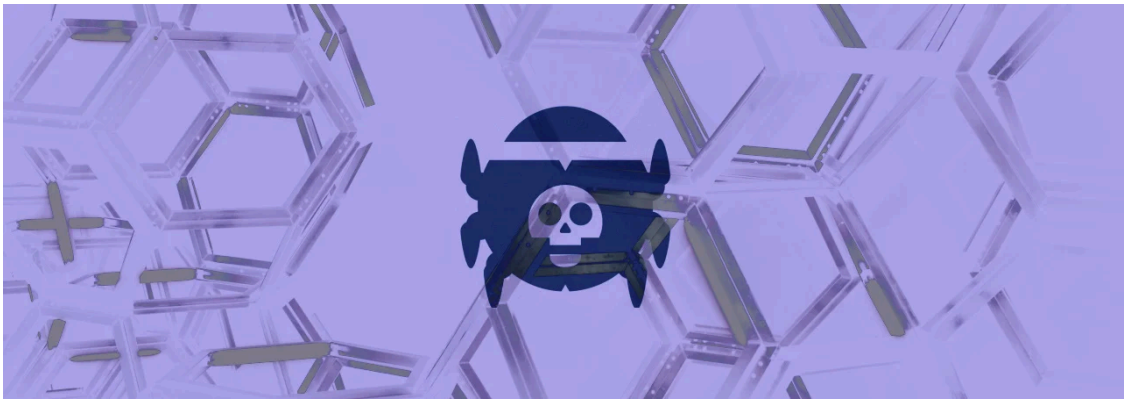
GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic

By Ax Sharma

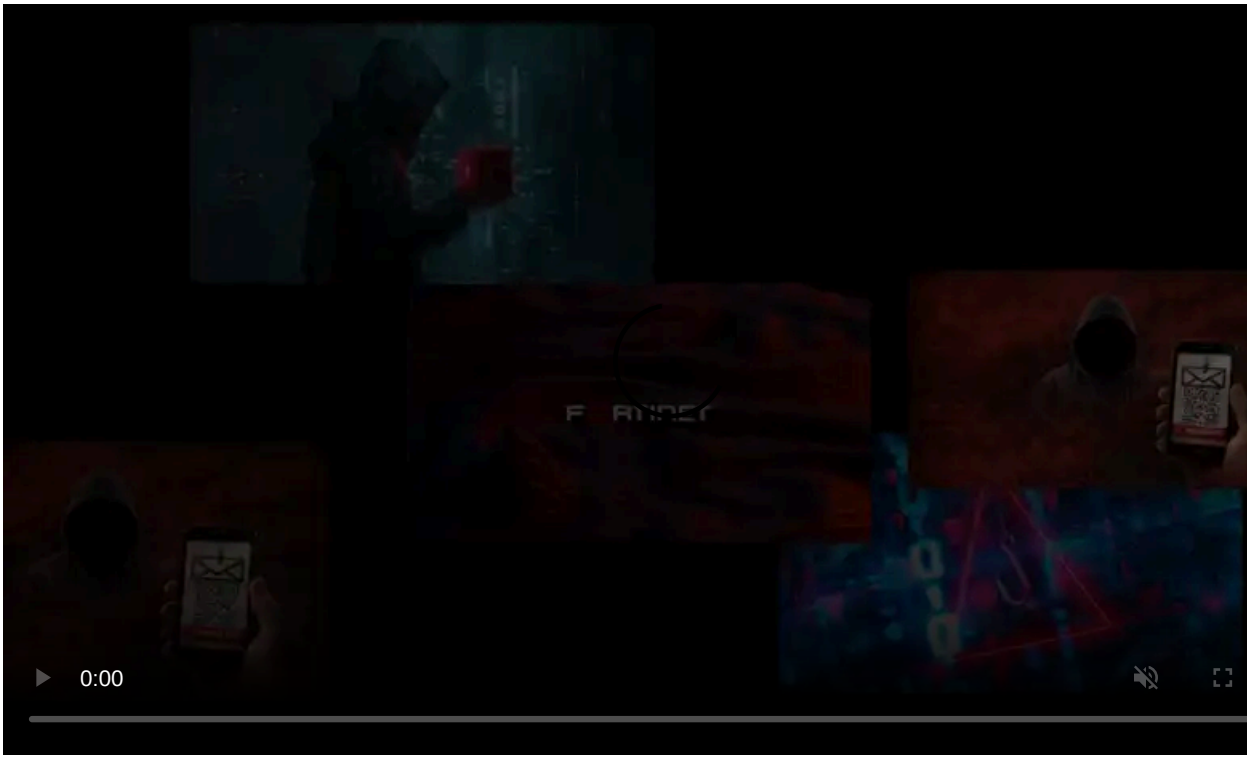
Published: 2020-12-28 · Archived: 2026-04-06 01:04:18 UTC

