When Trust Becomes a Weapon: Google Cloud Storage Phishing Deploying Remcos RAT

By ANY.RUN

Published: 2026-04-14 · Archived: 2026-04-23 02:44:49 UTC

Modern phishing campaigns increasingly abuse legitimate services. Cloud platforms, file-sharing tools, trusted domains, and widely used SaaS applications are now part of the attacker's toolkit. Instead of breaking trust, attackers borrow it.

This shift creates a dangerous asymmetry. Security controls often whitelist or inherently trust these services, while users are far less likely to question them. The result is a smoother path from inbox to infection.

Key Takeaways

- Attackers are shifting to trusted cloud infrastructure (Google Storage) to bypass email filters and reputation checks.
- The multi-stage chain uses obfuscated JS/VBS/PowerShell and legitimate RegSvcs.exe for process injection, making static detection ineffective.
- Remcos RAT provides full remote control, keylogging, and data exfiltration — turning one compromised endpoint into a persistent foothold.
- Credential harvesting combined with malware delivery creates dual risk: immediate data theft plus long-term network compromise.
- Traditional EDR relying on file reputation misses these attacks; behavioral sandboxing and real-time TI are required.
- ANY.RUN's Interactive Sandbox, TI Lookup, and TI Feeds enable proactive detection and rapid response, closing the gap before damage occurs.

The New Face of Phishing: When "Legitimate" Becomes Lethal

According to ANY.RUN's annual Malware Trends Report for 2025, phishing driven by multi-stage redirect chains and trusted-cloud hosting has become the dominant attack vector, with RATs and backdoors rising 28% and 68% respectively. The abuse of legitimate platforms has made traditional reputation-based filtering fundamentally unreliable.

Early detection is no longer simply a technical performance metric. It is a business continuity imperative. When threats hide inside trusted infrastructure, the window between initial infection and serious organizational impact

can be measured in hours, not days. Security teams that cannot identify and contain an attack in its earliest stages — before the payload executes, before the C2 channel is established, before the attacker pivots deeper into the network — face an exponentially harder response challenge.

Phishing Campaign Hiding Remcos RAT Inside Google Cloud Storage

In April 2026, ANY.RUN's threat research team identified a sophisticated multi-stage phishing campaign that perfectly exemplifies this new breed of attack. The campaign abuses Google Cloud Storage to host HTML phishing pages themed as Google Drive document viewers, ultimately delivering the Remcos Remote Access Trojan (RAT).

View the attack in real time in a live sandbox session

Sandbox analysis of a phishing attack

The attackers parked their phishing pages on a legitimate, widely-trusted Google domain. This single architectural choice allowed the campaign to bypass a wide range of conventional email security gateways and web filtering tools.

Convincing Google Drive-themed phishing pages are hosted on storage.googleapis.com subdomains such as pa-bids, com-bid, contract-bid-0, in-bids, and out-bid. Examples include URLs like hxxps://storage[.]googleapis[.]com/com-bid/GoogleDrive.html. These pages mimic legitimate Google Workspace sign-in flows, complete with branded logos, file-type icons (PDF, DOC, SHEET, SLIDE), and prompts to "*Sign in to view document in Google Drive*."

The pages are crafted to harvest full account credentials: email address, password, and one-time passcode. But the credential theft is just the opening act. After a "successful login," the page prompts the download of a file named Bid-Packet-INV-Document.js, which serves as the entry point for the malware delivery chain.

Attack Chain

The delivery chain is deliberately complex and layered to evade detection at every stage:

1. Phishing Email Delivery. Because the sending domain and the linked domain are both associated with legitimate Google infrastructure, the email passes standard DMARC, SPF, and DKIM authentication checks, and is not flagged by reputation-based email filters.

2. Fake Google Drive Login Page. The googleapis.com link opens a convincing replica of the Google Drive interface, prompting the victim to authenticate with their email address, password, and one-time passcode. Credentials entered here are captured and exfiltrated to the attacker's command-and-control infrastructure.

3. Malicious JavaScript Download. The victim is prompted to download Bid-Packet-INV-Document.js, presented as a business document. When executed under Windows Script Host, this JavaScript file contains time-based evasion logic — it can delay execution to avoid sandbox detection environments that analyze behavior within a fixed time window.

4. VBS Chain and Persistence. The JavaScript launches a first VBS stage, which downloads and silently executes a second VBS file. This second stage drops components into %APPDATA%\WindowsUpdate (folder name chosen to blend in with legitimate Windows processes) and configures Startup persistence, ensuring the malware survives system reboots.

Malicious script activity captured by the sandbox

5. PowerShell Orchestration. A PowerShell script (DYHVQ.ps1) then orchestrates the loading of an obfuscated portable executable stored as ZIFDG.tmp, which contains the Remcos RAT payload. To remain stealthy, the chain simultaneously fetches an additional obfuscated .NET loader from Textbin, a text-hosting service, loading it directly in memory via Assembly.Load, leaving no file on disk for traditional antivirus engines to scan.

6. Process Hollowing via RegSvcs.exe. The .NET loader abuses RegSvcs.exe for process hollowing. Because RegSvcs.exe is signed by Microsoft and carries a clean reputation on VirusTotal, its execution appears benign in endpoint logs. The loader creates or starts RegSvcs.exe from %TEMP%, hollowing the process and injecting the Remcos payload into its memory space. The result is a partially fileless Remcos instance: most of the malicious logic executes entirely in memory, never touching the disk in a form that a signature-based scanner would recognize.

Remcos RAT detected in the sandbox analysis

7. C2 Establishment. Remcos establishes an encrypted communication channel back to the attacker's command-and-control server and writes persistence entries into the Windows Registry under HKEY_CURRENT_USER\Software\Remcos-{ID}, ensuring continued access across reboots. From this point, the attacker has full, persistent, covert control over the compromised endpoint.

ANY.RUN's sandbox analysis clearly visualizes this chain: wscript.exe spawns multiple VBS and JS scripts, cmd.exe and powershell.exe handle staging, and RegSvcs.exe is flagged for Remcos behavior. The entire process tree demonstrates how attackers chain living-off-the-land binaries (LOLBins) with obfuscation and in-memory execution.

Why This Attack Works — and Why Remcos Makes It So Dangerous

The attack succeeds because it weaponizes trust at every layer. Google Storage provides reputation immunity. RegSvcs.exe is a signed Microsoft binary used for .NET service installation: its clean hash means endpoint protection rarely flags it. Combined with heavy obfuscation, time-based evasion, and fileless techniques, the campaign slips past static analysis and many EDR rules that rely on file reputation or known malicious domains.

At the heart of the final payload is Remcos RAT — a commercially available Remote Access Trojan that has become a favorite among cybercriminals due to its affordability, ease of use, and powerful feature set. It grants attackers full remote control over the compromised system. Capabilities include keylogging, credential harvesting from browsers and password managers, screenshot capture, file upload/download, remote command execution, microphone and webcam access, and clipboard monitoring. It supports persistence mechanisms, anti-analysis tricks, and encrypted C2 communication.

The dangers of Remcos extend far beyond initial access. It serves as a beachhead for further attacks: ransomware deployment, lateral movement across the corporate network, data exfiltration of intellectual property or customer records, and even supply-chain compromise if the infected machine belongs to a vendor. Because it runs in memory inside a trusted process, it can remain undetected for weeks or months, silently harvesting sensitive data.

Why This Matters for Businesses

Enterprises face amplified risk because these campaigns target high-value users (executives, finance teams, and procurement staff) who routinely handle sensitive documents and have elevated privileges. A single successful infection can lead to:

- **Data Breaches and Regulatory Fines**: Stolen credentials and exfiltrated files can trigger GDPR, CCPA, or industry-specific compliance violations costing millions.
- **Financial Losses**: Direct wire fraud from compromised email accounts or indirect losses from ransomware.
- **Operational Disruption**: Lateral movement can encrypt servers or exfiltrate intellectual property, halting production or R&D.
- **Reputation Damage**: Clients and partners lose trust when a breach is publicly disclosed.
- **Supply-Chain Ripple Effects**: If a vendor’s system is compromised via this vector, attackers can pivot into larger organizations.

In attacks that exploit legitimate services, the Mean Time to Detect (MTTD) for conventional security tools is dramatically extended. When the initial link is clean, the host domain is trusted, and the payload runs inside a legitimate Microsoft process, the alert chain that SOC teams depend on generates few or no signals. The attacker operates in silence while gathering intelligence, escalating privileges, and expanding their foothold.

Enabling Proactive Protection Against Trust-Abuse Phishing

Defending against phishing campaigns that abuse legitimate services requires a security capability that operates at the behavioral level — one that can observe what happens after a link is clicked or a file is opened, not just assess

whether a URL or hash matches a known-bad list. ANY.RUN's Enterprise Suite is built precisely for this purpose, and its three core modules address the threat at complementary stages of the detection and response lifecycle.

Triage & Response: See the Full Kill Chain Before It Reaches Production

The foundation of ANY.RUN's detection capability is its Interactive Sandbox: a cloud-based, fully interactive analysis environment that allows security analysts to safely detonate suspicious files and URLs in real time. Unlike automated sandboxes that analyze behavior passively within a fixed time window, ANY.RUN's sandbox supports genuine human interaction: analysts can click, type, scroll, and navigate within the isolated virtual machine, triggering behavior that might be blocked by time-delay evasion or anti-automation logic.

In the Google Cloud Storage / Remcos campaign, this capability is decisive. The malicious JavaScript embedded time-based evasion logic is a mechanism designed specifically to defeat automated sandbox analysis. An interactive sandbox can wait out that delay, manually trigger the next stage, and observe the complete execution chain from the initial JS download through the VBS stages, the PowerShell orchestration, the process hollowing via RegSvcs.exe, and the final Remcos C2 callback.

The result is not just a verdict but a full behavioral map: every process spawned, every network connection initiated, every registry key written, every file dropped. This map translates directly into actionable detection logic — MITRE ATT&CK-mapped TTPs, Sigma rules that can be deployed to SIEM and EDR platforms, and concrete IOCs that can be operationalized across the security stack.

MITRE ATT&CK matrix of the attack analyzed in the sandbox

For SOC teams, this means the difference between seeing an alert that says 'suspicious JavaScript file' and understanding the complete threat: this is Remcos RAT, delivered via process hollowing, with these C2 addresses, using these persistence mechanisms, and these are the detection rules that will catch the next variant.

Threat Hunting: Enrich, Pivot, and Hunt Proactively

ANY.RUN's Threat Intelligence Lookup is a searchable, continuously updated database of threat intelligence drawn from real-time malware analysis conducted by a community of over 600,000 cybersecurity professionals and 15,000 organizations worldwide. It functions as a force multiplier for threat hunting and incident response, providing instant enrichment for any indicator — IP address, domain, file hash, URL, or behavioral signature.

In the context of the Google Cloud Storage / Remcos campaign, Threat Intelligence Lookup enables analysts to move rapidly from a single observed indicator to a comprehensive understanding of the campaign's scope. A C2 IP address flagged by sandbox analysis can be pivoted to reveal all associated Remcos samples in the database, the infrastructure pattern used across the campaign, related file hashes, and behavioral indicators that might be present in other systems.

destinationIP:"198.187.29.19"

Domain associated with Google Cloud Storage/Remcos campaign in TI Lookup

This pivoting capability is particularly valuable for detecting multi-stage attacks where the initial indicators are clean (a googleapis.com URL, a signed Microsoft binary) but later-stage indicators — C2 domains, specific PowerShell script signatures, anomalous RegSvcs.exe activity — can be correlated against historical data to confirm campaign attribution and expand detection coverage.

