Devolutions

Threat landscape 2024 for password manager

Author: William Matos
Date: October 16, 2024
Version: 1.0
TLP: Clear

Table of content

Introduction

What is a Threat Landscape Report

It is a detailed report that outlines the current and emerging cybersecurity threats impacting organizations, industries, or specific regions. In this report, we will focus on threats to password management and security incidents affecting password management companies.

Objectives of the threat landscape report

However, despite their advantages, password managers are not immune to threats. The evolving threat landscape poses significant risks to these tools, with cybercriminals constantly devising new methods to compromise their security. This whitepaper aims to define the global threat landscape associated with password managers, providing a comprehensive overview of the challenges and risks that users and developers face.

Importance of Password Manager

In today's digital landscape, password managers have become indispensable tools for individuals and organizations seeking to secure their passwords. As the reliance on digital services grows, so does the threat. Password managers offer a convenient and secure way to store, manage, and retrieve complex passwords, reducing the risk of credential theft and enhancing overall cybersecurity posture.

Current Threat Landscape

Overview of Cyber Threats

As password managers become more essential, they have increasingly attracted the attention of cybercriminals. The threat landscape encompasses various attack methods, including infostealers, malvertising, and advanced malware campaigns, all designed to compromise sensitive data such as passwords and personal information. Key threats include:

1. Infostealer & Malware
2. Malvertising
3. Sophisticate Attacks & Campaign

Infostealer

An **infostealer** is malware designed to steal sensitive information like passwords, banking details, and personal data from an infected device. It typically spreads through phishing, malicious downloads, or software vulnerabilities, quietly collecting and sending stolen data to attackers for misuse.

According to IBM's X-Force team, common initial attack vectors for breaches frequently involve the use of valid credentials and malware such as infostealers.

In summary, the increase in infostealer activity and the use of valid credentials for system access demonstrates a growing trend in cybercriminals favoring stealthy, indirect approaches to infiltrate networks and steal valuable information. These methods often allow them to avoid detection for longer periods, increasing the damage they can cause.

Initial access from valid credentials

71% surge from 2022 to 2023

The usage of infostealer by cybercriminals

surge of 266% from 2022 to 2023

Emerging Threats from infostealers malware

In this section, we will examine an infostealer campaigns, including Meduza Stealer, Stealc, and Luca Stealer Trojan. These malicious campaigns are targeting at least 13 password managers, seeking to compromise accounts by exploiting data dumps, instant messaging platforms, and bot-operated dump services to harvest credentials.

These attacks result in the theft of highly sensitive data, such as login credentials, which are then sold on the underground market. Those cybercriminals are financially motivated, and they are focusing on monetizing on compromised accounts.

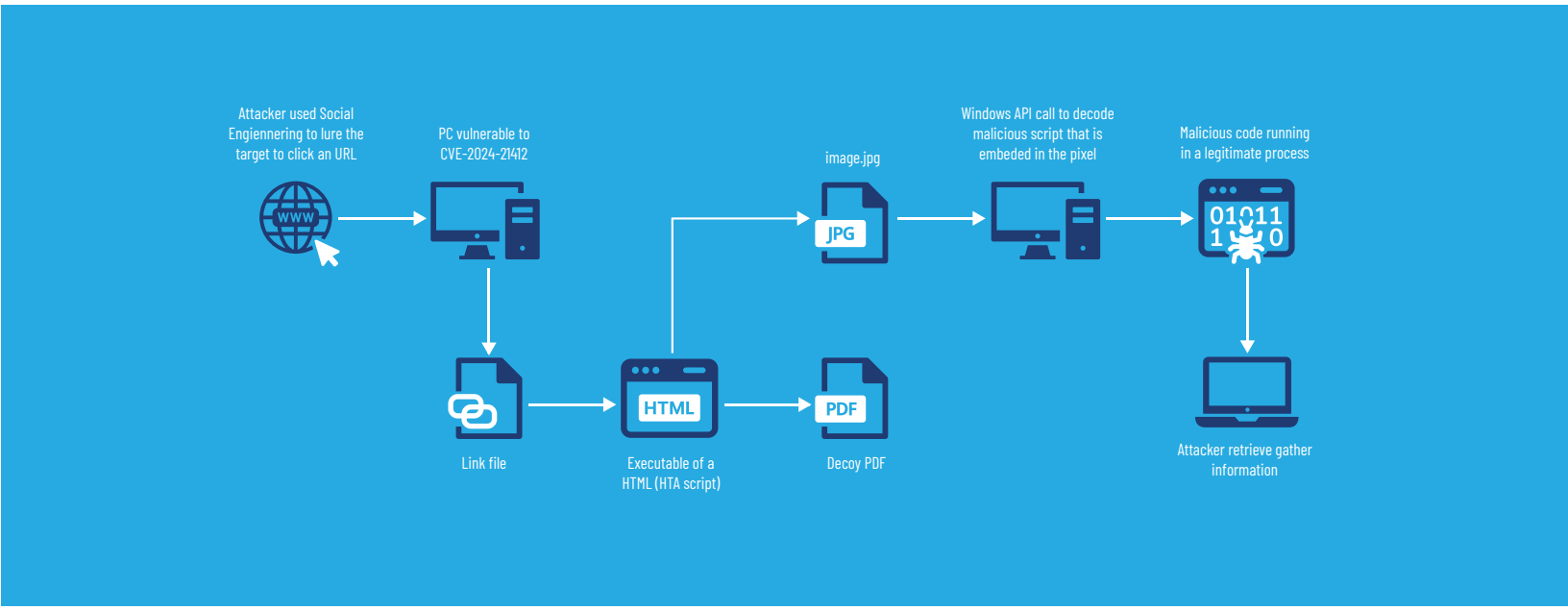
Ransomware groups try to reduce the time to exploit a target and using compromised accounts can help save time and make it more difficult for defenders to detect suspicious behavior from a validate account. This will explain why infostealers gain so much popularity in these recent years.

