FBI Publishes IOCs for LockBit 2.0 Ransomware Attacks

By Ionut Arghire on February 07, 2022

The Federal Bureau of Investigation (FBI) on Friday released indicators of compromise (IOCs) associated with the LockBit 2.0 ransomware.

LockBit 2.0, which is distributed as a Ransomware-as-a-Service (RaaS), makes detection and mitigation difficult, due to the use of a variety of tactics, techniques, and procedures (TTPs).

The ransomware's operators breach enterprise networks either by purchasing access or by compromising them through unpatched vulnerabilities, zero-day exploits, or insider access, the FBI says.

Once inside a network, publicly available tools such as Mimikatz are employed for privilege escalation. Both off-the-shelf and custom tools are employed for data exfiltration, and then the LockBit ransomware is used to encrypt the victim's files.

A ransom note that the attackers place in the affected directories provides the victim with instructions on how they can obtain a decryption tool, but also contains the threat that the stolen data will be leaked online on a LockBit 2.0 site, unless a ransom is paid.

[READ: SecurityWeek Cyber Insights 2022: Ransomware]

"In July 2021, LockBit 2.0 released an update which featured the automatic encryption of devices across windows domains by abusing Active Directory group policies. In August 2021, LockBit 2.0

began to advertise for insiders to establish initial access into potential victim networks, while promising a portion of the proceeds from a successful attack," the FBI warns.

The ransomware's operators also created a Linux-based malware variant that exploits vulnerabilities within VMware ESXi virtual machines.

Heavily obfuscated, the LockBit 2.0 malware uses bitwise operations for string decoding and the loading of modules, which increases evasion. It attempts to escalate privileges when needed and only targets systems that do not use a set list of Eastern European languages.

The ransomware deletes log files and shadow copies, harvests system information and then attempts to encrypt all data on local and remote drives, while skipping files used for core system functions. Once the encryption process has been completed, the malware deletes itself from the disk.

Readily available in the LockBit panel, the Stealbit application that is typically used for data exfiltration allows attackers to configure the desired file types that will be copied to an attacker-controlled server over HTTP. Commercially available tools and sharing sites may also be used for data theft.

LockBit operators last week claimed they hacked cryptocurrency exchange PayBito and stole the information of roughly 100,000 customers, threatening to publish the data online on February 21.

Related: Walmart Dissects New 'Sugar' Ransomware

Related: Ransomware Gang Leaks Files Allegedly Stolen From Accenture

Related: Attackers Encrypt VMware ESXi Server With Python Ransomware

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Microsoft Ups Office Protections With Improved Blocking of Macros
Android's February 2022 Security Updates Patch 36 Vulnerabilities
Data of Puma Employees Stolen in Kronos Ransomware Attack
High-Severity Flaw in Argo CD Is Information Leak Risk
Google Cloud Gets Virtual Machine Threat Detection

Tags:

NEWS & INDUSTRY Virus & Threats Virus & Malware Malware Cybercrime