Hive Pro

THREAT ADVISORY

LockBit 2.0 Ransomware affiliates targeting Renowned Organizations	TA2022057
Threat Level RED	**Publish Date –** Mar 15, 2022

Since September 2021, LockBit 2.0 has targeted 500+ organizations in vital areas globally. The most recent attack targeted well-known tire producer Bridgestone, software behemoth Accenture, and the French Ministry of Justice. LockBit 2.0 ransomware compromises victim networks through a variety of techniques, including, but not limited to, purchased access, unpatched vulnerabilities, insider access, and zero-day exploit. Some of the know vulnerabilities exploited are CVE-2021-22986 affecting BIG-IP products and CVE-2018-13379 impacting FortiOS.

The ransomware first assesses the system and user language settings and only targets those that do not match a predefined list of Eastern European languages. It then erases system logs and shadow copies on disk as soon as the infection begins. In addition to this, it also collects system data such as hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices. Furthermore, it tries to encrypt all data stored to any local or remote device, but it ignores files linked with critical system operations. After the encryption, the ransomware deletes itself from the disk and creates persistence upon startup.

Lockbit 2.0 affiliates typically employ the Stealbit program received straight from the Lockbit panel to exfiltrate certain file types prior to encryption. The affiliate can adjust the desired file types to adapt the attack to the target. Additionally, they frequently employ publicly accessible file-sharing platforms such as privatlab.net, anonfiles.com, sendspace.com, fex.net, transfer.sh, and send.exploit.in. While some of these programs and services may serve legitimate reasons, others may be exploited by threat actors.

The Organizations can mitigate the risk by following the recommendations:

- Use multi-factor authentication.
- Keep all operating systems and software up to date.
- Remove unnecessary access to administrative shares.
- Maintain offline backups of data and Ensure all backup data is encrypted and immutable.
- Enable protected files in the Windows Operating System for critical files.

The Mitre TTPs commonly used by LockBit 2.0 are:

TA0040 - Impact
TA0042 - Resource Development
TA0001 - Initial Access
TA0002 - Execution
TA0003 - Persistence
TA0005 - Defense Evasion
TA0006 - Credential Access
TA0007 - Discovery
TA0008 - Lateral Movement
TA0009 - Collection
TA0011 - Command and Control
TA0010 - Exfiltration
T1190: Exploit Public-Facing Application

T1047: Windows Management Instrumentation
T1059: Command and Scripting Interpreter
T1059.003: Windows Command Shell
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1055: Process Injection
T1070.004: Indicator Removal on Host: File Deletion
T1112: Modify Registry
T1497: Virtualization/Sandbox Evasion
T1110: Brute Force
T1056.004: Credential API Hooking
T1012: Query Registry
T1018: Remote System Discovery
T1057: Process Discovery
T1021: Remote Services
T1021.001: Remote Services: Remote Desktop Protocol
T1021.002: Remote Services: SMB/Windows Admin Shares
T1056.004: Credential API Hooking
T1090.003: Proxy: Multi-hop Proxy
T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage
T1486: Data Encrypted for Impact
T1490: Inhibit System Recovery

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-22986	On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.5.3 amd BIG-IQ 7.1.0.x before 7.1.0.3 and 7.0.0.x before 7.0.0.2.	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:ssl_orchestrator:*:*:*:*:*:*:*:*	Remote code execution in iControl REST API in multiple F5 BIG-IP products	CWE-78
CVE-2018-13379	FortiOS 6.0 - 6.0.0 to 6.0.4 FortiOS 5.6 - 5.6.3 to 5.6.7 FortiOS 5.4 - 5.4.6 to 5.4.12	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	A path traversal vulnerability in the FortiOS SSL VPN web portal	CWE-22

Hive Pro

THREAT ADVISORY

Indicators of Compromise (IoCs)

Type	Value
MD5	af9ff037caca1f316e7d05db86dbd882, b7f1120bcff47ab77e74e387805feabe, 4d25a9242eac26b2240336fb94d62b1e, 84866fca8a5ceb187bca8e257e4f875a, f91095ae0e0632b0f630e0c4eb12ba10, b0916724ff4118bf213e31cd198c0afd, 6fc418ce9b5306b4fd97f815cc9830e5, 66b9ccb41b135f302b3143a5d53f4842
SHA-1	844e9b219aaecb26de4994a259f822500fb75ae1, a185904a46b0cb87d38057fc591a31e6063cdd95, c7b2d4a22f788b1b942f993fff33f233dca960ce, 038bc02c0997770a1e764d0203303ef8fcad11fb, 6c4040f2a76e61c649e1ff4ac564a5951c15d1fa, 12ac32d012e818c78d6db790f6e11838ca75db88, 95838a8beb04cfe6f1ded5ecbd00bf6cf97cd564, 3d532697163e7c33c7c906e8efbb08282d3efd75
SHA-256	f3e891a2a39dd948cd85e1c8335a83e640d0987dbd48c16001a02f6b7c1733ae, 4de287e0b05e138ab942d71d1d4d2ad5fb7d46a336a446f619091bdace4f2d0a, f32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202, acad2d9b291b5a9662aa1469f96995dc547a45e391af9c7fa24f5921b0128b2c, 717585e9605ac2a971b7c7537e6e311bab9db02ecc6451e0efada9b2ff38b474, 4bb152c96ba9e25f293bbc03c607918a4452231087053a8cb1a8accb1acc92fd, 0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049, d089d57b8b2b32ee9816338e96680127babc5d08a03150740a8459c29ab3ba78
IPs	139.60.160.200, 93.190.139.223, 45.227.255.190, 193.162.143.218, 168.100.11.72, 93.190.143.101, 88.80.147.102, 193.38.235.234, 174.138.62.35, 185.215.113.39, 185.182.193.120

Recent Breaches

bridgestoneamericas.com
accenture.com
justice.fr

Patch Link

https://www.fortiguard.com/psirt/FG-IR-18-384
https://support.f5.com/csp/article/K03009991

References

https://www.ic3.gov/Media/News/2022/220204.pdf
https://threatpost.com/accenture-lockbit-ransomware-attack/168594/