SOCレポート

1.1 はじめに

IIJでは、2016年10月31日にセキュリティ事業の新ブランド「wizSafe(ウィズセーフ)」を発表し[*1]、お客様が安全にインターネットを利用できる社会に向けて日々活動しています。その一環として、SOCで観測したセキュリティに関する脅威情報をwizSafe Security Signal[*2]を通してブログ形式でタイムリーに発信しています。この中では、IIJの情報分析基盤を通して解明した脅威情報の一部を公開しています。情報分析基盤の概要については、過去のInternet Infrastructure Review(IIR) Vol.38[*3]をご覧ください。

ここでは、情報分析基盤を活用した分析の概要を紹介します。情報分析基盤には、IIJサービスとして提供しているファイアウォールやIPS/IDS、アンチウイルスなどのセキュリティ機器のログをはじめ、DNSクエリやWebアクセス、メール送受信ログなど、様々なログが集約されています。これらのログには、大量の正常通信の中にごくわずかな異常(脅威)通信が含まれるという特性があります。そのため、脅威が明確に確認できるよう、集計方法や可視化の検討が必要となります。

1.2節では2018年に情報分析基盤を通して明らかになった脅威情報について紹介し、1.3節では情報分析基盤を活用した新たな取り組みについて紹介します。なお、2018年の観測情報はwizSafe Security Signalにまとめています[*4]。

1.2 観測情報

まずは、昨年wizSafe Security Signalで報告した内容の中から、情報分析基盤を活用して明らかになった特筆すべき活動について取り上げます。

1.2.1 仮想通貨に関連する攻撃

2018年は、攻撃者が仮想通貨を用いて攻撃の収益化を試みる事例が注目を集めた年でした。IIJの情報分析基盤を用いた分析でも、攻撃者が仮想通貨の悪用を試みる事例を複数観測しています。

まず、Webサイトの改ざんに伴うマイニングスクリプトの埋め込み事例です。SOCの観測では、Webサイトに埋め込まれたマイニングスクリプトの中に、管理者が意図して埋め込んだもの

