Lumma Stealer: Advanced Threat Analysis & Protection Guide 2026

By Gridinsoft LLC

Archived: 2026-04-05 14:04:29 UTC

You download what looks like an innocent software crack or click a link from someone on Discord. Hours later, your cryptocurrency wallets are emptied, banking credentials stolen, and accounts compromised. This isn't random bad luck—you've encountered Lumma Stealer, an increasingly sophisticated information-stealing malware that's rapidly becoming one of the most dangerous threats to personal and financial data.

What is Lumma Stealer?

Lumma Stealer (also known as LummaC2) is a sophisticated information-stealing malware that emerged in late 2022, with widespread distribution beginning in early 2023. Written in C++, it's specifically designed to harvest sensitive data from infected systems, with a particular focus on cryptocurrency wallets, browser credentials, and two-factor authentication (2FA) extensions.

Developed by a threat actor known as "Shamel" (operating under the alias "Lumma"), this malware is distributed through a Malware-as-a-Service (MaaS) model on Russian-speaking cybercriminal forums. What sets Lumma apart from other stealers is its exceptional evasion capabilities, rapid development cycle, and focus on cryptocurrency theft.

Lumma Stealer Key Features

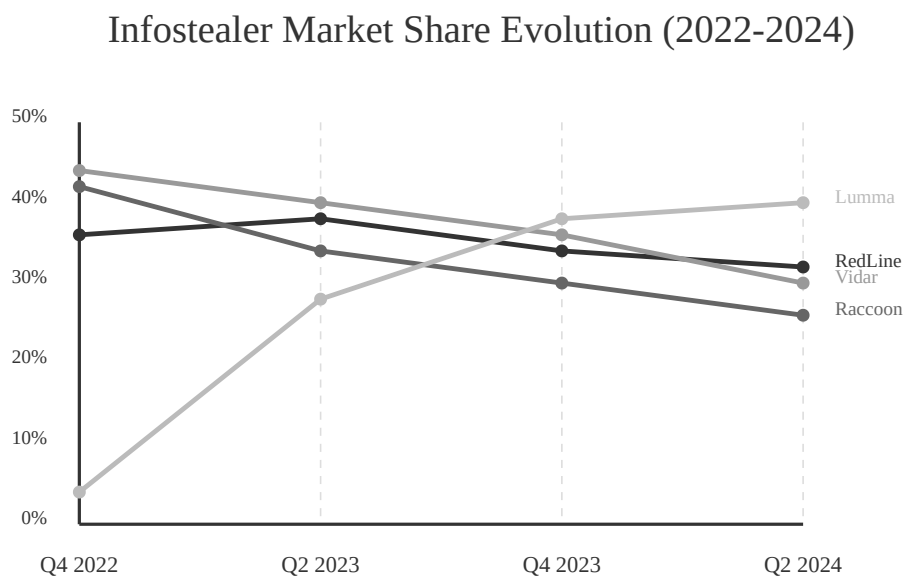
- Advanced anti-analysis techniques to evade security software
- Comprehensive browser data theft (passwords, cookies, form data)
- Cryptocurrency wallet targeting (40+ wallets supported)
- Two-factor authentication (2FA) extension theft
- Multiple infection vectors including cracked software, Discord, and email

- Sophisticated command and control infrastructure
- Regular updates and feature additions

Information stealers like Lumma represent one of the fastest-growing threats to personal and enterprise data security, with a 135% increase in detections throughout 2023.

Lumma Stealer: Evolution and Impact

Within months of its initial appearance, Lumma Stealer achieved remarkable success in the cybercriminal ecosystem. By mid-2023, darknet forums were offering Lumma logs (stolen data packages) at volumes comparable to established players like Vidar and Raccoon Stealer.



Source: Analysis of darknet forum offerings and security reports from 2022-2024

Lumma's rise coincides with an increase in cryptocurrency-related theft. According to the CISA cybersecurity advisory, information stealers like Lumma have contributed to over $5.2 billion in cryptocurrency theft since 2022.

