本レポートの要点

2022年第3四半期にマルウェアとネットワークのどちらの攻撃も再び減少し、この数年になかったトレンドが続くことになりました。四半期ごとにどちらかが増加したり減少したりすることはあったものの、両方の減少がこれほど続いたことはありません。3四半期連続の減少は防御側にとって喜ばしいことですが、過去の数字からは予想できなかったことです。しかしながら、誰もが安心できるわけではありません。表面的な脅威の件数は減少しましたが、その巧妙さと潜在的な影響が増大していることを示す、表面には現れにくいトレンドが隠れています。そして、この後すぐに紹介するように、この件数の減少には誤解を招きかねない理由もあるのです。

例えば、ほとんどのマルウェアが暗号化された接続経由で到着していることが引き続き確認されています。Fireboxユーザの5分の4がそうであるように、ほとんどの防御者が暗号化されたトラフィックをスキャンしていないことを攻撃者が知っていれば、大量に仕掛けることなく攻撃を成功させることができます。この事実を考慮すると、回避型のマルウェア、つまりゼロデイマルウェアの件数は減少したものの、50%がかなり大きな数字であることがわかります。

このようなマルウェアの高度化が、上位の亜種の分析でも確認されました。例えば、我々は第3四半期に、国家（政府）が支援する犯罪者と強い関連性がある最初の脅威を確認しました。これまでに断言できなかったのは、政府が支援する可能性のある脅威を何の後ろ盾もない犯罪者も利用している可能性があったためです。しかしながら、この四半期に最も拡散した脅威の1つが中国政府と関連性のある脅威集団だけに帰属するものであることがわかりました。

最後に、マルウェアの数が少ないように見える理由の仮説となるような、予備的な知見が見つかりました。実際には、既存のデータが示すよりはるかに多い可能性があり、問題は、最新のマルウェアの捕捉に必要とされる、Fireboxの無料でより高度な機能の利用者が少ないことなのかもしれません。この点については本レポートで詳しく説明しますが、暗号化されたWebトラフィックをスキャンするようにFireboxが構成されている場合、ほとんどのマルウェア（80%以上）が暗号化された接続経由で到達することがわかっています。ところが、暗号化されたトラフィックをスキャンするように構成されているのは、レポート対象のFireboxの約20%に過ぎません。前述のとおり、サイバー犯罪者は、多くの防御側がそのようなトラフィックをスキャンしないことを知っているため、暗号化されたネットワークを利用するなどの高度で回避型の戦術に移行するようになっています。つまり、FireboxのオーナがTLS/SSLインスペクション（Fireboxで無料で利用できる機能）の構成を開始しない限り、このようなマルウェアを目にする機会がどんどん少なくなるということです。残念ながら、この暗号化されたトラフィックがマルウェアの本当の数をわからなくしているだけでなく、暗号化を解除していない防御側はマルウェアをブロックする機会を失い、他のエンドポイントベースの保護を採用していなければ、マルウェアを受け取ってしまう可能性があるということです。すなわち、マルウェアの数は、現在得られているデータから推測されるよりはるかに多い可能性があり、レポート対象のFireboxの80%のオーナは、本レポートの精度の向上だけではなく、自らを保護するために、HTTPSインスペクションを有効にする必要があるということです。

総論とすれば、脅威の数の減少は興味深いことではあるものの、防衛側にとって悪いニュースではありません。しかしながら、これも完全に正しいと断言できるものではなく、ユーザの構成が今日の暗号化の時代に追いついていないだけなのかもしれません。いずれにしても、安易に安心するべきではありません。それは、今も多くの危険な脅威が数多く存在し、我々が確認した脅威は成熟度の低い防御を突破できるからです。