかった事例である．

表 4：Case f03＜観測事象＞

Date	Time	Observable event
1/18	16:03	検体(.exe)を実行。C&Cサーバとの接続が確立。
	17:00:09	tasklist
	17:10:43	logoff /f
	17:19:40	dir C:¥Users¥
	17:28:57	dir c:¥users¥HitachiSato¥desktop¥
	17:29:34	net view /domain
	17:31:22	net view
	17:32:22	net user /domain
	17:32:46	net user HoshiKentaro /domain
	17:33:04	c:¥users¥HitachiSato¥
	17:33:16	dir c:¥users¥HitachiSato¥Documents
	17:34:07	ipconfig
	17:34:16	net use
	17:34:23	powershell "Get-ItemProperty HKLM:¥ Software¥ Microsoft¥ Windows¥ CurrentVersion¥ Uninstall¥* | Select-Object DisplayName, DisplayVersion"
	17:34:48	ping 192.168.12.8
	17:35:21	dir ¥¥192.168.12.8¥c$
	17:35:44	net group /domain
	17:36:07	net group "Domain Controller" /domain
	17:36:15	net group "Domain Controllers" /domain
	17:38:31	net group "domain admins" /domain
	17:38:52	net user
	17:39:11	net user Administrator

3.3 考察

(1) **検体 Chches について**

BOS_2017 の動的活動観測 f03，f04，f06～f08 で使用している検体 Chches は，2016 年 9 月頃から電子メールにより伝搬されており，各所からも調査レポートが公開されている(表 5)．大きく exe 型と PowerShell 型に分類され，調査レポートで報告されているハッシュ値などから，2017 年 3 月時点で，ユニークな検体として 43 検体を確認した．考察では，このうち，確認可能な 33 検体について，exe 型と PowerShell 型などの種別毎の出現傾向，バージョン番号の出現傾向，exe 型の場合には検体のコンパイル日付の分布について調査を実施した．

表 5：Chches 調査レポートで報告されているハッシュ値の件数

調査報告	ハッシュ値の件数
#1 [13]	25 件
#2 [14]	11 件
#3 [15]	25 件
#4 [16]	24 件
#5 [17]	9 件
上記以外	12 件

(a) exe 型と PowerShell 型などの種別毎の出現傾向

検体 Chches は, 大きく exe 型と PowerShell 型に分類される．図 3 に種別毎の出現時期を示す．当初は exe 型のみだったが, 2017 年 1 月から検知されにくい PowerShell 型が登場している．

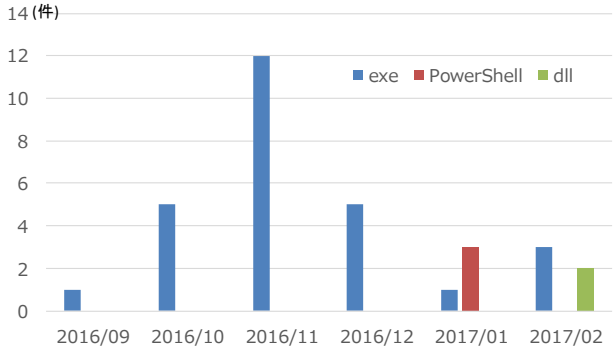

図 3：検体 Chches の種別毎の出現傾向

(b) バージョン番号の出現傾向

検体 Chches の通信にはバージョン番号が含まれており，コンパイル日付とバージョン番号には相関があることが報告されている[13]．そこで，Case#007 の観測で得たバージョン 1.6.4 を PowerShell 型のバージョンとして適用すると共に，調査報告#1[13]の結果と組み合わせることで，バージョン番号の出現傾向を推定することとした(表 6)．図 4 に示す通り，攻撃者は短期間でバージョンアップを繰り返した検体 Chches を順次使用していることがわかる．

表 6：検体 Chches のバージョン推定方法

コンパイル日付		バージョン
2016 年 10 月 31 日まで		1.0.0
2016 年 11 月 1 日～8 日		1.3.0
2016 年 11 月 9 日～19 日		1.3.2/1.4.0
2016 年 11 月 20 日以降		1.4.1
上記以外	2016 年以外	VirusTotal への投稿の初出日をコンパイル日付として推定
	PowerShell 型	1.6.4

