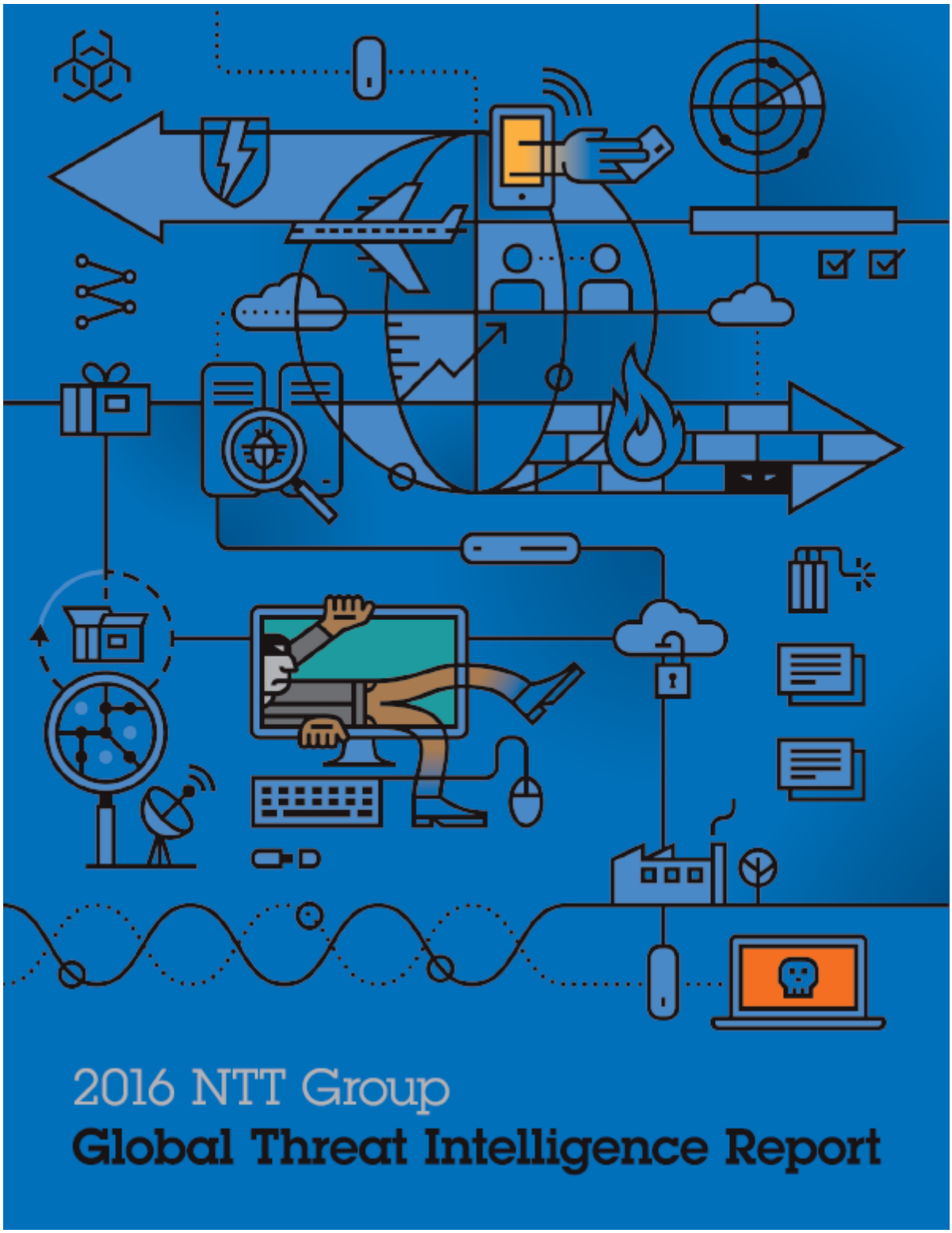


（日本語版）

目次

エグゼクティブサマリー 5

NTT グループ 2016 年グローバルスレットインテリジェンス報告書 5

主な調査結果 6

地理的・垂直的な市場動向 6

脆弱性、攻撃とエクスプロイト 6

インシデントレスポンス及び事例研究 7

グローバルデータ分析と調査結果 8

攻撃の情報源 9

業種ごとの攻撃 12

攻撃の類型 14

脆弱性サマリー 16

マルウェアの考察 19

Exploit Kit Summary エクスプロイトキットのサマリー 20

サイバーキルチェーンに対するセキュリティ対策の実用的な適用 26

ケーススタディ概要 27

サイバーキルチェーンフェーズ 1 ：偵察（Reconnaissance） 29

ケーススタディ時間軸、観察と影響 29

サイバーキルチェーン考察 29

ピンポイント対策 30

サイバーキルチェーンフェーズ 2 ：武器化（Weaponization） 33

ケーススタディ時間軸、観察と影響 33

サイバーキルチェーン考察 33

ピンポイント対策 34

サイバーキルチェーンフェーズ 3 ：配送（Delivery） 36

ケーススタディ時間軸、観察と影響 36

サイバーチェーン考察 36

ピンポイント対策： 36
サイバーキルチェーンフェーズ４－エクスプロイト（Exploitation） 39
ケーススタディ時間軸、観察と影響 39
サイバーキルチェーン考察 39
ピンポイント対策....40
サイバーキルチェーンフェーズ５：インストール（Installation） 43
ケーススタディ時間軸、観察と影響 43
サイバーチェーン考察....43
ピンポイント対策....44
C サイバーキルチェーンフェーズ６遠隔操作（Command and Control (C2)） 47
ケーススタディ時間軸、観察と影響 47
サイバーキルチェーン考察 47
ピンポイント対策....48
サイバーキルチェーンフェーズ 7:目的実行（Actions on Objectives） 50
ケーススタディ時間軸、観察と影響 50
サイバーキルチェーン考察 50
ピンポイント対策....51
PPFC ケーススタディ：結論 52
インシデントレスポンス：傾向が示す組織の対応不足....53
不十分な投資と準備不足が未だに主な原因である....53
インシデントレスポンスのタイプ....54
垂直的市場によるインシデント 55
インシデントレスポンス例: Emdivi....56
インシデントレスポンス推奨事項....57
スレットインテリジェンスにおけるサイバーキルチェーンの役割 59
スレットインテリジェンスディベート....59
関連付けられたスレットインテリジェンスと CKC....60
外部のスレットインテリジェンス情報源 60

属性の重要性 61
スレットインテリジェンス：サマリー 61
グローバルハニーネット分析 62
攻撃カテゴリ 62
攻撃元となっている国 64
プロバイダー 64
ASNs (AS 番号) 65
識別子 65
IP アドレス 66
地政学的考察 67
グローバルハニーネット：サマリー 67
アンチサンドボックス技術―なぜあなたのボックスが静かなのか？ 68
サンドボックスの特徴 68
アンチサンドボックスの技術の分類 69
アンチサンドボックス例 70
例１：タイムボム 70
例２：GUID ボリュームチェック 70
例 3: Sleep Duration Shortening Detection 70
推奨事項 71
サンドボックス開発者 71
サンドボックスユーザーに対するヒント 71
NTT グループのリソース情報 72
Solutionary について 72
Dimension Data について 72
NTT Com Security について 72
NTT Innovation Institute について 73
NTT Secure Platform Laboratories について 73
NTT-CERT について 73
ＮＴＴのグローバルデータ分析手法 について 73
Wapack Labs について 74

Recorded Future について 74
Lockheed Martin について 74
The Center for Internet Security について 74
用語解説 75

エグゼクティブサマリー

NTT グループ 2016 年グローバルスレットインテリジェンス報告書

あらゆる組織が、セキュリティ予算と資源を如何に最適に割り当てるべきかという決断を日々求められている。マルウェア、攻撃そして技術の進歩に伴い、その状況は複雑になっていくばかりである。真にセキュリティ対策を進歩させ、限りある資源をより効果的に運用するには、細かな問題への個別の解決策ではなく、インフラ全体に行き渡った包括的な解決策が必要なのである。防御策を考え抜くことが重要なのである。包括的、統合的かつ一体的な解決策は効率性や効果をもたらすばかりでなく、組織全体のセキュリティライフサイクルの確立に寄与すると我々は考えている。

本年の GTIR は、「Lockheed Martin サイバーキルチェーン（CKC）」をベースとし、各フェーズで有効となる対策を特定するために、「Center for Internet Security」の「クリティカルセキュリティコントロール」を利用している。CKC の各フェーズに対する対策を確立することで、あらゆる組織は攻撃を阻止する能力を強化できる。我々は、サイバーキルチェーンに対する実用的なセキュリティ対策について一章を割き、ケーススタディを紹介している。

攻撃者が今何をしているのかを検知し、有効なセキュリティ対策をするためには、現在の脅威（攻撃）の状況がどうなっているかを理解することが重要である。脅威環境の現状を理解しやすくするために、本年のグローバルデータ分析と調査結果の章において攻撃者の活動のサマリーを、グローバルハニーネット分析の章において広い見地からの考察を、それぞれ明示した。

攻撃者が今何をしているのかを検知し、有効なセキュリティ対策をするためには、現在の脅威（攻撃）の状況がどうなっているかを理解することが重要である。

セキュリティ対策の最終目的は、組織や環境の回復力と生存能力を強化することにある。奇妙なことに、マルウェア開発者は同じような目的を有している。アンチサンドボックス技術の章では、マルウェアがそれ自体の能力として回復力と生存能力をどのように組み込んでいるかに焦点を当てている。

スレットインテリジェンスにおけるサイバーキルチェーンの役割の章では、アクティブなスレットインテリジェンスプログラムが組織のセキュリティ対策全体にもたらすインパクトの重大さについて論じている。そのプログラムには、データや情報、インテリジェンスを適切に取扱い、それらインテリジェンスを現在の環境に活用・反映する方法も含んでいる。

GTIR が４年目を迎えたこともあり、ＮＴＴグループは、いくつかの重要な協力企業の調査結果を取り入れて、脅威の実態を多角的に分析した。我々は、ご協力頂いた Lockheed Martin、Wapack Labs、Recorded Future そして Center for Internet Security に感謝の意を表す。

我々は、ＮＴＴグループ２０１６年グローバルスレットインテリジェンス報告書が示唆に富み、皆さんのお役に立つことを願っている。ご一読頂き、ありがとうございます。

主な調査結果

地理的・垂直的な市場動向

2016 年 GTIR では、 NTT グループは、顧客に対する脅威及び、業種間・地域をまたがったハニーネットを評価対象とした。

- 小売業は、顧客単位で見ると、全業種の中で最大の攻撃対象となった。小売に次いで、サービス、レジャー、エンターテイメント、そして保険、政府、製造が続いた。小売業の顧客では、金融の顧客の 2.7 倍の攻撃数を検知した。
- 2015 年に検知された攻撃のうち、米国拠点の IP アドレスが 65%を占めた。米国は、2015 年、NTT グループによって観察された攻撃元 IP アドレスの最大の発生源のままで、2013 年から 49%、2014 年から 56%増加している。米国拠点の攻撃とは、攻撃者が必ずしも米国にいるという意味ではない。米国外にいる攻撃者は地理的な IP ブロッキングを避けるために、米国のインフラを利用しているのである。
- 米国本拠以外の攻撃のうち、3 つの拠点―イギリス及びトルコ、中国―が 38%を占めた。残りの 62%は、199 の国々からの攻撃である。
- NTT グループは、教育以外のすべての産業においてマルウェア検知の 18%の増加を観測した。NTT の教育業界の顧客は不特定多数の学生やゲストが接続するネットワークにはあまり注力しない傾向があった。しかし、他の分野でのマルウェアは増加した。

脆弱性、攻撃とエクスプロイト

2015 年の脆弱性と攻撃を詳細に分析することによって、何が顧客の環境に潜んでいるかや何を攻撃者が利用しているかが明らかとなった。

- クライアントネットワークで検知された脆弱性のほぼ 21%は 3 年以上潜んでいたものであった。12%以上は 5 年以上で、5%以上は 10 年以上だった。更に、分析結果には、1999 年よりもはるか前、16 年以上経つ脆弱性も含まれていた。この脆弱性は共通脆弱性評価システム（CVSS）において 4.0 又はそれを超えるスコアだった。
- トップ 10 の外部脆弱性は、識別可能な外部脆弱性のほぼ 52%を占めた。何千もの脆弱性が他の 48%を占める。
- トップ 10 の内部脆弱性は、2015 年の内部脆弱性全体の 78%以上を占めた。10 の全ての内部的脆弱性は、標的システム上の期限切れのパッチレベルと直接関係がある。
- 2015 年にエクスプロイトキットが標的にしたトップ 10 の脆弱性は全て Adobe Flash と関係があった。2013 年には、エクスプロイトキットが標的にしたトップ 10 の脆弱性は、1 つが Flash 及び 8 つが Java の脆弱性であった。新しい Java 脆弱性は 2013 年以来着実に減ってきたので、その状況は変わった。公表された Flash 脆弱性の数は 2014 年のレベルからほぼ 312%急上昇した。
- ブルート・フォース攻撃は、2014 年レベルから 135 パーセント急上昇した。全顧客に対し、年間を通じて 75 の異なる国から SSH ブルートフォース攻撃があったことを、NTT グループは検知した。
- DoS/DDoS 攻撃の量は、2014 年に観測されたレベルから 39%減少した。より良い対応ツールの導入と攻撃数の減少が相俟って、サービス妨害攻撃（DoS）と分散型サービス妨害攻撃（DDoS）の検知減少に繋がった。しかし、DDoS 攻撃を回避又は停止させるために攻撃対象に支払いを強要する恐喝がより表面化してきた。

- 2015 年、ウェブアプリケーション攻撃の 24%はインジェクションベースだった。これは、ウェブアプリケーション攻撃の 26%がインジェクションベースという 2014 年から引き続きの傾向にある。インジェクション攻撃は遠隔からのコマンド実行を許し、データの不正転送に繋がっていく。
- NTT グループのグローバルハニーネット上では、1 日当たり平均 128,000 回の攻撃があり、SMB、NetBios 及び Samba に関する攻撃が最も多かった。ハニーネットデータには、372,000 以上のユニークな IP アドレスから約 1 億 500 万の事象が含まれていた。SSH、HTTP、SQL そして VoIP(SIP)もトップ 5 の攻撃に寄与した。

インシデントレスポンス及び事例研究

- インシデントレスポンスの 22%は、小売り垂直市場の顧客ベースから派生しており、続いて僅差の 18%で金融の垂直市場が 2 位となっている。小売に対する攻撃の多くはスピアフィッシング攻撃関連であった。
- 過去 3 年にわたるインシデントレスポンス支援活動のトレンド・データは、サイバーインシデントに効果的に対応できるのは、平均すると 23%の組織のみに限られるということを示している。77%は、重大なインシデントに対応する能力を有さず、しばしばインシデントが生じた後にインシデントレスポンスサポートを契約している。
- スピアフィッシング攻撃は、2015 年に実施したインシデントレスポンス活動のおよそ 17%を占めた。スピアフィッシングは、2014 年の 2%以下から劇的に増加した。
- PCI 準拠を求められた顧客に対する遠隔操作（C2）活動は、PCI 非準拠に対する C2 活動の半分強に過ぎなかった。PCI 準拠を求められた顧客は、PCI 非準拠の顧客より 57%少ない C2 トラフィックを観察する傾向にあった。
- マルウェア及び DDoS 関連の攻撃は、前年と比較してより少ないインシデントレスポンスサポートを必要とした。マルウェアに特化した対応活動は約 33%、DDoS は 12%減少した。我々は、インシデントレスポンスにおいてだけでなく、ログや事象モニタリングにおいても、DDoS 活動が全体的に減少していると見ている。

グローバルデータ分析と調査結果

この章では、２０１５年にＮＴＴグループのセキュリティ会社によって収集された世界中の攻撃データの分析について紹介する。この分析は、ログ、攻撃、インシデントと脆弱性に関する顧客からのデータと、我々の運用サービスとは異なった環境で稼働する我々のグローバルハニーポットとサンドボックスを含む NTT グループの研究リソースに基づいている。これにより我々は、利用可能なデータを異なった視点から考察することが可能となる。本年の GTIR は、Lockheed Martin、Wapack Labs、Recorded Future と Center for Internet Security を含む我々のいくつかの重要なパートナーからの貴重な考察を含んでいる。各組織は、我々の考察上のデータとセキュリティ問題に対してユニークな見解をもたらしている。これら組織の協働により、本年の分析結果は過去最良のものとなっている。

オペレーションの間に、NTT グループは、セキュリティログ、アラート、イベントと攻撃情報を収集し；それらを分類整理し；そして整理されたデータを分析する。 ＮＴＴグループは毎年何兆というログと何十億という攻撃を処理する。 我々の顧客基盤の広さと多様性により、これらのデータは、ほとんどの組織が遭遇する脅威を代表するものとなっている。

この章で示されたデータは、２０１５年に認知された攻撃に関連したログイベントから得られている。生のログデータやネットワークトラフィック量ではなく、認知された攻撃イベントを使用することにより、攻撃実態がより鮮明に浮き上がってくる。ＮＴＴグループは２０１５年を通じ、非標的型ネットワーク偵察トラッフィックと DDoS 活動を大量に観察した。攻撃イベントの積極的な分析と類型化が為されなければ、実際に発生するこのような攻撃実態を正確に捉えることはできない。

この分析結果を示すために、グローバルなデータ分析と調査結果が関連する章で紹介されている。

1. アタックの情報源 – 観察された顧客に対する攻撃の発生国の分析
2. セクタによる攻撃 – 関連業種の顧客に対する攻撃の分析
3. 攻撃のタイプ – 顧客に対して使われた攻撃のタイプの分析
4. 脆弱性サマリー – 顧客の環境で観察された脆弱性のタイプと発生年の分析
5. マルウェア観察 – 顧客の環境で観察されたマルウェアの分析
6. エクスプロイトキットサマリー – 顧客の環境で観察されたエクスプロイトキットとその挙動の分析

グローバルなデータ分析の章の最大の価値は、それが実際の顧客の環境で観察された詳細に基づいていることである。これは、ラボや逸話から集められたデータではなく、実際の組織で１年を通じて観察された実際のログ、イベント、脆弱性と攻撃なのである。

攻撃の情報源

図１に示されるように、ＮＴＴグループの顧客基盤に対して検知された攻撃の６５パーセントが米国内の IP アドレスからとなる。これは、ＮＴＴグループが過去数年にわたって観察した傾向を引き継いでいる。 過去の分析では、２０１３年には４９%の攻撃が、２０１４年には５６%の攻撃が、米国内からとなっていた。インターネットの利用と接続率が米国で上昇しており、それがこの増加の一因となっているが、攻撃の増加率は現在のインターネットの成長を上回っている。

年	アメリカからの攻撃%	前年度からの上昇率（% ）
2013	49%	
2014	56%	14%
2015	65%	16%

図１．アメリカにおける攻撃ソース

準備のし易さ、安いコスト、米国基盤の高品質なクラウドホスティングサービスのために、敵対的活動の主要発生源としての米国の歴史は継続している。検出された相当数の攻撃が米国の顧客を標的にしており、つまり、攻撃者はこのような攻撃をローカル、被害者と同じ地理的領域で、敢行する傾向にある。これらの攻撃の多くが真に米国内から行われていると判明しており、おそらく攻撃者は、没頭する攻撃者を探し出して止めようとする行為への対抗心もあり、彼らの居場所をさほど気にしていないことを示している。

発信源 IP アドレスが米国内にあるのに対し、実際の攻撃者は世界中のどこにでもいることができる。攻撃者が IP アドレスを容易に隠すことができるため、攻撃の情報源は、しばしば、攻撃が実際に行われている場所というよりは、むしろ攻撃者が位置している国、又はおそらく攻撃者が踏み台サーバや借りているサーバの場所を明示すことがある。

図２で見られるように、２０１５年には、トップ５の攻撃発信源国が、すべての識別された攻撃の８１%を占めた。

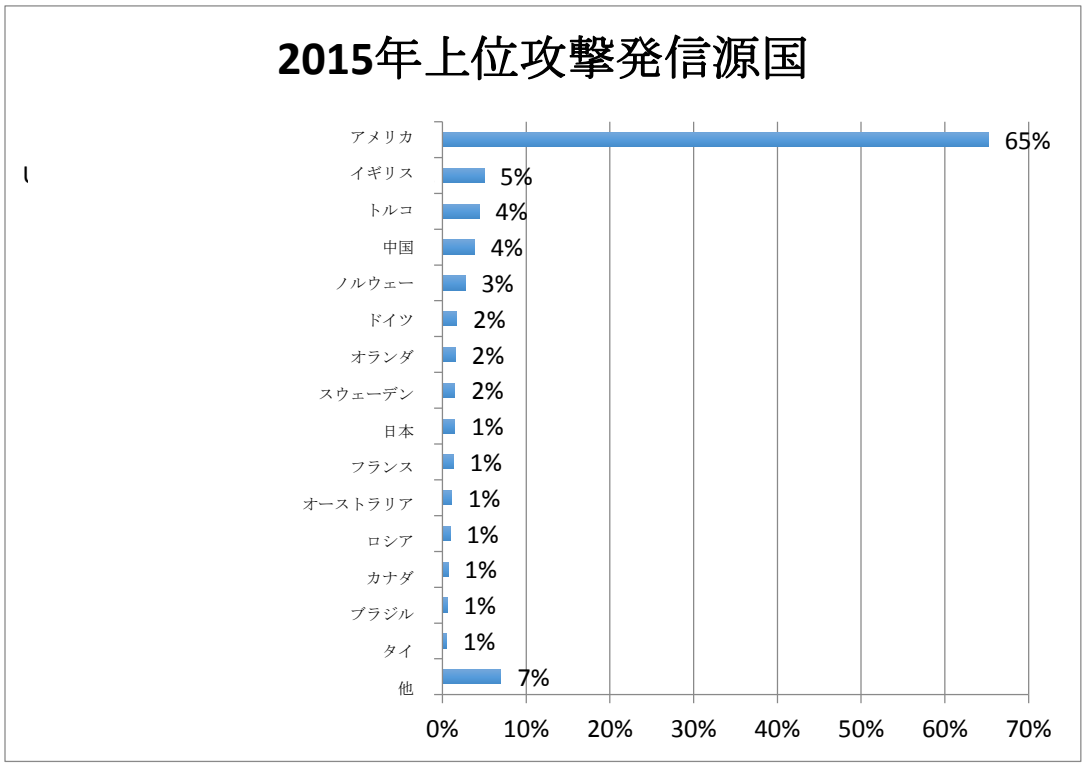


図２：攻撃発信源国, 2015

２０１５年に、英国（ＵＫ）に本拠地を置くアドレスからの攻撃が少し増え、他方中国内のアドレスからの攻撃が減少し、ＵＫは非アメリカベースの攻撃のナンバー１の発信源になった。図３で提示されるように、米国外が発信源の攻撃の３８％がトップ３の発信源国からの IP アドレスとなっている。トップ 10 発信源国以外では、発信源 IP アドレスの分布は均一だった。ＮＴＴグループは２０１５年に合計２１７の異なった国から攻撃を検出した。１９７の国が攻撃の１％以下を占めていて、「その他」の分類に含まれている。

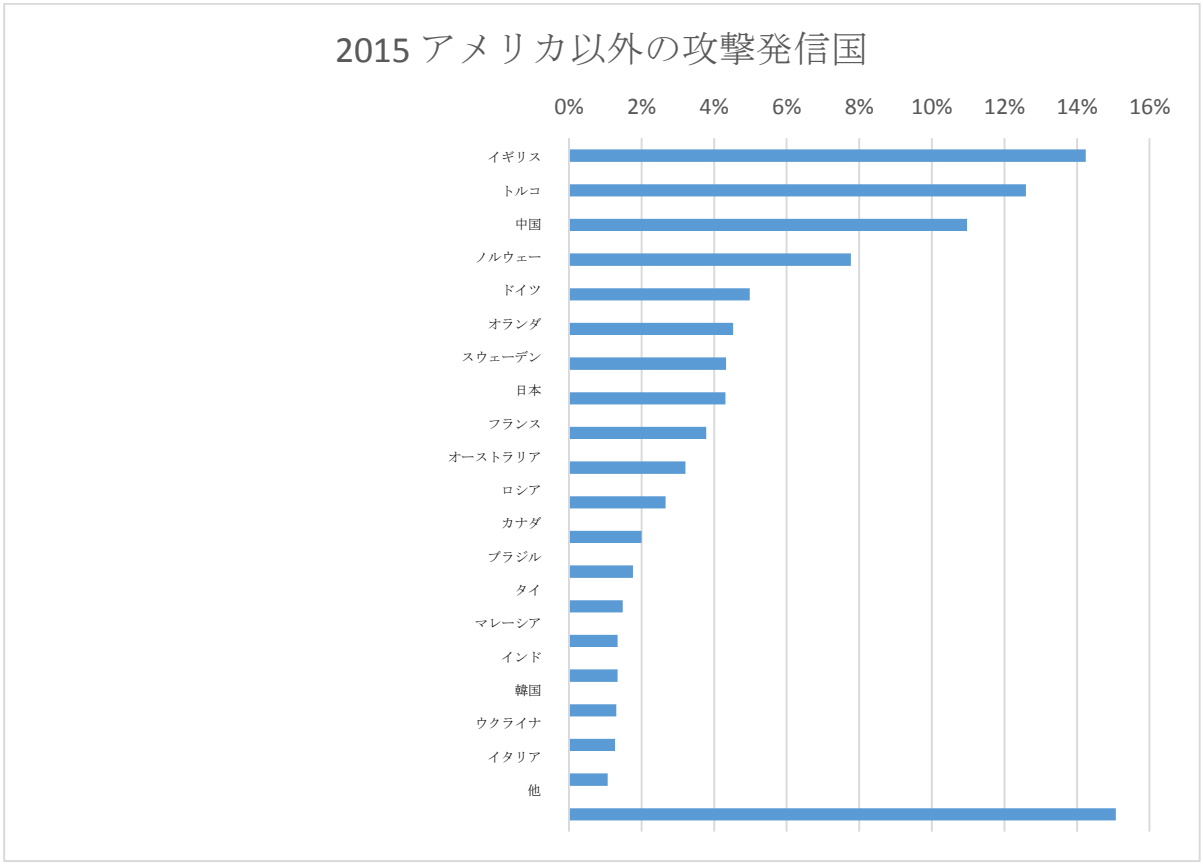


図３：アメリカ以外の攻撃発信国 2015

業種ごとの攻撃

図４がＮＴＴグループの業種ごとの顧客分布を示している。

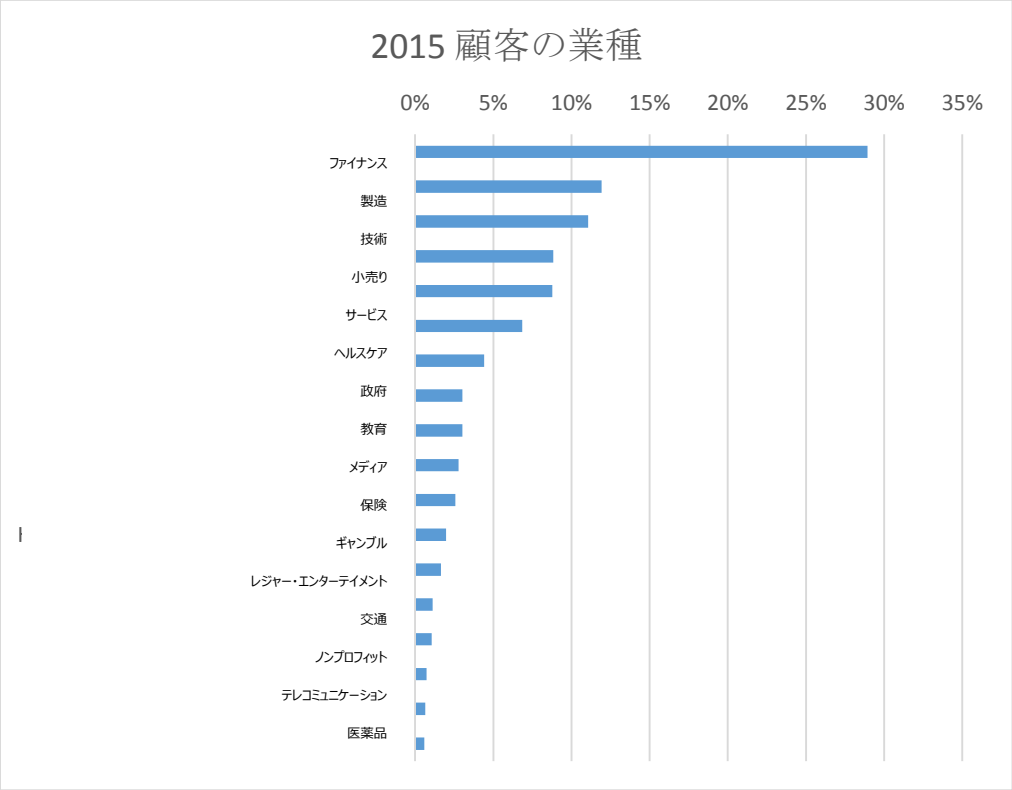


図 1: NTT グループの業種ごとの顧客分布 2015

図 5 は、以前の NTT グループの報告とは異なる方法で攻撃データを表している。2015 年のデータに関しては、NTT グループは、業種ごとの攻撃量を当該業種の顧客数で除すことにより攻撃データを平準化した。その結果、金融業が全業種中で最高の攻撃数を示したが、それは NTT グループが他の業種よりも金融業の顧客を最も多く有しているからである。各業界の顧客数を考慮して攻撃数を平準化した結果、小売業が顧客単位の攻撃数で最も高い 11%弱という数値（金融業の顧客のほぼ 3 倍）を示した。

