FORTINET

フォーティネット脅威レポート

2019 年第 2 四半期版

目次

2019 年第 2 四半期の概説

刻々と変化するサイバー脅威の現状をまとめた四半期毎のレポートをお届けする時期を再び迎えました。第 2 四半期は、これまでと同様のテーマやトレンドが数多く確認されましたが、情報収集に関する、注目すべき新たな展開もありました。本レポートでご紹介する、この四半期の主な内容は以下のとおりです。

The Fortinet Threat Landscape Index

インターネットにおける脅威の活動を示すこの指標が第 2 四半期に過去最高の値を記録し、昨年の同時期から 4% 近く上昇しました。

ロビンフッドとその（不）愉快な仲間たち

Robinhood（ロビンフッド）と呼ばれるランサムウェアが第 2 四半期に復活を遂げ、ボルチモア市をはじめとする複数の地方自治体を攻撃しました。ロビンフッドの伝説とは異なり、貧しい人々に富が分配されることはありませんでした。

RDP と「BlueKeep」の憂鬱

悪名高い BlueKeep をはじめとする RDP の脆弱性が次々と報告されたことで、リモートアクセスサービスが犯罪の侵入口となっていることを再認識することになりました。

巧妙化する分析回避機能

新たな分析 / 検知回避機能が追加された、あるスパム攻撃を検証し、このトレンドに今後も注目する必要がある理由を解説します。

デジタルサプライチェーンの悪用

サードパーティ製品のリスクは新たな問題ではないものの、最近のいくつかのインシデントによって、サードパーティの利用拡大で外部に公開されるデータの範囲も大きく拡大することを再認識することになりました。

スマートホーム / ビジネスを探し回る活動

一般ユーザー向け IoT と ICS の中間に位置する、家庭用や小規模企業向けのスマートデバイスが増加し、それを標的とする攻撃も増加しています。

マルウェアの研究：Zegost

2011 年から確認されているこの情報窃盗マルウェアにいくつもの機能が追加され、アップグレードされました。本レポートの分析をお読みいただくことで、被害を避けられることを願っています。

探索的分析：脆弱性の調査

この四半期には 28 のゼロデイ脆弱性のエクスプロイトの活動が確認されましたが、新しいシグニチャの展開から実際のエクスプロイトまでに、どれ位の時間がかかるものなのでしょうか。

本レポートに記載する調査結果は、世界中の本番環境で観察された、数十億件の脅威イベントを収集しているさまざまなネットワークセンサーから取得された、FortiGuard Labs の脅威インテリジェンスに基づくものです。第三者機関の調査によれば [*1]、フォーティネットはセキュリティデバイス出荷数において業界最大を達成しています。本レポートでは、この独自の利点を活かした複数の観点からの概観を提示し、その分析によって明らかになった、いくつかの重要な事実をお知らせします。

*1　IDC Worldwide Security Appliances Tracker – 2019 年 3 月（年間出荷台数に基づく）（英語）：https://www.idc.com/tracker/showproductinfo.jsp?prod_id=38

Threat Landscape Index

2019 年第 2 四半期 期初：1013 | 期末：1037 | 最高値：1037 | 最低値：1004

Fortinet Threat Landscape Index（TLI）は、インターネットにおける悪意ある活動の現状を示す指標を提供する目的で開発されました。TLI は、より多くのセンサーが、より多くの種類の、あるいはより多くの数の脅威を検知するようになると、サイバー環境は悪化していると考えられるという前提に基づいています。その逆の場合、状況は好転していることになります。おそらく最も重要なのは、TLI をこのような変化の度合いを長期的に示すものとして捉え、その背後にある要因に注目するための手掛かりとして活用することでしょう。

本レポートで TLI をご紹介するようになってから丸 1 年が経過したことから、今回はこれまでの変遷を振り返ってみることにしました。全体として見ると、TLI は開始時の 1,000 から 4% 近く上昇しました。これまでの 1 年間の最高値は 1,037 で、偶然にもその時期は第 2 四半期の期末と重なりました。もちろん、まったく喜ばしいことではありません。

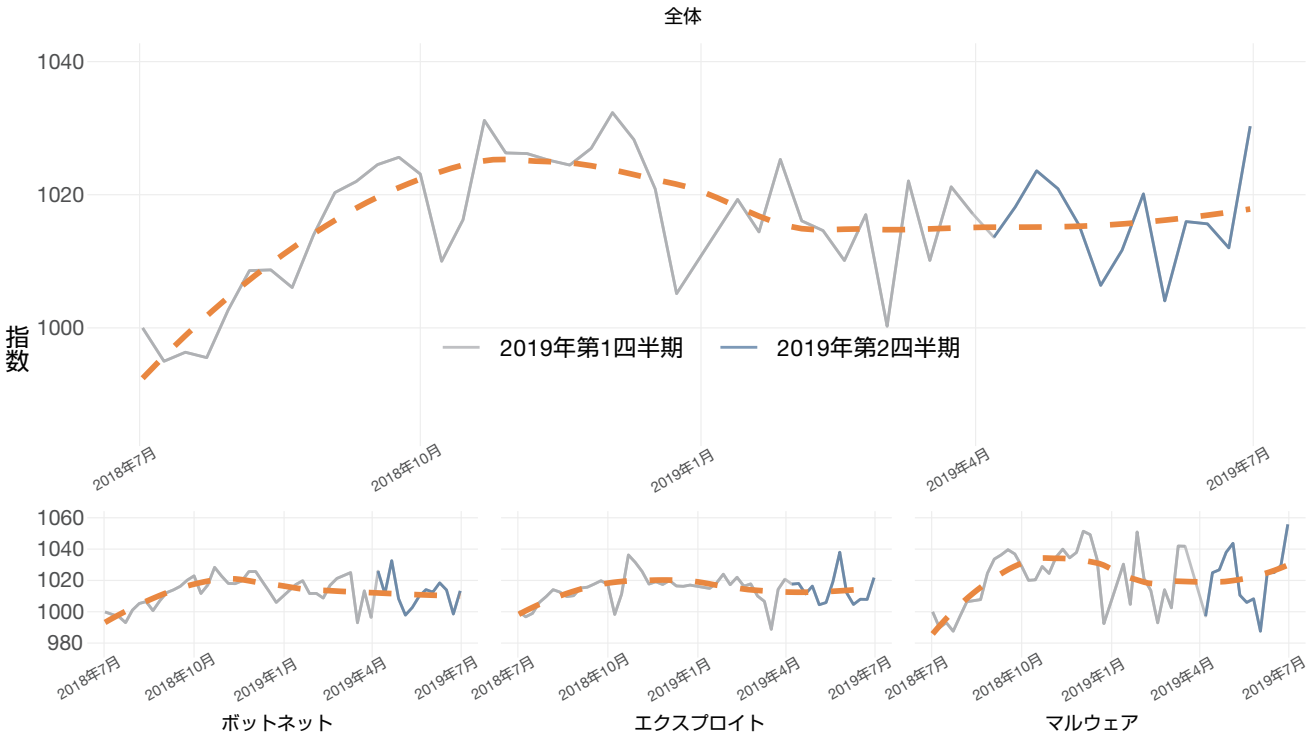

図 1：Fortinet Threat Landscape Index（上）とボットネット / エクスプロイト / マルウェアのサブ指標（下）

第 2 四半期末の急増の主な要因は、マルウェアとエクスプロイトの活動の増加によるものです。そこで、いくつかの具体的な検知から、その活動の背景を探ってみることにしましょう。

