2017 年 1 月 20 日
株式会社セキュアソフト

サイバーセキュリティ 2016 年振返りと 2017 年予測

セキュアソフト　脅威分析チームによる 2017 年の予測についてレポートいたします。

1.　2016 年のサイバーセキュリティの振返りトピックス『ランサムウェアと DDoS 攻撃が猛威を振る』

2016 年のサイバーセキュリティのトレンドとしては「ランサムウェア被害の急増」や「IoT デバイスを悪用した DDoS 攻撃」の 2 大トピックスがありました。一般のメディアでも数多く取り上げられました。こうしたサイバー攻撃の脅威に注目が集まったこともあり、各企業や団体ではセキュリティ製品の導入やクラウドサービスへの移行が進んでいます。企業や団体の IT システムは対策にともなう更新や運用方法の変更を伴い、運用者の大きな負担や課題となっています。

1.1　ランサムウェアの傾向

・巧妙化する標的型メール

国内で発生したセキュリティインシデントでは、ドメインの詐称や、悪性サイトへの誘導や添付ファイル（マルウェア）を開くよう誘導する文書がとても洗練され巧妙化しています。標的型メールはランサムウェアが猛威を振るう原因になっています。

図 1 [宅配業者を騙った巧妙な標的型メールの例]

・RaaS(Ransomware-as-a-Service)の拡大

RaaS(Ransomware-as-a-Service)というランサムウェアをサービスとして販売する業者が出てきています。RaaS を利用することで高度な技術がなくても攻撃が出来るため攻撃者が急増しています。

・機密情報を人質にした脅迫

従来のランサムウェアではデータを暗号化し復号のための身代金の要求だけでしたが、最近では身代金の要求とともに身代金を支払わない場合は機密情報を削除、または公開するといった脅迫が行われています。

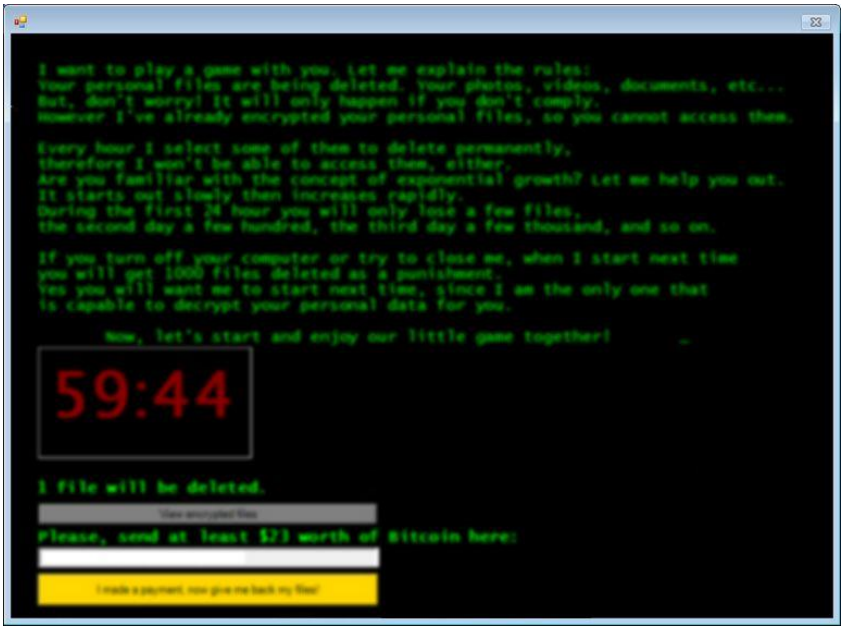

図 2 [ランサムウェアの脅迫画面例]

1.2 DDoS 攻撃の傾向

・IoT デバイスを悪用するマルウェアのソースが公開

IoT デバイスを悪用して構築したボットネットを利用することで DDoS 攻撃を行うマルウェアのソースコードが公開されため、マルウェアを悪用する攻撃者が増加しました。

図 3 [IoT デバイスを悪用した DDoS 攻撃に関する検索結果(Google)]

・IoT デバイスの急増

IoT 時代到来で様々なモノがインターネットに繋がるようになりましたが数多くの製品で脆弱性が内在していたため、マルウェアによる攻撃の踏み台となる傾向が顕著化しました。その結果、大規模 DDoS 攻撃に悪用される等の問題が発生しています。

2. 2017 年の予測 『2016 年に続き脅威が増加』

2017 年もランサムウェアや DDoS 攻撃が猛威を振るうことが予測されます。セキュアソフトではランサムウェア対策に SecureSoft コンテナシリーズ、DDoS 対策に SecureSoft Sniper ONE といったソリューションを提供いたしておりますので、是非ご活用ください。また、被害に遭った場合は今後の対策や被害の算出が必要です。調査部門は感染ルートの特定やマルウェアの活動を解析するために有用なログが必要になります。しかし、"ログを取得していない"または"ログは取得しているが有用な状態ではない"といったケースが多くみられます。今後のセキュリティ対策では被害を出さないための対策とともに、被害発生後の対応を一層強化する取組みが必要となるでしょう。

以上

«SecureSoft 推奨ソリューション一覧»

■SecreSoft Sniper ONE 『多層防御型 DDoS 対策』
https://www.securesoft.co.jp/products/one/outline/

■SecureSoft S-コンテナ 『情報漏洩防止+内部統制』
https://www.securesoft.co.jp/products/s-container/outline/

■SecureSoft i-コンテナ 『マルウェア対策+内部統制』
https://www.securesoft.co.jp/products/i-container/outline/

■SecureSoft mamoret 『お手軽マルウェア対策』
https://www.securesoft.co.jp/products/mamoret/

«お問合せ先»

株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp