セキュリティレポート

2023.9

YOU DESERVE THE BEST SECURITY

最新マルウェアランキング

国内で活発な上位のマルウェアファミリー

8月の国内ランキングでは、7月に3位だったNanoCoreが2.08%の国内組織へ影響を及ぼし、1位へ順位をあげました。5月に続きQbotが国内組織の3.80%に影響を及ぼし首位に立ちました。2位にはRemcos（2.97%）、そしてグローバルランキングでも首位にあるFormbook（1.98%）が続く結果となりました。

NanoCoreの主な特徴

Nanocoreは、Windows OSユーザーを標的とするリモートアクセス型トロイの木馬（RAT）で、2013年に初めて流行が観測されました。そのすべてのバージョンで、画面キャプチャ、暗号通貨マイニング、デスクトップの遠隔操作、Webカメラセッションの窃取といった基本的なプラグインと機能性を備えています。

順位	呼称
1位	**NanoCore**
2位	**Remcos**
3位	**Formbook**

Webカメラセッションの窃取

監視カメラ・WEBカメラが乗っ取られ、遠隔操作や盗撮に使われる

脆弱性攻撃

脆弱性攻撃は、Webカメラを乗っ取り、プライバシーを侵害する方法の1つで、いかなるソフトウェアも、人が開発している以上不具合が起こり得ます。不具合によっては、攻撃者に悪用され遠隔からデバイスへ不正侵入される恐れがあります。

リモートアクセス型トロイの木馬（RATs）

標的のコンピューターやデバイスを遠隔で制御する、特別な種類のマルウェア。遠隔操作によって、ライトを点灯させることなくカメラを起動し、撮影した動画ファイルを攻撃者自身へ転送できます。このソフトウェアを使えば、キーボード入力を不正に記録し、パスワードや銀行口座の情報などを盗むことも可能となります。ほかのマルウェアと同様、**リモートアクセス型トロイの木馬**は以下のような方法で感染します。

- **フィッシングメールに添付されたリンクやファイル**
- **メッセージングアプリやソーシャルメディアのリンク**
- **正規に見せかけた悪意のあるモバイルアプリ**

CHECK POINT

Insecam

WEBカメラにおける被害のひとつとして有名なものがこの『Insecam』

2016年1月に始まったロシアのウェブサイトで、世界中の監視カメラの映像が誰でも自由に覗き見できる。

世界120か国の監視カメラの映像をリアルタイムで配信されていて、日本でも6,000台を超えるカメラが対象となっています。

流出した理由としては、カメラの購入時に初期パスワードのままだったため、簡単に見破られているケースが多く、監視カメラの製造メーカーまで分かるようになっています。

http://www.insecam.org/en/bycountry/JP/

ハッキングされていることを確認する方法

- カメラの状態表示ランプ（インジケーター）が点灯する
- パソコン内に見覚えのないファイルが保存されている
- 見覚えのないアプリがインストールされている
- 設定が変更されている

ハッキングを防ぐために

- あらゆるデバイスのアップデートを怠らない
- パスワードの定期的な変更且つ複雑でユニークなパスワードで設定
- 二要素認証がある場合は必ず設定する
- 万一の場合、カメラのレンズを覆う
- フィッシング対策しっかりと実施する

CHECK POINT

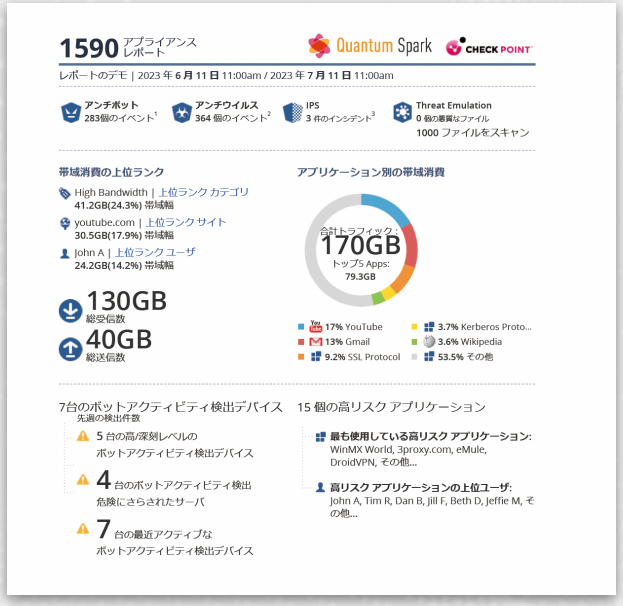
大企業向けに開発した最高レベルセキュリティ機能を中小企業へ

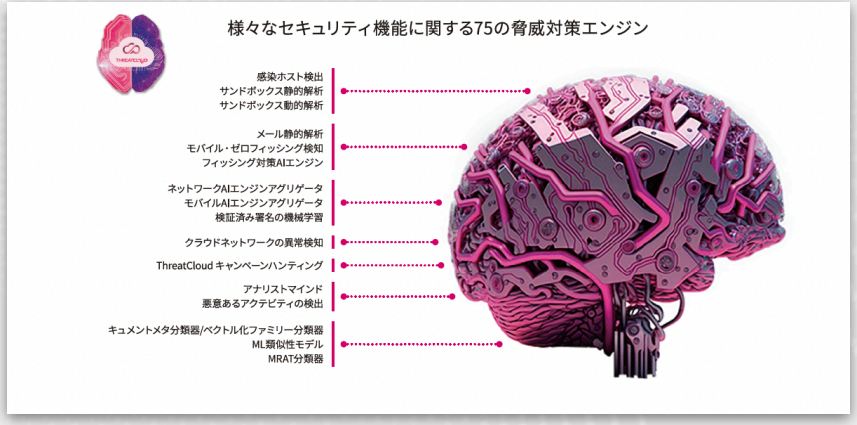
最先端の最高レベルセキュリティが１台で実現できるから
コストを抑えたトータル・セキュリティ・ソリューションが可能です

中小企業向けUTM

インターネット上に存在する様々脅威に対し、多段階の防御策を実現することができるネットワーク製品です。
社内ネットワークの手前で遮断することにより、安全なネットワーク環境でご利用いただけます。

Quantum spark





レポートも見やすく運用も容易！

導入から運用まで、システム担当者がいない中小企業様でも安心して管理・運用が可能な総合脅威対策機器です。

デジタルカタログは
https://cp-smb.com/catalog/

CHECK POINT