

Threat Bulletin: Critical eScan Supply Chain Compromise

 morphisec.com/blog/critical-escan-threat-bulletin

January 29, 2026



On January 20, 2026, Morphisec identified an active supply chain compromise affecting MicroWorld Technologies' eScan antivirus product.

Malicious updates were distributed through eScan's legitimate update infrastructure, resulting in the deployment of multi-stage malware to enterprise and consumer endpoints globally.

This document provides indicators of compromise (IOCs) to assist organizations in identifying affected systems.

CRITICAL: The malicious payload tampers with eScan registry, files and update configuration to prevent updates and proper function of the AV. Automatic remediation is therefore not possible for compromised systems. ***Impacted organizations and individuals must proactively contact eScan to obtain the manual update/patch.***

Incident Timeline

Date	Event
January 20, 2026	Malicious update package distributed via eScan update infrastructure
January 20, 2026	Morphisec detects and blocks malicious activity on customer endpoints
January 21, 2026	Morphisec initiates contact with MicroWorld Technologies (eScan)
January 21, 2026	eScan states they detected the incident via internal monitoring, isolated affected infrastructure within 1 hour, and took global update system offline for 8+ hours
Post-incident	Most Morphisec customers had to proactively contact eScan to receive remediation

Attack Chain Overview

Stage 1: Trojanized eScan Update

- ↓ Reload.exe (32-bit) replacement
- ↓ Drops Stage 3 downloader (CONSCTLX.exe)

Stage 2: Downloader

- ↓ Scheduled Task persistence, PowerShell execution, Defense evasion
- ↓ Tamper with hosts file and eScan registry to block remote updates
- ↓ Connects to C2 infrastructure for additional payloads

Stage 3: Persistent downloader

- ↓ CONSCTLX.exe (64-bit), dropped by Stage 1

Indicators of Compromise

Stage 1 – Trojanized eScan Component

Affected Component: Reload.exe (32-bit)

File Hashes (SHA-256):

36ef2ec9ada035c56644f677dab65946798575e1d8b14f1365f22d7c68269860 – The observed delivered payload

Additional related samples observed on VirusTotal:

- 674943387cc7e0fd18d0d6278e6e4f7a0f3059ee6ef94e0976fae6954ffd40dd
- 386a16926aff225abc31f73e8e040ac0c53fb093e7daf3fbd6903c157d88958c

Code Signing Certificate:

- **Issuer:** eScan (Microworld Technologies Inc.)
- **Thumbprint:** 76B0D9D51537DA06707AFA97B4AE981ED6D03483

Stage 2 – Command & Control Domains

C2 Infrastructure (Defanged):

- hxxps[://]vhs[.]delrosal[.]net/i
- hxxps[://]tumama[.]hns[.]to
- hxxps[://]blackice[.]sol-domain[.]org
- hxxps[://]codegiant[.]io/dd/dd/dd[.]git/download/main/middleware[.]ts
- 504e1a42.host.njalla.net
- 185.241.208.115

STATUS: C2 infrastructure status currently unconfirmed. Organizations should block these domains as a precaution.

Stage 3 – Persistent Downloader

Dropped by: Stage 1 (Reload.exe)

File Hashes (SHA-256):

Filename	SHA-256 Hash
CONSCTLX.exe	bec369597633eac7cc27a698288e4ae8d12bdd9b01946e73a28e1423b17252b1

Persistence Mechanisms

Scheduled Tasks:

Location: C:\Windows\Defrag\

Task naming pattern: Windows\Defrag\<Application>Defrag

Examples observed:

- Windows\Defrag\CorelDefrag
- Additional variants expected

Registry Persistence:

- **Key:** HKLM\Software\<randomly generated GUID>
- **Value:** Contains encoded PowerShell payload (byte array)

Update Blocking (Anti-Remediation):

- **Hosts File:** Modified to block eScan update servers
- **eScan Registry:** Modified to tamper eScan product

Program Data:

efirst directory: Sometimes generated under programdata as a marking indicator

Detection Guidance

Immediate Actions

1. **Search for malicious hashes** listed above across all endpoints
2. **Review scheduled tasks** under Windows\Defrag\ for unexpected entries
3. **Inspect registry** for suspicious GUID-named keys under HKLM\Software\ containing byte array data
4. **Check hosts file** for entries blocking eScan domains
5. **Block C2 domains** at network perimeter
6. **Review eScan update logs** for activity on January 20, 2026
7. Download eScan update to patch and fix your eScan installation.

Affected Products

- eScan Antivirus (Enterprise and Consumer editions)
- Specific affected versions: Pending vendor confirmation
- **All Morphisec customers running eScan were targeted by this attack**

Remediation

CRITICAL: Automatic updates will not work on compromised systems. The malicious payload tampers with eScan registry, files, and update configuration to prevent updates and proper function of the AV. Manual intervention is required.

EScan provides a patch that should fix the updater and revert eScan configurations and host file.

For Systems Protected by Morphisec

Morphisec prevented the malicious payload execution. These systems are safe but should still apply the eScan patch to restore normal eScan functionality.

For Systems Without Morphisec Protection

1. **Assume compromise** and conduct full forensic investigation
2. **Isolate** affected systems immediately
3. **Contact eScan directly** to obtain the manual update/patch
4. **Verify hosts file** – remove any entries blocking eScan update servers
5. **Check eScan registry settings** – restore proper update configuration
6. **Conduct forensic analysis** to determine if Stage 3 downloader was deployed
7. **Reset credentials** for any accounts accessed from affected systems
8. **Do not rely solely** on vendor-provided patches without forensic verification

IMPORTANT: Affected organizations may need to proactively contact eScan to receive remediation assistance.

We strongly encourage eScan customers to reach out directly rather than waiting to be contacted.

References

VirusTotal: Multiple samples uploaded from various countries

Contact

Morphisec Threat Labs

For questions or additional IOCs, [please contact Morphisec directly](#).

EScan Contact Information (Based on their advisory)

For Technical Support:

Email: support@escanav.com

Online Support: <https://escanav.com/livechat>

Phone: 18002672900/0091-22-67722911

For Security Inquiries:

Email: security@escanav.com

For Enterprise Customers:

Dedicated Support: 0091-99209 07188/0091-98692 58689/0091-95940 02570

Email: corpsupport@escanav.com

This document will be updated as the investigation progresses.

Authors note: 'backdoor' updated to 'downloader' at eScan's request.

About the author



Michael Gorelik

Chief Technology Officer

Morphisec CTO Michael Gorelik leads the malware research operation and sets technology strategy. He has extensive experience in the software industry and leading diverse cybersecurity software development projects. Prior to Morphisec, Michael was VP of R&D at MotionLogic GmbH, and previously served in senior leadership positions at Deutsche Telekom Labs. Michael has extensive experience as a red teamer, reverse engineer, and contributor to the MITRE CVE database. He has worked extensively with the FBI and US Department of Homeland Security on countering global cybercrime. Michael is a noted speaker, having presented at multiple industry conferences, such as SANS, BSides, and RSA. Michael holds Bsc and Msc degrees from the Computer Science department at Ben-Gurion University, focusing on synchronization in different OS architectures. He also jointly holds seven patents in the IT space.

Stop ransomware. Guaranteed, or your money back.



[Learn more](#)