Vol.2015-CSEC-71 No.14
2015/12/4

標的型攻撃に用いられるドメインの WHOIS を基にした被害の早期発見手法の提案

久山真宏[†1]　佐々木良一[†1]

概要：近年流行している標的型攻撃では，マルウェアに感染した後に C&C サーバとの間で様々な通信を行う．対策として，C&C サーバとの通信を監視する方法は有効であると考えるが，C&C サーバを特定するにはマルウェアおよびその通信を解析する必要があり，対策が後手になってしまう．そこで，本研究では，C&C サーバに用いられているドメインの WHOIS よりメールアドレスを抽出し，そのメールアドレスに紐づくドメインを調べることで，新たな C&C サーバを発見する手法を提案する．実験の結果，提案手法により複数のドメインが抽出された．今回抽出されたドメインとの通信を監視することで，被害の早期発見を図る．

キーワード：サイバー攻撃，標的型攻撃, C&C サーバ，ドメイン, WHOIS

Proposal of a new C & C servers identification method based on a WHOIS domain used for targeted attacks

MASAHIRO KUYAMA[†1]　RYOICHI SASAKI[†1]

Abstract: Targeted attack makes a PC perform various communications with the C&C server after infecting the PC by using malware. Though prohibiting communication with the C&C server seems to be effective, before identifying the server, time consuming analysis for the related malware and its communication is required. To speed up it, we pay our attention to that the e-mail address extracted from the WHOIS of the domain to be used in the C&C server has the probability to be used in other C&C Server. In this study, we propose a method to discover a new C&C server paying attention the e-mail address described above. The results of the experiment, a plurality of domains have been extracted by the proposed method. It is possible to find attack by monitoring the communication to the discovered domain using our proposed method.

Keywords: cyberattack, Targeted attack, C&C server, domain, WHOIS

1. はじめに

近年，標的型攻撃による被害が問題になっている[1]．標的型攻撃とは，金銭や知的財産等の秘密情報の不正な取得を目的として，特定の企業や組織を標的にしたサイバー攻撃の一種であり，ドライブバイダウンロード攻撃や，メールなどに添付されたマルウェアに感染することによって，情報の搾取や破壊活動が行われる．

日本では，国内の大手重工メーカや衆議院，日本年金機構などにおいて，標的型攻撃の被害に遭い，実際にニュースになるほどの重大なインシデントに繋がっている．標的型攻撃の対策が求められており，多層防御として入口対策や出口対策が求められる．

標的型攻撃では，初期侵入段階において，マルウェアに感染させる．その後，C&C サーバ（Command and Control server）と呼ばれる中継サーバを介して，遠隔操作を行うことにより侵入範囲の拡大や，情報摂取等を行う．そのため，出口対策として C&C サーバの通信を監視することにより，被害を発見することが出来る[2,3]．しかし，C&C サーバとの通信を監視するには，事前に C&C サーバを特定している必要がある．そのため，特定されていない C&C サーバが用いられた場合には監視対象から外れているため，被害に気づきにくくなる．

現在筆者らは，標的型攻撃に対してインシデント発生時にネットワークログ等のデータを適切に利用し，人工知能（AI ともいう）を用いて自動的な応急対応を可能とするとともに，運用者が適切な対策をとれるようにするための LIFT（Live and Intelligent Network Forensic Technologies）システムの開発を行っている[4,5]．さらに，防御側だけではなく，攻撃側にも人工知能を利用して Beyond the Attackers を実現し，Proactive な対策を実現する Supper-LIFT システム[6]を構想している（図 1）．

†1 東京電機大学
Tokyo Denki University

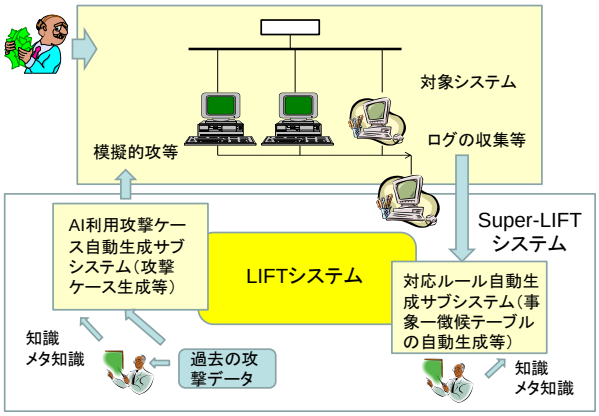

図 1　Supper-LIFT システムの研究

Supper-LIFT では，サイバー攻撃に関する情報の収集・分析としてシギント（signals intelligence）活動を行っており，その活動の一環として，C&C サーバの分析・調査を行っている．

本論文では，Supper-LIFT の活動から得られた知見をもとに，既知の C&C サーバに用いられているドメインの WHOIS に紐づく他のドメインを抽出することで，新たな C&C サーバを発見する手法の提案を行う．

