KELA

SUCCESS STORY

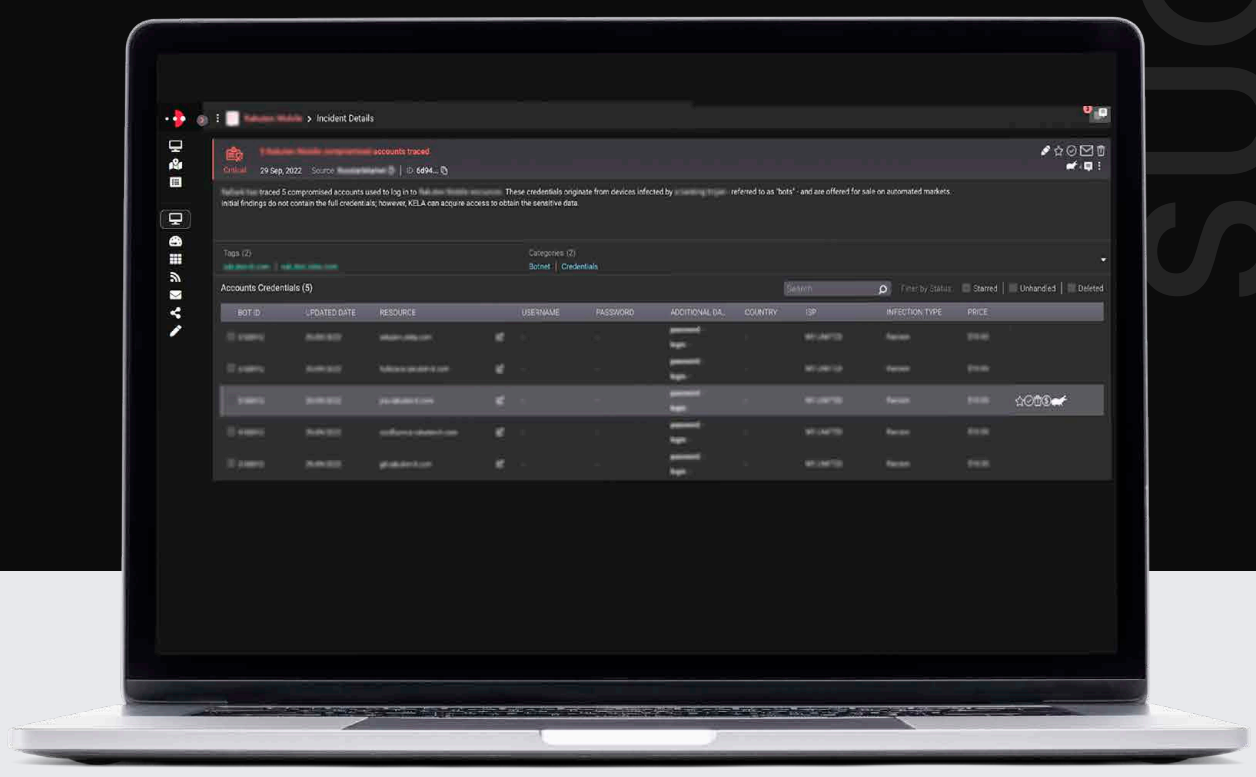
PREVENTING A COMPROMISED ACCOUNT THREAT FROM BECOMING A CYBERATTACK ON A MAJOR TELECOMMUNICATIONS COMPANY

Background

KELA's Cybercrime Intelligence Platform has detected a compromised account associated with a resource connected to the company's domain.
As the company requested to purchase the bot files to assess the risk severity, KELA's Cybercrime Intelligence Center found that the files were no longer available on the cybercrime market, which may often imply that the files were sold.

Detect a Victim's Identity Without the Files

When the stolen credentials are removed from underground bot markets, it raises the concern of threat actors using them to access the company's internal network. Such an intrusion may result in stolen company intellectual property, employee personal information, sensitive financial information, and other cyber attacks.
The company reached out to KELA requesting a further investigation for additional intelligence and insight into the victim's identity in order to mitigate the risk.



DEEPEN THE INVESTIGATION WITH ADDITIONAL INSIGHTS

01

KELA found that the information stealer behind the attack was Racoon Stealer. The malware gathers personal information such as credentials, browser cookies, autofill data, and crypto wallet details. Additionally, Raccoon Stealer records system information such as IP addresses and geo-location data.

02

In an effort to surface the identity behind the infected machine - the owner of the stolen file, which was no longer available for purchase on "Russian Market" (a cybercrime underground automated shop) - KELA's CIC team investigated the malware-infected URLs (the company's resources) on our Cybercrime Investigations module by pivoting on the bot ID.

03

In the search for unique URLs, KELA detected a WordPress blog that may include a first and last name.

04

KELA searched the verbatim name and found a LinkedIn profile owned by a person who seemed to have been an intern in the company back in 2019, and now is with a specific university that perfectly aligns with the rest of the bot's URLs.

05

KELA recommended that the company ensures the employee's past company credentials are disabled and thus lowers the threat level stemming from their exposure.

EMPOWERED BY KELA

Preventing Cybercrime Attacks with KELA

- KELA Cybercrime Intelligence Platform's real-time monitoring capability alerted about compromised accounts associated with the company.
- KELA's Cybercrime Intelligence investigation uncovered the victim of the infostealer attack without the bot file in hand.
- As a result, the company was able to prevent unauthorized access and mitigate the threat.

kelacyber.com / marketing@ke-la.com / +972-3-970-2720