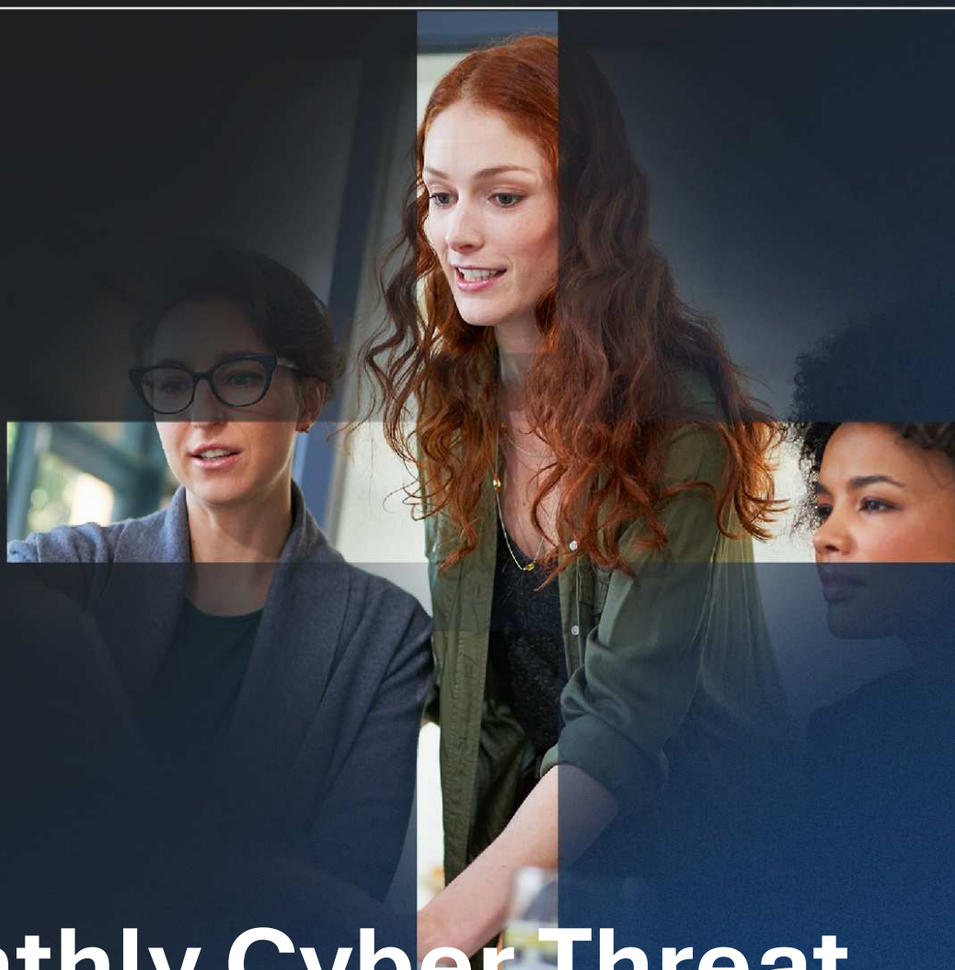
aDvens

For cyber, people & planet



Monthly Cyber Threat Intelligence report

June 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, the aDvens CERT presents an overview of recent vulnerabilities and cyber threats:

- Three vulnerabilities affecting widely deployed technologies are highlighted. Two of them are being actively exploited, while a third has a publicly available proof of concept (PoC), emphasizing the importance of promptly applying the available security updates.

- An in-depth study of the evolution of the LockBit ransomware, covering the origins of version 4.0, its partial disruption during Operation Cronos, its subsequent reconstruction, and the emergence of LockBit 5.0. The study is complemented by several matrices (MITRE ATT&CK, ransom psychology, recommendations, and IoCs) to support detection and incident response activities.

  These topics aim to help you anticipate cyber risks and strengthen your organization's security posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights **three** vulnerabilities affecting technologies widely used across enterprise environments. They are presented in order of priority, taking into account factors such as active exploitation and the availability of proof-of-concept exploits. Applying the available security updates or mitigations is strongly recommended.

2.1. CVE-2026-42271

A command injection vulnerability in the MCP server preview endpoints of BerriAI LiteLLM allows an authenticated attacker to execute arbitrary commands by submitting a specially crafted stdio configuration.

This vulnerability is being actively exploited.

2.1.1. Risk

- Arbitrary code execution

2.1.2. Type of vulnerability

- **CWE-77**: Improper Neutralization of Special Elements used in a Command ('Command Injection')

2.1.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	Low	Impact on integrity	Low
User Interaction	None	Impact on availability	Low

2.1.4. Affected products

- BerriAI LiteLLM versions prior to 1.83.7

2.1.5. Recommendation

- Upgrade BerriAI LiteLLM to version 1.83.7 or later.
- Additional information is available in the BerriAI security advisory.

2.1.6. Proof of concept

No proof-of-concept is currently available in public sources.

2.2. CVE-2026-47928

An improper input validation vulnerability in Adobe ColdFusion allows an unauthenticated attacker to execute arbitrary code by sending specially crafted data to an exposed endpoint.

2.2.1. Risk

- Arbitrary code execution

2.2.2. Type of vulnerability

- **CWE-20**: Improper Input Validation

2.2.3. Severity

Attack vector	Adjacent	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Affected products

- Adobe ColdFusion 2023 versions prior to 2023.19
- Adobe ColdFusion 2025 versions prior to 2025.8

2.2.5. Recommendation

- Upgrade Adobe ColdFusion 2023 to version 2023.19 or later.
- Upgrade Adobe ColdFusion 2025 to version 2025.8 or later.
- Additional information is available in the Adobe security advisory.