Details of an infostealer campaign

Infostealers have exploited the vulnerability CVE-2024-21412, a flaw in Microsoft Defender SmartScreen that allows attackers to bypass security checks using malicious internet shortcuts. Threats like Lumma Stealer, Water Hydra, DarkGate, Meduza, and ACR take advantage of this SmartScreen vulnerability to target their victims.

The attack method begins with victims being lured into clicking a URL that triggers the download of a shortcut (LNK) file. This file, in turn, downloads an executable containing an HTML Application (HTA) script with PowerShell code designed to retrieve decoy PDFs and malicious injectors. One notable injector decodes hidden malicious code from a JPG image file using the Windows API.

Once inside, the stealers implant themselves into legitimate Windows processes, allowing data exfiltration to begin. These stealers target a wide range of sensitive information, including data from web browsers (like Chrome and Firefox), crypto wallets (Binance, Ledger Live), messaging apps (Telegram, WhatsApp), password managers (Bitwarden, 1Password), VPN apps, email clients, and FTP clients.

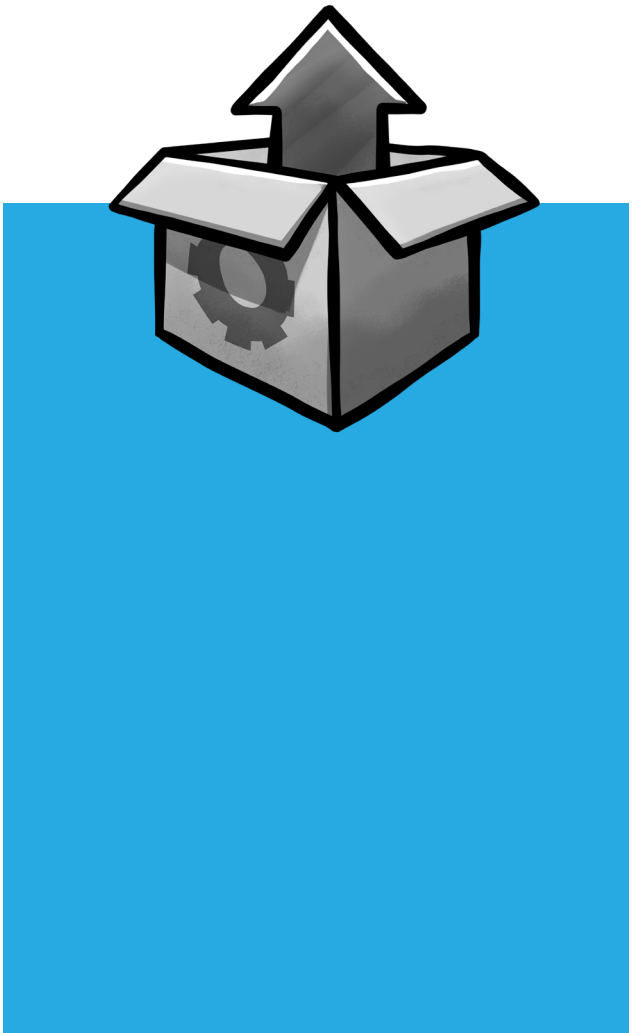


Malvertising

A second threat we discovered, is the malvertising. Malvertising is short for “malicious advertising” and refers to the practice of injecting malicious code or ads into legitimate online advertising networks. These ads will appear on well-known websites to have more exposure to infected large groups of people.

We found multiple ads for fake password manager and a fake Remote Desktop managers installer on a peer-to-peer website.

This technique will leverage the fact that many new users don’t fully understand the product, or they aren’t familiar with its normal appearance. The attacker will use this lack of knowledge to trick users into clicking or downloading these malwares that appears to be legitimate at first sight.

