

When AI Becomes the Lure: A Fake Gemini Installer Delivers Vidar

 darktrace.com/blog/when-ai-becomes-the-lure-a-fake-gemini-installer-delivers-vidar

Rushanth Ramanathan

August 19, 2026



With the growing prevalence of generative AI, attackers are increasingly exploiting interest in AI tools to distribute malware. Darktrace recently investigated an incident in which a malicious executable masquerading as a Google Gemini installer resulted in a Vidar information stealer infection.



Key takeaways

- *Darktrace observed a customer download a fake Google Gemini installer hosted on Google Colab, resulting in the execution of the Vidar information stealer.*
- *Darktrace identified the compromise through behavioral indicators, including suspicious process activity, anomalous network communications, and indicators of credential theft, before autonomously containing the threat.*
- *The incident highlights how threat actors are increasingly exploiting trusted platforms and a growing interest in AI tools to distribute malware through seemingly legitimate software acquisition workflows.*

The Growing Abuse of Generative AI

As organizations are increasingly adopting generative AI tools into their daily workflows, attackers are adapting their distribution methods accordingly too. As part of their day-to-day work, users are now searching for AI assistants, programming tools, browser extensions, desktop applications, and productivity integrations.

Recent reports have highlighted campaigns that use fake AI software and AI-related installers to distribute malware and steal credentials [1]. Researchers have documented campaigns that exploit

fake AI-themed websites and services to distribute information stealers and backdoors [2]. Security researchers have also observed attackers disguising malware as legitimate installers for AI software to increase the likelihood of victim interaction and execution [3].

In July 2026, Darktrace observed one such case within a customer environment in the Europe, Middle East and Africa (EMEA) region, where attackers used a fake generative AI installer to deliver [the prolific information stealer Vidar](#). This incident highlights how threat actors are exploiting interest in AI services to distribute established malware using increasingly convincing social engineering techniques.

How a Fake Gemini Installer Delivered Vidar

Initial Access: From Search Result to Malware Download

Unlike many malware campaigns that begin with a phishing email, this activity appears to have originated from a user searching for and downloading software.

Darktrace first observed unusual activity on the customer network after a suspicious executable file was launched from a user's Download folder. Further investigation revealed that the file purported to be a Google Gemini installer and was named "Download_Google_Gemini_For_Windows.exe".

During the initial analysis, it was noted that the top search result for the suspicious filename associated pointed to a file hosted on Google Colab, a cloud-based Jupyter notebook platform, commonly used by developers, researchers, and data scientists to run code and machine learning workloads through a web browser. By leveraging another trusted Google platform, the attacker increased the likelihood that users would perceive the download as legitimate, making the lure more convincing to those searching for Gemini-related software.