For threat hunters, Threat Intelligence Lookup supports proactive campaign identification before an organization is impacted. YARA-based searches, combined with industry and geography filters, allow security teams to identify whether active campaigns are targeting their specific sector and region and to build detection rules based on real-world attacker behavior rather than theoretical models.

Monitoring: Automated, Continuous, Real-World Coverage

ANY.RUN's Threat Intelligence Feeds deliver a continuous stream of fresh, verified malicious indicators directly into an organization's security infrastructure — SIEM, SOAR, TIP, XDR — via STIX/TAXII and

API/SDK integrations. These feeds are generated from live sandbox analysis across the ANY.RUN community, meaning they reflect actual attacker behavior observed in real-world campaigns, not synthetic or retrospectively compiled threat data.

TI Feeds benefits and integrations

A critical differentiator is the uniqueness rate: ANY.RUN reports that 99% of indicators in its feeds are unique to the platform, not duplicated from public threat intel sources. The feeds also dramatically reduce Tier 1 analyst workload by providing malicious-only alerts with full behavioral context, cutting through the alert fatigue that plagues security operations teams dealing with high volumes of false positives from tools that cannot distinguish between legitimate googleapis.com traffic and the specific pattern of googleapis.com traffic used in this campaign.

Conclusion

The Google Storage phishing campaign delivering Remcos RAT is a wake-up call. As attackers continue to abuse trusted cloud services and legitimate binaries, organizations can no longer rely on reputation or signatures alone. Early detection through behavioral analysis and proactive threat intelligence is no longer optional — it is essential for survival.

By leveraging ANY.RUN's Enterprise Suite, security leaders can stay ahead of these evolving threats, protect critical assets, and maintain business continuity in an increasingly hostile digital landscape. The time to strengthen defenses is now — before the next bid document lands in your inbox.

About ANY.RUN

ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, helps security teams investigate threats faster and with greater clarity across modern enterprise environments.

It allows teams to safely execute suspicious files and URLs, observe real behavior in an Interactive Sandbox, enrich indicators with immediate context through TI Lookup, and monitor emerging malicious infrastructure using Threat Intelligence Feeds. Together, these capabilities help reduce investigation uncertainty, accelerate triage, and limit unnecessary escalations across the SOC.

ANY.RUN is trusted by thousands of organizations worldwide and meets enterprise security and compliance expectations. It is SOC 2 Type II certified, demonstrating its commitment to protecting customer data and maintaining strong security controls.

FAQ

What makes this Google Storage phishing campaign different from traditional attacks?

It hosts the phishing page on legitimate storage.googleapis.com domains instead of suspicious new sites, bypassing URL reputation filters entirely.

How does the attack ultimately deliver Remcos RAT?

Through a layered chain of JS, VBS, PowerShell, and in-memory loading that culminates in process hollowing of the trusted RegSvcs.exe binary.

Why is RegSvcs.exe particularly dangerous in this context?

It is a signed Microsoft .NET binary with a clean VirusTotal reputation, allowing attackers to inject the Remcos payload without triggering file-based alerts.

What capabilities does Remcos RAT provide to attackers?

Full remote access, keylogging, credential theft, file exfiltration, screenshot capture, and persistence — all while running inside legitimate processes.

How can ANY.RUN's sandbox help my team detect similar threats?

It detonates suspicious files/URLs in a safe environment, reveals the complete behavioral chain, and provides IOCs and process trees for immediate response.

What should businesses do immediately to protect against these attacks?

Enable behavioral analysis tools, integrate real-time threat intelligence feeds, train staff on cloud-storage lures, and test suspicious links in an interactive sandbox before opening.