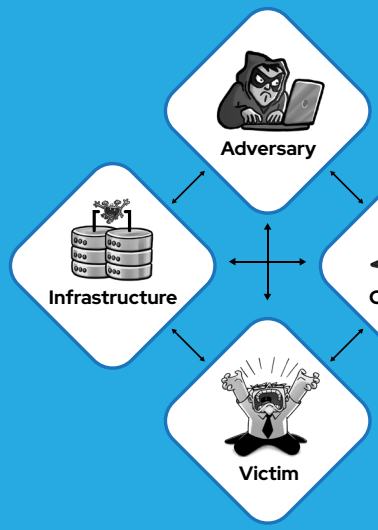


ZenRat malware

In 2023, ZenRat malware emerged as a significant threat, distributed through a fake installation package of the Bitwarden password manager. Cybercriminals used **malvertising** on Google Ads, abusing ad ranking to lead users to a cloned version of Bitwarden's legitimate website. This fake site even masqueraded as **Opensource.com**, copying an article by Scott Nesbitt to appear credible. The malware prompts users to enter their credentials—username, password, and secret key—allowing attackers to steal sensitive information. ZenRat is also distributed via **SEO poisoning**, adware bundles, and email phishing, and operates both internally and externally, with malicious IPs traced to various locations. The motive behind these attacks is largely financial, aiming to monetize stolen data or sell access.

ZenRAT is a malware strain that emerged as a Remote Access Trojan (RAT), often associated with cybercriminal activities. It is designed to give attackers unauthorized access to an infected system, allowing them to perform a wide range of malicious actions.

Motivation: Is to exfiltrate valuable information to sell on the darkweb.



C2 Server (what is command and Control).

In our case ZenRate was distributed via a fake installation package of password manager Bitwarden

Remote access control, the malware provide the attacker with full access to the victim's machine

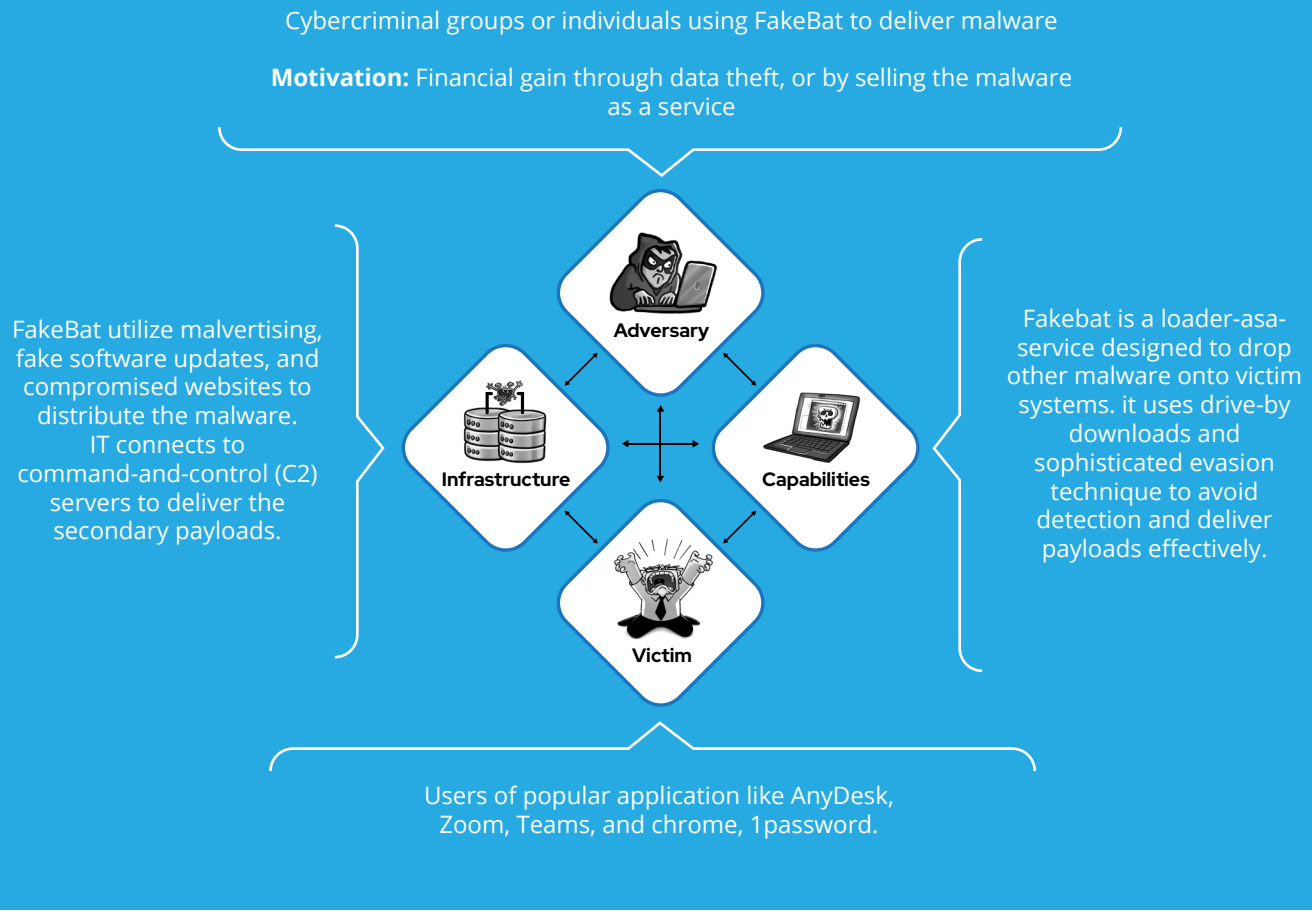
Logs keystrokes, takes screenshots, capture sensitive files.