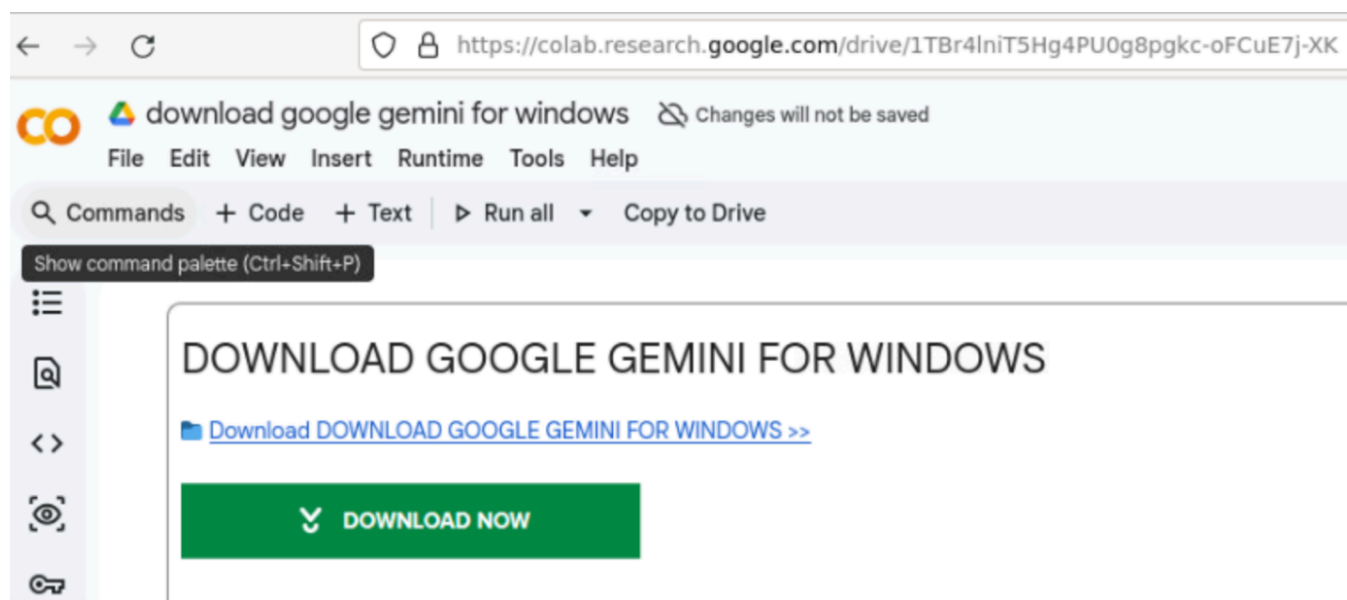


Figure 1: The Google Colab page containing a download prompt for the fake Google Gemini installer.

Further investigation of the Google Colab page revealed that the download prompt redirected users to a secondary site, `https://micronsoftwares.com`, which posed as a "Windows Software Hub" download page and offered the fake Gemini installer for download.