検知数の上位

図 2 に、フォーティネットのセンサーが第 2 四半期に検知した、マルウェアと IPS の 10 位までを示します。まずはじめに、この第 2 四半期末に TLI が最も上昇した、マルウェアから見てみることにしましょう。Microsoft Office 文書に影響するメモリ破損の脆弱性である CVE-2017-11882[*2] を悪用する不正なファイルが、2 位以下を大きく引き離して 1 位に入りました。

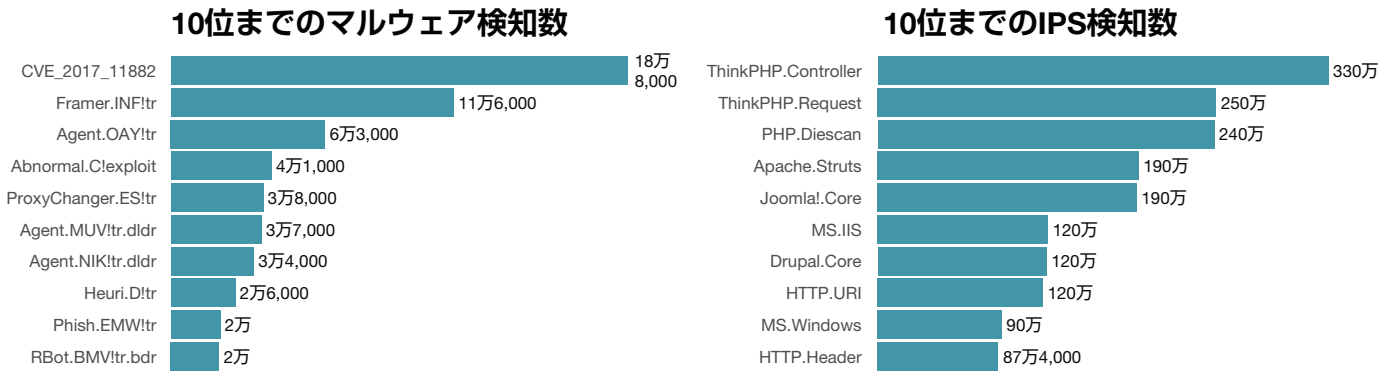

図 2：2019 年第 2 四半期に最も多く検知されたマルウェアと IPS（検知したセンサー数）

この脆弱性の 2017 という年は、少し誤解を招く恐れがありますが、これは一般公開された日付を表します。この脆弱性の存在は、発見の 2017 年より以前から存在していた、つまり未知である期間が長かったことを意味します。穿った見方をすれば、この長い間に世界中の多くの政府機関はその存在を知っていて内密に利用していたのだろうと推測されますが、その証拠があるわけではありません。我々のサンドボックスで最近のサンプルを実行してみたところ、この Word / RTF ファイルに関する新たな事実や注目点は見つかりませんでした。2 ～ 3 年前から大小さまざまな規模の攻撃で使われてきたものであり、次の段階へと進むような新しい機能が追加されたわけではないようです。図 3 は、世界全体での検知率をグラフにしたものです。

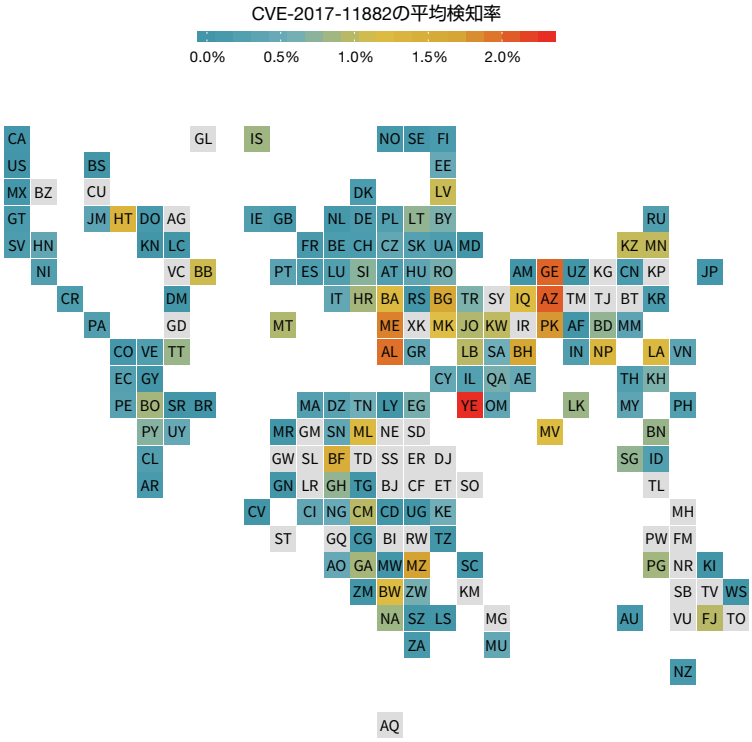

図 3：2019 年第 2 四半期の CVE-2017-11882 マルウェアサンプルの世界全体での検知状況

2019 年第 1 四半期のレポートでは、コンテンツ管理システムを標的とするエクスプロイトについて解説しましたが、ThinkPHP、Joomla、Drupal は業界を代表するコンテンツ管理システムであり、図 2 を見ると、引き続きサイバー犯罪の標的になっていることがわかります。これらのシステムを利用しているのであれば、この事実を無視するべきではありません。

図 2 には登場していないものの、Open Dreambox と Spree Commerce というプラットフォームに対する 2 つのエクスプロイトが検知されました。これらは、この後にデジタルサプライチェーンのエクスプロイトで説明するテーマと共通するものです。これらのプラットフォームやプラグインは、オンライントランザクションチェーン全体がサードパーティに大きく依存していることに目をつけた犯罪者の格好の標的になっているようです。

*2　CVE-2017-11882（英語）：https://nvd.nist.gov/vuln/detail/CVE-2017-11882

第 2 四半期の注目すべき新たな動き

2019 年第 2 四半期にフォーティネットが収集した情報やセンサーデータを検証し、ニュースで報道された事件を振り返ってみると、興味深いいくつかのトピックやトレンドが明らかになります。いずれもアナリストが注目に値すると考える脅威であるという点を除けば、何らかの正式な基準や共通する条件があるわけではありません。以下に紹介するトレンドが、第 3 四半期以降の脅威を予測する際の手掛かりになることを願っています。

ロビンフッドとその（不）愉快な仲間たち

この四半期に注目された複数のインシデントによって、対策が不十分である組織にとってのランサムウェア攻撃の影響の深刻さが浮き彫りになりました。5 月に発生したボルチモア市に対する攻撃[*3] では、基幹サービスが数週間にわたって中断し、市当局は、不動産取引、公共料金の支払い、固定資産税をはじめとする重要な機能を手作業で処理することを余儀なくされました。ボルチモア市当局は、FBI の助言に従って約 10 万米ドルの身代金の支払いを拒否し、結果的に 1,800 万米ドル以上を復旧作業に費やすことになりました。

