The Silent Threat Targeting Real Estate Professionals: Understanding Infostealers

Description

Article by Genady Vishnevetsky

The Digital Pickpocket in Your Computer

Imagine a thief who can quietly walk through your office, photographing every password you jot down, every client file you open, and every financial document on your deskâ??all without you ever realizing they were there. Thatâ??s basically what an infostealer does to your computer.

Infostealers are malicious programs aimed at stealing your sensitive information. Unlike older computer viruses that slowed down your system or displayed annoying pop-ups, these modern threats operate silently. They can run and exit very quickly; many infostealers complete the theft and transmission of data within just a few seconds to a minute.

VLTA Examiner

For real estate and title professionals who manage sensitive client information, financial records, and confidential transactions daily, this poses a serious threat.

How These Digital Thieves Enter Your System

Think of your computerâ??s security as the locks on your office building. Infostealers are like skilled burglars who know exactly which doors to try and what keys to use. Here are the most common ways they break in:

The Fake Email Trick: You get what looks like a legitimate emailâ??maybe from a client, vendor, or even a government agency. The email has an attachment or link that appears crucial to your business. When you click on it, youâ??re unknowingly installing the infostealer. Cybercriminals use info stealers on victim devices through various methods, including phishing emails.

The Software Trap: You download what seems like a helpful programâ??maybe a new real estate app or a document converter. Hidden inside this apparently legitimate program is an infostealer that installs itself when the program is run.

The Search Engine Deception: Cybercriminals use search engine optimization (SEO) techniques, malicious advertisements, or harmful links posted on social media platforms to make their malicious websites appear in your search results when youâ??re looking for legitimate software or services.

The Website Ambush: Simply visiting a compromised site can be enough. If your browser or computer has unpatched security vulnerabilities, the infostealer can install itself without any action on your part beyond loading a webpage.

What Theyâ??re After: Your Digital Identity

Once inside your system, infostealers function as highly efficient data collectors. They specifically target:

- **Login credentials** for all your accounts (email, banking, real estate platforms, client management systems)
- **Browser-saved passwords** (more on this critical issue below)
- **Financial information,** including credit card details and bank account information
- **Client data** stored in documents or applications
- **Browser cookies** that keep you logged into websites
- **Cryptocurrency wallet information** if you use digital currencies

The data is then packaged and sold as logs. These â??logsâ?• containing your stolen information are sold on underground marketplaces for surprisingly small amountsâ??sometimes as little as $10â??but can cause thousands of dollars in damage to your business and clients.

The Hidden Danger of Browser Password Vaults

VLTA Examiner

Hereâ??s where many well-meaning professionals unknowingly put themselves at greater risk. Most modern browsers offer to save your passwords for convenience. While this feature seems helpfulâ??and it can beâ??it creates a significant vulnerability when combined with browser account syncing.

When you save passwords in your browser and sign into your browser account (like Chrome with your Google account or Firefox with your Mozilla account), those passwords automatically sync across all devices where youâ??re signed in. This means that if you save work passwords on your home computer, they will also be available on your personal laptop, tablet, or phone.

Now imagine this scenario: your teenage child downloads a game with hidden malware onto the family computer where youâ??re signed into your browser account. The infostealer runs, capturing all your synced passwordsâ??including access to your real estate platform, email, and financial accountsâ??and sends them to cybercriminals. Suddenly, your work accounts are compromised due to activity on a completely different device in your household.

This synchronization feature means personal devices with weaker security controls can serve as entry points for attacks on your work accounts. Personal devices often lack consistent enforcement of enterprise security policies, which increases the risk to organizations.

The Real Estate Connection: Why Youâ??re a Target

Real estate and title professionals are appealing targets for cybercriminals for various reasons.

Financial Access: You regularly manage large financial transactions and have access to banking information, escrow accounts, and wire transfer details.

Personal Information: Your client databases hold exactly the kind of personally identifiable information that criminals seek: names, addresses, Social Security numbers, financial details, and employment information.

Time-Sensitive Transactions: The pressure to finish urgent real estate deals can increase the likelihood of professionals clicking on urgent-looking emails or links without proper verification, which can lead to security risks.

Multiple Device Usage: Many real estate professionals work from different locations using various devices, which expands the potential attack surface.

Protecting Yourself and Your Clients

The good news is that understanding how these threats work gives you an advantage over most potential victims. Here are practical steps to safeguard your business:

Use a Dedicated Password Manager: Instead of relying on browser password storage, choose a dedicated password manager like Bitwarden, 1Password, or LastPass. These tools are proven to offer better security.

Separate Personal and Professional: Never use personal devices for work-related logins, and vice versa. If you must use the same device for both, use different browser profiles or separate browsers entirely.

VLTA Examiner

Think Before You Click: Take a moment to verify the source of any email attachment or link, especially if it creates a sense of urgency. When in doubt, contact the sender through a different communication method to confirm legitimacy.

Keep Software Updated: Enable automatic updates for your operating system, browsers, and all software applications to ensure optimal performance and security. Patching is essential in fighting the growing threat of infostealer malware.

Regular Security Training: Stay informed about current threats and share this knowledge with your team to ensure everyone understands. The cybersecurity landscape is constantly changing, and protection strategies that worked yesterday might not be enough for todayâ??s threats.

Conclusion

Infostealers are becoming an increasing threat to real estate professionals. The report shows that infostealer attacks grew by 58% in 2024, and around 10 million personal and business devices were affected by infostealers in 2023. However, by understanding how these threats work and taking proactive security stepsâ??especially those related to password management and device separationâ??you can greatly lower your risk.

Remember: in cybersecurity, convenience often comes at the cost of security. Taking a few extra seconds to use a proper password manager and verify email sources could save you and your clients from costly financial and privacy breaches.

Your clients trust you with their most sensitive financial decisions. Safeguarding their data with the same care you give to their transactions isnâ??t just good businessâ??itâ??s a professional obligation in our increasingly digital world.



Genady Vishnevetsky
Genady Vishnevetsky serves as Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building successful security programs and developing the defense against emerging threats, Vishnevetsky leads security, governance, and compliance programs for global enterprises. Genady holds the following cybersecurity and risk management certifications â?? Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified in Risk and Information Systems Control (CRISK).

Category

1. Cybersecurity
2. Human Resources

3. In the News
4. Members
5. Uncategorized

Date Created
2025/09/24
Author
vltaexaminer

VLTA Examiner