悪名高いマルウェアも存在：

在宅勤務用ネットワークの45%にマルウェア発見　テレワークはなぜ危険か

https://techtarget.itmedia.co.jp/tt/news/2005/30/news01.html

新型コロナウイルスの感染対策として在宅勤務が広がる中、在宅勤務用のネットワークをいかに安全にするかが重要になっている。だが現状はセキュリティが十分に確保されているとはいえないようだ。

2020年05月30日 08時30分 更新

[Arielle Waldman, **TechTarget**]

関連キーワード

ネットワーク・セキュリティ | 在宅勤務

セキュリティベンダーBitSight Technologies（以下、BitSight）が2020年3月に実施した調査で、企業の従業員が在宅勤務に使用するネットワークにマルウェアが存在する割合は、企業内のLANやWANといった企業内ネットワークと比べてはるかに高いことが分かった。同社はこの結果をまとめ、同社が同年4月にレポート「Identifying Unique Risks of Work from Home Remote Office Networks」（リモートオフィスネットワークを利用した在宅勤務固有のリスクの特定）として発表した。それによると、従業員が在宅勤務に使用するネットワークにマルウェアが見つかった企業の割合は全体の45.0%であるのに対し、企業内ネットワークにマルウェアが見つかった企業の割合は13.3%にとどまるという。

併せて読みたいお薦め記事

在宅勤務のネットワークトラブル

- 在宅勤務1割から9割へ急増のバイオ企業、悩みは「社員宅の無線LANトラブル」
- 「Zoom」がテレワーク需要で不具合　自宅の無線LANトラブルが原因の苦情も

在宅勤務のセキュリティ確保

- 新型コロナで広がる“私物端末で在宅勤務”に「ゼロトラスト」が必要な理由
- 「VPN」はなぜ昔も今もこの先も変わらずに必要なのか
- 「野放しのテレワーク」はNG　自然にセキュリティ意識が上がるルール作りのコツ

BitSightは4万1000社以上の企業の在宅勤務用ネットワークを調査した。同社の研究者はこの調査のために、各企業の従業員が利用する在宅勤務用ネットワークのIPアドレスを、その企業と対応付けた資産マップを作成した。「これはユニークな調査だ。われわれが一歩踏み込んでこうしたネットワークを取り上げ、それらのセキュリティ状況を比較して分析したのは今回が初めてだ」。レポートを作成したBitSightの研究者ダン・ダールバーグ氏はそう説明する。

調査では、在宅勤務用ネットワークにマルウェアが存在する割合は、企業内ネットワークの3.5倍であることが明らかになった。レポートによると、ランサムウェア（身代金要求型マルウェア）の感染手段として使われるマルウェア「TrickBot」が存在する割合は、少なくとも3.75倍であるという。加えてマルウェア「Mirai」が形成したbotネット（マルウェアに感染したデバイスが形成するネットワーク）が家庭用ネットワークで観察された頻度は、少なくとも20倍高かった。

なぜ在宅勤務用ネットワークにマルウェアがはびこるのか

Miraiのような、同一ネットワークにあるデバイスを侵害するワーム型マルウェアは「企業内ネットワークよりも在宅勤務用ネットワークに影響を与える」とダールバーグ氏は指摘する。多種多様なIoT（モノのインターネット）デバイスやスマート家電を攻撃の踏み台にするように作られているからだ。

BitSightの共同創設者でCTO（最高技術責任者）を務めるスティーブン・ボイヤー氏によると、Miraiがはびこっている理由は他にもある。ネットワークの10%は、管理用インタフェースが無防備な状態にあるためだという。「ほとんどのエンドユーザーは管理用インタフェースの設定を初期状態から変えておらず、Miraiはこうした設定値を悪用してネットワークに侵入する」とボイヤー氏は説明する。

