Spooky RYUKy: The Return of UNC1878 | SANS STAR Webcast

Published: 2020-10-28 · Archived: 2026-04-02 10:44:46 UTC

Earlier this year, Mandiant published a blog on a fast-moving adversary deploying RYUK ransomware, UNC1878. Shortly after its release, there was a significant decrease in observed UNC1878 intrusions and RYUK activity overall almost completely vanishing over the summer. But beginning in early fall, Mandiant has seen a resurgence of RYUK along with TTP overlaps indicating that UNC1878 has returned from the grave and resumed their operations. Fear not! In this webcast presenters will cover recent RYUK activity, its attribution to UNC1878, and TTPs both old and new to aid defenders in detection and response. Van Ta and Aaron Stephens Van and Aaron are Senior Threat Analysts on Mandiant’s FLARE Advanced Practices Team, pursuing adversaries across the FireEye/Mandiant ecosystem and making that knowledge actionable to frontline responders. Van comes from an extensive background in detection and response, and directly supports Mandiant incident responders by researching active adversary tradecraft to surface net new evil across the rest of FireEye/Mandiant. Aaron focuses on automation and tooling which helps the team keep up with the high operational tempo of incident response investigations. He has previously presented at the Forum for Incident Responders and Security Teams and FireEye's Cyber Defense Summit. You can find them on Twitter at @Wanna_VanTa and @x04steve.
