

Attacks that used steganography techniques

Various types of threat actors, from crooks to cyberespionage groups, have used steganography to conceal information. One of the first powerful malware that took advantage of these techniques was [Duqu](#), discovered in 2011. Its makers encrypted data and embedded it into a JPEG file.

More recently, APT groups like Platinum, OceanLotus/APT32, K3chang/APT15/Mirage/Vixen Panda, and [MontysThree](#) relied on steganography for cloaking encrypted payloads or maintaining on-system persistence. Meanwhile, RedBaldKnight/Bronze Butler/Tick built tools that can create, embed, and hide executables or configuration files, and [Tropic Trooper/Pirate Panda/KeyBoy](#) masked its backdoor routines and evaded anti-malware and network perimeter detection.

Researchers at Kaspersky have also identified an APT gang they call BountyGlad, which used steganography to support multi-stage implant delivery as a part of a [supply chain attack](#), cloaking shellcode within a PNG file used to deliver the final stage payload. "The most sophisticated APT [groups] often use the simplest steganography techniques in elegant ways," says Kurt Baumgartner, principal researcher at Kaspersky. He noticed that, for these threat actors, steganography is more than data hidden in JPEGs or BMPs.

"Most frequently, steganographic imagery techniques are used to support multi-staged malicious implant deliveries in intrusions," Baumgartner adds. "We also see APT hide commands for their implants in web pages with whitespace and within debug logs posted to forums, covertly upload stolen data in images, and maintain persistence by storing encrypted code within specific locations of validly Authenticode-signed executables."

Ransomware gangs have also learned that using steganography could help them carry out their attacks. Lurk/Stegoloadr, for instance, encrypted URLs and hid them inside a white BMP file that downloaded a second payload. SyncCrypt and Cerber also cloaked parts of their code in image files, and TeslaCrypt cleverly included HTML comment tags in a 404 error page that had instructions for a command-and-control server.

Steganography has also been used by cryptomining malware. For example, [SentinelLabs](#) recently discovered a campaign affecting the Docker Linux platform. This threat actor embedded an ELF binary inside a JPEG file to bypass detections by many antivirus software products. "The file was 6MB, which was extremely large for a JPEG," Marco Figueroa, principal threat researcher at SentinelOne, says. "The size of the JPEG provided a clue that the file had malicious code within it."

Even actors conducting [malvertising](#) campaigns take advantage of steganography. The Stegano/Astrum exploit kit embedded malicious code inside the RGBA transparency value of each pixel of PNG banner ads. When ads were loaded, the

malicious code was extracted, and the user was redirected to the exploit kit landing page. Furthermore, the group behind DNSCharge created ads that contained code that launched [brute force attacks](#) against users' home WiFi routers.

What companies can do to protect against steganography

Using steganography during an attack is relatively easy. Protecting against it is much more complicated, as threat actors are getting more innovative and more creative. "Companies should embrace modern endpoint protection technologies that go beyond static checks, basic signatures, and other outdated components as code hidden in images and other forms of obfuscation are more likely to be detected dynamically by a behavioral engine," Figueroa says.

He has two more tips for organizations and their employees: First, if an image is unusually large, it might be a clue that steganography was used. Second, companies should focus detection efforts directly at the endpoints where encryption and obfuscation are easier to detect.

Trend Micro's Clay says more should be done to educate users and raise awareness. "Organizations should teach employees that image files can harbor malicious code," he says. "In addition, organizations should have web filtering for safer browsing and should also stay up to date with the latest security patches when updates are available."

Kaspersky's Baumgartner also thinks businesses should do more to protect against such attacks. "A solid host-based antimalware solution will identify actions based on the decrypted commands, find hidden malware and their loaders delivered with these techniques using heuristic, behavioral, machine learning, and other methods, and suspicious outbound siphoning of data," he says. "Also, network tracking may help support identification of new steganographically delivered malware or outbound stolen data."

While some researchers worry about the creativity of nation-state actors, others believe that any malicious entity could leverage steganography. "Less advanced adversaries are using fairly sophisticated stuff that can go undetected," Baumgartner says.

<https://www.csoonline.com/article/3632146/steganography-explained-and-how-to-protect-against-it.html>