Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:38:41 UTC

Other threat group: UNC1878

Names	UNC1878 *(FireEye)*
Country	[Unknown]
Motivation	Financial gain
First seen	2020
Description	(BleepingComputer) Wyckoff Heights Medical Center in Brooklyn and the University of Vermont Health Network are the latest victims of the Ryuk ransomware attack spree covering the healthcare industry across the U.S. Yesterday, the U.S. government hosted an emergency call with stakeholders in the healthcare industry to alert them to an 'increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.' Later in the day, CISA issued a joint advisory publicly warning that U.S. hospitals and healthcare providers are actively targeted in cyberattacks deploying the Ryuk ransomware. Charles Carmakal, senior vice president and CTO of Mandiant, told BleepingComputer that an Eastern European hacking group known as UNC1878 is responsible for these attacks and that they intend to attack hundreds of hospitals.
Observed	Sectors: Healthcare. Countries: USA.
Tools used	BazarBackdoor, Cobalt Strike, Ryuk.
Information	<https://www.bleepingcomputer.com/news/security/brooklyn-and-vermont-hospitals-are-latest-ryuk-ransomware-victims/> <https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>

Last change to this card: 05 January 2021

Download this actor card in PDF or JSON format
