Ransomware Roundup: LockBit, BlueSky, and More

fortinet.com/blog/threat-research/ransomware-roundup-new-variants

July 18, 2022

Over the past few weeks, FortiGuard Labs has observed several new ransomware variants of interest that have been gaining traction within the OSINT community along with activity from our datasets. This isn't new. This same thing has been going on, week in and week out, for years, with very little changing.

Unfortunately, ransomware is here to stay. Ransomware infections continue to cause significant impact to organizations, including—but not limited to—disruptions to operations, theft of confidential information, monetary loss due to ransom payout, and more. It's why we feel it's imperative that we increase our efforts to raise awareness about existing and emerging ransomware variants.

This new Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape, along with the Fortinet solutions that protect against these variants.

This latest edition of the Ransomware Roundup covers the LockBit, BlueSky, Deno, RedAlert, Dark Web Hacker, Hive, and Again ransomware.

LockBit Ransomware

LockBit is a ransomware strain that targets both Windows and Linux. It has been in the wild since December 2019. This ransomware employs a Ransomware-as-a-Service (RaaS) model. Ransomware operators develop LockBit ransomware and all the necessary tools and infrastructure to support it, such as leak sites and ransom payment portals. They offer these solutions, along with user support, to their affiliates (criminals who pay a fee to use their technology). Support is provided via TOX (a RaaS framework). They also offer additional services, such as ransom negotiation, for affiliates.

LockBit affiliates carry out the actual attacks that infect and deploy ransomware to targets and, in return, receive 20% of the ransom paid by victims. While rules prohibit affiliates from encrypting files in critical infrastructure environments, such as nuclear power plants or gas and oil industries, affiliates are allowed to steal data without encrypting critical files and or the infrastructure of these organizations. In addition, former Soviet countries (Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine, and Estonia) are off-limits from attack.

Figure 1. Affiliate rules for LockBit 3.0 on its Tor site

Prior to file encryption, data on victim machines is exfiltrated using “StealBit,” an information stealer tool developed by the LockBit gang. Files encrypted by the ransomware typically have a “.lockbit” file extension. The ransomware also leaves a ransom note in Restore-My-Files.txt.

Some variants of LockBit also replace desktop wallpaper with a message to let victims know that they are a victim of the ransomware, asking them to check the ransom note for how to reach out to the LockBit threat actor. LockBit employs a double-extortion tactic that demands victims pay their ransom in Bitcoin to recover affected files and not have stolen information leaked to the public.

LockBit 3.0 debuted in March 2022 as a successor to LockBit 2.0. The ransomware made the news again at the end of June because the ransomware gang introduced a “bug bounty” program with rewards of between $1000 and $1,000,000 (USD) for detecting flaws and weaknesses in its portfolio.

Figure 2. Bug bounty program advertised on LockBit Tor site

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected by the following signature(s):

W32/Filecoder.LOCKBIT!tr

W32/Filecoder_Lockbit.A!tr

W64/Lockbit.A!tr

W64/Lockbit.A!tr.ransom

W32/Lockbit.B!t

W64/Lockbit.B!tr

W32/Lockbit.D!tr.ransom

W32/Lockbit.E!tr.ransom

W32/Lockbit.D!tr.ransom

W32/Lockbit.E!tr.ransom

W32/Filecoder_Lockbit.E!tr

W32/Filecoder_Lockbit.E!tr.ransom

W32/LockBit.2513!tr.ransom

W32/LockBit.29EA!tr.ransom

W32/LockBit.29FC!tr.ransom

W32/Lockbit.2D74!tr.ransom

W32/LockBit.921B!tr.ransom

W32/Lockbit.A467!tr

W32/Lockbit.BF6C!tr

W32/Lockbit.C2F8!tr.ransom

W32/Lockbit.FSWW!tr

W32/Lockbit.GCZ!tr

W32/Lockbit.NVBZVOW!tr

W32/Lockbit.VHO!tr

W32/Lockbit.VHO!tr.ransom

W32/Ransom_Win32_LOCKBIT.ENC

HTML/Lockbit.FCBE!tr.ransom

BlueSky Ransomware

BlueSky is a recently discovered ransomware variant, with some BlueSky ransomware samples distributed online as “MarketShere.exe” and “SecurityUpdate.exe.” BlueSky encrypts files on a compromised machine and then adds a “.bluesky” file extension. It then drops a ransom note in “# DECRYPT FILES BLUESKY #.txt“and “# DECRYPT FILES BLUESKY #.html,” in which victims are asked to visit a BlueSky TOR site and follow provided instructions.

