The Sample: Beating the Malware Piñata

brighttalk.com/webcast/7451/538775

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.

More from this channel

Upcoming talks (**7**)

On-demand talks (**421**)
Subscribers (**91821**)
Mandiant provides public and private organizations and critical infrastructure worldwide with early threat insights through unmatched intelligence and response expertise for the highest-profile incidents.