2.2.6. Proof of concept

A proof-of-concept is currently available in public sources.

2.3. CVE-2025-48595

An integer overflow vulnerability in the Android *Framework* component allows a local attacker, without requiring user interaction or prior privileges, to achieve privilege escalation by exploiting memory corruption.

This vulnerability is being actively exploited.

2.3.1. Risk

- Privilege escalation

2.3.2. Type of vulnerability

- **CWE-190**: Integer Overflow or Wraparound

2.3.3. Severity

Attack vector	Local	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Affected products

- Android 14
- Android 15
- Android 16
- Android 16 QPR2

2.3.5. Recommendation

- Update Android 14, 15, 16, and 16 QPR2 devices to the 2026-06-01 Android Security Patch Level or later.
- Additional information is available in the Android Security Bulletin.

2.3.6. Proof of concept

No proof-of-concept is currently available in public sources.

3. LOCKBIT 4.0 VS. 5.0, RESILIENCE AND INNOVATION

3.1. Origins of LockBit 4.0

3.1.1. The Emergence of the RaaS Model

Within the cybercriminal ecosystem, few organisations have achieved the level of industrialisation and resilience of the LockBit syndicate. First appearing on underground forums in September 2019 under the name "ABCD," this ransomware operation quickly established itself as the dominant force in the Ransomware-as-a-Service (RaaS) market.

Figure 1. LockBit 5.0's logo

LockBit's rise was largely driven by the disciplined execution of its business model. This model is based on a clear division of responsibilities: the operators provide the ransomware suite, payment portals, and negotiation infrastructure, while affiliates handle the intrusion phase, from initial access to ransomware deployment. By recruiting highly skilled affiliates and standardising the double extortion model (encrypting the victim's information system while exfiltrating sensitive data to increase leverage) the group transformed targeted extortion into a large-scale criminal franchise.

The group's criminal toolkit evolved through successive iterations, each introducing new capabilities:

- LockBit 1.0 (2019-2020), known as ".abcd", laid the foundation for fast, automated encryption across local networks.
- LockBit 2.0 "**Red**" (2021), introduced the dedicated data exfiltration tool *StealBit* and leveraged Group Policy Objects (GPOs) to rapidly deploy the ransomware across compromised environments.
- LockBit 3.0 "**Black**" (2022), integrated advanced anti-analysis techniques, including debugger detection and code obfuscation derived from the **BlackMatter** source code, while also launching the first public cybercriminal Bug Bounty program.
- LockBit 4.0 "**Green**" (2024-2025), was rewritten in .NET (previously developed in C/C++) and introduced several enhancements, including a date-based execution validation mechanism and an optimised encryption engine.

Historically known for its adaptability, LockBit has distinguished itself through its resilience in the face of disruption campaigns conducted by law enforcement agencies and cybersecurity researchers. The group has consistently demonstrated a high level of responsiveness by regularly updating its code, improving the efficiency of its encryption engine and refining its negotiation strategies.

Like a real business, these cybercriminals use genuine marketing techniques to attract new collaborators:

- job posts on Dark Web forums,

Figure 2. LockBit post aimed at recruiting support staff for the LockBit Red project - Source - analyst1

