Update: Stopping Cybercriminals from Abusing Cobalt Strike | Cobalt Strike

By Cobalt Strike Team

Published: 2025-03-07 · Archived: 2026-04-05 12:43:35 UTC

Since 2023, Microsoft's Digital Crimes Unit (DCU), Fortra, and the Health Information Sharing and Analysis Center (Health-ISAC) have been working together to combat the use of unauthorized, legacy copies of Cobalt Strike and compromised Microsoft software, which have been weaponized by cybercriminals to deploy ransomware and other malware, causing significant harm to critical sectors like healthcare.

Microsoft, Fortra, and Health ISAC remain committed to this endeavor, leveraging legal, technical, and collaborative efforts to dismantle cybercriminal operations. This initiative underscores the importance of persistence and partnership in securing the digital ecosystem.

As we near the second anniversary, we want to highlight updates on our progress and share our planned focus for 2025.

Accelerated Takedowns: Limiting Dwell Time and Damage

Over the past two years, **the number of unauthorized copies of Cobalt Strike observed in the wild has decreased by 80%,** drastically reducing availability to cybercriminals. This reduction has had a tangible impact, with these tools now being abused far less often.

We have successfully seized and sinkholed over 200 malicious domains, effectively cutting off their ability to accept legitimate traffic and preventing further exploitation by threat actors.

Additionally, the average dwell time—the period between initial detection and takedown—has been reduced to less than one week in the United States and less than two weeks worldwide.

A Global Success with Operation MORPHEUS

In July of 2024, Fortra was part of Operation MORPHEUS, a three-year investigation that culminated in a coordinated global effort to takedown known IP addresses and domain names associated with criminal activity to further disable unauthorized versions of Cobalt Strike. A **total of 690 IP addresses were flagged to online service providers in 27 countries. In total, 593 of these addresses were taken down.**

The UK's National Crime Agency led this investigation, with support from law enforcement in Australia, Canada, Germany, the Netherlands, Poland, and the United States. Europol coordinated international operations and collaborated with private partners, including Fortra.

Continued Takedown Efforts and Next Steps

Our campaign to combat the malicious use of unauthorized Cobalt Strike copies are ongoing and evolving. We remain committed to providing any new and relevant information to law enforcement agencies worldwide to support their investigations. Fortra is also invested in other public-private partnerships, having signed onto the **Pall Mall Process**, an international initiative is focused on developing regulations to combat the unauthorized distribution and usage of commercial cyber intrusion tools.

Additionally, we are continuing to send takedown notices to hosting providers, raising awareness of the illicit use of unauthorized copies. We actively track these activities to the point of origin, identifying root causes to prevent reoccurrence. We concurrently issue notices on a persistent basis until these illegal versions are removed from web properties. Compliant web properties are also passively monitored in case of reappearance.

These efforts are gaining momentum and have entered a new phase of heightened efficacy. Automation processes have been put into place to further increase efficiency and simplify the takedown process. Additionally, just as cybercriminals adapt their techniques, Fortra continuously updates Cobalt Strike's security controls to thwart cracking attempts and protect legitimate users.

Strengthening Red Team Tool Security

The nature of the modern cybersecurity landscape makes the critical need for red team solutions undeniable. However, these tools inherently carry some risk of misuse..

By proactively sharing our disruption techniques through conference talks and webinars, we have provided the broader security community with a proven roadmap that other solution providers can follow to engage in public/private disruption partnerships when faced with similar challenges.

Collaboration is essential in advancing cybersecurity overall. This not only strengthens the collective defense against cybercriminals but also ensures that legitimate security tools can continue to be used responsibly and effectively to protect organizations worldwide.

We want to thank Microsoft DCU, Health ISAC, and every other organization we've joined forces with in these efforts and look forward to continuing our work together to defend the integrity of critical commercial cybersecurity tools.
