Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool

blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

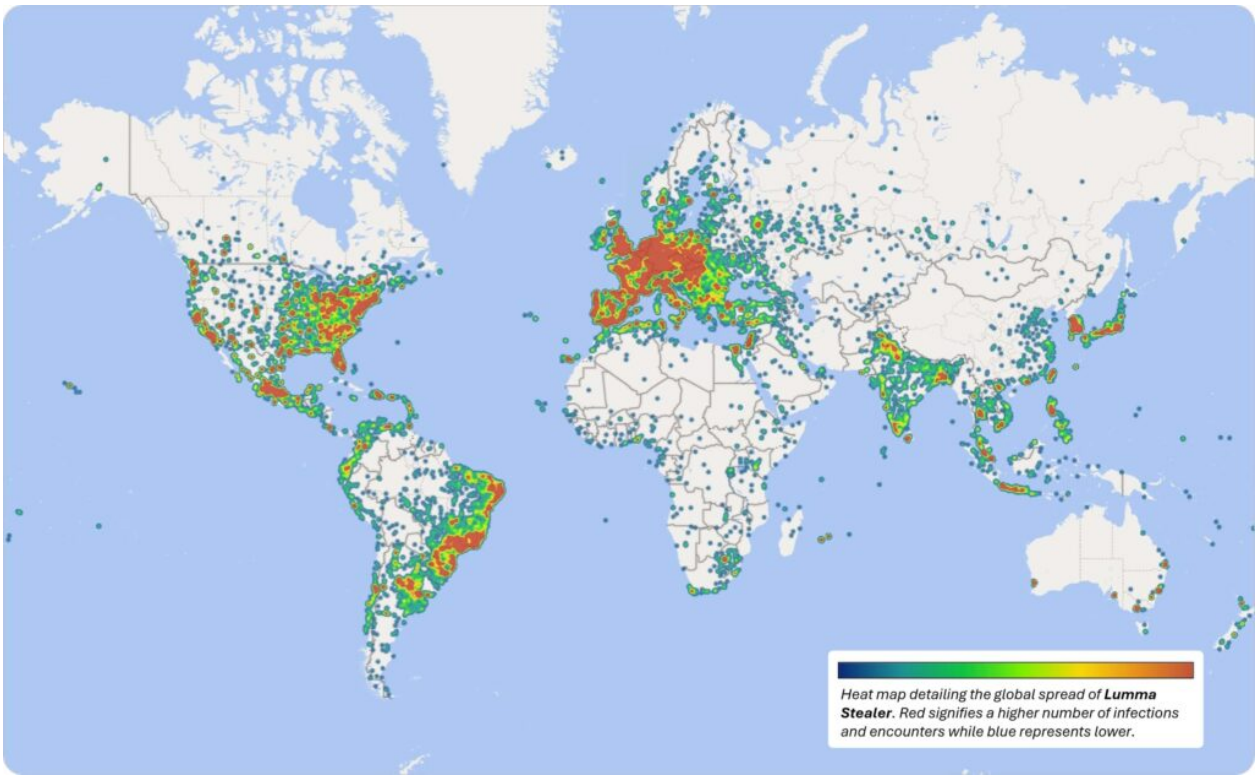
May 21, 2025

Microsoft's Digital Crimes Unit (DCU) and international partners are disrupting the leading tool used to indiscriminately steal sensitive personal and organizational information to facilitate cybercrime. On Tuesday, May 13, Microsoft's DCU filed a legal action against Lumma Stealer ("Lumma"), which is the favored info-stealing malware used by hundreds of cyber threat actors. Lumma steals passwords, credit cards, bank accounts, and cryptocurrency wallets and has enabled criminals to hold schools for ransom, empty bank accounts, and disrupt critical services.

Via a court order granted in the United States District Court of the Northern District of Georgia, Microsoft's DCU seized and facilitated the takedown, suspension, and blocking of approximately 2,300 malicious domains that formed the backbone of Lumma's infrastructure. The Department of Justice (DOJ) simultaneously seized the central command structure for Lumma and disrupted the marketplaces where the tool was sold to other cybercriminals. Europol's European Cybercrime Center (EC3) and Japan's Cybercrime Control Center (JC3) facilitated the suspension of locally based Lumma infrastructure.

