Ransomware Roundup: New Inlock and Xorist Variants

November 10, 2022

FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The bi-weekly Ransomware Roundup report provides brief insights into the evolving ransomware landscape along with the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers the Inlock ransomware and a new variant of the Xorist ransomware that appears to target Cuba.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption
Severity level: High

Inlock Ransomware

Inlock is a typical ransomware that encrypts files on a compromised machine and demands ransom from a victim in exchange for recovering the affected files.

Files encrypted by this latest variant have a “.inlock” file extension. It also leaves a ransom note titled READ_IT.txt, which contains a ransom message in Spanish.

Figure 1. Ransom message dropped by Inlock ransomware

The ransom message translated into English reads:

¡¡YOUR COMPUTER HAS BEEN ENCRYPTED!!! We are very sorry, but you have been the target of a cyber attack. All your personal data has been encrypted. Please contact me to negotiate the ransom. Once I receive the payment, I will send you the decryption tool to decrypt all the files. I hope you have nothing of great value ;)

Do not lose the following code or you will never be able to recover your data again:

It also changes the desktop wallpaper.

Figure 2. Desktop Wallpaper replaced by Inlock ransomware

An apparent design failure in the Inlock ransomware is that it does not provide any contact information so victims can reach out to the attacker about file decryption. The ransomware also deletes volume shadow copies. With no attacker contact information available, victims cannot recover their encrypted files.

New Variant of Xorist Ransomware

FortiGuard Labs also recently came across a new variant of the Xorist ransomware. The Xorist ransomware family has been in the wild for at least five years, with some reports suggesting its lifespan has been closer to a decade.

While we do not know precisely how this new Xorist ransomware variant is distributed to victims, there are a few clues. For example, the ransomware’s executable file is named “Ley del Presidente y Vicepresidente de la República de Cuba.pdf.exe,” which translates to “Law of the President and Vice President of the Republic of Cuba.pdf.exe.” Another clue is that relevant samples were primarily submitted to VirusTotal on October 31st from Cuba.

Coincidentally, a benign PDF file, “Ley del Presidente y Vicepresidente de la República de Cuba.pdf,” was submitted to VirusTotal on the same day. This PDF is labeled as the “Official Gazette of the Republic of Cuba” on the National Assembly of People's Power held in late 2020. Its parent file is a self-extracting .rar file that contains the PDF file but is also designed to launch a missing “You Are Hacked.exe” application, which is the name of the file being dropped by samples of this Xorist ransomware variant. We believe that the missing “You Are Hacked.exe” application was removed by the VirusTotal uploader prior to the file submission.

This information leads us to believe that the attacker prepared two types of files to distribute the Xorist variant: a fake PDF file that attempts to fool victims into thinking they’ve opened a legitimate file issued by the Cuban government and another fake PDF file that is actually a malicious executable.

Figure 3. Benign PDF file included in “Ley del Presidente y Vicepresidente de la República de Cuba.pdf.exe”

The Xorist ransomware variant leaves a ransom note in Spanish.

Figure 4. Ransom message dropped by the Xorist ransomware variant

The ransom message translated into English reads:

ATTENTION!
ALL YOUR FILES ARE ENCRYPTED! To restore your files and access them, please send $100 in Bitcoin to this QR code.

IF YOU DO NOT PAY WITHIN 48 HOURS ALL YOUR FILES WILL BE DELETED IRREVERSIBLY YOU HAVE 5 ATTEMPTS TO ENTER YOUR CORRECT CODE.

The ransom demand is $100 worth of Bitcoin, which is considered cheap for Enterprises.

These clues are enough for us to conclude that this Xorist ransomware variant was likely designed to target consumers in Cuba.

The ransomware also replaces the desktop wallpaper with a ransom message. It includes a QR code with the attacker’s Bitcoin wallet address. As of this writing, this wallet has not recorded a single transaction.

Figure 5. Desktop wallpaper with QR code replaced by the Xorist ransomware variant

Fortinet Protections

Fortinet customers are already protected from these malware variants through FortiGuard’s Web Filtering, AntiVirus, FortiMail, FortiClient, and FortiEDR services, as follows:

FortiGuard Labs detects the ransomware variants covered in this blog with the following AV signatures:

- W32/Filecoder.Q!tr.ransom
- PossibleThreat

- W32/PossibleThreat

IOCs

Inlock ransomware variant

96e48ea92e40ebe25e26aa769b38cbe27f26f2718d184a6ba2fd3bb900992ebd

Xorist ransomware variant

- 14cdb3735feec79d1bfbbcca899bc209b20e97283e7e600ff930b0019abeaef6
- 7d3075d8426c817154b05b695d6196e5ea977a67d0132cf552851f237c166f5e
- 097f45297c3595c45ccf60dff0508e77cbd7b96c9f1caca172635dcccf04f7a3
- 95c2dd45f074296cbbbfb37c004ebdf3db4240821cb8a8bba5ce6710285e4b4d

- 38f226d2c7ac8a803d3d1233a234a0c60d2ce88528fcf48092223e88eedf5023 (benign PDF file)

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.