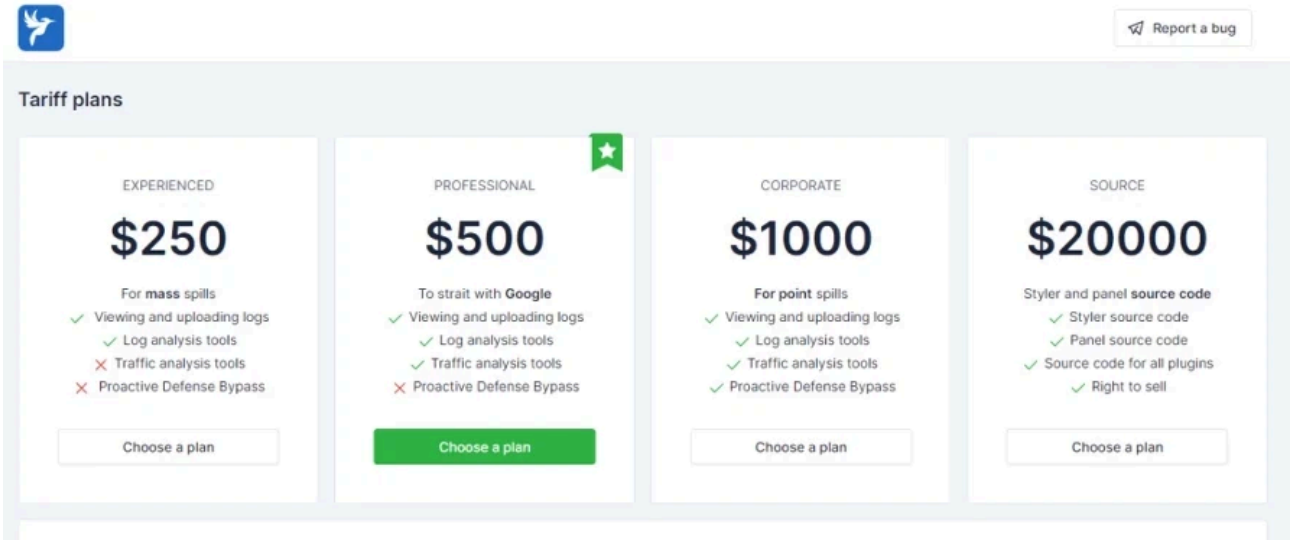
Commercial Offering and Pricing Structure

Lumma Stealer operates on a subscription-based model with different pricing tiers:

- **Basic Package:** $250/month
- **Premium Package:** $500/month

- **Enterprise Package:** $1000/month
- **Lifetime Access:** $5000 (one-time)

The higher-tier packages include additional features such as persistent cookie stealing (allowing access to accounts even after password changes), AI-assisted log filtering, custom builds with enhanced evasion, and dedicated customer support.



Subscription plans advertised on a Darknet forum

Lumma Stealer Infection Vectors

Lumma Stealer employs multiple distribution methods to maximize its reach. Each approach is carefully tailored to appear legitimate and bypass user suspicion.