C&C サーバを発見するための先行研究として，制御通信のペイロードに含まれる文字列などの特徴を分析することで検知を行う手法[7][8]，ドメイン情報や外部リポジトリから取得した情報を併用して，RIPPER と呼ばれるデータマイニング手法を用いて検知を行う手法[9]，C&C サーバと正規のサーバの DNS 情報に数量化理論 2 類を用いて C&C サーバの推定を行う手法[10]，テイント解析技術を応用したマルウェア解析を実施することで通信データの改ざんを検知し，C&C サーバを特定する手法[11]等があるが，それらと比べ，提案手法では正規のサーバが改ざんされ C&C サーバとして悪用された場合も，当該 C&C サーバを発見することが出来る利点がある．

2. 意図不明ドメインの発見

筆者らは Supper-LIFT 構想において，サイバー攻撃に関する情報の収集・分析としてマルウェアから抽出したドメインの WHOIS を調査していた．調査を実施していると，WHOIS への登録を代行するサービス（以後，登録代行サービスとする）を利用していないドメインを発見した．また，登録代行サービスを利用していないドメインとしては，国外のものが多く見受けられた．

登録者連絡先について調査を行っていると，登録されているメールアドレスに関係するドメインが，利用されている痕跡の無いドメイン（以後，意図不明ドメインとする）であるものであった．

元来，C&C サーバには攻撃者が攻撃に用いるために準備した C&C サーバ（以後，悪性 C&C サーバとする）と，正規のサーバが攻撃者によって乗っ取られ C&C サーバとして悪用されるケース（以後，改ざん C&C サーバとする）がある．

悪用 C&C サーバの多くは，身元を特定されないためにドメイン登録時に登録代行サービスの利用や，でたらめの情報が登録されている．しかし，でたらめな情報が登録されている場合において，ドメイン登録時に必要となる登録者連絡先のうち，メールアドレスについては，実際に連絡を行う時に必要となり，偽装困難であると考えられる．

改ざん C&C サーバでは，管理が不十分な管理者のサーバは同時に改ざんされている可能性がある．そのため，改ざん C&C サーバに紐づくドメインを調査することにより，同様に改ざんされ悪用されている改ざん C&C サーバを見つけ出せるのではないのかと考えた．

そこで，悪用 C&C サーバのドメインより抽出したメールアドレスに紐づくドメインは，攻撃者が次のサイバー攻撃のために準備したドメインであり，改ざん C&C サーバのドメインより抽出したメールアドレスに紐づくドメインは，同様に改ざんされ改ざん C&C サーバとして悪用されている可能性が高いと仮定し，今回の提案を実現するためのシステムの開発に着手した．

3. 提案手法

3.1 提案概要

提案手法では，まず標的型攻撃に用いられるマルウェアを収集し，サンドボックスなどの分析システムで当該マルウェアの C&C サーバの特定を行う（1）．特定した C&C サーバのドメインの WHOIS よりドメインに紐づいたメールアドレスを抽出する（2）．抽出されたメールアドレスから紐づくドメインを検索できるサービスを利用し，紐づくドメインを抽出する（3）．抽出されたドメインとの通信を監視することで，標的型攻撃の被害を発見する（図 2）．

図 2　提案手法概要図

(1) **マルウェアの収集・分析**

標的型攻撃での使用率の高い Emdivi，PlugX，PoisonIvy と呼ばれる 3 種類のマルウェア群[12]を対象に調査を実施した．

マルウェアの収集にあたっては, VirusTotal[13]を用いて，キーワードに Emdivi，PlugX，PoisonIvy の種別名で検索を実施し，計 163 件のマルウェアを収集した（表 1）．

表 1　収集したマルウェアの検体数

マルウェア種別	検体数
Emdivi	50
PlugX	63
PoisonIvy	50

収集したマルウェアを LastLine[14]と呼ばれる Sandbox を用いて解析を実施．解析結果より，マルウェアが通信を行う接続先のドメインを抽出した．そこから，重複などを削除して計 93 件の C&C サーバのドメインを抽出することが出来た．

(2) **WHOIS**

WHOIS からは一般的に以下の情報を得ることが出来る．

a) 登録ドメイン名
b) レジストラ名
c) ドメインが登録されている DNS サーバ名
d) ドメインの登録年月日
e) ドメインの有効期限
f) ドメイン名登録者の連絡先
g) 技術的な連絡の担当者連絡先
h) 登録に関する連絡の担当者連絡先
i) 登録者への連絡窓口の連絡先

今回筆者らは，上記の内，f) と g)，h)，i) に着目して，（1）で抽出した 93 件のドメインの WHOIS より，これらの連絡先として登録されてあるメールアドレスを対象に調査を行った．

