



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

20 Feb 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles	2
Darcula Allows Tech-Illiterate Crooks to Create, Deploy DIY Phishing Kits Targeting Any Brand.....	2
DeepSeek Found to Be Sharing User Data with TikTok Parent Company ByteDance	2
Microsoft's End of Support for Exchange 2016 and 2019: What IT Teams Must Do Now.....	2
Phishing Attack Hides JavaScript Using Invisible Unicode Trick	2

Articles

Darcula Allows Tech-Illiterate Crooks to Create, Deploy DIY Phishing Kits

A new, improved version of Darcula, a cat-themed phishing-as-a-service (PhaaS) platform aimed at serving Chinese-speaking criminals, will be released this month and will allow malicious users to create customized phishing kits to target a wider variety of brands than ever before, Netcraft researchers are warning. The current version of the platform offers pre-built phishing kits for targeting users of over 200 brands worldwide. The biggest innovation baked into the soon to be released Darcula v3 is the ability for any user to generate a phishing kit for any brand, the researchers discovered. The platform is able to create separate pages to perfect the illusion and maximize the extraction of information from targets: an initial lure page, a page that asks them to input their personal information and payment card info, and a page that asks them to enter the two-factor authentication code. Darcula v3 can leverage the stolen card details to generate an image of the victim's card, which makes it easier for crooks add them to a digital wallet by simply scanning the image.

<https://www.helpnetsecurity.com/2025/02/20/darcula-allows-tech-illiterate-crooks-to-create-deploy-diy-phishing-kits-targeting-any-brand/>

DeepSeek Found to Be Sharing User Data with TikTok Parent Company ByteDance

South Korea's Personal Information Protection Commission (PIPC) says it uncovered evidence that DeepSeek has secretly been sharing data with ByteDance, the parent company of popular social media app TikTok. PIPC said that DeepSeek—an app with over one million downloads at the time of writing—automatically transmitted information to ByteDance servers every time users accessed the app, doing so without disclosure or explicit consent. PIPC told South Korea's Yonhap News Agency that it was “yet to confirm what data was transferred and to what extent.” It also further illustrates the necessity for proper inquiry into these practices and may indicate an urgent need for transparent and comprehensive international regulations on data privacy, with some nations like Italy and Australia already leading the way in taking action against AI applications like DeepSeek over these issues.

<https://www.malwarebytes.com/blog/news/2025/02/deepseek-found-to-be-sharing-user-data-with-tiktok-parent-company-bytedance>

Microsoft's End of Support for Exchange 2016 and 2019: What IT Teams Must Do Now

Microsoft officially announced support for Exchange Server 2016 and Exchange Server 2019 will end on 14 Oct 25. The end of support means that Microsoft will no longer provide security patches, bug fixes or technical support, leaving organizations running on these versions exposed to security vulnerabilities, compliance risks and potential operational disruptions. This end of support also applies to several related Microsoft products, including Microsoft Office 2016, Microsoft Office 2019, Outlook 2016, Outlook 2019, Skype for Business 2016, Skype for Business 2019, Skype for Business Server 2015 and Skype for Business Server 2019. Whether you choose to stay on-prem with Exchange Server SE or migrate to the cloud with Microsoft 365 or Google Workspace, understanding the right migration steps is essential for a smooth transition.

<https://thehackernews.com/2025/02/microsoft-end-of-support-for-exchange-2016-and-exchange-2019.html>

Phishing Attack Hides JavaScript Using Invisible Unicode Trick

A new JavaScript obfuscation method utilizing invisible Unicode characters to represent binary values is actively abused in phishing attacks targeting affiliates of an American political action committee (PAC). The attacks are

tough to detect as empty whitespace reduces the likelihood that even security scanners will flag it as malicious. Since the payload is just a property in an object, it could be injected into legitimate scripts without raising suspicion; plus, the whole encoding process is easy to implement and doesn't require advanced knowledge.

<https://www.bleepingcomputer.com/news/security/phishing-attack-hides-javascript-using-invisible-unicode-trick/>