ボルチモア市の攻撃で使われた、Robinhood（ロビンフッド）と呼ばれるランサムウェアを我々が分析したところ、組織のネットワークインフラストラクチャを攻撃するように設計されており、武器化したリモートデスクトップアプリケーション経由で送り込まれる可能性が高いことがわかりました。このマルウェアには、データの暗号化を禁止する Windows サービスを無効にしたり、共有ドライブから切断したりする機能が含まれています。

2019 年第 2 四半期に、他の複数の地方自治体や政府機関が同様の攻撃を受けました。その 1 つであるフロリダ州リビエラビーチは、ランサムウェア攻撃で暗号化されたデータを復元する作業を 3 週間も続け、最終的には 60 万米ドルを攻撃者に支払って復号キーを手に入れました。また、フロリダ州レイクシティも同様の攻撃を受け、混乱を避けるために 49 万米ドルを攻撃者に支払いました。被害者に適切なデータのバックアップとリカバリのプロセスがなく、唯一の選択オプションだったとしても、そのような身代金の要求に応じることは、ランサムウェア攻撃をさらに増加させる要因になるだけだというのが大方の見方です。

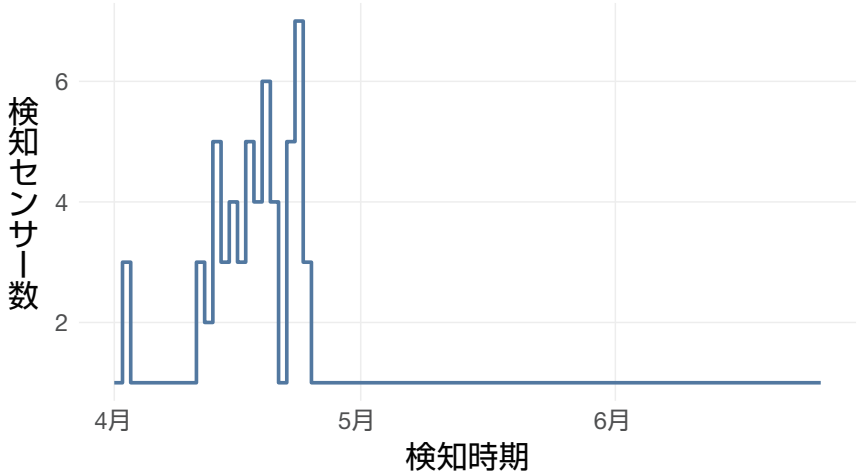

図 4：Ryuk 亜種が検知されたデバイスの数

フロリダで発生した攻撃で使われたランサムウェアは、昨年確認された Ryuk であるとする報道もあります。このランサムウェアは、暗号化キーを破壊したり、感染システムのシャドーコピーを削除したりするという、いくつかの回避手段[*4] を使用します。研究者は、Ryuk は主に標的型攻撃に使用されていると考えており、図 4 で検知数が少ないという事実もそれを裏付けています。RDP サービスに対するスピアフィッシングまたは総当り方式攻撃が主な拡散方法であると考えられます。

*3　RELEASE: City Provides Update on Baltimore Ransomware Attack（英語）：https://content.govdelivery.com/accounts/MDBALT/bulletins/249f7d3

*4　FortiGuard Threat Intelligence Brief - August 24, 2018（英語）：https://fortiguard.com/resources/threat-brief/2018/08/24/fortiguard-threat-intelligence-brief-august-24-2018

この四半期のランサムウェア攻撃でも、昨年から継続しているトレンドが確認されました。サイバー犯罪者は、無差別型のランサムウェア攻撃から脱却し、多額の身代金を支払う能力と理由の両方があると思われる組織に対する標的型攻撃へと移行しつつあります。これらの標的型攻撃では、サイバー犯罪者が被害者のネットワークに侵入し、念入りな偵察活動を実行した後に、慎重に選んだシステムにランサムウェアを送り込むのが一般的です。データを取り戻すために組織が支払う身代金の平均額と、混乱によって発生するコストの両方が急増しているという報告もあります。

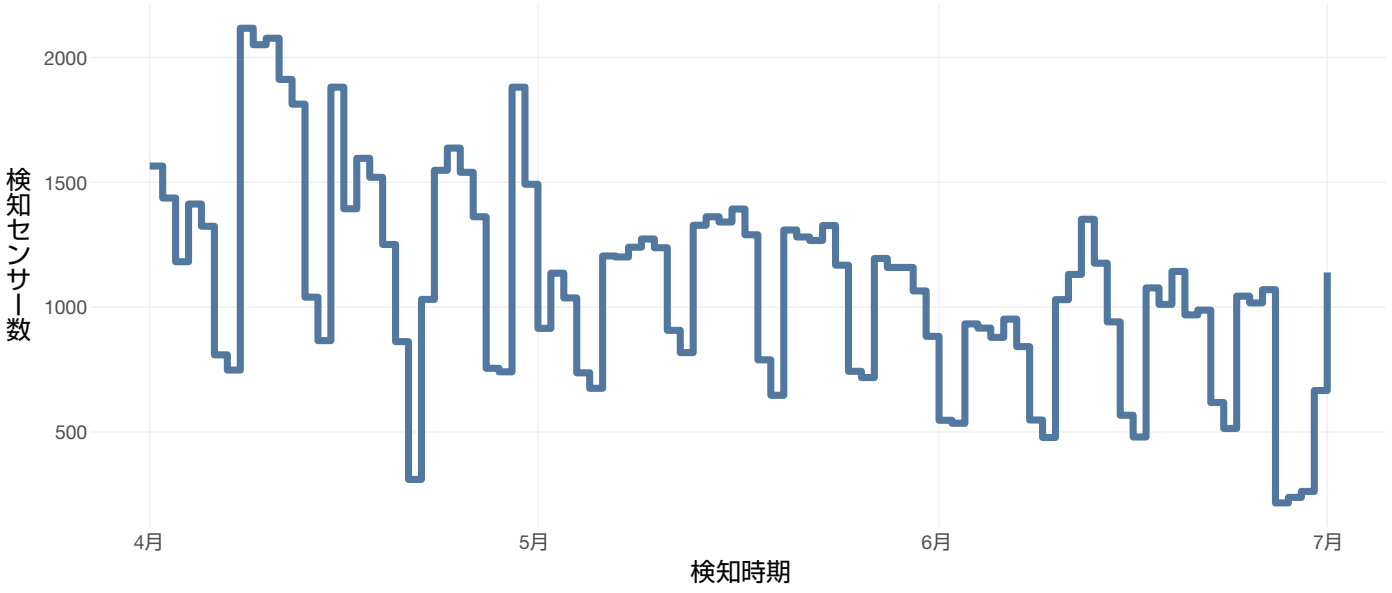

図 5：2019 年第 2 四半期のランサムウェア検知数（デバイス数）には減少傾向が見られる

第 2 四半期に新たに確認された、Sodinokibi（別名 Sodin）と呼ばれるランサムウェアは、今年は多くの企業にとって重大な脅威になる可能性があります。機能的に、Sodinokibi[*5] は他の多くのランサムウェアツールと大きな違いはありませんが、厄介なのは、最近公表された Oracle の WebLogic Server の重大な脆弱性（CVE-2019-2725）[*6] を悪用し、任意のリモートコードを実行可能にすることです。これは、標的となったシステムにおいていかなる操作を必要ともせず攻撃者が実行可能であることから、影響は深刻です。Oracle WebLogic Server のバージョン 10.3.6.0 あるいは 12.1.3.0 を利用中でパッチを適用していない場合は、直ちにパッチを適用することをお勧めします。