- bug bounty reward programs to fix vulnerabilities in its own malware,

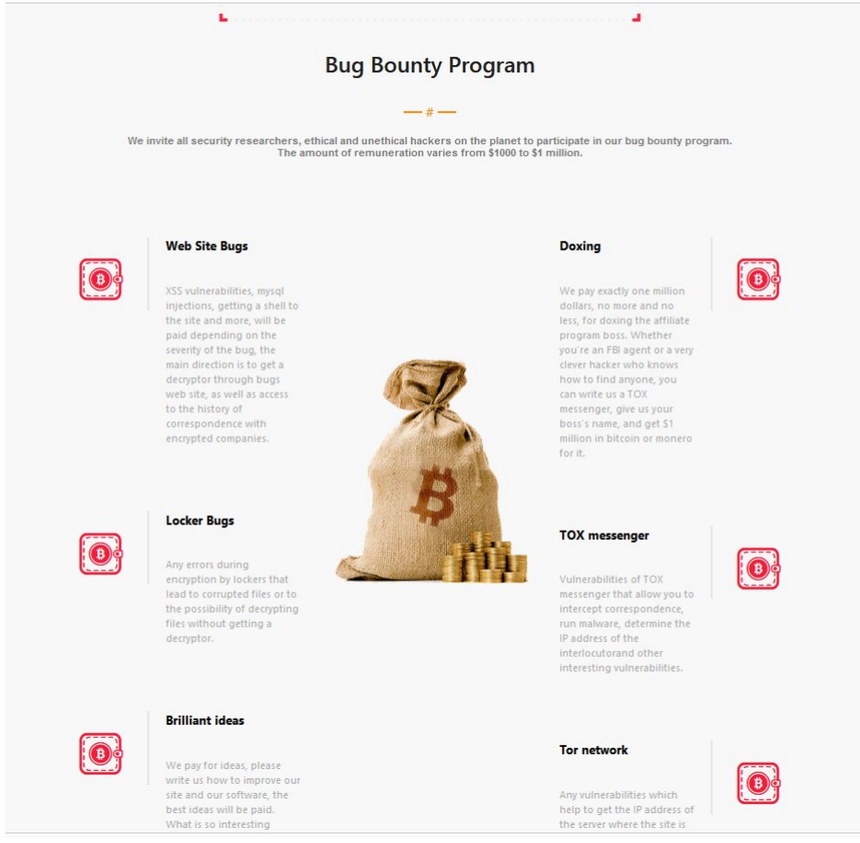


Figure 3. LockBit Bug Bounty Program - Source - analyst1

- advertisements and partnership announcements

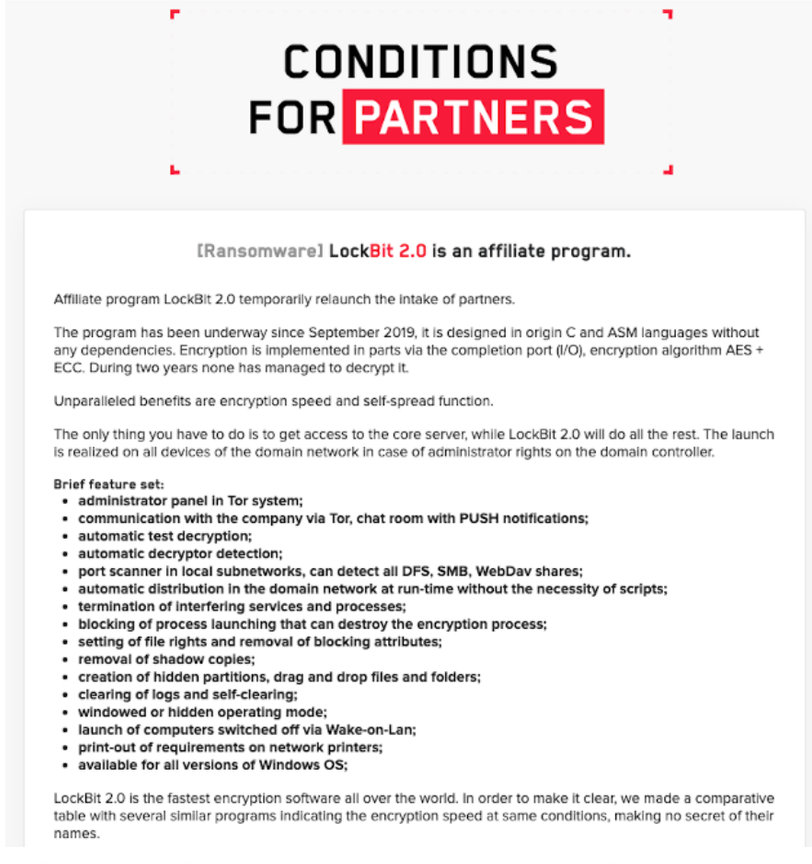
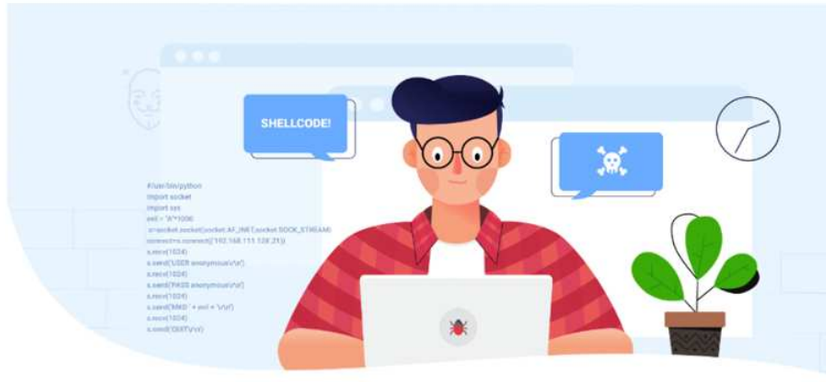


Figure 4. LockBit affiliate recruitment announcement - Source - analyst1

We're kicking off the ?summer PAPER CONTEST #4! With a prize fund - 15.000$



LOCKBIT

Летний конкурс статей

$15000 призовой фонд

Напиши статью - заработай на отдых

The winner of the competition (1st place) receives a prize -$5,000

2nd place - $4,000

3rd place - $3,000

4th place - $2,000

5th place - $1,000

Total prize pool **$15,000**

Ifa LockBItlikes your article, it will be rewarded additionally. Topics of interest to the sponsor: cryptolockers, networks.

Contest

Sponsor Sponsoredby LockBIt,locker team LockBit. Thanks for the financial sponsorship!

Accepted article topics:

- Hacks (web, *nix). Any. Methods for pouring shells, fixing, elevating rights. Your stories and tricks. Interesting hack stories.
- Malware and Malware coding. Bots-botnets, viruses, trojans. Bot development. Exploitation and monetization.
- Hacking programming: writing bruters, parsers, checkers, spammers, flooders, etc.
- SI and phishing in practice (phishing systems, point infections).
- "Wireless" hack. Hacking wi-fi, bluetooth, intercepting and sniffing traffic.
- Search for 0day and 1day vulnerabilities. Development of exploits for them.
- Spot infections and attacks.
- ART attack. LAN hacks, privilege escalation, domain controller capture, attack development
- Hidden internet. Alternative DNS. Cryptodomains. All about TOR. I2P.
- Traffic: mining methods, working with traffic.
- Non-standard methods of extracting material: admin, shells, roots, bases, socks, ssh, dedics, etc.
- Antidetects and Fingerprints. Work with antidetect systems. hiding methods. Working with collected fingerprints.
- Cryptography. Interesting combinations, algorithms. Writing your own cryptoalgorithm and hacking someone else's.
- Digital forensics. Up-to-date software, information collection, investigation methodology.

Figure 5. LockBit sponsors a hacking competition - Source - analyst1

3.1.2. International Takedown and Operation Cronos

On 19 February 2024, while LockBit was the most active ransomware group in the world, an international law enforcement colaboration known as **Operation Cronos** took full control of its infrastructure.