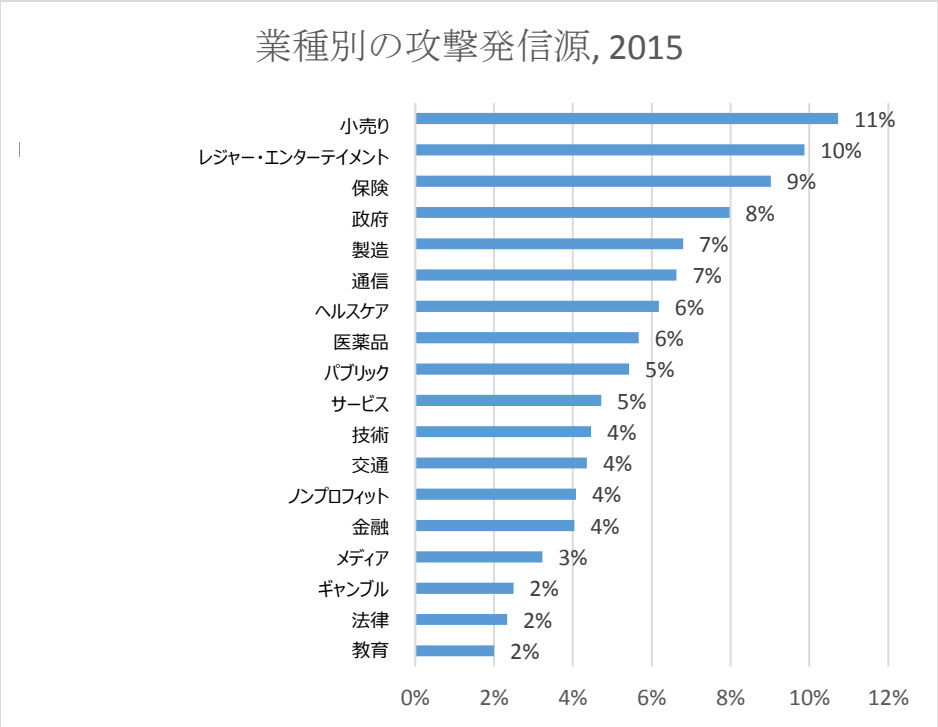


図 2: 業種別攻撃発信源

小売業者は依然として格好の標的となっている。小売業者は、しばしば多くの最終利用者や様々なサービス用のデバイスとのやり取りを通じて、クレジットカード情報を含む大量の個人情報を取り扱う。この多様性を帯びた環境が防御を困難にしている。

2015 年中、NTT グループは、サービス、レジャー、エンターテインメント業に関連する攻撃の増加も観察した。この業界も小売業と同様の問題に直面しており、クレジットカード情報を含む大量のセンシティブな情報を処理している。ホテルやリゾートを含むサービス業におけるトランザクションはかなりのボリュームになってきており、これらのカード番号を漏洩させる行為は、攻撃者にとってより魅力的なものに映る結果となっている。サービス業は、非常に多くのロイヤリティープログラムも有し、より多くの個人情報を抱えることとなっている。この業界は 2015 年に注目を浴びた Starwood Hotels & Resorts, the Trump Hotel Collection, Hilton Worldwide, Mandarin Oriental and White Lodging Services Corporation を含むいくつかのセキュリティ侵害の犠牲になった。

Oriental and White Lodging Services Corporation の例を挙げる。多くのセキュリティ侵害が、宿泊施設に関するサービスを提供するプロバイダーと小売業者に対して向けられた POS マルウェアに関係していた。最終的には、施設の情報セキュリティ対策を直接標的とせず、同じ顧客を標的としている。

保険業と政府機関は、双方とも 2015 年における最も攻撃を受けた業種トップ 5 にランクされた。製造業は、前年の状況を踏襲しつつ、重大な攻撃を検知し続けた。全体としては、トップ 5 業種に含まれる顧客は、2015 年に NTT グループによって観察された攻撃の 44%超を経験した。

I 業種ごとのサイバー攻撃：Recorded Future の考察

Recorded Future は、インターネット上での価値ある脅威データの収集を容易にし、自動化するツールを含め、様々なセキュリティ情報とセキュリティ情報サービスを提供している。

Recorded Future は、"リファレンス数（当該業種がサイバー攻撃という文脈で話題にされた回数）"を分析することにより各業種に対する攻撃に関連したインターネットトラフィック量を評価した。図 6 に示す通り、Recorded Future のデータは各業種に対する攻撃数が年間を通じて上下していることを示している。2015 年 1 月、9 月そして 10 月は、インターネット上でのサイバー攻撃の話題数がピークだった。1 月、キーとなるイベントとしては、製造会社に対する攻撃と、それに引き続いて起こったテクノロジー業へのセキュリティ侵害を含んでいた。9 月と 10 月の増加は、金融業における重大なセキュリティ侵害に加えて、有名なテクノロジー小売業者に関するマルウェアの影響によるものと（部分的には）みられた。Recorded Future は、NTT グループの検知と比較しつつ小売業に対する活動をトラックしており、小売業が最も標的となる（話題となる）業種の一つと位置づけた。

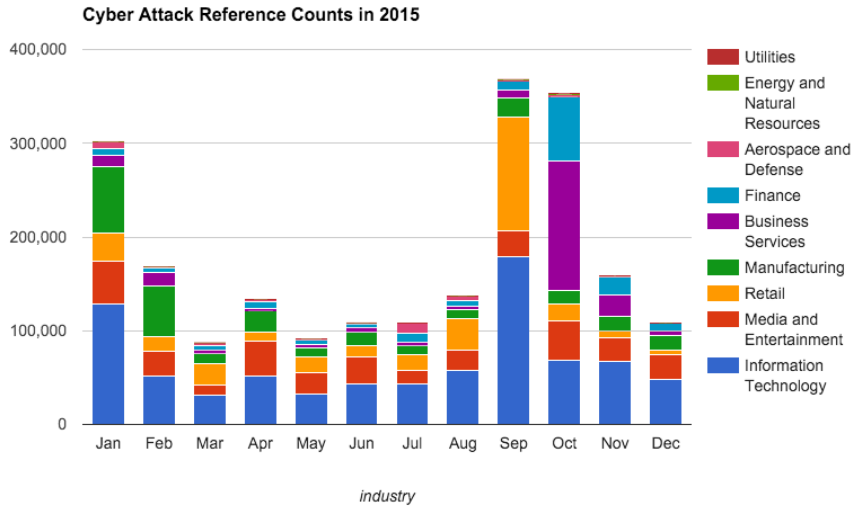


図 3: サイバー攻撃のレファレンス数, 2015

攻撃の類型

2015 年の分析は、検知された攻撃の類型に変化が生じてきていることを表している。特別なアクセス権限によるアクセス敢行、エクスプロイトソフトウェアその他通常ではない活動を含む異常活動が、2014 年における全体の攻撃の 20%から 2015 年には 36%に上昇している。ウェブアプリケーション攻撃が、2 番目に高い攻撃量となった。

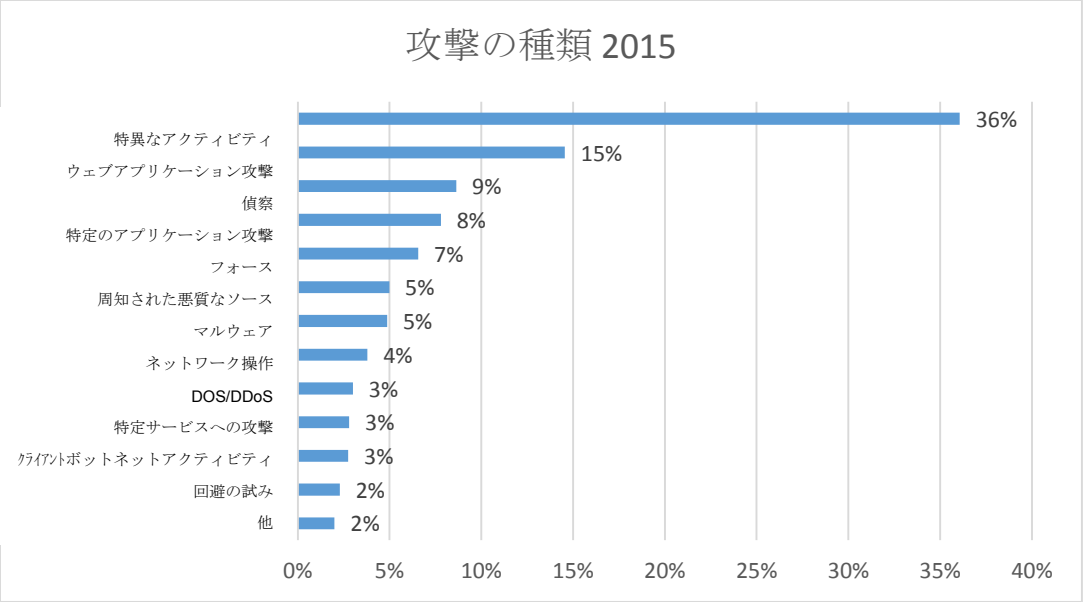


図 4: 攻撃の種類 2015

マルウェアの検知は 2015 年に次第に増加し、第 4 四半期だけで 6%の上昇を見せた。振り返ると、マルウェアは 2014 年には 2%以下の攻撃だったのが 2015 年には 5%に増加している。この増加は、特定のキャンペーン、マルウェア又は発生源によるものではなく、年間を通じてほとんどのマルウェアの類型が増加したことによる。

ブルートフォース攻撃は、2014 年の 2%以下から 2015 年にはほぼ 7%に増加した。ブルートフォース攻撃量は 2014 年レベルの 135%に増大した。年間を通じて、NTT グループはその全ての顧客基盤にわたり、75 の発生源国から SSH ブルートフォース攻撃を検知した。

2015 年における顕著な減少は、DoS/DDoS 攻撃量の 39%ダウンが挙げられ、2014 年における攻撃の 5%から 2015 年には 3%へと低下した。この減少は、一連のイベントの結果であることが分かる。第一に、攻撃者は、前年に比べて 2015 年には単純に Dos/DDoS 攻撃をほとんど実施しなくなった。第二に、2015 年は、より効果的な DoS/DDoS 対応技術とサービスの採用が見られた。インシデントレスポンス：傾向が示す組織の対応不足、というタイトルの章で示しているように、NTT グループにおいても DoS/DDoS インシデントレスポンスへの従事数は減少する結果となった。

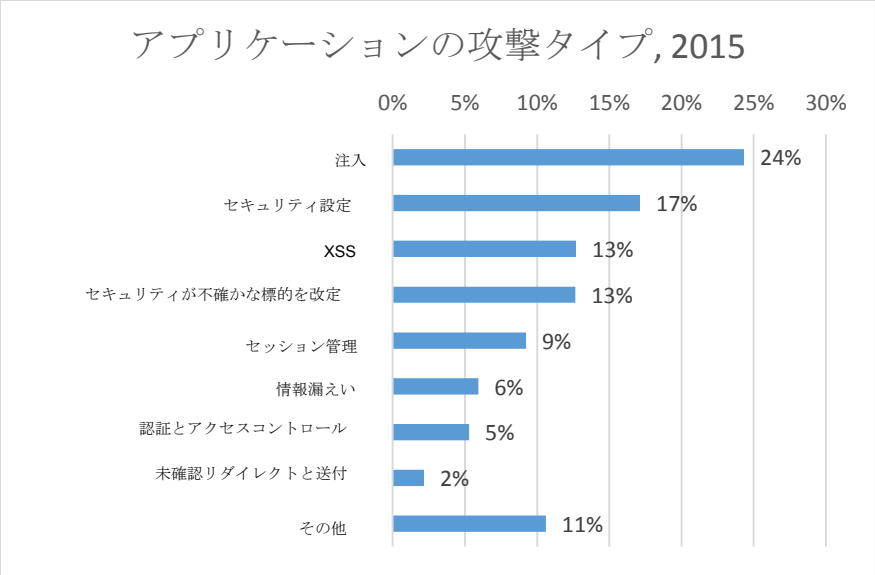


図 5:アプリケーション攻撃に対する脆弱性のタイプ

多数のウェブアプリケーション攻撃を考慮し、NTT グループは追加の分析を行う道を選択した。ウェブアプリケーション攻撃は、組織のインターネットとの接続点におけるアプリケーションに対する攻撃を映し出している。図 8 はこの分析の結果を表している。

2015 年に観察されたウェブアプリケーション攻撃の 24%は PHP コマンドインジェクションや SQL インジェクションのようなインジェクション型の攻撃であった。これは、"インジェクション"が脅威のトップとなっている OWASP(Open Web Application Security Project)のトップ 10 ウェブアプリケーション脆弱性リストと直接的な相関関係を示している。それはまた、2014 年に検知された 24%から大きく変化していない。

脆弱性サマリー

NTT グループは、サービス提供している全業種と地域的領域の顧客から 2015 年脆弱性データを集積した。脆弱性の結果は、広範囲にわたるスキャンデータと Qualys、Nessus、Saint、McAfee、Rapid7、Foundstone と Retina を含む複数のスキャンベンダーの製品からの情報を含んでいる。観察結果は、指定された共通脆弱性評価システム (CVSS) スコア 4 又はそれ以上を用いて実施した、全ての脆弱性の分析に基づいている。

図 9 は、外部及び内部のスキャンを基にしたトップ 10 脆弱性を列挙している。概ね、2015 年に見られた脆弱性のタイプは、2014 の状況に呼応している。2015 年のトップ 10 の外部脆弱性は、特定された外部脆弱性のほぼ 52%を占めた。外部脆弱性は、攻撃者が標的組織の外部から観察しているものを映し出している。

外部脆弱性 Top 10	外部脆弱性（%）
期限切れ PHP Version	8%
クロスサイトスクリプト（CSS/XSS)	7%
期限切れアパッチ Web サーバー	7%
SSL/TLS 情報崩壊	6%
Web 上のクリアテキストユーザー名/パスワード	5%
脆弱な SSL/TLS 暗号/認証	5%
期限切れアパッチトムキャットサーバー	4%
脆弱な/No HTTPS キャッシュポリシー	4%
HTTP の属性セットなしのクッキー	3%
脆弱なアルゴリズムを使った SSL 認証	3%

内部脆弱性 Top 10	内部脆弱性%
期限切れ Java Version	51%
期限切れ Adobe Flash Player	11%
期限切れ Adobe Reader と Acrobat	5%
期限切れ Microsoft Windows	3%
期限切れ Microsoft Internet Explorer	3%
期限切れ Mozilla Firefox	2%
期限切れ Microsoft Office	1%
期限切れ Linux Kernel	1%
期限切れ Novell Client	1%
期限切れ OpenSSH Version	1%

図 6:外部性・内部性脆弱性 Top 10 , 2015

トップ 10 の内部脆弱性は、もっぱらパッチレベルに関係しており、2015 年において観察された全ての内部脆弱性の 78%以上を占めた。

特定された脆弱性の量とタイプを考慮することに加え、NTT グループは図 10 に示された通り、それらの発生年を評価した。

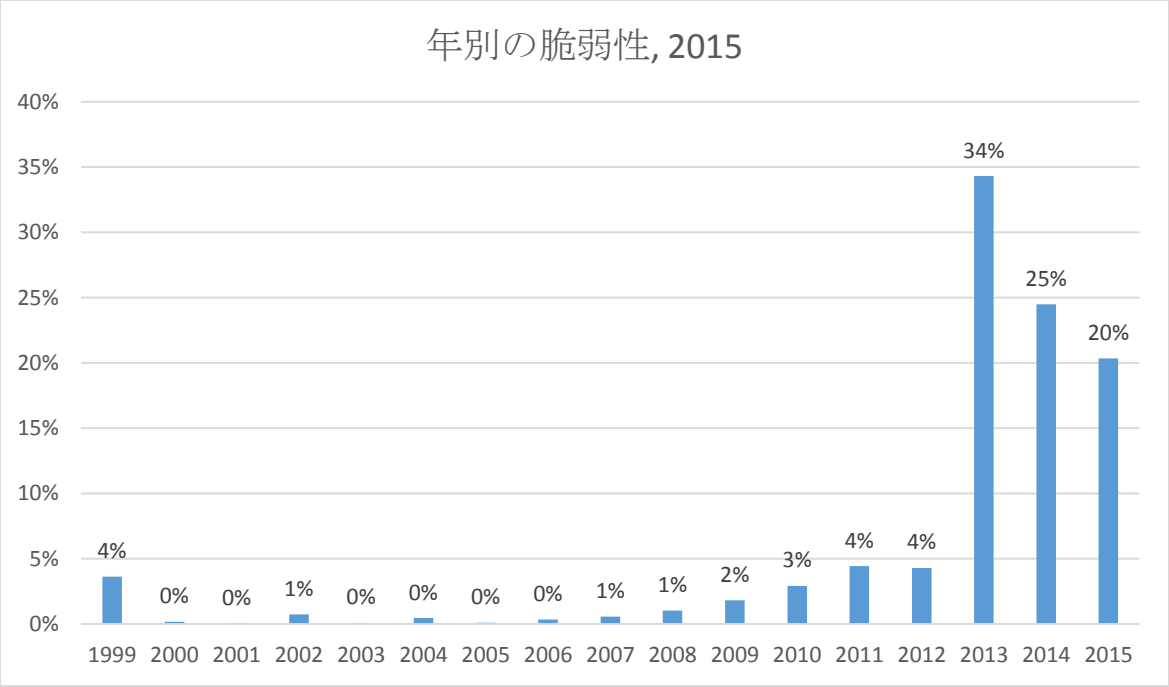


図 7: 年度別の脆弱性

特定された 79%超の脆弱性が過去 3 年以内に公開されており、それはほぼ 21%の脆弱性が 3 歳以上であったことを意味する。数年来から継続するこの古い脆弱性に関する傾向は、顧客の環境下に居座っており、観察された脆弱性の 12%以上が 5 歳以上だった。NTT グループは 16 歳の脆弱性を観察するとともに、脆弱性の 5%超が 10 歳以上だった。

脆弱性の詳細：**Recorded Future** の考察

NTT グループが 2015 年に検知した古めの脆弱性は Heartbleed と POODLE だった。2015 年以降金融業におけるいくつかの有名なセキュリティ侵害を含め、Recorded Future は金融業にて悪用された脆弱性を分析し、Heartbleed と POODLE、さらには Dyreza に結び付けられた脆弱性をトップ 3 に位置付けた。

最初は、スパム攻撃で銀行の顧客を狙った CVE-2015-0057 と CVE-2013-3660 を用いた Dyreza のアップデートバージョンが 2015 年 6 月に識別された。

一つには前年の金融業における大規模なセキュリティ侵害と関連して CVE-2014-0160（Heartbleed）が多数出現した。脆弱性の露呈後数ヶ月経った 2015 年 8 月、複数の銀行が CVE-2014-3566（POODLE)に対して脆弱と位置付けられた。

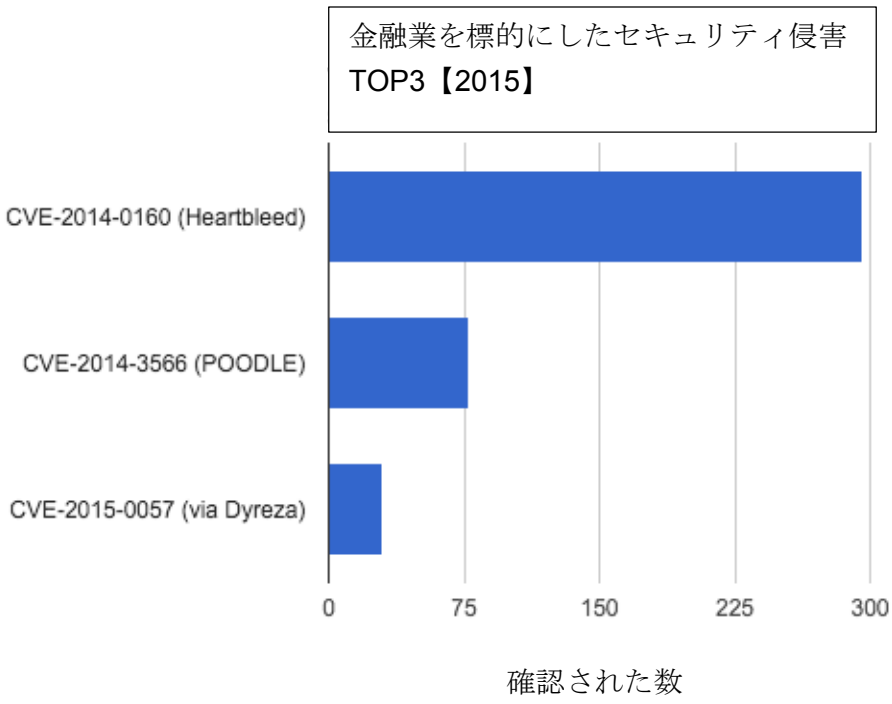


図 8: 主な金融行でのセキュリティ侵害

マルウェアの考察

NTT グループは、セキュリティ基盤、インシデントレスポンス調査、マルウェアレポジトリー、マルウェアフィード、顧客とのやりとりそして独自に管理するハニーポットネットワークを含む、広範囲にわたる情報源からのマルウェアサンプルを分析している。これらの分析は、固有の検知・予防シグナチャーの開発を可能にする。

米国は、2015 年に検知されたマルウェアの 62%超の発生源だった。NTT グループは、2015 年に 191 カ国からのマルウェアを検知した。米国発生源でないマルウェアのほぼ 79%がトップ 5 の国々から発せられていた。

2015 年は 2014 年に比べてマルウェアのトータルでの量が減少した。これは主に一つの産業内の結果によるものだった。教育業におけるマルウェア検知量は 2014 年から 2015 年にかけて 94%の減少を見せた。これは、2013 年から 2014 年にかけての減少の後に起こった。この直近の減少は、必ずしもマルウェアの減少を示しているのではなく、教育業が彼らの環境を管理する方法を変更したことを示している。2015 年に教育機関の顧客は、生徒やゲスト環境の管理へのフォーカスを減ずる傾向にあり、内部、機関内の環境へのフォーカスに集中した。生徒とゲスト環境へのフォーカスの減少は、歴史的に最も脆弱であった彼らのネットワーク部分への偏重を劇的に減少させ、結果として教育業全体のログとイベントを大きく減ずることになった。

発信国	マルウェア%
中国	32%
オランダ	18%
ドイツ	16%
トルコ	8%
ノルウェー	4%

図 12: マルウェアの発信国ベスト 5 （米国以外）

教育業を除く全業種のマルウェア検知は年間で観察されたマルウェアにおいて 18%超の増加を示している。このマルウェアの増加の大半は、年間を通じて 5, 6 業種にわたって継続的に高度化された活動が組み合わされたものであった。

図 13 に見られるように、2014 年に検知された 8%のマルウェアからの増加を受けて、政府機関はマルウェアに影響を受けた業種リストのトップに躍り出た。これは、基本的には、顧客である複数の政府機関に対して多種多様なマルウェアが年間を通じて継続的に増加したためであり、欧州の幾つかの政府機関に対する攻撃を含んでいた。

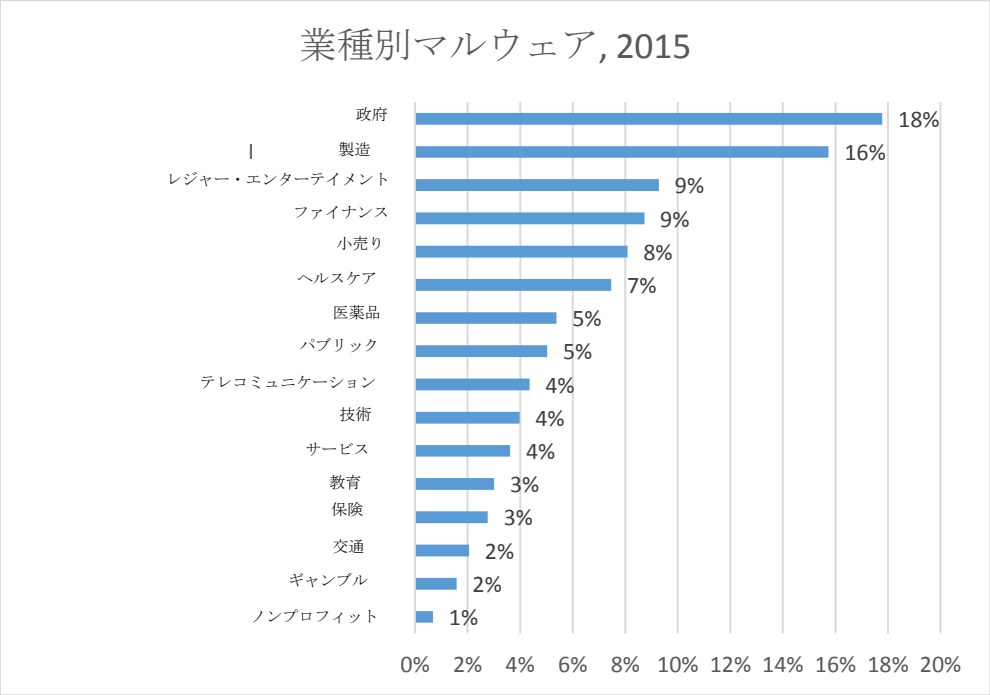


図 9:業種別マルウェア, 2015

金融業において検知されたマルウェア量は 2014 年から 140%の増加と急増した。金融業における検知は、Dyreza マルウェアのような長期継続的な活動と標的型攻撃を含んでいた。

