KPMG

KPMG Cyber Threat Intelligence Platform

GitHub Supply Chain Compromise

TLP : Clear

KPMG. Make the Difference.

On 20 May 2026, GitHub disclosed a large-scale supply chain compromise in which threat actors exfiltrated approximately 3,800 internal repositories via a malicious Visual Studio (VS) Code extension. The breach was confirmed to be carried out by TeamPCP, with LAPSUS$ collaborating on extortion and monetization. Stolen repositories included sensitive projects such as Copilot, CodeQL, Dependabot, and Codespaces, later listed on dark web forums for $50,000–$95,000.

The attack exploited the implicit trust placed in extension marketplaces. Microsoft's VS Code marketplace auto-updates extensions without manual review, allowing TeamPCP to publish a malicious version of Nx/NxConsole extension. Once installed, the extension fetched its payload not from attacker infrastructure but from an orphan commit embedded in the legitimate 'nrwl/nx' repository, meaning GitHub's own CDN delivered the malicious code. This tactic, weaponising trusted infrastructure against itself, mirrors TeamPCP's earlier compromises of Trivy and Checkmarx CI/CD pipelines. When executed, the payload harvested multiple credential classes including GitHub Personal Access Tokens, npm publishing tokens, AWS IAM keys, Kubernetes secrets, Vault tokens, and even unlocked password vaults. These credentials enabled bulk cloning of internal repositories, while automated malicious commits compromised an additional 5,561 public repositories, expanding the attack surface across enterprise and cloud environments.

On 20 May 2026, a compromised extension was briefly published to the marketplace and remained available for approximately eleven minutes before removal. Upon workspace initialization, the embedded payload executed on a GitHub employee device, activating a credential stealer. Threat actors then used stolen tokens throughout the day to clone thousands of internal repositories, including assets related to GitHub Actions, Copilot, CodeQL, Codespaces, Dependabot, infrastructure code, and other internal components.

Prior to public disclosure, TeamPCP listed the dataset for $50,000, followed by a joint "TeamPCPxLAPSUS" listing priced at $95,000. GitHub later confirmed the incident on X, stating that customer repositories were not impacted. Notably, on the same day as TeamPCP's operation, a Lazarus Telegram group claimed to have uploaded 158 million GitHub records, though this assertion remains unverified.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context.

The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

GitHub Supply Chain Compromise

TLP : Clear

KPMG. Make the Difference.

The GitHub breach has also been linked to a broader campaign observed between March and May 2026, where attackers leveraged related vectors such as the poisoning of the Nx Console extension, compromises in Trivy and Checkmarx CI/CD infrastructure, and the hijacking of Microsoft's DurableTask package on PyPI. Additionally, Shai-Hulud worm variants were deployed to enable self-propagation across developer supply chains, further amplifying the impact and reach of the GitHub compromise.

In addition, two other supply chain compromises were reported in May 2026 targeting Laravel-lang PHP packages and Packagist repositories. In the Laravel-lang case, attackers injected malicious code into language translation packages, enabling credential theft and remote code execution. In the Packagist attack, at least eight popular PHP libraries were infected with malware designed to steal secrets and propagate further compromise. While these incidents are part of the same broader supply chain exploitation wave, the direct involvement of TeamPCP, LAPSUS$, or Lazarus Group is not confirmed in the PHP ecosystem attacks, and attribution remains unclear.

What should you do?

- Rotate all GitHub tokens, AWS IAM keys, npm publishing tokens, and Vault secrets.
- Validate publisher integrity of installed VS Code extensions and remove suspicious plugins.
- Deploy endpoint firewalls and heuristic detection engines tuned for developer tooling ecosystems.
- Monitor for orphan commits or unauthorized publisher token use.

MITRE ATT&CK Mapping

Tactics	Techniques
TA0001 : Initial Access	T1195.001 : Supply Chain Compromise : Software Dependencies and Development Tools
	T1195.002 : Supply Chain Compromise : Compromise Software Supply Chain
	T1199 : Trusted Relationship
TA0002 : Execution	T1059.004 : Command and Scripting Interpreter : Unix Shell
	T1059.006 : Command and Scripting Interpreter : Python
TA0003 : Persistence	T1547.006 : Boot or Logon Autostart Execution : Kernel Modules and Extensions
	T1543.001 : Create or Modify System Process : Launch Agent
	T1546 : Event Triggered Execution
TA0004 : Privilege Escalation	T1548.003 : Abuse Elevation Control Mechanism : Sudo and Sudo Caching

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

GitHub Supply Chain Compromise

TLP : Clear

KPMG. Make the Difference.

