Spain warns of LockBit Locker ransomware phishing attacks

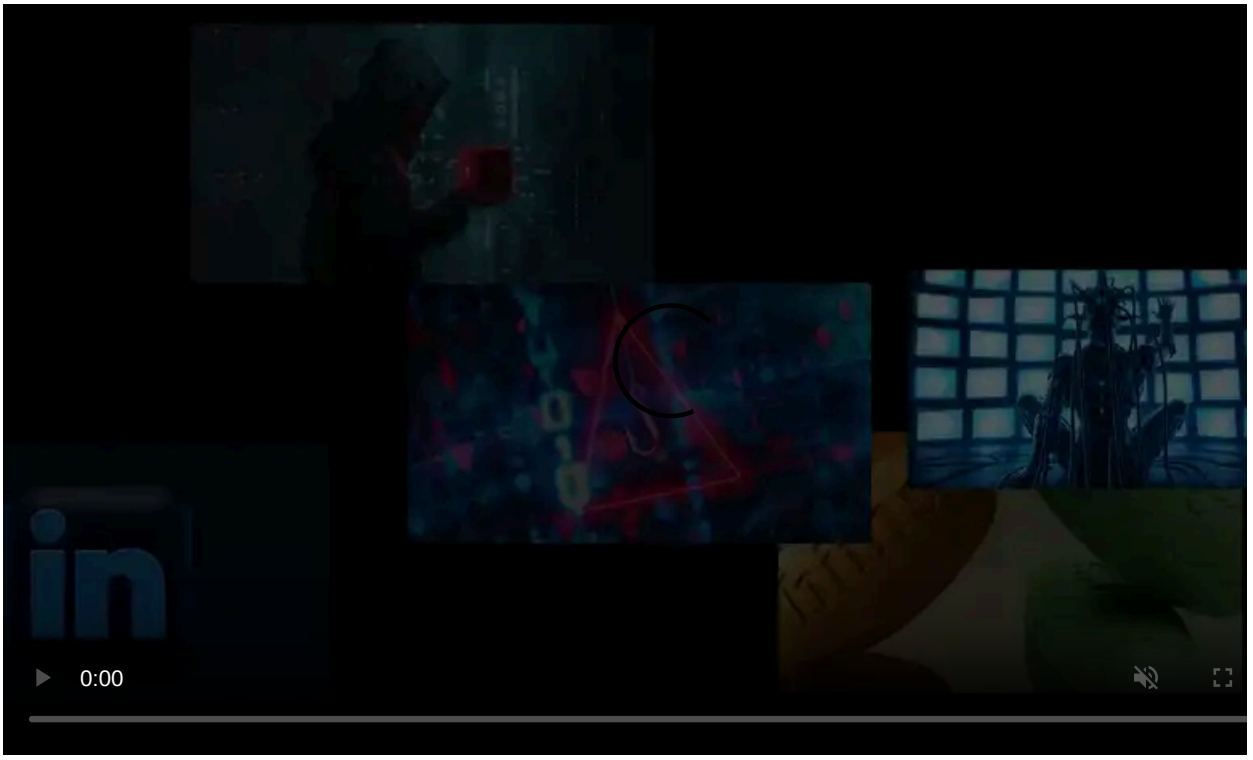
By Bill Toulas

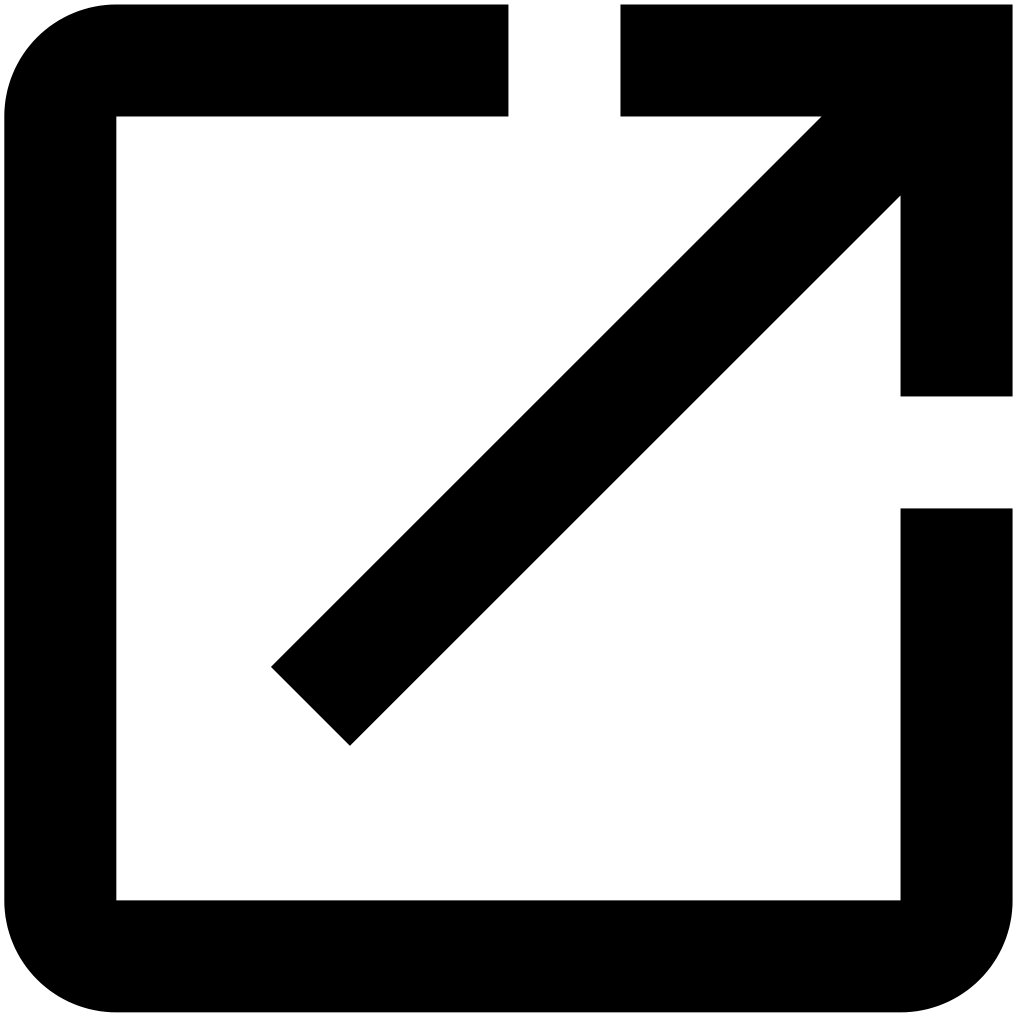
Published: 2023-08-28 · Archived: 2026-04-05 15:27:31 UTC

The National Police of Spain is warning of an ongoing 'LockBit Locker' ransomware campaign targeting architecture companies in the country through phishing emails.

"A wave of sending emails to architecture companies has been detected, although it