調査の結果，重複を除く計 44 件のメールアドレスを抽出した．

(3) **メールアドレスに紐づくドメインを検索**

メールアドレスから紐づくドメインを検索できるサービスとして DomainBigData.com[15]がある．

DomainBigData.com は，膨大な量のドメインとその WHOIS を蓄積したデータベースであり，主に以下のことを実現するオンライン調査ツールとして利用することが出来る．

a) WHOIS Research
b) Competitors Research
c) Network Intelligence
d) Domains Statistics
e) Actionnable results
f) It’s completely free

上記の内，a) の WHOIS からドメインを検索する機能を用いて，抽出したメールアドレスの紐づくドメインの抽出を行なった．その結果，計 2597 件のドメインを抽出した．

3.2 調査結果

マルウェアの収集からドメインの抽出までを行った結果, 計 2597 件のドメインの抽出することが出来た（表 2）．

表 2　調査結果

(1)C&C サーバのドメイン数	93 件
(2)抽出メールアドレス数	44 件
(3)抽出ドメイン数	2597 件

膨大な量のドメインが抽出されたが，この状態では，WHOIS の登録代行サービス業者のメールアドレスや攻撃者と関係のないメールアドレスも抽出されてしまうため，誤検知（false positive）を含む膨大な量のドメインが抽出されている．

3.3 WHOIS 登録代行サービス業者の除外

先の調査結果で抽出されたメールアドレスから登録代行サービス業者（クラウドサーバを含む）を除外する必要がある．しかし，登録代行サービスは複数存在する．そこで，登録代行サービス業者を除外するため，抽出されたメールアドレス 44 件を対象に調査を行い, 登録代行サービス業者である 36 件のメールアドレスをブラックリストにて除外した．その結果，最終的に 8 件のメールアドレスが残

り,抽出ドメイン数は 39 件に絞り込むことが出来た(表 3).

表 3　特定メールアドレス除去後の調査結果

	除外前	除外後
(1)C&C サーバのドメイン数	93 件	93 件
(2)抽出メールアドレス数	44 件	8 件
(3)抽出ドメイン数	2597 件	39 件

登録代行サービスとして利用されているものの多くは,世界中に展開している大手の業者が多くあった．また，日本の業者も次いで多く用いられていた．

また，抽出された 8 件のメールアドレスとしては，悪用 C&C サーバではプロバイダもしくはフリーのメールアドレスが用いられており，改ざん C&C サーバでは独自ドメインのメールアドレスが比較的多く用いられていた．さらに，フリーのメールアドレスとしては，世界中に展開している大手のものと中国のものであった．

4. 調査結果

提案手法により，悪性 C&C サーバ，改ざん C&C サーバの両者から抽出したメールアドレスに紐づいたドメインとして，計 39 件のドメインを発見することが出来た．これらのドメインが，今後のサイバー攻撃に用いられるのであれば，提案手法によって発見された意図不明ドメインを監視することで，より迅速に標的型攻撃を検知可能であると考える．

また，最終的に残った 39 件のドメインと C&C サーバのドメインを比較したが，同一ドメインを見つけることは出来なかった．しかし，最終的に残った 39 件のドメインを調査した結果，意図不明ドメインの他に，特定の攻撃グループが用いているドメインであるとしてブラックリストに登録されているものや,改ざんされたサイトのドメインなど,実際に悪用されているものもあった．

Aguse[16]を用いて Web アクセスできるか確認したところ,正規のサイトのように Web サーバとして機能しているものが多く見受けられたが，アダルトサイトや海外のサイトが多く，比較的英語と中国語のサイトが多く見受けられた．また，同一のメールアドレスに複数の言語の Web サイトが存在するものもあり，その中には，Google[17]での検索結果にて「このサイトは第三者によって改ざんされている可能性があります」と注意書きがあるものもあった．

調査元となったマルウェアから抽出したドメインと検討してみると，悪性 C&C サーバに紐づくドメインには意図不明のドメインが多く，改ざん C&C サーバに紐づくドメインには Web サーバとして機能しているドメインが多く見受けられた．これらは，当初の仮定を裏付けられるものと考える．

悪性 C&C サーバに紐づくドメイン，改ざん C&C サーバに紐づくドメインともに,悪用される可能性を秘めており,提案手法により抽出されたドメインの監視を行うことにより，今後発生しうるサイバー攻撃の早期発見に役立つものと考える．

5. 今後の方針

本研究を発展させるため，引き続き調査を行うとともに,今後は，横浜国立大学の松本らの提案手法[18]を用いて,類似のマルウェアを見つけ出し，仮定を証明・評価を行なう．さらに，より詳細に分析を行うために，悪性 C&C サーバと改ざん C&C サーバの分類手法についても検討を行い，各々の結果をもとに研究を進める予定である．