Opportunistic , they will try to catch any one with the fake bitwarden campaign

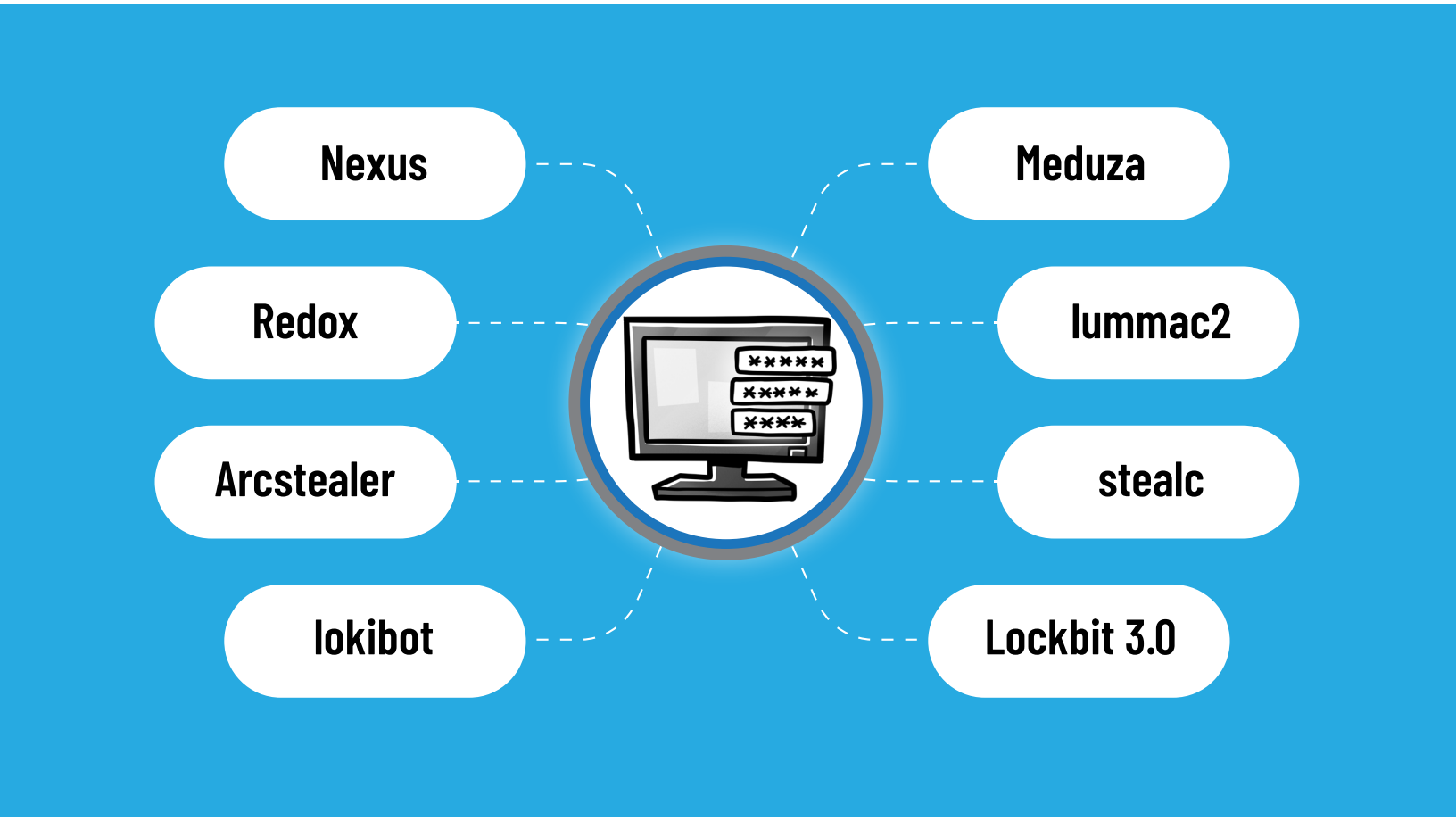
FakeBat Malware

Another Malware that used similar technique is the FakeBat malware. The malware is a highly sophisticated threat distributed through malvertising, social engineering tactics, compromised websites, and fraudulent browser updates. They use a technique called a drive-by download, which involves automatically downloading malware onto the user's system by exploiting browser vulnerabilities or embedding it in legitimate software like password managers, AnyDesk, or Teams.

Fakebat Malware is a Loader-as-a-Service (LaaS), the malware is sold or rent for other cybercriminals. A loader's main purpose is to deploy additional malicious payloads onto a compromised computer. Cybercriminals use LaaS platforms to easily distribute their malware without needing to develop their own loaders, making it a key part of another service, malware-as-a-service (MaaS). The prices of the fakebat service can vary from $1000 USD to $5000 USD per week or month depending on the package.

