「日本企業を狙う特徴的手口と効果的な対策について」

株式会社ラック
サイバー・グリッド・ジャパン
次世代技術開発センター長
小笠原　恒雄　氏

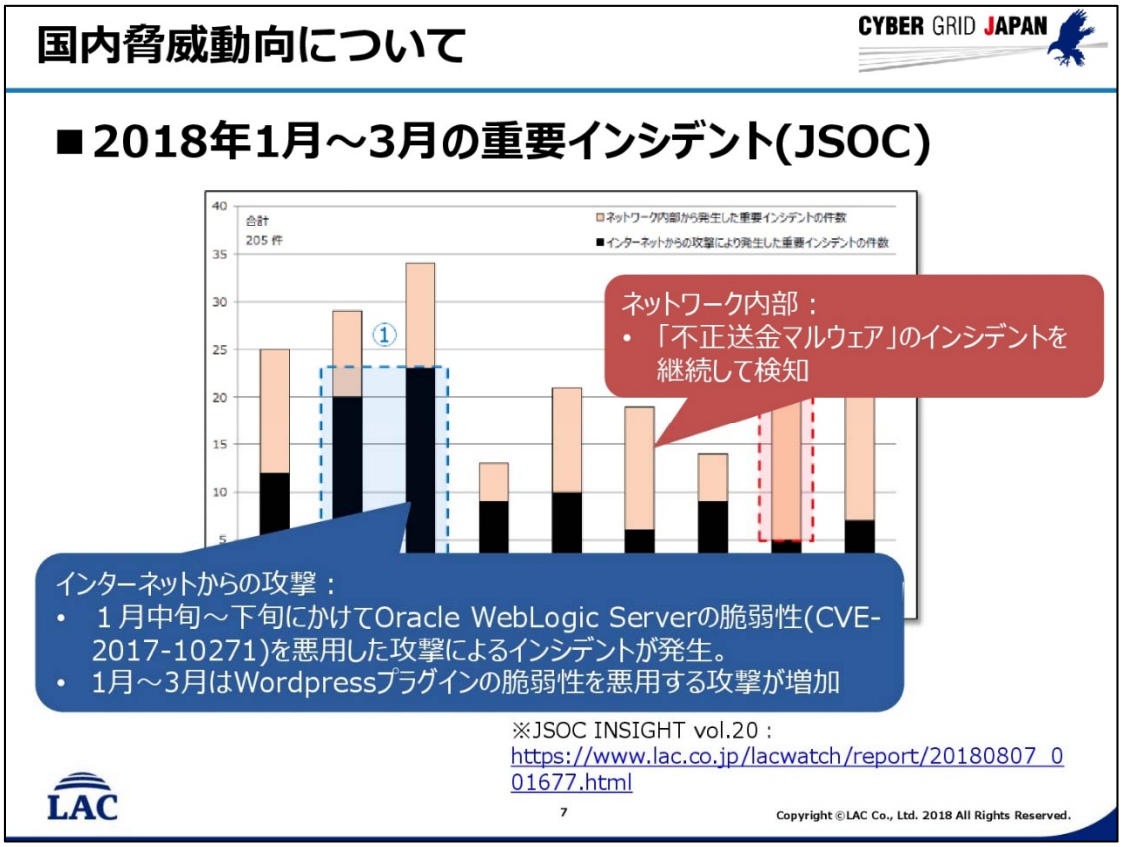
■はじめに

2001 年のラック入社後、製品サポート業務、脆弱性調査業務に従事し、ソリューションサービスの企画運用、企業のインシデント対応の支援、近年は製品評価、サイバー脅威インテリジェンスの研究開発に従事している。現在、当社では主に、①OSINT（Open Source Intelligence）、②被害観測、③脅威収集、④攻撃観測に関する脅威情報の集積と分析を行っているほか、CYBER GRID JOURNAL による情報発信、無料の自己診断サービス「自診くん」の提供、不正な IP アドレスや不正なファイルのハッシュ値といった情報を CSV 形式で MISP にインポートできるツール MISP-CSVImport の提供等を行っている。

