SpyCloud

CASE STUDY

lendingtree

How LendingTree seamlessly automates remediation of credential exposures to protect employee and consumer identities with SpyCloud >

As a financial services organization that must protect business-critical and sensitive consumer data, LendingTree knows the importance of having a robust security program. LendingTree's Security Operations Center (SOC) team, led by Security Operations Manager, Anthony Brunson, oversees 24x7 alert monitoring, security, and response support for employee and consumer accounts.

With the rising threat of cyberattacks on financial organizations putting corporate and consumer data at risk, it's been more important than ever for LendingTree's SOC team to have the tools they need to effectively monitor, detect, protect, and remediate exposed credentials in the event of a third-party security incident or malware-infected devices.

Criminals are eager to take advantage of any data they can get their hands on, and in particular data exfiltrated by malware-infected devices is a rising threat to the financial industry. SpyCloud's annual analysis of the darknet exposure of **Fortune 1000 companies** revealed:

15,274
MALWARE-INFECTED FINANCIAL SECTOR EMPLOYEES
(300% YoY▲)

551k
MALWARE-INFECTED FINANCIAL SECTOR CONSUMERS
(794% YoY▲)

THE OVERVIEW

LendingTree is the nation's largest loan marketplace that connects consumers with financial borrowing options for mortgages, auto loans, small business loans, credit cards, as well as comparison shopping services for vehicle and education programs. Their mission is to offer consumers the ability to comparison shop for financial services, partnering with more than 400 financial institutions worldwide. LendingTree brands include Compare Cards, Magnify Money, and Simple Tuition.

THE CHALLENGE

LendingTree's 24x7 Security Operations Center (SOC) team is charged with providing alert monitoring and remediation to protect employee and consumer accounts from security risks associated with account takeover (ATO) and ransomware.

SpyCloud

CASE STUDY

The LendingTree SOC team has had SpyCloud integrated into their primary workflows for more than five years now. It helps them identify compromised credentials associated with their brand domains, as well as identify consumer credentials that may be circulating the dark web from breaches and malware infections.

BETTER INSIGHTS WITH LESS EFFORT

Prior to using SpyCloud, LendingTree experienced frustration due to alert fatigue and heavier-lifting associated with traditional threat investigation and response.

When they found out they could use SpyCloud to identify and take action on compromised credentials to mitigate corporate account takeover (ATO) and ransomware attacks – as well as ATO and online fraud for their customers – it was a no-brainer.

SpyCloud allows LendingTree's SOC team to take action on reliable alerts and reduce the amount of false positives. ***"Our never-ending objective for the team is to reduce alert fatigue, and SpyCloud helps with that,"*** Anthony said. ***"I know if I get a SpyCloud alert, it's actionable."***

Anthony not only trusts the quality of SpyCloud alerts not just for their ability to more effectively keep both employee and consumer accounts safe, but also to support the best use of his team's time, saying, ***"When you need a tool that can give you comfort that you're using your time and security resources wisely, SpyCloud is the answer."***

HOW IT ALL WORKS

In the past, depending on the skill level of the analyst or the amount of potentially compromised data, the LendingTree SOC team would have spent hours manually researching an incident, and monitoring for dark web data was a full-time job. With their adoption of SpyCloud, they get earlier notifications of potentially exposed credentials related to their domains or consumer accounts, allowing the SOC team to start the triage process and more swiftly remediate via automation.

THE SOLUTION

For more than five years, LendingTree has used SpyCloud ATO Prevention to discover and remediate compromised employee and consumer credentials exposed in third-party security incidents or exfiltrated from malware-infected devices. SpyCloud helps LendingTree mitigate account takeover and follow-on attacks while maintaining its brand reputation as a secure, trustworthy financial option for consumers.

THE RESULTS

With SpyCloud, LendingTree leverages automation to protect more than 1,000 LendingTree employee accounts and millions of consumer accounts, aiming to keep user credentials secure without added effort from the company's SOC team.

SpyCloud enhances other threat intelligence tools LendingTree already had in place to further bolster its defenses. ***"We use a number of tools to cross-check data, and we consider SpyCloud as a trusted resource for any type of incident that may impact our consumers or employees,"*** Anthony says.

EMPLOYEE PROTECTION

In the event LendingTree's SOC team is alerted of potentially exposed employee data that may impact their organization, insights from SpyCloud's **Cybercrime Analytics** would allow them to perform additional investigation and analysis to determine the root cause of a compromise, including verifying the source of the data to determine whether it's an internal issue, and to initiate a password reset, if necessary. This information would also be used to determine if potential policy changes are necessary, such as adjustments to their internal password policies.

CONSUMER PROTECTION

Their SOC team also uses SpyCloud to assist in monitoring and detecting potentially exposed consumer credentials, giving them greater ability to identify, verify, and validate legitimate users at various points in the account lifecycle. In the event SpyCloud detects compromised consumer credentials, LendingTree can use an automated workflow that integrates the SpyCloud API, which initiates an automatic forced password reset at next log-in.

"With the number of consumers that we have nationwide, it could take a whole team to monitor accounts that may be exposed from a security incident or malware on a consumer's endpoint. SpyCloud is an invaluable tool that reduces administrative overhead in resetting consumer or employee accounts if they are detected on the darkweb," says Anthony.

SAVING TIME WITH AUTOMATION

Part of the LendingTree SOC team's due diligence is looking for ways to integrate and automate technology that enables an efficient security framework. SpyCloud allows LendingTree to be efficient by automating a lot of the identification and remediation of compromised credentials.

Instead of the team spending the equivalent of three full-time employees manually monitoring for potentially exposed data and acting in the event of compromised credentials, they now save 60% of administrative overhead time and can focus on other high-priority tasks.

Says Anthony, ***"SpyCloud is an invaluable tool that saves us time and resources in resetting employee accounts that may be compromised."***

SpyCloud

CASE STUDY

With SpyCloud, LendingTree's IT team saves more than 50% of their related response time within their SOC's workflows.

Additionally, the ease of use of the SpyCloud interface allows for quick onboarding for new analysts and the ability to show the value of SpyCloud's darknet data insights. Says Anthony, ***"It's reliable, the time to integrate and onboard is easy and simple, and it just works."***

ORGANIZATION-WIDE VALUE

The value of SpyCloud isn't limited to LendingTree's SOC team. ***"There are synergies around potential fraud that developers, engineers, and our product team are keen on detecting, and SpyCloud is a part of that feedback loop between security and those other teams. If there are questions around a potential threat actor that may come to our platform in an attempt to commit fraud, we leverage SpyCloud as one of the tools to protect our customers"*** Anthony said.

And by protecting customer accounts, the SOC team is also helping LendingTree maintain its brand reputation by ensuring high levels of security for an organization in an industry fraught with cyberattacks and online fraud.

"If your brand is important and you have employees that you want to protect from account takeover and ultimately protect consumer data, you have to get SpyCloud," says Anthony.

KEY OUTCOMES

- Protects **1,000 employee accounts** & **millions of customer accounts** from ATO and ransomware
- Saves **60% of SOC team's time and resources** with actionable data & automation
- Reduces alert fatigue with **high-fidelity notifications**
- Supports organization-wide **security posture & brand integrity**