Lumma Stealer Campaign Targets League of Legends World Championship Fans Through Social Media Ads

By Alina BÎZGĂ

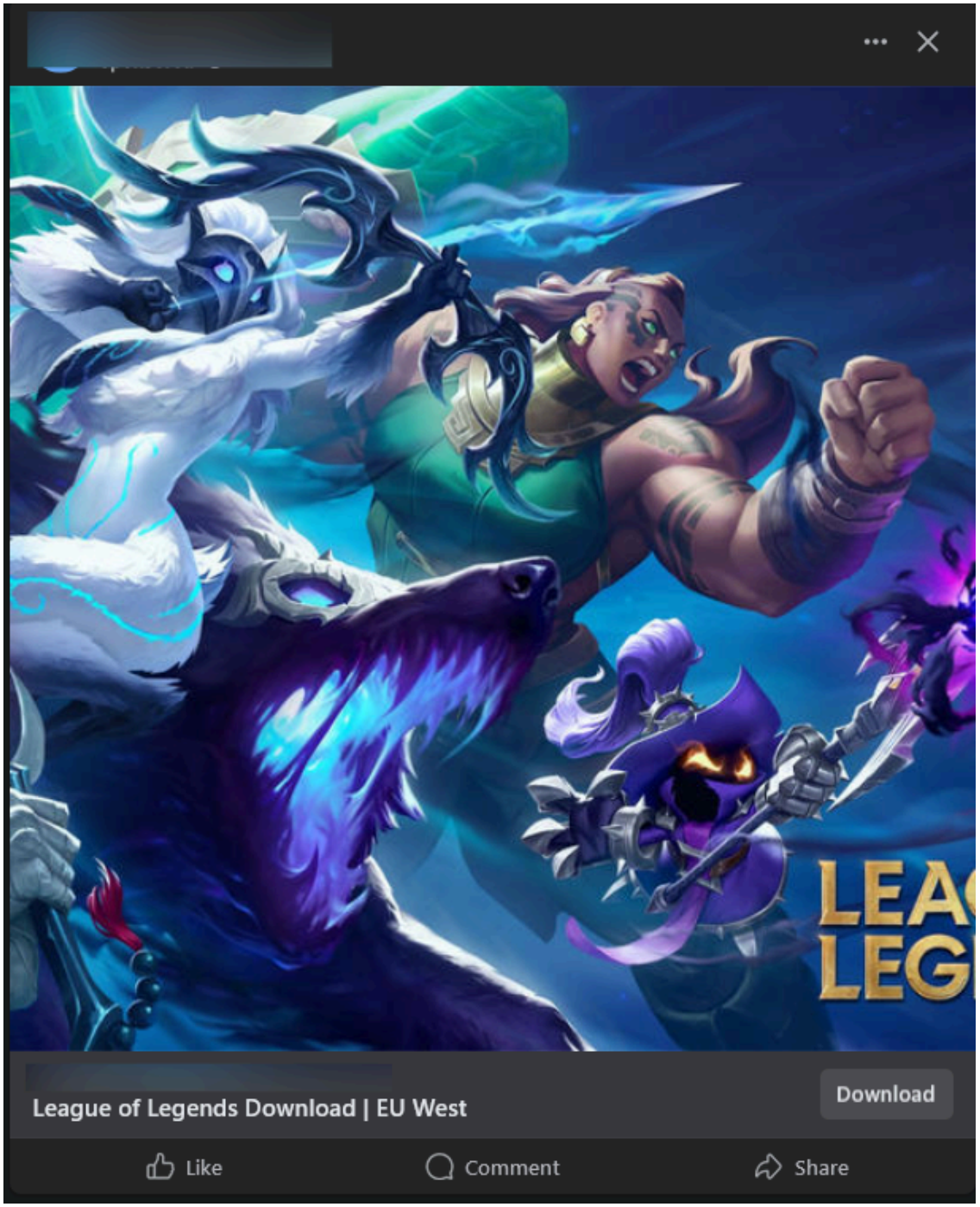
Archived: 2026-04-05 20:40:13 UTC

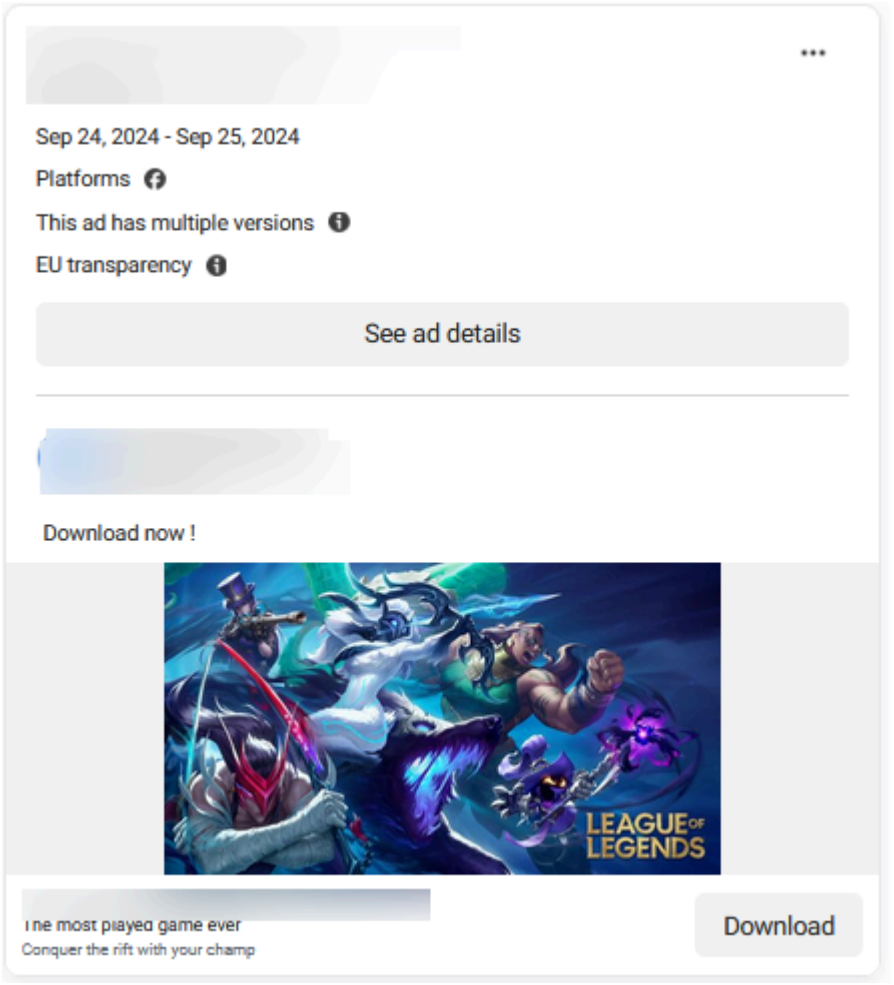
As the League of Legends (LoL) World Championship kicks off, Bitdefender Labs is warning that cybercriminals are exploiting the event to launch sophisticated malware campaigns targeting unsuspecting gamers across Europe.

Through carefully crafted social media advertisements, hackers are enticing fans to download what appears to be the popular multiplayer online battle arena (MOBA) game. However, what awaits victims is not a fun gaming experience, but rather a dangerous piece of malware known as Lumma Stealer.

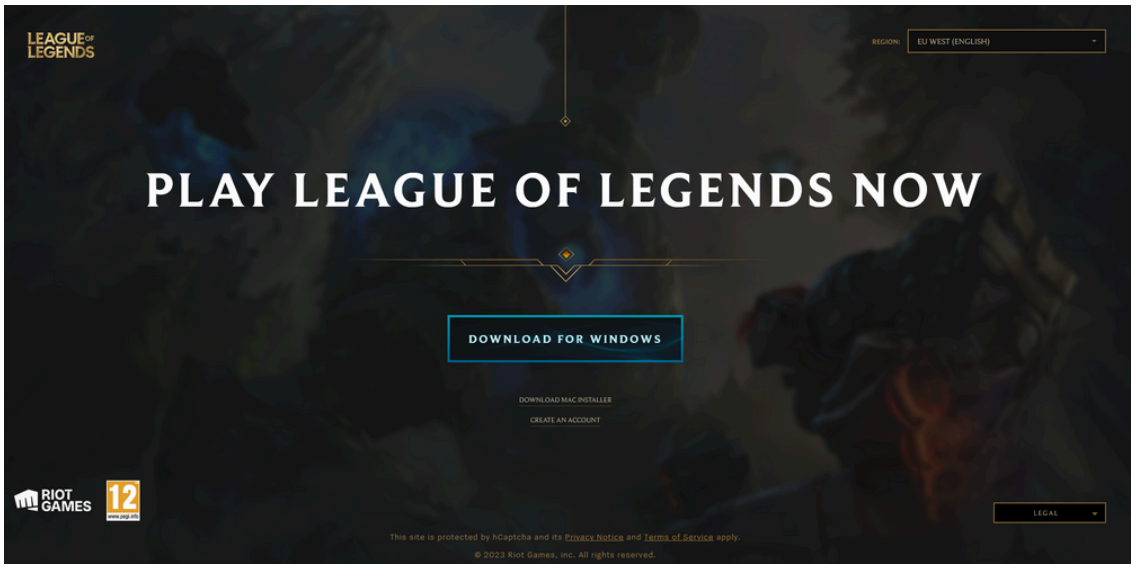
The Malicious Campaign

The malvertisement campaign, spotted by Bitdefender Labs researcher Ionut Baltariu, promotes a free download of League of Legends, which is ironic since the PC-only game is already free to play. However, with the LoL World Championship capturing the attention of millions of gamers, the timing is perfect for cybercriminals. Fans eager to immerse themselves in the excitement may fall for this trap, assuming it is an official promotion tied to the official e-sports event.