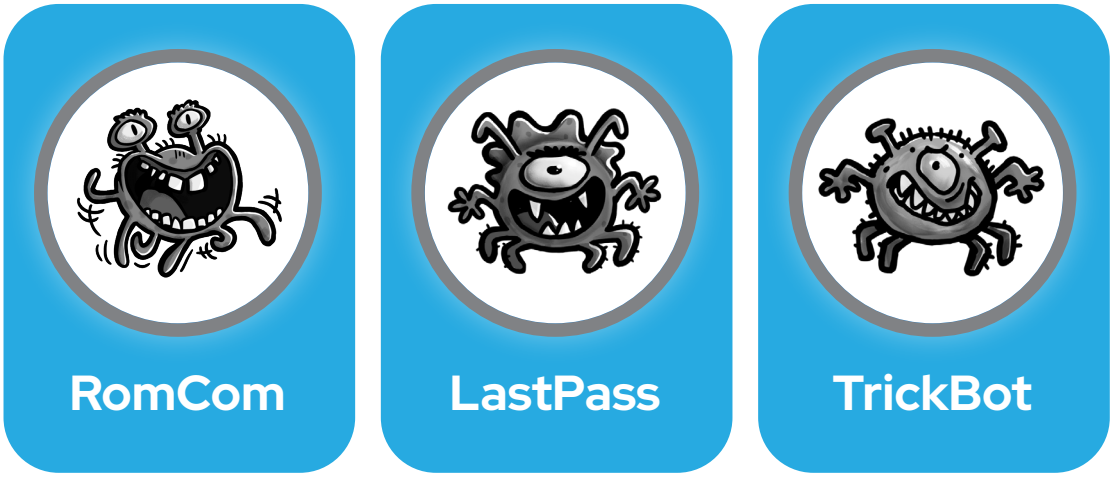


Top Malware who is known to target Password Manager



(https://securitysenses.com/posts/malware-targeting-password-managers)

Sophisticated Attack



This section explores several high-profile cyber threats that exemplify the growing sophistication of modern malware campaigns, focusing on RomCom, LastPass, and TrickBot. These attacks leverage advanced techniques such as phishing, typosquatting, and malware-laden applications to target victims across various industries. RomCom Backdoor, for example, impersonates Devolutions software to deliver malware, particularly focusing on Ukrainian and U.S. healthcare organizations. The LastPass breach highlights the risks posed by credential theft among privileged employees. Meanwhile, TrickBot continues to evolve with complex attack chains designed to steal credentials and infiltrate networks. Through these case studies, we gain insights into how sophisticated threats exploit vulnerabilities, revealing critical patterns in the evolving threat landscape.

The RomCom Backdoor

The RomCom Backdoor campaign involves attackers impersonating legitimate or fictional software websites to trick users into downloading malware. It uses techniques like phishing, typosquatting, and trojanized software, including popular applications like Devolutions Remote Desktop Manager and KeePass. Once installed, the malware provides remote access for data exfiltration. The campaign primarily targets Ukrainian politicians and U.S. healthcare organizations, with the attackers suspected to be the Cuba Ransomware group. This campaign, active between 2022 and 2023, is geopolitically motivated, with the primary objective of gathering sensitive information related to the Ukraine conflict, specifically targeting organizations and individuals involved in the ongoing crisis.

Overview of the killchain

1.

Reconnaissance: Attackers identify targets, primarily Ukrainian politicians and U.S. healthcare organizations, by focusing on those supporting pro-Ukraine eSorts.

2.

Weaponization: They create trojanized versions of popular software like Devolutions Remote Desktop Manager and KeePass, embedding malicious payloads within legitimate-looking applications.

3.

Delivery: The malware is distributed through spear-phishing emails and rogue websites that closely mimic legitimate software download pages. These sites are promoted via Google ads to lure victims.

4.

Exploitation: Victims are tricked into downloading and installing the trojanized software, unknowingly granting the attackers access to their systems.

5.

Installation: Once the malicious application is installed, the malware executes, establishing a backdoor that enables remote access.

6.

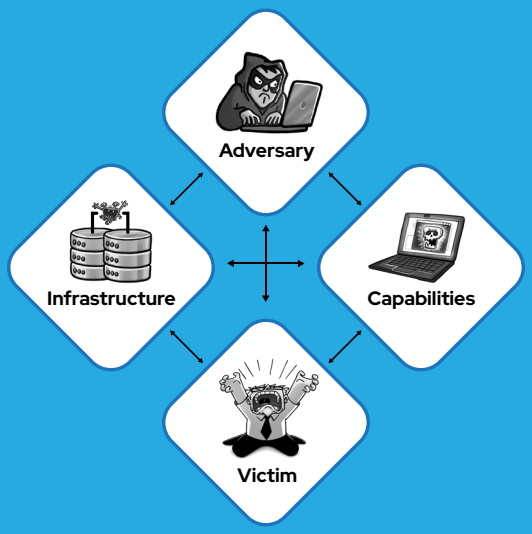
Command and Control (C2): The malware communicates with C2 servers, often using self-signed SSL certificates to encrypt traSic and evade detection..

7.

Actions on Objectives: The attackers exfiltrate sensitive data, including information related to the Ukraine conflict, using the backdoor for remote access. The campaign's objectives include both financial gain and geopolitical advantage.

The campaign is suspected to be conducted by the Cuba Ransomware group (also known as Tropical Scorpius or Void Rabisu), though the attribution is still being confirmed. Their motives appear to be both financial and geopolitical, targeting organizations supporting Ukraine.

