サイバーセキュリティ最前線

FSCE による抜本 する EMOTE

|別種のマルウェアをインターネット経由でダウンロードさせたり、1般的なウイルス対策ソフトで検知しづらくしたりする 機能を持つ「EMOTET(エモテット)」というマルウェアが、国内外で猛威を振るっている。そこで、今号では その最新動向とともに抜本的な対策につながる「HP SCE(旧Bromium)」について紹介したい。

サイバーセキュリティ業界 イタチこっこがつづく

П

ポール

最

7

jν

ウェ

ドレスが2万6000件ほど情 テットに感染した機器のIPア 用者への注意喚起をはじめるこ テットに感染したパソコンの利 月19日、警察庁と総務省はエモ り沙汰されている。 は2月下旬からこれらの情報を 報提供され、警察庁と総務省で の捜査当局より日本国内でエモ とを発表。それによると、 するように指導するそうだ。 特定して注意喚起を行い、感染 とに。ISPは機器の利用者を インターネットサービスプロバ イダー(ISP) に提供するこ に関して、さまざまな動きが取 した機器からエモテットを駆除 EMOTET(エモテット) 先 端 0) たとえば2

て「ハッキングに使われるツー ごっこがつづいており、脅威が ている株ブロード(東京都千代 キュリティシステムの提案をし うわけにはいかない。長年、セ のだ。しかし、これで安心とい が8カ国の治安当局などとの合 報じられたエモテットも特定の で流通・売買されており、今回 ムは、悪意を持つ行為者らの間 な脅威があらわれる」と。そし ひとつ摘まれてもすぐにあらた ュリティ業界ではつねにイタチ 田区)によると「サイバーセキ 摘発することに成功したという ットのコントロールサーバーを 同捜査を実施した結果、 グループのものとはかぎらない」 やマルウェアなどのプログラ エモテ

アの多くはメールやウェブサイ トを使用した手口で拡散されて そもそも、こうしたマルウェ

報道があった。1月27日にユー

他方、海外ではつぎのような

(欧州刑事警察機構) 判断ができるわけではないので 社員一人ひとりがつねに正しい だが、「これまでにこの訓練で ち検査などを行っているという。 キュリティの啓発活動の一環と えで、もっとも一般的に解放さ いく。 すべきではないか」とブロード より抜本的な課題解決法を模索 れている経路だからだ。そこで ク内にマルウェアを送り込むう は指摘する。 にしたことはない。もっとも して「標的型攻撃訓練」を実施 100点を取れたという話を耳 部の大手企業などではITセ

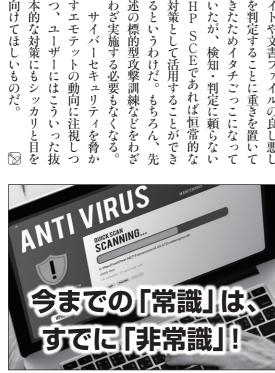
抜本的な対策の手段として (旧Bromium) 」を導入 HP SCE

その候補としてあげられるのが な対策となり得るのだろうか。 では、 いかなる手段が抜本的

向けてほしいものだ。

偽装メールを使った抜き打 企業や組織のネットワー 述の標的型攻撃訓練などをわざ 対策として活用することができ きたためイタチごっこになって セキュリティツールはウェブサ 隔離された仮想環境でウェブサ 製品であれば、「PC本体から わざ実施する必要もなくなる。 るというわけだ。もちろん、先 いたが、検知・判定に頼らない を判定することに重きを置いて ことができる」という。従来の かかわらず『すべてを隔離する ルの口上やマルウェアの種類に 全に開けるため、引っ掛けメー 活用だ。仮想技術を用いたこの HP SCEであれば恒常的な イトや文書ファイルの良し悪し イトの閲覧や文書ファイルを安 HP SCE(田Bromium)」

すエモテットの動向に注視しつ サイバーセキュリティを脅か ユーザーにはこういった抜



と費用は「()」にしましょう



る費用や専門家は、もう必要ありません。

※2013 年以降、Bromium は推計 20 億以上の MicroVM が実行されましたが、侵害報告件数はゼロです。(Bromium 社調べ)

詳細は[BROAD Security Square]で… https://bs-square.jp/columbus

株式会社ブロ

〒100-0014 東京都千代田区永田町1-11-30 サウスヒル永田町7F TEL: 03-6205-7463 (代表)