サービス、レジャー及びエンターテインメント業とともに、製造業で検知されたマルウェアは、2015 年に 30%超増加した。これらの業種は、顧客単位マルウェア数でそれぞれ 2 位、3 位にランクした。

小売業も、2014 年の数値で緩やかな増加を見せた。小売業の顧客は検知マルウェア数の 8%を経験し、最も影響を受けた業種の 5 番目となった。これらの結果は、小売、政府機関、サービス・レジャー・エンターテインメントそして製造業がマルウェアの標的にされるトップ 5 業種であり、攻撃標的にされるトップ 5 業種であることを表すとともに、結果としてそれらを全業種の中で最も被害を受けている業種とするに至っている。

マルウェアは使用される多くの攻撃ベクターの唯一のものであり、現代のエクスプロイトキットのキーコンポーネントと成り得る。

Exploit Kit Summary エクスプロイトキットのサマリー

ソフトウェアエクスプロイトは、OS やアプリケーションのパッチを当てられていない不備を利用する。エクスプロイトは、攻撃者に悪意あるソフトウェアを脆弱なデバイス上にインストールすることを許す。

エクスプロイトキットは、通常ハッキングフォーラムや IRC チャンネルで販売されるソフトウェアパッケージで、広範なエンドユーザー技術（Internet Explorer、Adobe Flash 等）の既知の脆弱性に対するソフトウェアエクスプロイトをフル活用している。エクスプロイトキットは、攻撃者が豊富な専門知識を必要とせずに脆弱なシステムに対して大規模な攻撃を実行することを可能とする。

2015 年エクスプロイトキットにより標的とされた技術

NTT グループは、 2012 年から 2015 にリリースされた人気のあるエクスプロイトキットによって標的とされたユニークなエクスプロイトを追跡した。この情報は、標的とされた技術ごとに整理し、図 14 に示した。このデータには 3 つの明確な傾向が存在する。

- Adobe Flash は、2015 年にエクスプロイトキットが最も標的にしたソフトウェアであった。
- New Java エクスプロイトは、事実上 2015 年にエクスプロイトキットから姿を消した。
- Internet Explorer エクスプロイトは一貫して存在していた。

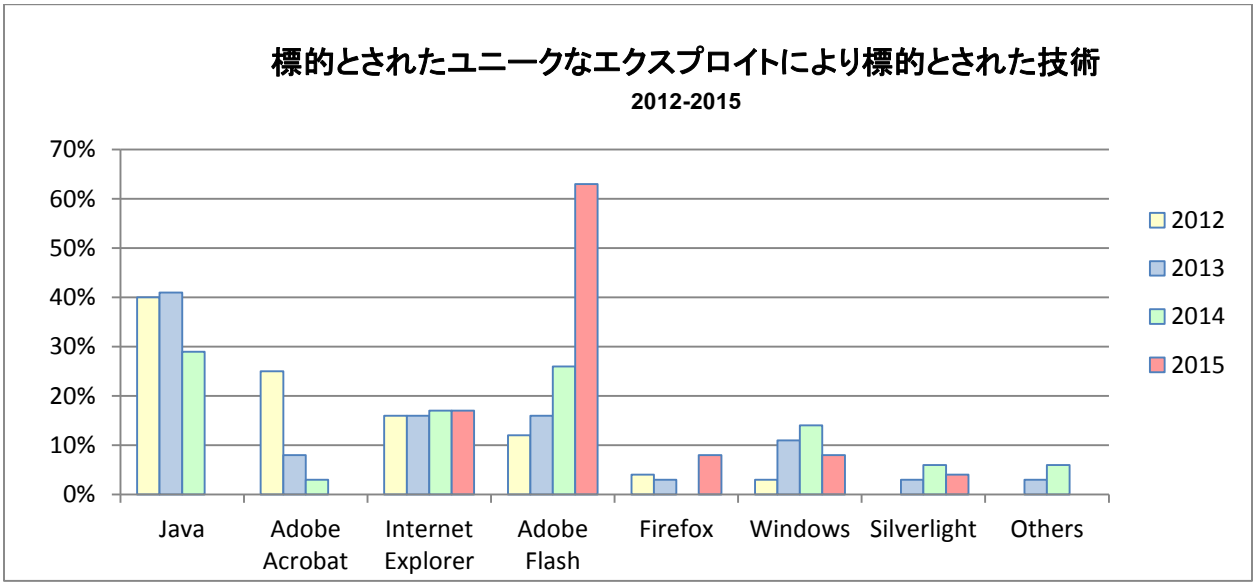


図 10: エクスプロイトキットにより標的とされた技術

このグラフで観察された傾向は次のような議論を呼んでいる。

- **Adobe Flash 標的の増加 –** 2012 年から 2014 年にかけて、エクスプロイトキットにおける Adobe Flash エクスプロイトの使用は安定して増加しており、2015 年には急増した。エクスプロイトの研究者は 2014 年に Java のセキュリティに非常に大きな改善が施された後は次第に Flash に移行していった。2015 年に特定された Flash の脆弱性数は、図 15 に示された通り、2014 年対比 312%増となり過去最高だった

Flash はインターネット上に広く普及し、現在の全ての OS でサポートされている。これらの事実により、いつもタイムリーにパッチを当てられる訳ではない重要なセキュリティ上の欠陥の流れと相俟って、2014 年以来エクスプロイトキットが急激に Flash に移行していったことが説明できる。

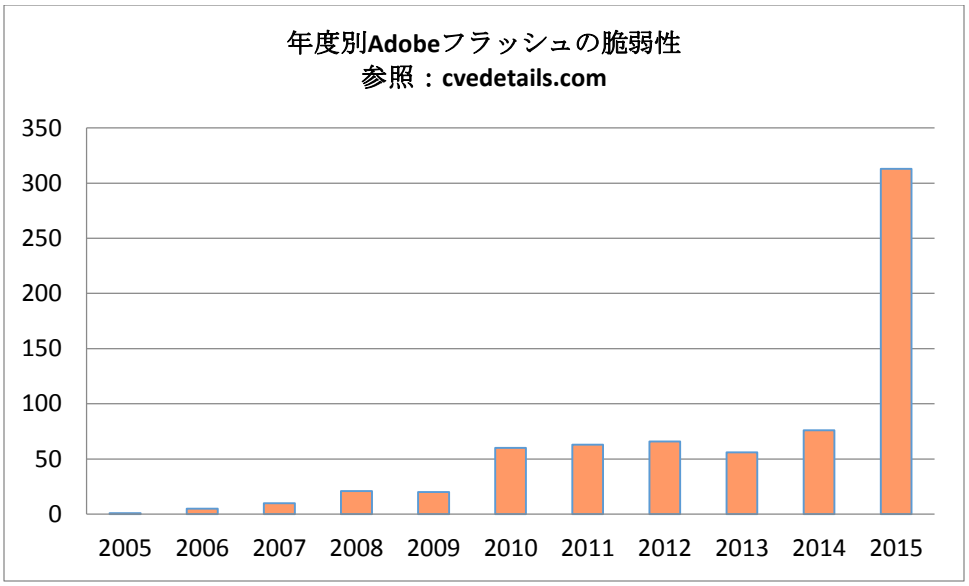


図 15: 年度別 Adobe フラッシュの脆弱性

- **Java 標的の減少–** エクスプロイトキットにおいて標的にされる Java 脆弱性数は、少なくとも一つには Java に導入されたセキュリティ技術（デフォルト設定で署名なしアプレットのブロックを含む。）の向上によって、2013 年から 2015 年にかけて安定的に減少した。これらのセキュリティの向上は、図 16 に表されたように、過去 2 年にわたって特定された Java 脆弱性の減少に反映されている。

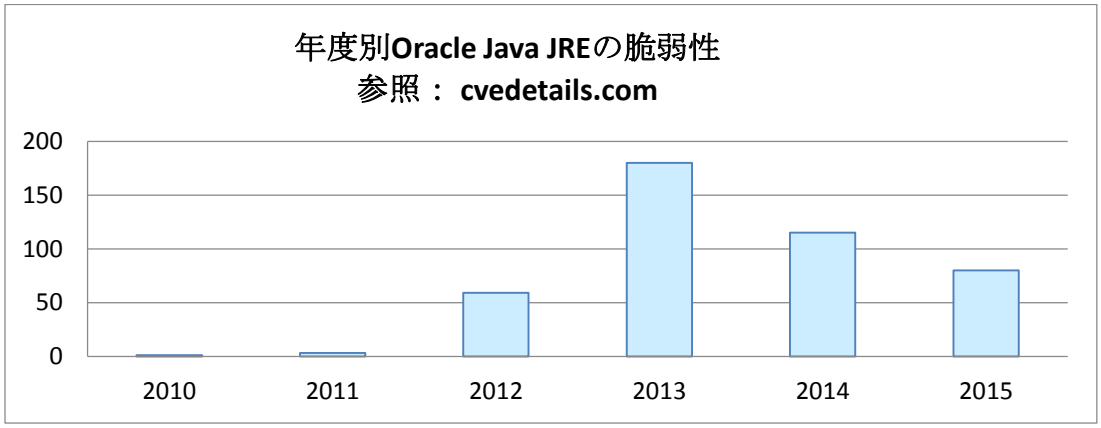


図 16: 都市別 Java の脆弱性

- **一貫して標的とされる Internet Explorer**- Internet Explorer は引き続き Windows OS 上の基本ブラウザであり、企業における通常のエンドユーザーシステムとなっている。図 17 に示されたように、Internet Explorer は引き続き標的として選択されており、それは普及しているというだけではなく、脆弱性がコンスタントに Internet Explorer で発見され続けているからなのである.

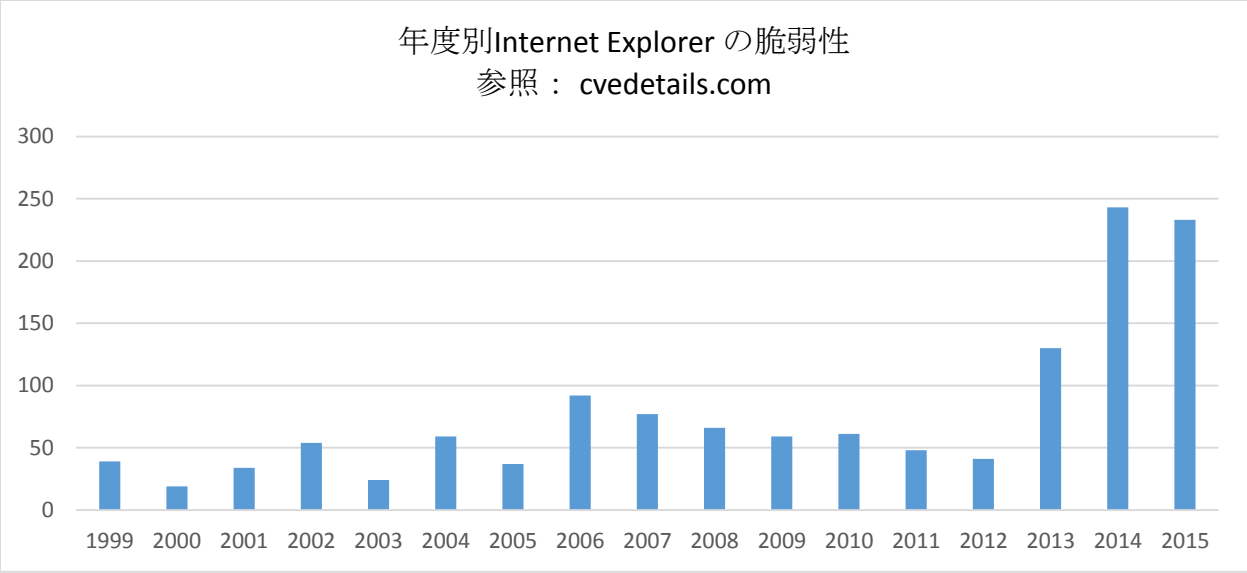


図 11:年度別 Internet Explorer の脆弱性

2015 年にエクスプロイトキットの標的となった最も一般的な脆弱性

2015 年にリリースされたエクスプロイトキットの中で、最も一般的な 10 の脆弱性は下表の通り。

CVE	影響を受けた技術
CVE-2015-0311	Adobe Flash
CVE-2015-5119	Adobe Flash
CVE-2015-5122	Adobe Flash
CVE-2015-0359	Adobe Flash
CVE-2015-0313	Adobe Flash
CVE-2015-2419	Adobe Flash
CVE-2015-3090	Adobe Flash
CVE-2015-3113	Adobe Flash
CVE-2015-0336	Adobe Flash
CVE-2015-7645	Adobe Flash
CVE-2015-3105	Adobe Flash

図 12: 最も一般的なエクスプロイトキットの10.の脆弱性

2013 年、Adobe Flash は、エクスプロイトキットの中で最も一般的な 10 のエクスプロイトの中に一つだけあった。2014 年、4 つの Adobe Flash のエクスプロイトがトップ 10 に含まれていた。2015 年、トップ 10 は Adobe Flash のエクスプロイトで占められた。

2013 年、トップ 10 のエクスプロイトのうちの 8 つが Java 関連だった。2014 年、トップ 10 のエクスプロイトのうち 4 つだけが Java 関連だった。2015 年にはトップ 10 に Java の脆弱性は含まれていない。

エクスプロイトキットに関係するリスクを減らすために、組織は以下の事項を考慮すべきである。

- **効果的なパッチマネジメントを徹底する** –エクスプロイトキットは典型的にはパッチが存在するエクスプロイトを使用する。エクスプロイトキット開発者は、最初の脆弱性の公表とエンドユーザーや組織によるパッチ導入の間の時間を利用する。エンドユーザーのデバイスに効果的なパッチマネジメントプロセスを徹底することは、エクスプロイトキットからの防御において最初の重要なステップとなる。組織は Adobe Flash のようなウェブブラウザのプラグインと技術に特段の注意を払うべきである。これらの組織は、Microsoft と同じようなタイプの企業クラスの展開力を有していないと思われ、よってパッチを当てて確認するツールの導入を徹底する必要がある。
- **スレットインテリジェンス**–スレットインテリジェンスサービスは、組織が活発に稼働している脆弱性を特定するのを助けることができる。これらのサービスは、パッチマネジメントプロセスの補完的対策として機能し、攻撃者の標的となっている脆弱性に対して確実にパッチを当てることを助ける。
- **ソーシャルエンジニアリング(フィッシング)訓練** –エクスプロイトキットは頻繁にソーシャルエンジニアリングとフィッシング攻撃を通じて配布される。標準的なセキュリティ認知訓練は高度なセンシティブデータを取り扱う組織にはもはや無意味となっている。組織は、主要な社員に対し、現実の世界で発生するソーシャルエンジニアリングのテストを実施し、彼らの実際のフィッシングシナリオへの対応能力を確認すべきである。
- **広告ブロックソフトウェア** – 攻撃者は、被害者をエクスプロイトキットのランディングページに誘い込むためにマルバタイジングをよく使う。コンテンツフィルタリング機能を備えた広告ブロックソフトウェアやウェブプロキシーの効果はこの攻撃手法には限定的である。
- **IP レピュテーションサービス** – IP レピュテーションサービスは認識された悪い IP アドレスとドメインにユーザーが訪問することを警告又はブロックできる。これらのサービスは、補完的対策と考えられるべきである。エクスプロイトキットのアドレスは検知を逃れるために随時変わっており、また、このサービスが正確で包括的なランディングページ URL のリストをリアルタイムで保持する見込みはない。グローバルハニーネット分析の章で議論されるように、攻撃者は新しい評判の良い IP アドレスを定期的に利用するし、URL ブラックリストは更新に時間を要す。
- **エンドポイント防御** – エンドポイント防御の実施は、重大な損害が発生する前に、エクスプロイトキットによりデバイス上に落とされたマルウェアの検知を助ける。

エクスプロイトキット詳細：Angler とマルバタイジング

NTT グループ CERT は、2015 年のほぼ第 3Q 中に一連のマルバタイジング攻撃を識別した。セキュリティ研究者は、日本の 3,000 以上のウェブサイトに対するマルバタイジング攻撃があり、50 万ユーザーが攻撃に晒されたと報告した。標的にされたウェブサイトはほとんどが合法的なものであった。ユーザーは悪用された合法サイトからのドライブバイダウンロードを通じて感染していたので攻撃は広まった。

NTT グループは、同時期に同様の行為を観察した。Angler エクスプロイトキットは、Microsoft Internet Explorer、Adobe Flash Player そして他のクライアントベースソフトウェアにおける脆弱性を悪用して被害者のパソコンにマルウェアを注入した。図 19 にまとめているように、攻撃者は同じプロセスを経てランサムウェアと銀行詐欺マルウェアを含むマルウェアを追加でインストールした。

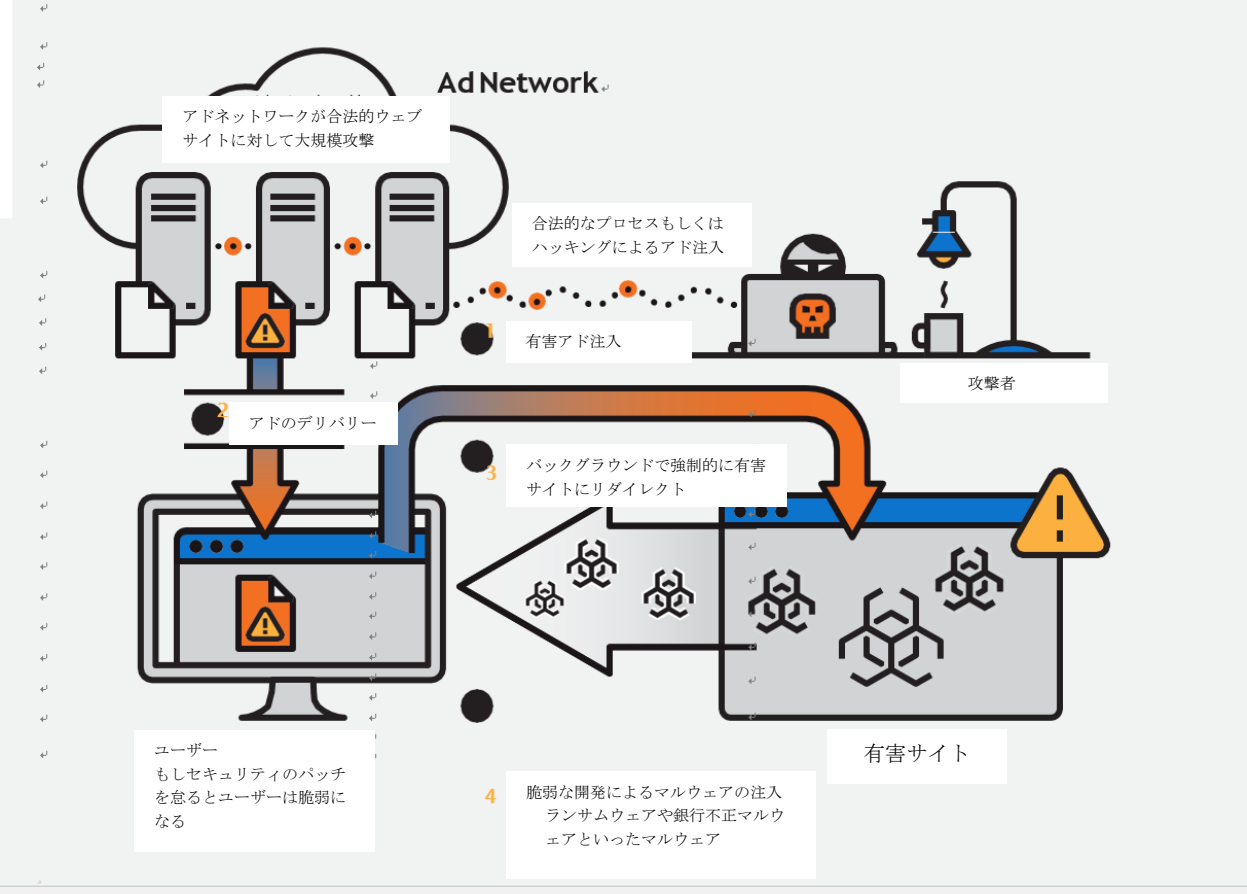


図 13: Angler とマルバタイジング

NTT グループは、Angler によって悪用されている脆弱性を特定しパッチを当てるために、顧客と協働した。また、NTT グループは、対応作戦において参照されたブラックリスト URL と IP アドレスを提供し、追加の更新を支援するために対応作戦をモニターした。ひとたび影響を受けた組織が明示的に関係サイトをブラックリストに追加し始めると、攻撃の成功確率は低下した。攻撃に晒された可能性のあるコンピューターのフォレンジック分析により、追加の攻撃が不成功に終わっていたことが確認された。ブラックリスト管理のおかげで、合法サイトから悪意のあるサイトへの多段階リダイレクトは失敗に終わっていた。

サイバーキルチェーンに対するセキュリティ対策の実用的な適用

キルチェーンの概念は軍事に起源を有し、最初に Lockheed Martin の Hutchins, Cloppert と Amin によって cyber intrusions in an influential 2011 paper にて適用された。その文書の中で、次の各フェーズを用いたサイバー攻撃に対する“Intrusion Kill Chain”が説明されている。

サイバーキルチェーン分析モデルはいくつかの基本要素を提示している。最初に、攻撃者は上位フェーズを通過して来なければならない。第二に、攻撃者はフェーズ 7（目的実行）を完了するまでは成功に至らない。最後に、防御者は、各フェーズにおいて攻撃を中断させ侵入者の成功を阻止する機会を有する。

サイバーセキュリティ過程の管理には他の複数の枠組みが存在する。一つのフレームワークは、20 の詳細な推奨事項を含む Center for Internet Security(CIS) のクリティカルセキュリティコントロール (CSC)である。現バージョンの全文はこちらで入手できる。https://www .cisecurity .org/critical-controls .

“複数のスタンダードが存在することの利点は選択できる対策がたくさんあることである。”

なぜそんなに多くのフレームワークが存在するか？それぞれが独自の問題認識と可能な解決策についての見解を提示している。Solutionary の Defense Strategies for Advanced Threats: Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain という白書は、先進的な持続的標的型攻撃(APTs)に対する防御の観点でこれら二つのフレームワークと関連している。NTT グループは、多くの組織がサイバー攻撃に対する明確な防御計画を有していないという経験知から、これらのフレームワークを推奨する。防御と分析のアクションについて検討するフレームワークを採用することは計画策定につながり、そして成功する防御には必ず計画が必要なのである。

なぜサイバーキルチェーンなのか？

サイバーインシデントレスポンス計画を持っていない組織ですら、ほとんどがファイアウォールや侵入検知/防御システム(IDS/IPS)のような周辺防御に多額の投資をしてきた。このアプローチは、しばしば部分的な対策と脅威情勢に関する狭い視野での理解に依存していた。それにより組織は、E メールフィッシング、感染サイト閲覧、携帯メディア端末、BYOD、悪意ある従業員に対して脆弱となってしまう。セキュリティ侵害に通じるこれらや他の経路を考慮すると、我々は、ほとんどの組織が一定程度のセキュリティ侵害の被害者になると結論づけることとなる。しかしながら、たとえ攻撃が発生しても、サイバーキルチェーンが、攻撃による損害を抑える機会を 7 つのフェーズ全体に渡って明示する点を認識することは重要である。組織は、起こり得る攻撃の影響を抑えることとサイバーキルチェーン全体を通じた防御機会の重層化に焦点を当てる必要がある。このフレームワークを通じ、組織は攻撃に対する防御力を強化するための多くの方法を認識し、防御者は敵に対して有する固有のアドバンテージを理解することとなる。

一般的なリソースを利用する攻撃者にとっては、100 万通のフィッシングメールを送る費用は取るに足りず、成功率はそれに伴って低くなる。また、標的とされた脅威は、サイバーキルチェーンの各フェーズを通過するので、目的達成までに相当の時間と労力を要することとなる。キルチェーン分析は敵が望んでいる目的を達成する前にチェーンの各フェーズを問題なく通過しなければならないことを示し、他方たった一つの対策がチェーンと敵を阻止できるのである。サイバーキルチェーンとクリティカルセキュリティコントロールで、組織は以下の事項を得ることができる。

- サイバーキルチェーンの各ステップに対して防御を可能とする重層的対策のより明確な可視化と理解。

- 攻撃の影響の最小化と防御効果の最大化を図りつつ、キルチェーンにおける攻撃の早期発見の機会。
- 攻撃者が既にネットワーク上に存在していて、しかし彼らがその環境からデータを抽出できるようになる前に、進行したステージでの攻撃を検知する機会。

ケーススタディ概要

この 2016 GTIR では、我々は、NTT グループインシデントレスポンスチームが対応した実際の攻撃についての詳細なケーススタディを紹介している。我々は、サイバーキルチェーンの 7 つのフェーズを進み、最終的に金融業者の会員データベースからデータを抽出した攻撃者の足跡を辿る。ケーススタディは、攻撃者のサイバーキルチェーンの 7 つの各フェーズでとった行動に焦点を当てる。各ステップにおいて、NTT グループは、ピンポイント対策、標準的な推奨内容そしてケーススタディの理解を助ける追加の詳細事項を含めて概要を紹介する。これらの推奨内容は対策全てを意味するわけではないが、サイバーキルチェーン上の攻撃者の通過を妨げる有効な対策を表している。

ピンポイント対策は、攻撃者の通過を妨げる又は中止させるために取り得る個々のアクションに焦点を当てて、組織がサイバーキルチェーンの各フェーズを解決するために実行できる特定の対策を強調している。これら解決策の多くが複数のキルチェーンのフェーズに適用される一方で、この文書では、それらはそれらが大きな影響を与えると期待されるフェーズのみで紹介されている

標準的な推奨内容は解説画像に列挙されており、この文書の中では記述されていない。標準的な推奨内容は、よく認知されるべき対策で、何度もセキュリティコミュニティー内で価値あるものと証明され、高度化されている。

それぞれのステップには、CIS のクリティカルセキュリティコントロールの参照が含まれている。CIS の対策は、実際的かつ実践的な方法で定義され、よって組織が意味のある形でそれらを実施することを可能にする。

CIS の対策は実際的かつ実践的な方法で定義されているので、組織は実効性を伴ってそれらを実施できる。

組織は、しっかり実施された大多数のセキュリティ対策がキルチェーンの複数のフェーズに影響を与えると期待するべきである。現実的には、本当のセキュリティ認知・訓練プログラムや効果的なスレットインテリジェンスプランの実施のように、キルチェーンの全てのフェーズに影響を与えるかもしれないものはわずかである。しかし最終的には、全ての対策が、組織の情報資産の防御を志向した統合セキュリティ対策の要素として貢献する。

サイバーキルチェーンフェーズ 1 – 偵察

定義: Lockheed Martin によって定義されているように、サイバーキルチェーンにおけるこのフェーズは、“しばしば会議結果、E メールアドレスのメーリングリスト、社会的関係、特別な技術に関する情報などを含むインターネットウェブサイトのクローリングに代表される、ターゲットの調査、認知及び選択 [7]”に関連する活動から構成される。

防御者の目的：偵察を制限し、攻撃者が標的の痕跡を並べ上げることを阻止する。

- 偵察活動の焦点を決定する
- 個人情報が公に晒されないことを確実にするためにサーチエンジンを利用する
- ソースボリュームトラフィックの上限値とタイプを管理する
- 積極的な侵入テストを実施する
- 内部的な偵察を特定する

標準的な推奨事項：

- 外部への露出をモニターする
- IDS/IPS ベースのホストとネットワークをインストールし、設定し、管理する
- 適切な ACL を更新し、維持する

クリティカルセキュリティコントロール：

- CSC 6: 監視ログの保全、モニタリング、分析
- CSC 9: ネットワークポート、プロトコル、サービスの限定とコントロール
- CSC 11: ファイアウォール、ルーター、スイッチのようなネットワークデバイスの安全な設定
- CSC 12: 境界での防御 CSC 12: Boundary Defense
- CSC 20: 侵入テストと Red Team 演習

サイバーキルチェーンフェーズ 1 ：偵察（Reconnaissance）

ケーススタディ時間軸、観察と影響

偵察フェーズのイベントの発生順は次の時間軸で表される。

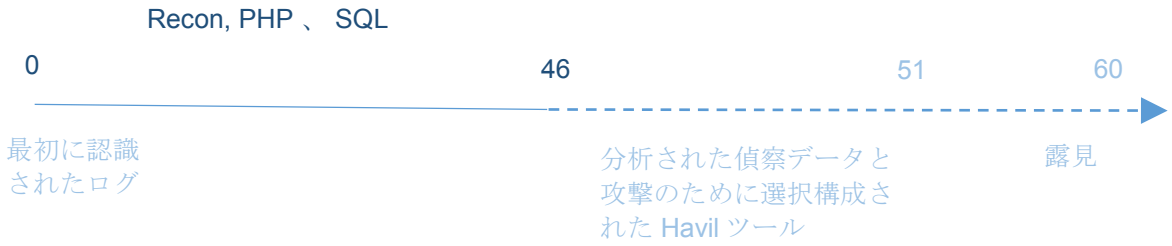


図 14 イベントの発生時系列

Peaceful Panda Financial Corporation[8] (PPFC)での敵の行動の最初の兆候は、侵入が行われる 2 ヶ月程前に発生した偵察活動だった。敵は、攻撃面のプロファイル作りのために、特別なアプリケーション、システムとサービスを一覧化する外部システムをスキャンした。これは、敵が組織の構成や技術における弱点を特定でき、更に敵の次の一手のための最初のポイントを提供することとなるので、CKC において非常に重要なフェーズであることが判明した。

PPFC はシステム、アプリケーションとデータベースイベントのログを取ることの必要性は認識していたものの、 彼らの実装は防御のためにこれらのログを活用するよう設計されていなかった。偵察活動に見当を付けるためのいくつかの主だったチャレンジは次の通りである。

- リアルタイムでの攻撃を特定する能力 – PPFC は悪意ある行為についての情報を集めていたが、セキュリティインシデントの集約、相関分析、リアルタイム分析を遂行する SIEM（Security Information and Event Management）は導入していなかった。
- 存在するログとイベント保存ポリシー – 全てのシステムは集中型サーバ上にイベントログを記録するよう設定されていた。しかしながら、ストレージの容量の限界で、ログは 2 ヶ月後に上書きされていた。これは、PPFC が、偵察活動が開始された時に特定できないことを意味していた。
- ログとインシデントデータのレビュー – 組織はネットワークやアプリケーションのパフォーマンスに顕著な悪化があった時だけにログやイベント分析を実施するが、これがログの防御的価値と攻撃者の初期活動の検知能力を更に減退させることにつながる。

サイバーキルチェーン考察

NTT グループが観察した偵察活動は、ログ全体のほぼ 89%を占め、取り扱われた事案活動の約 35%の結果となった。

偵察フェーズでは防御者にとっていくつかの特有な難題が存在する。偵察は非常に広範囲な活動を含み得て、その多くは本来的に悪意あるものではなく（例 プレスリリースへのアクセス）、標的の環境や対策の外側で発生し得る（例 サーチエンジン、ソーシャルネットワーク）。偵察活動特定の成功は、どの人達が、システムが、アプリケーションが標的になる可能性があるかを示すこととなり、あなたの防御方針を改善することになる。

攻撃者がキルチェーンを通過することを阻止するためのアクションを組織が早く取れるほど、事態は良くなる。これらの初期攻撃ステップの特定と理解を助ける検知能力への適切な投資は、攻撃の可能性が最大レベルに達する前に対応策を講じようとする時に極めて重要なアドバンテージと成り得るのである。もし組織が攻撃者の標的を理解できるなら、攻撃者の意向、能力及び目的についての知識を通じて CKC のその後のフェーズにて攻撃を阻止するアクションを取ることができる

いくつかのケースでは、偵察活動はインシデント発生後分析を通じて遡及的にのみ特定された。攻撃活動と先んじて行われる偵察活動との相関関係は、組織が全体セキュリティ対策の強化部分を理解するのを助けることができる。

ピンポイント対策

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有し、その結果、次の攻撃フェーズに成功裏に進む彼らの能力を妨げることになる。

偵察活動の焦点を決定する-その活動はあなたの全 IP スペースで観測されたか、それともほんの一つのシステム上か？その活動は特別なポート群（HTTP、SSH 等）を標的としているか？偵察活動を評価し、偵察されているエリアの直接的な改善に焦点を当てよう。例えば、もし攻撃があなたの SFTP サーバにブルートフォース攻撃を行っているなら、そのシステムがインターネットにて利用可能となる必要があるかを考慮する、又は対策は特定の IP アドレスからの接続のみを許容するよう実施可能か？SFTP サーバはミッションクリティカルか、又はそれは一時的にオフラインにできるだろうか？偵察の標的を直接的に守るために実施できる他の対策があるだろうか?

- **個人情報が公に公開されないことを確実にするためにサーチエンジンを使う–** “受動的な”偵察によって情報を得る攻撃者による全ステップを阻止する。これは、ソーシャルエンジニアリング、従業員のソーシャルメディアサイト探索、ユーザーネームとパスワード収集、従業員の E メールアドレス、その他多数のものを含む。攻撃者は、不満を抱いている社員や以前の脅威実行者による Pastebin のようなサイトにダンプされた内部情報を定期的に活用する。この情報は速やかに取り除かれなければならず、認証情報は無効化されなければならない.
- **情報源のトラフィック量の上限値とタイプを管理する**– 偵察と指紋収集の活動は、非常に多くなりがちで、しばしば限定的な数の IP アドレスから発生する。悪意の可能性のある活動を特定したり、データ量の多い攻撃を回避するために IDS/IPS、ファイアウォールや SIEM に上限値を設定することは、攻撃者が自動的に情報収集する能力を減少させることができる。これは多量の活動に対して有効な防御に成り得るが、回避技術を使う攻撃に対する成功確率は限定的となってしまう。
- **積極的な侵入テストを実施する**– 攻撃者が偵察活動を用いて見ることができるものを特定するために侵入テストを実施する。そして偵察を通じて収集されるものを限定するために、明らかにされた情報を隠す又は難読化するアクションを取る。
- 内部偵察を特定する – 全ての偵察が外部のものではない。攻撃者はインフラを通じて攻撃を横展開するために内部偵察を敢行する。このような偵察はより特定し難いかもしれない。内部でのスキャンや探知のような内部偵察を認知する。組織は、型通りのネットワーク区分を明確にし、内部システムを複雑にすることによって自身の環境に関する知識を活用し、成功する内部偵察の阻止を助けることができる。

-


unusual
scanning
nexpose
synfin
port
host
attempt
portmapper
vulnerability
packet
security
access
community
brute
query
behavioral
login
sslscan
scanner
force
tool
architect
local
setup
unix
remote
scan
syn
smb
user
1433
ice
isakmp
null
rdp
failure
sweep
name
snmp
http
script
tcp
udp
et
activity
infection
ssl
sql
php
ftp
request
windows
scan36266
attempt40004
bruteforce
detection36268
traffic
probe
password
scan8001
squid

サイバーキルチェーンフェーズ２：武器化

定義: Lockheed Martin によって定義されているように、CKC におけるこのフェーズは、“典型例としては、自動ツール（ウェポナイザー）を用いてエクスプロイトを伴ったリモートアクセス型トロイの木馬を標的に到達可能なデータ本体に埋め込むことや、増加傾向にあるのは、Adobe の PDF や Microsoft オフィス文書のようなクライアントのアプリケーションデータファイルを武器化された配送物として使うこと” に関連した活動から構成される。

防御者の目的: 次フェーズ以降への進行阻止に向けて、利用可能な情報に基づいて実施可能な武器化を解明する。

ピンポイント対策：

- スレットインテリジェンスを適用する
- 防御のためにハニーポットを使い署名を検出する
- 予期せぬ事態に備えてインシデントレスポンスチームを訓練する
- どんな偵察が行われているかを特定する
- 武器化の特徴を識別する

標準的な推奨事項：

- 設定管理プログラムを実装する
- 型通りのリスク管理を実施する
- 強力なログ監視を実施する
- 積極的に内部コミュニケーションを促進させる

クリティカルセキュリティコントロール：

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバのハードウェアとソフトウェアを確実に設定
- CSC 9: ネットワークポート、プロトコルとサービスの限定と管理
- CSC 17: ギャップを埋めるためのセキュリティスキル調査と適切な訓練
- CSC 19: インシデントレスポンスと管理

サイバーキルチェーンフェーズ 2 ：武器化（Weaponization）

ケーススタディ時間軸、観察と影響

武器化フェーズに関連するイベントの発生順は次の時間軸で表される。

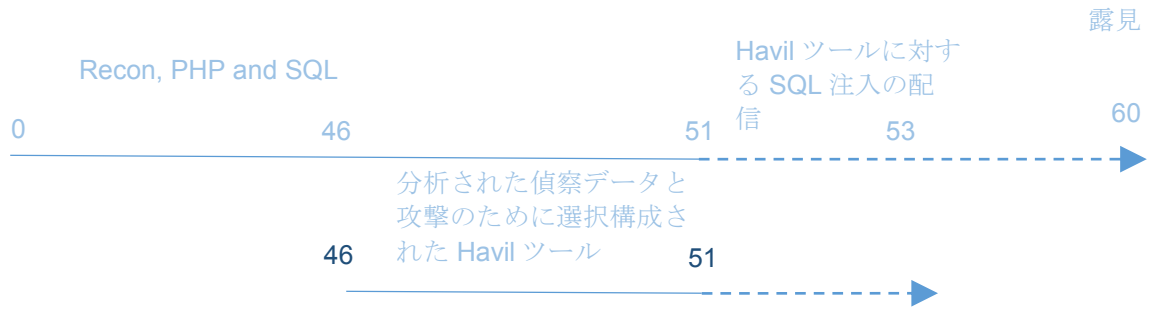


図 15: 武器化フェーズに関連するイベントの時系列

武器化は防御者の環境外で行われるので、その実際の動きを探知するのは現実的ではない。

我々のケーススタディでは、攻撃者は偵察結果をレビューしてから、PPFC に対する自動化された SQL インジェクション攻撃を敢行する Havij ツールを選択し、設定した。

この攻撃の時点では、PPFC は発生した偵察の結果を特定できる状況で、狙われる可能性のある標的を特定するためにその情報を利用できた。PPFC はウェブアプリケーションに対するスキャンのログ、特に将来の攻撃を示唆する PHP と SQL ステートメントを成功裏に収集することができた。もし PPFC が例えば SQL スキャンを識別していたら、彼らは攻撃者と見られる者が SQL インジェクションの脆弱性を突いていると判断できたかもしれない。これは PPFC にこの攻撃ベクターから彼ら自身を守るための追加的アクションを取る機会を提供できた。代わりに、PPFC は彼らがスキャンされていることを探知できず、よって防御的行動を起こすことができなかった。

その後のフェーズにおいて、PPFC は指標や残された“ツールマーク”を特定できるかもしれない。武器化活動を特定するためのいくつかの主だったチャレンジは次の通りである。

- PPFC はセキュリティ事象のログを取れていたが、それらをレビューする能力又は攻撃者の意向に関する手がかりに繋がり得る活動を特定する能力はなかった。
- たとえ彼らがログと事象をレビューしたとしても、PPFC はその後の活動に焦点を当て得る意味のあるインシデントレスポンスプロセスを有していなかった。インシデントレスポンス：傾向が示す組織の対応不足、の章で説明されているように、良く作り込まれたインシデントレスポンス手順は重要である。

サイバーキルチェーン考察

武器化の行動は、何かを武器として使用できるようにすることである。このフェーズでは、攻撃者は攻撃ベクターを特定するために偵察フェーズで収集した情報を利用し、その後、武器を選択し設定するであろう。これは、エクスプロイトやマルウェアを無害な PDF に同梱（“ウェポナイザー”を用いて実施）しているかもしれないが、今回のケースで行われたように、偵察の間に発見された脆弱性を利用してツールや技術をカスタマイズしたり、他の準備行為を含めることもできる。攻撃者はまた、発見を避け、かつ標的が攻撃元を追跡する能力を減ずる対策を採用するだろう。

ピンポイント対策

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有し、その結果、次の攻撃フェーズに成功裏に進む可能性を妨げることになる。

- スレットインテリジェンスの適用　ー　敵になる可能性のある者についての情報を、彼らの戦術、技術、手続き（TTP）とともに収集し適用し、攻撃活動を追跡する準備をそれらが実施される前に整える。他の阻止策と成り得る傾向を特定する。スレットインテリジェンスの効果的な追跡手段なしでは、防御は極端に難しくなり、より受動的になる。防御者が攻撃を追跡し、相関させ、より理解できることにより、あなたは敵の活動の指標を主体的に特定できることとなる。これは、スレットインテリジェンスにおけるサイバーキルチェーンの役割の章で述べられているように、主体的な防御体制を敷く上で重要な要素である。
- 防御のためにハニーポットを使い署名を検出するー 適切に設定されたハニーポットやハニーネットは、攻撃者にとって格好の標的と成り得る。攻撃者は、本当の組織の環境から分離されたハニーネット内で侵入に向けた努力を続けるかもしれない。ハニーポットで利用されている攻撃は、追加の探知や緩和メソッド（例　HIPS、AV、IDS/IPS）に繋がり得る攻撃者の TTP 情報を提供できる。
- 予期せぬ事態に備えてインシデントレスポンスチームを訓練するー 最も起こり得る攻撃に備えることと高効率な対応を確保することは非常に価値が高いが、予期せぬ事態に備えることは少なくとも同じくらい価値がある。インシデントレスポンスチームは継続して訓練し、訓練の一貫としてチャレンジングな状況を含んでいなければならない。
- どんな偵察が行われているかを特定するー 偵察活動の理解は、攻撃者が計画していることについての気付きを与えるかもしれない。もし攻撃者が DB をスキャンしたなら、SQLi 不正アクセスのような DB 活動をチェックしよう。もし攻撃者が Cold Fusion をスキャンしたなら、Cold Fusion に対するエクスプロイト実施に備えて欲しい。入ってくる偵察の目的を検知することは、続いて行われる配送の試みを組織が阻止することを可能とする。
- 武器化の特徴を識別する　ー　攻撃が次のフェーズに達するのを阻止するために、武器化の特徴に基づく脅威を見つけ、減らす機会を利用する。武器化技術に使われていた“ツールマーク”（中間生成物、メタデータ、構造、属性）を理解する。例えば、Havij という言葉は、ツールによって生成されたウェブリクエストに関係するユーザーエージェントテキストの初期値にしばしば見られる。

サイバーキルチェーンフェーズ３―配送

定義: Lockheed Martin によって定義されているように、サイバーキルチェーンにおける配送フェーズは“標的の環境への武器の伝送と、Lockheed Martin コンピューターインシデントレスポンスチーム(LM-CIRT) 2004-2010 によって観察されている通り、APT 実行者によって武器化された本体データの最も一般的な 3 つの配送ベクターは電子メールの添付物、ウェブサイトと USB メモリーであるという事実 [10]”に関連する活動から構成される。

防御者の目的: 敵の行動を識別し、悪意あるコンテンツの配送を妨害し、攻撃者に戦術を変えさせる。

ピンポイント対策 :

- ブラウザのセキュリティを管理する
- ホワイトリストの管理を可能とする
- アンチウィルスを組み込む
- ウェブアプリケーションファイアウォール（WAF）の効果的な設定と管理
- 自動デバイス指紋採集
- セキュアウェブゲートウェイ(SWG)の導入

標準的な推奨事項 :

- 詳細なログ収集を可能とする
- 周辺装置のセキュリティを管理する
- 物理的セキュリティを評価する
- 専門的なセキュリティの啓発と訓練を実施する
- 電子メールフィルタリングとサニタイズを実施する
- 適切なブラックリスト管理を実施する
- アンチウィルスを組み込む
- 安全なウェブアプリケーションを開発する

クリティカルセキュリティコントロール :

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバ上のハードウェアとソフトウェアに対する安全な設定
- CSC 6: 監査ログの保全、監視と分析
- CSC 7: 電子メールとウェブブラウザの保護
- CSC 11: ファイアウォール、ルーターとスイッチのようなネットワークデバイスに対する安全な設定
- CSC 13: データ保護
- CSC 17: ギャップを埋めるためのセキュリティ能力評価と適切な訓練

サイバーキルチェーンフェーズ 3：配送（Delivery）

ケーススタディ時間軸、観察と影響

配送フェーズに関連するイベントの順序は以下の時間軸で表される。

図 16: 配送フェーズに関連するイベントの時系列

攻撃者は、SQL インジェクション攻撃を実行するようデザインされたウェブリクエストを送るために、Havij ツールを使用した。これらの特別に作られた本体データは、ウェブアプリケーションリクエストのフォームの中で配送フェーズを展開し、攻撃を先に進める。この活動は、PPFC ウェブとセキュリティログの中に現れていたが、PPFC がセキュリティインシデントのログをチェックし処理しなくなって以降、攻撃は察知されなくなった。

配送は、Havij ツールを事前設定し、攻撃実施のためのボタンを押す事によってなされ、ほぼ自動で行われた。そして攻撃者は、指令が標的上で展開される間、ツールをモニターし、配送された攻撃の成否に関する指標を見守った。

サイバーチェーン考察

サイバーキルチェーンにおける配送フェーズは、組織が攻撃者の進行を確実に阻止しなければならない最初のチャンスなのである。

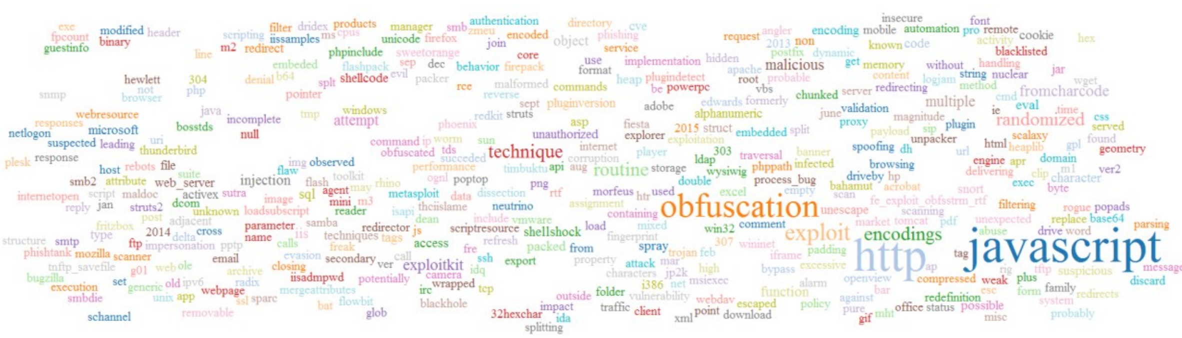
検証された全事案の 5%足らずがサイバーキルチェーンの配送ステップに関連するものであり、結果として配送ステップは 2 番目に事案の少ないステップであった。

ピンポイント対策：

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有し、その結果、次の攻撃フェーズに成功裏に進む彼らの能力を妨げることになる。

- **ブラウザのセキュリティの管理ー** ウェブブラウザ上での適切なパッチマネジメントとセキュリティ設定を実施する。典型的には、被害者はリダイレクションを通じて本体データが配送された悪意あるウェブサイトに引き寄せられる。これらの攻撃は被害者のウェブブラウザやアプリケーションの脆弱性を突くので、もしウェブブラウザやプラグインが最新、つまり脆弱でなければ、攻撃は有効とはならない。ブラウザのセキュリティやプライバシーを設定することでも、悪意ある本体データの配送を阻止することができる。

- **ホワイトリスト管理を可能とする－** 通常のセキュリティ対策は、悪意あると知られたサイトとアプリケーションをブラックリスト化している。ブラックリストは、“これらの既知の悪意あるウェブサイトには行かないこと”や“これらの既知の悪意あるドメインからの電子メールを拒否すること”といった宣言を行う。ホワイトリストは“良いと知られた”サイト、つまりユーザーが正当な仕事上の訪問理由を有するサイトを含んでいる。もしサイトがホワイトリスト上にない場合、それは自動的にブロックされる。これは全ての環境で実用的ではないが、やりとりが細かく定義されたセンシティブな環境では効果的かもしれない。
- **アンチウィルスを組み込む－** アンチウィルス/アンチマルウェアやリアルタイムヒューリスティックの製品は電子メールや添付物を分析するのに使われ、これらを自動的にブロックできる。アンチウィルスサービスによって計算されたハッシュ値は、（悪意あるオブジェクトの配送阻止のための複数のオープンソースリソースに基づく）信頼性のために、スレットインテリジェンスデータベースに関連づけられるかもしれない。組織は、これらが環境に入ってきた場合に徹底的に調べる能力を開発し、防御者が攻撃者のツールをより良く理解し、更に防御を改善できるようにするべきである。
- ウェブアプリケーションファイアウォール(WAF)の効果的な設定と管理—WAF は、ウェブベースの端末、ソフトウェアとサービス間のトラフィックを分析する。WAF は第 7 層（アプリケーション）のセキュリティに焦点を当て、ウェブのトラフィックのみに関係するパケットを分析する。これは、パブリックに面したサイトに対する本体データの配送を検知する能力を提供できる。
- **自動的なデバイス指紋採集－** モバイル端末を有する者（自分のものであろうが会社のものであるが）は全員、それを用いて組織のネットワークに悪意ある本体データを配送できてしまう。モバイル端末接続は、Cisco ISE のようなシステムを用いて、そのメーカー、モデルと製造者を特定するために端末の指紋を採集することで拒否できる。DHCP サーバもスマートフォンの MAC アドレスをブロック（又は許可）するのに使うことができる。オフィス外であなたの従業員の端末に誰がアクセスできるかを管理できないのなら、あなたの会社の環境に誰がこのような端末を接続しているかを管理することが重要である。
- セキュアウェブゲートウェイ**(SWG)を導入する －** SWGs は、エンドユーザーがバックドアのマルウェア亜種をインストールするのを防ぐ手助けをできる。これらは、URL フィルタリング、HTTP/S スキャン、アプリケーションコントロールなどを提供する。エンドユーザーのウェブ閲覧が標的となったシステム上で必要となるなら、これは重要と成り得る。フレキシブル SWGs は電子メールとデータの管理と有効化を容易にしてくれる。電子メールの添付物はバックドアマルウェア亜種を配送するのに使われる一般的な技術である。



サイバーキルチェーンフェーズ 4 – エクスプロイト

定義: Lockheed Martin はサイバーキルチェーンのエクスプロイトフェーズを次のように定義する。“武器が被害者のホストに配送された後、エクスプロイトが侵入者のコードのトリガーを引く。エクスプロイトは、通常、アプリケーションと OS の脆弱性を標的にするが、直接的にユーザー自身を悪用したり、OS の自動実行コードの特性を活用したりもできる。”

防御者の目的: エクスプロイトの機会を最小限にする対策に集中し、 脆弱性を減少させ、攻撃者に別の攻撃やより目立った攻撃をさせることを強いる。

ピンポイント対策 :

- アプリケーション/プロセスサンドボックスを実行する
- 積極的に侵入テストを実施する
- 外部に面するウェブアプリケーション用のリモート管理コンソールを取り除く
- 脆弱性緩和ツール(EMET)のような専用ツールを使用する
- アプリケーションのホワイトリスト化を実施する
- データ実行防止(DEP)を実施する
- アドレス空間のレイアウトのランダム化を実施する

標準的な推奨事項 :

- 多因子認証を実施する
- 不要なサービスとプロトコルを除去する
- パッチマネジメントプロセスを導入する
- 脆弱性管理プログラムを実行する
- システム展開にセキュアなホストベースラインを用いる
- 事前にインシデントレスポンス計画を作成しテストする
- 標準的なリスク評価を実施する

クリティカルセキュリティコントロール :

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバ上のハードウェアとソフトウェアに対する安全な設定
- CSC 4: 継続的な脆弱性評価と改善
- CSC 8: マルウェア防御
- CSC 17: ギャップを埋めるためのセキュリティスキル評価と適正な訓練

サイバーキルチェーンフェーズ 4ーエクスプロイト（Exploitation）

ケーススタディ時間軸、観察と影響

エクスプロイトフェーズに関連するイベントの順序は以下の時間軸で表される。

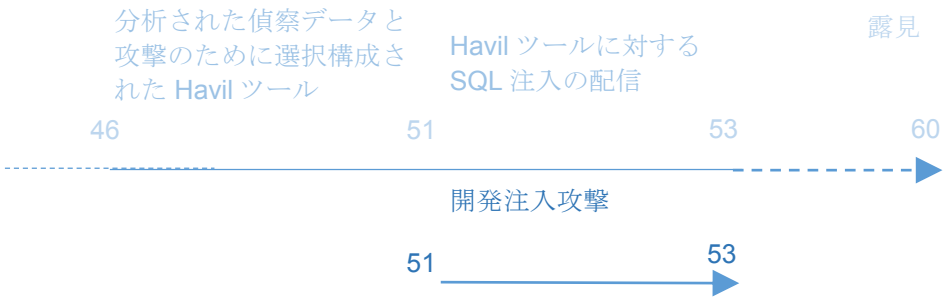


図 17: エクスプロイトフェーズに関連するイベントの時系列

インシデント後の調査は、脆弱性のエクスプロイトが、PPFC 顧客情報が"ペーストサイト"上に公開される約 9 日前に開始されていたことを示した。情報が公開された後、セキュリティ分析者は成功した Havij ベースの SQL インジェクション攻撃を特定するためにウェブとセキュリティのログを調査した。攻撃が公になるまではエクスプロイトは識別されなかった。

PPFC に対する攻撃は、いくつかのウェブフォーム内でパラメータ化されたクエリを適切に扱うことに失敗していた PHP で構築されたウェブサイトの構造上の脆弱性を利用していた。インシデント後の分析では、SQL サーバを有効化するために取られたステップやユーザー、データベース、表、情報スキーマの列挙を含めて、攻撃者の複数のエクスプロイトフェーズの通過を識別した。攻撃者は、体系的に顧客データベース全体を抽出でき、そして持続能力を保つために追加的なステップを踏むことができた。（このケーススタディのインストールと遠隔操作フェーズにおいて詳細を解説）

成功するエクスプロイト活動の阻止におけるいくつかの主だったチャレンジは次の通りである。

- **アプリケーション開発とセキュリティ訓練 ー**– もし組織がセキュアなコーディング作りの慣習を徹底するなら、SQL インジェクションやクロスサイトスクリプティングのような攻撃は限定的にできる。もしセキュリティテストがソフトウェア開発過程の一部になっていたら、この攻撃は回避されていたかもしれない。
- ウェブアプリケーション攻撃の探知と防止能力– PPFC は、多くのセンシティブ情報が収集される間、約 40%のトランザクションをオンラインで行っている。 オンラインビジネスが大部分を占めるにも拘わらず、ウェブサイト、アプリケーションやサブデータベースに対する標的型攻撃を緩和するための対策は何ら講じられていなかった。
- **脅威の認識と改善**– PPFC は情報漏洩の前にルーティーンとなったウェブアプリケーションの脆弱性テストを実施していたが、スキャン活動はウェブサイトの一般的な脆弱性を見つけるウェブチェックを含んでいなかった。伝統的な脆弱性スキャナは強力なウェブアプリケーションの脆弱性の認識機能は提供していない。