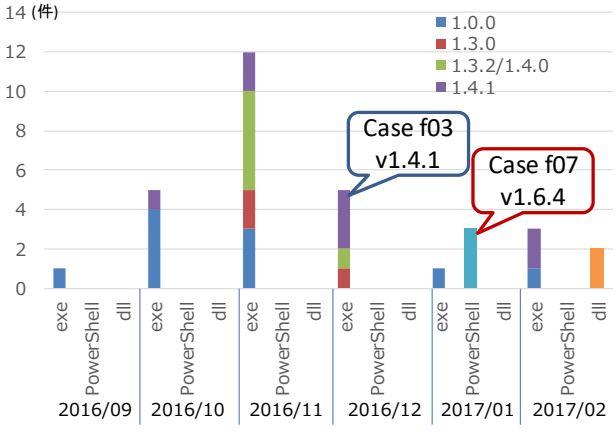

図 4：バージョン番号の出現傾向

(c) 検体のコンパイル日付の分布傾向

exe 型検体のコンパイル日付の分布を図 5 に示す．観測日時とコンパイル日付は，ほぼ同期している検体がある一方，2011 年や 2014 年のコンパイル日付のものがある．

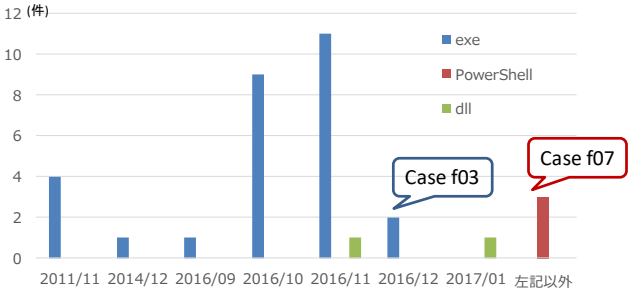

図 5：コンパイル日付の分布

(2) BOS_2016 以前の観測事象との比較

調査レポート[18]によれば，ChChes と 2015 年に侵害活動で使用された EMDIVI の検体には，次のような類似性があると指摘している．

- 感染した PC でのみ実行可能とするために SecurityIdentifier を暗号化鍵として利用している．
- 侵入した後に，別途潜伏用の RAT 本体を準備する．

そこで，表 4 に示す Case f03(BKDR_CHCHES.NAK)の観測事象を，BOS_2016 以前の観測事象と比較した結果，BOS_2015 Case d18(BKDR_EMDIVI.I)で観測された事象が，一部パスや引数に違いがあるもののコマンドとその操作順序がほぼ一致していることがわかった(表 7)．攻撃者の行動観測から，ChChes と EMDIVI には，検体だけではなく，攻撃者による環境情報の取得についても類似性を示すことができたと言える．

4. おわりに

本稿では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS(Behavior Observable System)とその研究用データセット「動的活動観測 2017 (BOS_2017)」について報告した．

研究用データセット「動的活動観測 2017 (BOS_2017)」は，攻撃者の行動観測を通したサイバー攻撃活動分析と共に，攻撃者のアトリビューションに着目したデータセットである．「動的活動観測 2017 (BOS_2017)」では，攻撃者行動視点での特徴付けとして，標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例だけではなく，進行度という動的活動観測における攻撃活動の進み具合の区分を設け，標的型攻撃の段階に応じた事例を含んでいる．

表 7：Case f03 と Case d18 における観測事象の類似性

Case f03		Case d18	
Time	Observable event	Date and Time	Observable event
2017/01/18 17:00	tasklist	2014/10/09 15:14	tasklist /v
2017/01/18 17:10	logoff /f		
		2014/10/09 15:18	cmd /c ipconfig
2017/01/18 17:19	dir C:¥Users¥		
2017/01/18 17:28	dir c:¥users¥HitachiSato¥desktop¥	2014/10/09 15:19	cmd /c dir C:¥Users¥ADMINI~1¥desktop
2017/01/18 17:29	net view /domain	2014/10/09 15:18	cmd /c net view /domain
2017/01/18 17:31	net view	2014/10/09 15:18	cmd /c net view
2017/01/18 17:32	net user /domain	2014/10/17 10:49	cmd /c net user ad /domain
2017/01/18 17:32	net user HoshiKentaro /domain	2014/10/17 10:49	cmd /c net user ad67 /domain
2017/01/18 17:33	c:¥users¥HitachiSato¥		
2017/01/18 17:33	dir c:¥users¥HitachiSato¥Documents	2014/10/09 15:21	cmd /c dir C:¥Users¥ADMINI~1¥documents
2017/01/18 17:34	ipconfig	2014/10/09 15:18	cmd /c ipconfig
2017/01/18 17:34	net use	2014/10/16 20:23	cmd /c net use
2017/01/18 17:34	powershell "Get-ItemProperty HKLM:¥ Software¥ Microsoft¥ Windows¥ CurrentVersion¥ Uninstall¥* | Select-Object DisplayName, DisplayVersion"		
2017/01/18 17:34	ping 192.168.12.8	2014/10/17 10:48	cmd /c ping Cae002-av02 -n 1
2017/01/18 17:35	dir ¥¥192.168.12.8¥c$	2014/10/16 20:51	cmd /c dir ¥¥CAE003-AV03¥c$
2017/01/18 17:35	net group /domain	2014/10/17 10:49	cmd /c net group "domain users" /domain
2017/01/18 17:36	net group "Domain Controller" /domain	2014/10/17 10:47	cmd /c net group "domain computers" /domain
2017/01/18 17:36	net group "Domain Controllers" /domain	2014/10/17 10:47	cmd /c net group "domain computers" /domain
2017/01/18 17:38	net group "domain admins" /domain	2014/10/17 10:47	cmd /c net group "domain admins" /domain
2017/01/18 17:38	net user	2014/10/16 20:49	cmd /c net user
2017/01/18 17:39	net user Administrator	2014/10/16 20:50	cmd /c net user admin

