NightSpecterは、バイオテクノロジー、通信、金融といった高付加価値産業を標的に、巧妙化を続けている秘密裏に活動するAPT（Advanced Persistent Threat）グループです。
このグループは、欺瞞的なフィッシングペイロード、認証情報の窃取、パッチ未適用の公開インフラの悪用などを組み合わせて侵入を開始します。
アクセスに成功すると、脅威アクターは独自のツールキットを展開し、ノイズの少ない内部偵察を実施します。これには、体系的なネットワーク列挙、権限昇格、機密データリポジトリまたは運用制御システムの特定が含まれます。
NightSpecterのキャンペーンは、主に機密の研究開発資産、機密通信、技術設計図の窃取を目的としています。窃取されたデータは、計画的なリークによって武器化されるか、恐喝に利用されます。これは、長期的な情報収集と短期的な金銭的利益という、このグループの二重の戦略的目的を示しています。
NightSpecterは、正規のシステムプロセスを模倣し、日常的な管理トラフィックに紛れ込む「living-off-the-land」（LOLBin）バイナリを活用することで、自身の活動を難読化します。この戦術は、動作分析とエンドポイント検出を著しく複雑にし、監視環境内で従来のセキュリティ管理とフォレンジック調査を意図的に回避しようとしていることを示唆しています。

脅威ハントの過程で、環境内で3つの侵害されたシステムを特定しました。

- WEB01
- DB01
- HRIS

タイムライン

タイムスタンプ	**観察**	**影響を受ける資産**
6/23/25 10:07:11.000 AM	WebShell（ws.phtml）を通じて `whoami` コマンドを実行を確認。 uploads → ファイルアップロード機能経由で置かれた可能性が高い。 ここでws.phtmlが最初にアクセスしたファイルと判断。	WEB01
6/23/25 11:44:19.354 AM	Web サーバ侵害後に、権限昇格調査ツール（linPEAS）を外部からダウンロードしている	WEB01
6/23/25 11:44:34.013 AM	linpeas.sh に実行権限を付与しているのを確認。	WEB01
6/24/25 6:37:52.000 AM	外部HTTP サーバからSharPersist.exe をダウンロードし、net.exeとして保存	DC01

タイムスタンプ	観察	影響を受ける資産
6/24/25 6:45:59:000 AM	外部HTTP サーバからbits.exe をダウンロードし、bits.exeとして保存	DC01
6/24/25 6:45:59:000 AM	tasksにbits.exeが置かれているのを確認	DC01
6/24/25 6:50:16.000 AM	新規にbitssを登録されているのを確認	DC01
6/24/25 12:41:51.000 PM	horilla.zipをPowerShell の Compress-Archiveコマンドで、 特定のフォルダを ZIP に圧縮して別の場所に保存	HRIS
6/24/25 12:45:45.000 PM	horilla.zip の持ち出しを確認	HRIS
[...]	[...]	[...]

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
bits.exe	
net.exe	E9711F47CF9171F79BF34B342279F6FD9275C8AE65F3EB2C6EBB0B843
SharPersist.exe	E9711F47CF9171F79BF34B342279F6FD9275C8AE65F3EB2C6EBB0B843

ネットワーク通信

種類	価値
C&C	192.168.12.60
ファイルダウンロード	SharPersist.exe
ファイルダウンロード	bits.exe
ファイルダウンロード	horilla.zip