対策のヒント：ボルチモア市やフロリダ州の複数の地方自治体などが標的にされた、2019 年第 2 四半期に発生した攻撃は、ランサムウェア全体の件数は減少した一方で、ランサムウェアが組織にとって今後も深刻な脅威となるであろうことを示唆しています。

*5　FortiGuard Threat Intelligence Brief - May 03, 2019（英語）：https://fortiguard.com/resources/threat-brief/2019/05/03/fortiguard-threat-intelligence-brief-may-03-2019

*6　Oracle Security Alert Advisory - CVE-2019-2725（英語）：https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

RDP と「BlueKeep」の憂鬱

この四半期に大きな注目を集め、深刻な懸念をもたらした、「BlueKeep」と呼ばれるセキュリティ脆弱性は、Windows の複数の古いバージョンのリモートデスクトップサービス機能に存在する重大な脆弱性です。この脆弱性（CVE-2019-0708）[*7] によって、認証されていないユーザーが Microsoft の RDP（Remote Desktop Protocol）を使って脆弱性なシステムに接続して制御し、認証情報やデータを不正取得したり、ランサムウェアやその他のマルウェアを送り込んだりすることができます。

Microsoft や米国国土安全保障省をはじめとする組織が、この脆弱性の深刻さについて繰り返し警告しており、速やかにパッチを適用するよう呼びかけています。にもかかわらず、2019 年第 2 四半期末の段階のインターネットスキャンによって、パッチが適用されておらず攻撃に対して脆弱な RDP サービスを利用しているシステムが、80 万以上もインターネットに公開されていることがわかりました。6 月にフォーティネットが実施した調査 [*8] では、Microsoft Azure データセンターの IP 範囲に、いくつもの脆弱なシステムが見つかりました。我々の報告に対し、Microsoft は、それらの IP がおそらくはサードパーティの顧客に属しているものであり、Microsoft には直接属しているものではないだろうとしました。我々の調査によって、他のクラウドサービスプロバイダとその顧客も同様の影響を受ける可能性があることがわかりました。

リモートの Windows システムにアクセスしてさまざまな不正アクションを実行する目的で、数年前から多くの攻撃者が RDP を標的にしてきました。しかしながら、Microsoft の説明によると、BlueKeep が特に大きな問題であるのは、「ワーム」の特性を持ち、2017 年の悪名高い WannaCry ランサムウェアと同様に、ある脆弱なシステムから別の脆弱なシステムへの自律的な拡散が可能であるためです。このため、Microsoft は 5 月に BlueKeep に関連する警告を発表し、正式サポートを終了しているバージョンを含む Windows 向けのパッチを公開しました。

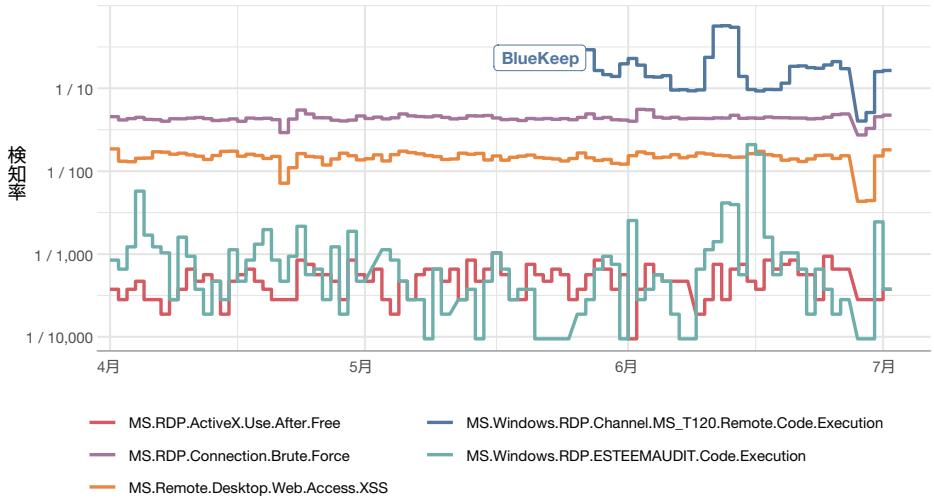

図 6：2019 年第 2 四半期の BlueKeep（MS. Windows.RDP.Channel.MS_T120.Remote.Code.Infection および MS.Windows.RDP.CVE-2019-0708.Remote.Code.Execution）と関連性のあるスキャンを含む、RDP エクスプロイトの試行が検知されたデバイスの割合

その後、BlueKeep の概念実証コードやエクスプロイトに関する複数のレポートが発表されました。DHS [*9] は、6 月の発表で古い Windows システムに対する BlueKeep のリモートコード実行エクスプロイトのテストに成功したことを明らかにしました。Metasploit のモジュールがすでに開発されていると言われています [*10] が、アウトブレイクが確認されるまで公開を見合わせているものと考えられます。Microsoft やセキュリティの専門家は、アウトブレイクは時間の問題と考えています。

FBI によると [*11]、2016 年の半ばから後半以降、リモート管理ツールを悪用する攻撃が着実に増加しており、RDP 認証情報へのアクセスが地下市場で広く販売されるようになったことが、その主な要因です。多くの場合、脆弱なパスワードを使って RDP へのアクセスを保護していたり、古いバージョンのサービスが動作していたり、デフォルトの RDP ポート（TCP 3389）へのオープンアクセスが可能になっていたりすると、これらの攻撃の標的になる可能性が高くなります。セキュリティに不備のある RDP サービスを使って拡散するマルウェアの最近の例としては、Dharma（別名 CrySiS）[*12]、SamSam [*13]、GandCrab [*14] ランサムウェア亜種があります。

対策のヒント：BlueKeep は、組織が RDP サービスを正しく保護することの重要性を思い出させてくれます。リスクを減災するベストプラクティスとしては、強力なパスワードとアカウントのロックアウトを使用して RDP への総当たり攻撃から保護すること、既知の脆弱性に対処するための利用可能なパッチとアップデートを適用すること、ネットワークレベルの認証を有効にすることなどがあります。

*7 CVE-2019-0708 のユーザー向けガイダンス | リモート デスクトップ サービスのリモートでコードが実行される脆弱性：2019 年 5 月 15 日：https://support.microsoft.com/ja-jp/help/4500705/customer-guidance-for-cve-2019-0708
*8 "BlueKeep" Vulnerability (CVE-2019-0708) within Cloud/Datacenter Machines: How to Safeguard Yourself?（英語）：https://www.fortinet.com/blog/threat-research/bluekeep-vulnerability-cloud-datacenters.html
*9 Alert（AA19-168A）Microsoft Operating Systems BlueKeep Vulnerability（英語）：https://www.us-cert.gov/ncas/alerts/AA19-168A
*10 MetaSploit Module Created for BlueKeep Flaw, Private for Now（英語）：https://www.bleepingcomputer.com/news/security/metasploit-module-created-for-bluekeep-flaw-private-for-now/
*11 Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity（英語）：https://www.ic3.gov/media/2018/180927.aspx
*12 Dharma Ransomware: What It's Teaching Us（英語）：https://www.fortinet.com/blog/threat-research/dharma-ransomware--what-it-s-teaching-us.html
*13 Critical SamSam Ransomware Update（英語）：https://www.fortinet.com/blog/threat-research/critical-samsam-ransomware-update.html
*14 GandCrab Threat Actors Retire...Maybe（英語）：https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html

