KASPERSKY

Kaspersky Security Bulletin 2016

2017年サイバー脅威の予測:「脅威存在痕跡」の信頼性が低下

GREAT

目次

はじめに

注目すべき情報セキュリティの出来事に関して、2016年は歴史に残る1年でした。衝撃的な出来事、悪意ある企て、エクスプロイトに見舞われました。Kaspersky Labのグローバル調査分析チーム（GReAT）は、これまでのさまざまな調査で観測してきた傾向に基づき、2017年の脅威動向を予測しました。脅威インテリジェンス分野のリサーチャーおよび読者の一助となることを願っています。

2016 年の予測を振り返る

2015年末に発表した、2016年の脅威動向予測は概ね当てはまり、一部は想定よりも早い時期に実現しました。主な予測について振り返ってみます：

APT：APT攻撃においては、感染し続けることを重視する傾向が弱まるとともに、コモディティ化されたマルウェアの利用により、一般的な所にマルウェアが潜伏する傾向が強まると予測しました。このことは、メモリ常駐型またはファイルレスマルウェアの増加、およびNJRat、Alienspy、Adwindなどの既製のマルウェアに依存した活動家や企業への無数の標的型攻撃を通じて観測しています。

ランサムウェア：2016年はまさにランサムウェアの年でした。金融機関の利用者を狙ったマルウェアは、その影響を受けて事実上ランサムウェアのみとなり、さらに効果的な恐喝の企てのため、収益性の低い分野からマルウェアの開発リソースが取り込まれています。

サイバー銀行強盗の増加：金融系サイバー攻撃が過去最高の水準で拡大するという仮説には、証券取引所などへの攻撃が含まれていました。この予測は、SWIFTネットワークへの攻撃により現実のものとなり、標的を定めた巧妙なマルウェアによって、数百万ドルの被害が発生しました。

インターネットへの攻撃：ごく最近になりますが、これまで見過ごされる傾向にあったインターネットに接続した低水準のデバイスが、ついにIoTボットネットという形で悪用されました。IoTボットネットにより主要なインターネットサービスのサービス停止が発生し、特定のDNSプロバイダーに依存するサービスにも不具合が生じています。

誹謗中傷：誹謗中傷と脅迫が引き続き大きな注目を集めています。戦略的で見境のない個人情報の流出により、プライベートに関わる問題、評判を損なう問題、および政治的な問題が至るところで発生しました。このような情報流出の規模と損失については驚くべき状況だと言わざるを得ません。

2017 年サイバー脅威の予測

APT の脅威

カスタマイズと受動的な埋め込まれたマルウェアが増加

脅威存在痕跡（Indicators of Compromise：IOC）は、ハッシュ、ドメイン、実行の痕跡などの、既知のマルウェアの特徴を共有して活動中の感染を検知する有効な手段です。しかし、サイバースパイ活動に関して、これらの一般化された手段では対抗できないことが明らかになりました。最近発見したProjectSauron APTで明らかになったのは、巧妙にカスタマイズされたマルウェアプラットフォームでは、それぞれの標的に合わせ機能が変ってしまうため、IOCは別の感染を検出する手段として役に立ちません。しかし、セキュリティ業界に打つ手はあり、Kaspersky Labは、YARAルールの採用を拡大していくべきだと考えています。YARAを活用することで、企業の隅々にまでスキャンを実施し、休止中のバイナリの特徴を検査・特定するとともに、メモリをスキャンして既知の攻撃の断片を探し出すことが可能になります。

