1989 Virus Response: Then and Now

A source-checked cybersecurity case study and MacBook file-integrity lab | 26 September 2026

Research question

How much of today's incident response was recognizable in a Soviet KGB directive issued on 28 July 1989?

Finding

The directive and its attached advisory describe stopping work to limit spread, examining suspected programs against trusted reference copies, and restoring affected programs from those references. These are recognizable response concerns today. The document does not demonstrate how consistently or effectively the guidance was carried out.

What the primary source establishes

Evidence	Location	Assessment
A dated directive addresses acquisition, use, and copying of foreign software.	Scan pp. 1-2	The date and title are visible.
The attached advisory reports virus incidents in Soviet organizations and KGB departments during 1987-1989.	Scan pp. 3-4	This is the KGB's report; individual incidents still need corroboration.
It prescribes suspension of affected work, testing, comparison with references, and restoration.	Scan p. 9	Directly visible in the response passage; English here is a careful paraphrase.

Source rule: a statement in a 1989 memo proves what the memo said. It does not independently prove every incident the memo reports. The 2026 article supplies context and selected translation, and is labeled separately.

Historical timeline

Dates from the scan are separated from later analysis and modern comparison.

Date	Event or claim	Evidence status
1982	The advisory recalls a factory program sabotage incident.	Retrospective background in scan p. 3; not established as a self-replicating virus.
From 1985	It says foreign reporting on computer viruses grew.	Retrospective claim in scan p. 4.
1987-1989	It reports more virus incidents at Soviet computing centers and within the KGB.	Contemporaneous institutional claim in scan p. 4.
1988	Vienna was detected in Soviet institutions; an early antivirus was developed.	Specific month and release dates come from Shakirov's later account; further verification needed.
29 Jun 1989	The advisory refers to an earlier technical circular about detecting known viruses.	Reference in scan p. 9; the circular itself was not obtained.
28 Jul 1989	Directive and attached computer-virus advisory.	Date visible in primary-source scan p. 1.
2025 / 2026	NIST revision 3; Shakirov historical analysis.	Modern comparison and secondary interpretation, respectively.

Virus descriptions: one unresolved identity

1989 description	Later match	Assessment
648-byte .COM virus, DOS-62/TIMEBOMB/VHS-648 (p. 6)	Vienna	Strong match to later virus references.
1,701-byte virus; falling screen characters (p. 7)	Cascade	Strong match to F-Secure description.
710-byte virus; damages programs run on Friday the 13th (p. 7)	Possibly Jerusalem	Behavior fits, but size conflicts with documented variants. Keep open.

MacBook lab and modern comparison

Hands-on demonstration using harmless text files on a 2019 Intel MacBook Pro

The user made an approved test file, recorded its SHA-256 digest, copied it as a reference, and changed only the working file. The digests differed. A unified diff showed one line replaced: “Approved version” became “Changed version.” This illustrates file integrity checking. SHA-256 is a modern demonstration, not a method prescribed by the 1989 directive. A mismatch shows change, not malicious intent.

Response comparison

Concern	1989 advisory	NIST SP 800-61r3 (2025)
Contain	Suspend work on suspected and connected PCs (scan p. 9).	Contain incidents to prevent expansion; isolation may be used (PDF pp. 39-40).
Investigate	Test programs and compare with clean references (scan p. 9).	Validate and prioritize incidents; establish events, affected assets, and root cause (PDF pp. 34-36).
Recover	Restore programs from trusted references (scan p. 9).	Verify restoration assets and recovered systems before use (PDF p. 41).

Limits and next questions

The scan is a faint Russian image. These English summaries are paraphrases, not a certified full translation. The 710-byte virus identity remains unresolved. The reported incident counts and the 1988 antivirus chronology need independent contemporary corroboration. Modern NIST guidance addresses organizations and many technologies, so similarity of goals does not imply identical capability.

References

1. 1989 directive, ten-page scan supplied by the user as KGB RESEARCH.pdf; Lithuanian archive F. K-51, ap. 3, b. 58, l. 70-74.
2. Oleg Shakirov, How the KGB Discovered Computer Viruses (2026): https://fromcyberia.substack.com/p/how-the-kgb-discovered-computer-viruses
3. NIST, SP 800-61 Revision 3 (2025): https://csrc.nist.gov/pubs/sp/800/61/r3/final
4. F-Secure threat descriptions, Vienna, Cascade, Jerusalem; Virus Bulletin, January 1991, Vienna entry.