1. Cracked Software and Pirated Applications

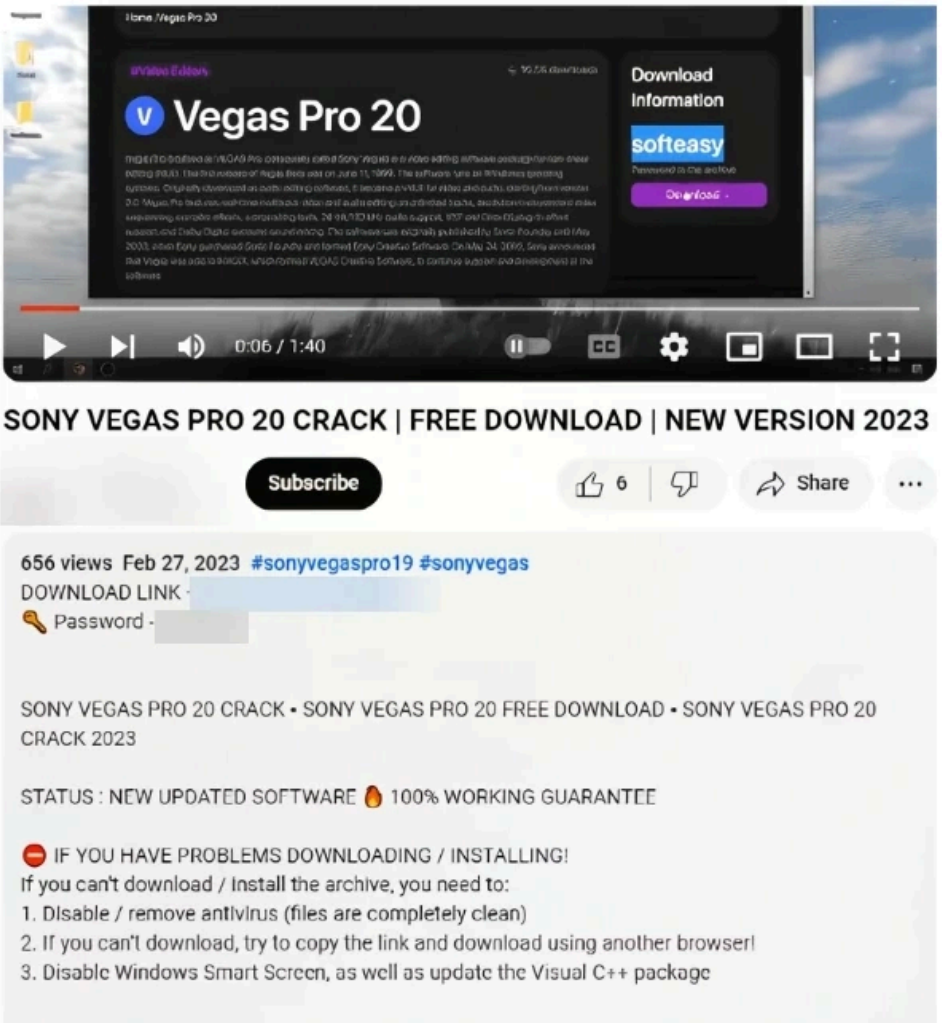
The most common vector for Lumma Stealer infections is through cracked software distribution. This method is particularly effective because:

- Users downloading pirated software often intentionally disable security tools
- Cracked software is expected to trigger some security warnings, making users more likely to ignore them
- The installation process provides cover for malware execution

Threat actors employ SEO poisoning to promote malicious websites offering free versions of popular software. When users download and execute these pirated applications, a staged loader downloads and executes the Lumma Stealer payload.

Hacked YouTube Channels Campaign (January 2024)

In January 2024, security researchers identified a sophisticated campaign where threat actors compromised YouTube accounts with substantial followings. These hacked channels posted videos promoting free software, with download links leading to Lumma Stealer installers.

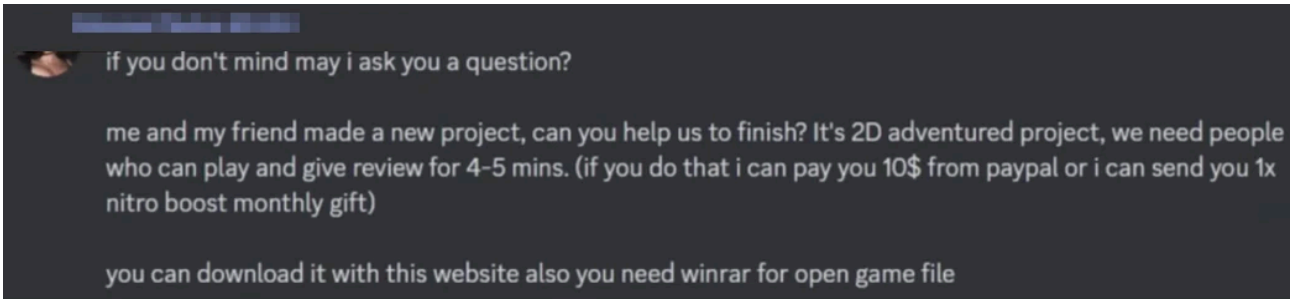


Compromised YouTube channel promoting malicious download

2. Discord Social Engineering

Discord has become a prime target for Lumma Stealer distribution due to its popularity among gamers and cryptocurrency enthusiasts. The attack typically follows this pattern:

1. Attackers join popular Discord servers or send unsolicited direct messages
2. They build rapport or immediately send messages with malicious links/files
3. Messages often disguise payloads as game mods, cheat tools, or free software
4. When executed, the payload connects to the command server to download Lumma Stealer



Discord message promoting malware disguised as a game that needs testing

3. Phishing Emails and Malicious Attachments

While less common than the previous methods, phishing emails remain an effective distribution vector for Lumma Stealer. These typically take the form of:

- Fake invoice or shipping notification emails with malicious attachments
- Spear-phishing campaigns targeting specific individuals or organizations
- Fake job offers with "application forms" containing embedded malware

4. Fake CAPTCHA Pages

A more recent infection method involves redirecting users to fake CAPTCHA verification pages. According to Trojan Killer security analysis, these pages claim to verify that the visitor is human but actually trigger the download of malicious JavaScript that ultimately deploys Lumma Stealer.