ProjectSauronでは、そのほかにも、今後増加が予想される「受動的な埋め込まれたマルウェア」の特徴が明らかになっています。ネットワークを介して攻撃を行うバックドアは、メモリ上に存在もしくはゲートウェイやインターネットに接続したサーバーに存在するバックドア型ドライバーとして、マジックバイトによって機能が活性化されるまで潜伏します。この受動的な埋め込まれたマルウェアは、活性化されるまで感染の兆しをほとんど示しません。そのため、徹底的に調査をおこなうセキュリティ業者、またはインシデントレスポンスシナリオの一部以外では、検出されることはほとんどありません。このような埋め込まれたマルウェアには、関連付けと匿名性の高い拠点を提供するための事前に定義された指令サーバーのインフラがない点に留意してください。このマルウェアは、標的とするネットワークへの速やかな侵入が必要な攻撃者が最も好むツールになっています。

一過性の感染

Windowsの管理者にとってPowerShellは理想的なツールですが、一方で、密かな開発、横展開、標準的な構成でログに残らない偵察機能などを探しているマルウェア開発者達にも効率的な環境です。メモリやレジストリに保存されたPowerShellを悪用した小さなマルウェアが、最新のWindowsシステムで活動する可能性が高くなっています。さらには、全般的なスパイ活動と認証情報の収集を目的とし、感染の継続は目的としないメモリ常駐型マルウェアによる、一過性の感染が出現する見込みです。機密性の高い環境において、マルウェアがセキュリティリサーチャーに発見されることを回避できるのであれば、攻撃者はシステムの再起動時にマルウェアをメモリから削除することは問題無いと考えられます。一過性の感染が出現することで、高度なアンチマルウェアソリューションのプロアクティブで、洗練されたヒューリスティックによる防御の必要性が浮き彫りになるでしょう。(参照：システムウォッチャー)

スパイ活動がモバイルを標的に

これまで複数のサイバー犯罪者達は、HackingTeam社の顧客やNSO 社の疑わしいiOS版マルウェアスイートPegasusの顧客と同様に、モバイルアプリに埋め込まれたマルウェア（Sofacy、RedOctober、CloudAtlasなど）を利用してきました。しかしながら、これらには主にデスクトップ用ツールキットをベースとした補完されたキャンペーンが存在します。今後は、デスクトップ環境導入に対する関心の低さ、および人々のデジタルライフのモバイル化が進んでいることから、モバイルを主な標的とするスパイ活動が増加すると予測します。その背景には、注目度の低下、およびフォレンジックツールによる最新のモバイルOSの分析が困難な現状があります。

金融システムへの攻撃の予測

サイバー銀行強盗の増加

2016年にはSWIFTネットワークに対する攻撃が発表され、大胆かつ細心な手口による数百万ドルもの窃取が明らかになり、金融サービス業界全体に衝撃を与えました。この動きはCarbanakサイバー強盗グループやそのほかのサイバー犯罪者グループにとっては自然な流れでした。これらの事例は確かな能力を備えたAPTグループによるものですが、サイバー銀行強盗で多額の金銭を得ることに関心を持つのは彼らだけではありません。

サイバー犯罪への関心が高まるにつれて、多層の犯罪組織で構成される闇市場では、SWIFTを標的としたサイバー銀行強盗の仲介者の増加が予想されます。サイバー銀行強盗を実行するには、初期アクセス、専用のソフトウェア、粘り強さ、マネーロンダリングの仕組みが必要です。これらの各ステップには、サービスを提供して報酬を得る犯罪組織が既に存在し、欠けている要素はSWIFTを攻撃するための専用マルウェアだけです。専用のリソースが闇フォーラムで、またはas-a-service形態で販売され、これらの攻撃の商品化が起きると思われます。

抵抗力のある電子決済システム

電子決済システムの普及が進むにつれて、犯罪者の関心も高まって行きますが、現在、導入されている電子決済システムは強固な弾性があり、大規模な攻撃は現在のところ確認されていません。これは消費者にとっては喜ばしいことですが、サイバー犯罪者は電子決済システムのプロバイダーを標的とし、そのインフラを直接攻撃するため、プロバイダーにとっては悩みの種になっています。電子決済システムへの攻撃が、直接的な経済的損失を引き起こしても、あるいはサービスの停止や中断が発生するだけであっても、その普及につれて悪質な攻撃者の関心を集めるでしょう。