Between March 16, 2025, and May 16, 2025, Microsoft identified over 394,000 Windows computers globally infected by the Lumma malware. Working with law enforcement and industry partners, we have severed communications between the malicious tool and victims. Moreover, more than 1,300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to

Microsoft sinkholes. This will allow Microsoft's DCU to provide actionable intelligence to continue to harden the security of the company's services and help protect online users. These insights will also assist public- and private-sector partners as they continue to track, investigate, and remediate this threat. This joint action is designed to slow the speed at which these actors can launch their attacks, minimize the effectiveness of their campaigns, and hinder their illicit profits by cutting a major revenue stream.



Heat map detailing global spread of Lumma Stealer malware infections and encounters across Windows devices.

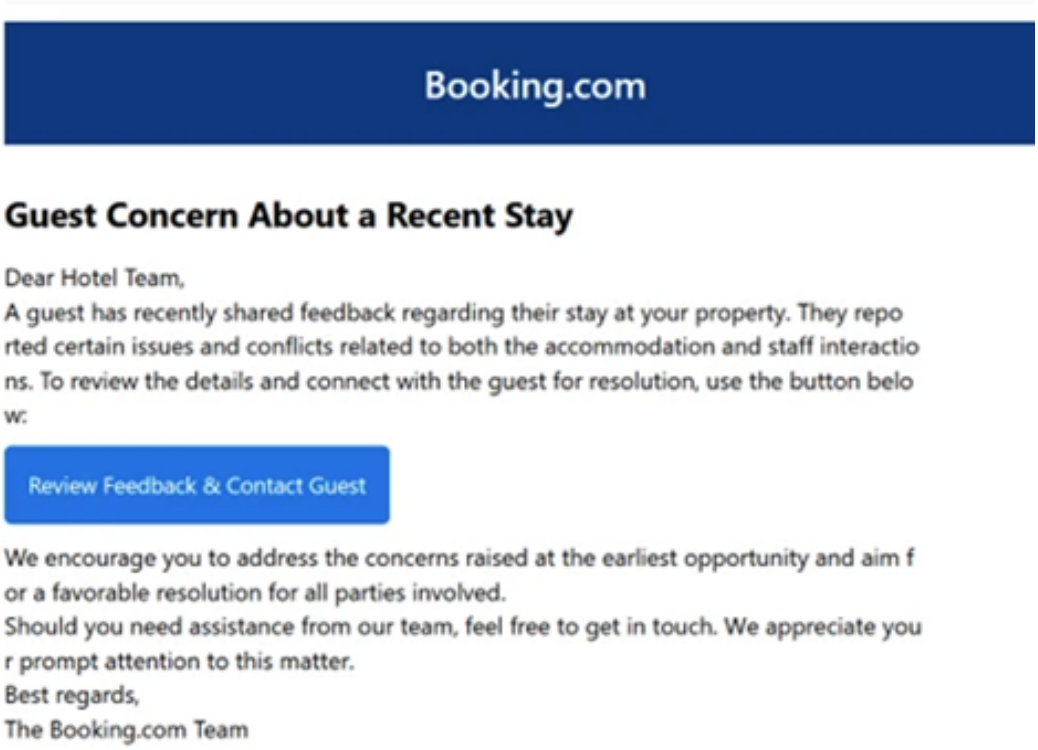
Splash page displayed on 900+ domains seized by Microsoft.

What is Lumma?

Lumma is a Malware-as-a-Service (MaaS), marketed and sold through underground forums since at least 2022. Over the years, the developers released multiple versions to continually improve its capabilities. Microsoft Threat Intelligence shares more details around the delivery techniques and capabilities of Lumma in a recent blog.