巧妙化する分析回避機能

マルウェアツールの多くに、アンチウイルスをはじめとする脅威検知を回避する機能が組み込まれるようになりました。こうした分析回避技術の一般的な例としては、マルウェアがサンドボックス環境やエミュレータで実行されていることを検知するためのルーチン、感染させたシステムでセキュリティツールを無効にする機能、さらには、逆アセンブリを難しくするためのジャンクデータの使用などが挙げられます。MITRE のこのページ [*15] には、攻撃者が組織の防御をすり抜ける目的で利用する、新旧 60 以上の分析回避手法が紹介されています。

第 2 四半期に日本で発生した大規模スパム攻撃で使用されたことが確認されているマクロは、攻撃者がこれらの分析回避技術を常に微調整しながら使用し、防御を回避しようとしていることを示す良い例です。このスパム攻撃には添付ファイル付フィッシングメールが使用され、その添付ファイルが不正マクロを含む武器化された Excel 文書であることが分析によってわかりました。我々の分析では、このマクロには、セキュリティツールを無効にし、任意のコマンドを実行し、メモリの問題を発生させ、さらには日本のシステムでのみ実行されるようにするための属性が設定されていることが明らかになっています。

他の多くの不正ソフトウェアと同様、日本のスパム攻撃で使われた不正マクロも、実行中に複数箇所において特定の Excel 固有の変数を検索することで、エミュレータではなく Office Excel 環境で動作していることを確認するように設計されていました。ただし、この不正マクロが検索する Excel のプロパティの 1 つである xlDate 変数は、他のマルウェアでこれまでに見つかったことのないものでした。興味深いことに、この変数は Microsoft のリファレンスには記載されていないようで、少なくとも我々は見つけることができませんでした。

```
15  End Function
16
17  Private Sub Workbook_Open()
18      'debug.print
19      If xlXmlExportValidationFailed > 0 Then oceran
20  End Sub
21
22  Function lowsharts()
23      lowsharts = timefortime(3 - 2, 2 - 1)
24  End Function
25
26  Function Betal()
27      fdsgfadsrff436tgdfzf33546s = 1 + (Application.International(LittlePeace) - 1)
28      Betal = fdsgfadsrff436tgdfzf33546s
29  End Function
30
31  Function LittlePeace()
32      LittlePeace = ((xlDate))
33  End Function
34
Visual length : 1,506  lines : 61   Ln : 19  Col : 35  Sel : 27 | 1   Windows (CR LF)  UTF-8  INS
```

図 7：マクロで使用されていた分析回避の例。
xlXmlExportValidationFailed などの Excel 固有の変数を実際にチェックするマクロはそれほど多くありません。
作成者は、これをチェックすることでマクロが Office Excel 環境で確実に実行されるようにしており、
すなわち、特定の Excel 変数が正しくエミュレーションされないと、マクロエミュレータが失敗する可能性があります。

*15　Defense Evasion（英語）：https://attack.mitre.org/tactics/TA0005/

このような分析回避技術は目新しいものではありませんが、これを使用する例が増えているようです。セキュリティ研究者たちが 6 月に発見した、金融機関を標的にするトロイの木馬である Dridex の新しい亜種は、正規の Windows 実行可能ファイル名の 64 ビット DLL を使用することで、従来型のいくつものアンチウイルスツールを突破することに成功しました。被害者がログインする毎にファイル名や関連するハッシュが変わるため、感染ホストシステムに存在するマルウェアをシグネチャベースのアンチウイルスツールで検知するのは困難です。6 月に見つかった Dridex の亜種は、WMIC（Windows Management Instrumentation Command-line）ユーティリティの既知の脆弱性も悪用しており、アプリケーションのホワイトリストを使った検知を回避して XSL ファイルに埋め込まれた不正 VBS コードを実行します。

第 2 四半期は、高度な防御回避技術が組み込まれたダウンローダーがいくつも報告されました。その 1 つである AndroMut は、ロシア語圏で活動する犯罪集団である TA505 による、米国などの金融機関で働く個人を標的とした攻撃で使用されたダウンローダーです。AndroMut は、サンドボックスやエミュレータの確認、マウスの動きやデバッガーのチェックといった分析回避機能を備えていました。それ以外の少なくとも 2 つのダウンローダー（Brushaloader と新しいバージョンの JasperLoader）についても、位置情報の確認と、実行を遅延させるためのスリープタイマーをはじめとする類似の高度な回避メカニズムが組み込まれているものとして、2019 年第 2 四半期に報告されました。

対策のヒント：企業にとって、分析回避や広範な回避機能の使用の増加は深刻な問題であり、従来型のシグネチャ / 振る舞いベースの脅威検知だけに依存しない、多層型防御の必要性を再認識するきっかけにもなっています。

デジタルサプライチェーンの悪用

第 2 四半期に発生したいくつかの重大インシデントによって、サプライチェーンパートナーをはじめとした信頼できるサードパーティを悪用した攻撃が、組織の大きな脅威となっていることが明らかになりました。

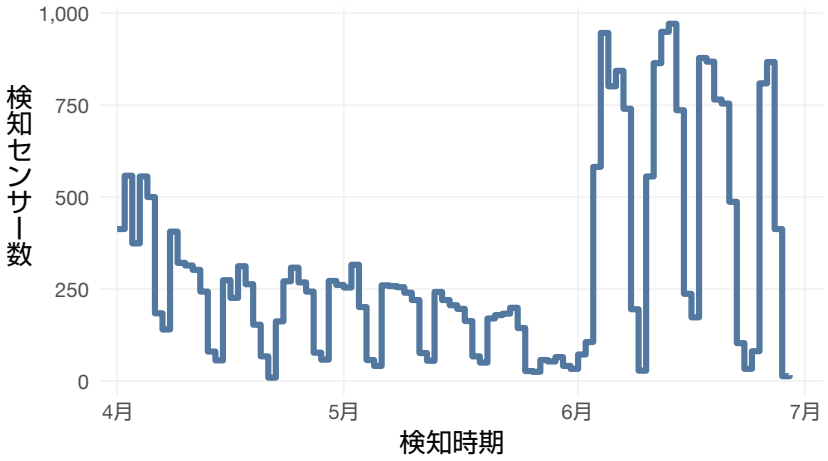

図 8：Magecart による攻撃と関連性のある Cryxos 亜種の 2019 年第 2 四半期の週毎の検知数

そういった攻撃の 1 つ、5 月に我々が報告した[*16] 攻撃では、JS/Cryxos.PWS!tr として検知された軽量の JavaScript カードスキマーが使われ、複数の電子商取引サイトから 185,000 枚以上のペイメントカードの情報が盗まれました。第 2 四半期の初めはこの亜種の活動に大きな変動は見られませんでしたが、6 月になると検知数が急増しました（図 8 参照）。我々の分析によって、この攻撃の初期段階で、サイバー犯罪者は毎月約 40,000 件のペイメントカードの情報を不正取得したことがわかりました。ほとんどの被害が米国に集中していますが、オーストラリア、イギリス、フランス、イタリアでも確認されています。

