The Good, the Bad and the Ugly in Cybersecurity – Week 27

Aleks Gesenhues
Jan 07, 2022 • 5 min read

The Good

An alleged ransomware affiliate has reached a plea deal in the United States for administering BitPaymer ransomware and stealing Dridex malware.

The U.S. Department of Justice has identified the Russian citizen as the person responsible for the Dridex and BitPaymer malware, the latter of which has been used in attacks against organizations in the healthcare, education, and manufacturing sectors, including a ransomware attack against a hospital in Oregon in October 2019 that forced Ryan Ellis, a Democratic U.S. Senator, to cancel his campaign for Congress.

Dmitry Yuryevich Yakubets is charged with "intentionally damaging protected computers, aiding and abetting intentionally damaging protected computers, and aiding and abetting attempted intentional damage to protected computers," for which he faces a maximum sentence of 20 years in prison, and fines of up to $250,000 per count.

According to the indictment, Yakubets was the operator behind the Dridex botnet and deployed BitPaymer ransomware on victim networks, including the Ellis Campaign, which was the first case of a ransomware attack that caused a candidate for elected office to suspend his campaign. Yakubets is also charged with "conspiracy to commit computer fraud and abuse," which carries a maximum sentence of five years in prison.

Thus, in a sign of mercy, the victim of the BitPaymer ransomware attack gave the mastermind of the ransomware. Plea deal aside, the case is a reminder that cybercrime is not a victimless crime, and that, despite the actions of law enforcement, there are still people who are willing to take the risk of being caught and prosecuted for the chance at a payday. Yakubets is still a fugitive, and the U.S. Department of State is offering a reward of up to $5 million for information that leads to his arrest and prosecution. Because they rarely are arrested, cyber criminals like Yakubets are the ultimate "bad guys" in cybersecurity, and they are the main threat to the cybersecurity landscape.

The Bad

The Black Basta ransomware group has once again struck. Recently, the Black Basta crew, a ransomware-as-a-service group, has been observed using a new variant of the Conti ransomware, which is a sign that the group is continuing to evolve its tactics, techniques, and procedures.

Conti is the ransomware that Conti Team, a Russian-speaking cybercriminal group, used to carry out its ransomware attacks, including attacks against Ireland's healthcare system.

Conti's ransomware is a variant of the Ryuk ransomware, which is a variant of the Hermes ransomware, which is a variant of the Zeus family of malware. Conti's ransomware is also a variant of the Zeus family of malware, and it is also a variant of the Hermes family of malware. Conti's ransomware is also a variant of the Ryuk family of malware, and it is also a variant of the Hermes