KELA

サクセス・ストーリー

SUCCESS STORY

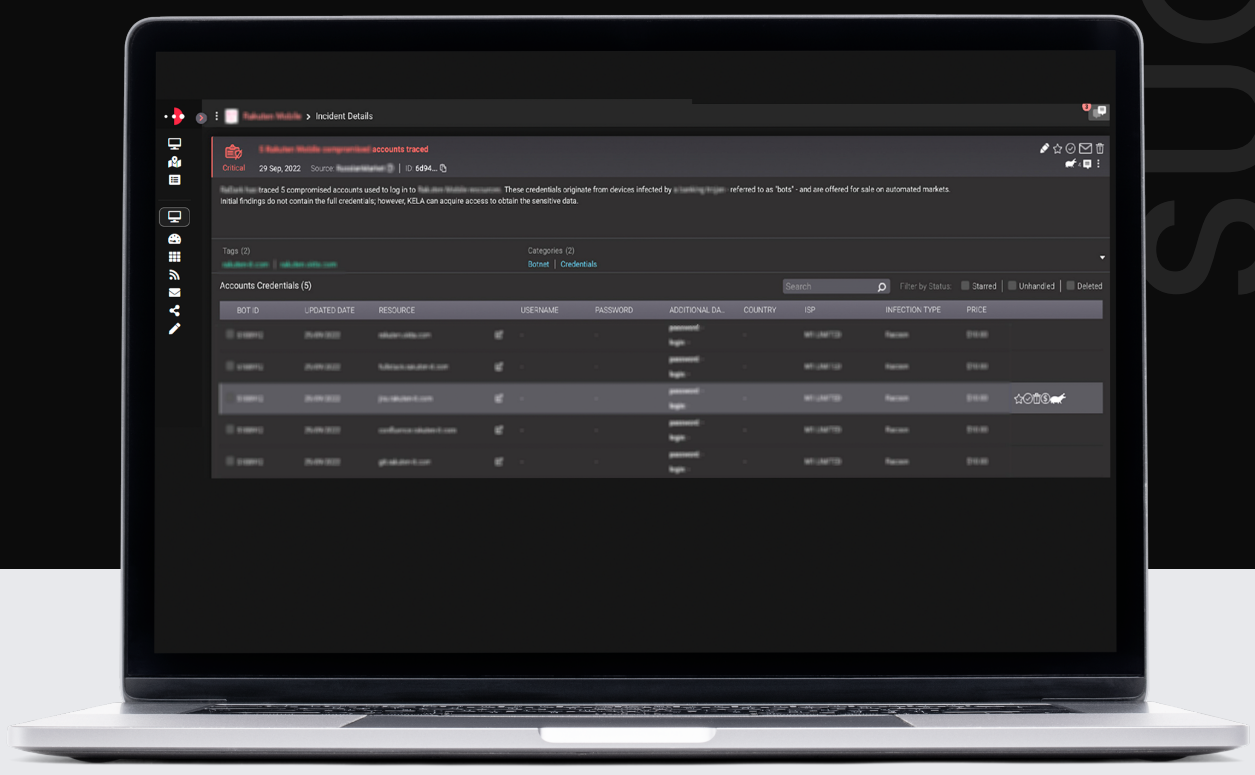
不正アクセスされたアカウントが大手電気通信企業へのサイバー攻撃に発展する事態を阻止

背景

KELAのサイバー犯罪インテリジェンスプラットフォームは、顧客である某大手電気通信企業と関連のあるアカウントが不正アクセスされ、サイバー犯罪マーケットでボットとして売り出されていることを検知した。顧客企業はリスクの重大度を評価するため、ボットのデータを入手するようKELAに依頼。そこでKELAのCIC（サイバー犯罪インテリジェンスセンター）が調査を行ったところ、もはやサイバー犯罪マーケットには問題のボットが存在しないことが判明した。ボットがマーケットから消えた場合、大抵はそのボットが何者かに買い取られてしまったことを意味する。

ボットなしでも被害者を特定

アンダーグラウンドのボットマーケットで売り出されていたはずのデータや資格情報が消えれば、企業にとっては「脅威アクターに資格情報を悪用され、社内ネットワークに不正アクセスされるかもしれない」という懸念が生じる。そして、もしこの懸念が現実になってしまえば、企業の知的財産や従業員の個人情報、機密性の高い財務情報を窃取されたり、様々なサイバー攻撃を実行されかねない。同社は攻撃を受けるリスクを緩和するため、このアカウントユーザーの身元や関連情報を入手するべくKELAに調査を依頼した。



さらなるインテリジェンスで調査を深化

01

KELAが調査を行った結果、問題の資格情報を窃取する際に使用されたマルウエアは「Racoon Stealer」であったことが判明した。このRacoon Stealerは、資格情報やブラウザのクッキー、自動入力データ、暗号資産のウォレット情報をはじめ、さまざまな個人情報を窃取するマルウエアだ。また、ユーザーのIPアドレスや地理的位置情報データなど、システム情報を収集する機能もある。

02

マルウエアに感染した端末の所有者、すなわち資格情報を窃取されたユーザーの身元を特定しようとしたものの、問題のボットが販売されていたはずの「Russian Market※1」から消えていることが判明。そこでKELAのCICチームはこのボットのIDをもとに、被害者のデータに含まれていたURL情報※2について調査を行った。

※1) アンダーグラウンドでサイバー犯罪者が商品を自動売買するマーケット

※2) ボットには、感染端末のユーザーが利用していたサービスのURLが含まれている。

03

各URLを調査する中で、KELAは問題のアカウントユーザーの氏名が含まれていると思われるブログにたどり着いた。

04

さらにKELAは、LinkedInのプロファイルで同一氏名の人物を発見。そのプロファイル情報によると、この人物は2019年に、KELAの顧客である電気通信企業でインターンとして在籍していた大学生であることが判明した。まさにこの事実はボットに含まれていたその他のURL情報とも一致していた。

05

KELAは電気通信企業に対し、この人物が同社で使用していた資格情報を完全に無効化して、「企業のエクスポージャー」から生じる脅威を低減するよう助言した。

KELAのサービスでサイバー攻撃を防止

- KELAのサイバー犯罪インテリジェンスプラットフォームに搭載されたリアルタイムな監視機能が、電気通信企業と関連のあるアカウントへの不正アクセスを検知し、アラートを送信
- ボットが入手不可能な状況でも、KELAのサイバー犯罪インテリジェンスチームが情報窃取マルウエアの被害者を特定
- その結果、同社は不正アクセスを阻止し、脅威を緩和することに成功

EMPOWERED BY KELA

www.kelacyber.com/ja / marketing@ke-la.com / 03-6634-7836