WastedLocker explained: How this targeted ransomware extorts millions from victims

By Lucian Constantin

Published: 2020-09-22 · Archived: 2026-04-06 00:07:17 UTC

WastedLocker definition

WastedLocker is a ransomware program that started hitting businesses and other organizations in May 2020 and is known for its high ransom demands reaching millions of dollars per victim. It is the creation of a group of highly skilled cybercriminals that have been operating for over a decade despite being criminally indicted in the US.

Evil Corp and the Dridex botnet

The group behind WastedLocker calls itself as Evil Corp and some of the individuals associated with it have a long history in the cybercrime world. The group is best known for operating the Dridex malware and botnet since 2011 but has also been responsible for creating and distributing ransomware programs over the years.

Dridex, also known as Cridex or Bugat, started out as a Trojan program designed to steal online banking credentials from victims by injecting fake login pages into their browsers. In December 2019, the US Department of Justice indicted two Russian nationals named Maksim Yakubets and Igor Turashev for creating and operating the Dridex malware together with other individuals.

Yakubets has also been named in separate complaints in connection with older money heists that date back to 2009 and involved the infamous Zeus banking trojan. The source code of the Zeus trojan was leaked online in 2010 and served as a basis and inspiration for many other banking Trojans, including Dridex. Both Yakubets and Turashev are on the FBI's Cyber's Most Wanted list and US authorities are offering up to $5 million for information leading to Yakubets' arrest. The Department of Treasury has also imposed sanctions against the Evil Corp group.

Over the years, Dridex evolved from a banking Trojan into a malware distribution platform and its creators collaborated with other infamous cybercriminal groups including Carbanak/FIN7 and TA505. According to a report from security firm NCC Group, in late 2017 Dridex operations were scaled back and the group almost exclusively focused on the distribution of ransomware starting with BitPaymer. The gang even had a partnership with the group behind the TrickBot Trojan, which was used to deploy BitPaymer for a short period before starting pushing Ryuk, one of the most successful targeted ransomware programs to date.

BitPaymer targeted primarily companies from the US and a few in Western Europe, but in 2019 a fork dubbed DoppelPaymer appeared. According to NCC, DoppelPaymer followed a ransomware-as-a-service model that's different from BitPaymer's. While there's been some overlap in activity with Evil Corp, the group's links to this threat are not very clear.

“After the unsealing of indictments by the US Department of Justice and actions against Evil Corp as a group by the US Treasury Department, we detected a short period of inactivity from Evil Corp until January 2020,” NCC said in its report. “However, since January 2020 activity has resumed as usual, with victims appearing in the same regions as before. It is possible, however, that this was primarily a strategic move to suggest to the public that Evil Corp was still active as, from around the middle of March 2020, we failed to observe much activity from them in terms of BitPaymer deployments. Of course, this period coincided with the lockdowns due to the COVID-19 pandemic.”

WastedLocker replaces BitPaymer

WastedLocker is an entirely new ransomware program from Evil Corp that started infecting organizations in May. It does not share code with BitPaymer but exhibits other similarities in the ransom note and per-victim customization. The lack of Evil Corp activity between March and May might be explained by the group working on developing this new threat as well as other components that make up its toolset.

Researchers have recently seen the group deploying a variant of the Gozi malware, which might replace Dridex at some point in the future as the persistent backdoor inside victim networks, along with a customized Cobalt Strike loader, which could be a potential replacement for the Empire PowerShell framework the group was known to use. Both CobaltStrike and PowerShell Empire are post-exploitation frameworks designed for penetration testers that have also become popular with hacker groups and cybercriminals over the years. The main developers of PowerShell Empire decided to abandon the project a few months ago.

Evil Corp “has access to highly skilled exploit and software developers capable of bypassing network defenses on all different levels,” NCC warns. “The group seems to put a lot of effort into bypassing endpoint protection products; this observation is based on the fact that when a certain version of their malware is detected on victim networks the group is back with an undetected version and able to continue after just a short time. This shows the importance of victims fully understanding each incident that happens. That is, detection or blocking of a single element from the more advanced criminal actors does not mean they have been defeated.”

One of the more prominent victims of WastedLocker to date was Garmin, a US tech company that manufactures consumer wearables and GPS navigation products used in aviation, maritime, fitness and other markets. The company was hit with WastedLocker in July and had many of its services disrupted worldwide as a result, including some used by pilots. The ransom demand was reportedly $10 million and the company eventually obtained a decryption key from the attackers, although it’s not clear how much they paid for it.

