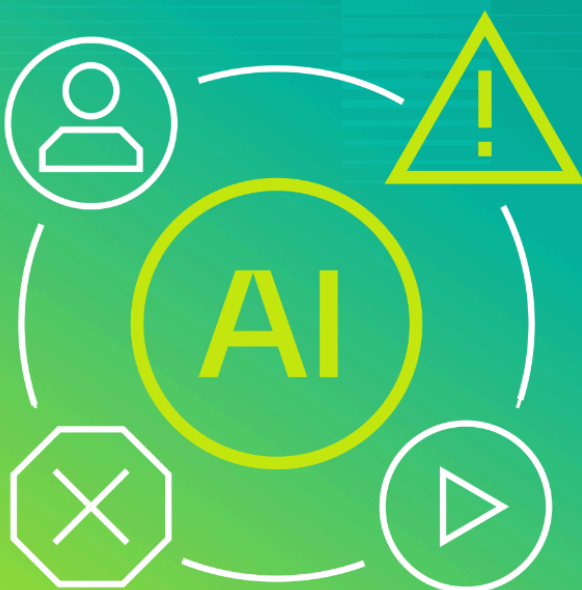


Weaponizing Workplace Communications

How Videoconferencing Impersonation
and AI Exploitation Enable Malicious
ScreenConnect Deployment



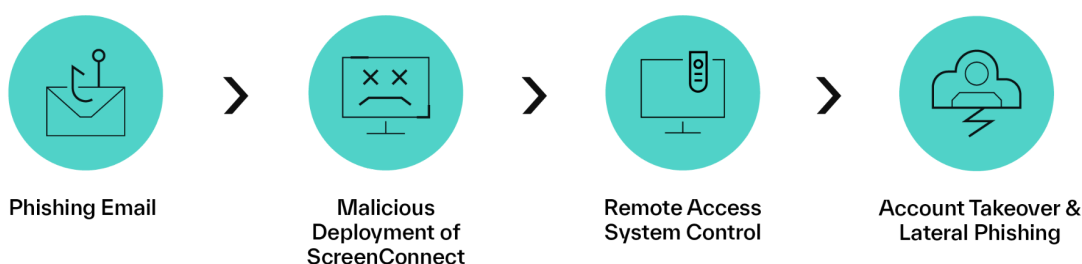
Executive Summary

An ongoing phishing campaign is targeting organizations across multiple industries, using sophisticated social engineering tactics to convincingly impersonate well-known videoconferencing platforms and deploy ConnectWise ScreenConnect for unauthorized system access. Unlike traditional credential-harvesting attacks that steal login information, this campaign deceives targets into downloading legitimate remote monitoring and management (RMM) software, granting cybercriminals complete control over end-user devices.

To manipulate targets into engaging and downloading ScreenConnect, the attackers employ advanced deception techniques built around impressive impersonations and familiar business contexts, effectively creating workflows that align with end-user expectations. Specific tactics observed include the utilization of compromised legitimate email accounts, AI-generated phishing components, and strategic URL obfuscation methods, as well as the exploitation of trusted business tools such as file-sharing platforms for hosting malicious links.

ScreenConnect, a commonly used RMM tool with extensive functionality, allows malicious activity to blend seamlessly with sanctioned IT operations, making detection and response significantly more challenging. Thus, once ScreenConnect is installed, threat actors can achieve system control while maintaining operational stealth.

What: Attack Progression



Initial Access: Cybercriminals send phishing emails impersonating trusted entities (e.g., Zoom and Microsoft Teams) from compromised legitimate accounts, incorporating timely themes and familiar branding to maximize credibility.

Deployment: Targets are deceived into installing ScreenConnect through one of several vectors: AI-generated landing pages, legitimate file-sharing platforms, direct session links, or executable email attachments.

Persistence: Once installed, ScreenConnect provides bad actors with remote access capabilities that enable comprehensive system control equivalent to direct access while avoiding detection due to minimal signal activity.

Post-Compromise: Attackers leverage compromised systems for account takeover (ATO), including lateral phishing campaigns and credential harvesting, often using the target's email accounts to target colleagues and business partners with additional ScreenConnect deployments.

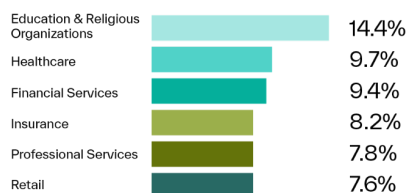
So What: Impact Analysis

TARGET SCOPE

900+

Organizations worldwide targeted by ScreenConnect weaponization attacks

SECTORS



THREAT IMPACT

Weaponizing ScreenConnect enables comprehensive system control equivalent to IT administrator access, facilitating lateral phishing and persistent organizational compromise while evading detection.

This campaign represents a significant evolution in cybercrime tactics. The weaponization of a legitimate IT administration tool—one designed to grant IT professionals deep system access for troubleshooting and maintenance—combined with social engineering and convincing business impersonation creates a multi-layered deception that provides attackers with the dual advantage of trust exploitation and security evasion.

Additionally, the sophisticated and resilient infrastructure supporting these attacks indicates a mature criminal ecosystem where dark web vendors operate like legitimate software providers, investing heavily in user-friendly ScreenConnect packages that enable any threat actor to launch sophisticated attacks. The commoditization of advanced attack capabilities—driven by bad actors who profit from widespread tool adoption—has democratized complex cybercrime operations and poses an escalating threat to organizations across all sectors, particularly those with legacy security infrastructure or limited security awareness programs.

Now What: Strategic Actions for CISOs

- **Implement Advanced Email Security:** Deploy AI-powered email security solutions capable of detecting complex social engineering attacks that bypass traditional security controls.
- **Enhance Endpoint Monitoring:** Establish comprehensive monitoring for legitimate remote access tools, focusing on unauthorized installations and suspicious usage patterns.
- **Strengthen Security Awareness:** Update training programs to address the evolving tactics of legitimate software abuse and the psychological manipulation techniques employed by modern attackers.
- **Deploy Zero-Trust Architecture:** Implement network segmentation and access controls that limit the potential impact of compromised systems with remote access capabilities.

Attack Overview

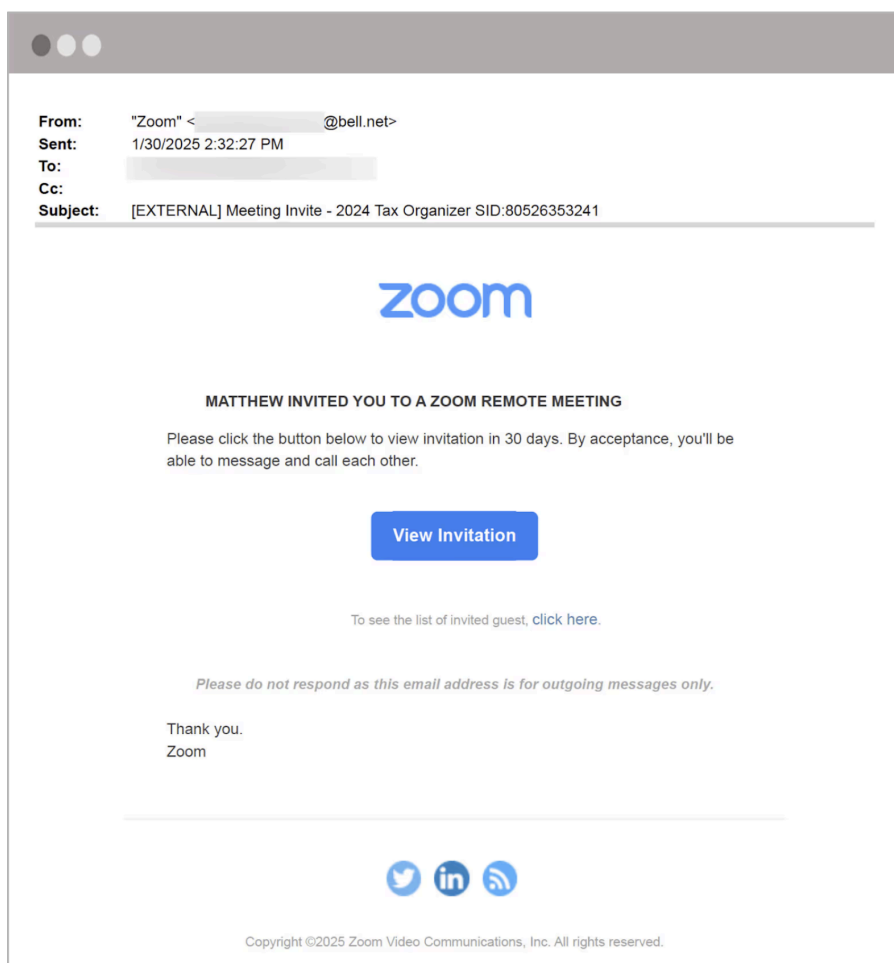
The attack methodology involves a carefully orchestrated sequence designed to exploit specific vulnerabilities in user behavior and organizational trust frameworks. By mimicking expected business workflows at each stage, attackers minimize red flags for targets and maintain the appearance of legitimate business activity throughout the process of establishing persistent, covert access.

Stage 1: Phishing Email

The multi-stage attack is initiated via phishing emails that are designed to appear as routine business communications or friendly correspondence—leveraging familiar branding and timely context to maximize believability.

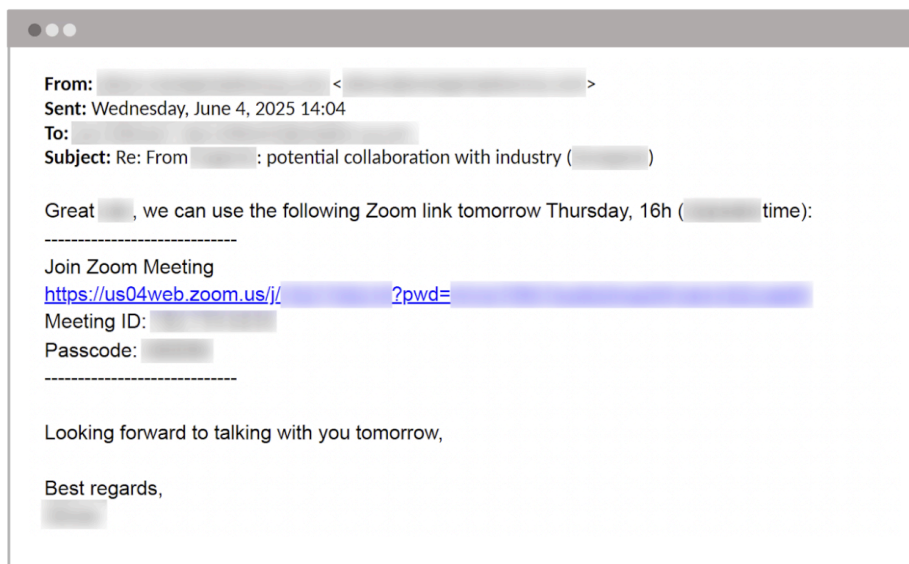
Videoconferencing Platform Impersonation

Among the most common tactics we observed in this campaign is attackers disguising the initial phishing email as a Zoom meeting invitation. The email's subject line references a seemingly legitimate purpose—for example, "Meeting Invite - 2024 Tax Organizer SID:80526353241," tying in timely tax season relevance to make the message feel even more genuine.

