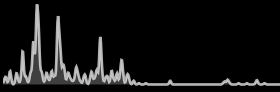


RANSOMWARE

LockBit3.0

0 mentions in the last 2 weeks



596 articles in the last 12 months

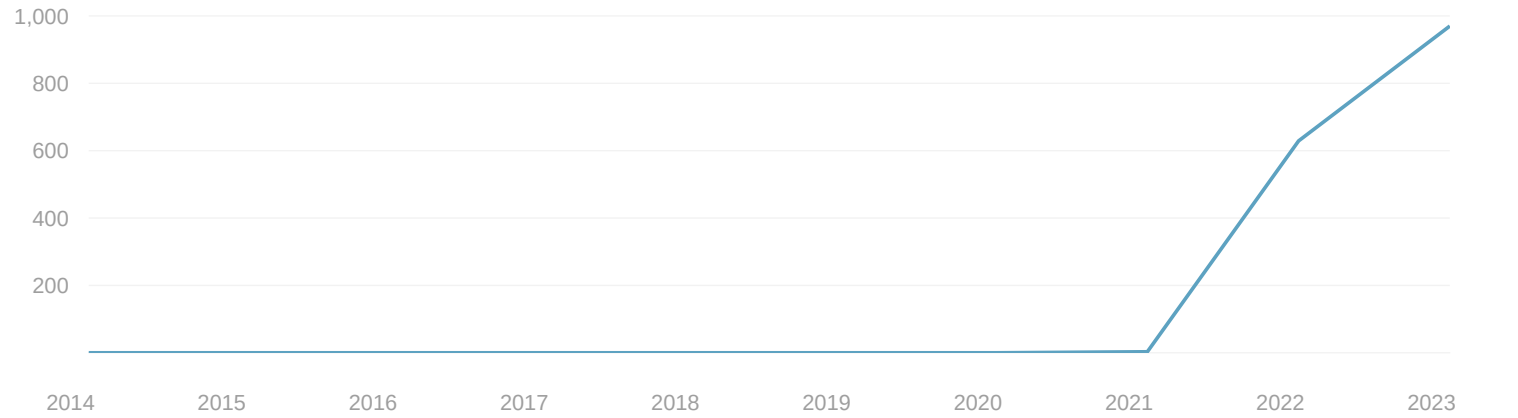


Using open-source data collected by Feedly AI.

Overview

LockBit 3.0, also known as LockBit Black, is a sophisticated ransomware variant that emerged in June 2022. It operates under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to target a wide range of organizations globally. This variant is modular and evasive, featuring a payload that remains encrypted until execution, complicating malware analysis and detection. LockBit 3.0 checks the... [See More](#)

Article count



Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
Others	<ul style="list-style-type: none">SIRVASummit Health	<u>1</u> <u>2</u>	12 months ago 13 months ago
3 articles			

Top threat actors using this malware

No threat actors have been linked to this malware at the moment

Tactics, Techniques, and Procedures

Last mentioned ▾

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES
Financial Theft	T1657	<u>15</u>	<u>2</u>	<u>14</u>
Data Encrypted for Impact	T1486	<u>2</u>	<u>2</u>	<u>2</u>
Phishing	T1566	<u>5</u>	<u>5</u>	<u>4</u>
Valid Accounts	T1078	<u>3</u>	<u>7</u>	<u>2</u>
Create Account	T1136	<u>1</u>	<u>4</u>	<u>1</u>

Resource Hijacking	T1496	<u>1</u>	0	<u>1</u>
Clear Windows Event Logs	T1070.001	<u>1</u>	<u>3</u>	<u>1</u>
Disable or Modify Tools	T1562.001	<u>1</u>	<u>4</u>	<u>1</u>
Remote Desktop Protocol	T1021.001	<u>3</u>	<u>8</u>	<u>2</u>


Exploited vulnerabilities

CVE ID	CVSS SCORE ↕	EPSS SCORE ↕	VENDOR	PRODUCT	TREND	WEAPONIZED ↕	ARTICLES ↕
CVE-2023-4966	CVSS 7.5	97%	Citrix	netScaler_gateway		Nov 10, 2023	<u>27</u>
Sensitive information disclosure vulnerability in Citrix NetScaler ADC and NetScaler Gateway products when configured as a Gateway (VP...							