The operation carried out a genuine cyber counter-offensive. Rather than simply disconnecting the machines, authorities infiltrated the group's technical environment, which enabled them to:

- seize the Data Leak Site (DLS): the public portal used by LockBit to display its victims and publish stolen data was taken over,
- infiltrate the administration panel: authorities gained access to the central servers used by affiliates to manage their attacks on a daily basis,
- recover decryption keys: more than 1,000 decryption keys were seized, enabling the creation and distribution of a free tool to help victim organisations recover their files without paying the ransom.

The true strength of **Operation Cronos** lay in damaging LockBit's reputation using its own marketing tactics. Authorities transformed the group's leak site into a police information platform. Instead of the usual threats of data publication, they posted articles exposing LockBit's security flaws, evidence that the group retained stolen data even after payment, and clues about the true identity of the network leader: LockbitSupp.

Figure 6. Homepage of the LockBit website, now under the control of authorities

The operation significantly disrupted LockBit's operational infrastructure, as well as the confidence of its affiliates. In the weeks following the seizure, the volume of attacks declined, and several affiliates publicly defected to join competing ransomware programs, notably **ALPHV** and **RansomHub**.

However, within a few weeks, LockBit rebuilt itself. A new infrastructure was deployed, and the data leak site reappeared. LockBitSupp published a lengthy statement on cybercriminal forums, attributing the compromise to his own failure to patch a known PHP vulnerability (CVE-2023-3824), and announced a new ransomware version, codenamed "Green", intended to restart operations.

3.2. LockBit 4.0

The release of LockBit 4.0, dubbed "**LockBit-NG-Dev**" by researchers at *TrendAI* (previously *Trend Micro*), was likely accelerated by the aftermath of **Operation Cronos**. However, analysis shows that the malware had been under active development since at least January 2024, indicating that this version was not merely a reaction to the police raid.

The most significant evolution in LockBit 4.0 concerns its software architecture. Unlike previous versions, particularly LockBit 3.0 "Black", which relied on optimised C/C++ code, this new version fully adopts the **.NET** environment. In addition, the binary was compiled using CoreRT, a method that converts .NET code into a standalone native binary, improving its portability across different operating systems.

Analysis of the binary reveals a shift toward a more modular configuration model and a more efficient encryption workflow.

- Centralised JSON configuration: analysis by *TrendAI* shows that LockBit 4.0 stores its configuration in an encrypted JSON block embedded directly within the binary. This file contains all runtime parameters, including the attacker's RSA public key, the list of processes to terminate, directories to exclude and the ransom note template.

- Adaptive partial encryption: the ransomware implements a file size-based encryption strategy. Smaller files are encrypted in their entirety, whereas larger files are only partially encrypted. This approach serves a dual purpose: accelerating the encryption of large volumes of data while evading heuristic detection mechanisms that are triggered by the full encryption of a file.

Version 4.0 also strengthens its self-protection and anti-analysis capabilities to hinder security and forensic investigations:

- LockBit 4.0 implements an advanced API hashing mechanism that dynamically resolves the required Windows APIs without relying on explicit imports. This technique increases code obfuscation and makes static analysis significantly more difficult.

- The ransomware variant employs a detection evasion technique based on the unhooking of loaded modules. After comparing in-memory modules with their reference DLLs stored in the *KnownDlls* directory, the Windows APIs *NtOpenSection* and *NtMapViewOfSection* are used to map a clean copy of the targeted DLL into memory. The *WriteProcessMemory* function is then used to overwrite the already loaded DLL, effectively removing hooks that may have been inserted by security or monitoring tools.

- The ransomware introduces an innovative stealth technique by manipulating the *LdrRegisterDllNotification* and *LdrUnRegisterDllNotification* functions. By disabling DLL load notifications, it prevents the operating system from reporting the loading of new modules, depriving security solutions of valuable telemetry.

- The ransomware neutralises Vectored Exception Handlers (**VEH**) by registering a dummy handler and removing existing handlers from the VEH chain. This technique interferes with security solutions that use VEHs for monitoring, behavioral analysis or debugging.

Although this initial release exhibits some regressions, most notably the absence of a self-propagation capability, it nevertheless introduces significant improvements in anti-analysis and EDR evasion. These missing capabilities are expected to be reintroduced in subsequent releases. However, the lack of autonomous network propagation would ultimately prompt the group to further evolve its operational strategy.

3.3. Reconstruction and alliance

Despite the significant impact of **Operation Cronos**, the group successfully rebuilt its operational capabilities and maintained a high level of activity throughout 2024 and 2025. Its primary targets remained the healthcare, manufacturing, legal services and financial sectors. One of the defining events of 2025 was the announcement, on 8 October of an operational alliance between LockBit, Qilin and DragonForce. This formal partnership represented a significant shift in the ransomware ecosystem, which was traditionally characterised by competition among criminal groups. The agreement includes infrastructure sharing, affiliate cross-referrals and enhanced coordination of operational security measures.

Figure 7. Alliance between LockBit, Qilin and DragonForce - Source - dexpose.io

Each group brings complementary strengths:

- LockBit maintains the most developed affiliate ecosystem and strong brand recognition,
- Qilin contributes technical expertise and strong cross-platform capabilities, particularly on Linux and ESXi environments,
- DragonForce stands out for its aggressive extortion methods and its role as a provider of criminal tooling.

Together, these actors pool their technical resources, affiliates and infrastructure to increase their resilience against law enforcement actions. It is within this context of shared capabilities, infrastructure and reputation that the new version of LockBit emerges: LockBit 5.0.

