CIRT.GY Guyana National Computer Incident Response Team

AL2026_08 Glassworm Malware Hits 400+ Code Repositories on GitHub, npm, VSCode, and OpenVSX (March 20th, 2026)

Description

Security researchers have identified a large-scale software supply-chain attack involving the **Glassworm** malware campaign, which has compromised more than 400 code repositories and packages across development platforms such as GitHub, npm, Visual Studio Code Marketplace, and OpenVSX.

The campaign targets developers by injecting malicious code into open-source repositories and packages that appear legitimate. Once installed or incorporated into development environments, the malware can steal sensitive information such as credentials, authentication tokens, and development secrets.

Because developers frequently rely on third-party packages and extensions, the attack poses a significant risk to software supply chains and organizations that depend on open-source development ecosystems.

Attack Details

The Glassworm campaign represents a sophisticated supply-chain attack designed to spread through widely used development tools and repositories.

Key characteristics include:

- **Large-scale compromise:** Researchers discovered malicious code injected into hundreds of repositories and packages hosted on GitHub, npm, and developer extension marketplaces.
- **Hidden malicious code:** Attackers use invisible Unicode characters to hide malicious payloads within source code. These characters appear as blank spaces in many editors, making them extremely difficult to detect during manual code reviews.
- **Payload execution:** The injected code includes obfuscated loaders that decode hidden instructions and execute them using functions such as eval(), enabling the malware to run additional malicious scripts.
- **Blockchain-based infrastructure:** The malware retrieves second-stage payloads from decentralized infrastructure such as the Solana blockchain, making takedown efforts more difficult.

- **Data exfiltration:** Once active, the malware can steal authentication tokens, developer credentials, and other sensitive information stored in development environments.
- **Propagation through dependencies:** Because the malicious code is embedded in open-source packages and extensions, developers may unknowingly introduce the malware into their projects when installing or updating dependencies.

Glassworm was previously identified as one of the first self-propagating malware campaigns targeting Visual Studio Code extensions and open-source development environments.

Remediation

Organizations and development teams should implement the following security measures to mitigate risks associated with software supply-chain attacks:

- **Audit dependencies:** Carefully review third-party packages, extensions, and repositories before installing them in development environments.
- **Monitor repositories:** Regularly audit code repositories for suspicious commits, hidden characters, or unauthorized modifications.
- **Use automated security scanning:** Deploy tools that detect hidden Unicode characters, obfuscated code, and malicious dependency behavior.
- **Limit extension installation:** Enforce policies that restrict the installation of unverified extensions in development environments.
- **Credential protection:** Store development credentials securely using vaults and avoid embedding secrets directly in source code.
- **Rotate exposed secrets:** If a compromised package or repository is detected, immediately rotate all potentially exposed API keys, authentication tokens, and credentials.
- **Enable multi-factor authentication:** Implement MFA for developer accounts on platforms such as GitHub, npm, and package registries to reduce the risk of account compromise.
- **Supply-chain monitoring:** Implement software composition analysis (SCA) tools to detect malicious or vulnerable dependencies within projects.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2026). *Glassworm malware hits 400+ code repos on GitHub, npm, VSCode, OpenVSX.* Retrieved from BleepingComputer:

https://www.bleepingcomputer.com/news/security/glassworm-malware-hits-400-plus-code-repos-on-github-npm-vscode-openvsx/