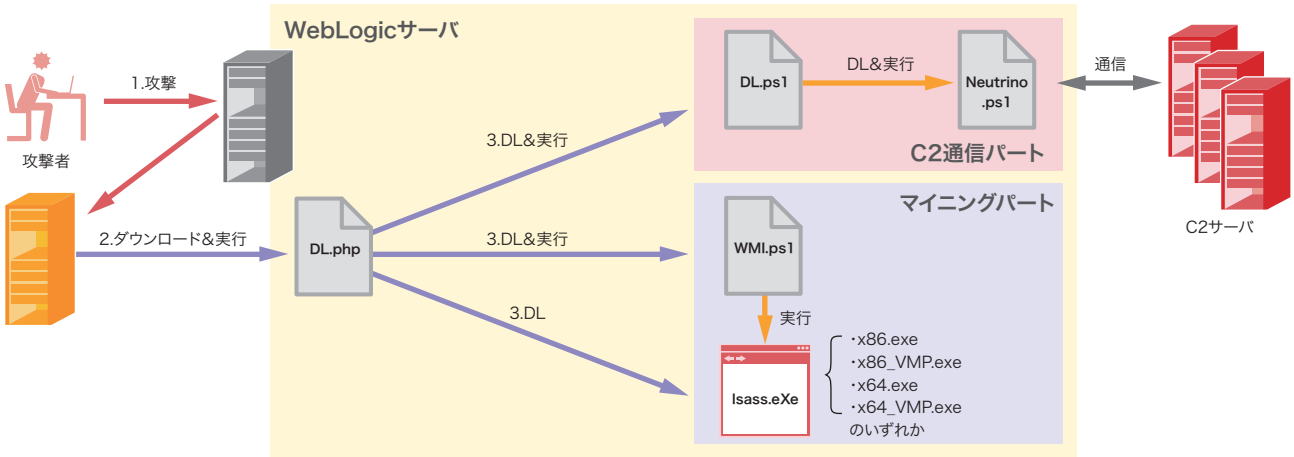

図-1 GhostMinerによる攻撃の流れ

＊1　IIJ、セキュリティ事業の新ブランド「wizSafe(ウィズセーフ)」を発表(https://www.iij.ad.jp/news/pressrelease/2016/1031.html)。
＊2　wizSafe(https://wizsafe.iij.ad.jp)。
＊3　Internet Infrastructure Review(IIR)Vol.38(https://www.iij.ad.jp/dev/report/iir/038/01.html#anc02)。
＊4　wizSafe、「wizSafe Security Signal 2018年 年間サマリ」(https://wizsafe.iij.ad.jp/2019/03/601/)。

ではないと考えられるケースが複数見つかっています。攻撃者は、Webサイトに存在する脆弱性を悪用するなどの方法で、ユーザが閲覧するWebページにマイニングスクリプトを埋め込みます。これにより、被害サイトを閲覧したユーザのコンピュータで仮想通貨がマイニングされ、収益が攻撃者の手に渡ります。

上記の事例はクライアントを狙ったものですが、サーバに仮想通貨をマイニングさせる攻撃も観測しています。具体例の1つとしては、GhostMiner(図-1)と名付けられた攻撃キャンペーン[*5]が挙げられます。GhostMinerキャンペーンは2018年3月に観測しており、Oracle WebLogic Serverの脆弱性(CVE-2017-10271)が悪用されました。脆弱性はリモートコード実行が可能となるもので、攻撃者は最終的にWebサーバに対し仮想通貨をマイニングさせようと試みます。なお、この他にもリモートコード実行の脆弱性を利用して、サーバに仮想通貨をマイニングさせる試みを多数観測しています[*6][*7]。

また、マイニングではなく不正送金を目指す試みとして、2018年12月にはEthereumのクライアントが備えるJSON-RPCを狙ったスキャン活動(図-2)を観測しました[*8]。スキャン活動では、設定の不備によりインターネットからアクセスできる状態にあるEthereumのクライアントを探索していました。なお、実際に不正な送金を成立させるには、複数の条件を満たす必要があります。

仮想通貨は、攻撃を直接的に収益化でき、種類によっては匿名性も高いという、攻撃者にとって都合の良い特性を備えています。また、仮想通貨のマイニングを意図した攻撃では、攻撃対象としてクライアントとサーバの事例が混在しているように、計算リソースさえあればどのような環境も標的となります。今後も、仮想通貨は攻撃を収益化する方法の1つとして用いられていくと考えられます。

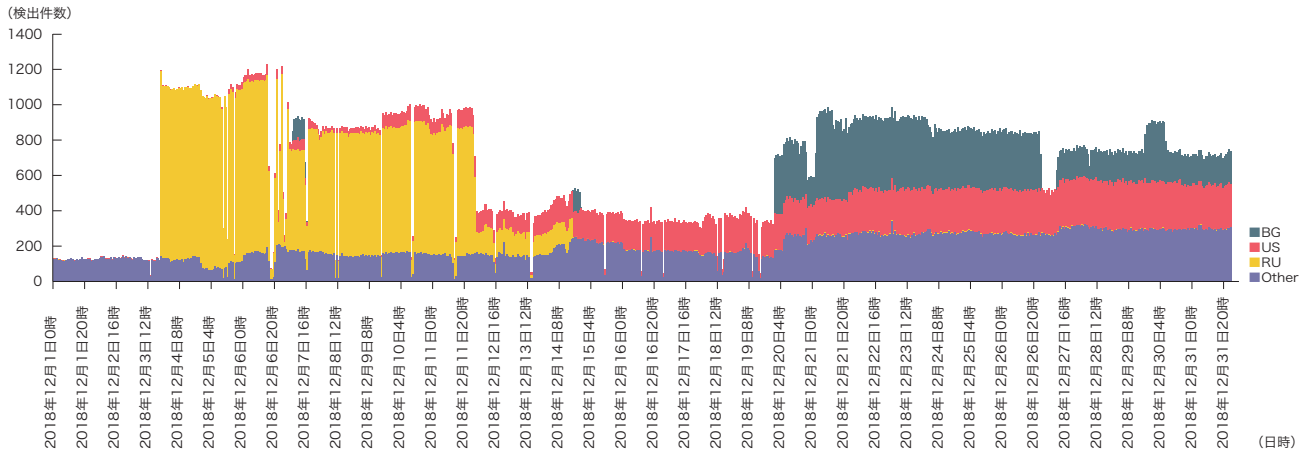

図-2 8545/TCPに対するスキャン活動(2018年12月)

*5 wizSafe、「GhostMinerの感染拡大」(https://wizsafe.iij.ad.jp/2018/04/323/)。
*6 wizSafe、「wizSafe Security Signal 2018年1月 観測レポート」(https://wizsafe.iij.ad.jp/2018/02/247/)。
*7 wizSafe、「wizSafe Security Signal 2018年2月 観測レポート」(https://wizsafe.iij.ad.jp/2018/03/286/)。
*8 wizSafe、「EthereumのJSON RPCにおけるスキャン活動の観測」(https://wizsafe.iij.ad.jp/2019/01/541/)。

1.2.2 SYN/ACKリフレクション攻撃

2018年にSOCで観測したDDoS攻撃の中で特徴的だった事例は、wizSafe Security Signal 2018年9月[*9]に掲載した80/TCPを利用したSYN/ACKリフレクション攻撃です（図-3）。送信元アドレスを偽装したTCPのSYNパケットを多数のアドレスに同時に送信し、その応答であるSYN/ACKパケットを利用して送信元アドレスに対してDDoS攻撃を行うものです。

このSYN/ACKリフレクション攻撃をSOCで観測したのは2018年9月26日でしたが、10月以降も小規模ながら観測しており、情報分析基盤を通して日々、同種の攻撃を検知しています。9月26日に観測したDDoS攻撃の1つの特徴は、攻撃の送信元がインターネット上に80/TCPを公開している各サーバに対して少量のSYNパケットを送信して攻撃を実現している点です。仮に攻撃者が単一のサーバに対してSYNパケットを大量に送信してしまうと、SYNパケットを受け取ったサーバの管理者がTCP SYN Flood攻撃[*10]を受けていると判断して通信を遮断してしまう可能性があります。その場合、攻撃者が想定している攻撃規模を実現できない可能性があります。また、サーバ1台あたりに届くSYNパケットの量が少量であるため、攻撃者は広範囲にSYNパケットを送信していると考えられます。

前述の攻撃で利用されていたポートは80/TCPであり、80/TCPを公開しているサーバは一般的にWebサーバであると考えられます。そのため、正常なWebアクセス通信の中にSYN/ACKリフレクション攻撃で利用するSYNパケットが少量送信されていたところで、そのパケットが攻撃に利用されていると判断するのは困難です。この事例の場合は、情報分析基盤上に存在する複数のお客様のファイアウォール・ログを横断的に分析することで検出しました。

ファイアウォール・ログを用いた検知では、内外部からのアクセス情報が確認できるため、複数のファイアウォール・ログで、80/TCPの応答通信が特定のIPアドレス（攻撃対象となっている偽装されたIPアドレス）に対して発生している場合に検知可能となります。ただし、この特徴はDDoS攻撃ではなくスキャン活動である可能性もあります。そのため、ファイアウォール・ログから集計された送受信バイト数や継続時間などを基にDDoS攻撃とスキャン活動を区別しています。

2018年9月に掲載したSYN/ACKリフレクション攻撃については、IIJのハニーポットにおいても観測しており、IIJ SECTブログの「IoT機器を踏み台として利用するSYN/ACKリフレクション