また，本稿では，動的活動観測で使用している検体 Chches について，exe 型と PowerShell 型などの種別毎の出現傾向，バージョン番号の出現傾向，exe 型の場合には検体のコンパイル日付の分布傾向を報告すると共に，ChChes と EMDIVI には, 攻撃者による環境情報の取得についても，類似性がみられることを示した.

今後は，研究用データセット「動的活動観測」として，各進行度の事例拡充など，サイバー攻撃に関する脅威情報データベースと連携した「動的活動観測」の推進を検討していきたいと考えている.

謝辞

大規模ネットワーク実験環境 StarBED を本実験環境として利用するにあたりご協力を頂いた国立研究開発法人情報通信研究機構総合テストベッド研究開発推進センター(現北陸 StarBED 技術センター)の関係者各位に深く感謝致します. また，本研究は総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験の請負」で実施したものです．本研究を進めるにあたって有益な助言と協力を頂いた関係各位に深く感謝致します.

参考文献

1) 寺田、青木、楠美、重本、萩原. 研究用データセット「動的活動観測 2014」. コンピュータセキュリティシンポジウム. (2014)
2) 寺田、堀、成島、吉野、萩原. 研究用データセット「動的活動観測 2015」. コンピュータセキュリティシンポジウム. (2015)
3) 寺田、佐藤、堀、吉野、萩原. 研究用データセット「動的活動観測 2016」. コンピュータセキュリティシンポジウム. (2016)
4) 髙橋、小林、陳、米持、吉岡、松本. RAT サーバの動作を遠隔操作者と同じ操作画面で観測する方法. コンピュータセキュリティシンポジウム. (2013)
5) 髙橋、小林、陳、小山、金井、吉岡、松本. RAT サーバの動作を遠隔操作者と同じ操作画面で観測する方法 その 2. コンピュータセキュリティシンポジウム. (2014)
6) 国立研究開発法人情報通信研究機構. サイバー攻撃誘引基盤 "STARDUST"(スターダスト)を開発. https://www.nict.go.jp/press/2017/05/31-1.html (2017)
7) B Farinholt, M Rezaeirad, P Pearce, H Dharmdasani, H Yin, S Le Blond, D McCoy and K Levchenko. To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild. In 38th IEEE Symposium on Security and Privacy. (2017)
8) David A. Wheeler, et.al.：Techniques for Cyber Attack Attribution (Institute for Defense Analysis, IDA Paper)(2003.10)
9) FireEye：高度なサイバー攻撃の痕跡 ～攻撃者の素性を特定する 7 つの手がかり～(2013)
10) Structured Threat Information eXpression (STIX), http://stix.mitre.org/
11) Trusted Automated eXchange of Indicator Information (TAXII), http://taxii.mitre.org/
12) Automated Indicator Sharing (AIS), https://www.us-cert.gov/ais
13) JPCERT/CC. Cookie ヘッダーを用いて C&C サーバとやりとりするマルウエア ChChes. https://www.jpcert.or.jp/magazine/acreport-ChChes.html (2017).
14) JPCERT/CC. PowerSploit を悪用して感染するマルウエア. https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html (2017)
15) Palo Alto Networks, Inc. menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations. http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/ (2017)
16) ラック. 攻撃者グループ menuPass とマルウェア（Poison Ivy、PlugX、ChChes）の関連性. https://www.lac.co.jp/lacwatch/people/20170223_001224.html (2017)
17) Cylance Inc. The Deception Project: A New Japanese-Centric Threat. https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html (2017)
18) トレンドマイクロ. 「ChChes」を操る標的型サイバー攻撃集団「ChessMaster」による諜報活動の手口. http://blog.trendmicro.co.jp/archives/15551 (2017)