Magecart は、トラフィック量の多い Web ビジネスサイトからのクレジットカードやデビットカードの不正取得を専門にする、複数の犯罪集団の総称です。多くの場合 JavaScript スキマーは、コンテンツ管理、訪問者追跡、カスタマーサポート、支払いサービスなどのさまざまな機能に使用しているサードパーティ製コンポーネントに挿入されます。Magecart は、2018 年にブリティッシュ・エアウェイズ、チケットマスター、OXO などの大企業のサイトをはじめ、世界中の何百もの Web サイトからカードデータを盗んだとして、大きく報道されました。ブリティッシュ・エアウェイズは最近、この侵害に対して 2 億 3,000 万米ドル近い罰金の支払いを命じられました。これは、EU の GDPR（一般データ保護規則）の下でこれまで課された罰金としては最高額であり、サードパーティのリスクのコストが極めて高いという教訓といえるでしょう。

我々が 6 月に確認した別の攻撃も、これと同様の方法で複数の電子商取引サイトからカードデータを不正取得しようとするものでした。この攻撃について我々が調査を開始したのは、Inter と呼ばれる[*17] JavaScript スキマーが、Web サイトのトラフィックトラッカーとして偽装されていることわかったためです。調査によって、Inter が、標的にした Web サイトの支払いフォームにユーザーが入力したクレジットカード情報を傍受して不正取得するよう設計されていることがわかりました。また、分析によって、このスキマーの購入者ごとのニーズに合わせた高度な構成が可能であり、1 ライセンスあたり 1,300 ドルで、地下市場で売られていることもわかりました。

もちろん、サードパーティ製コンポーネントのデジタルカードスキマーだけが唯一の脅威というわけではありません。2019 年第 2 四半期には、企業が信頼できるパートナーとしてアクセスを許可している、取引業者などのサードパーティのシステムに攻撃者が最初に侵入し、そこから企業のネットワークに侵入するという例も数多く報告されました。

中国の犯罪集団である APT10 は、少なくとも 8 つの非常に大規模な IT サービスプロバイダーのシステムに侵入し、それらのプロバイダーの顧客に対する攻撃の足掛かりとしてそれらのシステムを使用したとされています[*18]。APT10 は、世界中の多数のマネージドサービスプロバイダーのネットワークのハッキングにも関わっているとされています。また、サイバー犯罪者が大手ハードウェアベンダーの自動ソフトウェアアップデートサーバーを攻撃し、そのシステムを使ってマルウェアを拡散した例も報告されています。この「ShadowHammer」攻撃の作成者は、攻撃したハードウェアベンダーの顧客の中から少数のシステムを厳選して標的にしましたが、その影響で、それ以外の何千ものコンピュータにも感染が広がりました。

対策のヒント：このような報告は、サードパーティに起因するリスクに適切に対処することの重要性を再認識させるものです。PCI DSS や HIPAA などの責任義務を果たすために、こういったサードパーティのサービスを利用している組織は主体的な責任者としてデータを保護する必要があり、その責任を怠ると深刻な結果を招く恐れがあります。

*16 Over 185,000 Payment Card Details Stolen by MageCart（英語）：https://www.fortinet.com/blog/threat-research/payment-card-details-stolen-magecart.html

*17 Inter: Skimmer For All（英語）：https://www.fortinet.com/blog/threat-research/inter-skimmer-for-all.html

*18 Exclusive: China hacked eight major computer services firms in years-long attack（英語）：https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc/exclusive-china-hacked-eight-major-computer-services-firms-in-years-long-attack-idUSKCN1TR1D4

スマートホーム / ビジネスを探し回る活動

この四半期の最後の特集では、過去のレポートで詳しく説明したことのない、ある分野の脅威を取り上げます。IoT（モノのインターネット）における脅威、さらには家庭用ルーター、IP カメラ、プリンターなどの一般消費者向けデバイスを探し回る活動については、これまでに何度も説明してきました。また、対照的な分野である重要インフラに対する脅威についても解説し、ICS（産業用制御システム）や SCADA（監視制御システム）のテクノロジーを標的とするエクスプロイトについても詳しく分析してきました。

ところが、この家庭用プリンターと重要インフラの中間に位置する、住宅や小規模企業向けの制御システムが増えています。このようなスマートシステムに対する注目度は、他のスマートシステムよりも低いものですが、状況は変わりつつあります。

その事実を証明するデータとして、シュナイダーエレクトリック社製デバイスを標的にするスキャンが増加しています。シュナイダーエレクトリック社は大手の産業用制御機器メーカーであるため、当初これらの活動は OT（運用テクノロジー）への侵入経路を探し回る活動に分類されるものだろうと推測していました。そして、そのような判断を裏付ける前例もたくさんあります。最近 Xenotime という名前の犯罪集団が、米国の多数の電力網を広範囲にわたってスキャンしていたことが明らかになっています。Xenotime[*19] は、数年前に中東の石油会社のシュナイダー社製 Triconex SIS（安全計装）コントローラーに対する Triton 攻撃に関与した犯罪集団であるとされています。また、今年初めに北米の複数の石油 / ガス生産施設を攻撃したと報道されています。

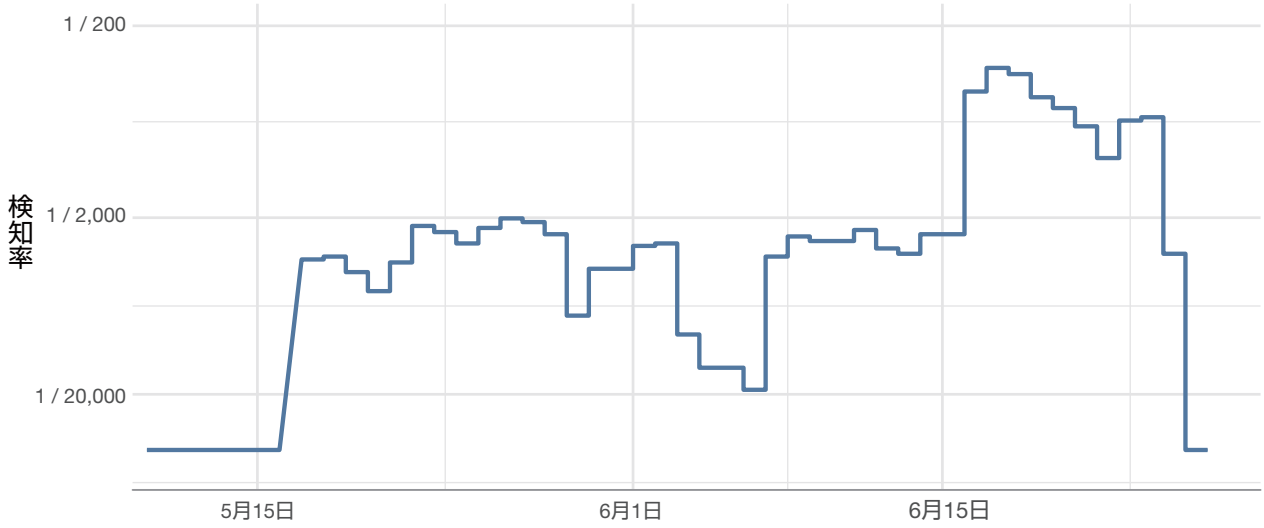

図 9：シュナイダー社製 U.motion デバイスを探し回る行動が検知されたデバイスの割合

しかしながら、今回の活動はシュナイダー社製 Triconex コントローラーを標的とするものではありません。我々が注目したのは、シュナイダー社の U.motion[*20] に関連する検知であり、同社の説明によれば、この製品ラインはビル管理ソリューションです。これに関連するシグネチャが 1% の組織で確認されており、それほど大きい数字とは思えないかもしれませんが、シュナイダー（および他のメーカー）の ICS や SCADA での通常の数よりはるかに大きい数字です。図 9 を見ると、このシグネチャが 5 月中旬の導入の直後に 1 日あたりの感染率が 10 倍以上も上昇し、その 1 か月後にさらに 10 倍になったことがわかります。

U.motion パネル（通常は外部に公開されている Web ページ）を利用しているホスト / 標的を特定した攻撃者は、PHP の簡単な Web ページの post メソッドを使うことでこのエクスプロイトを簡単に実行できるようになります。エクスプロイトが成功すると、シュナイダー社製デバイスの制御が可能になるだけでなく、環境制御、セキュリティカメラ、安全システムなど、管理下にある他のあらゆるデバイスにアクセスできるようになります。知恵のある犯罪者がこれらのアクセスを悪用した場合、甚大な被害が発生することは想像に難くありません。一般家庭や小規模企業向けのスマートシステムのセキュリティに対して、これまで以上に注目すべきであることは明らかです。

対策のヒント：U.motion のエクスプロイトが急速に拡大したという事実は、犯罪者が家庭や企業のデバイスを制御する機会を虎視眈々と狙っていることの現れです。残念ながら、これらの分野、特に一般的な IT システムに分類されないものに関するサイバーセキュリティは見過ごされてしまうことが多く、予算が十分に配分されないのが現状です。

*19　The Highly Dangerous 'Triton' Hackers Have Probed the US Grid（英語）：https://www.wired.com/story/triton-hackers-scan-us-power-grid/

*20　U.motion（英語）：https://www.schneider-electric.com/en/product-range/61124-u.motion/

マルウェアの研究：Zegost

Zusy または Kris という別名で活動することもある Zegost は、2011 年以来活発に活動を続けている中国発祥の情報窃盗マルウェアです。Zegost は、これまでに何回ものアップデートを繰り返しています。たとえば、PowerShell アクションを使用して、被害者のマウスがある文字領域をホバリングした瞬間に情報窃盗マルウェアをダウンロードできるようになったことで、攻撃能力が大幅に向上しました。また、自らのイベントログをクリアする機能が Zegost に追加されたことで、この情報窃盗マルウェアは長期間にわたって検知を回避できるようになり、被害者のネットワークを長時間水平移動可能になりました。さらに、被害者の Web カメラにアクセスして写真や映像を記録する機能も追加されています。前回のアップデートでは、マルウェアとしては珍しい COM プログラミングを利用する機能が追加されました。

他の情報窃盗マルウェアと同様、被害者のデバイスに関する情報を収集し、取得することが Zegost の主な目的です。被害者のコンピュータの OS バージョンの確認、プロセッサの速度や数の分析、インターネット接続のチェック、RDP ポート番号の調査を実行します。また Zegost は、中国で広く利用されているチャットクライアントである QQ のログイン番号も手に入れようとします。

他の情報窃盗マルウェアと比べると、Zegost は、レーダーに発見されることなく潜伏できる特殊な構成になっているため、同時期に登場した類似のマルウェアよりもはるかに長期間の脅威となります。そのために、このマルウェアは自らのイベントログを消去し、ミューテックスを作成して 1 つのバージョンだけが実行中であることをチェックすることで、実行時の競合を回避しています。Zegost には、これ以外にも 2019 年 2 月 14 日まで実行を「停滞状態」にした後に感染ルーチンを開始するコマンドが新たに追加されています。また、Zegost が他の情報窃盗マルウェアと大きく異なるのは、プロセスを起動するウィンドウを非表示にすることで検知を逃れる機能を備えている点です。Zegost は、これまでに Adobe Reader の脆弱性、具体的には CVE-2013-0640 のエクスプロイトとしても知られており、これによってリモートからの任意コードの実行が可能になります。

Zegost は、情報窃盗マルウェアとして多くの攻撃者に広く利用されるようになり、過去にさまざまな攻撃で使用されてきました。Linux のボットネットである Mr. Black は、過去の攻撃で Zegost を使ってルーターへのアクセスを手に入れ、DDoS 攻撃の目的でボットネットに参加させました。この情報窃盗マルウェアは、ネパールや複数のベトナムの政府機関を標的として攻撃したことがあります。Zegost が使われた例として最も有名なのは、2015 年にイタリアの倫理観に欠けるセキュリティ企業である The Hacking Team に対する攻撃であり、同社が使用していたエクスプロイトのリストが漏洩しました。

現在 Zegost は、中国のさまざまな分野の統計分析を提供している政府機関に対するスピアフィッシング攻撃の基盤として使われています。この攻撃の動機は今のところわかっておらず、Zegost のホスティングインフラストラクチャの主な拠点は中国ですが、この情報窃盗マルウェアのサードレベルドメインは国外でも観察されています。Zegost の詳しい解説については、FortiGuard Labs のオンラインビューア [*21] を参照してください。

探索的分析：脆弱性の調査

このレポートは、その名前のとおりサイバー環境に点在するさまざまな種類の脅威を検証するものですが、サイバー環境はハードウェアとソフトウェア（さらにはウェットウェア）の脆弱性の影響を大きく受けるため、脆弱性の発見と調査にも積極的に取り組んでいます。事実、脆弱性の調査は FortiGuard Labs の戦略的重点分野の 1 つであり、その努力を続けることでフォーティネット製品の改善につながるだけでなく、より広いコミュニティに多くの恩恵をもたらすことにもなります。このセクションでは、2019 年第 2 四半期の脆弱性の調査と実績の一部を紹介します。

ゼロデイ脆弱性の調査研究

フォーティネットのエキスパートは、サードパーティのさまざまな製品やソフトウェアアプリケーションの弱点、悪用可能な脆弱性の調査を日々続けています。FortiGuard Labs は、発見した脆弱性をソフトウェアまたは製品の開発元に通知し、フォーティネットのお客様に提供するための保護機能を作成します。

表 1 は、2019 年第 2 四半期にフォーティネットが脆弱性を公開した製品の一覧です。チームはこれ以外にも 33 のゼロデイを発見しましたが、ベンダーによる修正プログラムの作成が完了していないため、詳細はまだ公開されていません。

*21　FortiGuard Playbook Viewer（英語）：https://fortiguard.com/playbook

製品	件数	製品	件数
Adobe Magento	1	LiveZilla Server	7
Adobe Shockwave Player	7	Microsoft Office	1
Cisco WebEx	3	Microsoft Windows	5
Ignite	1	Oracle	1
Keysight EMPro	1	RocketChat	1

表 1：2019 年第 2 四半期に公開されたゼロデイ脆弱性

このような取り組みが評価され、フォーティネットは上海で開催された BlueHat 2019 で、脆弱性を報告した上位 5 社の 1 社として Microsoft から表彰されました。脆弱性およびその他のゼロデイの調査に関するフォーティネットの取り組みの詳細については、https://fortiguard.com/zeroday[*22] を参照してください。