The attackers rely on rogue websites that mimic legitimate software download pages (e.g., for Devolutions Remote Desktop Manager and KeePass). These cloned sites are promoted using Google advertisements to drive traffic to the malicious downloads. The command-andcontrol (C2) servers use self-signed SSL certificates to encrypt traffic, making detection and attribution more difficult.



The attackers employ several sophisticated techniques:

Phishing and typosquatting to trick victims into visiting malicious sites.

Trojanized software that includes x64 DLL payloads to infiltrate victim systems.

Once installed, the malware grants remote access and enables data exfiltration.

The attackers also employ anti-debugging techniques and obfuscation to evade detection.

The primary targets are Ukrainian politicians and U.S. healthcare organizations. These victims were chosen based on their proximity to pro-Ukraine organizations, particularly those involved in providing aid to refugees during the ongoing conflict.

LastPass Incident Overview

In 2022 and 2023, LastPass experiences significant breaches, mainly driven by cybercriminals seeking financial gain. In the first, hackers compromised a corporate laptop to access a cloud development environment, stealing source code and sensitive data. This gave the hackers access to LastPass systems, allowing them to steal client vault backups and related metadata.

More than six months after the initial breach, LastPass linked the August attack to a prolonged campaign. Hackers used data from the initial breach, a third-party breach, and a remote code execution vulnerability on a DevOps engineer's home computer to steal multiple resources and backups. They captured the engineer's master password, gaining access to encrypted vaults and critical database backups. The attack exploited keylogging malware through a vulnerable software package. The attacker targeted one of the four DevOps engineers with access to decryption keys, captured their master password after multi-factor authentication, and accessed the engineer's corporate vault, enabling access to sensitive resources and backups.

For more information about the incident visite this article:
https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

In addition to these breaches, LastPass users were targeted by cybercriminals posing as staff members, utilizing the **Crypto Chameleon phishing kit** to further their attacks. Although these phishing attacks impacted employees and users, LastPass reported that their core systems remained unaffected.

What is Crypto Chameleon phishing kit

The **Crypto Chameleon phishing kit** is a tool used by cybercriminals to create phishing attacks that impersonate legitimate services. It provides templates and mechanisms to deceive users into disclosing sensitive information, such as login credentials, making it easy for attackers to conduct targeted and effective phishing campaigns.

Summary of the Attack Flow:

1. **Initial Access:** Likely through a phishing attack or social engineering targeting an employee with privileged access.
2. **Privilege Escalation:** Attackers escalated privileges, likely gaining access to key systems.
3. **Lateral Movement:** They navigated through the network, eventually reaching and exfiltrating encrypted customer vaults.
4. **Data Exfiltration:** Stolen vault data was transferred out of LastPass's systems over encrypted channels, likely in small batches to evade detection.
5. **Defense Evasion:** Throughout the attack, the adversary used techniques to evade detection, possibly leveraging legitimate tools within the environment.

Cyberkill chain

Reconnaissance:
Attackers likely gathered information on LastPass employees with privileged access.

Weaponization:
A phishing campaign targeting a Senior DevOps engineer was launched.

Delivery:
A phishing email delivered the keylogger malware to the engineer's device.

Exploitation:
Attackers captured the employee's master password and credentials.

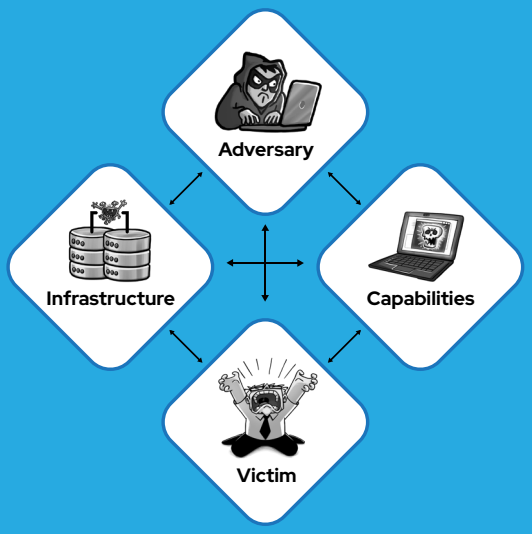
Installation:
The keylogger allowed attackers to maintain persistence.

Command & Control:
Remote access to cloud storage and corporate vaults.

Actions on Objectives:
Data exfiltration of encrypted vaults and sensitive metadata.

Who: A sophisticated cybercriminal group targeting financial gain, using phishing and exploiting vulnerabilities on a DevOps engineer's system.

How: The attackers used phishing emails, keylogging malware, and remote code execution vulnerabilities, leveraging third-party software to maintain access.



What: They captured master passwords, gained access to cloud storage decryption keys, exfiltrated encrypted vaults, and sensitive backup data.

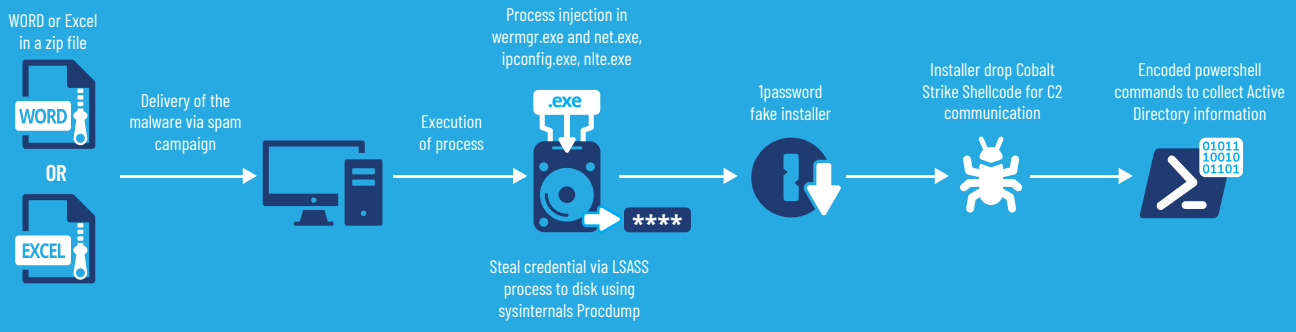
Who: LastPass, its development environment, DevOps engineers, and affected customers who had their vault data and metadata compromised.

TrickBot Overview

A sophisticated attack occurred in which the popular TrickBot Malware facilitated the installation of a fake 1Password application, allowing deeper infiltration and evasion. In this case, TrickBot malware was delivered via a phishing email and deployed on the victim's system. It used built-in Windows tools for reconnaissance, stealing credentials, and enabling remote access via Cobalt Strike. The attackers installed a fake 1Password manager to mask their activities, which secretly delivered more malware. Despite infiltrating multiple systems, the operation stopped without data exfiltration, leaving the reason unclear.

What is TrickBot Malware

TrickBot is a modular banking Trojan that started in 2016, designed to steal financial and login information. It spreads through phishing emails or other malware and can move across networks. TrickBot can deploy other malware, like ransomware, making it a major threat. It communicates with command-and-control servers for instructions and uses evasion techniques to avoid detection.



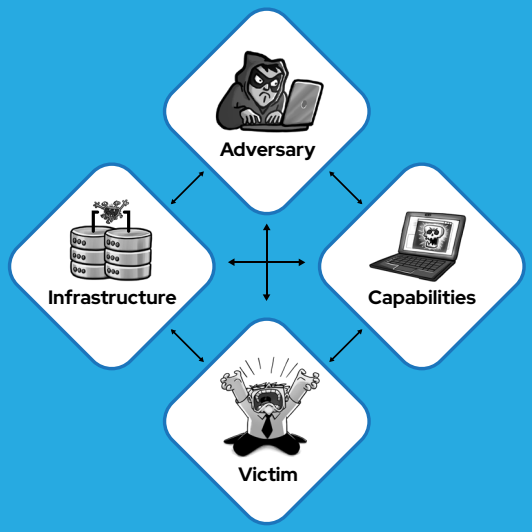
Who: Likely a financially motivated cybercriminal group or threat actors using TrickBot as a tool to conduct phishing, steal credentials, and deploy other malware such as ransomware.

How:

Malspam: Used to deliver TrickBot via phishing emails containing malicious attachments (e.g., Word/Excel files).

Command and Control (C2) Servers: TrickBot communicates with its C2 infrastructure to receive instructions, download additional modules, and exfiltrate stolen data.

Tools: TrickBot utilized built-in system tools (e.g., PowerShell, WMIC) and third-party utilities (like Sysinternals ProcDump) to perform reconnaissance, persistence, and data exfiltration.



What:

Credential Theft: TrickBot dumps the LSASS process and uses registry edits to steal authentication data. Process

Injection: Injects into legitimate processes (e.g., wermgr.exe) to evade detection.

Reconnaissance: Uses network discovery tools like net.exe and ipconfig.exe to gather information on the compromised network.

Persistence: Creates scheduled tasks and deploys a fake 1Password installer to maintain presence and mask further malicious activity.

Who: The target could be both individual users and organizations

Environment: Typically targets Windows systems and organizations with networked environments, making it easier for TrickBot to move laterally and exfiltrate data.

Conclusion

Summary Findings

Password managers are essential tools for security but are increasingly targeted by cybercriminals. Infostealers, such as Meduza Stealer and Stealc, aim to steal sensitive data from password managers and other applications. Attackers use phishing, malvertising, and social engineering tactics to gain access to users' credentials and valuable information.

Emerging Threats:

1. Infostealers: Malware such as Meduza, Lumma, and ACR exploit vulnerabilities like CVE-2024-21412 in Microsoft Defender SmartScreen to bypass security checks, infecting devices to steal data from browsers, crypto wallets, messaging apps, and password managers like Bitwarden and 1Password.

2. Malvertising: This technique involves placing malicious ads, tricking users into downloading fake password managers or remote desktop managers. ZenRat is a notable example, distributed through cloned websites and phishing emails to steal user credentials.

Sophisticated Campaigns:

3. ZenRat Malware: Distributed through fake Bitwarden installers, ZenRat hijacks user credentials and sensitive data by leveraging malvertising on platforms like Google Ads.