Like other gangs behind targeted and manually operated ransomware attacks, Evil Corp customizes its malicious program and ransoms for each victim depending on their size and business profile. The WastedLocker ransom demands seen so far have ranged between $500,000 and $10 million, making them some of the largest in the threat landscape.

Like with BitPaymer, the vast majority of WastedLocker victims have been U.S. organizations. The gang puts a lot of effort into locating and destroying its victims’ backups, but so far it has not adopted fail-over techniques like stealing data and extorting victims under the threat of releasing it online or putting it up for auction, like some other ransomware gangs have done recently.

“In general, we can state that if this gang has found an entrance into your network it will be impossible to stop them from encrypting at least part of your files,” researchers from Malwarebytes said in an analysis. “The only thing that can help you salvage your files in such a case is if you have either roll-back technology or a form of off-line backups. With online, or otherwise connected backups you run the chance of your backup files being encrypted as well, which makes the whole point of having them moot.”

How does WastedLocker work?

According to reports from Symantec, Malwarebytes and other security firms, the infection chain for WastedLocker starts with a JavaScript-based attack framework called SocGholish that is distributed as a fake browser update by alerts displayed on legitimate but compromised websites. Hacked news websites are a common vector. The SocGholish framework is delivered as a ZIP file and, if opened and run, it starts an attack chain that involves downloading and executing PowerShell scripts and the Cobalt Strike backdoor. Evil Corp used this same distribution technique and framework in the past to deploy the Dridex Trojan, so it’s been part of its arsenal for a long time.

Once the hackers gain access to a computer on the network of an organization they perform reconnaissance and start deploying various living-off-the-land tools to steal credentials, escalate privileges and move laterally to other machines. The attackers’ goal is to identify and gain access to high-value systems such as file servers, database servers and even virtual machines running in the cloud before deploying a victim-tailored WastedLocker binary on them.

The use of manual hacking and system administration or open-source penetration testing tools are part of a trend observed over the past few years where cybercriminals, including ransomware gangs, are increasingly adopting attack techniques that in the past used to be associated with cyberespionage activity by state-sponsored groups. This trend poses a serious problem for smaller organizations who do not have the IT budgets and resources to deploy defenses against advanced persistent threats but are a frequent target for ransomware gangs and other financially motivated cybercriminals.

WastedLocker uses a combination of AES and RSA cryptography in its file encryption routine that is similar to other targeted ransomware programs. Every file is encrypted with a unique 256-bit AES key that’s generated on the fly. Those AES keys together with other information about the encrypted files are then encrypted with a 4096-bit public RSA key that is hardcoded in the WastedLocker binary. The attackers retain the private part of the RSA key pair which is needed to recover the AES keys and decrypt individual files.

According to an analysis by Kaspersky Lab, the encryption routine is strong and properly implemented, so victims cannot recover their files without the attackers’ private RSA key. Since this is a manually deployed ransomware threat that’s customized for every target, the attackers generate unique RSA key pairs for each victim. This means a private key received by one organization after paying the ransom won’t work to decrypt files from another impacted organization.

Some aspects of WastedLocker make it stand apart. The ransomware has a mechanism that allows attackers to prioritize certain directories during the encryption routine. This is likely used to ensure that the most important

and valuable files are encrypted first in case the encryption process, which can take some time, is detected by system administrators and is halted while in progress.

The malware attaches a file extension made from the victim's name and the word "wasted" to every encrypted file, for example, original_file_name.garminwasted for the Garmin attack. It also generates a text file with the ransom note for every file, meaning every directory will contain hundreds or thousands of copies of the ransom note.

WastedLocker is designed to delete shadow copies — the default backups made by the Windows OS — and tries to encrypt files over the network, including remote backups. It uses privilege escalation techniques such as DLL hijacking to obtain system privileges and installs a service that performs the encryption routing. This service is stopped when the encryption process is complete.

"The attackers behind this threat appear to be skilled and experienced, capable of penetrating some of the most well protected corporations, stealing credentials, and moving with ease across their networks," the Symantec researchers said. "As such, WastedLocker is a highly dangerous piece of ransomware. A successful attack could cripple the victim's network, leading to significant disruption to their operations and a costly clean-up operation."

Source: https://www.csoonline.com/article/3574907/wastedlocker-explained-how-this-targeted-ransomware-extorts-millions-from-victims.html