ultraviolet

THREAT ADVISORY

SMOKESCREEN RMM Abuse

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
August 6 2026
TLP:GREEN

Executive Snapshot

Security researchers have identified an active campaign, SMOKE#SCREEN, that impersonates Adobe and Zoom software updates, business document reviews, and system maintenance utilities to trick users into installing ConnectWise ScreenConnect, a legitimate RMM tool that provides attackers with full, persistent remote desktop access. The actor uses a rotating toolkit of obfuscated scripts and compiled loaders, some of which disable Windows Defender and SmartScreen before installation. They deliver payloads through trusted platforms like Dropbox and Cloudflare Tunnels to evade domain reputation filtering. Because the final payload is a validly signed, vendor-trusted binary, the threat is effective against organizations that rely primarily on certificate and reputation-based controls rather than behavioral detection. The campaign targets both Windows and macOS and shows clear evidence the actor is actively adjusting tradecraft in response to specific EDR products.

- Inventory and restrict RMM tools: identify which remote access tools (ScreenConnect, AnyDesk, Atera, etc.) are approved for use in your environment, and block installation or execution of any RMM client not on that list via application control policy.
- Implement AppLocker or WDAC rules to prevent MSI and EXE execution from user-writable locations such as %TEMP%, Downloads, and AppData, where these payloads are staged.
- Set UAC to "Always notify" and remove local admin rights from standard users where feasible, to prevent silent privilege escalation during installation.
- Run targeted user awareness training on fake software update prompts, specifically warning staff not to download or run Zoom, Adobe, or "system check" updates delivered via email links, and to route update installation through IT rather than end-user action.

TIDE Team Analysis

Securonix Threat Research has disclosed an active, multi-wave campaign, tracked as SMOKE#SCREEN, that uses fraudulent Adobe and Zoom update notices, spoofed business document reviews, and fake "system check" utilities to trick users into silently installing ConnectWise ScreenConnect, a legitimate remote monitoring and management (RMM) tool. Rather than deploying a purpose-built remote access trojan, the actor abuses a signed, vendor-trusted product to gain full remote desktop access to victim machines while evading detections that treat known-good software as low risk. The campaign has not been attributed to a specific threat group, but researchers assess it is active, well-resourced, and under continuous development.

Initial access relies on a diversified toolkit: obfuscated VBScript droppers, unobfuscated WMI-based scripts, a security-tampering batch loader, and compiled .NET executables, all engineered to defeat both automated sandboxes and human suspicion. Early samples used XOR-encrypted state-machine logic and environment checks (minimum RAM thresholds, detection of tools such as Wireshark, Process Monitor, and VMware Tools) to avoid analysis. Later samples escalated to a nine-step sequence that disables AMSI, bypasses UAC, disables SmartScreen, and adds Windows Defender exclusions, including excluding the entire C: drive, before delivery of the payload. Regardless of the specific chain, every path terminates in a ConnectWise-signed ScreenConnect MSI validated by a legitimate DigiCert certificate, giving the payload the appearance of trusted IT software.

The infrastructure behind the campaign reflects deliberate operational security. A single WsgiDAV-based staging server was found hosting the full payload arsenal while doubling as a ScreenConnect relay, and researchers identified three independently keyed relay clusters so that the loss of one node does not disrupt overall command and control. The actor rotates payload hashes between download sessions to blunt hash-based detection, and it abuses trusted cloud infrastructure, including Dropbox links and Cloudflare Quick Tunnels, to bypass corporate domain reputation and proxy filtering. A macOS .pkg variant connecting to the same primary relay confirms the operation targets both Windows and macOS estates, not Windows alone.

Perhaps most notable for defenders is the campaign's visible evolution in tradecraft. The actor shifted from an aggressive "destroy the endpoint agent" approach, fully disabling Defender before payload delivery, to a stealthier model that avoids tampering altogether and instead inserts deliberate timing delays (a 180-second sleep) explicitly designed to break correlation windows in specific EDR platforms. This shift indicates the actor is actively testing against commercial detection stacks and adjusting technique based on what gets flagged, a pattern that should be read as an early indicator of adversary reconnaissance against defensive tooling rather than a one-off campaign.

For enterprise environments, the risk is best framed as a gap in trust-based controls rather than a signature-detection failure: certificate validation, vendor allow-lists, and domain reputation filtering are each individually satisfied by this campaign's payloads and infrastructure. Recommended mitigations include enforcing AppLocker or WDAC policies to block MSI execution from user-writable directories, alerting on any attempt to modify Defender exclusions or stop the WinDefend service, auditing and allow-listing authorized RMM tools while blocking unauthorized ScreenConnect, AnyDesk, or Atera connections to raw IP addresses, enforcing UAC at "Always notify," and deploying behavioral EDR rules to catch anomalous parent-child process chains such as PowerShell or cmd.exe spawning msiexec.exe with silent-install flags. Given the campaign's demonstrated cross-platform reach and infrastructure resilience, organizations should treat RMM governance and Defender-tamper alerting as immediate priorities rather than routine hygiene items.

Why It Matters

The abuse of legitimate RMM tools by threat actors is not a new tactic, but it has accelerated sharply over the past two years as attackers have recognized the asymmetry it creates. A signed, vendor-trusted RMM client like ScreenConnect carries the same certificate reputation and code-signing trust as any authorized IT deployment, which means traditional controls built around known-bad signatures, untrusted certificates, or unfamiliar binaries are structurally blind to it. Ransomware affiliates and initial access brokers have used this technique for years to embed themselves in environments prior to extortion or data theft, and SMOKE#SCREEN represents a continuation of that trend rather than a novel technique. What distinguishes it is the scale of tooling investment and the discipline of the operational security behind it, indicating this is not an opportunistic actor but one treating RMM abuse as a durable, reusable capability.

The trajectory of this campaign also reveals where this class of threat is heading. Early campaigns of this type typically relied on a single dropper and a single C2 path, making them relatively easy to disrupt once discovered. SMOKE#SCREEN's compartmentalized infrastructure, independently keyed relay clusters, rotating payload hashes, and cross-platform coverage across Windows and macOS show that actors are now building resilient, redundant delivery ecosystems designed to survive partial takedown and continue operating even after some infrastructure is burned. The explicit code comment referencing evasion of a specific EDR vendor's correlation window is a meaningful signal in itself: it confirms that threat actors are actively testing payloads against commercial detection stacks before deployment, effectively conducting their own private red-team exercises against defensive products ahead of live use.

Looking forward, organizations should expect this pattern to intensify rather than fade. As EDR and SIEM vendors improve behavioral detection of Defender tampering and RMM misuse, actors will likely continue the pivot already visible in this campaign: away from loud, destructive evasion and toward quiet, patient techniques calibrated to specific security stacks. This raises the bar for defenders in two ways. First, static and signature-based defenses will offer diminishing returns against binaries that are legitimately signed and infrastructure that rides on trusted cloud services like Dropbox and Cloudflare. Second, defenders will need continuous, adaptive behavioral baselines for what "normal" RMM and administrative activity looks like in their own environment, since the attacker's core strategy depends entirely on blending into that baseline rather than standing apart from it.

How to Respond

- Strictly adhere to cybersecurity fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Inventory and restrict RMM tools: identify which remote access tools (ScreenConnect, AnyDesk, Atera, etc.) are approved for use in your environment, and block installation or execution of any RMM client not on that list via application control policy.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---