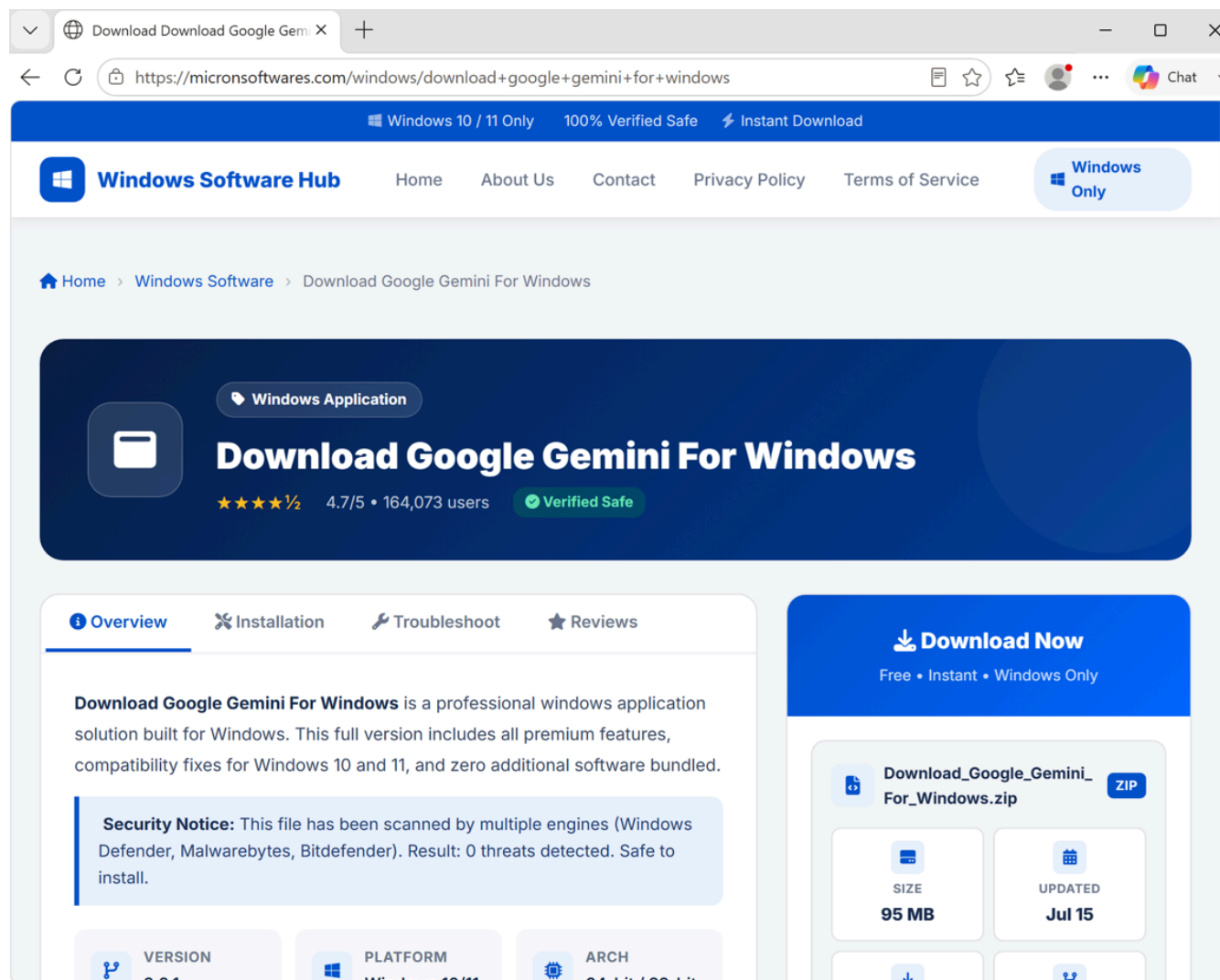


Figure 2: The secondary website posing as a "Windows Software Hub" download page, which likely hosted the fake Gemini installer.

While the investigation did not uncover any HTTP or file-download telemetry data that conclusively identified the download source, SSL communication sessions with Google Colab were detected immediately before the suspicious file was executed. The timing of these connections suggests that the user interacted with the Colab resource before being redirected to the secondary site from which the executable was downloaded.

The user was not simply tricked into opening an email attachment; instead, the attacker embedded malicious content into a process many users would consider entirely legitimate: searching for and downloading software associated with a trusted platform.

Weaponizing Trusted Platforms

At the time of review (July 15, 2026), Darktrace's Threat Research team confirmed that the Google Colab page was still active and prompting users to download a ZIP archive containing the binary file.

The archive also appeared to contain a README file instructing users to run the binary file with administrator privileges and add it to their antivirus software's exception lists. These instructions suggest that the campaign relied heavily on social engineering, convincing users to take actions that would facilitate malware execution and potentially bypass security checks.

The use of a legitimate platform also complicates the user's decision-making. Downloads associated with a trusted service are often perceived as less suspicious than those hosted on unfamiliar domains. When combined with the branding of a widely used AI tool, the lure becomes even more convincing.

Malware Analysis

Darktrace's Threat Research team identified the executable file as the information-stealing malware Vidar. Analysis revealed that the binary file was a newer Go-compiled variant that communicated with Telegram-based infrastructure. Darktrace's researchers also identified dtm[.]kijangturbo88[.]top as a command-and-control (C2) endpoint associated with the activity. While the malware itself was not novel, the lure and delivery mechanism was.

For a deeper look at the information stealer, see [Darktrace's 2023 analysis of Vidar](#).

Figure 3: Darktrace's detection of the unusual outbound connection associated with the fake Gemini installer.

Shortly after execution, the process established communications with the external IP address 91.98.98[.]86 via port 443, directly linking the executable to suspicious network activity observed on the device. Subsequent open-source intelligence (OSINT) analysis of the revealed multiple malicious associations [5].