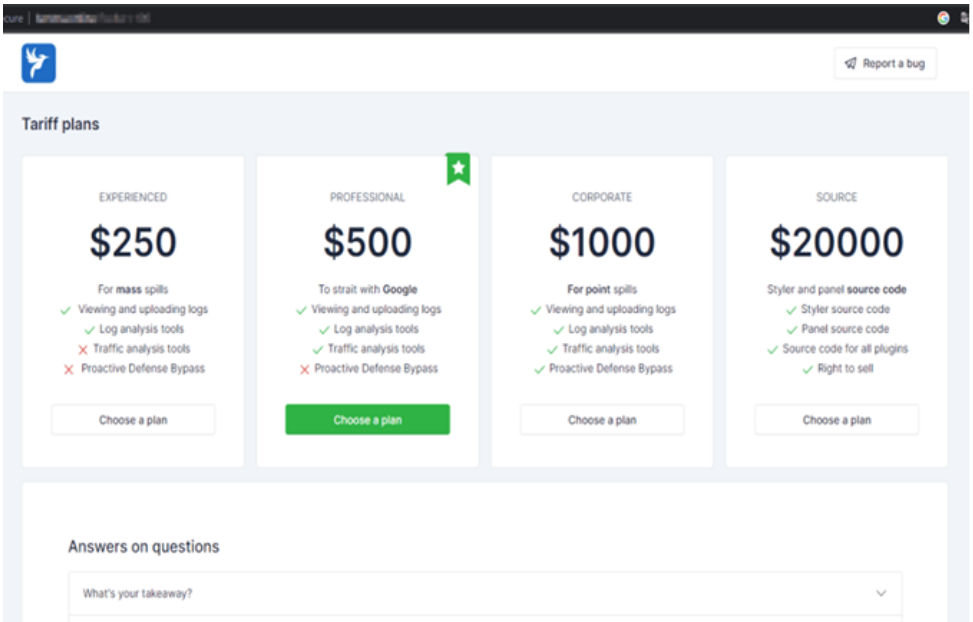
Typically, the goal of Lumma operators is to monetize stolen information or conduct further exploitation for various purposes. Lumma is easy to distribute, difficult to detect, and can be programmed to bypass certain security defenses, making it a go-to tool for cybercriminals and online threat actors, including prolific ransomware actors such as Octo Tempest (Scattered Spider). The malware impersonates trusted brands, including Microsoft, and is deployed via spear-phishing emails and malvertising, among other vectors.

For example, in March 2025, Microsoft Threat Intelligence identified a phishing campaign impersonating online travel agency Booking.com. The campaign used multiple credential-stealing malware, including Lumma, to conduct financial fraud and theft. Lumma has also been used to target gaming communities and education systems and poses an ongoing risk to global security, with reports from multiple cybersecurity companies outlining its use in attacks against critical infrastructure, such as the manufacturing, telecommunications, logistics, finance, and healthcare sectors.



Example of phishing email impersonating Booking.com and fake CAPTCHA verification prompt. (Source:[Microsoft – Phishing campaign impersonates Booking .com, delivers a suite of credential-stealing malware](#))

The primary developer of Lumma is based in Russia and goes by the internet alias “Shamel.” Shamel markets different tiers of service for Lumma via Telegram and other Russian-language chat forums. Depending on what service a cybercriminal purchases, they can create their own versions of the malware, add tools to conceal and distribute it, and track stolen information through an online portal.



Different tiers of service for Lumma, as well as Lumma's logo used on marketing material. (Source: Darktrace – The Rise of MaaS & Lumma Info Stealer)

In an interview with cybersecurity researcher "g0njxa" in November 2023, Shamel shared that he had "about 400 active clients." Demonstrating the evolution of cybercrime to incorporate established business practices, he effectively created a Lumma brand, using a distinctive logo of a bird to market his product, calling it a symbol of "peace, lightness, and tranquility," and adding the slogan "making money with us is just as easy."

Shamel's ability to operate openly underscores the importance for countries worldwide to address the issue of safe havens and to advocate for the rigorous enforcement of due diligence obligations under international law.

Continuing to work together to disrupt prolific cybercrime tools

Disrupting the tools cybercriminals frequently use can create a significant and lasting impact on cybercrime, as rebuilding malicious infrastructure and sourcing new exploit tools takes time and costs money. By severing access to mechanisms cybercriminals use, such as Lumma, we can significantly disrupt the operations of countless malicious actors through a single action.

Continued collaboration across industry and government remains imperative. We are grateful for the partnership with others across government and industry, including cybersecurity companies ESET, Bitsight, Lumen, Cloudflare, CleanDNS, and GMO Registry. Each company provided valuable assistance by quickly taking down online infrastructure.

Finally, we know cybercriminals are persistent and creative. We, too, must evolve to identify new ways to disrupt malicious activities. Microsoft's DCU will continue to adapt and innovate to counteract cybercrime and help ensure the safety of critical infrastructure, customers, and online users.

Organizations and individuals can protect themselves from malware like Lumma by using multi-factor authentication, running the latest anti-malware software, and being cautious with attachments and email links. More information for security professionals can be found here.

Tags: cyberattacks, cybersecurity, Microsoft Digital Crimes Unit, The Digital Crimes Unit