3.4. LockBit 5.0

While competing groups such as **RansomHub**, **Akira** and **BlackSuit** are increasingly gaining ground in the cybercriminal landscape, LockBit released its version 5.0 (also known as "**ChuongDong**") in September 2025. This version marks a significant evolution in its capabilities, substantially expanding its attack surface and its ability to target an organisation's entire IT environment, while retaining its advanced detection evasion features.

3.4.1. The Evolution of LockBit 5.0

Analysis of this new strain highlights several new capabilities and technical developments:

- Research by *TrendAI* indicates that version 5.0 represents a major shift with the introduction of natively compiled binaries designed to target Windows, Linux and VMware ESXi hypervisors. The ransomware no longer focuses solely on Microsoft workstations and servers but aims to compromise the entirety of a victim's data and infrastructure.

- To maximise damage in ESXi environments, this variant incorporates destructive pre-encryption routines. The malware leverages native hypervisor tools by executing command-line utilities such as *esxcli* or *vim-cmd* to enumerate and forcibly shut down running virtual machines. This step releases virtual disks (.vmdk or .vswp files) from system locks, ensuring complete encryption without access conflicts.

The malware also introduces new anti-investigation techniques:

- It neutralises the *EtwEventWrite* function by overwriting it with a *0xC3* (return) instruction, effectively disabling Windows Event Tracing capabilities.

- It disrupts security-related services by comparing hashed service names against a hardcoded list of 63 values. Once encryption is complete, it clears Windows event logs using the *EvtClearLog* API.

The use of obfuscation techniques in this new variant significantly complicates the development of detection signatures. Finally, additional improvements, including the removal of infection markers, faster encryption routines and enhanced stealth mechanisms, make LockBit 5.0 considerably more dangerous than its predecessors.

Figure 8. LockBit 5.0 adds a uniquely generated, pseudo-random extension to encrypted files. This feature complicates file decryption. - Source - TrendAI

In addition, to counter law enforcement interventions such as **Cronos**, the architecture of Data Leak Sites has been redesigned. In line with a new doctrine of "maximum decentralization" announced by LockBitSupp in February 2024, LockBit has moved away from a single centralised administration panel. Stolen data is now distributed across multiple mirror sites.

Figure 9. LockBit data leak mirror sites - Source - Acronis

3.4.2. The LockBit 5.0 Attack Chain

Initial access

The Techniques, Tactics and Procedures used in attacks attributed to the LockBit group vary from one affiliate to another. However, according to the *Unit 42 incident response report (2026)*, **phishing** and **vulnerability exploitation** are the two dominant initial access vectors in extortion cases, each accounting for approximately 22% of observed incidents.

LockBit 5.0 affiliates align with these trends by exploiting three primary routes to breach target environments:

- AI-enhanced phishing campaigns: the use of AI-assisted tools now enables the creation of highly contextual and convincing lures, significantly improving the success rate of social engineering attacks.
- Vulnerability exploitation: attackers focus on widely deployed, internet-facing systems where exploiting a vulnerability can provide high-value access at relatively low technical cost.
- Use of previously compromised credentials: obtained from data breaches or purchased on underground markets, these credentials allow direct access to VPNs, remote access gateways and cloud portals, while reducing the risk of detection during the early stages of intrusion.

Execution and persistence

Once a system is compromised, attackers establish persistence using PowerShell scripts, scheduled tasks, registry modifications, and legitimate administrative tools (LOLBins, RMM) to conceal their activity.

Lateral movement and privilege escalation

Affiliates spread across the network via SMB or RDP, harvest credentials and escalate privileges to gain control over as many systems as possible.

Data exfiltration

Before being encrypted, files are first staged and then transferred to cloud storage services, FTP/SFTP servers or dedicated exfiltration channels. Exfiltration via web services is the most commonly observed method. This phase is accelerating significantly. In 2025, the fastest 25% of intrusions reached the exfiltration stage in just 72 minutes, compared to around 285 minutes the previous year. It is therefore no longer possible to rely on a multi-hour window to detect and interrupt such attacks.

Encryption and extortion

Finally, the ransomware encrypts accessible systems and threatens to publish the stolen data (double extortion). In some cases, attackers even forgo encryption entirely, relying solely on the threat of the data leak to put pressure on victims. They may also directly contact employees or customers to intensify this pressure.

4. CONCLUSION

The evolution of LockBit from versions 4.0 to 5.0 highlights the remarkable adaptability of ransomware groups in the face of sustained pressure from law enforcement agencies and the cybersecurity industry. Rather than leading to its disappearance, **Operation Cronos** forced the organisation to rethink both its technical and operational models, accelerating its transition toward a more modular, resilient and distributed architecture.

With LockBit 4.0, the group demonstrated its commitment to modernising its arsenal through the adoption of a new .NET-based codebase and significantly enhanced anti-analysis and evasion capabilities. LockBit 5.0 represents a further step forward, expanding its operational scope to encompass entire enterprise environments, including Linux systems and VMware ESXi hypervisors, while refining its destructive capabilities, obfuscation techniques and security monitoring bypass mechanisms.

