2020 年 10 月 7 日

ブリテン：ATM キャッシュアウト ペイメントセキュリティの脅威

PCI セキュリティ・スタンダード・カウンシル(PCI SSC)と ATM 産業協会(ATMIA) は緊急の注意喚起を必要とする最新の脅威について強調してお伝えします。

何が脅威なのか？

ATM キャッシュアウトは犯罪者が顧客のアカウントを改ざんし短時間に多数の ATM から無制限に現金を引き出せるようにするだけでなく、カード会社やペイメントカードプロセサーに侵害し不正検知コントロールを操作するなど非常に精巧で指揮された攻撃です。

これらの攻撃はどのように行われるのか？

ATM キャッシュアウト攻撃は綿密な計画と実行を必要としています。しばしば、犯罪組織はカード管理システムへアクセスし、例えば引出限度額や PIN が盗まれたアカウントなど不正予防コントロールを改ざんします。これは共通してフィッシングやソーシャルエンジニアリングを介し、マルウェアを金融機関やペイメントカードプロセサーに侵入させ行われます。

犯罪組織はそこで新しいアカウントもしくは入手した既存アカウントを使いクレジットカード/デビットカードを連携された手法でATMで現金を引き出すグループに渡されます。カード管理システムをコントロールすることにより犯罪者は残高と引出限度額を改ざんし、ATM内の現金が無くなるまで引き出しができるようにします。

これらの攻撃は大抵の場合 ATM 自体に攻撃をしかけるものではありません。ATM はカードイシュアのオーソリゼーションシステム内の脆弱性が攻撃された後に現金を引き出すために使われます。

誰がリスクを負うのか？

金融機関、そしてペイメントプロセサーが主としてファイナンスリスクを負うことになります。これらの大掛かりな組織化された攻撃の標的になりやすいのです。 これらの機関は極めて短時間に数百万ドルの損失を被る立場になります、そして非常に組織化、周到化された犯罪の結果として世界中の複数の地域でリスクにさらされます。

これらを検知するためのベストプラクティスとは？

ATM キャッシュアウト攻撃は非常に短時間で数百万ドルもの現金が流出するため、その前にこれらを検知する能力は非常に重要です。このようなタイプの攻撃を検知する方法として

- ✓ アカウントとボリュームを基礎としたベロシティ・モニタリング
- ✓ FIM(File Integrity Monitoring System) を含む 24 時間体制のモニタリング能力
- ✓ 不審行為を検知した場合即座にアラートを発信する報告システム
- ✓ インシデント対応システムの開発と実践
- ✓ 想定外のトラフィックリソース（例えば IP アドレス）のチェック
- ✓ 未承認のネットワークツールの実行を発見

これらを予防するためのプラクティスとは？

ATM キャッシュアウト被害を緩和するための最善の保護措置は人材、処理そしてテクノロジーを含む多層的な防御の採用です。 ATM キャッシュアウト予防のためのいくつかの推奨策は以下の通りです。

- ✓ あなたのシステムへの強力なアクセスコントロールとサードパーティーリスクの特定
- ✓ 内部犯罪を防ぐための従業員モニタリングシステム

- ✓ 従業員に対する継続的なフィッシング対策トレーニング
- ✓ 多要素認証の導入
- ✓ 口座残高や取引限度をリモートで変更するための承認手続きの重層化
- ✓ タイムりー(速やか)に求められているセキュリティパッチの実行
- ✓ 定期的なペネトレーションテスト
- ✓ アクセスコントロールのメカニズムと特典の頻繁なレビュー
- ✓ 機微な機能を実行できるユーザーID が使われないようにするために特典のあるアクセスとの役割の厳格な分離
- ✓ 検知メカニズムとして使うことができる FIM ソフトウェアの導入
- ✓ 全体としての PCI DSS 準拠の厳格な確保

組織はそれらのシステムへのすべてのアクセス、特にサポート提供や管理機能を司るシステムに多要素認証を導入すべきです。そうするために、組織は悪意のある脅威ベクターからのアクセスの可能性から防御し、よりセキュアなインフラストラクチャーとすることができます。

すべてのソフトウェアに対しセキュリティパッチを適用することは非常に需要です。 ATM キャッシュアウト攻撃は犯罪者がペイメントシステムに有害なマルウエアを首尾よく侵入させた時から始まります。最新のアンチウィルスソフトウェアを使用し、またパッチで最新状態の維持することによりこのリスクは大きく減少できます。

組織は高品質なモニタリングソフトウェアを導入し信頼できるソフトウェアベンダーのみを使うべきです。FIMソフトウェアでは稀なパターンを検知し潜在的な問題/攻撃をアラートできます。ソフトウェアプロダクトにセキュリティを構築しソフトウェアライフサイクルを通じ継続的なサポートを提供できるソフトウェアベンダーを選択してください。

不審な行為を警報する報告システムは組織が攻撃をすばやく検知し処理する能力を高めます。ATM キャッシュアウト攻撃はしばしば数か月間にわたりシステムにアクセスしたサイバー犯罪者が関与しており、彼らは組織システム内の脆弱性を学び組織化され攻撃を計画します。 不審行為をプロセスの早い段階でアラートする報告システムを持つことは攻撃を中止させることに役立ちます。

PCI DSS 準拠はあなたの組織内でのセキュリティの文化の良好な基礎です。PCI DSS では ATM キャッシュアウトテスト攻撃に対抗するため、例えば多要素認証、パッチ、FIM ソフトウェアの導入など多くの実務慣習を求めています。

リソース:

https://www.retail-fcl.com/wp-content/uploads/2018/08/atmia-information-alert-unlimited-operations1.pdf

https://research.nccgroup.com/wp-content/uploads/2020/07/1992-Insight-Space-Technical-Deep-Dive-June-v2.pdf

https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/

https://www.cbsnews.com/news/fbi-reportedly-warns-of-unlimited-atm-cash-out-scheme/

https://money.cnn.com/2018/08/13/news/companies/atm-cash-out-fbi-warning/index.html

https://www.enisa.europa.eu/publications/info-notes/atm-cash-out-attacks

###

PCI Security Standards Council について

The PCI Security Standards Council (PCI SSC)は 事業者がサイバー攻撃や情報流出を予防、緩和、検知することを支援する業界主導、柔軟で効果的なデータセキュリティ基準とプログラムを提供することにより ペイメントセキュリティを向上するため、グローバル、業界横断的な取組みをリードします。 PCI SSC との連絡は LinkedIn. Twitter による会話への参加 @PCISSC. ブログの購読 PCI Perspectives Blog.

ATMIA について

ATMIA はグローバルな ATM 業界を代表する非営利の業界団体です。ATMIA は 70 か国に 650 社以上 11,000 以上のメンバーに 金融機関、独立系 ATM 設置、装置メーカー、プロセサー、過剰 ATM サービス、付加価値ソリューションプロバイダーを含む ATM 生態圏全体に奉仕しています。ご参加についてはこちらをご覧ください: https://www.atmia.com/membership/join/