We Are Garfield（WAG）は、急速に台頭している高度な持続的脅威（APT）グループであり、特に金融、医療、製造業などの業界を標的としています。彼らの活動は通常、フィッシング攻撃、クレデンシャルスタッフィング、または公開システムの脆弱性を悪用することで初期アクセスを取得することから始まります。侵入後は、WAGは徹底的な調査活動を行い、価値の高い標的を特定します。主な目的は、機密データの窃取と抽出、そしてランサムウェア攻撃の実行です。
WAGの活動における特徴的な点の一つは、月曜日に活動が著しく減少することです。

脅威ハントの過程で、環境内で 2 つの侵害されたシステムを特定しました。
WK3
DB01

タイムライン

| **タイムスタンプ** | **観察** | **影響を受ける資産** |
|---|---|---|
| 7/24/24 2:00:13.000 PM | n.harrisがsecurity_update.exeをダウンロード、実行 | WK3 |
| 7/24/24 6:13:13.000 PM | n.harrisがtickets.exeをダウンロード | WK3 |
| 7/25/24 12:49:26.000 PM | New AccountとしてhelpdeskI_1を作成 | DB01 |
| 7/26/24 9:51:17.000 AM | garfield-apt2 から、DB1 に対して helpdesk_1 でログオン | DB01 |
| 7/26/24 10:39:34.000 AM | EventCode=11でdb_exfil.exeが作成 | DB01 |
| 6/24/25 10:40:07:000 AM | db_exfil.exeがEventCode=1で実行 | DB01 |

IOCs

添付は、脅威ハンティングスプリント中に検出された結果のIOCのまとめリストです。

### ファイルハッシュ

| **ファイル名** | **SHA256** |
|---|---|
| security_update.exe | 55773552DEC6ED7B5083BDCE3EBBBC85AAA6915B140E11003F551 |
| tickets.exe | 27AB9570AF93CA2C53169762C9FBFDFE5C1DBE62E1E9397561F4E |

| ファイル名 | SHA256 |
| --- | --- |
| db_exfil.exe | 44601FD7EDBCE9C68E5979D92D162A886FD005862E0587BA8A926 |

### ネットワーク通信

| 種類 | 価値 |
| --- | --- |
| C&C | 10.25.26.50 |
| ファイルダウンロード | security_update.exe |
| ファイルダウンロード | tickets.exe |