STAR Webcast: Spooky RYUKy: The Return of UNC1878

Published: 2020-10-28 · Archived: 2026-04-05 16:19:04 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. FOR MORE STAR WEBCASTS PLEASE VISIT: https://www.sans.org/star-webcast Speaker Bios Katie Nickels Katie is a SANS instructor for FOR578: Cyber Threat Intelligence and a Principal Intelligence Analyst for Red Canary. She has worked on cyber threat intelligence (CTI), network defense, and incident response for nearly a decade for the DoD, MITRE, Raytheon, and ManTech. Katie hails from a liberal arts background with degrees from Smith College and Georgetown University, embracing the power of applying liberal arts prowess to cybersecurity. With more than a dozen publications to her name, Katie has shared her expertise with presentations at Black Hat, multiple SANS Summits, Sp4rkcon, and many other events. Katie has also served as a co-chair of the SANS CTI Summit and FIRST CTI Symposium. She was the 2018 recipient of the President's Award from the Women's Society of Cyberjutsu and serves as the Program Manager for the Cyberjutsu Girls Academy, which seeks to inspire young women to learn more about STEM. You can find Katie on Twitter @LiketheCoins 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.
