- NEWS RELEASE -

2015 年 1 月 30 日

超スパイウェア・プロジェクト「コブラ」の発見

――G DATA セキュリティラボによる分析結果――

株式会社グローバルワイズ

株式会社グローバルワイズ(本社：名古屋市中村区、代表取締役：伊原　栄一)は、パートナー企業である、ドイツのセキュリティソフト会社 G DATA Software AG（本社：ボーフム市、代表取締役：カイ・フィゲ他）のラボが、これまで発見された高度なスパイウェア「Agent.BTZ」「ウロボロス」「ComRAT」などが、いずれも共通の開発元（＝プロジェクト・コブラ）によって作成された可能性が高いという分析結果を出したことを、ここにお伝えします。

国家間サイバー攻撃に深くかかわるプロジェクト「コブラ」

2014 年 3 月、G DATA セキュリティラボは、「ウロボロス」という強力なスパイ機能をもったルートキットを発見したことを発表しました。その後この「ウロボロス」は、マルウェア「Agent.BTZ」と関係があるのではないかという見方がなされました。

「Agent.BTZ」は、最初に発見されたのは 2006 年ですが、2008 年秋に大きく話題になりました。スパイウェア「SillyFDC」の亜種で、コンピュータのデータをスキャンして外部と自由にやりとりのできるバックドアを開き、そこを通じて遠隔操作を行い、サーバーをコントロールし、データを送りだします。USB メモリを介して、アフリカ・中東地域を管轄するアメリカ中央軍基地のパソコンが感染し、最終的には、米国の中央司令部に置かれているラップトップコンピュータに侵入し、イラクやアフガニスタンにいる司令官が使う戦闘計画など、いくつかの機密情報が盗まれました。もちろん当時このことは極秘でしたが、2014 年になって

明らかにされました米国はこのワームを駆除すべく「バックショット・ヤンキー作戦」を敢行しますが、軍事ネットワーク全体が健常化するのに、およそ 14 カ月もの歳月を費やしました。その状況をふまえて米国は「サイバー軍」を開設しました。

また、2013 年に G DATA セキュリティラボはきわめて強力なルートキット「ウロボロス」を発見しました。これには、外部から情報を盗み出すスパイウェアが搭載されており、その挙動はすべて表には見えません。しかも、インターネットに接続されていないコンピュータも、間接的にネットワークを通じて感染可能という特徴をもっています。プログラム設計のデザインや複雑さから、これは、個々のネット犯罪者たちの仕業ではなく、「Agent.BTZ」をつくりだした組織のような、国家レベルの諜報機関によるものと推測されました。また、その後、2014 年 2 月にベルギーとフィンランドの外務省も「ウロボロス」によって機密情報が狙われました。

そして、2014 年 11 月には「Agent.BTZ」の亜種と思われるスパイウェア「ComRAT」が出現しました。「ComRAT」は、その名から分かるとおり、「Com」という、アプリケーションソフトウェアの開発を容易にするためにマクロソフトが用意した「コンポーネント・オブジェクト・モデル」の略称のとおり、マルウェア作成者はこの仕組みを悪用しユーザーやセキュリティソフトに気づかれないように活動できる隠れ場所をつくりだし、その結果、コンピュータを乗っ取り、一見ブラウザがデータをやりとりしているように見せかけて、実は、ネットワークの外部へとデータを盗みだすものです。また、後半の「RAT」は、サポートなど、外部からパソコンを操作するために用いられる「リモート管理ツール」の略称で、ハッカーはこの機能を悪用して外部からマルウェアを操作するのです。

「カーボン」の分析とプロジェクト「コブラ」

今回、G DATA セキュリティラボが特に解析を行ったのは、2009 年に作成された「カーボン・システム」(Carbon System)です。解析の結果、「カーボン」もまた、「Agent.BTZ」や「ウロボロス」「ComRAT」ときわめて類似した仕組みをもっており、技術的特徴として、暗号鍵、アルゴリズム、デザインなどに共通点がありました。また、時期としては「Agent.BTZ」の後に開発され、「ウロボロス」よりも前に開発されたものと推定されました。「カーボン」を分析することによって、プロジェクト「コブラ」とこれらのマルウェアとの関連性が見えてきました。

「カーボン」もまた、大規模ネットワークへの攻撃に利用されるための仕組みを備えています。モジュラー構造をもち、標的のシステムに合わせて内容を変えてマルウェアをダウンロードさせます。「カーボン」のなかで「コブラ」が果たす役割は、拡張可能なフレームワークと考えられます。このフレームワークは、たいていはダウンロードさせるか、偵察機能をもったマルウェア(＝「Tavdig」 別「Wipbot」(シマンテック)、「Epic Backdoor」(カスペルスキー))によってコンピュータに投げ込まれます。