サイバーキルチェーン考察

ひとたび、攻撃者が悪意ある本体データ（武器化された添付物、武器化されたウェブページへのリンク又は特別に作成されたウェブリクエストかを問わず）を配送したら、次のフェーズはエクスプロイトである。悪意ある本体データは、たとえ配送されても、実行されなかったり、標的に影響を与えなければ、攻撃者の目的達成に貢献できない。

攻撃者が本体データの配送に成功した後でさえも、防御者がキルチェーンを遮断できるならば、この時点でも攻撃自体を阻止できる。

伝統的に、エクスプロイトはアプリケーションの脆弱性と考えられていて、脆弱性管理の文脈で調査されている。多くの攻撃と環境にとって、人間の行動に付け入ること、ユーザーにリンクをクリックさせたり添付ファイルを開かせることは、最初の（時には唯一の）必要とされるエクスプロイトなのである。

攻撃者が彼の本体データの配送に成功した後でさえ、防御者はキルチェーンを中断できれば、攻撃者の成功を依然として阻止できる。エクスプロイトなしでは、これらの本体データは組織内に成功した配送の結果として存在するが、何も成し遂げない。防御者は、配送が探知されているなら、戦術的優位性を持つこととなる。この点において、攻撃者は手の内を見せてしまったことになり、組織は攻撃者の能力と目的を分析できることとなる。攻撃者はバイナリ値を知るのみである。その攻撃は後のフェーズに進んだのだろうか？進めなかったのだろうか？

エクスプロイト行為の成功と失敗双方の探知は重要である。インシデントレスポンスチームは、情報漏洩範囲の特定を助けるのと同様に、分析とフォレジック活動の焦点を当てる場所を決定するのを助けるかもしれない価値ある情報を入手できる。

ピンポイント対策

これらのピンポイント対策は、このキルチェーンフェーズで攻撃者の活動を阻止する可能性を有しており、次の攻撃フェーズに成功裏に進む彼らの能力を妨げることとなる。

- **アプリケーション/プロセスサンドボックスの実施** – 悪意あるプログラムの可能性のあるものを分析するために管理されたホスト（サンドボックス）を使う。これらのプログラムをサンドボックスの中で動かすことは、ネットワーク活動の分析、プログラムの指紋利用（ハッシュ）、ソースコードの詳細分析等を可能とする。もしサンドボックスが適切に設定されているなら、悪意ある本体データはネットワークに害をもたらさないであろう。サンドボックスと攻撃者がそれらから逃れるために使っている技術の詳細については、アンチサンドボックス技術の章を参照して欲しい。
- **積極的な脆弱性テストの実施** – 攻撃に先んじて、組織は脆弱性の程度を決定するための侵入テストを実施するべきである。もしテストが脆弱性を明らかにしたなら、ネットワークの改修、適切なパッチ適用、アップデートや緩和策の適用などの積極的なアクションを取るチャンスがある。
- **外部に面するウェブアプリケーション用のリモート管理コンソールを取り除く**– PHP のようなウェブプラットフォームや WordPress、Joomla のようなアプリケーションプラットフォームは、しばしばリモート管理能力を含んでいる。これらはプラットフォームを管理するのに使われるが、もし外部に晒されたら、それらは容易に攻撃者によって付け入られてしまう。これらはしばしば、ファイルアップロードの能力を提供し、攻撃者にウェブシェルやバックドアを仕掛けるパスを容易に与えてしまう。
- **脆弱性緩和ツール（EMET)のような専用のツールを使用する** – 現在サポートしている全ての Windows プラットフォームと EMET は、メモリー破壊やバッファオーバーフローに対するエクスプロイトを防ぐために、特定の緩和技術を使用した無料のセキュリティツールである。
- **アプリケーションのホワイトリスト化を実施する**– 認証ソストウェアをホワイトリストにするのは、たとえそれらのプログラムが合法なようだとしても、改ざんされたりカスタマイズされたプログラムが標的とされたシステム上で実行されるのを防ぐ助けをすることができる。組織は、アプリケーションの完全度チェックを実施し、プログラムのハッシュを統合し、追加的認証層を作成できる。
- **データ実行防止(DEP) を可能とする** – データ実行防止は、最も新しい OS における、あるメモリエリアが実行可能か不可能かを定義するために使われたセキュリティ特性である。これはある種のエクスプロイト、バッファオーバーフロー行為と悪意あるコードを阻止できる。特にメモリエリアに応じて実行の可否を決定する実行可能コードのためのファイアウォールと考えよう。
- アドレス空間レイアウトのランダム化を可能とするーWindows と UNIX プラットフォームの双方で利用可能で、ASLR はバッファオーバーフローの脆弱性を標的とする悪意ある本体データを阻止することができる。これは、実行中のアプリケーションに割り当てられたランダム

メモリーアドレス空間を使用することにより実施され、事前決定されたメモリーアドレスを使ったエクスプロイトの実施を困難にすることができる。

サイバーキルチェーンフェーズ５　インストール

定義: Lockheed Martin は、サイバーキルチェーンのインストールフェーズを“被害システム上にリモートアクセス型トロイの木馬やバックドアをインストールすることにより、環境内部における敵の継続的な活動を許してしまう。[12]”と定義する。

防御者の目的: マルウェアのインストールや他のアクションを防ぎ、継続的なアクセスを設定し、維持しようとする攻撃者の活動を阻害する。

ピンポイント対策：

- 必要時にのみ、コマンドラインベースのツールと機能を可能とする
- ユーザー行動モニタリングと行動探知/防御能力を導入する
- ファイル実行制限の実施
- Windows 環境に対し、ユーザーアカウント制御(UAC)を設定する
- 多層型ファイアウォール(MLF)を設定し、管理する

標準的な推奨事項：

- 「最小権限」設定を実施する
- プロセスとバッチジョブに認証情報をハードコードしない
- システムとデータベースのユーザーアカウントセキュリティを評価する

クリティカルセキュリティコントロール:

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバ上のハードウェアとソフトウェアに対する安全な設定
- CSC 4: 継続的な脆弱性評価と改善
- CSC 8: マルウェア防御

サイバーキルチェーンフェーズ 5 ：インストール（Installation）

ケーススタディ時間軸、観察と影響

インストールフェーズに関連するイベントの順序は以下の時間軸で表される。

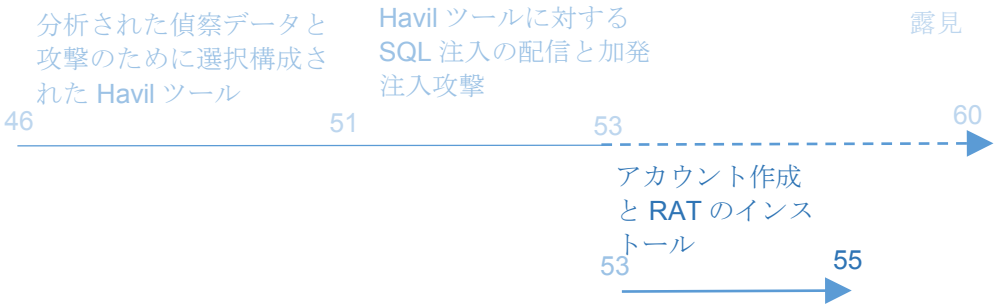


図 18: インストールフェーズに関連するイベントの時系列

攻撃者は、データベースに対するコマンドを実行し、データベーステーブルを見つけ出し、そしてデータ抽出を行うために SQL インジェクションを利用した。攻撃者は抽出データが価値あるものと分かり、新しいデータベース管理者を作成するために、追加的インジェクティド SQL を利用した。そのアカウントは下層の OS 上のユーザーアカウントを作成するために使用され、さらにリモートアクセス型トロイの木馬（RAT）をダウンロードしてインストールするために使用された。これは攻撃者に、データベースとデータベースが稼働するシステム双方への多くのアクセスと RAT を通じた一貫したリモートアクセスを提供してしまった。これらのアクションのほとんどはログに収められていたが、攻撃が明るみになるまでは敵として認識されていなかった。

成功するインストール活動を防ぐ上でのいくつかの主だったチャレンジは以下に表す通りである。

- 環境の積極的モニタリング
  組織環境の積極的なモニタリングは、組織に進行中の攻撃の識別と対応の機会を提供する。PPFC のケースでは、攻撃者はステルスでいようとしなかったので、どのような有意のモニタリングでもこの活動を探知する助けとなったはずである。
- 最近のマルウェアは探知を回避するよう設計されている
  最近の攻撃者が使っている先進的なマルウェアの多くが、多様なステルス技術を含んでいる。マルウェア対策が助けになる一方で、組織は先進的な攻撃者から安全なままでいるためにそれらに頼りきるわけにはいかない。

サイバーチェーン考察

キルチェーンにおけるインストールフェーズは、攻撃を継続する攻撃者にとって重要である。もし攻撃者が、さらなる攻撃のために、アクセスを確立し、標的の環境を調査し、情報を抽出又は被害者のシステムを利用したいのなら、攻撃者にとってプレゼンスを継続させることは極めて重要である。

いくつかのケースでは、持続能力は、後々のステップ（例　データベースのデータにアクセスし、取り出す）を容易にするためのアカウント作成から成るかもしれない。

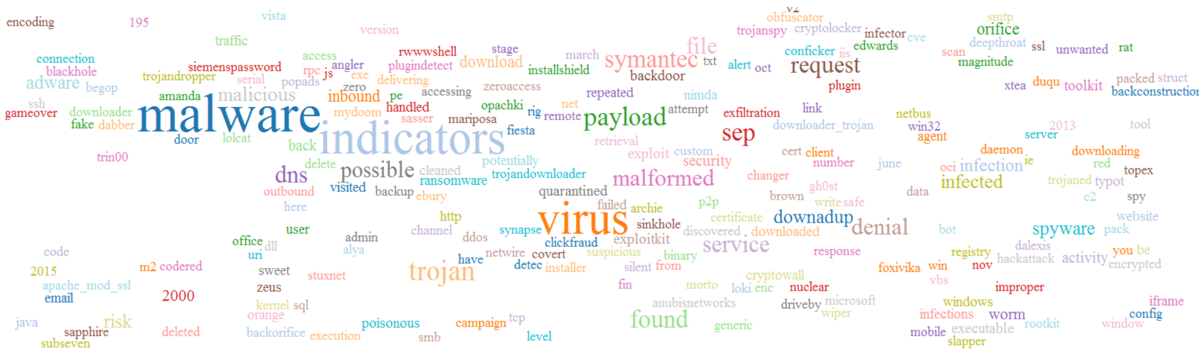
組織が、セキュリティ侵害が発生する前に、攻撃者の意欲を削ぐためのセキュリティ対策を計画することは重要である。これは、インストール活動を妨害し、キルチェーンの他のフェーズにおける活動の阻止を助ける。

NTT グループによって観察されたインストール活動は、全ログ数の 0.2%以下、全ての対応イベント活動の約 2%を占め、確実性の高いイベントの一つであった。

ピンポイント対策

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有し、その結果、次の攻撃フェーズに成功裏に進む彼らの能力を妨げることになる。

- **必要時にのみコマンドラインベースのツールと機能を可能とする**– 配送において、カスタマイズされたエクスプロイトは、必ずしも実行可能なバイナリデータである必要はなく、Windows の PowerShell や Linux terminals のようなコマンドラインツールを活用したカスタマイズされたスクリプトも有り得る。ほとんどのエンドユーザーにとって、これらのツールは必要なく、決してインストールされ稼働されるべきではない。
- ユーザー行動モニタリングと行動探知/防止能力を導入する—攻撃者は探知回避に次第に慣れてくるので、防御者はより動的に悪意ある行動を特定する手段を考えるべきである。行動モニタリングは、しばしば悪意のある予期せぬ活動を識別するために、類似性探知からマシンラーニングまで幅広い複数の技術を利用する。
- **ファイル実行制限の実施**– ファイル実行制限は、グループポリシーオブジェクト(GPO) からホスト型侵入防止システム(HIPS) まで様々な手段で実施され得る。使用される技術対策に関わらず、防御者にとっての目的はマルウェアのインストールと実行を防止することである。許可されていない場所からや外部（例：インターネット）からのアプリケーションの実行を防止することは、マルウェアのインストールを止めることになる。
- **Windows 環境に対し、ユーザーアカウント制御(UAC) を設定する**– UAC は、上位権限を要求する活動を探知するために活用される。この探知の間、ユーザーは管理者パスワードの入力を促される。C2 サーバから送られるコマンドに基づいた、リアルタイムのボット利用型悪意活動は、もし認証情報が処理前に必要とされるなら、阻止され得る。多層型ファイアウォール**(MLF**) を設定し、管理する– MLF は、ネットワークトラフィックの更なる確認、典型的には、ファイアウォール ACLs（アクセスコントロールリクエスト）、OSI のレイヤー2（データリンク）、レイヤー3（ネットワーク）、レイヤー4（トランスポート）の検査を通じて提供する。このようなファイアウォールアーキテクチャーは、パケット調査中の詳細データ分析同様、管理者が用意したハイレベルのポリシーを処理できる。積極的に“拒否又は許可”ルールを維持することで、MLF はバックドアのセットアップやアクセス行為を阻止することを可能とする。



malware
indicators
virus
trojan
found
payload
symantec
request
malformed
sep
possible
dns
denial
service
downadup
spyware
infected
infection
file
malicious
adware
inbound
download
backdoor
orifice
exploit
exploitkit
security
risk
2000
encoding
195
vista
version
traffic
connection
blackhole
siemenspassword
trojandropper
gameover
downloader
fake
dabber
amanda
door
lolcat
trin00
access
angler
rwwwshell
stage
march
installshield
pluginDetect
zeroaccess
opachki
mydoom
sasser
mariposa
fiesta
rig
remote
repeated
nimda
attempt
exfiltration
link
plugin
trojanspy
cryptolocker
infector
edwards
conficker
alert
oct
magnitude
deepthroat
ssl
unwanted
rat
xtea
duqu
toolkit
packed
struct
backconstruction
netbus
win32
agent
server
daemon
downloading
topex
ransomware
trojandownloader
quarantined
backup
visited
outbound
ebury
http
archie
sinkhole
synapse
clickfraud
channel
ddos
user
admin
office
uri
code
2015
m2
codered
apache_mod_ssl
email
java
sapphire
subseven
deleted
sweet
zeus
stuxnet
sql
kernel
orange
backorifice
execution
poisonous
campaign
smb
level
generic
anubisnetworks
driveby
microsoft
wiper
nuclear
cryptowall
loki
enc
fin
morto
foxivika
win
nov
improper
windows
infections
worm
mobile
executable
slapper
rootkit
config
iframe
window
registry
activity
hackattack
dalexis
encrypted
you
be
vbs
bot
pack
website
c2
spy
typot
trojaned
red
ie
june
number
client
cert
changer
brown
gh0st
write
safe
data
response
netwire
covert
detec
installer
suspicious
binary
silent
from
discovered
downloaded
certificate
p2p
failed
cleaned
potentially
delete
back
here
retrieval
custom
downloader_trojan
2013
tool

サイバーキルチェーンフェーズ 6　遠隔操作（C2）

定義: Lockheed Martin は、このフェーズを“不正アクセスされたホストは、通常、C2 チャネルを確立するインターネット上のコントローラーサーバへと繋がる起点となる。APT マルウェアは、自動的に活動開始するのではなく遠隔からの手動での命令を待つこととなる。ひとたび C2 チャネルが確立されると、侵入者は標的の環境内でハンズオンでのキーボード操作が可能となる。[13]”と説明する。

防御者の目的: 長期に亘る攻撃者のリモートアクセス能力を削ぎ、敵のアクセスを止める。

ピンポイント対策

- 適切なネットワーク分離を確保する
- 偵察からの阻止的戦術に戻る
- ピアツーピア (P2P) トラフィックを制限する
- 単独マシンによる DNS クエリの上限値をセットする
- 外部 C2 サーバへの通信をブロックする
- DNS シンクホールを利用する
- 積極的にドメインカテゴリのブロックを行う

標準的な推奨事項:

- 進入と退出の監視を行う
- 監査/トラフィックログを確保する
- ログのモニタリングを実施する
- 認証プロキシーを利用する

クリティカルセキュリティコントロール:

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバ上のハードウェアとソフトウェアに対する安全な設定
- CSC 5: 管理者権限の使用をコントロール
- CSC 6: 監査ログの保全、モニタリングと分析
- CSC 9: ネットワークポート、プロトコルとサービスの限定と管理
- CSC 16: アカウントのモニタリングとコントロール

C サイバーキルチェーンフェーズ 6 遠隔操作（Command and Control (C2)）

ケーススタディ時間軸、観察と影響

遠隔操作(C2)フェーズに関連するイベントの順序は以下の時間軸で表される。

図 19:遠隔操作フェーズに関連するイベントの時系列

この時点の攻撃までに、攻撃者は RAT のインストールを経て、持続能力を確保し、インフラへの遠隔操作の接続を構築できた。C2 フェーズでは、RAT はリモートの IRC サーバと通信し、人気のあるソーシャルメディアサイト上の攻撃者がコントロールするプロフィールから指示を得た。RAT は定期的にプロフィール上に投稿された内容を確認し、更なる悪意ある活動のためにその内容を指示として解釈した。これらの通信のいくつかはログに記録されたが、PPFC では、ひとたび異常行動を探す分析がスタートすると、それらを"敵"と認識するだけだった。

攻撃者は、複数の C2 チャンネルを使って、PPFC 環境内に持続する存在を確立し、さらに彼らのアクセスを広げて PPFC 内のエクスプロイトを継続する意志を示した。このような C2 活動をあぶり出す上での重要なチャレンジは、全ての有効なネットワーク活動においてそれを探知することである。

サイバーキルチェーン考察

この後半フェーズでも、C2 が起こるのを防げれば、防御者はまだ成功の可能性があることを認識することは極めて重要である。攻撃者は、C2 の確立が成功するまでは、彼らが獲得したアクセスを活用できない。たとえ攻撃者がホストに RAT をインストールすることに成功しても、もし攻撃者がそれとやり取りできなければ、彼らは目的を達成できないであろう。

遠隔操作は、攻撃者が標的システムを直接支配できるようにし、彼らに更なるアクション（例　データの不正転送、破壊又は操作）を取るために余裕を持ってその環境に戻ってくる能力を与える。多くの攻撃において、攻撃者がアクセスし、被害者の環境から標的となるデータを抽出できるようになるまでに C2 は数ヶ月継続している。C2 はまた、攻撃者が当初不正アクセスしたシステムから標的の環境にある他のシステムに移ることも許容する。

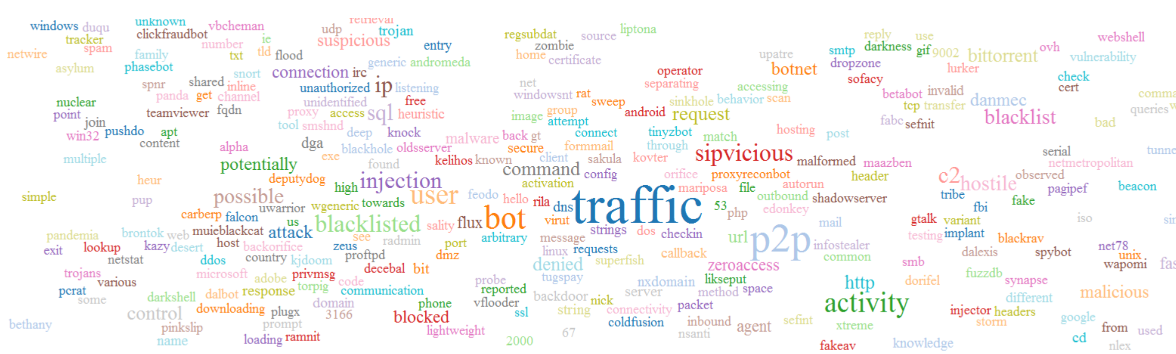
もし防御者が C2 通信を認知してブロックし、侵入された内部システムを修正するなら、これらの成果は全て不可能となる。組織は、多くの C2 システムが代替の通信手段をもっていることを認識すべきである。一つのチャンネルをブロックしてその他を開けたままとするのは、攻撃を止められないばかりか、さらに侵入する攻撃者の時間を買うことができるといった間違った安心感を作り出してしまう。

クライアントによって観察された敵のトラフィックの 14%超は遠隔操作に関連していた。PCI が重要であるクライアントにおいては、遠隔操作は敵のトラフィックの 8%以下であった。

ピンポイント対策

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有し、その結果、次の攻撃フェーズに成功裏に進む彼らの能力を妨げることになる。

- 適切なネットワーク分離を確保する– ネットワークセグメンテーションに検出と警報を統合することで、侵入されたホストによる更なる活動を止めることができる。適切なセグメンテーションは、ネットワーク構造の集合において、許可された通信を通し、許可されない活動をブロックするための ACL や内部ファイアウォールを含んでいる。不正な内部通信の認知は不正侵入の広がりを抑える助けと成り得る。
- **偵察からの阻止的戦術に戻る–**脅威が侵入プロセスの深いところまで達し、攻撃者は遠隔操作の確立に成功しているかもしれないけれども、攻撃者が内部システム上で更なる偵察を実施するために侵入されたホストを利用するのは一般的である。このようなアクセスは、本来的に、セキュリティ侵害の継続的な拡張のために内部偵察で始まるキルチェーンフェーズを繰り返す。組織は、探知とこの行為のブロックに向けて、内部をモニターすべきである。
- **ピアツーピア (P2P) トラフィックを制限する** – 組織は、Microsoft Skype、Cisco Jabber などの P2P ツールをサポートするかもしれない。ボットマスターはしばしばコマンド、ツールや追加的リソースを侵入されたホストに送付するために P2P を利用する。適切に P2P を無効化すれば、もし攻撃者の計画が P2P ベースの C2 インフラを用いているなら彼らを阻止するだろう。
- **単独マシンによる DNS クエリの上限値をセットする**– ボットはしばしば彼らの遠隔操作のサーバを辿られないようにするためにドメイン生成アルゴリズム(DGA) を使用し、当該サーバのブロックを困難にする。しかしながら、単独マシンからの DNS クエリ回数を制限することは、これらコネクション行為を阻止するかもしれない。
- 外部 C2 サーバへの通信をブロックする– 対応者はしばしば最初に感染を除去しようとする。しかしながら、最初に既知又は C2 予備軍のトラフィックに注意を向けるべきである。この"蛇の頭切り"の方法はその後の通信を邪魔することになる。影響を受けるホストを特定し全ての C2 手法をブロックすること。ホストの修復は、ひとたび通信がブロックされ分析が完了したら行うことができる。
- **DNS シンクホールを使う**– 悪意あるドメインとの通信を阻止するために DNS シンクホールを設定する。これは、それらのドメインに対する信頼できる DNS サーバのなりすましによって行われる。攻撃者がこれらのドメインにクエリを投げると、DNS シンクホールがルーティングできない IP アドレスを返し、その後のいかなる活動も破壊することとなる。
- 積極的にドメインカテゴリブロッキングを行う–ほとんどの組織が、既知の悪意あるドメインをブロックするためにプロキシカテゴリ化を利用する。攻撃者はこれを知っていて、カテゴリブロッキングを避けるために使い捨てのドメインをしばしば作成する。攻撃者はまた、ダイナミック DNS、オンラインストレージや メッセージングドメインのような他のサービスを利用するかもしれない。積極的な姿勢を示しこれらのカテゴリ（とカテゴライズされていないいかなるもの）をブロックすることにより、多くの C2 の源に成り得るものへのアクセスを拒否することができる。



サイバーキルチェーンフェーズ 7　目的実行

定義: Lockheed Martin は、“侵入者は、6 つのフェーズを経た後になって初めて、当初設定した目的を達成するためのアクションを取ることができる。この目的の典型例は、被害環境から情報を収集、暗号化そして抽出する、データ不正転送である。データの完全性や可用性を壊す行為も有り得る。又は、侵入者は、最初の侵入システムを他のシステムへの侵入やネットワーク内の横展開のための踏み台として利用するだけかもしれない。”と定義している。

防御者の目的: 攻撃者がセンシティブな情報を発見し、アクセスし、抽出する能力を削ぐ。

ピンポイント対策

- センシティブ情報を含む共有フォルダーへのアクセスを制限する
- ID 管理を強化する
- データアクセスコントロールを実施する
- 不正な横展開を探知し、軽減する対策を実施する

標準的な推奨事項:

- 組織のリスクプロフィールを更新する
- 適切なネットワーク分離を確保する
- 定期的なデータとシステムのバックアップを実施する
- 全データベースへのセキュリティレイヤーを維持する
- DDoS 発生時には他の悪意ある活動に注意する
- ウェブアプリケーションディレクトリーをパスワードで保護する
- 多様なログモニタリングを実施する

クリティカルセキュリティコントロール:

- CSC 3: モバイル端末、ラップトップ、ワークステーションとサーバ上のハードウェアとソフトウェアに対する安全な設定
- CSC 13: データ保護
- CSC 14: Need-to-know 原則に基づくアクセスコントロール
- CSC 19: インシデントレスポンスと管理

サイバーキルチェーンフェーズ 7:目的実行（Actions on Objectives）

ケーススタディ時間軸、観察と影響

目的実行フェーズに関連するイベントの順序は以下の時間軸で表される。

図 20: 目的実行フェーズに関連するイベントの時系列

ある第三者機関が PPFC に接触し、PPFC の内部情報がペーストサイトに掲示されていたことを伝えた。この接触まで、PPFC は彼らが不正侵入を許し、攻撃者が最も価値のある情報のいくつかを抽出していたことを認識していなかった。攻撃者は全 CKC 行程を検知されずに進み、価値ある情報を探し、選んだデータベーステーブルの内容をダンプしていたのである。

PPFC がそのセキュリティ侵害を知らされた後、彼らはインシデントレスポンスサポートを受けた。分析者はほとんどのアタックの証左をウェブ、システムそしてセキュリティログ内に見つけた。

成功する目的実行を防ぐためのいくつかの主だったチャレンジは次の通りである。

- **最も価値のあるデータの特定**—最も価値のあるデータを守るために、組織はそのデータと重要システム、プロセスそしてその管理するスタッフを特定しなければならない。もし組織がその鍵となるデータとシステムを正確に把握していなければ、それらを適切に守ることは困難となる。
- **鍵となるデータの能動的管理–** ひとたび特定されたとしても、鍵となるデータの管理はまだ難しい。組織は通常、守るべきシステムと環境に関するセキュリティを定義し、実データを守るために設計されたセキュリティ対策は疎かにしてしまう。

サイバーキルチェーン考察

キルチェーンにおける目的実行フェーズは、攻撃のゴールである（しかしいつも攻撃者の活動の最後とは限らない。）。
他の各フェーズ、つまり標的の発見、その調査、脆弱性の発見とエクスプロイト、アクセスの獲得、そして利用又は販売するデータ抽出のような目的の達成は、ここに到達するために行われてきた。

ひとたび攻撃者がアクセスしたならば、防御者のゴールは横展開を防ぎ、データ不正転送を検知することとなる。組織は、特に極めて重要なデー

目的実行は全ログの 0.0003%と最も少ない数のログで確認されたが、全アラートタイプの中で最も確実性が高かった。

タを有するシステムに関して、検知された横展開や権限の獲得を阻止する対策を実施するべきである。

組織は攻撃者が標的環境に滞在できる時間を少なくできる。彼らの環境内の行動のログを取り、モニタリングすることによって、その"標的上の時間"を少なくできる。組織は攻撃者の"標的上の時間"を目立たせることができるので、アクセスを制限し、データを保護する対策を含むことによって、彼らが目的実行を取る前に攻撃者に対応する時間を組織に与えることとなる。

ピンポイント対策

これらのピンポイント対策はこのキルチェーンフェーズにおける攻撃者の活動を阻止する可能性を有する。

- **センシティブ情報を含む共有フォルダーへのアクセスを制限する**– 攻撃者は、しばしば、センシティブ情報を保護する対策が全くなされていない共有フォルダーを発見する。これらのリソースは、攻撃者が上位権限者のユーザーネームやパスワードを特定することを許してしまうかもしれない。この共有情報へのアクセスは制限され、通常のユーザーよりも厳しい権限を要求すべきである。
- **ID 管理を強化する** – 効果的なグループ権限で管理された利用者集団に紐付けられた強固な認証は、誰がどの資産へのアクセス権を有するのか制御するのを助けることができる。組織のセキュリティの改善に向けて、これをよく定義された need-to-know システムと積極的なアクセスモニタリングに組み合わせることも有効である。もしデータアクセスが厳格なプロセスを経て調査され、承認されるなら、主要データへの不正アクセスの可能性を減少させることができる。強力な ID 管理策も、効果的な DLP ソリューションと効果的なロギングのような追加策として非常に重要である。
- **データアクセスコントロールを実施する**– 組織は、センシティブデータの不正使用や持出しを検知するために、情報のタグ付け、パケット調査、ネットワーク監視などと共に、適正な DLP ソリューションを設定し、テストするべきである。データベースアクティビティの監視と共に、データアクセスの精緻化を改善する。アクセスされているデータを監視することにより、攻撃が現に進行している間に、組織が被害を軽減するためのアクションを取ることができるかもしれない。
- **不正な横展開を検知し、軽減する対策を実施する**– 目的実行フェーズでは、しばしば攻撃者は、彼らがネットワーク内でリーチを広げようとするとき、ゆっくりかつ慎重に動くだろう。内部 IDS、IPS その他の対策を境界だけでなくネットワーク内で実施することは、不正アクセス行為の特定を助けることにつながり、インシデントレスポンスを行っている際にその有効性を感じることとなる。

PPFC ケーススタディ：結論

我々のケーススタディは、実際の NTT グループセキュリティンシデントレスポンスの事案を紹介した。このスタディでは、どのように攻撃者が検知されずに PPFC の環境に侵入したのかについて述べた。

攻撃者はサイバーキルチェーンの全 7 フェーズを辿った。彼は以下の行為を行った。

- 脆弱な標的を見つける偵察
- 脆弱性をエクスプロイトできるソフトウェアを選択し設定する武器化
- SQL インジェクション攻撃を伝送する配送
- 標的データベースと基本システムの詳細情報を入手するエクスプロイト
- 一貫したアクセスを許容することとなる、リモートアクセス型トロイの木馬、攻撃者コントロールアカウントのインストール
- 検知されずに攻撃を継続する遠隔操作
- PPFC の大量のデータを外部に持ち出す目的実行

適切な対応の導入により、PPFC はこれらのフェーズのいずれかの時点で攻撃を阻止できたかもしれない。代わりに PPFC は、NTT グループが多くのケースで見てきたように、攻撃を検知し、阻止するためには不適切である一貫性のない対策を実施した。これは、価値ある PPFC のデータが公のウェブサイトにアップロードされるという事態を招くことに繋がった。

インシデントレスポンス：傾向が示す組織の対応不足

ケーススタディとサイバーキルチェーンの調査で示されたように、インシデントは発生する。そしてそれらが発生した時、組織は対応する準備を整えていなければならない。2015 年において、NTT グループは顧客に影響を与えるサイバーインシデントの対応に関与し続けた。年間を通して、極秘情報の漏洩、サービス妨害攻撃、内部者の脅威といった見出しがメディアに踊っていたが、2015 年に NTT グループが収集したデータは、組織がこのような攻撃に対する備えを十分に行っていないことを物語っている。

CKC のような概念を活用する上で求められる重要なことは、検知や防御の対策だけでなく攻撃が発生した時の対応能力にも投資をするということである。

2015 年 GTIR のこの章では、組織がどれだけ準備しているのか、NTT グループによって観察されたインシデントの種類、そして効果的なインシデントレスポンスのために考慮すべき基本ステップについて説明している。

不十分な投資と準備不足が未だに主な原因である

インシデントレスポンスへの従事の間、NTT グループはインシデントの影響ばかりでなく組織がどれだけ適切に対応準備を行ったかに関する指標を追跡した。残念ながら、多くが NTT グループインシデントサポートを利用した。なぜなら、彼らはインシデントレスポンス能力にほとんど投資してこず、よって対応に必要な技術知識も攻撃をその発信源に突き返す能力も持ち合わせてなかったからである。

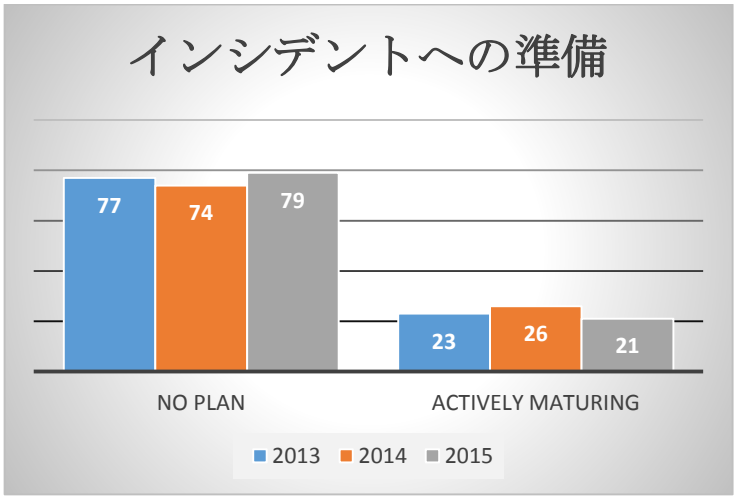


図 21: 適切に対応準備をおこなった企業の割合

2013 年以降サポートしたインシデントの傾向を観察してみると、準備に関してはほとんど改善が見られなかった。2015 年に、準備せず、正式なインシデントレスポンスプログラムを有していなかった組織にわずかな上昇傾向が見られた。過去 3 年間、平均 77%の組織が、このカテゴリに含まれ、残りの 23%だけが効果的に対応する何らかの能力を備えていた。

インシデントレスポンスのタイプ

2015 年、NTT グループは、マルウェア、 DDoS とセキュリティ侵害調査、スピアフィッシングと内部的脅威を含むいくつかのコアなインシデントカテゴリに焦点を当てた顧客サポートの提供を継続した。これらの分野で、昨年までと比べると、セキュリティ侵害調査、内部的脅威とスピアフィッシングが上昇し、マルウェアと DDoS 緩和サポートが減少する点を含むいくつかの顕著な変化があった。インシデントが複数のタイプに及ぶ場合は、最も重要なスレットベクターに応じて分類した。

NTT グループは、セキュリティ侵害調査の増加率に関し、昨年の 16%に対し今年は 28%を計測した。そして活動の多くがデータと知的財産の盗難に集中した。分析では、これらが標的型であり、偶然の攻撃ではなかったことが示されていた。

しばしば従業員や業務委託が関与する内部的脅威に関する攻撃の増加により、NTT グループはこれらの攻撃タイプに対する新たなカテゴリを作成した。2015 年、内部的脅威は昨年の 2%から全調査の 19%に急上昇した。これらの調査の多くは、情報やコンピューター資産を乱用した内部の従業員や業務委託者の結果であり、人事部によって事案化された。

同じような状況がスピアフィッシング攻撃に対するカテゴリを分割する結果となった。スピアフィッシング 攻撃はインシデントレスポンスへの従事の中で約 17%を占め、昨年から 2 ポイント上昇した。攻撃の多くが、小売業顧客の幹部と財務部社員を標的とした金融詐欺に関連していた。しばしば攻撃者は組織構成の詳細な知識を得ていて、巧妙に作成されたソーシャルエンジニアリングやスピアフィッシング 攻撃を行っていた。これらの攻撃のいくつかは組織をだまして架空の請求書を支払わせるものであった。

2015 年は DD4BC や Armada Collective といった DDoS ハッキンググループの台頭が見られたが、NTT グループは過去 2 年と比較して DDoS 関連サポートの減少に気付いた。この減少は、この種のタイプの脅威に対する守りの投資が継続していることに関係していると思料される。DDoS 軽減のための適切なツールとサービスの利用は、良く練られた攻撃に適切に対応するために不可欠である。NTT グループによって観察された成功した DDoS 攻撃も下降線を辿り、2015 年にはより少ないサポートが必要とされる結果となった。

NTT グループのインシデントデータでは、2014 年から 2015 年にかけてその顧客の中で DDoS 攻撃が減少している一方で、Recorded Future の分析では、ウェブ上での DDoS に関する調査において、DoS/DDoS についての議論が 25%から 35%増加したと説明している。

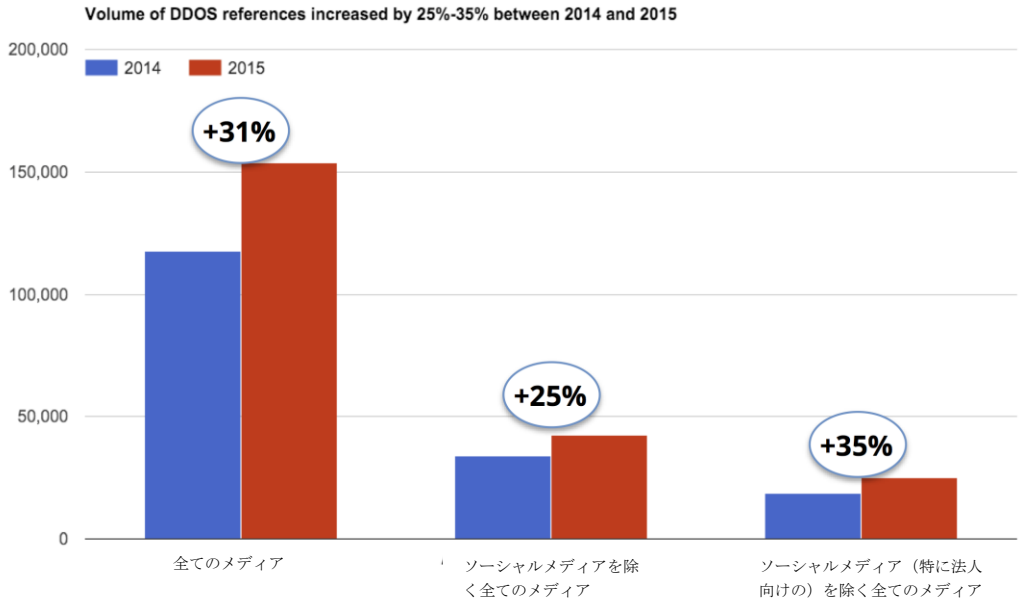


図 28: 記録されたインシデントの種類と上昇率

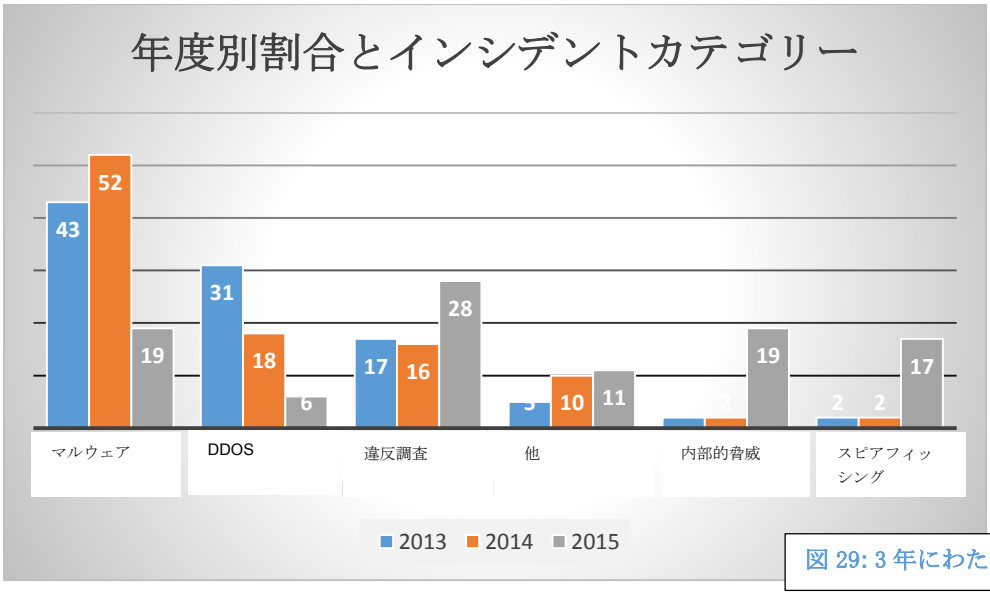
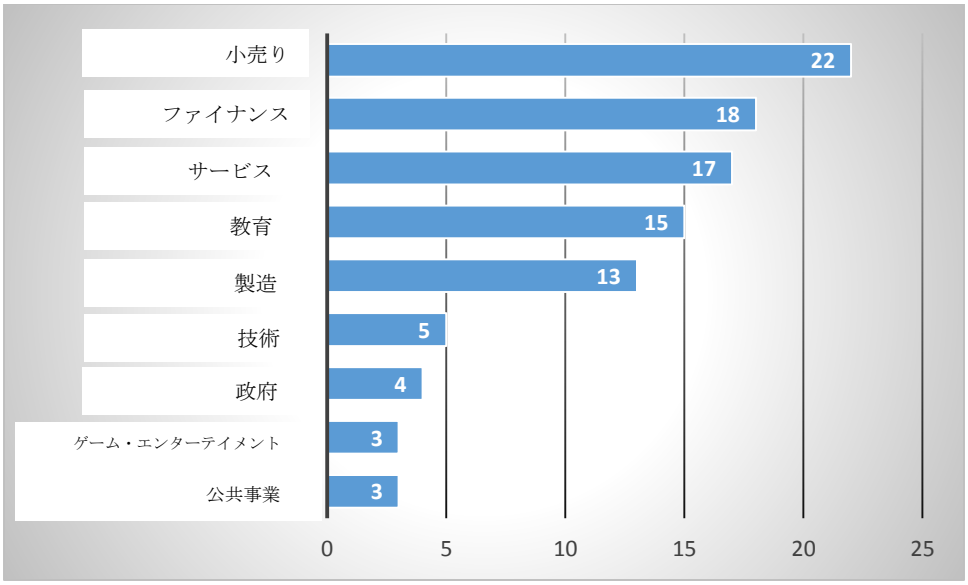


図 29: 3 年にわたるインシデントの割合

垂直的市場によるインシデント

金融業は我々の昨年の年次報告においてインシデントレスポンスに関するリーディング産業であったけれども、小売業が昨年から 12 ポイント上昇し、レスポンスへの従事数全体の 22%を占めるに至り 2015 年をリードした。これは、業種毎の攻撃の章で示した通り、小売業の顧客が顧客当たり最も高い攻撃数を経験したことを示すデータと呼応している。金融業は昨年の観察から約 10%減少した。前述したスピアフィッシング攻撃のほとんどは、小売業に集中しており、この領域におけるインシデントレスポンスの増加の一因となっている。



22: 業種別のインシデントエンゲージメントの割合

NTT グループの独立系サイバーインテリジェンスパートナーである Wapack Labs は、 2015 年活動における最大の増加は、キーロガーの世界的展開だったと報告した。Wapack Labs は、アカウント詳細をトーアベースのフォーラムで販売しているナイジェリアの実行者が、85 カ国以上に及ぶ 12,000 超のユニークなインフラに侵入したと報告した。“Daily Show”と参照される活動は、いくつかの地理的ロケーションに焦点が当てられているようで、主として海洋共同体と南シナ海でそれに賛同している国家、さらにはナイジェリアと黒海、スカンジナビア、スエズ運河を結ぶ海路が標的となっていた。.

Angler エクスプロイトキットは、観察された脅威活動において 2 番目の上昇となった。Wapack Labs は、この脅威に関する技術的な報告書を発行した。分析によると、標的にされた組織は観察された悪意ある活動のおよそ 90%が Angler の配送と推定する。

Wapack Labs は、ウクライナとの争いにおけるロシアのサイバーアクションのアカウントについて詳述した。Wapac Lab の意見としては、その活動のサイバー上の基盤は、Ivanov 理論（身体的活動と連動してサイバーや他の情報戦争ツールを用いる計画）を忠実に辿ることにある。

イランは、ツールの蓄積を開始し、他のサイバー戦争に関連する実行者達との関係を構築し続け、脅威世界のトップに躍り出た。イランは一つの大きな違いを伴ってニュー中国となったようである。イランは諜報活動に興味はないが、サイバー戦争能力に焦点を当てている。

Wapack Labs は、2015 年の攻撃が、物品、サービスやお金の移送を可能とする文書操作を伴った、完全性の攻撃に焦点を当てた諜報活動や盗難から変化したと報告した。サイバーセキュリティは急速に詐欺や物理的セキュリティ空間に移行しているのである。

なぜあなたは気にすべきなのだろうか？この報告で挙げられた組織のほとんどは、この種の攻撃を止めるに十分なセキュリティ対策を持ち合わせていない。この報告は、組織がより効果的なセキュリティ対策を作成するために必要な対策を特定するためのガイダンスを含んでいる。

インシデントレスポンス例: Emdivi

NTT グループが 2015 年に観察した多くのマルウェア変数の中に、Emdivi マルウェアに関連するいくつかのインシデントがあった。Emdivi は、日本の政府機関を標的とし 100 万人以上のパーソナルデータのセキュリティ侵害に貢献した APT 攻撃の鍵となる要素だった。

攻撃者はその機関を標的とし、電子メールの添付ファイルを通じ、ワークステーションを Emdivi マルウェアで感染させた。結果として、攻撃者は約 125 万人のパーソナルデータを曝け出した。その機関は唯一の例である。なぜなら攻撃は Emdivi 攻撃だけではなかったからである。Emdivi の分析は、次の一貫した特性を示した。

- RAT（リモートアクセス型トロイの木馬）が関連していた
- 日本の機関に焦点を当てた
- ワークステーションシステムを通じて情報を収集した
- 標的型攻撃の中でも水飲み場型攻撃を用いた

最終的にその機関に対する攻撃は成功した。NTT グループはこれらの攻撃の成功に貢献したいくつかの要因を観察した。

要因	詳細
情報共有の欠如	● C2 サーバと同じようなドメインを使ったインシデントが以前にも発生していたが、日本政府は情報を共有しなかった。2015 年 4 月から 5 月にかけて、日本政府内の複数の他の機関で、これらのインシデントは発生した。 ● 5 月の攻撃は防御できたが、詳細は十分に共有されず、他の機関は重要な的を絞った改善をできなかった。
規則に関する対応の欠如	● 規則は適切な内容を欠き適用されなかった。 ● 規則の遵守は優先的位置付けとされなかった。 ● その機関は規則上で実行不可能な内容を強要していた。
不適切なモニタリング	• その機関はログを収集していたがそれらを監査していなかった。
不適切な初動対応	• 添付ファイルのチェックの遅れが、更なる感染を許した。 • その機関は、1 台の感染したコンピューターを検知しネットワークから隔離した。しかしながら、他の感染し、検知されなかったコンピューターは依然接続されていた。

図 23:機関別の要因

Emdivi のようなマルウェア感染は検知された時でさえも非常に重要な影響をもたらし得る。この機関の場合、個人情報のセキュリティ侵害の拡散は、正式な対応とコミュニケーションの欠如に起因する感染によってもたらされた。

インシデントレスポンス推奨事項

2015 年、NTT グループは、多様な垂直的市場の顧客に影響する、多くの異なる種類のインシデントレスポンス活動を支援した。組織が効果的に対処する上で一貫して能力不足に陥いるいくつかの状況がある。以下の推奨事項は、包括的なプログラムとするのに必要なことと NTT グループが観察したいくつかの共通問題の明示に資する内容の一部に過ぎない。

- **インシデント管理プロセスと"対応指示書"を準備する** – 多くの組織がインシデントを宣言し、分類する方法に言及した十分なガイドラインを有していない。これらは確実に対処を開始するのに極めて重要であるにもかかわらずだ。攻撃タイプ、想定される影響その他要因に応じて、対応活動はかなり異なってくる。インシデントレスポンスの常識は、組織は共通インシデントがどのように彼らの組織内で対処されたのかを述べた"対応指示書"を作成するべきと示唆している。例えば、もし DDoS 活動があなたの組織に対してしばしば用いられるならば、あなたの対応チームが、利用可能なツールと能力に基づいて参考にできる手続きについて言及した対応指示書を作成することは有効な投資となる。
- **あなたの対応の効果を評価する** – 我々は、ほとんどの組織が彼らの計画の効果をテストしているのを見たことがない。インシデントが発生した時、あなたが最も望まないのは、標準的なインシデントレスポンスの手続きの理解が欠如していることだろう。準備状況の評価は、定期的なテストのシナリオに含めるべきである。文書に対する事後検証を念頭に置き、改善を要する部分と同様に上手にできた対応活動を元にする。

- **あなたのエスカレーション名簿を更新する**– 組織が成長し、役割が変わるにつれて、誰がインシデントレスポンス活動に関係するかに関連した文書を更新することは重要である。時間はインシデントレスポンスにとって重要で、必要な人をすぐに巻き込めないことは、あなたたちの有効な対応の妨げになる。あなたの ISP、外部のインシデントレスポンスサポート、その他提供者のようなベンダーのコンタクト情報を更新することも同様に重要である。
- **技術文書を準備する**– 間違いのない決断を下し、影響を受けたシステムを特定するために、あなたはネットワークについて包括的で正確な詳細を保有しなければならない。これには以下を含むべきである。
    - IP レンジとホストネーム
    - DNS 情報
    - ソフトウェアと OS の名前、バージョン、パッチレベル
    - ユーザーとコンピュータのロール
    - ネットワーク間の出入ポイント

組織がインシデントへの対応準備を整えた時にだけ、影響を効果的に軽減することを望める。これらの推奨事項とサイバーキルチェーンケーススタディにて特定された他のものは、高レベルの脅威に対する備えの実現を助けることができるのである。

スレットインテリジェンスにおけるサイバーキルチェーンの役割

NTT Group は、最近、Lockheed Martin のサイバーセキュリティアライアンス（ベストプラクティスを共有し、洞察を得て、強みを掛け合わせるために形成されたコミュニティ）に加入した。今回の GTIR では、CKC そのものと、スレットインテリジェンス（TI）と CKC が如何に相互に補完し、強化し合っているかに焦点が当てられている。

NTT グループグローバルスレットインテリジェンス報告書 2015 年版で、我々は、スレットインテリジェンスの中心的役割は脅威環境において進むべき道を示すものと定義した。

この章では、効果的な TI プログラムと、実績のあるインテリジェンスに基づく（Lockheed Martin が CKC のベースとしている）防御の組合せが、どのようにあなたの組織に適用できるかについて述べられている。NTT グループのセキュリティ分析者は、この組み合わせが提供するいくつかの利点について指摘し、スレットインテリジェンスの特定要素としての属性の重要性を示し、そしてあなたのインテリジェンス情報源の妥当性と信頼性の確保に関する洞察を共有している。

スレットインテリジェンスディベート

2015 年を通じ、スレットインテリジェンスの有益さに関する議論は留まることを知らず、ディベートはなおも続いている。

スレットインテリジェンスプログラムは本当に価値があるか？挑戦者は、“スレットインテリジェンス”はせいぜい使われ過ぎの産業界のバズワードであり、曖昧であると思っている。同様の調子で、反対者は、ベンダーは“情報（intelligence）”とは別の“情報（information）”を売っていると思っている。

しかしながら、適切に定義され実践され、スレットインテリジェンスは絶対的に必要なものとなっている。まばたきする間に変わる漏洩データと指標によって、ネットワーク防御者は単純に彼らのネットワーク環境における ID、トラッキング、ロギング、実行の変化について行けなくなっている。実際、いくつかの漏洩データと指標（例　悪意ある本体データ、URL、IP アドレス）は非常に短命な存在なので、標的型攻撃で一度使われるだけかもしれない。

あなたの組織は、スレットインテリジェンスの活用によって、あなたを標的としている攻撃者を特定し、彼らの戦術、ツールや手続きを分析するのが容易となり、結果として組織の対応能力が強化される。スレットインテリジェンスはまた、あなたの環境の脆弱性に対する非常に価値のある洞察を与えてくれる。

> スレットインテリジェンスはまた、攻撃者の動機と意向に気付きを付加してくれる。盗難データがどのように利用されるか考えてみよう。誰があなたのデータを欲しいのだろうか、なぜ？攻撃者は単に脆弱なホストを探すためにインターネットをスキャンしているのだろうか？それとも彼らは狙いをつけてあなたの組織を狙っているのだろうか？攻撃者の経歴、能力、意向と方法を理解することは、あなたの組織が標的になるかどうかを決定する上で助けとなり、あなたのサイバー防御費用の最適化に役立つだろう。

ここで最低限言えることは、スレットインテリジェンスが特にあなたのサイバー防御戦略で他のツールと一緒に使われた時、信じられないほど価値あるものとなるということである。

*2015 年 NTT グループグローバルスレットインテリジェンス報告*で述べられているように、有意義かつ実行可能なインテリジェンスは“全てに通じる”解決策ではなく、あなた自身の組織にとって最適なインテリジェンスを定義することは、スレットインテリジェンスプログラムの実施を成功させる上で極めて重要なのである。

関連付けられたスレットインテリジェンスと CKC

サイバーキルチェーンとスレットインテリジェンスのどちらも万能ではないが、一緒になるとそれらはサイバー防御戦略に大きな力を与えてくれる。CKC は、良く知られた産業概念で、その効果が証明されているモデル（典型的なサイバー攻撃の進行の可視化を助けるよう設計された青写真）であり、阻止的アクションが攻撃者に対して取られることを通じてポイントを明らかにしている。スレットインテリジェンスプログラムと一緒にこのモデルを使用することにより、脅威を解決するための見事なロードマップが作成でき、その結果、組織が優勢になり、攻撃者の計画を阻止することになる。サイバーキルチェーンケーススタディでは、NTT グループは、まさにこれを行うためのフレームワークの確立を手助けするために、Center for Internet Security のクリティカルセキュリティコントロールを使っている。

CKC のゴールは、敵を最も早いフェーズで食い止めることである。より野心的なゴールは、サイバーキルチェーンに先行し続けることであり、また、攻撃者が CKC のフェーズ 1（偵察）を開始する前に脅威を阻止又は特定することである。

スレットインテリジェンスは、あなたのセキュリティギャップを特定するばかりでなく他の CKC フェーズにおける阻止策を特定するために、CKC の各フェーズを通じて利用できる。しかし、CKC が作用する前であっても、スレットインテリジェンスはベストな形で実施される必要がある。

敵がコンピューターの前に座る前に、彼は動機と意向を持っており、標的リストを作っている。攻撃者の意向、経歴、能力又はサプライチェーンの知識を有することにより、組織は自らとその顧客を守る道を増やすことができる。セキュリティ分析者は、ツール、技術と手続きの特定を助け、可能であれば特定の攻撃者又は攻撃グループを隔離するために、トラフィックログ（例　ポートスキャニングや他の偵察ステップの観察）を調査してこの情報のいくつかを集めることができる。

CKC はまた、マルウェアベース攻撃の概要を把握する優れたツールである。マルウェア配送に非常に強く関係している攻撃ベクターは、おそらく攻撃者の作戦帳で最も過小評価されているソーシャルエンジニアリングである。これは、強力なサイバー意識向上プログラムで最も適切に取り組まれている。