Figure 1. BlueSky ransom message in a text file

Figure 2. Bluesky Ransom Message (HTML)

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected by the following signature(s):

W32/Conti.F!tr.ransom

W64/GenKryptik.FSFZ! tr

Deno Ransomware

Deno is a new ransomware variant that encrypts files on a compromised machine and adds a “.DENO” file extension to targeted files. It then drops a ransom note in “readme.txt” which provides two ProtonMail email addresses for victims to contact the attacker to recover affected files. Interestingly enough, there is no information on how much this will cost and if payment is what the threat actor is ultimately after.

Figure 3. Readme.TXT for DENO ransomware

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected by the following signature(s):

W32/Filecoder.OLQ!tr

MSIL/Agent.MDO!tr.ransom

Malicious_Behavior.SB

W32/PossibleThreat

RedAlert

RedAlert, also known as N13V, is a new ransomware discovered in early July. It affects Windows and Linux VMWare (ESXi) servers. It encrypts files on the compromised machine and steals data from it. One reported file extension that this ransomware variant adds to affected files is ".crypt658", but this may change depending on the victim.

This ransomware uses a double-extortion tactic, which demands a ransom payment to recover affected files and prevents the release of stolen data to its data leak site for anyone to download. To pressure victims into paying a ransom, the authors also ask the victim to contact the attacker within 72 hours, or else the threat actor will publish part of the stolen data to their leak site. Additional threats include launching Distributed Denial of Service (DDoS) attacks against the victim and making phone calls to the victim's employees as a shame tactic.

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected by the following signature(s):

ELF/RedAlert.A!tr.ransom

Dark Web Hacker

Dark Web Hacker is another recently discovered ransomware. It encrypts files on a compromised machine and appends ".[4 random characters}" to target files and the end of the file name. It also leaves a ransom note in "read_it.txt" containing an attacker's contact email address and Bitcoin address. Ransom demand is $3,000 worth of Bitcoin.

Figure 4. Ransom note

The ransomware also replaces any desktop wallpaper with its own wallpaper that includes a Bitcoin QR code to "help" victims to pay a ransom.

The ransomware also deletes shadow copies, which makes file recovery difficult.

Fortinet Protections

Fortinet Customers running the latest (AV) definitions are protected by the following signature:

MSIL/Filecoder.AGP!tr

Hive

Hive ransomware is another Ransomware-as-a-Service (RaaS) that attempts to encrypt files on victims' machines, steal data, and demand a payment to recover affected files and prevent stolen data from being published to their data leak site, called "HiveLeaks," on the DarkWeb. This ransomware notoriously affected Costa Rica's public health system, which was reportedly disrupted by the ransomware.

The latest iterations are written in the Rust programing language. Older variants are written in Go.

Decryptor Tool Now Available

On July 13th, security researcher @reecDeep released a v5 keystream decryptor tool for Hive ransomware. The tool can be found on @reecDeep's Github page.

Fortinet Protections

FortiGuard Labs previously released a Threat Signal for Hive ransomware report. For additional information on Hive ransomware, please visit this link.

Fortinet Customers running the latest (AV) definitions are protected by the following signature:

W64/Filecoder_Hive.A!tr.ransom

W64/Filecoder_Hive.A!tr

What is 'Again' ransomware?

The Again ransomware is another new ransomware variant that seems to have its origins in Babuk. It appears to share the same source code as Babuk (which had its entire source code leaked in 2021) and can safely be considered a fork of that variant. The Again ransomware seeks out files to encrypt and appends ".again" to the filename, rendering them inoperable.

Victims are presented with a text file entitled "How To Restore Your Files.txt." It contains information on contacting the bad actor(s) behind the ransomware using a predefined TOR website. On this site, the page has a submit message page to the ransom actor, who will likely seek something in return from the victim in exchange for their files.

Fortinet Protections

Fortinet Customers running the latest (AV) definitions are protected by the following signature:

W64/Filecoder_Rook.B!tr.ransom

Best practices include not paying a ransom

Victims of ransomware are cautioned against paying ransom by organizations such as CISA, NCSC, the FBI, and HHS, partly because payment does not guarantee files will be recovered. 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, according to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory. The FBI has a Ransomware Complaint page, where victims can submit samples of ransomware activity via the Internet Crimes Complaint Center (IC3).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.