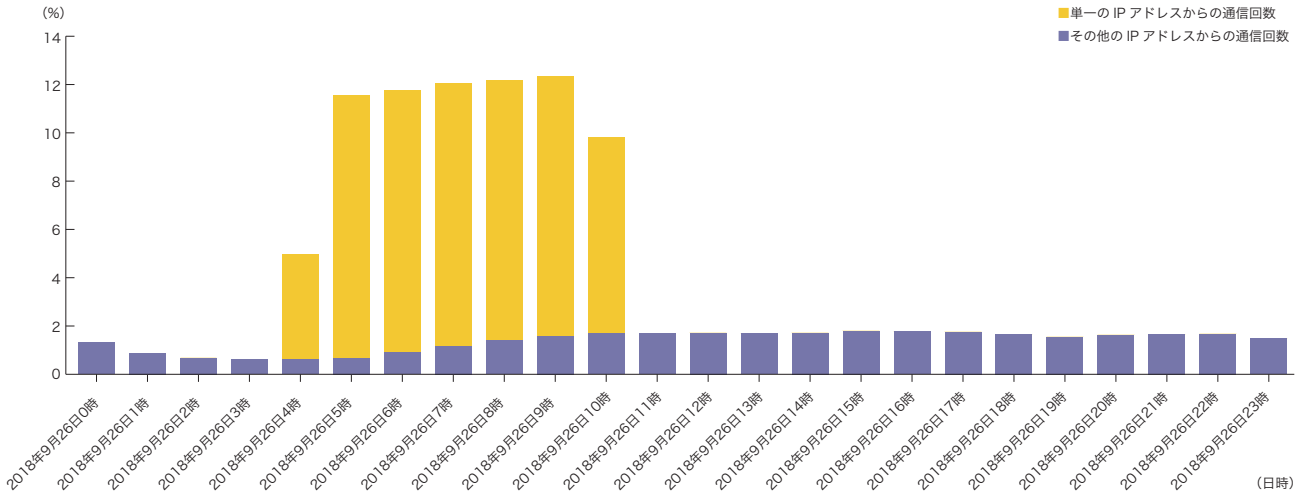

図-3 単一のIPアドレスから80/TCPへの通信の増加

＊9　wizSafe、「wizSafe Security Signal 2018年9月 観測レポート」（https://wizsafe.iij.ad.jp/2018/10/470/）。

＊10　TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリなどを無駄に利用させる。

攻撃」[*11]で詳しく報告しています。攻撃に利用されているポートの変化やUDPプロトコルを利用した複合型のDDoS攻撃であることが解説されていますので併せてご覧ください。

1.2.3 既知の脆弱性を狙った攻撃の再興

2018年の情報分析基盤を用いた分析で印象的だったのが、過去に発表されて既に問題を修正したパッチが提供されている脆弱性が、時間をあけて再び狙われる事例です。具体例の1つとしては、Microsoft Officeの数式エディターの脆弱性(CVE-2017-11882)を悪用したマルウェアが挙げられます。

マルウェアが悪用した脆弱性は、Microsoft Officeの数式エディターにバッファオーバーフローの問題があり、リモートコード実行が可能になるというものです。Microsoft社は、この脆弱性を修正するパッチを2017年11月に提供しています。また、パッチを適用する以外の回避策として、数式エディターの機能を無効化する、という方法もありました。

情報分析基盤では、修正から1年近く経った2018年9月に、この脆弱性を狙った攻撃を観測しました(図-4)[*12]。攻撃者は、脆弱性を悪用するマルウェアをメールに添付して送付しています。脆弱性に関する意識が世間から薄れたタイミングで、未対策あるいは一時的に機能を無効化することで問題を回避していた環境を意図的に狙ったと考えられます。

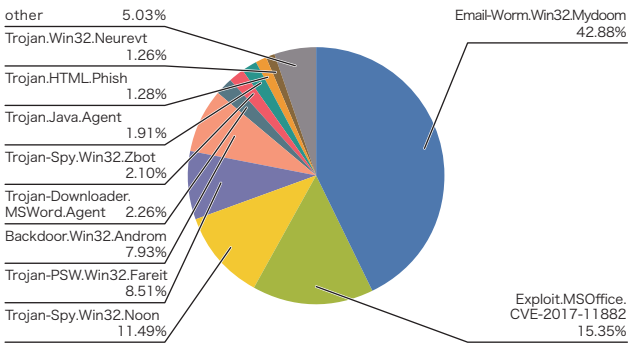

図-4 メール受信時に検出したマルウェア種別の割合(2018年9月)