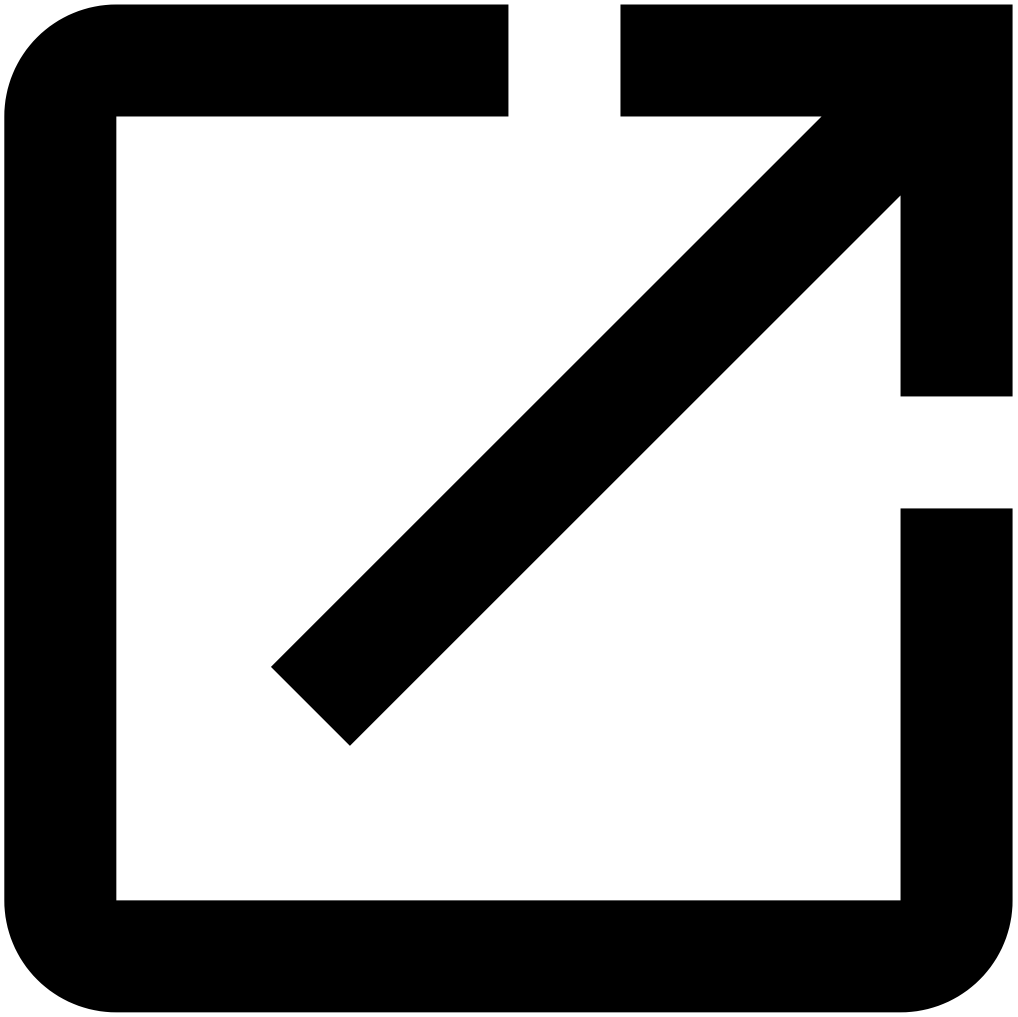


A new strand of malware uses Word files with macros to download a PowerShell script from GitHub.

This PowerShell script further downloads a legitimate image file from image hosting service Imgur to decode a Cobalt Strike script on Windows systems.