利用の流れは、まず、PDF や Java の脆弱性を利用してコンピュータに偵察ツール(Wipbot/Tavdig)を

潜入させ、感染したシステムによって、攻撃者は、「カーボン」か「ウロボロス」か、いずれかを次のツールを投下します。

このマルウェアは、あえてプログラムの記述を細かく変え、マルウェアをさまざまなディレクトリに投下して、特定させないようにしているため、通常のソフトウェアでは検出できませんし、IOC（脅威指標）を使っても、うまく突き止められません。

ただし G DATA のセキュリティソフトの場合、このマルウェアは、以下の名称で検出されます。

エンジン A： Backdoor.TurlaCarbon.A
エンジン B： Win32.Trojan.Cobra.B

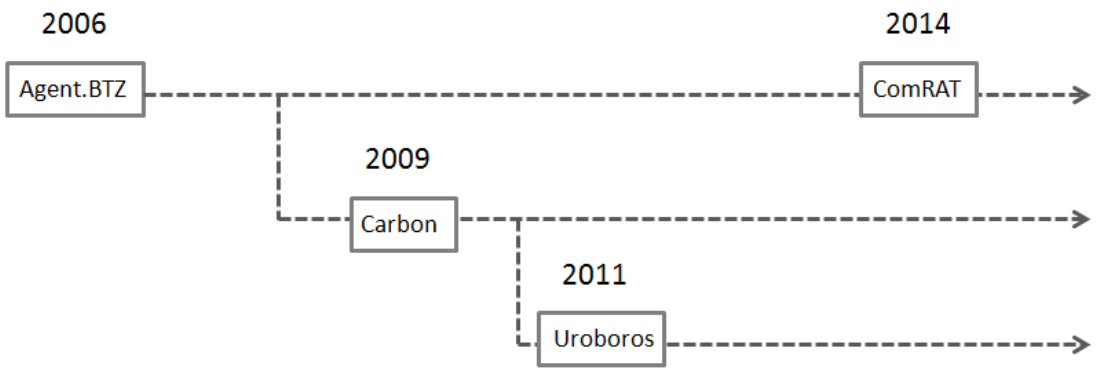
また、コンパイルのパスを次のように特定されます。

f:¥Workshop¥Projects¥cobra¥carbon_system¥x64¥Release¥carbon_system.pdb

このパスから、「カーボン」が「コブラ」の一部であることが容易に理解できるでしょう。

以上、「カーボン」の分析によって判明した、これらのマルウェアの系譜ですが、時間軸に並べると、次のようになります。

2006 年　Agent.BTZ
2009 年　Carbon
2011 年　Uroboros
2014 年　ComRAT （Agent.BTZ の直系の亜種）



プロジェクト「コブラ」の大きな特徴としては、新たなツールを開発すると、これまでのツールは一度使うのを止め、別系統のツールに移行しますが、しばらく時間が経過すると、かつての亜種が再び現れるということになりそうです。

現在、世界では、目に見える形でテロや人質による要求の提示や戦闘が行われていますが、同時に、サイバー空間においても、熾烈な戦いが続いています。日本語圏においても、決して他人事ではなく、サイバー攻撃を受ける可能性を常に自覚して、インターネットやコンピュータを利用しなければならない時代となりました。攻撃は官公庁だけとはかぎりませんので、みなさまにおかれましては、くれぐれもご注意ください。

＊さらに詳細な情報は、下記のリンク URL 先にあります（英文）。
https://blog.gdatasoftware.com/blog/article/analysis-of-project-cobra.html

ジーデータソフトウェアについて

G DATA Software は、1985 年に創業し、1987 年に世界初の個人向けウイルス対策ソフトを開発したドイツのセキュリティソフトウェア会社です。最大の特徴は、世界最高位のウイルス検出率。既知ウイルスはもちろんのこと、新種や未知ウイルスの防御、フィッシング対策、オンラインバンキング対策、スパム対策など、インターネットやメール環境を、安全・快適にする機能を豊富に搭載しています。現在は、Windows PC にかぎらず Mac や Android 端末向けのセキュリティソフトも開発しています。

■問い合わせ先
本公開内容に関するお問い合わせについては、下記までお願いします。

株式会社グローバルワイズ G DATA 公式ページ　http://gshop.g-wise.co.jp/
セキュリティソリューション推進室　浦瀬・山本
〒450-0003　名古屋市中村区名駅南 2-14-19　住友生命名古屋ビル 21F
TEL：052-581-2600　FAX ：052-533-3611
E-Mail pr_gdata@g-wise.co.jp