また，除外した WHOIS の登録代行サービスについても分析を行い，どの業者のサービスが攻撃者に利用されやすいのかを明らかにするとともに，その特徴を見つけ出せるのではないかと考える．

今回，除外するメールアドレスとして，WHOIS の登録代行サービス業者のメールアドレスを挙げた．しかし，この他にも，失効した C&C サーバのドメインを取得してマルウェアの感染状況などを調査する DNS シンクホールを運用している登録者のメールアドレスが誤検知の要因として挙げられる．そのため，DNS シンクホールを特定する手法についても検討する必要がある．

6. おわりに

Supper-LIFT における攻撃データ収集・分析の一環として実施した C&C サーバの調査より，WHOIS を基にした新たな C&C サーバと考えられるドメインを抽出する手法について提案した．提案手法にて実験を行った結果，39 件の疑わしいドメインを抽出することが出来た．

抽出されたドメインには，意図不明ドメインの他に，特定の攻撃グループが用いているドメインであるとしてブラックリストに登録されているものや，改ざんされたサイトのドメインなど，実際に悪用されているものもあった．

提案手法により抽出されたドメインは，実際に標的型攻撃に悪用される可能性を秘めており，当該ドメインへの接続を監視することにより，今後発生しうる標的型攻撃の早期検知および防止に寄与できると考える．

標的型攻撃は，特定の企業や組織を標的にしているため,用いられるマルウェアや C&C サーバも目的が遂行されることで使い捨てられ，次の標的型攻撃においては新たなマルウェアと C&C サーバでサイバー攻撃が行なわれることが考えられる．そのため，既知の C&C サーバを遮断する方法では防ぎきれない．そこで，提案手法をもとに，標的型攻撃に用いられる前段階で C&C サーバを見つけ出すこ

とは，C&C サーバとの通信を早期に検知することができ，後手にまわりつつあるサイバー攻撃対策に対して先手を打つことが出来るのではないかと考える．

参考文献

1) 標的型攻撃等の脅威について
http://www.nisc.go.jp/conference/suishin/ciso/dai18/pdf/2.pdf
2) 標的型攻撃 対策指南書（第 1 版）
http://www.lac.co.jp/anti-apt/guidebook/pdf/anti-apt_guidebook_ver1.pdf
3) 「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/files/000046236.pdf
4) 比留間裕幸，橋本一紀，上原哲太郎，松本隆，佳山こうせつ，柿崎淑郎，八槇博史，佐々木良一：標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発（その１）－予兆検知と対策指示方法の提案－，マルチメディア，分散協調とモバイルシンポジウム 2015 論文集
5) 橋本一紀，比留間裕幸，上原哲太郎，松本隆，佳山こうせつ，柿崎淑郎，八槇博史，佐々木良一：標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発（その２）－プロトプログラムの開発と評価－，マルチメディア，分散協調とモバイルシンポジウム 2015 論文集
6) 佐々木良一，八槇博史：標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発（その３）－今後の研究構想－，マルチメディア，分散協調とモバイルシンポジウム 2015 論文集
7) D. I. Jang, M. Kim, H. C. Jung, B. N. Noh：Analysis of HTTP2P Botnet: Case Study Waledac, 2009 Ieee 9th Malaysia International Conference on Communications (Micc), pp. 409-412, 2009.
8) Wei. Lu, M. Tavallaee, Ali. A. Ghorbani：Automatic Discovery of Botnet Communities on Large-Scale Communication Networks, ASIACCS '09 Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009.
9) M. H. Tsai, K. C. Chang, C. C. Lin, C. H. Mao, H. M. Lee：C&C Tracer: Botnet Command and Control Behavior Tracing, in IEEE International Conference on Systems, Man and Cybernetics (SMC), Anchorage, AK, pp.1859-1864, 2011.
10) 岡安翔太，佐々木良一：ボットネットの C&C サーバ特定手法における数量化理論と機械学習での評価と提案，マルチメディア，分散協調とモバイルシンポジウム 2015 論文集
11) 幾世知範，青木一史，八木毅，針生剛男：改ざんデータの出自確認に基づいた C&C サーバ特定手法の提案，電子情報通信学会ソサイエティ大会講演論文集 2014 年 通信(2), 16, 2014-09-09
12) 国内標的型サイバー攻撃分析レポート 2015 年版
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150409062703.html
13) VirusTotal
https://www.virustotal.com/
14) LastLine
https://www.lastline.com/
15) DomainBigData.com
http://domainbigdata.com/
16) Aguse
https://www.aguse.jp/
17) Google
https://www.google.co.jp/
18) 森島周太，筒見拓也，田辺瑠偉，高橋佑典，小林大朗，吉川亮太，吉岡克成，松本勉：動的解析と統合型マルウェア検査サービスの活用によるサイバー攻撃情報収集手法，信学技報，vol. 114, no. 489, ICSS2014-81, pp. 109-114, 2015 年 3 月．