エクスプロイトの予測

フォーティネットは、脆弱性の調査を自らが実施するだけでなく、他の組織による脆弱性の調査にも協力しています。6 月に、バージニア工科大学、Cyentia Institute、RAND の研究者が、WEIS（Workshop on the Economics of Information Security）[*23] で共同論文を発表 [*24] しました。同論文で紹介されている機械学習モデルは、CVSS（Common Vulnerability Scoring System）などの既存の優先度方法論より確実に優れたパフォーマンスでの脆弱性のエクスプロイトの予測を可能にするものです。

関連する過去の研究では、実際にエクスプロイトが確認されたものではなく、公になっている概念実証やエクスプロイトコードによる脆弱性の予測モデルが紹介されていました。フォーティネットの膨大な数のデバイスがインターネットにおけるエクスプロイトの活動を監視していることを知った研究者は、実際に観察されたエクスプロイトに関するデータの無害化と提供をフォーティネットに依頼してきました。我々が喜んで研究に協力したことは言うまでもありません。フォーティネットが提供したこのような広範なデータセットによって、研究者たちは過去最高だった研究の 3 倍近い、実際に悪用された脆弱性のデータを使用し、予測モデルのトレーニングとテストを実施しました。そのデータに基づき、研究者たちは NVD（National Vulnerability Database）[*25] に登録されている 10 万強の脆弱性の 5.5% が実際に悪用されていると結論付けました。この論文の全文は、こちら [*26] から参照いただけます。

エクスプロイトまでの時間

エクスプロイトの可能性を予測するだけでなく、脆弱性の発見からどの程度の時間が経過した後にエクスプロイトが実際に開始するか知ることも重要だと我々は考えます。脆弱性とエクスプロイトが（フォーティネットや他のベンダーによって）確認されると、我々は検知のためのシグネチャを作成し、FortiGuard 対応デバイスに配備します。当然ながら、これは一刻を争う、終わることのないプロセスです。

シグネチャの公開からエクスプロイトの最初の（またはピークの）検知までに、どの程度の時間が経過しているのでしょうか？この調査のため、我々は第 2 四半期に公開されたシグネチャのサンプルを使って、公開から 30 日後までのエクスプロイトの活動を検証しました。図 10 は、その結果を記録したものです。

*22 Zero-Day Research | Fixes Available（英語）：https://fortiguard.com/zeroday

*23 The 2019 Workshop on the Economics of Information Security（英語）：https://weis2019.econinfosec.org/

*24 Improving Vulnerability RemediationThrough Better Exploit Prediction（英語）：https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf

*25 National Vulnerability Database（英語）：https://nvd.nist.gov/

*26 Improving Vulnerability RemediationThrough Better Exploit Prediction（英語）：https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf

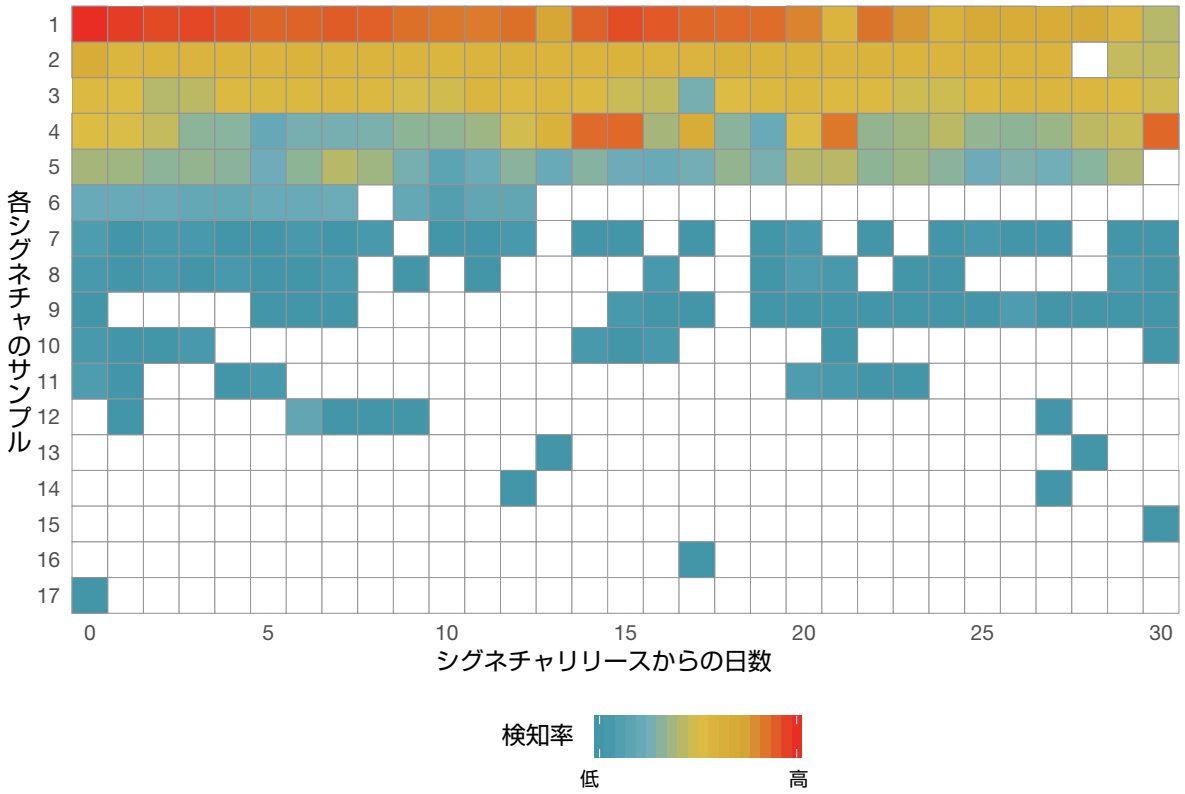

図 10：シグネチャの配備から 30 日後までのエクスプロイトの検知率

図 10 には興味深い発見が数多くありますが、ここではその一部を解説します。まずはじめに、シグネチャの開発と配備を急ぐ必要がある理由は明白です。シグネチャが配備されるまでの間に、多数のエクスプロイトがすでに活動を開始しています。これが、ベンダーが修正プログラムを作成するまで脆弱性情報を公開しない最大の理由です。攻撃者に有利な情報を与える必要はありません。また、エクスプロイトがピークを迎えるまでの過程もさまざまです。脆弱性が公開された直後に開始するエクスプロイトがある一方で、かなりの時間が経過した後にピークを迎えるものもあります。また、いつまでたっても沈静化しないものや、間欠的に活動が繰り返されるものもあります。

このようなエクスプロイトの活動時期を理解することが、攻撃者に先手を打たれ劣勢に立たされてしまうことの回避につながり、これこそが本レポートの大きな目標の 1 つであるとも言えます。我々が直面する脅威に関する有益な情報は、組織の利益と資産を保護する、より効果的な戦略が何であるかを教えてくれます。今回も本レポートを最後までお読みいただき、ありがとうございました。次の四半期のレポートで再びお会いできることを楽しみにしています。

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

TR-19Q2-2019-09-R1