Detection Rules

RULE	ARTICLES	COUNT	ACTION
Sigma rules	0	1	<div>Download</div>
YARA rules	<u>2</u>	4	<div>Download</div>

Threat intelligence reports




LockBit 3.0 Malware Using Weaponized Word Doc To Drop Ransomware Via Amadey Bot

 13 TTPs •


GBHackers – Latest Cyber Security News by Priya James / 25mo


The Amadey Bot has been found to be used by attackers to install LockBit 3.0 with the help of malicious MS Word document files, eventually dropping the ransomware strain. It is necessary to use the following command to execute the...

Also in [secrutiny.com](#), [ASEC](#), +24 feeds




LockBit 3.0 Being Distributed via Amadey Bot

 IoC > 9 hashes and 7 URLs • [ASEC BLOG](#) by [jcleebobgatenet](#) / 25mo •



 12 TTPs


1) – Ransomware/PowerShell.Lockbit.S1945 (2022.10.29.00) [AMSI Detection] – Ransomware/PowerShell.Lockbit.SA1945 (2022.10.29.00) [Behavior Detection] – Ransom/MDP.Decoy.M1171 – Ransom/MDP.Event.M1875 –...

Also in [Information Security...](#), [Security Risk Adviso...](#), +33 feeds




Lockbit ransomware case study



 IoC > 18 URLs and 1 IP • by [Criminal IP](#) / 26mo •  10 TTPs •

 LockBit Ransomware

submitted by [/u/cheeztoshobo](#) [link] [comments]

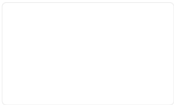


NSIS Type of LockBit 3.0 Ransomware Disguised as Job Application Emails Being Distributed


 IoC > 2 hashes • [ASEC BLOG](#) by [jcleebobgatenet](#) / 26mo •  9 TTPs

[File Detection] Ransomware/Win.LockBit.C5226681
Ransomware/Win.LockBit.R521104 [Behavior Detection]
Ransom/MDP.Event.M4353 [IOC Info] 2c0eeb266061631845a9e21156801afd...

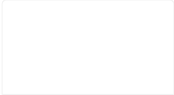
Also in [r/CyberCrime](#), [Vzrisksteam's Favorit...](#), +6 feeds





A technical analysis of the leaked LockBit 3.0 builder

 2 TTPs • by [CyberMasterV](#) / 26mo

submitted by [/u/CyberMasterV](#) [link] [comments]



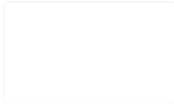
Back in Black: Unlocking a LockBit 3.0 Ransomware Attack

 IoC > 1 domain, 1 IP, and 1 hash • by [Published by](#) / 28mo •  44 TTPs

submitted by /u/digicat [link] [comments]

[See 4 more references](#)

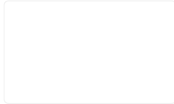
News



NY: Equinox notifies clients and employees of April data security incident

↗ [Equinox reports health data breach](#) • DataBreaches.Net by Dissent / 21d
With a little digging, DataBreaches realized that it was an attack by LockBit3.0.

Also in The Register, Cybersecurity Inside..., +41 feeds



Still in the dark: A “500 marker” is updated, but too many still aren’t. Is HHS doing anything about this??

DataBreaches.Net by Dissent / 31d
In March 2024, LockBit3.0 added Redwood Coast Regional Center (RCRC) to its leak site.



JPCERT Explains How to Identify Ransomware Attacks from Windows Event Logs

CySecurity News - Latest Information Sec... by Ridhika Singh / 32d
The variants such as Akira, Lockbit3.0, HelloKitty, and Bablock all generate almost identical logs because they share code from Lockbit and Conti.

Also in CySecurity News, IT Security News



Artifact Tracking: Workstation Names

🔗 [3 TTPs](#) • Windows Incident Response by Unknown / 44d
For example, Huntress analysts saw logins via legacy TeamViewer installations ahead of attempts to deploy LockBit3.0 ransomware, and in multiple observed incidents, logins originated from a workstation named WIN-8GPEJ3VGB8U.

Also in Windows Incident Res..., IT Security News