SpiderLabs Blog

Archived: 2026-04-05 16:03:38 UTC

Major Supply Chain Compromise in the Popular axios npm Package

April 03, 2026 | Karl Sigler

Read More

Stay Informed

Sign up to receive the latest security news and trends straight to your inbox from LevelBlue.

Using RF Power Levels to Defeat MAC Address Randomization Enabling Passive Device Tracking

March 31, 2026 | Tom Neaves

I came up with a theory (based on science) that it may be possible to passively ...

Read More

The Value of Microsoft Security Copilot: SCU Billing and Why Agent Design Matters

March 27, 2026 | David Broggy

Most organizations start by using Microsoft Copilot the way it looks in demos: ...

Read More

Azure ServiceBus WebSockets as a C2 Channel

March 24, 2026 | Stuart White

In offensive security, the ability to blend seamlessly with legitimate traffic ...

Read More

Tracing a Multi-Vector Malware Campaign: From VBS to Open Infrastructure

March 23, 2026 | Sean Shirley

Recently LevelBlue SpiderLabs initiated an investigation into a multi-stage ...

Read More

“Say My Name”: How MioLab is building MacOS Stealer Empire

March 20, 2026 | Mark Tsipershtein and Evgeny Ananin

As Apple computer’s market share continues to grow, threat actors are ...

Read More

Fake CAPTCHA Campaign: Inside a Multi-Stage Stealer Assault

March 19, 2026 | Shabtay Barel, Serhii Melnyk, Rodel Mendrez

This report expands LevelBlue’s ongoing investigation into a multi-stage ...

Read More

KongTuke: A King Among Threat Groups

March 18, 2026

This blog is the latest in a series that delves into the deep research ...

Read More

How LevelBlue OTX and Cybereason XDR Detected a North Korea-Linked Remote IT Worker

March 17, 2026 | Tue Luu

Talk about dodging the insider threat from hell. From August 15 to 25, 2025, ...

Read More

Epic Fury Update: Stryker Attack Highlights Handala's Shift from Espionage to Disruption

March 12, 2026 | Arthur Erzberger

On March 11, 2026, the medical technology vendor Stryker disclosed a global ...

Read More

Weaponizing Safe Links: Abuse of Multi-Layered URL Rewriting in Phishing Attacks

March 12, 2026 | John Kevin Adriano

In 2024, threat actors were already abusing URL rewriting mechanisms in ...

Read More

Beware the ClickFix Trap: REMCOS RAT Hiding in "Helpful" PUAs

March 09, 2026 | Hema Loganathan

Cybereason GSOC has observed a notable increase in infections involving REMCOS ...

Read More

Discover and Exploit: Memory Corruption in CUPS (CVE-2025-61915)

March 05, 2026 | Ariel Silver

CVE-2025-61915 is a stack based out-of-bound write bug in CUPS. An unauthorized ...

Read More

LevelBlue SpiderLabs Breaks Down the Role of Cyber Operations Taken in the Iran Crisis

March 04, 2026 | Gal Romano

As combat operations that began on February 28 with joint US-Israeli strikes on ...

Read More

Operation Epic Fury: From Regional Escalation to Global Cyber Risk

March 03, 2026 | LevelBlue SpiderLabs

In light of escalating geopolitical tensions involving the United States, ...

Read More

From Shadow IT to GhostOps: The Rise of Unauthorized AI Agents in the Enterprise

February 24, 2026 | Grant Hutchons

If you have worked in enterprise IT for long enough, you have lived through the ...

Read More

Phishing with OAuth Redirect

February 18, 2026 | Federico Cedolini

The LevelBlue SpiderLabs team identified phishing emails in January 2026 that ...

Read More

Pwning Malware with Ninjas and Unicorns

February 16, 2026 | Cade Wriglesworth

During a DFIR engagement, LevelBlue was asked to assist with reverse ...

Read More

How ClickFix Opens the Door to Stealthy StealC Information Stealer

February 12, 2026 | Rodel Mendrez

This analysis examines a complete attack chain targeting Windows systems ...

Read More

Stealerium Unmasked: Inside a Multi-Lure, Multi-Stage Stealer Campaign

February 11, 2026 | Bernard Bautista

In this investigation, we tracked a malware spam campaign that ultimately ...

Read More

Notepad-Plus Fuss: Notepad++ Supply Chain Attack Analysis

February 10, 2026 | King Orande

LevelBlue SpiderLabs' Cyber Threat Intelligence Team investigated the ongoing ...

Read More

19 Shades of LockBit5.0, Inside the Latest Cross-Platform Ransomware's Newest Leaked Samples: Part 3

February 05, 2026 | Alexander Sevtsov, Chen Aviani

In the first two parts of our LockBit 5.0 series, we provided a comprehensive ...

Read More

19 Shades of LockBit5.0, Inside the Latest Cross-Platform Ransomware's Newest Leaked Samples: Part 2

February 04, 2026 | Mark Tsipershtein, Evgeny Ananin, Nikita Kazymirskyi

In the first part of our LockBit 5.0 series, where we analyzed 19 samples of ...

Read More

The Godfather of Ransomware? Inside DragonForce's Cartel Ambitions

February 03, 2026 | Mark Tsipershtein and Evgeny Ananin

The Cybereason, A LevelBlue Company, Threat Intelligence Team conducted an ...

Read More

LockBit 5.0 Introduces New Features: ChaCha20 Encryption, Stealthy Installation, and Anti-Analysis to Target Windows, Linux, and ESXi Environments

January 30, 2026 | SpiderLabs Researcher

The prolific LockBit ransomware-as-a-service (RaaS) group shows its dedication ...

Read More

19 Shades of LockBit5.0, Inside the Latest Cross-Platform Ransomware's Newest Leaked Samples: Part 1

January 30, 2026 | Mark Tsipershtein, Evgeny Ananin, Nikita Kazymirskyi

This three-part blog series presents an analysis of 19 samples of a ...

Read More

Scenario 3: SOC/SIEM Takes in and Summarizes Windows Events (Log Files)

January 29, 2026 | Tom Neaves

In September last year I penned this blog Rogue AI Agents In Your SOCs and ...

Read More

The Hard Lessons Learned by Analyzing Education Sector Cyberattacks

January 26, 2026

In the last quarter of 2025, LevelBlue SpiderLabs used telemetry from the ...

Read More
