

# The Sample: Beating the Malware Piñata

Published: 2022-05-05 · Archived: 2026-04-05 16:27:37 UTC



## Presented by

Christopher Gardner, Principal Reverse Engineer • R&E - Mandiant Advantage Labs

## About this talk

In The Sample FLARE analysts present stories of notable malware samples they have reverse engineered. The FLARE team studies hundreds of malware samples each month and here they share highlights of real-world malware and analysis techniques. These talks aim to educate and entertain technical and non-technical attendees alike. In this first iteration, join Chris Gardner of the FLARE team as he examines the malware gift that keeps on giving. Even after politely asking it to stop. This talk covers: - How to analyze droppers that just won't stop dropping more PE files. - How to extract new payloads when a sample performs process injection. - Why open-source intelligence is both beautiful and dangerous. - What analysis tricks reduced analysis time to a mere 45 hours.

 [Mandiant | Intelligence and Expertise](#)

[Mandiant | Intelligence and Expertise](#)

180748 subscribers161 talks

Make Google part of your security team

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of front...

---

Source: <https://www.brighttalk.com/webcast/7451/538775>