Lumma Stealer Technical Analysis

Lumma Stealer employs a sophisticated multi-stage infection process designed to evade detection and analysis.

Infection Chain Overview

Typical Lumma Stealer Attack Sequence

---

1. **Initial Access:** User downloads crack/malicious file or clicks on compromised link
2. **Stage 1 Loader:** Typically a PowerShell or JavaScript downloader with basic obfuscation
3. **Environment Checks:** Verifies the system is not a virtual machine or analysis environment
4. **Payload Download:** Retrieves the encrypted Lumma DLL from the C2 server
5. **Process Injection:** Injects malicious code into legitimate Windows processes
6. **Data Collection:** Harvests credentials, cookies, crypto wallets, and system information
7. **Data Exfiltration:** Encrypts and sends stolen data to the C2 server
8. **Self-Cleanup:** Removes evidence of infection (optional feature)

The initial infection typically begins with a staged loader—a small script that performs preliminary system checks before downloading the main Lumma Stealer payload. This approach provides multiple advantages:

- Smaller initial file size, which is less likely to trigger security alerts
- Ability to customize the payload based on the victim's system configuration
- Option to abort the infection if security tools or analysis environments are detected

What makes Lumma especially interesting is its use of GitHub profiles as intermediary command and control servers. This technique allows the malware to disguise its traffic as legitimate GitHub API requests, making detection more difficult.

Detection Evasion Techniques

Lumma Stealer employs an extensive array of anti-analysis techniques to evade detection by security solutions and researchers. These evasion methods have significantly contributed to its rapid rise in popularity among cybercriminals.

Anti-VM and Anti-Sandbox Techniques

Upon execution, Lumma conducts thorough system checks to determine if it's running in a virtualized environment or analysis sandbox. The malware calls the Windows function *GetForegroundWindow* to check for debugging tools by comparing window titles against known debuggers:

- IDA Pro
- HyperDbg
- x32dbg / x64dbg
- Any window with "debug" in the title

- Cheat Engine
- WinDbg
- OllyDbg
- Immunity Debugger
- dnSpy

Lumma also checks for sandbox environments by scanning for DLLs associated with security tools such as:

- 360 Total Security
- Sandboxie
- Cuckoo Sandbox
- Comodo Containment

To evade Wine-based analysis (used in some Linux analysis environments), Lumma searches for the *wine_get_unix_file_name* API in kernel32.dll or ntdll.dll.

Username and System Property Analysis

Continuing its anti-analysis efforts, Lumma examines usernames for common sandbox indicators:

- CurrentUser
- Virus
- Sandbox
- test user

- malware
- maltest
- WDAGUtilityAccount
- John Doe

The malware also examines system properties for virtualization indicators:

- Checks .sys files in system32 for virtualization drivers
- Scans device identifiers for generic VM vendor names
- Inspects running services for VM-related processes
- Analyzes hardware information for virtualization artifacts

If any of these checks indicate an analysis environment, Lumma terminates execution to prevent researchers from studying its behavior.

Code Obfuscation and Encryption

Lumma employs sophisticated obfuscation techniques to hide its malicious code:

- **String Encryption:** All hardcoded strings are encrypted to avoid static analysis
- **Control Flow Obfuscation:** Code flow is deliberately complicated with junk instructions
- **Payload Concealment:** Encrypted payload is stored in PNG resource files
- **API Call Hiding:** Windows API calls are resolved dynamically at runtime

These techniques make static analysis and signature-based detection extremely difficult.