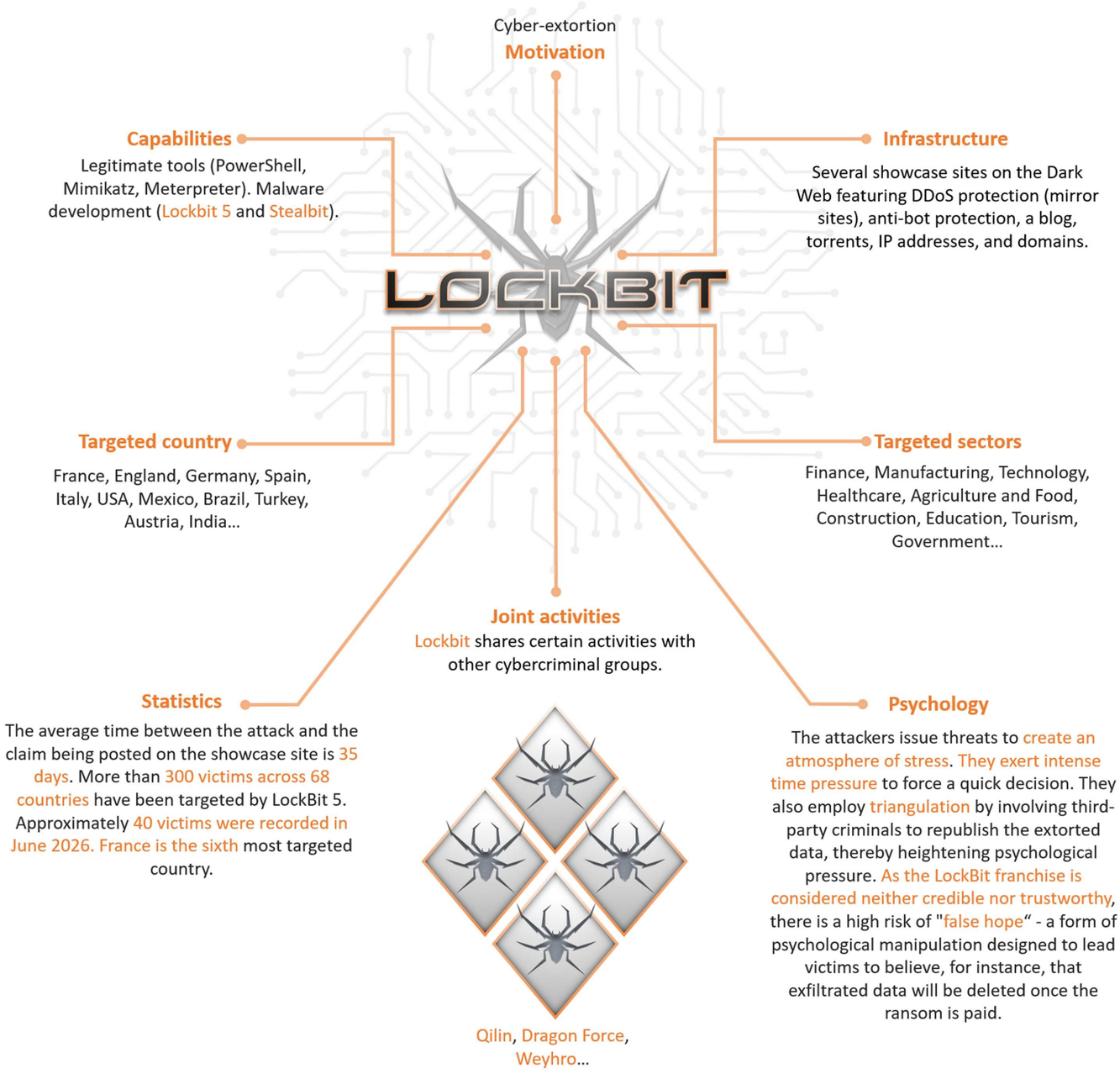
Alongside these technical developments, LockBit's organisational strategy has also undergone significant transformation. The decentralisation of its infrastructure, the proliferation of mirror leak sites and the operational alliance established with Qilin and DragonForce reflect a deliberate effort to pool resources, increase resilience against disruption and ensure the continuity of criminal operations. This collaborative approach represents a notable shift within the ransomware ecosystem, where collective resilience is increasingly becoming as important as technical sophistication.

The analysis of LockBit 4.0 and 5.0 illustrates a broader trend across the ransomware landscape: threat actors are no longer focused solely on improving encryption capabilities but are building mature criminal ecosystems capable of absorbing disruption, sharing resources and rapidly innovating. In this context, combating ransomware cannot rely exclusively on infrastructure takedowns or the arrest of individual operators. Effective defense requires a comprehensive approach combining attack surface reduction, timely vulnerability remediation, enhanced detection capabilities, user awareness and sustained international cooperation.

Ultimately, the recent history of LockBit demonstrates that within the modern ransomware ecosystem, resilience has become just as critical as technical innovation. The group’s ability to recover, adapt and evolve, following one of the most significant law enforcement operations ever conducted against a ransomware organisation, underscores the challenges that defenders will continue to face in the years ahead.

4.1. Diamond model

Below is the LockBit 5.0 diamond model.