League of Legends Download | EU West
Download
Like
Comment
Share



Upon clicking the ad, victims are taken to a page that mimics an older version of the League of Legends download page.



This phishing page uses typosquatting, a technique where the domain is slightly altered to resemble the official site, making it harder to detect. Once the user clicks the download link, they are directed to a Bitbucket repository that contains a malicious archive.

The Malicious Payload: Lumma Stealer

According to Bitdefender Lab researcher Andrei Mogage, the downloaded archive contains an executable along with a legitimate Windows file, *user32.dll*. The executable acts as a dropper for the Lumma Stealer, a dangerous piece of malware known for its extensive ability to harvest data from infected devices.

Lumma Stealer is one of the many types of data-stealing malware that can be rented or bought on underground forums as part of the MaaS (Malware-as-a-Service) economy. It's designed to extract a wide range of sensitive information, including:

- Passwords
- Credit card details
- Cryptocurrency wallets
- Browser session cookies

What makes Lumma particularly dangerous is its stealthy approach. Once deployed, it injects itself into a legitimate Windows process, *bitlockertogo.exe*, to remain undetected by basic antivirus software.

Stolen Data and Its Impact

This malvertising campaign has already targeted over 4000 people, focusing primarily on male adults—the typical demographic for League of Legends. Once cybercriminals access sensitive information, they can steal social media accounts, which allows them to perpetuate malware distribution and other scams through compromised profiles. Stolen data can also be sold on underground markets which can facilitate identity theft and phishing attacks against victims.

How to Protect Yourself: Bitdefender as a Shield Against Malvertising

Adopting strong cybersecurity practices is crucial to protecting yourself from falling victim to this or similar malware campaigns.

- **Always verify URLs:** Before clicking any links, especially from ads you see on Facebook, double-check the URL for misspellings or inconsistencies.
- **Avoid downloading software from unofficial sources:** Always download games and software from official websites or platforms like Steam.
- **Be cautious with online ads:** Cybercriminals often use legitimate-looking ads to trick users into visiting harmful websites or handing over personal information
- **Use security software:** Reliable antivirus and security tools can help detect and block malicious files and phishing attempts.

One of the most effective ways to safeguard against Lumma malware and other online threats is to use a trusted security solution like **Bitdefender**.

Bitdefender detects and blocks the malicious executable *as* ***Trojan.Agent.GMTH***.

Bitdefender security solutions **provide** industry-leading protection against malicious ads, phishing websites, and malware that often lurks behind seemingly legitimate online promotions through:

1. **Real-Time Threat Detection:** Bitdefender's advanced algorithms can detect malicious activity in real-time, blocking harmful websites and suspicious ads before they have a chance to infect your system.
2. **Web Protection:** Bitdefender's anti-phishing and anti-fraud features ensure that you never fall prey to typosquatted domains or fake download pages. By analyzing website URLs, Bitdefender can flag and block any malicious attempts to mimic legitimate sites like League of Legends.
3. **Multi-Layered Ransomware Protection:** Should malware like Lumma Stealer try to deploy additional payloads such as ransomware, Bitdefender's multi-layered defenses will stop the threat in its tracks, ensuring that your login credentials, financial information, and social media accounts remain secure.
4. **Automatic Updates:** Having up-to-date protection is essential in today's threat landscape. Bitdefender continuously updates its virus databases to ensure your system stays protected from the latest threats, including malware distributed via malvertising campaigns.

For on-demand checks of scams or potentially malicious and fraudulent content, why not give Bitdefender Scamio a try for free!

Our next-gen AI scam detector is always ready to help you instantly check links, QR codes or even screenshots to get an instant analysis.

Scamio can be accessed on any device or operating system via **web browser**, **Facebook Messenger**, or **WhatsApp**. You can also help others stay safe by sharing Scamio with them in France, Germany, Spain, Italy, Romania, Australia, and the UK

With **Bitdefender's** **suite of security products**, you can browse, play, and connect online without worrying about lurking threats in the background. You can enjoy the perks of customizable user profiles designed to reduce system workload and slowdowns for an uninterrupted gaming experience.

We'll temporarily halt pop-ups and alerts and postpone any automatic updates or scheduled systems scans so you can fully enjoy your game session while continuing to benefit from award-winning threat detection.