■国内脅威動向

2015 年から 2018 年のインシデント出動傾向（当社緊急対応チームが駆けつけた事例）を紹介する。2018 年は特にマルウェア（コインマイナー）と BEC（ビジネスメール詐欺）に関する相談が相次いだ。マルウェア系のインシデントは約 4 割、サーバ不正侵入が約 3 割を占めた。

ファイアウォール、IDS、IPS、マルウェア対策製品のログ分析をしている JSOC（セキュリティ監視・運用センター）の 2018 年 1 月～3 月の重要インシデント観測結果を見ると、不正送金マルウェアのインシデントといったインターネット内部からのインシデントが多数見られた（図 1）。また、3 月にポート 445/tcp に関連するインシデントが多く発生、昨年蔓延したランサムウェア WannaCry に関するインシデントの可能性があると見ている。



（図１）

インターネットからサーバへの攻撃については、WebLogic Server の脆弱性（CVE-2017-10271）によるインシデントの発生が特徴的であった。Wordpress プラグインの脆弱性を悪用する攻撃は 2018 年 1 月～3 月に増加傾向にあるが、2018 年以前からも見られる攻撃であり、多くの企業が Wordpress を用いて Web サイトを作成しているので、自社 Web サイトの設定を再度見直して頂きたい。

現行の脅威は、①2018 年も APT（Advanced Persistent Threat：高度かつ組織的な脅威）の脅威が継続、②不正送金を目的としたマルウェア、ランサムウェア、不正マイニング行為、ビジネスメール詐欺といった金銭目的の攻撃が増加、③攻撃手口やツールが高度化する一方、自社・組織のネットワークの複雑化により対応が困難になっている点がポイントとして挙げられる。最近の標的型攻撃メールは、ピンポイントで本当に必要な宛先のみに絞って送られるものや、ウイルススキャンによる検知を困難にするために添付ファイルが本文中にあるパスワードで保護されているものなど攻撃が精緻化している。

■近年の APT の特徴

近年の APT では、マルウェア本体が送られてくるケースもあるが、Office 文書系のファイルが添付されることが多く、開封すると DLL（Dynamic Link Library）化されているマル

ウェア本体のダウンロードと実行が始まるケースがある。ダウンロードされた DLL ファイルは、正規ファイルのモジュールとしてロードされる。これは実行プロセスは正規の動作であるため、ウイルス検知しづらい手口を使っている。Office マクロの悪用以外にも、exe ファイルを作らなくてもメモリ上でマルウェアを実行させるような手口もあり、一般的なウイルス対策ソフトによる検出が困難なものが増えているといえる。また、正規の証明書を盗みマルウェアに添付することによりウイルス検知をすり抜ける正規機能の悪用、Cobalt Strike、Quasar RAT といった、既知の攻撃フレームワークを改変して悪用する事例も見受けられる。

■金銭目的の攻撃

2018 年もメールを介した金銭目的の攻撃や不正マイニング行為が急増するなど、金銭目的の攻撃が継続して流行している。メールを介した攻撃は、①感染手口が APT に近づいている不正送金マルウェアやランサムウェアなどに感染させる不正メールやフィッシング詐欺を意図する不正メール等のばらまき型メール、②フィッシング攻撃やマルウェアを用いた認証情報の窃取といったビジネスメール詐欺（BEC）が増加している。

さらに、①Coinhive を使ってブラウザ上でマイニングをする Web ベースの攻撃、②Web サイト改ざんによるマイニングスクリプトの埋め込みやサーバ不正侵入による採掘ソフトの実行、③ボットネットによる不正採掘や、ワーム拡散機能を有するマイニングマルウェアによるものなど、不正マイニング行為が急増している。