しかしあなたは、簡単には一般的要件に基づく訓練プログラムを開発することはできない。効果的なセキュリティ認知・訓練プログラムを作成するためには、あなたの組織にとって最も重要な脅威と対策に焦点を当てた内容を計画する必要がある。

あなたの組織に内在する資産を超えて、サードパーティベンダーやビジネスパートナーのような関係者も考慮する必要がある。彼らは彼らのネットワーク上で脆弱性を有し、それが共通インフラを介して攻撃者にあなたのビジネスに入り込む道を与えるかもしれない。あなたは顧客データと共にあなたのデータを守る必要がある。あなたがどんな情報を有しているのか、誰がそれを欲しがっているのか、そして敵はそれを何に使うのかを知ることは必要不可欠である。効果的なスレットインテリジェンスにより、攻撃者がいかにあなたに直接的又はベンダーやパートナーを通じて間接的に忍び寄るかの分析が容易となる。

CKC とあなたのスレットインテリジェンスプログラムはセキュリティシステム上の不可欠な部分として位置付けられなければならず、そうすることによってあなたの組織は、脅威に対して積極的かつ回復力を有する組織になれるだろう。インテリジェンスは終わりなきプロセスであり、あなたの環境で起こっているイベント、あなたの産業のトレンドそして地政学的イベントは全て、あなたのスレットインテリジェンスプログラムの成功に影響を与える重要な要素なのである。

外部のスレットインテリジェンス情報源

あなたの内部データを外部のスレットインテリジェンス情報源で補完すれば、あなたは内部で発生した（本来的に極めて限定的な）スレットインテリジェンスに制限されない。様々な情報源からのデータ収集、それを全て繋ぎ合わせること、文脈を理解し、それを何度も精査することは強力なスレットインテリジェンスのソリューションにとって重要な点となる。

24/7 のセキュリティオペレーションセンター(SOC)を有する組織との提携を模索し、そこからあなたは最新の IOC を入手できる。外部のスレットインテリジェンスサービス提供者は、様々な情報源を有し、出現している脅威に対する実施可能な忠告から、より戦略的な思考のための毎月、四半期毎の報告書まで幅広い報告を提出するべきである。

属性の重要性

セキュリティ産業は、過去数年に亘り、サイバー防御においてより大きな役割を担っている属性（サイバー攻撃や情報漏洩の背後に潜む実行者を決定する）を観察してきた。既知の悪い IP とドメインをブラックリスト化する標準的な方法は、次第に無駄な努力になってきている。多くの IOC は、実行者が彼に繋がるドメインを変更するかもしれず、攻撃後に無意味になる。

それはそれとして、決定的な属性を掴むのは極めて困難である。このためにはフォレンジック能力は必要だけれども、ただ属性追跡するだけでも、あなたの組織が直面しているサーバ防御への挑戦の高度な理解につながることとなる。敵は依然人間で、敵の活動の分析はしばしば目に見える人為的結果を示す。敵はエゴ、意向、動機を有している。これらの意向は、主に Anonymous のようなハクティビストグループによって公にされる。しかし他の場合の意向は不明瞭である。

敵の TTPs の分析は多くの点で役に立ち得る。

- あなたが積極的にブロックできる敵のインフラを特定する
- あなたの優先順位の高いインフラと資産（あなたの環境で攻撃者が標的としているものをベースに）を特定する
- 敵の TTPs に基づき、Red-teaming とあなたの環境に対する脆弱性評価を支援する

加えて、属性によって、あなたの組織は、サイバー防御優先順位に基づいて資金をどのように投下すべきか決定できる。例えば、あなたがサイバー攻撃の原因を幹部陣が耳にしたことのある特別な持続的標的型攻撃(APT)とできるならば、グループの悪評を避けるために幹部陣にサイバー防御に資金を当てるよう働きかけることができる。

より多くの国とハクティビストがサイバー上で抜け目なく行動しているので、地政学も次第に重要な役割を演じるようになっている。実行者たる国家とハクティビストは同様にマシン、ダム、送電網の維持システムに対する影響から、標的の考え方（例　プロパガンダの普及）に対する影響へと軸足を移している。もし標的が、敵がそれを使う能力や単に意向を有していると知ったら、これにより標的が自らを守る手段を変更するかもしれない。例えば、ロシアとの衝突が継続していた時にウクライナ国民の多くに対する恣意的な停電があったことを考えてみよう。属性はまだ決定的ではないものの、利用されたマルウェアと TTP はロシア関係の実行者を示唆している。この属性は、正確か否かは分からないが、ウクライナの民衆がもしロシアがそれを使う能力と意向を有していると思えば、彼らの心理に影響を与えるのである。同様の攻撃でこの力を主張するロシアの考えは、将来のウクライナの行動を決める要因になるかもしれない。

属性と敵の TTP 分析の根本的なゴールは、各ステークホルダーにスレットインテリジェンスを提供する広範なプログラムの一部に組み込まれることにあり、また、セキュリティへの資産を優先的に配分するための積極的な働きかけをサポートすることにある。

スレットインテリジェンス：サマリー

境界の防御という伝統的な手法は攻撃の防止という点では次第に無力になってきている。攻撃者は攻撃手法を継続的に洗練させ、開発者はアンチウィルス回避能力を有するマルウェアを開発するとともに攻撃者は防御対策の数歩先を行っている。これらの全ては、サイバー防御に対し、より積極的な、回復力のある、適用力のあるアプローチを要求している。

スレットインテリジェンスプログラムの目的は、出現している脅威がビジネスに影響を与える前にそれらを特定することにある。直接的な脅威の数を減らすことはリスクを減らすことになり、よって収益性を維持又は向上させることとなる。脅威事案と発生源を特定し、分析することを優先させるために、スレットインテリジェンスチームは最初に組織が脆弱性として何を特定したかを理解しなければならない。

これらのツール（CKC, スレットインテリジェンス, 属性, 外部リソース）は、あなたのサイバー防御プログラムをより有能に、機動的にそして適合性の高いものにするのを助ける不可欠な要素であることを肝に銘じて欲しい。また、あなたは、防御プログラム全体の開発と実施において柔軟であるとともに、あなたのネットワーク全体の回復力と生存能力を高めなければならない。

グローバルハニーネット分析

NTT グループのセキュリティ研究者は CKC の偵察フェーズをより良く理解するために NTT グループのグローバルハニーネットからのハニーネットデータを分析した。

2015 年からのデータは、100 カ国以上に設置されたハニーネットセンサーに対して行われた約 1.05 億回の攻撃から成っていた。データは 206 カ国、372,000 ユニーク IP アドレスからの攻撃を含んでいた。研究者たちは、その事案をサービス関連カテゴリに分類し、偵察の観点からそのデータを分析した。

攻撃カテゴリ

セキュリティ研究者は、年間を通じて、多くの異なる攻撃カテゴリを観察した。トップ 5 カテゴリは、SMB/NetBios/Samba (Directory Services)、SSH、HTTP、SQL そして VoIP 攻撃だった。

攻撃回数順	攻撃カテゴリ	平均攻撃回数/日
1	Samba	128,000
2	HTTP	80,000
3	SSH	14,300
4	SQL	6,400
5	VOIP (SIP)	3,700

図 32:攻撃カテゴリのランキング

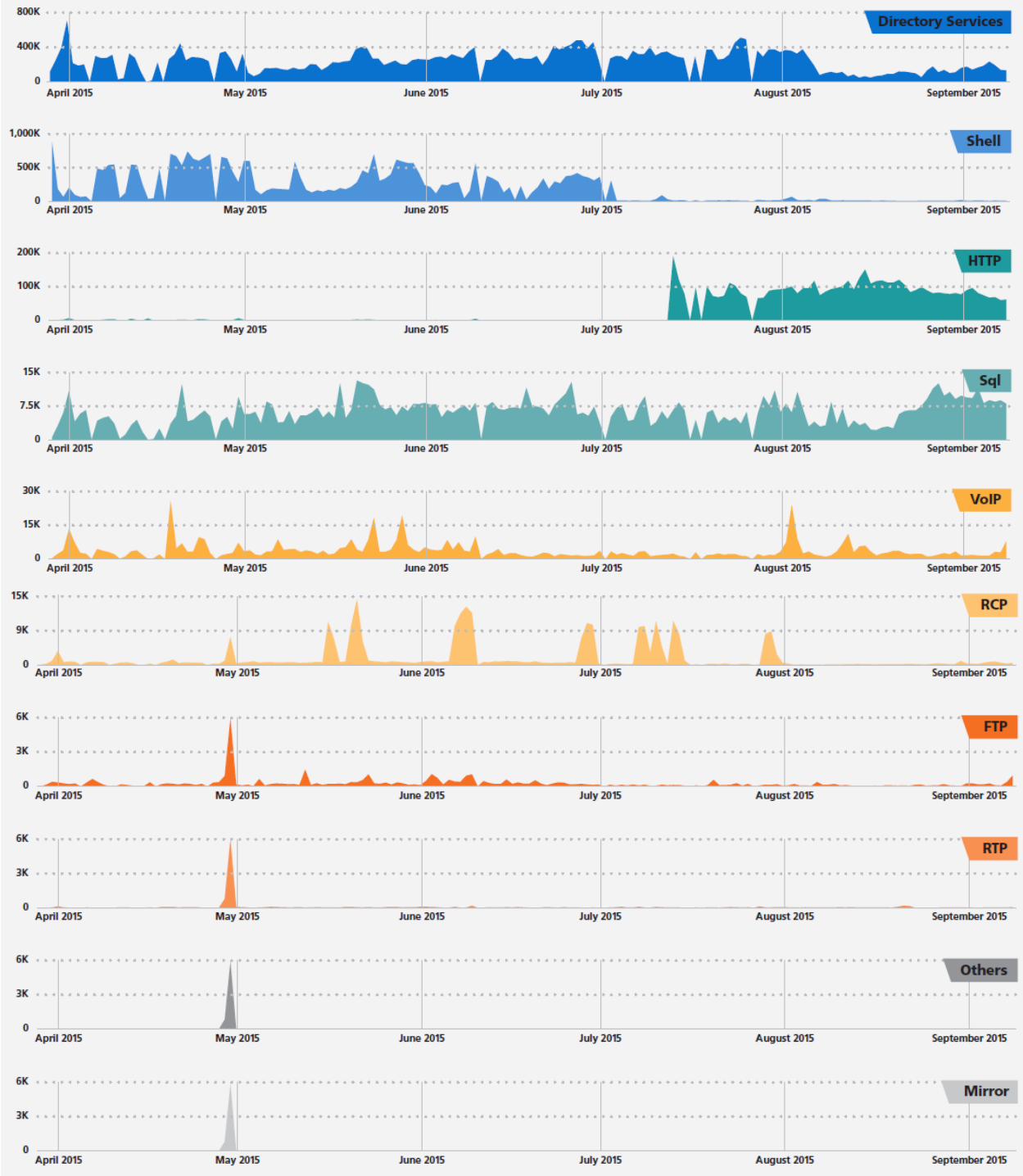


図 33: ハニーネット別のカテゴリ

2015 年 5 月 1 日は、年間で最も騒々しい 1 日であった。101 ヶ国への又はからの、21 カテゴリに亘る、3,100IP アドレスと 1,000 以上のサービスプロバイダー、企業その他エンティティーが関係する攻撃を記録した。SSH はその日のトップ攻撃手法で、主に中国からのものだった。

攻撃元となっている国

ランク	攻撃元	計
1	香港	21,954,881
2	中国	11,942,219
3	アメリカ	9,398,814
4	ロシア	9,153,213
5	ベネゼーラ	7,286,212
6	台湾	5,044,451
7	インド	4,004,119
8	マレーシア	3,219,336
9	ブルガリア	2,679,374
10	ルーマニア	2,399,730

ランク	攻撃元	計
11	ウクライナ	2,279,747
12	フランス	2,166,165
13	ブラジル	1,813,481
14	韓国	1,389,191
15	ドイツ	1,380,097
16	インドネシア	1,345,938
17	アイルランド	1,317,324
18	日本	1,186,717
19	ハンガリー	1,017,004
20	カナダ	916,258

図 24: ハニーネット攻撃元の国ランキング

このリスト上の多くの国について驚きはない。ファイアウォール、侵入防止システム(IPS)、その他境界上の装置は、中国とロシア両国からの定常的な攻撃に慣れている。攻撃者が使っている大半の企業のインフラは、インターネット、電話網、又は時代遅れの OS とサービスの上で動くホスティングプロバイダーである。このことは、大量のトラフィックが恐らく侵入を許したネットワークとプロバイダーから来ており、法的に問題なく調達されたホスティングサービス経由でないことを示している。大量の SSH 攻撃と HTTP 攻撃のトラフィックがこのことを反映しており、これらの攻撃ベクターが依然としてネットワーク侵入手段となっていることを表している。

この情報は、セキュリティサービスを管理、モニターしている期間に観察されたソース情報とは異なっている。まず最初に、ハニーポットネットワークの分布は NTT グループの顧客基盤とは異なっている。そのハニーポットネットワークは、分離された環境、すべての企業及び機関のネットワークから区分されている。第二に、ハニーネットトラフィックは主に偵察トラフィックである。

プロバイダー

最も標的にされたトップ 5 インターネットプロバイダーの攻撃トラフィックは、年間を通じて観察された全ての攻撃トラフィックの約 31%を占めた。

Rank	プロバイダ	初期攻撃ベクタ
1	ISP Rainbow Network	SSH Brute Force
2	ChinaNet Jiangsu Province Network	SSH Brute Force
3	Cantv Servicios Venezuela	Samba/Microsoft Directory Service
4	Data Communication Business Group	Samba
5	Shimizu Hang Road Causeway Bay Hong Kong International	SSH Brute Force

図 25: Top 5 最も騒々しい ISPs

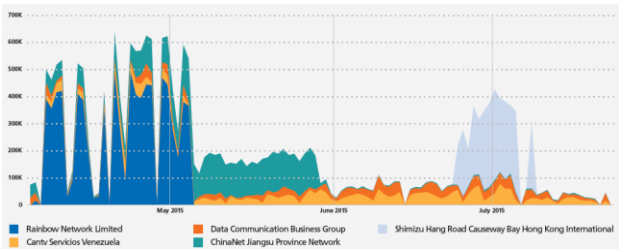


図 26: グローバルハニーネット分析トップ 5

ASNs (AS 番号)

ASNs は、一つ又はそれ以上の組織の管理下における外部 IP アドレスとネットワークのグループである。これらは、様々なネットワークルーティングプロトコルを用いて通信する外部 IP アロケーションとなる。発生源国調査とともに、 AS 番号分析は、防弾ホスティングサービスを提供しているか、又はネットワーク上に主要な問題を抱えているかもしれない複数国のオペレーションをピンポイントで見つけることができる。双方とも攻撃者に偵察フェーズにおける顕著な利点を提供することとなる。NTT グループのセキュリティ研究者は、ハニーポットセンサーを叩いた全ユニーク IP アドレスに関する約 11,000 個の異なる ASN を特定した。これはトータルで、66,000 個の異なる識別子と 370,000 個超のユニーク IP アドレスであった。下表は、大量の敵のトラフィックを平均化したトップ 10 の ASN である（例：254 利用可能 IP アドレスでの/24 識別子、これは 25IP アドレスと同等とみなす。）。

Rank	*ASN*	*割合*	*ISP*	*場所*
1	41578	60%	Level Next Ltd	ジブラルタル
2	57004	57%	VOLJAGLAS d.o.o.	クロアチア
3	62540	44%	Drake Holdings LLC	アメリカ
4	57063	41%	Klass Ltd.	ロシア
5	58182	41%	Kadroviy reserv ltd.	ロシア
6	58244	38%	ProektProfDevelopment ltd.	ロシア
7	58061	35%	Trade House _BelRosResursu_ LTD	ロシア
8	58137	33%	GazInvestProekt ltd.	ロシア
9	3189	32%	Atlant-Stroy ltd.	ロシア
10	58062	27%	Transport company UGRA LTD.	ロシア

図 27: 観測された ASNs トップ10.

識別子

NTT グループは識別子が攻撃活動に含まれていたと特定することを目指して、 研究者達は 66,000 個超のユニークな識別子とそれらの関係するプロバイダー、AS 番号と AS 番号オーナーを特定した。前述した思考過程に従うと、約 8,900 個の識別子が存在し、そこに研究者達は利用可能な IP アドレス空間の 10%又はそれ以上を平均化した約 220 個の識別子を観察した。一方、トップ 7 の識別子は、以下に示すように、それらの利用可能な IP アドレス空間の 2/3 又はそれ以上を占めた。

識別子	割合	ISP	ASN	国
1.1.1.0/24	100%	Research Prefix for APNIC Labs	15169	オーストラリア
104.128.66.0/24	84%	Vegasnap LLC	53340	アメリカ
104.128.67.0/24	80%	Vegasnap LLC	53340	アメリカ
192.92.196.0/24	80%	Drake Holdings LLC	62540	アメリカ
104.128.65.0/24	78%	Vegasnap LLC	53340	アメリカ
112.215.123.0/24	74%	PT Excelcomindo Pratama	24203	インドネシア
202.58.99.0/24	66%	Kingcorp KH	131178	カンボジア

図 28: 観測された識別子トップ 7

IP アドレス

372,000 個超の IP アドレスのうちのトップ 5 の IP アドレス(0 .00134%) が、ハニーネットが観察した全事案の 6%超を発生させていた。一般的に、トップの実行者は同時実行可能な活動に関わらない。代わりに、研究者達は、トップの実行者が年間を通じて特定の期間に攻撃するのを観察した。

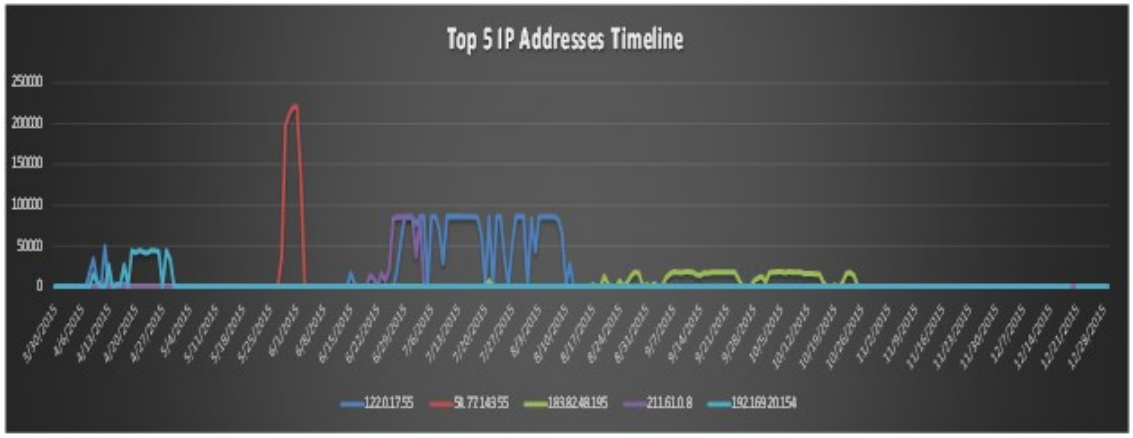


図 29: ハニーネットが観察した IP アドレストップ 5 Top

下表は、トップ 5 の敵の IP アドレスを、全観察事案のうちの%表示で表示している。

Rank	IP Address	観測回数の割合
1	122.0.17.55	3%
2	54.77.143.55	1%
3	183.82.48.195	< 1%
4	211.61.0.8	< 1%
5	192.169.20.154	< 1%

図 30: 敵の IP アドレストップ 5—ハニーネット

図 31:122.0.17.55 の詳細

地政学的考察

地政学的風潮を考慮しないで、ある偵察活動の背後にある攻撃者の動機を完全に理解することは不可能である。NTT グループの**セキュリティ**研究者は、地政学的思考を通してデータを分析し、政治的動揺のある地域においてサイバー活動との相関を確認又は否定するためにデータを精査した。

特に驚きはなかったが、攻撃者は中近東における他の国よりも多くイスラエルを標的としていた。その地域の外部の標的としては、主として米国に焦点が当たっており、中近東からのトップ攻撃者はイランだった。

更に、ウクライナ東部、攻撃を行ったトップ **4** ヶ国は最もウクライナの政治的発展に既得権益を有する国であった。順に、これらの国々を示すと以下の通り。

Rank	*攻撃元の国*	*攻撃回数*
1	United States	320,014
2	China	240,917
3	Ukraine	224,216
4	Russian Federation	109,197

図 **32:** ウクライナへの攻撃元の国

グローバルハニーネット：サマリー

差し迫った損害という観点からすると、偵察は CKC の中で最も無害なフェーズである。しかし、議論はあるだろうが、攻撃者にとってそれは最も重要なのである。攻撃者が組織のネットワーク内を検知されずに長い間動き回れれば回れるほど、彼のネットワークマッピングはより正確になり、そしてその後のフェーズでの作戦の成功確率はより大きくなるだろう。

新たな攻撃が日々出現している一方で、古い脆弱性のエクスプロイトによって攻撃者はあっさりと侵入に成功している。これは、時代遅れのソフトウェアをエクスプロイトする攻撃者が、このようなソフトウェアを改修又は交換しない組織に侵入し続けている現実のせいである。最低限言えることは、ネットワーク侵入とその後の攻撃を阻止するために必要な対策を講じるかは、それぞれの組織次第なのである。

アンチサンドボックス技術—なぜあなたのボックスが静かなのか？

サンドボックスは、マルウェアを検知してその行動を高度に可視化する基本的な分析システムとなった。サンドボックスはコントロール下にある環境で不審なコードを実行し、ネットワーク関連活動、ファイル交換やレジストリオペレーションのようなマルウェアの行動を観察する。マルウェア開発者は、暗号やポリモーフィズムを使用した署名ベースや静的分析ベースの検知手法を容易に回避できるけれども、サンドボックスは、既知の悪意ある活動の観察によってマルウェアを検知することができる。サイバーキルチェーンのケーススタディの章で議論されたように、これらの侵入技術は他の攻撃手法に共通する。

サンドボックスが広く分析に利用されていることを知っているので、攻撃者は検知を回避するためにアンチサンドボックス技術を開発している。これらの技術のいくつかは、サンドボックスに関連する特定の中間生成物を調査することによりサンドボックスの存在を検知する。そしてこれらの技術はマルウェアを終了させたり偽の挙動を見せることにより、マルウェア分析を妨害する。もう一つの一般的なアンチサンドボックス技術は、実行を引き止めたり、リブートのようなイベントを待つ行為を利用する。

セキュリティ実行者が既知のアンチサンドボックス技術に対して抵抗力のあるサンドボックスを作成しようとする一方で、攻撃者はサンドボックスの抵抗力を回避するためのより洗練された技術を開発する。

2015 年、NTT グループは、アンチサンドボックス技術に対抗することを狙ったサンドボックスを開発する一方で、マルウェア分析を大々的に行った。NTT グループは、毎日、数千のマルウェアサンプルを自動分析し、サンドボックス内で悪意ある活動を示さなかったサンプルを手動で分析した。この後の章では、研究者はサンドボックスの特徴、アンチサンドボックス技術の分類、そして分析したマルウェアバイナリデータにおける観察されたアンチサンドボックス技術の詳細について説明する。

サンドボックスの特徴

マルウェアは、一般的に、検知を回避するためにサンドボックスの特徴の幾つかを悪用する。

- **制限された分析時間** – サンドボックスは基本的に多くのマルウェアを分析する必要があるので、それらはしばしば事前に決められた時間内でそれぞれの慎重な分析を終了する（例　サンドボックスは 1 分後に分析を終了する）。もしマルウェアがその時間枠内に検知可能な挙動を示さなかったら、サンドボックスはたとえマルウェアが依然活動していても分析を停止するだろう。
- **自動かつ高度な並列処理** –　効果的なマルウェア分析のために、サンドボックスは自動かつ高度な並列処理を行う必要がある。これを実施するために、サンドボックスは通常バーチャルマシン技術を使用する。これらは、サンドボックスが容易に分析環境をコピーし、併用できるようにするとともに、分析後に（その後の分析との干渉防止を含む）その環境を元に戻すことができるようにする。
- **モニタリングファシリティ** – サンドボックスは二つの分析機能を有する。
    - マルウェアの行動をモニターする
    - アンチサンドボックス技術を無効化する

  マルウェアは、悪意ある活動を行い、サンドボックスに関連する特定の中間生成物を調査するために、Windows API と Windows のネイティブシステムコールを利用する。マルウェアの挙動をモニターするために、サンドボックスはこれらのコールを捕捉してマルウェアの引数を記録し値を返す。加えて、いくつかのサンドボックスはアンチサンドボックス技術をくぐり抜けるために戻り値を変更する。

アンチサンドボックスの技術の分類

マルウェア開発者は日頃から様々なアンチサンドボックス技術を使用する。図 43 は、前述のサンドボックスの特徴を利用した技術の例を含んでいる。

サンドボックスの特徴	アンチサンドボックス技術
(A) 制限された分析時間	**タイムボム: 指定日時に悪意ある活動を動作させること**(例 1) **実行の一時停止:分析が終了するまで、悪意ある活動の実行を遅らせること**
(B) 自動かつ高度な並列処理	**ユーザーインターフェースチェッキング: マウス操作のようなユーザーとのやりとりがないことを検知すること** **エミュレータ検知: エミュレートされたハードウェアとリアルなハードウェアとの違いを調査することによりバーチャルマシンを検知すること** **サービスネーム/レジストリー/ファイルチェッキング: 特定の文字列を元にバーチャルマシンを検知すること**(例 VMware、vBox) **ハードウェアスペシフィケーションチェッキング: 一般的なハードウェアのスペックの違いを検知する**こと(例 CPU はシングルコアのみを有する。) **エンバイアラメントフィンガープリントチェッキング: グローバリーユニークアイデンティフィアー** (GUID)を元に、サンドボックスと感染したホストを区別すること (例 2)
(C) モニタリングファシリティ	**フッキング検知: モニターしているマルウェアに対し注入されたコードを検知すること**(例 API フックに対するコード) **ランタイムオーバーヘッド検知: フッキングやログの記録によって起こるオーバーヘッドを検知すること** **アンチアンチサンドボックス検知: アンチサンドボックス技術を回避する修正を検知すること**(ケーススタディ 3)

図 43 : アンチサンドボックス技術

アンチサンドボックス例

研究者と分析者は、タイムボム、Volume GUID checking と Sleep duration shortening detection を含むいくつかのアンチサンドボックス技術に直面する。

例 1 ：タイムボム

ロジックボムの一種であるタイムボムは、指定された日時のみに悪意ある活動を引き起こす。条件を満足させるのが難しいので、サンドボックスはしばしば悪意ある活動の観察に失敗する。NTT グループは、日本の公的・私的機関を標的とした攻撃作戦で利用された Emdivi マルウェアが、この技術を使ってマルウェアをビジネスアワーのみに動作させていたのを確認した。

図 44 は、Emdivi において実行されたタイムボムコードを含んでいる。このプログラムは現在の日時をチェックし、現在時刻が平日の午前 9 時から午後 6 時でない限り実行しない。これは、分析が通常のビジネスアワー外でスタートしている間は、サンドボックスが決して悪意ある活動を観察しないことを意味している。

