資料27－２

VPN脆弱性とマルウェアの直近の状況

株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp

VPN 機器の脆弱性を悪用したサイバー攻撃

VPN 機器の脆弱性を悪用したサイバー攻撃 ～ ソフトウェア更新の徹底と多要素認証の活用を
約 53 %の企業や組織が「新型コロナウイルス感染拡大を機に」テレワークを実施
https://www.cybertrust.co.jp/blog/certificate-authority/client-authentication/vpn-multi-factor-authentication.html

2020年09月08日　テクニカルレポート
VPN機器を狙ったサイバー攻撃が継続中！セキュリティ事故を防ぐ3つのポイントとは
https://www.lac.co.jp/lacwatch/report/20200908_002277.html

Pulse Secureの「情報漏えいの脆弱性（CVE-2019-11510）」
「コマンドインジェクションの脆弱性（CVE-2019-11539）」などは、実証コードを含む情報が公開

SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/

リモートワーク時代の脅威の一つのトレンドに?

- 大きくICT環境が変化する中、脅威の新たなトレンドとなり得るのでは。
  - 内部ネットワークにアクセスする手法 - マルウェアに加えてVPN

- NOTICEに、VPNの脆弱性スキャンも加えてはどうか。
  - 今後も同様の事象は発生する可能性がある。しかも極めて深刻な事象になる可能性もある。
  - VPNサービスのDBがあればスキャンを待たずとも通知可能では(固定IPが多い)。
  - 本来は各企業の責任で対応すべき所。
  - 大規模なインシデントとなり得るケースにおいては関与する(?)
  - NOTICEの趣旨・目的そのもののあり方の議論も必要

一般企業を狙うマルウェアの直近の状況

- 最近、企業はEmotetなど各種マルウェアへの対応に相当神経質に。
  中小零細も問い合わせが急増。

- 「感染しているかもしれないので確認したい」
  「もし感染した場合、どのような事が起きるのかを整理している。そのうえで、事前に取れる対策を検討している」
  「不安なので情報がほしい」
  「感染した取引先からメールがあちこちに送られているのを何とかしたい」
  ・・・etc

  特に中堅中小からの問い合わせが多い。
  あまり今まで見られなかった傾向。Wanna Cry発生時よりも問い合わせは圧倒的に多い。

- 事例 (Emotet)

  取引先が感染。メールが送られてきて感染。
  - GWでのマルウェア対策をバイパス
  - 返信を装った普通のメール
  - アンチウィルスも効かず感染

- 一般的な感染後の対応

  感染端末をリカバリーして対策製品を買って終わり。
  それ以上の調査等はしていない(出来ない)ケースが多い。

- 暴露系ランサムウェアは今後も増えていくのでは。
  - 攻撃プロセスの自動化が進み、小規模事業者に被害が拡大？

- リモートワーク時代においては、一層ユーザーのサイバーセキュリティに関するリテラシー向上が重要。広く情報発信できる仕組みが必要。