Additional Darktrace detections included unusual SSL activity from the affected device. Analysis of related SSL telemetry identified 91.98.111[.]49 as additional infrastructure associated with the activity [6].

Subsequent alerts from the customer's [Microsoft Defender for Endpoint integration](#) later confirmed activity consistent with the theft of browser credentials and other sensitive data from the affected endpoint.

Taken together, these detections provided a clear picture of the attack, from the execution of a suspicious file and unusual network connections to indicators of C2 activity and credential theft.

Figure 4: Darktrace's detection of anomalous activity following the execution of the fake Gemini installer, seen in the Model Alert Event Log.

Darktrace's Autonomous Response

Following the detection, Darktrace's Autonomous Response took immediate containment action, including blocking communication with suspicious external infrastructure, including 91.98.98[.]86, and quarantining the compromised device.

Despite the apparent legitimacy of the activity, with the installer hosted on a trusted platform and resembling a routine software download, Darktrace was able to detect and contain the attack because the device's behavior deviated from its normal pattern.

Figure 5: Automated containment actions implemented by Darktrace's Autonomous Response following the detection of activity associated with the fake Gemini installer.

Conclusion

This investigation highlights how threat actors continue to adapt established malware delivery techniques to emerging technology trends. While the malware itself was not new, the distribution method was. By disguising Vidar as a Google Gemini installer and hosting the malicious content on a trusted platform, the attack aligned its lure with a growing behavioral trend: users actively searching for AI tools and services as part of their day-to-day work.

Although fake installers are not a new phenomenon, the rapid rise of generative AI has created new opportunities for threat actors. Rather than relying solely on traditional delivery methods, attackers can now target users who are actively searching for AI applications. As AI adoption continues to accelerate across enterprise environments, organizations should remain alert to campaigns that exploit this interest through fake applications, malicious websites, manipulated search results, the misuse of trusted platforms, and AI-themed social engineering.

Credit to Rushanth Ramanathan (Cyber Analyst) Joanna Ng (Detection Engineer)

Edited by Ryan Traill (Content Manager)

Appendices

Darktrace Model Detections

- Security Integration / C2 Activity and Integration Detection
- Endpoint / New Suspicious Executable Launched
- Endpoint / Process Connection / Unusual Connection from New Process

- Anomalous Connection / Rare External SSL Self-Signed
- Security Integration / High Severity Integration Detection
- Antigena / Network / Significant Anomaly / Antigena Significant Security Integration and Network Activity Block

•Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block

List of Indicators of Compromise (IoCs)

IoC	Type	Description
Download_Google_Gemini_For_Windows.exe	File	Fake Gemini-themed installer observed during the investigation.
GoogleAppInstaller.exe	File	Related executable identified through endpoint telemetry.
91.98.98[.]86	IP Address	External destination contacted by the malicious executable.
91.98.111[.]49	IP Address	Related infrastructure identified through SSL certificate pivoting.

IoC	Type	Description
dtm[.]kijangturbo88[.]top	Domain	Command-and-control endpoint identified during malware analysis.
1e13c2c9eac72daf63fd00a9946878949e159ae6ec51b54ec64f942d79d61913	SHA256	Malware sample associated with the fake Gemini installer.

MITRE ATT@CK Mapping

MITRE ATT&CK Mapping	Tactic	Technique
Initial Access	T1204	User Execution
Execution	T1204.002	User Execution: Malicious File
Defence Evasion	T1036	Masquerading
Credential Access	T1555	Credentials from Password Stores
Credential Access	T1555.003	Credentials from Web Browsers
Command and Control	T1071	Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

Newsletter

Enjoying the blog?

