Contents

Executive Summary ........................................................................................................................................................................... 3
BL00dy ......................................................................................................................................................................................... 5
Ballacks ...................................................................................................................................................................................... 6
BISAMWARE .................................................................................................................................................................................. 7
BlackBit ....................................................................................................................................................................................... 8
Executive Summary

Orion is an integral department in Cynet’s research team that works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in Bleeping Computer – the most up-to-date website that summarizes the newest ransomware variants – and shares how Cynet detects against these threats.
Bl00dy Ransomware
- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .bl00dy
- Ransomware note: How To Restore Your Files.txt
- Sample hash: ef0ee6a6a64347082e09729cd535150b2d4196f4e4e925a307c2ca46f96a

Cynet 360 AutoXDR™ Detections:

Bl00dy Overview
Bl00dy ransomware renames the encrypted files with .bl00dy in the extension.

Once a computer’s files have been encrypted and renamed, it drops a note as “How To Restore Your Files.txt”:

The ransomware note contains general information, warnings, and the attacker’s email address.
Ballacks Ransomware

- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .ballacks
- Ransomware note: ReadthisforDecode.txt
- Sample hash: 6e457720acc91317e6318ab1b1cc053d67ea3b8082a0b22ea970f6fe299c8f14

Cy.net 360 AutoXDR™ Detections:

Ballacks Overview
Ballacks ransomware renames the encrypted files with .ballacks in the extension:

Once a computer's files have been encrypted and renamed, it drops the ransomware note named ReadthisforDecode.txt:

The ransomware note contains general information, warnings, and the attacker's email address:
BISAMWARE Ransomware
- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .BISAMWARE
- Ransomware note: SYSTEM=RANSOMWARE=INFECTED.TXT
- Sample hash: 26ed1ffe74abd8a56fd4f34a6e2ebbaa04d43e7a9b9d4b9d283e184b35fd4

Once a computer’s files have been encrypted and renamed, it drops a note named:
SYSTEM=RANSOMWARE=INFECTED.TXT

The ransomware note contains general information, warnings, and the attacker’s Tor chat:
BlackBit Ransomware
- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .BlackBit
- Ransomware note: Restore-My-Files.txt
- Sample hash: 1d0930fed7eb72f1338b0aed5d47e7271dce9f920d839050acc2df9d85b71c8

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and several attacker’s links:

BlackBit Overview
BlackBit ransomware renames the encrypted files with .BlackBit in the extension:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and several attacker’s links:
Thank you!

September, 2022