PC Matic マルウェア報告書(サンプル)

マルウェア情報	脅威度(1～5)	脅威レベル 3 (中)
	マルウェア呼称	Win32.Floxif.A
	MD5	0x329FDA280142430AFB7D15B0E710218B
	侵入日時	2021年3月12日 12:31 JST(3/21 0:31 UTC)
	活動開始	2021年3月12日 12:42 JST(3/21 0:42 UTC)
	悪意行動開始	悪意活動なし
端末情報	顧客名	ABC SEA LINE SERVICE Inc, (Panama)
	端末ID	5195347
	端末名	Bridge-PC
	端末MAC	08:9E:01:C9:98:2A
	端末メーカ	DELL Inspiron 5100
	OS	■Windows 7 SP1 □macOS □Linux □iOS,iPadOS
	CPU	Intel Core i3-4158U
	RAM	8GB
マルウェア概要	種類	□一般ウイルス □ワーム □トロイの木馬 □キーロガー □バックドア □ルートキット ■ダウンローダー □ボット □ランサムウェア □スパイウェア □詐欺ウェア □金融マルウェア □アドウェア
	概要	暗号化マルウェアをC2サーバからダウンロードする機能をもつ
対応	PC Matic対応策	SuperShield 3.0.36.0にて対応予定

マルウェア挙動詳細

●パソコン内の各ルートディレクトリに、ショートカットと実行ファイル、各1つを自己複写。レジストリへ自動起動を登録。各ファイルは、削除キーにて削除可能。

●他パソコンへの感染、ファイル送信、暗号化などの機能を持たない。

●ブラウザーでの入力をC&Cサーバを通じて送信を試みる。
※既知C&CサーバであるためPC Matic EDRにて通信遮断確認

●パソコン再起動後は、SuperShield保護にて起動阻止