A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

4 Nov 22

Cyber Threat Roundup

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

Contents

Articles

Cyber Incident at Boeing Subsidiary Causes Flight Planning Disruptions

Jeppesen, a wholly-owned Boeing subsidiary that provides navigation and flight planning tools, confirmed on Thursday that it is dealing with a cybersecurity incident that has caused some flight disruptions. A red banner was added to the company's website on Wednesday, warning that the Colorado-based firm was experiencing "technical issues with some of our products, services and communication channels".

https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions/

LockBit Ransomware Gang Claims the Hack of Continental Automotive Group

LockBit ransomware gang announced to have hacked the German multinational automotive parts manufacturing company Continental. The group added the name of the company to its Tor leak site and is threatening to publish alleged stolen data if the victim will not pay the ransom.

https://securityaffairs.co/wordpress/138062/cyber-crime/lockbit-gang-claims-continental-hack.html

FIN7 Cybercrime Group Likely Behind Black Basta Ransomware Campaign

FIN7, a financially motivated cybercrime organization that is estimated to have stolen well over $1.2 billion since surfacing in 2012, is behind Black Basta, one of this year's most prolific ransomware families.

https://www.darkreading.com/attacks-breaches/fin7-cybercrime-group-likely-behind-black-basta-ransomware-campaign

Supply Chain Attack Pushes Out Malware to More than 250 Media Websites

The cyber-threat threat actor known as "TA569", or "SocGholish", has compromised JavaScript code used by a media content provider in order to spread the FakeUpdates malware to major media outlets across the United States. The supply chain attack is being used to spread TA569's custom malware, which is typically employed to establish an initial access network for follow-on attacks and ransomware delivery.

https://www.darkreading.com/application-security/supply-chain-attack-pushes-out-malware-to-more-than-250-media-websites

U.S. Treasury Thwarts DDoS Attack from Russian Killnet Group

The U.S. Treasury Department has thwarted a distributed denial of service (DDoS) attack that officials attributed to Russian hacktivist group Killnet. These are the same pro-Kremlin miscreants that claimed responsibility for knocking more than a dozen U.S. airports' websites offline on October 10 in similar network-traffic flooding incidents. The large-scale DDoS attack didn't disrupt air travel or cause any operational harm to the airports.

https://www.theregister.com/2022/11/02/killnet_us_treasury_ddos/?&web_view=true

Microsoft Rolls Out Fix for Outlook Disabling Teams Meeting Add-In

Microsoft is rolling out a fix for a known issue affecting Outlook for Microsoft 365 users and preventing them from scheduling Teams meetings because the option is no longer available on the app’s ribbon menu. The Teams Meeting add-in can be found in the Calendar view, and it helps Outlook users to create Teams meetings from Outlook.

https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-out-fix-for-outlook-disabling-teams-meeting-add-in/