このような事例は、今回取り上げたMicrosoft Officeの脆弱性以外にも情報分析基盤で複数観測しています[*13]。脆弱性について、根本的な対策や様々な事情から回避策を用いる場合には継続的な対応が要となることが、教訓として得られる事例といえます。

1.3 機械学習を用いた悪性通信の検出

情報分析基盤が取り扱うデータには、大量の正常通信の中にごくわずかな異常(脅威)通信が含まれるという特性があります。これを機械学習によって発見する取り組みが進んでいます。タスクとして主に扱うのは、不均衡データ(Imbalanced Data)からの異常検知(Anomaly Detection)です。ここでは、進行中の2つのプロジェクトとその課題について紹介します。

1.3.1 DNSクエリデータへの適用

マルウェアは、C2(Command and Control)サーバの通信先として、DGA(Domain Generate Algorithm)と呼ばれる手法で機械的に生成したドメインを用いる場合があります。DGAで生成されるドメインは、アルゴリズムの種類や動作する際のパラメータによって大きく異なります。そのため、あらかじめマルウェアの通信先をブラックリストとして管理することや、検知するシグネチャを表現することが困難な場合があります。

*11 IIJ-SECT Security Diary、「IoT機器を踏み台として利用するSYN/ACKリフレクション攻撃」(https://sect.iij.ad.jp/d/2019/02/128021.html)。
*12 wizSafe、「wizSafe Security Signal 2018年9月 観測レポート」(https://wizsafe.iij.ad.jp/2018/10/470/)。
*13 wizSafe、「wizSafe Security Signal 2017年11月 観測レポート」(https://wizsafe.iij.ad.jp/2017/12/184/)。

そこで、このプロジェクトでは情報分析基盤のDNSクエリデータと機械学習を組み合わせることで、その問題の解決を目指しています。人間によるルール化が難しいタスクであっても、機械学習を用いることで解決できる場合があるためです。機械学習のアルゴリズムには、識別に有効な特徴量を含むデータを与えることで、異常データを分類する能力を自律的に獲得できるという、望ましい特性があります。例えば、前号のIIR Vol.41でURL文字列に着目してニューラルネットワークで詐称サイトを識別する取り組みについて紹介しました[*14]。

DGAを機械学習で検出する試みは、既に実用化されているものも含めて、いくつかの研究が知られています。現在は、その中でもUSENIX Security '18で発表されたFANCI(Feature-based Automated NXDomain Classification and Intelligence)[*15]という手法の追試に着手しています。この手法について書かれた論文では、先行研究の知見などを基にしたドメインの特徴量とランダムフォレストと呼ばれる機械学習のアルゴリズムを組み合わせることで、高い汎化性能が得られるとされています。

追試において目指している最初のステップは、論文の手法はなるべくそのままで、データとして情報分析基盤から得られたDNSクエリデータを用いるというものです。このステップでは、情報分析基盤のデータに対して手法がそのまま適用できるのかを見極めます。なぜなら、使用するデータが異なれば、同じ手法を用いても得られる結果が同じになるとは限らないからです。その上で、適用できないと判断した場合には原因の調査と解消を、できると判断した場合には更なる性能向上を含む実用化に向けた検討を進める予定です。性能向上の余地については、例えば近年盛んに用いられる勾配ブースティング決定木(Gradient Boosting Decision Tree)の適用や、アンダーサンプリング(Undersampling)とバギング(Bagging)を組み合わせたアンサンブル学習(Ensemble Learning)の応用が挙げられます。

ただし、情報分析基盤で処理するデータの流量が多いことから、現実的な問題として、モデルには高いスループットも求められます。モデルやワークフローの複雑化による計算量の増大と、得られる性能向上の間でバランスを取りながら、様々なチューニングを通して、最終的には異常検知の仕組みの1つとして、情報分析基盤に組み込むことを目指しています。

