👨‍💻 PolyGlot Malware Analysis - IcedID Stager 💾

Published: 2023-05-03 · Archived: 2026-04-05 17:22:47 UTC

🔥 Learn how polyglot malware stagers are evolving 👨‍💻 Buy Our Courses: https://guidedhacking.com/register/ 💰 Donate on Patreon: _/guidedhacking_ ❤️ Follow us on Social Media: https://linktr.ee/guidedhacking 🔗 Article Link: https://guidedhacking.com/threads/ana... 📜 Video Description: Threat actors consistently innovate in their efforts to infect victims and avoid those conducting malware analysis and reverse engineering on their creations. In this malware analysis tutorial, we'll explore the concept of polyglot malware and how to analyze it, particularly for beginners. We start by examining a file posted on Twitter that appears as an image, instructing viewers to download and change its file extension. Upon downloading and changing the file extension to a ZIP, we can then extract the source code for a Python script that generates the polyglot file. Polyglot files capitalize on non-restrictive file formats, where the data within can be positioned anywhere. A polyglot file fundamentally embeds two or more file formats into one, functioning differently depending on the software that opens it. Although information on polyglot files is abundant, they are primarily used for fun or malware purposes rather than regular use. Naturally, when creativity meets computer science, threat actors find ways to exploit it, and polyglot files are no exception. We first review coverage on a RAT (Remote Access Trojan) spread within a CAB file, which can also be run as a JAR file. The file itself contains various pieces of garbage data to evade antivirus software and a fake PE header to confuse antivirus programs. This technique may also hinder researchers attempting malware analysis and reverse engineering on a polyglot file. The primary polyglot file we examine is an IcedID stager disseminated through email. Brad from Malware Traffic provided coverage on this file, explaining that it begins as an encrypted ZIP, which opens to an ISO file and then a CHM polyglot file. Upon opening the ISO, two files reside within: a hidden DLL representing the IcedID malware and a Windows help file. Help files are HTML files displayed in Windows and typically used for help documentation. Within the help file is a script that reruns itself using mshta, subsequently calling a command process that executes rundll32 on the hidden IcedID DLL. This process stages the IcedID malware to infect the victim. In this malware analysis tutorial, we've delved into the world of polyglot malware, showcasing the creativity of threat actors and the challenges faced by researchers conducting reverse engineering and malware analysis. As beginners in the field, understanding these concepts and techniques is essential for success in combating and analyzing malware like IcedID . The IcedID malware, sometimes referred to as BokBot, is a sophisticated form of banking Trojan that primarily aims to exfiltrate sensitive financial information. Initially identified around 2017, its insidious reach has since grown, becoming a significant threat in the cybersecurity landscape. The IcedID malware usually infiltrates systems through carefully crafted phishing emails or as a secondary payload delivered by other malware. Once inside the target system, it lies dormant, stealthily monitoring the user's activities. When the user attempts to access a banking site, IcedID springs into action, employing 'web injection' techniques to mimic legitimate banking websites and deceive the user into entering their login credentials. The ingenuity of IcedID malware lies not just in its deceptive capabilities but also in its adaptability. Over time, it has undergone several evolutions to better avoid detection and increase its destructive impact. It has diversified its targets beyond just financial institutions to other sectors, expanding its trove of stolen data. Polyglot files are cool indeed. Combatting threats like IcedID malware requires constant vigilance, proactive defense measures, and robust cybersecurity infrastructure. It is an ongoing battle against the ever-evolving landscape of digital threats. Polyglot files! Polyglot

files, remarkable in their multifaceted nature, are files designed to be valid in multiple formats. A classic example might be a JPG image that is also a ZIP archive. While often used for creative purposes, they can pose a cybersecurity risk, as they can be used to conceal malware. 📝 Timestamps: 0:00 - Introduction to Polyglot Files 0:49 - What are Polyglot Files? 1:37 - Polyglots Database Overview 2:14 - Real-World Malware Examples 3:23 - HTML and JAR File Combination 4:04 - Join GuidedHacking.com 4:30 - Exploring CHM and DLL Files 6:11 - Understanding CHM Files 7:35 - Finding Hidden Code 8:40 - Conclusion and Outro ✏️ Tags: guidedhacking malware analysis reverse engineering polyglot file IcedID malware #malwareanalysis #reverseengineering #malwareanalysis fr3dhk malware analysis at guidedhacking.com

---