卑劣で嘘つきなランサムウェア

すべての人にとってランサムウェアは嫌悪すべき存在ですが、多くのランサムウェアには、標的とサイバー犯罪者の奇妙な信頼関係が存在します。この犯罪エコシステムは、犯罪者が標的と結んだ暗黙の約束（身代金の支払いでファイルが戻ってくる）の上に成り立っています。犯罪者がこの約束を守る態度を示してきたことで、犯罪エコシステムは成功を収めてきました。しかし、ランサムウェアの攻撃が引き続き増加し、程度の低い犯罪者がこの分野へ参入している中で、実際にこの約束を守れるだけの品質や一般的なコーディング能力がない「ランサムウェア」が増加する可能性が高まっています。

スキルのない犯罪者によるランサムウェアが、ファイルやシステムのロックや、ファイルを削除して、標的に身代金を支払わせても何も戻ってこないケースが予想されます。この段階ではランサムウェアと削除攻撃はほとんど見分けがつかず、ランサムウェアのエコシステムでは「信頼性の危機」が起こるでしょう。これによって高度なスキルを持つ大規模な犯罪グループが攻撃を止める可能性は低いのですが、ランサムウェアの拡大に対抗する諸機関が、標的になった人に身代金の支払いをアドバイスするという発想を捨てるきっかけになるでしょう。

サイバー妨害工作に対する脆弱性

大きな注目を集めたStuxnetは、産業システムへの攻撃の可能性を現実のものとしました。Stuxnetは特定の標的への長期的な妨害工作を目的とし、慎重に設計されていました。世界規模で感染が拡大したにもかかわらず、ペイロードの確認によって副次的なダメージは免れ業界全体に被害が及ぶことはありませんでした。しかしその後は、産業事故や原因不明の爆発に関する噂や報道がきっかけとなり、サイバー妨害工作が注目を集めるようになっています。

確かにサイバー妨害工作による産業事故の誘発はあり得ます。重要インフラや製造システムは依然としてインターネットに接続されており、ほとんど、あるいはまったく保護されていないことも珍しくなく、高度なスキルを備え大規模な破壊を狙う攻撃者にとっては魅力的な標的です。過度の心配は別として、このような攻撃には、ある程度のスキルと目的が必要な点に注目すべきです。サイバー妨害工作による攻撃は、地政学的な緊張の高まりとともに、脅威の攻撃者達によって引き起こされる可能性が高くなります。

過密状態のインターネットによる反撃

別の名前のレンガ

Kaspersky Labはこれまで、モノのインターネット；Internet of Things、またはThreat（脅威）の脆弱なセキュリティによって攻撃を被ると予測してきましたが、今まさにそれが現実のものとなっています。ボットネット「Mirai」により最近明らかになったように、不必要にインターネットに接続したデバイスの脆弱性が、ほとんど、または全く責任を問われることなく大規模な損害を引き起こす機会を攻撃者に与えています。情報セキュリティに精通した人にとっては驚くようなことではありませんが、次のステップは特に興味深いかもしれません。私的制裁を加えようとするハッカーが、自らの手で問題に対処する可能性があります。

既存のパッチ処理の概念や報告された脆弱性は、セキュリティリサーチャーの真摯な（多くの場合無償の）取り組みの証として、神聖な地位を得ています。セキュリティ保護がされていないIoTデバイスが次々と市場に投入され、さまざまな問題を引き起こしている中、私的制裁を加えようとするハッカーが自らの手で問題に対処するかもしれません。脆弱なデバイスをレンガのように積み上げてメーカーに突き返すよりも効果的な方法は何でしょうか？ IoTボットネットがDDoS攻撃やスパム配布の問題を引き起こす中、消費者やメーカーにとっては遺憾なことですが、エコシステムの免疫反応によって脆弱なデバイスが全て無効にされる恐れがあります。レンガのインターネット（Internet of Bricks）が現実のものとなる可能性が高まっています。