Tactics	Techniques
TA0005 : Stealth	T1497.001 : Virtualization/Sandbox Evasion : System Checks
	T1036 : Masquerading
TA0006 : Credential Access	T1003 : OS Credential Dumping
	T1552.004 : Unsecured Credentials : Private Keys
	T1552.005 : Unsecured Credentials : Cloud Instance Metadata API
TA0007 : Discovery	T1082 : System Information Discovery
TA0011 : Command and Control	T1102.001 : Web Service : Dead Drop Resolver
	T1132 : Data Encoding
	T1572 : Protocol Tunneling
TA0010 : Exfiltration	T1041 : Exfiltration Over C2Channel

Below are the Indicators of Compromise (IOCs) associated with the Github Supply Chain Activity:

Indicators of Compromise
513c510e363ba99cd72da81210b5c80b
f3eb2508c26b36761c1045183541bb6e
1783b4126a3a66de875114c42853df7a
d7e56bd2ed9310748b22d0445af508483623ebbe
cd157dc43092882ccb7cd5b70d61802c9e593fff
0e502c0114fd95dd8e7cb508f88f9a0508e91864
1a4afce34918bdc74ae3f31edaffffaa0ee074d83618f53edfd88137927340b8
b0cefb66b953e5184b6adb3035e9e267335ac5eabfe1848e07834777b9397b74
43f2b001846c4966073ebffa5be8f15e491a1e7d32bbd805d57406ff540e0dd9

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

GitHub Supply Chain Compromise

TLP : Clear

KPMG. Make the Difference.

Below are the Indicators of Compromise (IOCs) associated with TeamPCP and LAPSUS$:

Indicators of Compromise: IP Addresses	
63.251.162[.]11	209.34.235[.]18
83.142.209[.]11	83.142.209[.]203
45.148.10[.]212	212.71.124[.]188
195.5.171[.]242	23.142.184[.]129

Indicators of Compromise: Domains	
checkmarx[.]zone	scan.aquasecurtiy[.]org
models.litellm[.]cloud	tdtqy-oyaaa-aaaae-af2dq-cai.raw.icp0[.]io

Indicators of Compromise: Hashes
07a8f7de8abd1e877ad96a72d385e019
8cf49650b7a000d09e8af77c314dfdad
20fb3b0944a88aa7f635cb2e7c491704
d761a6a7ae9f2254bd81ac234033a8b8
dbb50ce36bb5b87a381cce1dfb59084a
8bfefb76454efe404359831d4fe7137c
46e7a5c4cf645b77f24023eef873f56f
633b465ec04a3b7b5a908ad6ec5adc2e
188d8592f393ce45f7273102f02efee1
333a1ec6eb53400986529c86423c01a5
df43394b926e609e6ad020b157b151a1
805c08686e755c063a0bb460bdf9dcc4
55405de62427ac56106f0fdb1c33dedd

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

GitHub Supply Chain Compromise

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
284037d485efbf7c54efcc7a4ba1516b
43a466cf0d6af34e09acc03a058061ef
60180783702e13238a8311233fc23d3e170eb4b9
53495d74e72a0e74a2e1fdfe69f39fd538abd9e6
1bb57746c4ddf4c47df653ca327a642b3040a313
4fed54d88f919c675ee2f575f70698a8d3649287
1307f0b2ddec0aedca484d7c9f83024e5f558b62
3950fa21431ad211e1292119ff1c77e1797fa595
4e574710f80ada2abe7cf2ffd78f99592bb6c2c2
27bbebdd418835967fcf00d6ff3315109cf61750
61ff00a81b19624adaad425b9129ba2f312f4ab76fb5ddc2c628a5037d31a4ba
6328a34b26a63423b555a61f89a6a0525a534e9c88584c815d937910f1ddd538
7321caa303fe96ded0492c747d2f353c4f7d17185656fe292ab0a59e2bd0b8d9
7b5cc85e82249b0c452c66563edca498ce9d0c70badef04ab2c52acef4d629ca
7df6cef7ab9aae2ea08f2f872f6456b5d51d896ddda907a238cd6668ccdc4bb7
822dd269ec10459572dfaaefe163dae693c344249a0161953f0d5cdd110bd2a0
c37c0ae9641d2e5329fcdee847a756bf1140fdb7f0b7c78a40fdc39055e7d926
cd08115806662469bbedec4b03f8427b97c8a4b3bc1442dc18b72b4e19395fe3
e4edd126e139493d2721d50c3a8c49d3a23ad7766d0b90bc45979ba675f35fea
e6310d8a003d7ac101a6b1cd39ff6c6a88ee454b767c1bdce143e04bc1113243
e64e152afe2c722d750f10259626f357cdea40420c5eedae37969fbf13abbecf
e87a55d3ba1c47e84207678b88cacb631a32d0cb3798610e7ef2d15307303c49
e9b1e069efc778c1e77fb3f5fcc3bd3580bbc810604cbf4347897ddb4b8c163b
f398f06eefcd3558c38820a397e3193856e4e6e7c67f81ecc8e533275284b152
f7084b0229dce605ccc5506b14acd4d954a496da4b6134a294844ca8d601970d

Follow us on:
kpmg.com/in/socialmedia