Data Theft Capabilities

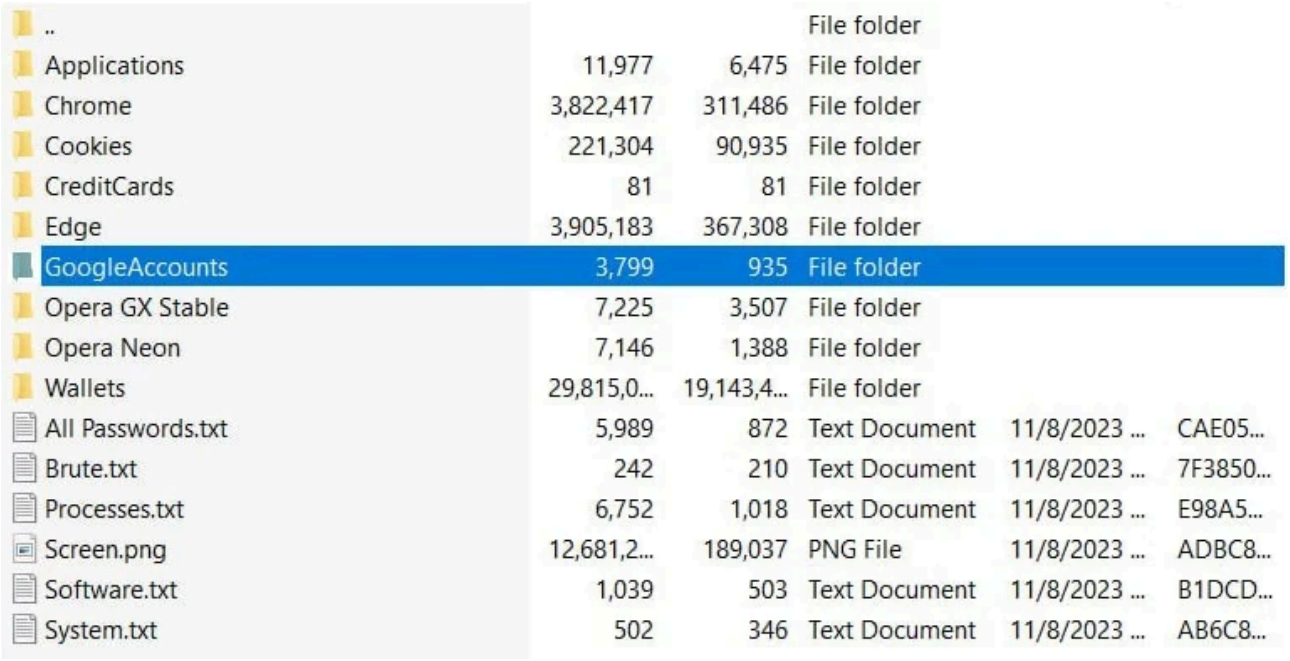
After bypassing security measures, Lumma Stealer focuses on its primary objective: harvesting valuable data from the infected system.

Communication with Command & Control

Before beginning data collection, Lumma establishes communication with its command and control (C2) server. Each sample contains encrypted addresses for the primary C2 server and multiple backup servers. The malware tests each server in sequence until it finds a responsive one.

Communication with the C2 server uses encrypted HTTP POST requests. This approach allows the malware to blend in with legitimate web traffic, making network-based detection more difficult.

Data Collection Targets



..			File folder		
Applications	11,977	6,475	File folder		
Chrome	3,822,417	311,486	File folder		
Cookies	221,304	90,935	File folder		
CreditCards	81	81	File folder		
Edge	3,905,183	367,308	File folder		
GoogleAccounts	3,799	935	File folder		
Opera GX Stable	7,225	3,507	File folder		
Opera Neon	7,146	1,388	File folder		
Wallets	29,815,0...	19,143,4...	File folder		
All Passwords.txt	5,989	872	Text Document	11/8/2023 ...	CAE05...
Brute.txt	242	210	Text Document	11/8/2023 ...	7F3850...
Processes.txt	6,752	1,018	Text Document	11/8/2023 ...	E98A5...
Screen.png	12,681,2...	189,037	PNG File	11/8/2023 ...	ADBC8...
Software.txt	1,039	503	Text Document	11/8/2023 ...	B1DCD...
System.txt	502	346	Text Document	11/8/2023 ...	AB6C8...

Example of data collected by Lumma Stealer

Lumma Stealer targets an extensive range of data sources:

Browser Data

- **Credentials:** Usernames and passwords from all major browsers
- **Cookies:** Browser cookies, including persistent authentication cookies
- **Autofill Data:** Saved addresses, credit cards, and form data
- **Browsing History:** Complete browsing history logs

Cryptocurrency Data

- **Wallet Extensions:** Data from 40+ browser-based crypto wallet extensions
- **Wallet Files:** Local cryptocurrency wallet files and keys
- **Wallet Applications:** Data from desktop cryptocurrency applications

System Information

- **Hardware Details:** CPU, RAM, GPU specifications
- **Software Inventory:** Installed applications and versions
- **Network Configuration:** IP address, hostname, MAC address
- **User Information:** Username, language settings, time zone

```
        "t": 0,
        "p": "%userprofile",
        "m": "*bitcoin*",
        "z": "Important Files/Profile",
        "d": 3
},
{
        "t": 0,
        "p": "%userprofile",
        "m": "*binance*",
        "z": "Important Files/Profile",
        "d": 3
},
{
        "t": 0,
        "p": "%userprofile",
        "m": "*exodus*",
        "z": "Important Files/Profile",
        "d": 3
},
{
        "t": 0,
        "p": "%userprofile",
        "m": "*coinbase*",
        "z": "Important Files/Profile",
        "d": 3
{
        "p": "%localappdata%\\Google\\Chrome\\User Data",
        "z": "Chrome"
},
{
        "p": "%localappdata%\\Chromium\\User Data",
        "z": "Chromium"
},
{
        "p": "%localappdata%\\Microsoft\\Edge\\User Data",
        "z": "Edge"
},
{
        "p": "%localappdata%\\Kometa\\User Data",
        "z": "Kometa"
},
{
        "p": "%localappdata%\\Opera Software\\Opera Stable",
        "z": "Opera"
},
{
        "p": "%localappdata%\\Opera Software\\Opera GX Stable",
        "z": "Opera GX Stable"
},
{
```

Code segment specifying browser and crypto wallet targets

The premium version of Lumma includes capabilities to steal persistent cookies, which maintain user sessions even after password changes. This feature allows attackers to maintain access to compromised accounts even after the victim changes their credentials.

Data Exfiltration

After collecting data, Lumma compresses and encrypts it before transmission to the C2 server. The encryption ensures that network security solutions cannot easily identify the stolen information as it leaves the network.

According to Gridinsoft security research, Lumma Stealer employs a sophisticated C2 panel with AI-assisted filtering to organize stolen data and identify the most valuable targets. This filtering helps attackers prioritize high-value victims for further exploitation.

Warning Signs of Lumma Stealer Infection

Detecting a Lumma Stealer infection can be challenging due to its stealthy nature, but several indicators may suggest your system has been compromised:

System Performance Issues

- Unexplained system slowdowns, especially during browsing sessions
- Increased CPU usage when no resource-intensive applications are running
- Browser crashes or unusual behavior when accessing secure websites

Account Security Anomalies

- Unexpected account logouts or password reset notifications
- Unauthorized transactions in financial accounts or cryptocurrency wallets
- Login notification emails from services you didn't access
- Two-factor authentication prompts you didn't initiate

Suspicious Network Activity

- Unusual outbound connections to unfamiliar IP addresses
- Increased network activity when the system should be idle
- Browser extensions you don't remember installing

If you notice any of these warning signs, it's crucial to take immediate action to verify and address a potential infection.

How to Remove Lumma Stealer

If you suspect your system has been infected with Lumma Stealer, follow these steps to remove the malware and secure your accounts:

Windows Removal Steps

---

1. Disconnect from the internet to prevent further data exfiltration
2. Boot into Safe Mode with Networking (restart while holding Shift, then Troubleshoot → Advanced options → Startup Settings → Restart → press F5)
3. Run a full system scan with an updated anti-malware solution
4. Remove any identified threats following your security software's recommendations
5. Check Task Manager for unusual processes and remove any suspicious startup items
6. Reset all browsers or reinstall them completely

For more comprehensive removal, consider using specialized anti-malware tools:

- GridinSoft Anti-Malware - Our specialized tool with infostealer detection capabilities
- Microsoft Defender - Built-in Windows security with regular updates for new threats

Post-Infection Security Measures

After removing Lumma Stealer, take these critical steps to secure your accounts and prevent further damage:

1. **Change all passwords** from a clean device (not the previously infected one)
2. **Enable two-factor authentication** on all accounts that support it
3. **Monitor financial accounts** for unauthorized transactions
4. **Revoke and reissue API keys** for developer accounts
5. **Create new cryptocurrency wallets** and transfer funds from potentially compromised wallets
6. **Check browser extensions** and remove any you don't recognize

How to Protect Against Lumma Stealer

Preventing a Lumma Stealer infection is far easier than dealing with its aftermath. Implement these security practices to protect your system:

Software and System Security

- **Avoid pirated software and cracks** - The most common Lumma infection vector
- **Keep your operating system and applications updated** with the latest security patches
- **Use a reputable security solution** with real-time protection
- **Enable Windows Defender SmartScreen** to block malicious downloads
- **Implement application control policies** in enterprise environments

Safe Browsing Practices

- **Be skeptical of unsolicited messages** on Discord, social media, or email
- **Verify software downloads** by using official websites only
- **Check URLs carefully** before entering credentials or downloading files
- **Avoid clicking on suspicious links**, especially those promising free software
- **Be wary of fake CAPTCHA pages** that prompt you to run code or download files

Cryptocurrency Security

- **Use hardware wallets** for storing significant cryptocurrency assets
- **Implement separate browsing environments** for financial activities
- **Consider a dedicated device** for cryptocurrency transactions
- **Regularly audit installed browser extensions**

For enterprise environments, consider implementing these additional protections as recommended by Microsoft Security:

- Restrict PowerShell and script execution using AppLocker or Windows Defender Application Control
- Deploy network monitoring solutions to detect suspicious outbound connections
- Implement least privilege access controls to limit the impact of compromised accounts
- Conduct regular security awareness training focusing on current social engineering tactics

Lumma Stealer Indicators of Compromise (IoC)

Security professionals can use these indicators to identify potential Lumma Stealer infections in their environment:

Operation	MITRE ATT&CK Techniques
Information collection	T1217: Browser Information Discovery T1083: File and Directory Discovery

Operation	MITRE ATT&CK Techniques
Executed the encrypted payload using powershell.exe	T1059.001: Command and Scripting Interpreter: PowerShell T1027.013: Obfuscated Files or Information: Encrypted/Encoded File
PowerShell downloaded Lumma Stealer and executed	T1059.001: Command and Scripting Interpreter: PowerShell
Executed the initial PS code	T1204: User Execution T1059.001: Command and Scripting Interpreter: PowerShell
Download the payload using mshta, which had overlayed script	T1218.005: System Binary Proxy Execution: Mshta T1027.009: Obfuscated Files or Information: Embedded Payloads
Lumma Injected malicious payload in BitLockerToGo	T1055.012: Process Injection: Process Hollowing
Injected process executed killing.bat script	T1059.003: Command and Scripting Interpreter: Windows Command Shell
Batch script discover the process and start autoit	T1057: Process Discovery
Autoit executes the script	T1059.010: Command and Scripting Interpreter: AutoIT
Fake captcha verification	T1566: Phishing
Exfiltration	T1041: Exfiltration Over C2 Channel

Commonly Used C2 Domains and IP Addresses

Security teams should monitor for connections to these known Lumma Stealer command and control servers:

176.113.115.224
176.113.115.226
176.113.115.227
176.113.115.229
176.113.115.232
144.76.173.247
45.9.74.78

77.73.134.68
82.117.255.127
82.117.255.80
82.118.23.50

Suspicious Domains

These domains have been associated with Lumma Stealer distribution campaigns:

futureddospzmvq[.]shop
writerospzm[.]shop
mennyudosirso[.]shop
deallerospfosu[.]shop
quialitsuzoxm[.]shop
complaintsipzzx[.]shop
bassizcellskz[.]shop
languagedscie[.]shop
celebratioopz[.]shop

Related Resources

For more detailed information about Lumma Stealer and similar threats, refer to these resources:

- Fake CAPTCHA Sites Trick Users to Run Lumma Stealer
- Lumma Stealer Spreads Via Fake Browser Updates
- How to Detect, Remove, and Prevent Infostealer Infections
- Comprehensive Malware Removal Guide
- Spyware Removal and Protection

Source: https://gridinsoft.com/spyware/lumma-stealer