4.2. Matrices

4.2.1. Technology - Mitre ATT&CK matrix

REFERENCES	TACTICS	TECHNIQUES
T1059	Execution	Command and Scripting Interpreter
T1129	Execution	Shared Modules
T1112	Persistence	Modify registry
T1547	Persistence	Boot or Logon Autostart Execution
T1543	Persistence	Create or Modify System Process
T1055	Privilege Escalation	Process Injection
T1134	Privilege Escalation	Access Token Manipulation
T1543	Privilege Escalation	Create or Modify System Process
T1547	Privilege Escalation	Boot or Logon Autostart Execution
T1027	Defense Evasion	Obfuscated File or Information
T1045	Defense Evasion	Software Packing
T1055	Defense Evasion	Process Injection
T1112	Defense Evasion	Modify Registry
T1134	Defense Evasion	Access Token Manipulation
T1497	Defense Evasion	Virtualization Sandbox Evasion
T1497	Defense Evasion	Virtualization Sandbox Evasion
T1562	Defense Evasion	Impair Defenses
T1003	Credential Access	OS Credential Dumping
T1552	Credential Access	Unsecured Credentials
T1010	Discovery	Application Windows Discovery
T1012	Discovery	Querry Registry
T1057	Discovery	Process Discovery
T1082	Discovery	System Information Discovery
T1083	Discovery	File and Directory Discovery
T1497	Discovery	Virtualization Sandbox Evasion
T1518	Discovery	Software Discovery
T1005	Collection	Data From Local System
T1074	Collection	Data Staged
T1114	Collection	Email Collection
T1115	Collection	Clipboard Data
T1125	Collection	Video Capture
T1125	Command and Control	Application Layer protocol
T1486	Impact	Data Encrypted for Impact
T1489	Impact	Service Stop
T1529	Impact	System Shutdown / Reboot

4.2.2. Psychology / Cyberpsychology - DECEPTION and RESISTANCE Matrices

Two concepts are used; they are essential for fully understanding the psychological dimension.

- **PCM: Psychological Countermeasure**, this refers to the set of manipulation tactics and techniques employed **offensively** to assert mental superiority over a target.

- **PCCM: Psychological counter-countermeasure**, a set of cognitive resistance mechanisms mobilised **within a defensive framework** to limit the impact of an adversary's psychological countermeasures and preserve one's capacity for reasoning, judgment, and decision-making in the face of an attempt at psychological destabilisation or domination.

DECEPTION Matrix

The table below lists the **psychological countermeasure (PCM)** tactics and techniques used by attackers for manipulation. These PCMs are derived from the DECEPTION model 5.0.

REFERENCES	TACTICS	TECHNIQUES
T3.36	Initialisation	Dissimulation
T4.36	Intrusion	Dissimulation
T6.09	Impact	Restriction of choice
T6.10	Impact	Disclosure of a secret
T6.08	Impact	Intimidation and Threats
T6.14	Impact	Urgency effect
T6.18	Impact	Attractive offer
T6.46	Impact	Internal Corruption
T6.27	Impact	Triangulation
T6.01	Impact	False hope

RESISTANCE Matrix

The table below lists the cognitive resistance efforts of attackers. These are the **psychological counter-countermeasures (CCMPs)** used by attackers to maintain effectiveness, resilience, and psychological defense in the face of adversity. These CCMPs are derived from the RESISTANCE model 1.0. This model is currently under development.

REFERENCE	TACTIQUE	TECHNIQUE	DESCRIPTION
T1-1-A	Reduction of emotional impact	Multi-emotional competition	An effort at multi-emotional recontextualisation is applied to counter an attempt at emotional manipulation. The goal is to prevent attentional monopolization by a single affective charge.
T3-3-B	Restoration of autonomous judgment	Cognitive asymmetry reversal	Create protocols that force the opponent to improvise. The goal is to counter the opponent's preparation (automation, scripts, arsenal preparation, etc.).
T6-6-A	Behavioral immunization	Controlled cognitive pre-fatigue	Identify one's own states of cognitive vulnerability (fatigue, multitasking, information overload, etc.).
T7-7-A	Reduction of inhibitions	Dilution of identity	Identity dissociation allows for a reduction in the sense of individual responsibility.
T7-7-B	Reduction of inhibitions	Normalization of behavior	The activities are part of a collective dynamic perceived as ordinary, which helps to legitimize the actions performed and provide reassurance regarding them.
T7-7-C	Reduced inhibitions	Cognitive offloading	The efforts being undertaken build upon a set of actions already completed, thereby reducing mental load and freeing up attention for other tasks.
T7-7-E	Reduced inhibitions	Heightened sense of impunity	Certain configurations (geographical distance, state protection, technological advantage, etc.) reinforce the sense of impunity by limiting perceived risks, thereby notably reducing the fear of consequences.
T7-7-F	Reduced inhibitions	Shared motivation	In addition to contributing collectively to the entity's operations, a portion of the profits is allocated on an individual basis, thereby reinforcing the motivation to act through a mechanism of operant conditioning (Skinner: reinforcement via positive reward).