Sign up to receive the latest news and insights from the Darktrace newsletter – delivered directly to your inbox

Trending blogs

[Prompt Security in Enterprise AI: Strengths, Weaknesses, and Common Approaches](#)

[May 20, 2026](#)

[What the Darktrace Annual Threat Report 2026 Means for Security Leaders](#)

[Feb 26, 2026](#)

[Journey of a Threat: How Multi-Layered AI Works in Darktrace / EMAIL](#)

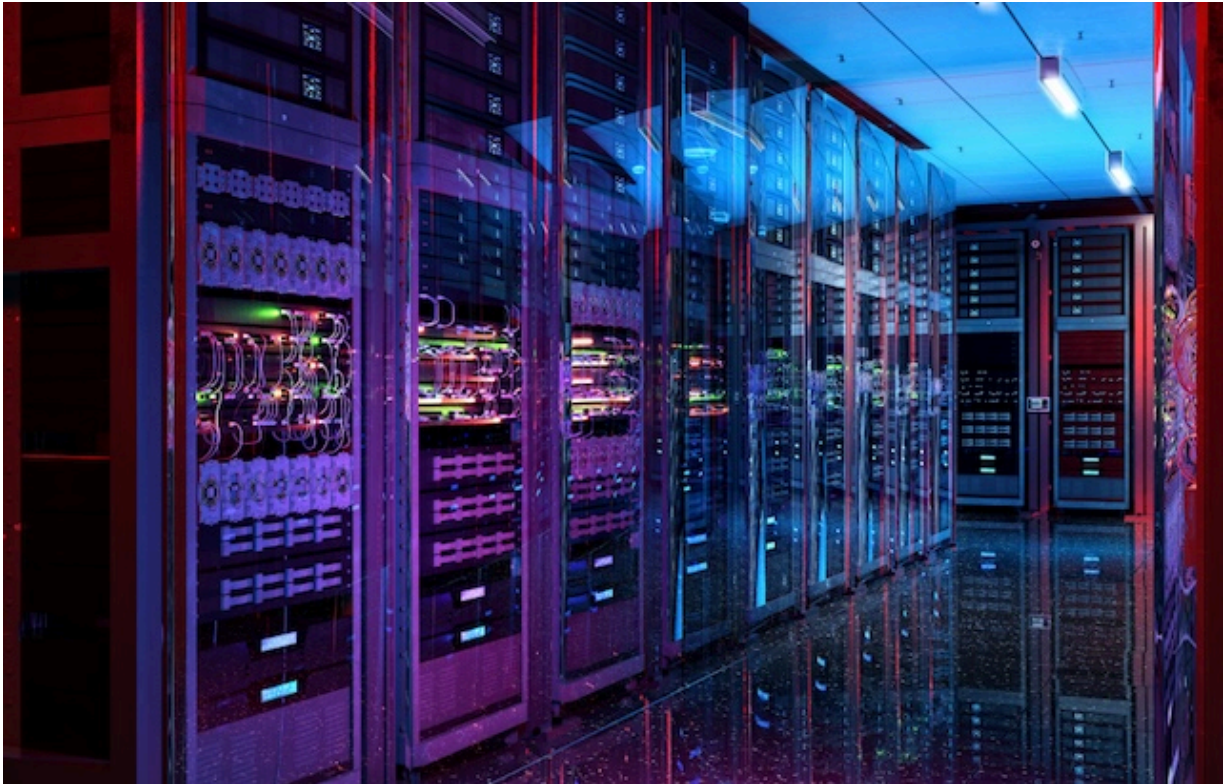
[May 26, 2026](#)

[How to Evaluate AI Vendors: 5 Key categories for AI Adoption](#)

[May 27, 2026](#)

[Darktrace Unites Human Behavior and Threat Detection Across Email, Slack, Teams, and Zoom](#)