4. FakeBat Malware: Uses drive-by download techniques to exploit browser vulnerabilities and deliver additional malicious payloads.

5. TrickBot: A sophisticated attack involving TrickBot malware, which installed a fake 1Password application to enable deeper infiltration and malware delivery through tools like Cobalt Strike.

Final Recommendations

Malware like Citadel, Arkei, and Racoon Stealer are increasingly targeting password managers such as Bitwarden, LastPass, and KeePassXC. Although these infostealers can capture active passwords, they don't retrieve all stored passwords at once. We've observed a rising number of infostealers like Meduza Stealer appearing on dark web platforms, reflecting the increasing trend of malware-as-aservice, which enables less skilled criminals to more easily launch cyberattacks.

To avoid password-stealing trojans, don't fall for social engineering tricks, as most are installed when users unknowingly run something malicious. Regularly patch your software, especially those listed on CISA's Known Exploited Vulnerability Catalog. Despite the threats targeting password managers, we still recommend using one to prevent greater risks like password reuse or weak passwords. While password managers aren't completely foolproof, they significantly reduce the chances of compromise by addressing these bigger vulnerabilities, which are far more likely to be exploited than the password manager itself.

MITRE ATT&CK

ZenRat

Tactic	Technique (MITRE ATT&CK)	Description
Initial Access	Malvertising (T1598)	Distributed via malicious ads and cloned websites.
Execution Credential	Phishing (T1566)	Uses phishing emails to lure victims to fake sites.
Access Defense	Credential Dumping (T1003)	Steals user credentials, including from password managers.
Defense Evasion	Obfuscated Files or Information (T1027)	Uses obfuscation to evade detection.
Exfiltration	Exfiltration Over C2 Channel (T1041)	Transmits stolen data to command-and-control servers.

FakeBot

Tactic	Technique (MITRE ATT&CK)	Description
Initial Access	Drive-by Download (T1189)	Distributed via compromised websites or malicious browser updates.
Execution	Process Injection (T1055)	Injects itself into legitimate processes to evade detection.
Persistence	Persistence via Scheduled Task/Job (T1053)	Establishes persistence by creating scheduled tasks.
Credential Access	Credential Dumping (T1003)	Steals credentials by capturing input from various applications.
Defense Evasion	Command and Scripting Interpreter (T1059)	Uses malicious scripts for execution, such as PowerShell.

RomCom

Tactic	Technique (MITRE ATT&CK)	Description
Initial Access	Phishing (T1566)	Uses spear-phishing emails leading to trojanized software downloads.
Persistence	Typosquatting (T1596.002)	Sets up fake domains resembling legitimate software sites.
Execution	Trojanized Software (T1072)	Uses altered versions of legitimate software to deliver malware.
Command and Control	Command and Control via Encrypted Channel (T1573)	Communicates with C2 servers using encrypted traffic.
Exfiltration	Exfiltration Over Web Service (T1567)	Transfers stolen data through secure, encrypted channels.

LastPass Incident

Tactic	Technique (MITRE ATT&CK)	Description
Reconnaissance	Gather Victim Identity Information (T1589)	Attackers likely gathered information on LastPass employees with privileged access.
Initial Access	Phishing (T1566)	Phishing emails sent to a Senior DevOps engineer to gain initial access.
Execution	Exploitation for Client Execution (T1203)	Keylogger was installed after phishing email, exploiting the system.
Persistence	Account Manipulation (T1098)	Keylogger installed to maintain persistence and monitor the engineerâ€™s activity.
Privilege Escalation	Valid Accounts (T1078)	Attackers used the stolen credentials to access privileged systems.
Defense Evasion	Obfuscated Files or Information (T1027)	Attackers used techniques to evade detection and blend with legitimate network traffic.
Credential Access	Input Capture (T1056)	Captured master password as it was entered during authentication.
Discovery	System Information Discovery (T1082)	Attackers gathered information about the compromised environment.
Lateral Movement	Remote Services (T1021)	Used compromised credentials to move laterally across the network.
Exfiltration	Exfiltration Over C2 Channel (T1041)	Transferred stolen encrypted vaults and metadata over encrypted channels.

TrickBot

Tactic	Technique (MITRE ATT&CK)	Description
Initial Access	Phishing (T1566)	Delivered through phishing emails with malicious attachments or links.
Execution	Process Injection (T1055)	Injects malicious code into legitimate processes to evade detection.
Credential Access	Credential Dumping (T1003)	Steals credentials by dumping memory from processes like LSASS.
Lateral Movement	Remote Services (T1021)	Uses compromised credentials to move laterally within a network.
Persistence	Scheduled Task/Job (T1053)	Establishes persistence through scheduled tasks or jobs.
Defense Evasion	Obfuscated Files or Information (T1027)	Obfuscates malicious code to evade detection by security tools.

CONTACT DEVOLUTIONS

Based in Lavaltrie, Québec, Canada, Devolutions delivers productivity and security solutions to more than 800,000 IT professionals and business end users in over 140 countries worldwide. Please direct your inquiries and free trial requests to us via the following:

Email: sales@devolutions.net

Phone: +1 844 463.0419

Live Chat via our Website: https://devolutions.net/