1. 攻撃者は1台以上の外部マシンを悪意のある目的で使用しました。攻撃者がこれらのマシンに使用したホスト名またはDNS名は何ですか？
garfield-apt2
4df21cd23074fa076764e73ae8c74a07

2. 攻撃者がネットワーク内での横方向の移動を可能にする情報を収集するために使用したスクリプト、アプリケーション、またはコマンドレットの SHA-256 ハッシュは何ですか?
tickets.exe
27AB9570AF93CA2C53169762C9FBFDFE5C1DBE62E1E9397561F4E91232EBAC41
c94fe3ab3909af1d4f0ef057958a0215

3. 攻撃者は機密情報の流出や暗号化を行うことで知られています。これらの流出やランサムウェア活動に使用されたスクリプト、アプリケーション、またはコマンドレットのSHA-256ハッシュ値は何ですか？
db_exfil.exe
44601FD7EDBCE9C68E5979D92D162A886FD005862E0587BA8A926CCD37BDA7FC
940af9d40d95c1f9444063fa4a8d28af

4. データの流出やランサムウェア活動に関連する最新のイベントのタイムスタンプは何ですか?
7/26/24 10:48:34.000 AM
f92e238c2cec1d7dd18b24d7c8e118d1

5. 攻撃者は、権限昇格や横展開といった特定のアクションの後に、様々な永続化メカニズムを利用することで知られています。Megacorp One環境で利用されている永続化メカニズムとして使用されているオブジェクトの名前は何ですか？オブジェクトとは、ファイル名、レジストリキー、ユーザー名、スケジュールされたタスク名などです。（形式：パス、ドメイン名、コンピューター名、デバイス文字などのプレフィックスやサフィックスを含まない ObjectName）
helpdesk_1
90b380edb07c238f838c7c26391908e6

6. 攻撃者が Megacorp One 環境への初期アクセスを取得するために使用した実行可能ペイロードの SHA-256 ハッシュは何ですか?
security_update.exe
55773552DEC6ED7B5083BDCE3EBBBC85AAA6915B140E11003F5513AF6ABDAFED
8c4b9a113ff13e61415f21ce900be266

7. 攻撃者がMegacorp One環境に最初にアクセスした実行可能ペイロードはいつ実行されましたか？タイムスタンプを入力してください。

7/24/24 2:00:13.000 PM
7e07133a672240ec965eba9727f78f2b