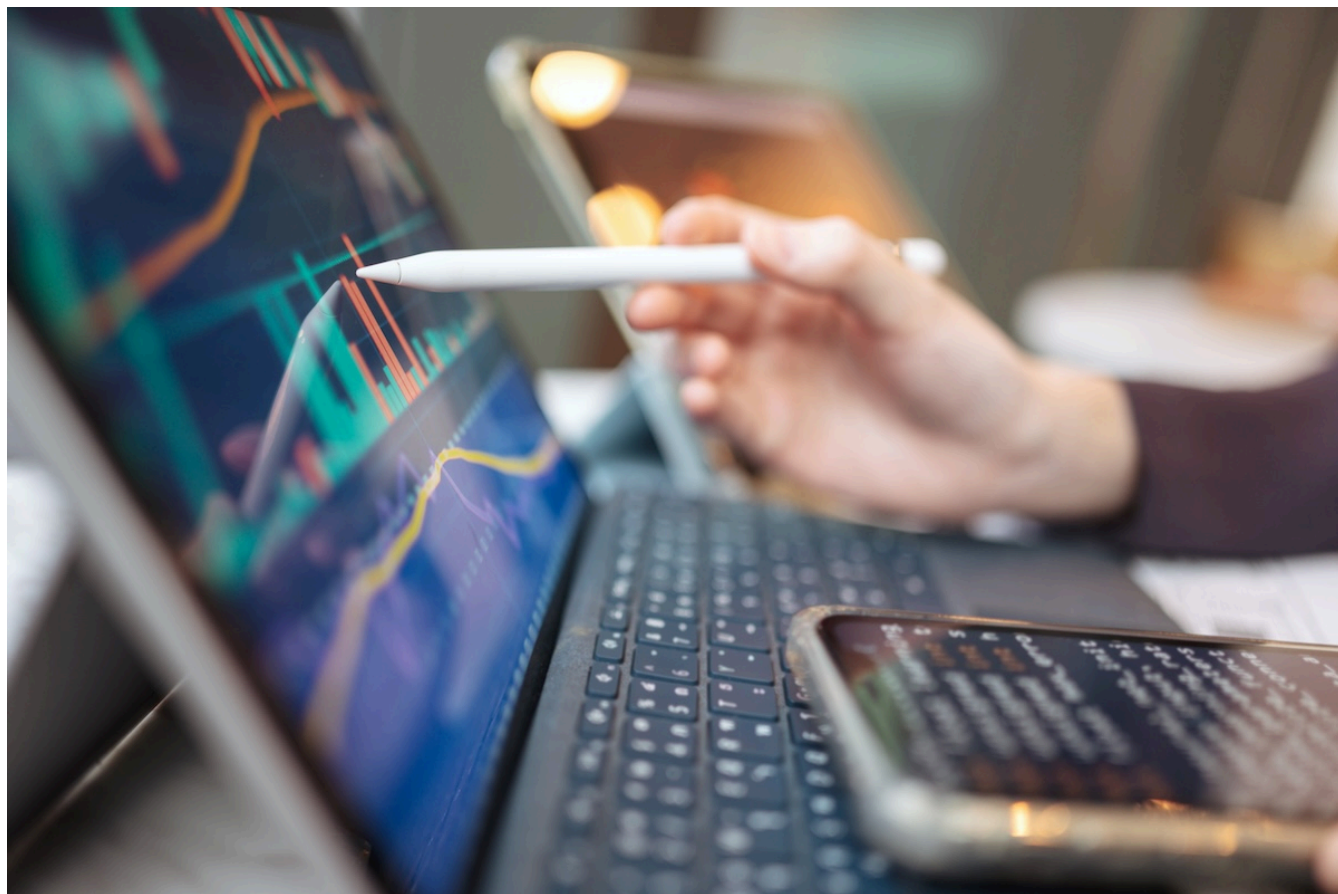
[Mar 24, 2026](#)



AI Agents: Securing the Path from Intent to Action

Margaret Cunningham, PhD

VP, Security & AI Strategy, Field CISO



Testing a Prompt injection Attack Against an Enterprise AI Agent

Carlo Loregian
Solutions Engineer



Extending AI Security Visibility with Darktrace and Microsoft Agent 365

Your data. Our AI.

Elevate your network security with Darktrace AI