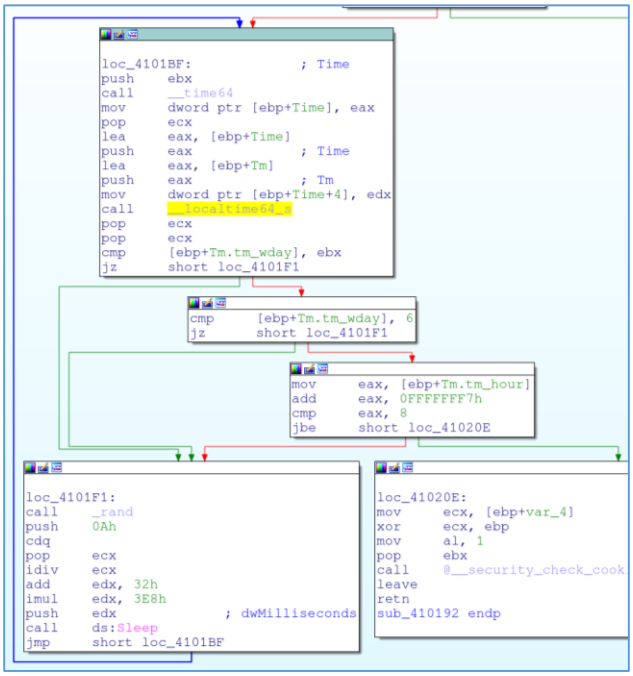


図 33:Emdivi において実行されたタイムボムコード i

Emdivi は複数のバージョンを有しており、最も有名なのは t17 と t20 である。両バージョンに関し、研究者は、複数のサンプルがこの機能を示したことを確認した。

例 2 ：GUID ボリュームチェック

また研究者は、感染したホスト上のマルウェアを分析するためにサンドボックスを利用できる。その場合、サンドボックス内のマルウェアは感染したホストとは別の環境で実行されてもよい。いくつかのマルウェアは感染フェーズの間感染したホストの指紋を採るので、それは分析環境をホストの環境と区別できる。

ホストの指紋を採る技術の一つは Volume GUID checking である。マルウェアがホストを感染させて GUID をバイナリイメージの一部として自分自身に埋め込む際、マルウェアは Volume GUID をホストのユニークな指紋として読み取る。続いて、マルウェアが実行された時、マルウェアは現在の環境の Volume GUID と埋め込まれたものを比較する。もし GUID が異なっていれば、マルウェアは実行を中止する。Zeus マルウェアはこの技術とその変種を過去に使っていた。

NTT グループは、2012 年から 2015 年にかけて NTT グループウェブクライアントハニーポットを用いて集められた 5,000 個以上のマルウェアサンプルを研究し、これが一般的な技術であることを確認した。2015 年、研究者はこの技術を使った 11 個のユニークなマルウェアを特定した。

例 3: Sleep Duration Shortening Detection

いくつかのサンドボックスは sleep duration を変更して Sleep API calls をスキップしようとする。この対策は効果的でないことが証明されている。なぜなら、マルウェアはしばしばそれを検知するアンチサンドボックス技術を使うからである。

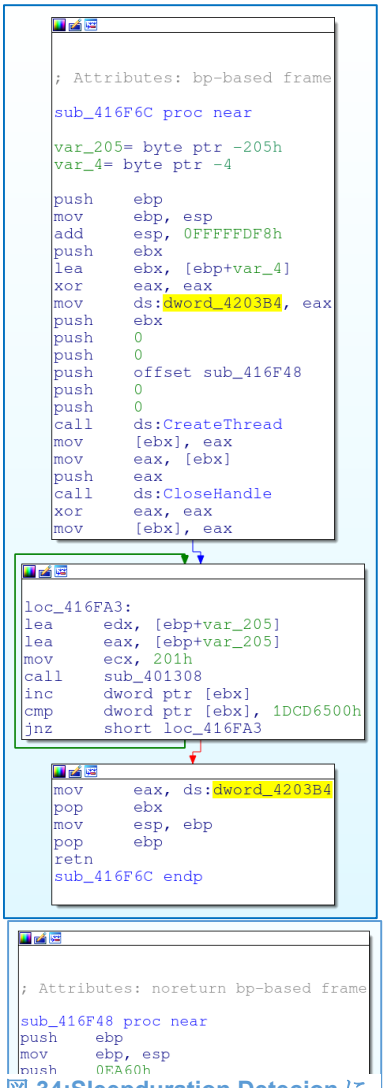


図 34:Sleepduration Detecion におけるアンチサンドボックス

マルウェアは停止時間をチェックすることにより、この対策の使用を検知できる。このチェックを行うために、マルウェアは Sleep API を呼び出す前後に x86 Read Time Stamp Counter Instruction (RDTSC)又は Windows API (例 GetTickCount)を使う。もし停止時間が要求されたものより短い場合、マルウェアはサンドボックスの存在を検知する。研究者は一般的なランサムウェアである TeslaCrypt がこの技術を使用しているのを確認した。

しかしながら、サンドボックスはシステムの時間を増加させて容易にこの技術を打ち負かす。NTT グループの研究者達は、Shiotob スパイウェアが回避するのを困難にする、より洗練された技術を使用しているのを確認した。図 45 は、Shiotob のアセンブリコードを示している。Shiotob は、Windows API や RDTSC の指示の代わりに、wasted loop execution を利用する。メインスレッドは新しいスレッドを作成し、wasted loop を実行する。作成されたスレッドは、Sleep API を用いて実行を停止し、Sleep API を呼んだ後にグローバル変数を変更する。メインスレッドは、ループが終了した時、グローバル変数をチェックする。もしこの変数が変更されていた場合、Shiotob は sleep duration shortening を検知する。

推奨事項

サンドボックス開発者

サンドボックスは、マルウェアを特定し分析するのを助ける効果的なツールである。しかし、マルウェア開発者はサンドボックスをよく知っていて、アンチサンドボックス技術を実行する。結果として、サンドボックス開発者は攻撃者の打倒と検知の改善に向けて彼ら自身の技術を高度なものにしなければならない。

- 最初に、研究者が、攻撃者が使用するアンチサンドボックス技術を理解することは重要である。研究者と分析者が単一のサンドボックス技術の結果を信頼するのは危険であり、異なるサンドボックスからの結果を比較するのは非常に有益である。既知の技術に基づいた結果を比較することにより、分析者と研究者は攻撃者が使っている侵入技術を決定することができる。例えば、特定のサンドボックスでのみ振る舞いを変えることは、見つけることができる回避戦略である。
- サンドボックスは設定をカスタマイズするオプションも提供するべきである。これらの設定は、分析期間に加えてユーザー環境も含むべきである。NTT グループの研究者は、異なるタイムゾーンを設定した複数のサンドボックスを使って Emdivi タイムボムの効果を軽減することができた。
  もう一つの例として、研究者が感染したホストの volume GUID を知った時、NTT グループのサンドボックスは、感染したホストの volume GUID を返す API の戻り値を変更することにより volume GUID checking を成功裏に回避した。
- sleep duration shortening detection を使用する時、sleep duration より分析期間を長くすることにより、 自動的にマルウェアの挙動を分析することが可能である。異なる sleep duration でテストできたり、sleep duration をカスタマイズ可能な研究者はしばしばこの侵入技術を用いるマルウェアの捕捉に成功できる。

サンドボックスユーザーに対するヒント

- サンドボックス開発者はアンチサンドボックス技術を回避するために継続的に彼らのサンドボックスを改良しているので、ユーザーはサンドボックスの効果を最大とするために定期的にアップデートの確認と適用を行うべきである。
- サンドボックス開発者がサンドボックスを定期的に改良するために、組織は分析結果を開発者と共有することを真剣に考えるべきである。
- サンドボックスはそれぞれ特殊な特性を有しているので、複数の（異なる侵入対策技術を利用する）サンドボックスを利用することは侵入リスクの軽減を助けることができる。

NTT グループのリソース情報

Solutionary について

Solutionary は次世代のマネージドセキュリティサービスプロバイダー（ＭＳＳＰ）です。主にマネージドセキュリティサービス、プロフェッショナルセキュリティサービス、および、グローバルスレットインテリジェンスを提供しています。

Solutionary の総合的なセキュリティ監視およびセキュリティ端末管理サービスは、従来のＩＴインフラおよび仮想のＩＴインフラ、クラウド環境およびモバイルデータを守ります。

Solutionary の顧客は、既存のセキュリティ対策を最適化し、確かな情報に基づくセキュリティ上の決定を行い、法令順守を達成し、コストを下げることができます。特許権を有するクラウドベースの ActiveGuard® サービスプラットフォームは、高度な脅威から保護するために、多重の検知技術と高度な分析を用いています。Solutionary セキュリティエンジニアリングリサーチチーム（ＳＥＲＴ）はグローバルな脅威の情勢を調査し、実用的なスレットインテリジェンスを提供、脅威の検知と軽減のための制御を強化します。経験のある Solutionary の有資格セキュリティエキスパートは、顧客の内部チームの延長として振舞い、業界トップのサービスを、金融ヘルスケア小売政府機関などの様々な分野のグローバル企業および中堅企業に提供します。サービスは、複数の最新のセキュリティオペレーションセンター（ＳＯＣｓ）を通じて、毎日２４時間体制で提供されます。

詳しくは www.solutionary.com をご覧ください。

Dimension Data について

Dimension Data は、２６，０００人以上の従業員を有し、５８か国で事業を行う、７５億ドルのＩＣＴソリューションおよびサービス事業者です。セキュリティ事業においては、ネットワーキング、コミュニケーション、データセンター、およびエンドユーザーコンピューティングなどの、ＩＴ統制の様々な分野を横断する幅広い技術とインテグレーションの専門知識を提供します。当社は、金融、通信、ヘルスケア、製造、政府機関、教育などのすべての業界にわたる６，０００以上の顧客にサービスを提供しております。コンサルティング、システムインテグレーション、総合的なマネージドセキュリティサービスのスイートおよびスレットインテリジェンスを含む、当社の広いセキュリティの能力をもって、データセキュリティの全てのライフサイクルのプランニングで組織を支援します。

詳しくは www.dimensiondata.com をご覧ください。

NTT Com Security について

NTT Com Security は、ＮＴＴグループのセキュリティ子会社（ＮＹＳＥ：ＮＴＴ）であり、情報セキュリティとリスクマネジメントの事業を行っています。当社の WideAngle コンサルティング、マネージドセキュリティアンドテクノロジーサービスをお選びいただくことで、当社がリスク管理に集中している間に、お客様はビジネスチャンスに集中できます。当社のガバナンス、リスク、コンプライアンス（ GRC ）の契約事例および革新的なマネージドセキュリティサービスと実用的な技術の実装の幅は、我々がお客様とユニークな視点を共有できることを意味しており、プロジェクトの優先順位付けと標準化の推進でお客様を支援します。当社は常に適切かつ客観的なアドバイスを心がけております。情報セキュリティおよびリスクマネジメントが高成長ビジネスにおける差別化要因と認識した上で、当社のグローバルアプローチはコストと複雑さの低減を意図して設計されています。革新的かつ独立した、NTT Com Security は南北アメリカ、ヨーロッパ、アジアパシフィックにオフィスを持ち、世界最大の通信会社の一つであるＮＴＴによって所有され、そのグループの一部となっています。

NTT Com Security の情報セキュリティとリスクマネジメントのための WideAngle サービスについての詳細は、www.nttcomsecurity.com をご覧ください。

NTT Innovation Institute について

NTT Innovation Institute, Inc.（NTT i3）は、シリコンバレーを本拠地とする、ＮＴＴグループのリサーチアンドデベロップメントセンターです。当研究所は、市場主導型、顧客重視のソリューションやサービスを開発するために、NTT 事業会社および世界中の顧客と密接に連携しています。NTT i3 はＮＴＴグループの膨大な知的資本を基盤として、さらに年間２５０億ドル以上を開発に投資しています。NTT i3 とその世界に誇る科学者および技術者は、戦略、ビジネスアプリケーション、データおよびインフラにまたがる市場を主導するソリューションを提供するため、卓越した技術を持つ会社やスタートアップと提携しています。

詳しくは www.ntti3.com をご覧ください。

NTT Secure Platform Laboratories について

ＮＴＴグループの一部として、NTT Secure Platform Laboratories は進化し続けるセキュリティ脅威に対抗するセキュリティと情報収集の技術を向上させることを任務としています。研究所は、暗号化、マルウェア分析、セキュリティログ分析、および IoT デバイス/システムセキュリティなどの最先端技術の研究開発を行っています。

詳しくは www.ntt.co.jp/RD/e/ をご覧ください。

NTT-CERT について

NTT-CERT は、NTT Secure Platform Laboratories の一部門です。NTT-CERT は、コンピュータセキュリティインシデント対応チーム（CSIRT）のスペシャリストのための信頼できる窓口として機能し、ＮＴＴグループ内にあらゆる種類の CSIRT のサービスを提供しています。NTT-CERT は、サイバーセキュリティの脅威に関する独自の情報を生成し、セキュリティサービスとセキュアなネットワークサービスの分野において、ＮＴＴグループ会社の能力強化を支援しています。

詳しくは www.ntt-cert.org をご覧ください。

ＮＴＴのグローバルデータ分析手法 について

ＮＴＴグループ２０１６年グローバルスレットインテリジェンス報告書（ＧＴＩＲ）には、グループのセキュリティ会社が２０１５年１月１日から２０１５年１２月３１日までの間に収集したグローバル攻撃データが含まれています。分析は、クライアントからのログ、イベント、攻撃、インシデントおよび脆弱性データに基づいています。また、１００か国以上のグローバルハニーポットおよびサンドボックスを含む、ＮＴＴグループの調査情報源からの詳細情報が含まれています。２０１６ＧＴＩＲは３.５兆個のログと６２億個の攻撃データをサマライズしています。ＮＴＴグループは、セキュリティログ、アラート、イベントと攻撃情報を収集し、前後関係を明確にするためそれを加工し、そして、整理されたデータを分析します。このプロセスはリアルタイムのグローバルスレットインテリジェンスおよびアラートを可能にしています。約８,０００のセキュリティ顧客のサイズと多様性によって、ほとんどの組織が直面するようなセキュリティ上の脅威の情報がＮＴＴグループに提供されています。イベントの種類と量に基づき攻撃を識別する世界中のログイベントから、データが導き出されます。有効な攻撃イベントの活用は、未加工の大量のログデータやネットワーク通信とは対照的に、実際の攻撃数をより正確に表します。攻撃イベントの適切な分類をしなければ、セキュリティオペレーションセンター（ＳＯＣｓ）によって観察される過度に大量のネットワーク偵察通信、誤検出、許可されたセキュリティスキャンおよびＤＤｏＳ攻撃の大洪水によって、攻撃による本当のインシデントが覆い隠されてしまいます。ＮＴＴグループ

のセキュリティ会社の２４のセキュリティオペレーションセンターと７つの研究開発センターからのデータを組み入れることで、グローバルな脅威の情勢を非常に正確に表しています。

Wapack Labs について

Wapack Labs はセキュリ上の脅威を、攻撃になる前に特定します。２０１３年に設立された Wapack Labs は、非上場で運営されるサイバーインテリジェンスと脅威分析の会社です。インターネットの監視業務、データ収集、経済、金融および地政学的課題の綿密な分析を通じて検知した脅威についての早期警告を提供することで、世界中の会社と組織にサービスを提供しています。インテリジェンス情報は、顧客のサイバーセキュリティの必要性と損益に見合う一連のパッケージで顧客にシェアされます。

詳しくは www.wapacklabs.com をご覧ください。

Recorded Future について

当社は顧客をリアルタイムのスレットインテリジェンスで武装します。これにより顧客は組織を狙ったサイバー攻撃に対し事前対策を講じることができます。何億もの事実をインデックス化し、特許権を有する当社のウェブインテリジェンスエンジンは継続してウェブを分析し、新たな脅威に関する比類ない洞察を顧客に与えます。当社は、世界トップ５の企業のうち４つを守ることに役立っています。

詳しくは www.recordedfuture.com をご覧ください。

Lockheed Martin について

Lockheed Martin（ＬＭ）は、フォーチュン１０００社およびグローバル１０００社のために、開発、実装、保守、および重要インフラの保護に焦点を当てたサイバーセキュリティソリューションの世界的プロバイダーです。ＬＭのエンジニアは文字通り世界に広がり、５０の州と７５の国の６００拠点において、４,０００のプログラムを監督しています。当社は３,０００人以上のサイバーセキュリティのプロフェッショナルを雇用し、ＩＴとＯＴ技術の強固なパートナーシップを有しています。ライフサイクルに焦点を当てた当社の製品やプログラムは、当社の商業顧客のインフラ全体の成功と持続可能な保護ネットワークの両方を可能にします。当社のアプローチは、攻撃をしようとしている者の情報を活用し、それを彼らに対して使うことにフォーカスする Intelligence Driven Defense® の考え方に基づいています。

詳しくは www.lockheedmartin.com をご覧ください。

The Center for Internet Security について

The Center for Internet Security（ＣＩＳ）は米国の内国歳入法典第 501 条Ｃ項３号の規定に基づく非営利公益法人であり、公共および民間組織のサイバーセキュリティの備えと対策の強化を推進しています。業界と政府の強力なパートナーシップを活用し、ＣＩＳは地球規模でのサイバーセキュリティの課題の進化と戦い、サイバー攻撃に対する迅速かつ効果的な防御を達成するためのキーとなるベストプラクティスを、組織が適用することを支援します。ＣＩＳは、マルチステート情報共有分析センター（ＭＳ－ＩＳＡＣ）、ＣＩＳセキュリティベンチマーク、およびＣＩＳクリティカルセキュリティコントロールを運営しています。

詳しくは CISecurity.org をご覧いただくか、または、ツイッターで @CISecurity をフォローしてください。

用語解説

ゼロデイ攻撃：今まで知られていなかったソフトウェアの脆弱性をついた攻撃をいう。脆弱性が発見されて修正プログラムが提供されるまでの間にその脆弱性を攻略する攻撃(Wiki)。

ＡＰＩ（アプリケーションプログラミングインタフェース）：ソフトウェアのモジュールが、他のモジュールまたは下層のオペレーティングシステムと、情報のやり取りを行うための文書化された手法。

ＡＰＴ（持続的標的型攻撃）：政府や犯罪組織からの十分な資金があり、高度な技術と長期的な目標を持つ攻撃者。ＡＰＴは、最大利益のために、通常、複数の技術を用いる非常に複雑な攻撃になる。

ＡＳＮ（ＡＳ番号）：大きなＩＳＰのような管理主体によって管理されるＩＰ経路制御の集合に与えられる一意の番号 インターネットに参加しているインターネットサービスプロバイダー（ISP）や組織が必ず保有している固有の番号(IIJ)。

バックドア：不正アクセスを成し得る手段の一つ。通常、バックドアを仕込んだ悪意ある者だけが知るパスワードを用いて行われる。

ブラックリスト：マルウェアに侵されたと考えられるＩＰアドレスまたはドメイン名のリスト。セキュリティ戦略上、ブラックリスト上のアドレスへのアクセスは拒否するか、あるいは、ホワイトリスト上のアドレスだけにアクセスを許可したほうがよい。

ボットネット：攻撃者がコントロールでき、指示を受けることと命令の実行を同時に行う能力を持つ複数のシステム。ボットネットはＤＤｏＳ攻撃やその他のサイバー犯罪でしばしば観察される。

セキュリティ侵害：不正侵入されたネットワークまたはシステムから、組織のデータが盗み出されたり公開されてしまうこと。

ＢＹＯＤ：従業員の個人所有のモバイル端末を会社の業務環境で使用させること。

遠隔操作（Ｃ２）：サイバーキルチェーンのフェーズの一つ。ボットネット内のボットに対し指示を与えたり管理的な作業を行う。

ＣＩＡ（機密性、完全性、可用性）：情報セキュリティの三要素。攻撃者は通常これらの一つ以上を侵害する。

ＣＳＣ（Critical Security Controls）：クリティカルセキュリティコントロール。米国ＣＩＳ（Center For Internet Security）が発行する、サイバー攻撃に対する推奨防御対策。

ＣＶＥ（共通の脆弱性と危険性露出）：公知の脆弱性のカタログ 共通脆弱性識別子(IPA)。

ＣＶＳＳ（共通脆弱性評価システム）：脆弱性の深刻度のスコアリング手法。スコアの範囲は０（最小）から１０（最も深刻）まで。

サイバーキルチェーン：サイバー侵入に対抗するための分析と防御のためのフレームワーク。ロッキードマーティン社が２０１１年の論文で最初に論じた。

サイバー攻撃：コンピュータネットワークシステムを損傷、妨害または破壊する、ハッカーによる企て。

サイバー犯罪：コンピュータまたはネットワークが絡んだ法律違反。

サイバー犯罪者：サイバー犯罪を犯す一人の人間、または、グループ。コンピュータを道具または標的もしくはその両方として使用する。

サイバー攻撃の脅威：コンピュータネットワークやシステムを妨害する悪意ある企ての可能性。

ダークウェブ：不正または非合法な目的で使用される、一般の検索サイトからはアクセスできないネットワーク。

配送：サイバーキルチェーンのフェーズの一つ。マルウェアを攻撃対象の環境へ送信すること。

ＤｏＳ（サービス妨害攻撃）およびＤＤｏＳ（分散型サービス妨害攻撃）：コンピュータに対する攻撃の一種。コンピュータやネットワークのリソースを大量に消費して、本来のユーザが使えなくする。

ドライブバイダウンロード：ウェブサイトを閲覧したり、メールや添付ファイルを開いた際に、ユーザが気がつかないうちにマルウェアをダウンロードさせること。

不正転送：組織からデータを無許可で抜き取ること。

エクスプロイトキット：悪意あるプログラムを複数まとめてキット化したもので、ソフトウェアの脆弱性を攻撃するサイバー犯罪で用いられる。

エクスプロイト：サイバーキルチェーンのフェーズの一つ。マルウェアを攻撃対象の環境で実行することをいう。

ファイアウォール：ネットワーク通信の入出のコントロールを行うソフトウェアまたはハードウェア。データパケットを解析し、あらかじめ定義されたルールセットに基づいて、その通信を許可すべきかどうかを決定する。

フォレンジック（またはフォレンジック分析）：マルウェア（またはマルウェアに汚染されたシステム）に関する詳細な分析。マルウェアのデザイン、発信元、動作、その他の特徴を特定する。

ＧＵＩＤ（グローバルー意識別子）：ソフトウェアコンポーネントやハードウェアデバイスを一意に特定するための非常に長い数列。完全に同一に設定された 2 台のコンピュータもそれぞれ異なる GUID を持つ。

ハクティビスト：社会的あるいは政治的主張を広めるための行動（ハクティビスム）を行うハッカーをいう。

ハニーネット：ハニーポットが設置されたネットワーク。

ハニーポット：攻撃または攻撃者の情報を集めることや、攻撃者の目を会社のシステムからそらすことを目的とした、囮システム。

ＩＤＳ（侵入検知システム）：通常、ネットワークに設置される。害を及ぼそうとするネットワーク上の異常を検知するために、シグネチャーや経験を利用する。

インシデントレスポンスプログラム：サイバー攻撃への対処およびサイバー攻撃による影響を管理するための、組織の計画。

インジェクション：コンピュータに対する攻撃の一種。命令やデータに悪意あるコードを挿入し、受け取ったシステムに有効な命令と認識させるもの。インジェクション攻撃は PHP や SQL といったプログラミング言語でよく使われる。

インストール：サイバーキルチェーンのフェーズの一つ。攻撃者が継続してアクセスできるようにするために、攻撃対象の環境にマルウェアを常駐させることをいう。

ＩＰレピュテーション：ＩＰアドレスがマルウェアを宿しているかどうかを評価したデータベース。

ＩＰＳ（侵入防止システム）：通常、ネットワークに設置され、ＩＤＳに似た機能を持つ。違いは、もしも通信が悪意ある通信の特徴を持っていた場合その通信をブロックできること。

ＩＲＣ：インターネットリレーチャット。

ＩＳＰ：インターネットサービスプロバイダー。

マルウェア：ウィルス、ワーム、トロイの木馬、スパイウェアを含む、悪意あるソフトウェアの総称。

マルバタイジング（悪意ある広告）：ウェブページ上の無害な広告のように見せかけて、ユーザーがクリックした時に活動するマルウェア。

ＮＴＰ（ネットワークタイムプロトコル）：ネットワークに接続された機器が内蔵する時計を、正しい時刻に同期させるために用いるプロトコル。

難読化：ソースコードやドメイン名の意味や動作をわかりにくくするために、暗号化またはテキスト置き換えすること。

OWASP：オープンウェブアプリケーションセキュリティプロジェクト。

ペーストサイト：匿名のユーザーが情報を載せることができる公開ウェブサイト。違法に集められた情報も含まれる。これらのサイトを検索することは、ある組織の情報が漏洩しているかどうか知るための一つの方法。

パッチマネジメント：ベンダーが提供するソフトウェアパッチを確実に適用するための体系的なプロセス。

侵入テスト（またはペンテスト）：脆弱性チェックのためにネットワークに対し意図的に仕掛けられる、許可され管理された攻撃。

境界：組織をインターネットに接続するインターフェースシステム。

持続能力：攻撃者が攻撃対象の環境内で活動を継続するための能力。

フィッシング：ユーザーネーム、パスワード、クレジットカード情報（間接的には金銭）などの情報を得るために、電子メールやＥＣサイトなどで、信頼できる実体を装った詐欺。

PHP：ウェブアプリケーションの開発でよく使われるプログラミング言語。

プロキシサーバ：他のサーバとインターネットの（通常は）間を仲介するサーバをいう。代理サーバには、フィルタリングと追加的な防御措置、あるいは、ホワイトリストやブラックリストに照らしてリクエストを評価するセキュリティ機能を実装することができる。

ランサムウェア：被害者のデータを暗号化するマルウェア。復号鍵と交換に身代金の支払いを要求する。

偵察：サイバーキルチェーンのフェーズの一つ。攻撃対象とその脆弱性を特定するために攻撃者が調査することをいう。

リモートアクセス型トロイの木馬（ＲＡＴ）：悪意あるユーザーが遠隔アクセスをできるようにするために設計されたトロイの木馬の一種**。**

サンドボックス：高度に保護された領域で疑わしいコードを実行させてその動作を検証するソフトウェア。

サニタイジング：値の正確性の確認及びマルウェア攻撃の可能性排除のために、ウェブフォームの入力値を検証すること。

ソーシャルエンジニアリング：面会や電話、SNS のような手段を通じ人間の心理的な隙や行動のミスにつけ込み、重要情報を不正入手することをいう。

スリープ：呼び出したプログラムそれ自体を一定時間停止または遅延させるＡＰＩ。

スピアフィッシング：高度に標的を絞ったフィッシング攻撃のこと。特定の人物や組織に関する情報を用いる。

標的型攻撃：特定のユーザー、会社、組織を狙った攻撃。

スレットインテリジェンス：すぐに実行可能な推奨対策を導くための、サイバー攻撃の脅威に関する情報の集約と専門的な分析。

トーア（Tor）：もともとは The Onion Router の頭文字。匿名でウェブサイトにアクセスするためのネットワークソフトウェアをいう。

トロイの木馬：正規のファイルや役に立つプログラムを装ったマルウェアの一種。

脆弱性ライフサイクル管理：脆弱性の発見、文書化、追跡および修復の体系的なプロセス。

WAF：ウェブアプリケーションファイヤウォール。

武器化：サイバーキルチェーンのフェーズの一つ。セキュリティ上の弱点を仕込んだ配送可能なファイルを作成することをいう。通常、PDF のような無害なファイルタイプで作成される。

ウェブアプリケーション攻撃：ウェブサイト（通常、一般に公開されているもの）の脆弱性を狙った攻撃。

ホワイトリスト：マルウェアに侵されていないと考えられるＩＰアドレスまたはドメイン名のリスト（ブラックリストの項も参照のこと。）。許可されたアプリケーションプログラムやその他のものにも適用できる。