4.2.3. Ransom note

Below is an example of a ransom note deployed by LockBit 5:

```
RANSOM NOTE LOCKBIT 5
>>>>> You must pay us.
Tor Browser link where the stolen infortmation will be published:
http://lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad[.]onion
>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are
not a politically motivated group and want nothing but financial rewards for our work. If we defraud even one
client, other clients will not pay us. In 5 years, not a single client has been left dissatisfied after making
a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation
process. Treat this situation simply as a paid training session for your system administrators, because it was
the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be
paid for the same way you pay your system administrators' salaries. You can get more information about us on
wikipedia https://en.wikipedia.org/wiki/LockBit
>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption
of files!
>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They will forbid
you from paying the ransom and will not help you in any way, you will be left with encrypted files and your
business will die.
>>>>> When buying bitcoin, do not tell anyone the true purpose of the purchase. Some brokers, especially in the
US, do not allow you to buy bitcoin to pay ransom. Communicate any other reason for the purchase, such as:
personal investment in cryptocurrency, bitcoin as a gift, paying to buy assets for your business using bitcoin,
cryptocurrency payment for consulting services, cryptocurrency payment for any other services, cryptocurrency
donations, cryptocurrency donations for Donald Trump to win the election, buying bitcoin to participate in ICO
and buy other cryptocurrencies, buying cryptocurrencies to leave an inheritance for your children, or any other
purpose for buying cryptocurrency. Also you can use adequate cryptocurrency brokers who do not ask questions
for what you buy cryptocurrency.
>>>>> After buying cryptocurrency from a broker, store the cryptocurrency on a cold wallet, such as
https://electrum[.]org/ or any other cold cryptocurrency wallet, more details on https://bitcoin[.]org By
paying the ransom from your personal cold cryptocurrency wallet, you will avoid any problems from regulators,
police and brokers.
>>>>> Don't be afraid of any legal consequences, you were very scared, that's why you followed all our
instructions, it's not your fault if you are very scared. Not a single company that paid us has had issues. Any
excuses are just for insurance company to not pay on their obligation.
>>>>> You need to contact us via TOR sites with your personal ID
Download and install Tor Browser hxxp(:)/www.torproject[.]org/
Write to the chat room and wait for an answer, we'll guarantee a response from us. If you need a unique ID for
correspondence with us that no one will know about, ask it in the chat, we will generate a secret chat for you
and give you ID via private one-time memos service, no one can find out this ID but you. Sometimes you will
have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies
around the world.
Tor Browser link for chat with us:
http://lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd[.]onion
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Your personal identifier to communicate with us ID: REDACTED <<<<<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Advertising:
Want a lamborghini, a ferrari and lots of titty girls? Sign up and start your pentester billionaire journey in
5 minutes with us.
hxxp(:)//lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad[.]onion
After registration, you will receive the most flawless and reliable tools for encrypting almost all operating
systems on the planet and a platform for negotiating with attacked companies.
Version: LINUX v1.01 | Linux amd64
URLs
hxxp(:)//lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad[.]onion
hxxp(:)//lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd[.]onion
hxxp(:)//lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad[.]onion
```

4.2.4. Indicators of Compromise

Here is a list of hashes corresponding to LockBit ransomware artifacts.

TLP	TYPE	VALUE
TLP:CLEAR	MD5	5e1f61b9c1c27cad3b7a81c804ac7b86
TLP:CLEAR	MD5	ca93d47bcc55e2e1bd4a679afc8e2e25
TLP:CLEAR	MD5	a1539b21e5d6849a3e0cf87a4dc70335
TLP:CLEAR	MD5	9bcff8da7165977f973ace12dd4c0ce0
TLP:CLEAR	MD5	8f718979876dd1050ce4f729d69e0072
TLP:CLEAR	MD5	2513d6678b476a432af2e84fff485b44
TLP:CLEAR	MD5	c462c6b02b35df2910689947c5090fae
TLP:CLEAR	MD5	e47032b3d1b9cbbcf77741d5d260004d
TLP:CLEAR	MD5	95daa771a28eaed76eb01e1e8f403f7c
TLP:CLEAR	MD5	ca93d47bcc55e2e1bd4a679afc8e2e25
TLP:CLEAR	MD5	a1539b21e5d6849a3e0cf87a4dc70335
TLP:CLEAR	MD5	5e1f61b9c1c27cad3b7a81c804ac7b86
TLP:CLEAR	MD5	274e5ff2aa33e7ec980700e617eb2214
TLP:CLEAR	MD5	eb0c1d82187ec3fe980eed2419875e4b
TLP:CLEAR	MD5	2908589ca1a1f5d98c7f71563a3abac6
TLP:CLEAR	MD5	bf4443f6dbbdee8816aa9a1098374326

5. SOURCES

Vulnerabilities

- https://www.cve.org/CVERecord?id=CVE-2026-42271
- https://nvd.nist.gov/vuln/detail/CVE-2026-42271
- https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g

- https://www.cve.org/CVERecord?id=CVE-2026-47928
- https://nvd.nist.gov/vuln/detail/CVE-2026-47928
- https://helpx.adobe.com/security/products/coldfusion/apsb26-64.html

- https://www.cve.org/CVERecord?id=CVE-2025-48595
- https://nvd.nist.gov/vuln/detail/CVE-2025-48595
- https://source.android.com/docs/security/bulletin/2026/2026-06-01

Article - LockBit 4.0 vs. 5.0, resilience and innovation

- https://analyst1.com/ransomware-diaries-volume-1/
- https://www.dexpose.io/lockbit-ransomware/
- https://www.trendmicro.com/en_us/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html
- https://www.trendmicro.com/fr_fr/research/25/i/lockbit-5-targets-windows-linux-esxi.html
- https://www.lemagit.fr/actualites/366637075/Ransomware-comment-LockBit-met-en-scene-son-retour
- https://www.acronis.com/en/tru/posts/lockbit-strikes-with-new-50-version-targeting-windows-linux-and-esxi-systems/
- https://www.provendata.com/blog/lockbit-5
- https://www.ransomware.live/group/lockbit3
- https://www.ransomware.live/group/lockbit5
- https://www.lemondeinformatique.fr/actualites/lire-windows-linux-et-esxi-sous-la-menace-de-lockbit-50-97989.html
- https://fr.vectra.ai/blog/lockbit-is-back-whats-new-in-version-5-0
- https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
- https://www.trendmicro.com/fr_fr/research/25/i/lockbit-5-targets-windows-linux-esxi.html
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version/technical-appendix-lockbit-ng-dev-analysis.pdf

Psychology / Cyberpsychology

- DECEPTION model. Psychological countermeasures (PCM).
  https://deceptionmodel.sitew.fr/

- RESISTANCE model. Psychological counter-countermeasures (PCCM).
  https://cyber-virologie.my.canva.site/sigma-cyberpsychologie/modle-resistance