is not ruled out that they extend their action to other sectors," reads the machine-translated police announcement.

"The detected campaign has a very high level of sophistication since the victims do not suspect anything until they suffer the encryption of the terminals."


0:00



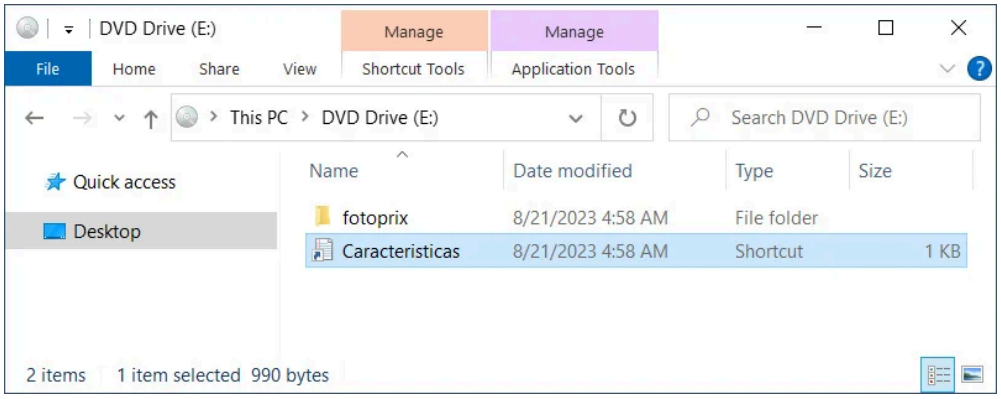
Spain's cyber police have detected that many emails are sent from the non-existent domain "fotoprix.eu" and impersonate a photographic firm.