物言わぬ点滅する箱

ShadowBrokersによる情報流出には、複数の主要メーカーのファイアウォールへの不正侵入が多数絡んでいました。その直後には大規模なエクスプロイトの報告が続き、メーカーは攻撃者に利用された脆弱性の把握と問題の修正に追われました。損害の程度はいまだ十分に把握されていません。このエクスプロイトによって攻撃者が手にしたものは何でしょうか。どのような種類のマルウェアが脆弱なデバイスに潜伏しているのでしょうか。

（2015年に発見されたJuniper社のScreenOSのバックドアに留意しつつ)これら特定のエクスプロイトの先に目を転じると、企業ネットワークの境界において重要な役割を持つデバイスに関しては、デバイスの統合という大きな問題が存在します。「設置したファイアウォールは誰のために機能しているのか」という問いに対する答えは、いまだ見出されていません。

偽旗作戦によるなりすまし

偽旗作戦と心理作戦（PsyOp）はKaspersky Labが特に関心を寄せるトピックであり、当然ながらその分野でいくつかの傾向の拡大が予測されています。

情報戦争の増加

標的を絞った情報流出や脅迫のための実在しない組織作りを最初に行ったのが、LazarusやSofacyなどのサイバー犯罪集団です。実存しない組織の利用は過去数か月で一定の成功を収め、悪評が高まっていることから、世論操作や人気の高いプロセスの全面的な混乱を狙った情報戦争の作戦が増えることが予想されます。ハッキングされたデータに関心を持つサイバー犯罪者にとって、偽りのハクティビスト集団を通じて作られた物語から失うものはありません。人々の注意を攻撃そのものから、暴露した情報へと転じさせるだけです。

この段階での真の危険はハッキングでもプライバシーの侵害でもなく、ジャーナリストや懸念を示す市民が、放出されたデータを事実として認識することに慣れてしまうことです。これは、データの操作や削除によって結果を操ろうとする、より狡猾なサイバー犯罪者にその機会を与えてしまいます。このような情報戦争の作戦に対する脆弱性は過去最悪の状況になっています。より多くの攻撃者（または多くの使い捨てマスクを使う同一の攻撃者）によってこの手口が利用されていることから、多くの人々が流出した情報を識別する力を持つことが期待されます。

抑止の展望

国際関係においてサイバー攻撃が果たす役割が拡大するにつれて、地政学的な交渉方針を決定する上でアトリビューションが重要な課題となるでしょう。政府機関が手続きや告訴に利用するアトリビューションの基準を決定するにあたっては熟慮が求められます。さまざまな公私機関の断片化された認知では正確なアトリビューションはほぼ不可能であることから、「緩やかなアトリビューション」で十分だと考えられるようになるかもしれません。狡猾なサイバー犯罪者は最初の段階でアトリビューションの試みの裏をかくことからも、報復によってさらに問題が生じないようにすることが重要です。報復と重大な結果がもたらされる可能性が高まっていることから、オープンソースの商用マルウェアの利用が急増する恐れがあります。Cobalt StrikeやMetasploitなどのツールは、クローズソースの独自のマルウェアにはない説得力のある反証機能を提供しています。

偽旗作戦の重大性

すでに発表した、偽旗（にせはた）作戦レポートに示した例は、その要素を利用するAPTに含まれますが、真の偽旗作戦は現時点で確認されていません。ここで言う真の偽旗作戦とは、サイバー犯罪者Aが別のサイバー犯罪者Bの方法とスキルを使用して完璧に模倣した作戦であり、目的は罪のないサイバー犯罪者Bに対する標的からの報復を誘発することです。真の偽旗作戦が既に起きていることをリサーチャーが把握していない可能性もありますが、このような作戦では、サイバー攻撃への報復が事実上影響を及ぼさない限り意味を成しません。報復（申し入れ、制裁、報復的なコンピューターネットワークの探査活動のいずれであっても）がより一般的で衝動的なものになるにつれて、真の偽旗作戦が注目されることが予想されます。