Multiple researchers have potentially linked this strain to MuddyWater (aka SeedWorm and TEMP.Zagros), a government-backed advanced persistent threat (APT) group, first observed in 2017 while mainly targeting Middle Eastern entities.


0:00



Word macro spins up PowerShell script hosted on GitHub

This week researcher *Arkbird* has shared details on a new macro-based malware that is evasive and spawns payload in multifaceted steps.

The malware strand which looks "like MuddyWater," according to the researcher, ships as an embedded macro within a legacy Microsoft Word (*.doc) file, in the style of the APT group.

In tests by BleepingComputer, when the Word document is opened, it runs the embedded macro. The macro further launches *powershell.exe* and feeds it the location of a PowerShell script hosted on GitHub (archived).

Macro script embedded within the malicious Word doc
Source: BleepingComputer

The single-line PowerShell script has instructions to download a real PNG file (shown below) from the image hosting service Imgur.

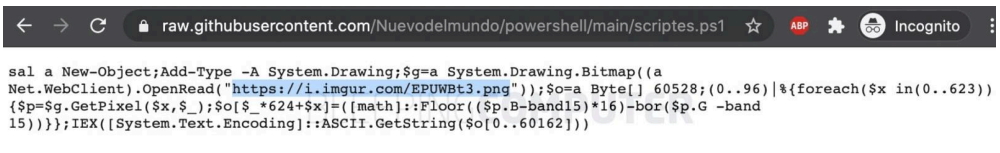
While this image itself may be benign, its pixel values are used by the PowerShell script in calculating the next stage payload.

Malware calculates the next stage payload by decoding the pixel values within this image
Source: Imgur

The technique of hiding code, secret data, or malicious payload within ordinary files, such as images, is known as steganography.

Tools like *Invoke-PSImage* make this possible by encoding a PowerShell script within the pixels of a PNG file and generating a one-line command to execute the payload.

As observed by BleepingComputer and shown below, the payload calculation algorithm runs a *foreach* loop to iterate over a set of pixel values within the PNG image and performs specific arithmetic operations to obtain functional ASCII commands.



PowerShell script hosted on GitHub downloads PNG from Imgur and uses it to calculate the payload
Source: BleepingComputer

Decoded script executes Cobalt Strike payload

The decoded script obtained from manipulating the PNG's pixel values is a Cobalt Strike script.

Cobalt Strike is a legitimate penetration testing toolkit that allows attackers to deploy "beacons" on compromised devices to remotely "create shells, execute PowerShell scripts, perform privilege escalation, or spawn a new session to create a listener on the victim system."

In fact, the decoded shellcode comprises an EICAR string to trick security tools and SOC teams into mistaking this malicious payload for an antivirus test being performed by security professionals.

The payload, however, indeed contacts the command-and-control (C2) server via a *WinINet* module to receive further instructions, according to *Arkbird*.

The domain associated with the C2 server *Mazzion1234-44451.portmap.host* was no longer accessible at the time of writing.

However, the researcher noted "the domain has been recorded near 20 December 2020. The GitHub account has got the script pushed the 24 December, the date of the submission in [VirusTotal]."

The emergence of this evasive malware strain around the holiday season gains adversaries another advantage: to mask their footsteps when most staff is likely to be away and less vigilant.

While authoritative attribution is challenging given the possibility of copycat attacks, security researcher Florian Roth from Nextron Systems has added the Indicators of Compromise (IOCs) associated with this malware to MuddyWater IOCs list.

The researcher has also provided YARA rules that can be used to detect the variant in your environment.

IOCs associated with the macro-laden Word documents used in this malware campaign are given below:

1. d1c7a7511bd09b53c651f8ccc43e9c36ba80265ba11164f88d6863f0832d8f81
2. ed93ce9f84dbea3c070b8e03b82b95eb0944c44c6444d967820a890e8218b866

If you receive a suspicious Word document in a phishing email or via any other means, do not open it or run "macros" within it.

This is not the first time legitimate services like GitHub and Imgur have been abused to serve malicious code.

Recently, wormable botnet Gitpaste-12 leveraged both GitHub and Pastebin to host its malicious payload and evade detection.

Additionally, ransomware groups like CryLocker have been known to abuse Imgur for data storage.

Source: https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/