1.3.2 Webプロキシデータへの適用

もう1つのプロジェクトでは、Webプロキシのデータからマルウェアが発生させるC2サーバへの通信の検知を目指しています。これについては、Black Hat Europe 2018でIIJエンジニアが発表した内容[*16]を情報分析基盤のログへ適用するため、現在、検証を重ねています。なお、Black Hat Europe 2018で発表した内容については、後述する「フォーカス・リサーチ(1)〜ディープラーニングを用いたログ解析による悪性通信の検出」で解説しています。

*14 IIJ、技術レポート「Internet Infrastructure Review(IIR)」(https://www.iij.ad.jp/dev/report/iir/041/02.html)。
*15 USENIX、"FANCI : Feature-based Automated NXDomain Classification and Intelligence"(https://www.usenix.org/conference/usenixsecurity18/presentation/schuppen)。
*16 Black Hat、"Deep Impact:Recognizing Unknown Malicious Activities from Zero Knowledge"(https://www.blackhat.com/eu-18/briefings/schedule/#deep-impact-recognizing-unknown-malicious-activities-from-zero-knowledge-12276)。

プロジェクトでは、Convolutional Neural Networkという画像認識でよく利用されるディープラーニングの一種を用いて、正常通信と異常通信（C2通信）の傾向を判断します。ここで重要となるのが、学習モデルの性能とその評価です。

仮に、機械学習のモデルとして95%以上の精度（Accuracy）を発揮できるモデルがあるとしたら、一般的に性能が良いと感じられます。しかし、情報分析基盤に収集されるログの量は膨大であるため、1%に対する量は人間が目で見て処理できる量ではありません。誤検知が発生したとしても、運用上、耐えうるだけの精度を提示しなければなりません。もちろん、これは機械学習だけで実現する場合であり、機械学習以外のシステム的な処理で誤検知数を減らすアプローチも考えられます。

また、精度の他に、扱うデータセットの分布の違いにも注意しなければなりません。各種カンファレンスや学会などで発表されている優秀とされている機械学習モデルで扱うデータセットの分布と、SOCで扱うデータセットの分布の特性が異なる可能性があるため、追試をする必要があります。

以上のことから、SOCでは、機械学習モデルの追試や精度向上をはじめ、機械学習モデルを利用するシステムの全体設計や運用を考え、現状のセキュリティ業務に負荷を与えずに品質を向上させるシステムの構築に注力しています。

精度向上の試みとしては、特徴量エンジニアリングを実施しています。特徴量エンジニアリングというと、あらかじめデータ分析に基づいて有効と考えられるものを追加していくイメージが強いですが、それ以外のアプローチもあります。例えば、既にある特徴量に対して様々な統計量を計算し、その元となったデータと結合したものを学習・評価に用いるというものです。この他にも様々な手法を用いて、特徴量の追加と評価を繰り返しながら、モデルの性能を向上させていきます。

1.4 おわりに

今回は、情報分析基盤を活用した分析の概要と、2018年の具体的な観測事例、そして機械学習に対する取り組みについて紹介しました。最後に紹介した機械学習を用いたアプローチは、従来の手法では検知が困難もしくは限界があった脅威に対して、現在よりも更に検知範囲を拡大できる可能性を秘めています。これらの取り組みが実現できているのは、ひとえにお客様から頂戴した通信に関するログを同意に基づいて情報分析基盤で活用できているためです。機械学習によるアプローチは特に大量のデータを必要とすることから、情報分析基盤を通して通信ログが活用できてこその取り組みといえます。今後も、wizSafe Security SignalやIIJ SECTブログを通して脅威情報をタイムリーに発信すると共に、お客様がより安全にインターネットを利用できる社会の実現に向けて邁進します。

執筆者：
小林 智史（こばやし さとし）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター データアナリスト。

執筆者：
守田 瞬（もりた しゅん）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター データアナリスト。