テレワーク時の自宅LANを襲う脅威

テレワークは、新型コロナウイルス感染症（COVID-19）の世界的な流行以前から存在していた。ここにきて一気に大きく利用が広がったことで、新たなリスクが生まれているという。「これまでテレワークの経験がなかった人がテレワークをするようになったことで、攻撃対象領域が拡大している。しかもこの変化は急激だ」とボイヤー氏は語る。

テレワーカーの急増に伴う懸念点として、ボイヤー氏は以下を挙げる。

- 誰もが会社からデバイスを支給されているわけではなく、適切な保護や監視の下にあるデバイスを全員が使っているとは言えないこと
- 脆弱（ぜいじゃく）なネットワークに常時接続すること
- 専門のセキュリティ担当部門が管理していないこと

「テレワークの拡大は、ネットワークに関して言えばセキュリティレベルの低下を招く」とボイヤー氏は説明する。適切なセキュリティ対策が施された企業ネットワークから、保護が薄くセキュリティレベルが低い自宅LANへの移行を伴うからだ。

「ゼロトラストセキュリティ」の有用性

「既に『ゼロトラストセキュリティ』を採用している企業の方が、テレワークの拡大という新たな状況に対処しやすい」とダールバーグ氏は指摘する。ゼロトラストセキュリティとは、エンドユーザーが企業内ネットワークの中にいるか、外にいるかにかかわらず、必要に応じて認証を要求するセキュリティモデルだ。

「社内LANの信頼性に重きを置き、社内LAN用のデバイスを導入して運用する企業は、全てのデバイスが社内LAN外に存在するようになる新たな状況では苦労するだろう」とダールバーグ氏は語る。それらのデバイスは、社内LAN接続時と同じ保護を受けられない場合があるからだ。そうした理由から、安全なデバイス運用方法としてゼロトラストセキュリティの重要性が高まっている。ボイヤー氏は「ゼロトラストセキュリティは比較的初期の段階にある」と指摘。テレワークが拡大している最近の状況ではゼロトラストセキュリティが役に立つと考えられるが「実際に導入している企業はあまり多くないようだ」と同氏は述べる。

ボイヤー氏は「エンドユーザーが業務遂行のために本来インストールしてはいけないアプリケーションをインストールすると、それがセキュリティホールになる可能性がある」と注意を促す。そうした問題に対しては、適切なポリシーを定めることでセキュリティを保つことができる。これはデバイス自体の保護に加え、データにアクセスするためのネットワークのセキュリティ強化も実現する。「これにより、ネットワークが攻撃者による侵害を受けたり、マルウェアに感染したりしても、デバイス自体が侵害される可能性は低くなるだろう」とダールバーグ氏は説明する。

エンドユーザーの教育も大きな要素だ。ダールバーグ氏は「自分が置かれた新しい環境とそのリスクを理解できるようにエンドユーザーを教育すべきだ」と語る。教育の一環として、在宅勤務用ネットワークと自宅LANでどのデバイスが稼働しているかを、従業員が把握できるようにする必要がある。「こうしたデバイスの利用時には何をすべきかが分かるように、エンドユーザーの理解を深めなければいけない」と同氏は指摘する。例えばエンドユーザーは更新の適用を確認する画面で「後で実行する」をクリックした後、そのまま適用しないことがしばしばある。「このようなリスクの軽減策を実施すべきだ」（同氏）

ボイヤー氏によると、マルウェア全体のうち90%は、企業内ネットワーク以外のネットワークにある。「人々がテレワークのやり方を学び、より効率的に実施できるようになれば、このマルウェア分布は定着していくだろう」と同氏は見解を示す。「企業内ネットワークと在宅勤務用ネットワークのセキュリティ製品市場は異なっており、それぞれ異なる製品が提供されてきた。今後はその違いを埋めていく必要がある」とボイヤー氏は述べる。

TechTarget発　先取りITトレンド

米国TechTargetの豊富な記事の中から、最新技術解説や注目分野の製品比較、海外企業のIT製品導入事例などを厳選してお届けします。