報道関係者各位

2015 年 9 月 29 日

サイバー攻撃が
ロシアの情報収集とつながる

（2015 年 9 月 17 日ヘルシンキ発 ― フィンランド本社発表資料抄訳）

エフセキュアラボが、ロシアが支援するハッカー集団による約 10 年の国家主体のサイバー攻撃のつながりを解明。

エフセキュアラボが発行した新しいレポートによると、国家主体のサイバー攻撃の多くが、ロシアの情報収集に関与するあるハッキング集団と関連しているとしています。ホワイトペーパーには、「デュークス」と呼ばれるハッキング集団について詳細な分析が記されており、米国、ヨーロッパおよびアジアの各国政府や関連団体に対する 7 年以上に及ぶ攻撃がまとめられています。

今回のレポートでは、他にないマルウェアのツールセット群を駆使し、コンピューターネットワークに侵入し、攻撃者にデータを返信する手口で情報を盗み出す攻撃者集団、「デュークス」について詳述が記されています。この集団は、先述のツールセットを使いサイバー攻撃を仕掛け、少なくとも 7 年以上、ロシアの情報収集を支援してきた、とレポートでは述べています。

レポートで取り上げられた攻撃の具体的な標的には、旧 NATO に関するジョージア情報センター（現、NATO および EU に関する情報センター）や、ジョージア防衛省、トルコおよびウガンダの外務省、その他、米国、ヨーロッパおよび中央アジアの政府機関や政治系シンクタンクなども含まれています。

今回の調査の責任者で、エフセキュアのリサーチャーである**アルツーリ・レティオ**は次のように述べています。

「新たな分析により、このグループがロシアの援助を受けており、ロシアの情報収集を支援するために活動しているという主張が強くなりました。今回の調査では、これらの攻撃で使われたマルウェアや戦術と、我々がロシアのリソースや利益になると理解している内容とのつながりを詳細にみています。こうしたつながりから、どこで攻撃が組織され、何を狙っていたのか、どのように実行されたのか、そして何が目的だったのかを示す証拠を導きだすことができました。そうして得られたすべてのサインが、ロシアによる国家的な支援を指し示すものでした。」

デュークは、9 つの異なるマルウェアのツールセットを使っており、研究者間でもそのうちの多くは把握されていたものの、レティオによる 2 つの新たな変異の発見のおかげで、研究者たちがこの集団と攻撃との間の新たなつながりを見いだすことができました。エストニアの防衛セキュリティ情報センターのジュニア・リサーチ・フェローである**パトリック・モールドレ**氏は、次の通り述べています。

「今回の発見は重要な情報で、この情報を使うことで、研究者やアナリストはいかにサイバー攻撃がロシアの情報収集や政治的目的のために利用されているかをより大きな絵として見ることができるようになります。レポートで特定されたつながりには、国際安全保障、特に北欧とコーカサス地域の

国にとっては重要な意味を持っています。ロシアが攻撃型のサイバー能力にどれだけ多くの投資をしてきたのかを示すもので、こうした能力が戦略的利益を前進させる上で重要な要素になったことも実証しています。ジョージア、ヨーロッパ、そして米国に対する 7 年に及ぶ個々の攻撃をつなぎ合わせ、既存の NATO 加盟国や将来の加盟国に対して、ロシアの情報戦争やスパイ活動、そして言い逃れなどの被害者にならないよう、サイバー空間での協力を強化し、集団的安全保障を高める 必要性を追認しています。」

フィンランド国際問題研究所のグローバル・セキュリティ・リサーチ・プログラムのディレクターを務める**ミカ・アールトラ**氏は、次のように述べています。

「この報告は、北欧諸国にとって特に重要な意味を持っています。スウェーデンやフィンランドといった小さな国は特に、こうしたスパイ活動に弱いのです。北欧およびバルト諸国は常に、ロシアと西側の利益の間でバランスを取ろうとしてきた中で、ロシアは自分たちに有利に働くよう、サイバー攻撃能力を活用しているのです。サイバー攻撃を仕掛けたと知られると批判の対象になるため、ロシアは自分たちの活動を否定しています。そして、自分たちの影響力をよりソフトに、より目に見えない形で及ぼそうとしているのです。」

マールドレ氏とアールトラ氏は現在、レティオ氏のデュークに関する調査を考慮した研究に取り組んでいます。レティオ氏による「デューク：ロシアのサイバースパイ活動の 7 年」と題したホワイトペーパーは、エフセキュアラボのサイトですでに提供しています。

詳細情報:

デュークのホワイトペーパー https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf
デュークの歴史 https://campaigns.f-secure.com/dukes-timeline/index.html
エフセキュアラボ https://www.f-secure.com/en/web/labs_global/home

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

F-Secure – Switch on freedom

エフセキュアは、25 年以上にわたり世界中の数千万人もの人々をオンラインの脅威から守ってきました。弊社の受賞歴のある製品は、クライムウェアから企業を標的としたサイバー攻撃に至るまで、あらゆる脅威から人々と企業を守っており、40 カ国を超える国々に広がる 6000 以上のリセラー、200 以上の通信事業者から購入することができます。弊社の使命は、人々が周りの世界と安全につながることができるように支援することです。この動きに参加し、自由のために闘いましょう。1988 年創業のエフセキュアは、NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2014 年 5 月に日本法人設立満 15 周年を迎えました。

会 社 名:	エフセキュア株式会社
カントリーマネージャ:	キース・マーティン
所 在 地:	〒102-0072 東京都千代田区飯田橋 3-11-14 GS 千代田ビル 5F
設　　立:	1999 年 5 月
事業内容:	セキュリティ関連製品・サービスの販売およびサポート

本件に関するお問合せ先
エフセキュア株式会社
マーケティング部
Tel: 03-3556-6301　Fax: 03-3556-6295
Email: japan@f-secure.co.jp
〒102-0072 東京都千代田区飯田橋 3-11-14　GS 千代田ビル 5F
URL: http://www.f-secure.com
Blog: http://blog.f-secure.jp