ランサムウェアのその後

ランサムウェアの脅威

- ワーム型マルウェア
- 脆弱性のある PC を狙う
- ファイルを暗号化して身代金を要求

- 要求金額が高騰
- ばらまき型から標的型へ
- 企業や自治体がターゲット
- 亜種が生成されている
- IoT 機器もターゲット
- 愉快犯から金儲けビジネスへ

2017 年に 5 月に日本を含め世界 150 か国 23 万台以上のコンピュータに感染した WannaCry（ワナクライ）によって、一般の人々にまで知れ渡った「ランサムウェア」はその後どうなったのでしょうか？
ランサムウェアにもいろいろな種類がありますが、たとえば典型的な WannaCry は Windows の脆弱性を利用して、セキュリティパッチが適用されていなかったコンピュータに感染し暗号化した後、身代金として 300 ドル、その後 600 ドル相当のビットコインを 1 週間以内に振り込むようホップアップが出るワーム型のマルウェアです。
ビットコインを送金しても、暗号化が解除されない悪質なものでしたが、その後、セキュリティツールや OS アップデートの重要性が認識され、攻撃そのものは増えているようですが、実際の被害は激減しました。しかしながら、未だ 100 万台以上のコンピュータに該当する脆弱性があるといわれており、完全になくなったわけではありません。
2017 年末辺りから、ビットコインの高騰によって、身代金要求よりも、仮想通貨マイニングをさせるコインマイナーなどのマルウェアの方が、多くのメディアを賑わすようになりましたが、2018 年春以降仮想通貨が暴落し、仮想通貨のマイニングでは儲からなくなったせいなのか、高額な身代金を要求するランサムウェアがニュースになるようになりました。
以前は、数万円の要求でばらまき型で思えたランサムウェアですが、あきらかに特定企業や団体にターゲットにして高額な要求をする標的型の攻撃が増えているようです。
たとえば、2019 年以降アメリカでは自治体を狙った攻撃が相次ぎ、5 月に発生したメリーランド州ボルチモア市の事例では、「RobbinHood」というランサムウェアが役所のコンピュータに感染し、800 万円以上に相当するビットコインを要求され、サーバの大部分をシャットダウンされる事態となり、ほとんどの部署が影響を受けました。6 月のフロリダ州レイクシティ市の事例では、人口 1 万 2000 人ほどの小さな町ですが、ランサムウェア「Ryuk」によって行政システムの全ファイルが暗号化され、ほぼ全システムを掌握されてしまい、仕方なく 5400 万円相当の身代金が支払われて、暗号解読のキーを取得しました。8 月には、テキサス州も 20 以上の自治体が攻撃にあっています。
愉快犯のイメージが強かったランサムウェアですが、完全にお金儲けの道具として使用されてきているようです。
またまだ、衰えを見せないランサムウェアに対し、私たちは継続したセキュリティ対策が必要です。