主役登場

未知なるリスクを排除せよ

岩村　誠
NTTセキュアプラットフォーム研究所
特別研究員

前回，この主役登場へ寄稿させていただいたのは2010年，あれから11年が経ちました．残念ながらサイバー攻撃やマルウェア（悪性ソフトウェア）の高度化はとどまることを知らず，未然に侵入を防ぐことは困難になってきています．こうしたマルウェアの侵入を前提とした状況を踏まえ，私たちはマルウェアの振る舞いやそれらが残す痕跡をIoC（Indicator of Compromise）として抽出，IoCを基にマルウェアの振る舞いを早期に発見する技術の研究開発に取り組んでいます．さらなるサイバー攻撃の激化に対抗するべく，今後もマルウェアの早期発見，対策といった取り組みは継続していくことが肝要です．

ところで，こうしたマルウェアにそもそも感染しないようにするにはどうすれば良いのでしょうか？　マルウェアに感染する大きな原因の１つにソフトウェアの脆弱性があります．これまで脆弱性対策は，利用しているソフトウェアの最新化で対応してきました．しかし脆弱性についても2010年以降，憂慮すべきケースが増えてきています．2010年に出現したStuxnetは，４つの未知の脆弱性を組み合わせて感染を広げました．また2017年に出現したWannaCryは，同年に修正された脆弱性を悪用していましたが，その脆弱性を悪用するモジュールはWnnaCry出現の５年以上前にすでに存在していたとの報告があります．そう，今ではソフトウェアの最新化は脆弱性対策の銀の弾丸ではなくなってしまったのです．最新版のソフトウェアであっても修正されていない脆弱性は，ゼロデイ脆弱性と呼ばれています．未修正である理由はさまざまですが，私が過去に発見したものにも多くのゼロデイ脆弱性があります．一例として，2006年に発見したWinnyというソフトウェアの脆弱性（CVE-2010-2360）をみてみましょう．当時からこのソフトウェアの修正は社会的に困難な状況にあり，今後も修正されることはないでしょう．私たちとしては修正不能な脆弱性は公にできないという立場から公開を控えましたが，2010年に海外のセキュリティ研究者がこの脆弱性を発見，警鐘を鳴らすべく公表したことにより，その存在が明らかにされました．未修正の脆弱性の公開を控えた私たちの判断が正しかったのか，発表に踏み切る行為が正しかったのか，今でも自分の中で答えは出ていません．ただいえるのは，ゼロデイ脆弱性というのは身近に数多く存在し，それらはいつ悪用されてもおかしくない状態にあるということです．今後はソフトウェアの最新化はもちろん，攻撃者に悪用される前に脆弱性を発見し，対処することが重要になっていくでしょう．私たちとしても引き続き，脆弱性発見や脅威実証の取り組みを推し進め，未知のリスクの排除に取り組んでいきます．そして，脆弱性発生や攻撃のメカニズムの体系化を進め，脆弱性が生まれることのないICTシステムの実現に邁進していく所存です．その実現の暁には，サイバーセキュリティの研究者がこの“主役登場”に現れることもなくなっているでしょう．