The threat actors pretend to be a newly launched photography store requesting a facility renovation/development plan and a cost estimate for the work from the architecture firm.

After exchanging several emails to build trust, the LockBit operators propose to specify a meeting date to discuss the budget and details of the building project and send an archive with documents on the exact specifications of the renovation.

While the Spanish polish does not provide much technical detail, in a sample seen by BleepingComputer, this archive is a disk image (.img) file that, when opened in newer versions of Windows, will automatically mount the file as a drive letter and display its contents.

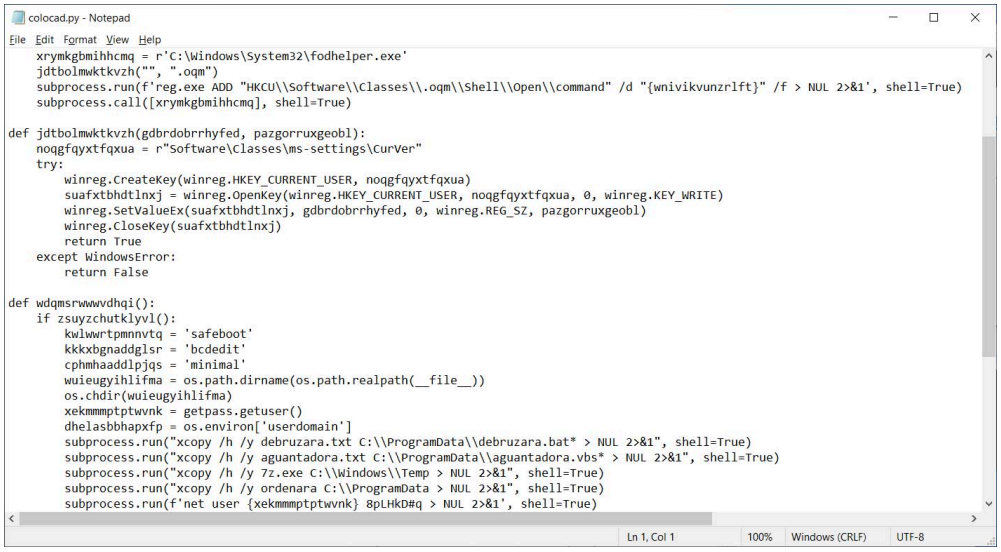
These archives contain a folder named 'fotoprix' that includes numerous Python files, batch files, and executables. The archive also contains a Windows shortcut named 'Caracteristicas,' that, when launched, will execute a malicious Python script.



IMG file contents

Source: BleepingComputer

BleepingComputer's analysis shows that the executed Python script will check if the user is an admin of the device, and if so, make modifications to the system for persistence and then executes the 'LockBit Locker' ransomware to encrypt files.



Malicious Python script

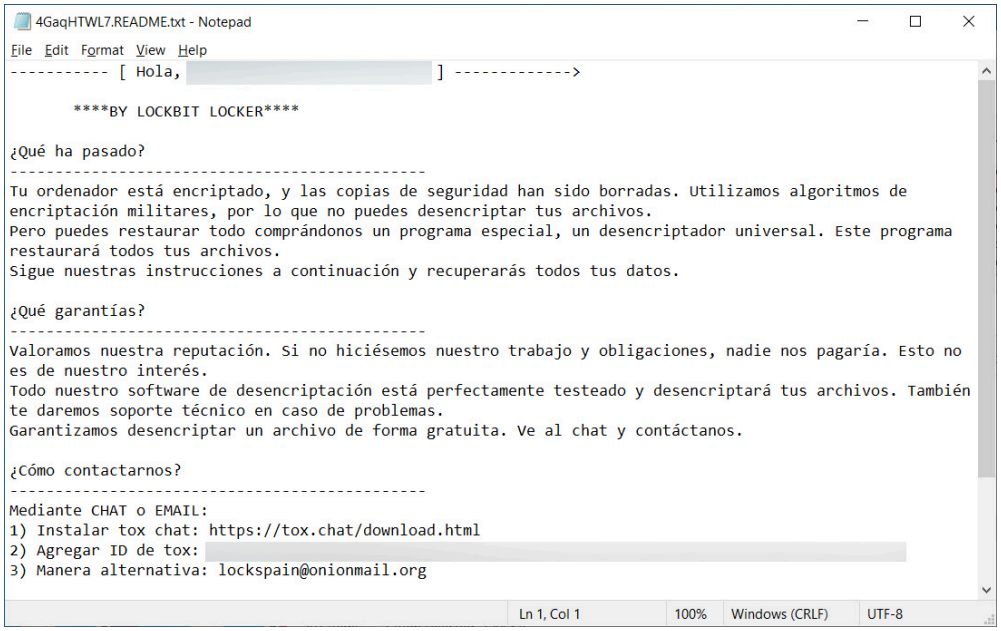
Source: BleepingComputer

If the Windows user is not an admin on the device, it will use the Fodhelper UAC bypass to launch the ransomware encryptor with admin privileges.