■高度化・複雑化

ある特定の遠隔操作ウイルス（RAT: Remote Access Tool）が、攻撃者からの指令を伝達する指令サーバ（C2 サーバまたは C&C サーバ）との通信に、DNS（Domain Name System）プロトコルを悪用する DNS Tunneling という攻撃手法がある。Cobalt Strike というペネトレーションテストツールは、C2 接続の通信経路を HTTP でも DNS でも容易に選択可能なため、これを使った DNS Tunneling 攻撃も確認されている。DNS のセキュリティ対策や通信ログをとっている企業は多くないと思われるため、注意が必要である。

また、標的型攻撃に Microsoft RDP、RMS、Team Viewer といった正規の遠隔操作ツールを悪用する事案や、日本企業を標的としたランサムウェア「ONI」を使用した金銭目的の攻撃グループが「Ammyy Admin」を使用、標的型攻撃の手法を取り入れた手口など、近年の攻撃は高度化、複雑化している。

Wordpress プラグインを対象にした攻撃を見ると、攻撃通信の宛先ディレクトリが異なっており、新しい脆弱性のみを選択しているのではなく、既知の脆弱性も含めて攻撃対象としていると思われる。

2017 年 5 月に大規模なサイバー攻撃が行われた WannaCry は、1 年経過した現在でも感染報告がある。SIM カード付きの PC でパッチを当てていない場合、グローバル IP アドレ

ス経由で感染し、組織内のネットワークで感染被害が拡大するので注意が必要である。Personal Firewall 機能があるウイルス対策ソフトもあるが、社内でプリンターやファイルの共有を許可するように設定するとポート 445/tcp がオープン状態になってしまうものもある。通常ポート 445/tcp は境界ではブロックされているので容易には感染しないが端末に直接 IP アドレスが振られているような場合には感染してしまう。

当社は、モバイル PC やルーターのネットワークに危険な設定がないか簡易診断できる「自診くん」https://jisin.lac.co.jp/というツールを公開しているので是非自社の設定を確認して頂きたい。

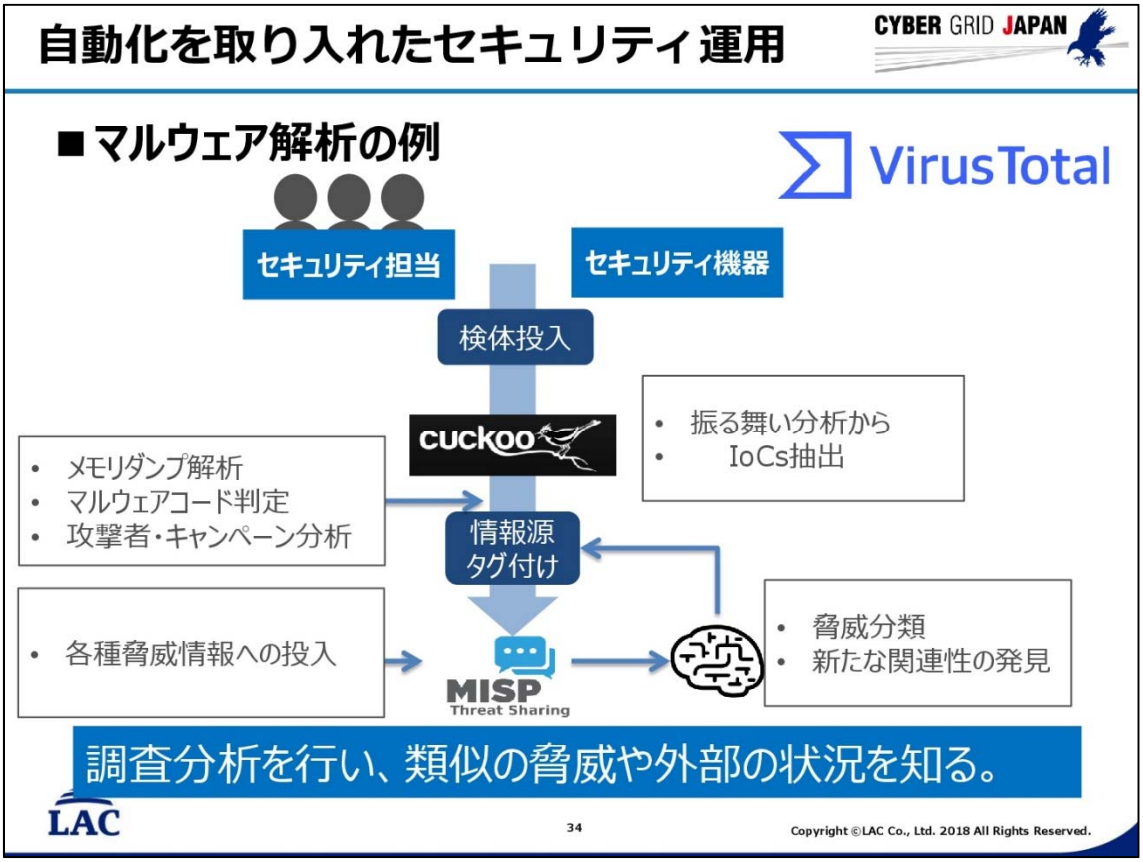
■今求められるセキュリティ対策

セキュリティ・パッチをあてる、アクセス・コントロールをする、認証をかけるという一般的な対策に加えて、①セキュリティ機器に依存せず、正規の機能や通信経路からいかに不正行為を見破ることができるかという、分析・検知能力の向上、②自社・組織のセキュリティ対策に注意を払うだけでなく、外部の脅威にもアンテナを張るよう対応範囲の拡大、③「脆弱性」「脅威」「リスク」を把握し、すぐセキュリティ対策に活かすセキュリティ耐性を備えた体制が、セキュリティ対策をする上で必要なポイントである。そうはいっても、人的リソース不足や技術スキルの課題などさまざまな課題がある中で、やるべきことが増えている。そこで、自動化によるセキュリティ対策を推進する手段の 1 つとしてサイバー脅威インテリジェンスの活用を提案する。

■サイバー脅威インテリジェンス

これからの CSIRT に求められるものは、被害（インシデント）を確認して対応するレスポンスから、未知の脅威を検出するプロアクティブなものへと変わってきている。しかし、一般的な企業でマルウェア分析の専門家を雇い入れて日々社外のインシデントも含めたマルウェア分析をするというのは一般的ではない。

少ないリソースの中でも脅威に関する情報を収集し、被害や攻撃の内容を分析し、レジリエンスを強化することが重要になっている。サイバー脅威インテリジェンスとは、「サイバー攻撃」という脅威に関する情報を集約・蓄積し、分析によって知見（＝インテリジェンス）を得て、セキュリティ対策に活かす取り組みのことである（図 2）。Abuse.ch が運用する URLhaus や、Open Threat Intelligence Community の IoC 共有コミュニティ AlienVault などにより脅威情報の投入をより充実化させることも可能である。また、マルウェアのコードを自動的に判定するツール Code Reuse Detection System もあるため、こうした外部のソリューションを活用し、自動化を推進してセキュリティ耐性を向上することも有効な手段の 1 つであろう。


自動化を取り入れたセキュリティ運用
CYBER GRID JAPAN
■マルウェア解析の例
VirusTotal
セキュリティ担当
セキュリティ機器
検体投入
cuckoo
• メモリダンプ解析
• マルウェアコード判定
• 攻撃者・キャンペーン分析
• 振る舞い分析から
• IoCs抽出
情報源
タグ付け
• 各種脅威情報への投入
MISP
Threat Sharing
• 脅威分類
• 新たな関連性の発見
調査分析を行い、類似の脅威や外部の状況を知る。
LAC
34
Copyright ©LAC Co., Ltd. 2018 All Rights Reserved.

（図 2）