Watch Out for 'Latrodectus' - This Malware Could Be In Your Inbox

Date: 11th April 2024 | Severity: High

Summary

A new malware strain named Latrodectus, considered an offshoot of the IcedID loader has been implicated in malicious email activities. This malware is introduced to targets through deceptive copyright infringement notices submitted via online forms, leading receipients to a malicious links.

Latrodectus functions as a downloader, and its primary objective is to download payloads and execute arbitrary commands. Its sandbox evasion techniques are noteworthy, and it shares similarities with the IcedID malware. This assessment suggests Latrodectus was likely developed by the same group as IcedID.

Attack Vectors

- The malware was likely created by the Lunar Spider, the developers of the IcedID banking Trojan and loader (AKA BokBot). Latrodectus is distributed by initial access brokers, such as TA577 (AKA Hive0118) and TA578, to load additional malware.
- Latrodectus, written in C, usually spreads as part of phishing campaigns that involve the sending of fake online contact forms or copyright infringement notices. These phishing messages entice victims into clicking on embedded links that lead to attacker-controlled URLs. These URLs download malicious JavaScript files that leverage the msiexec command to execute an MSI installer from a WebDAV share, which contains the Latrodecturs DLL payload.
- Once deployed, Latrodectus performs several anti-analysis and sandbox evasion checks before installing itself in a subdirectory of the user's AppData folder. The malware creates a scheduled task for persistence, and then establishes a connection with a command and control (C2) server over HTTP/S to launch incoming commands, such as file enumeration, process termination, shellcode execution, and collection of system data. In addition, Latrodectus can update itself and execute additional malware, such as DanaBot and Lumma Stealer.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 378d220bc863a527c2bca204daba36f10358e058df49ef088f8b1045604d9d05 • e27c6586dba78d5d302589f3b231be40 • d9471b038c44619739176381815bfa9a13b5ff77021007a4ede9b146ed2e04ec • dedbc21afc768d749405de535f9b415baaf96f7664ded55d54829a425fc61d7e • ee1e5b80a1d3d47c7703ea2b6b64ee96283ab3628ee4fa1fef6d35d1d9051e9f • f9c69e79e7799df31d6516df70148d7832b121d330beebe52cff6606f0724c62 • 3b63ea8b6f9b2aa847faa11f6cd3eb281abd9b9cceedb570713c4d78a47de567 • 5d881d14d2336273e531b1b3d6f2d907539fe8489cbe80533280c9c72efa2273 • 77270e13d01b2318a3f27a9a477b8386f1a0ebc6d44a2c7e185cfbe55aac8017 • 71fb25cc4c05ce9dd94614ed781d85a50dccf69042521abc6782d48df85e6de9 • 88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef • 97e093f2e0bf6dec8392618722dd6b4411088fe752bedece910d11fffe0288a2 • 9c27405cf926d36ed8e247c17e6743ac00912789efe0c530914d7495de1e21ec • 305031a6d93a744cf61552ab673ddb27843ee845 • 6e008b699fb7ba79a0fbd9ddc7fe975a • aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c • f9425561701935d358f4f5b7fc2e5502 • 46b5367c51540b5b78c64d01e70115b5fcc42aa3 • 9b5ee969ca96ba0d4547a6041c5a86bf80fd4c96 • 9b914f9c593b3e6c3af27ae2310e9ca9 • 876c5d995847eb3acfbe3a546648a7fb • d98cd810d568f338f16c4637e8a9cb01ff69ee1967f4cfc004de3f283d61ba81
URLs	• https://plwskoret[.]top/live/ • https://miistoria[.]com/live/ • https://zumkoshapsret[.]com/live/ • https://jertacco[.]com/live/ • https://ginzbargatey[.]tech/live/ • https://grebiunti[.]top/live/ • https://mastralakkot[.]live/live/ • https://lemonimonakio[.]com/live • https://mazdakrichest[.]com/live/ • https://nimeklroboti[.]info/live/ • https://plwskoret[.]top/live • https://miistoria[.]com/live • https://minndarespo[.]icu/live/ • https://peermangoz[.]me/live/ • https://riverhasus[.]com/live/ • https://drifajizo[.]fun/live/ • https://scifimond[.]com/live/ • https://sluitionsbad[.]tech/live/ • https://aprettopizza[.]world/live
Domains	• marypopkinz[.]com • defifya[.]org • interiourbydennis[.]com • luhuhu[.]org

Domains	• fuwer[.]org • simanay[.]org • nevujo[.]org • sabehey[.]org • zefos[.]org • hofaty[.]org • ticava[.]org • mayanui[.]com • cuxu[.]org • mypusau[.]org • gotuqoa[.]org • fazadoe[.]org • xacygo[.]org • qeqady[.]org • intellipowerinc[.]com • pubonao[.]org • web3rse[.]com • quwezui[.]org • zuwagie6[.]org
IP Address	• 77.91.73[.]187 • 104.21.78[.]216 • 74.119.193[.]200 • 178.208.87[.]21 • 178.23.190[.]199 • 95.164.3[.]171 • 128.140.36[.]37 • 157.90.166[.]88 • 162.55.217[.]30

Recommendation

- Prioritize application installations from your organization's library of approved applications (if implemented).
- Treat files downloaded from the Internet with the same vigilance as those delivered through email.
- Assume files are potentially hostile regardless of the path that got you there. Remember, a website hosting software advertised on a trusted search engine does not inherit that trust.
- Encouraging good cybersecurity hygiene among your users by using Phishing and Security Awareness Training (PSAT) when downloading software from the Internet.
- Protect endpoints against malware by:Ensuring antivirus signatures are up-to-date.
- Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/watch-out-for-latrodectus-this-malware.html
- https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/the-rise-of-latrodectus-malware/109122169
- https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice