WastedLocker Ransomware Insights

Background

On the December 5th, 2019 the U.S. Department of Justice announced indictments against 17 individuals including 2 Russian nationals Maksim Yakubets and Igor Turashev that were the primary ring-leaders of the Russian hacking group known as “Evil Corp”. The Treasury Department Office of Foreign Assets Control (OFAC) followed up with announcement of sanctions against “Evil Corp”.

“Wanted by FBI” posters for Maksim Yakubets and Igor Turashev

At least since 2012 the criminal group operated a malware known as “Dridex” (also known as “Bugat” and “Cridex”), which was primarily delivered to victims’ systems through phishing emails. Once infected, the “Dridex” malware was able to steal users’ credentials for online financial accounts and were ultimately leveraged by cyber criminals to transfer money from the victims bank accounts to offshore accounts held by Evil Corp. In 2017 the “Evil Corp” decided to change their methodology and started to release BitPaymer ransomware through Dridex.

Even with the indictments by the US DOJ, “Evil Corp” remained just as active operating as normal. According to the Arete Cyber Threat Intelligence, in recent weeks the number of victims compromised by Dridex grew significantly (i.e. 2-3x times more than the total numbers of Trickbot, Emotet and Qbot victims combined).

Alleged Evil Corp mastermind Maksim Yakubets stands next to his Lamborghini Huracan

The recent research article by analysts from NCC Group shared a theory that “Evil Corp” group might be behind the WastedLocker ransomware (aka Wasted) which was originally spotted in the wild in May 2020. Based on the NCC Group’s assessment the link between Wasted

and Bitpaymer was made based on a few similarities between the two ransomware variants – i.e. the use of alternative data stream (ADS) and SocGholish fake update framework. Arete conducted research and determined that evidence of the connection between "Evil Corp" group and WastedLocker ransomware variant is not conclusive for 4 main reasons:

1. **Alternate Data Stream (ADS)** is often being used by cyber criminals to hide malicious files/scripts inside of legitimate files. This method is not uniquely attributed to Wasted/Bitpaymer ransomware and has been used by other ransomware variants (e.g. TeslaCrypt, CrytoWall, Maze and etc.), at least since 2015.
2. **SocGholish** is a JavaScript-based framework that has been used in "fake updates" attacks and observed downloading Dridex, Azorult InfoStealer, NetSupport Manager RAT, and Chthonic. While the Dridex banking trojan has been directly associated with "Evil Corp" and Bitpaymer, SocGholish doesn't appear to have an exclusive relationship with this group primarily because cyber criminals have been observed using various malware families to exploit and establish persistence. These cyber criminals are known to change their tactics and many have demonstrated change by adopting other cyber criminals malware, e.g. trojans/RATs have been used in deployments of other ransomware variants – e.g. Azorult was observed in Phobos attacks, NetSupport RAT has been associated with GandCrab attacks in the past.
3. **Dridex** trojan was not found on any system for all WastedLocker ransomware matters that Arete has handled to date.
4. **No overlaps in money laundering infrastructure** – blockchain analysis of payments show no overlaps in the bitcoin wallets IDs nor the exchanges used by Dridex/Bitpaymer and WastedLocker operators. While Dridex/Bitpaymer use illegal exchanges in Russia to cash out their earnings, WastedLocker operators primarily use exchanges in Asia.

WastedLocker Overview

WastedLocker is a new variant of ransomware that was initially reported in May of this year. The WastedLocker ransomware encrypts files on the victims' systems using the AES algorithm and appends the file extension .[organization initials] wasted to each file it encrypts. Wasted also generates a separate ransom note for each encrypted file. For each victim, WastedLocker operators create 2 contact email addresses which are listed in ransom notes. The ransom demands also appear to be related to the amount of research the operators have done based on what they believe the victims can afford to pay. In some instances, clients have reported compromised accounts opening financial information during the period of unauthorized access. Unlike some other ransomware variants, the decryption tool for WastedLocker is universal, meaning it will work on every system within the compromised network without requiring a unique decryptor for each system.

Continuing Research

Arete Threat Intelligence continues to work with law enforcement contacts to conduct analysis into WastedLocker. The cyber criminals behind this variant have been quick to identify and infect victims' systems with ransomware resulting in a devastating blow to the victims IT infrastructure and interrupting profitable business operations. The tactics and techniques used by the group have been stealthy and have the entire security community reacting to improve defenses, share indicators, and preemptively secure their perimeters. Research continues into the tools, tactics and procedures used by these cyber criminals.