これが現実になれば、偽旗作戦が大きな投資価値を持つと予想され、インフラや用心深く守られてきた独自のツールキットの公開市場での投げ売りが誘発されることも考えられます。スクリプトキディ、ハクティビスト、サイバー犯罪者が、高度な脅威アクターの独自ツールを突如利用できるようになることで、多数の攻撃において匿名性が確保さて執行機関のアトリビューション機能が一部損なわれ、狡猾な脅威アクターがリサーチャーとセキュリティ業界に大きな混乱をもたらす恐れがあります。

プライバシーの問題

ベールをはがす

広告主にとってもスパイにとっても、サイバー空間に残った匿名性の痕跡には、発見されるべき大きな価値があります。広告主にとっては、永続的なクッキーを使用した追跡が価値ある手法です。これはさらなる拡大が見込まれており、ウィジェットやほかの無害な追加機能と組み合わせて一般的なWebサイトで使用することで、訪問者が特定のドメイン以外に移動する際に追跡できるため、企業は訪問者の閲覧傾向についての統合的なビューを得ることができます。

反体制派や活動家をインターネットで広範かつ詳細に追跡する斬新なツールを持つ、巧妙に配置された無名の会社に多額の資金が流入しています。世界の国々では、標的とした活動家の「政情不安を誘発する」ようなソーシャルメディア活動の追跡が続き、今後もそういったツールの高度化が進むと考えられます。通常このような活動は、地理的地域全体におけるソーシャルネットワークの傾向、および反体制派の声が地域に与える影響に強い関心を持っています。今後は、攻撃者が個人情報や不利なデータを求めてソーシャルネットワークへの不正侵入という大胆な行動に出ることも予想されます。

広告ネットワークを利用したスパイ活動

広告ネットワークは、普及している技術の中でも標的を絞った攻撃に最も効果的です。広告ネットワークの設置は完全に経済的な動機によるもので、主要サイトに対する悪意ある広告の攻撃が頻発していることからも明らかなように、規制はほとんどありません。広告ネットワークはその特性から、IPアドレス、ブラウザーのフィンガープリンティング、閲覧の傾向やログイン選択制の組み合わせによって、詳細なターゲットプロファイリングを提供します。標的を絞った攻撃者は、このような個人データを利用することで特定の標的の感染やペイロードへリダイレクトさせることができます。また、セキュリティリサーチャーの関心を引く付随的な感染とペイロードの継続的な利用回避もできます。このことから、高度なサイバースパイグループが、広告ネットワーク作成やそれを取り入れることは、わずかな投資で大きな利益が得られることだと理解し、自身の最新のツールキットを保護しつつ標的を攻撃するために利用すると考えられます。

私的制裁を加えるハッカーの増加

2015年に発生したHackingTeam社からの情報漏洩に続いて、実態の不明なPhineas Fisherによって、ハッカー志望者を対象とした不正な組織や疑わしい企業を攻撃するための手引きが発表されました。HackingTeam社から情報漏洩により活動中のAPTグループにゼロデイ攻撃のマルウェアが提供されたという事実にもかかわらず、このことは、私的制裁を加えるハッカーの善なる力だとする人々の意識に訴え、意欲的な新規顧客に対する激励にすらなっています。今回の選挙の展開においては陰謀説のレトリックの使用があちこちで見られました。このことは、データの流出や暴露は情報の不均衡を変えるための手段であるという考えに刺激されて、私的制裁を加えるハッカー分野への参入が増え、セキュリティ対策の不十分な組織に対してデータの暴露や組織的な情報流出を行う可能性があります。

株式会社カスペルスキー
PR-1029-201611