The Spanish police underline the "very high level of sophistication" of these attacks, particularly noting the consistency of the communications that convince victims they interact with individuals genuinely interested in discussing architectural project details.

While the ransomware gang claims to be affiliated with the notorious LockBit ransomware operation, BleepingComputer believes this campaign is conducted by different threat actors using the leaked LockBit 3.0 ransomware builder.

The regular LockBit operation negotiates through a Tor negotiation site, while this 'LockBit Locker' negotiates via email at 'lockspain@onionmail.org' or via the Tox messaging platform.



LockBit Locker ransom note

Source: BleepingComputer

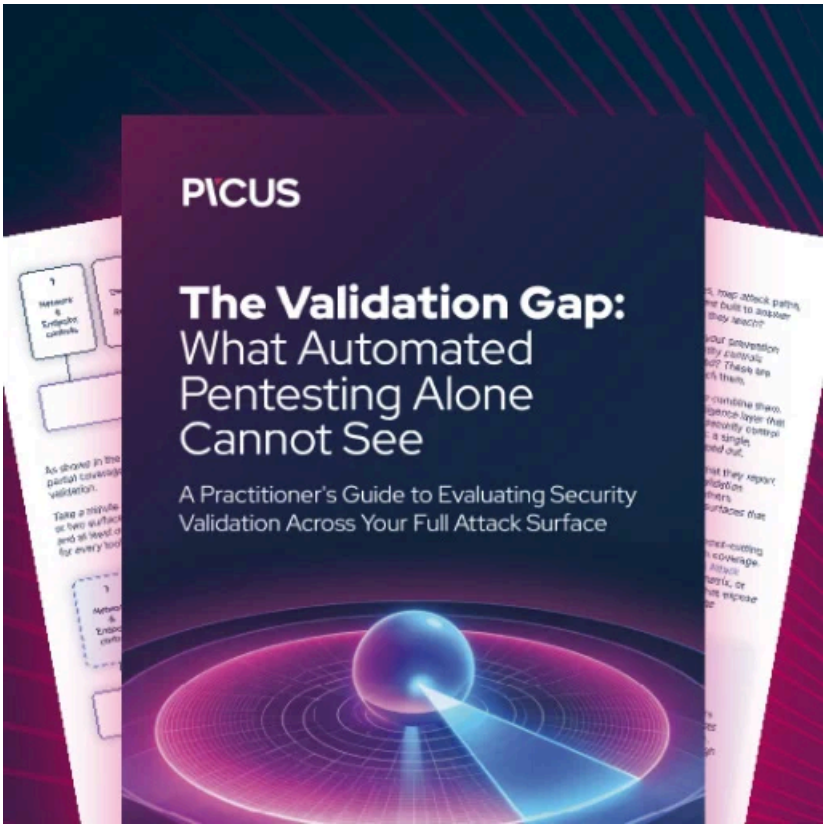
Furthermore, automated analysis by Intezer's scanning engine identifies the ransomware executable as being BlackMatter, a ransomware operation that shut down in 2021 and later rebranded as ALPHV/BlackCat.

However, this is expected, as the leaked LockBit 3.0 builder, also known as LockBit Black, is also identified by Intezer as BlackMatter for its use of BlackMatter source code.

Given the reported sophistication of the phishing emails and social engineering seen by BleepingComputer, it is likely that the threat actors behind this campaign are using different lures for companies in other sectors.

Phishing actors have extensively used the "call to bid" bait in campaigns impersonating private firms or government agencies and using well-crafted documents to convince of the legitimacy of their messages.

Notorious ransomware gangs adopting similar practices for initial compromise is a worrying development, as posing as legitimate customers could help them overcome obstacles like their targets' anti-phishing training.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/spain-warns-of-lockbit-locker-ransomware-phishing-attacks/