GreHack 2018: The Evolution Of GandCrab Ransomware

The vast majority of ransomware infections in the past years have been results of ransomware being sold as an easy-to-use service, following the Ransomware-as-a-Service (RaaS) model. In 2018, the RaaS-space was dominated by a new malware family: GandCrab.

VMRay Sr. Threat Researcher, Tamas Boczan tracked and analyzed the family from the earliest stages to the latest version, observing differences between versions, like added features and rewritten functions. Besides the reverse-engineering of the payload, Tamas analyzed the various distribution methods: drive-by downloads via exploit kits and different Javascript and Word doc droppers attached to spam e-mails.

In this GreHack 2018 presentation, you will learn the technical details about the different methods used to distribute GandCrab, interesting facts about the packer, and evolution of the payload.

Covered in The Webinar

About The Speakers

Explore Valuable Cybersecurity Resources