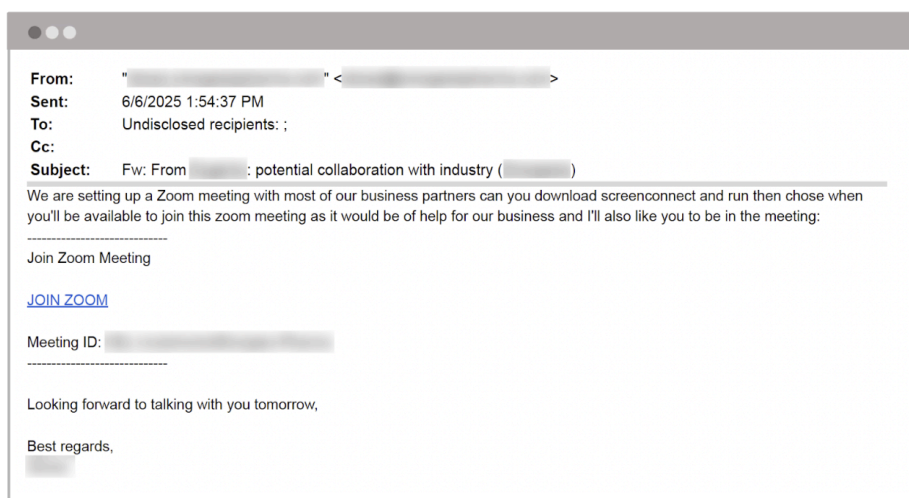


It features familiar Zoom branding and vague language meant to trick the recipient into clicking the "View Invitation" button. The email also originates from a compromised legitimate account, lending credibility and reducing the chance of detection by security tools. In this particular instance, the attackers appear to have found a real Zoom notification email and modified only the call-to-action (CTA) to further enhance the illusion of authenticity. Once the CTA is clicked, the target is redirected to a malicious site where the second stage of the attack is initiated.

In the second example, the threat actors again use a compromised account to deliver the malicious link. However, in this case, they hijack an ongoing thread that already contained a genuine Zoom meeting invitation, shown below.

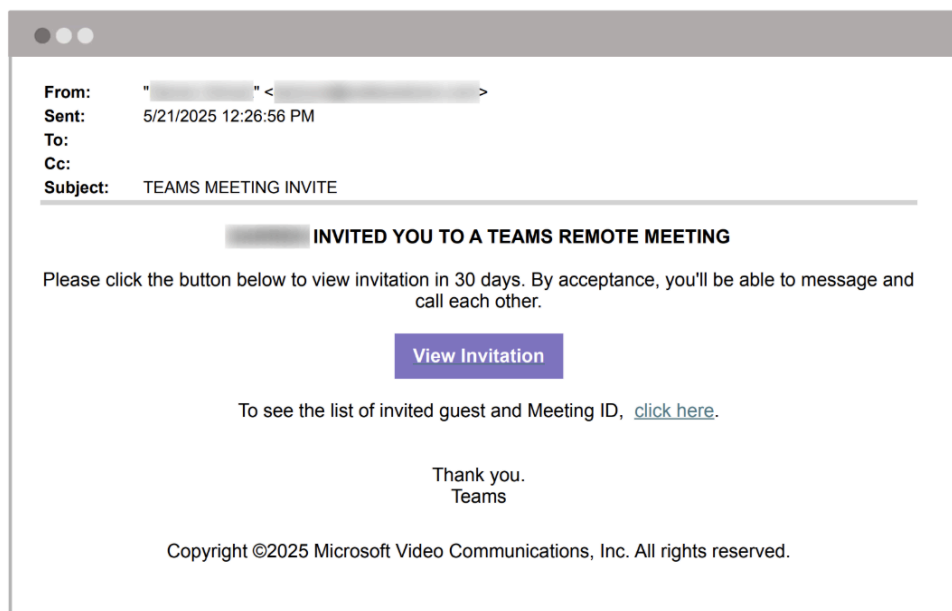


By injecting the malicious link into a conversation where a Zoom meeting is already being discussed, the attacker can leverage the existing pretext to convince the targets to click the link.



The screenshot above shows the fraudulent Zoom invitation the attacker inserted into the thread. If any recipient of the email clicks on the link labeled "JOIN ZOOM", they will be redirected to a live ScreenConnect session (if they already have the platform installed) or prompted to download the software.

Zoom isn't the only videoconferencing platform that bad actors opt to impersonate. We also uncovered malicious emails posing as Microsoft Teams invitations.



Similar to the fabricated Zoom emails, the fake Teams invitation was likely sent from a compromised account and features minimal text, along with a prominent CTA button. Clicking on the embedded link—which incorporates the impersonated sender's company name into the URL—redirects the target to a malicious site that prompts them to download what appears to be the latest version of Microsoft Teams but is, in reality, ScreenConnect.

Malicious Obfuscation

The sophistication of these attacks extends beyond social engineering to include advanced technical obfuscation methods designed to evade security controls and maintain operational persistence.

Email Service Provider Domain Wrapping

One technique we observed involves the abuse of legitimate email service providers, particularly SendGrid, to wrap malicious URLs within reputable domains. SendGrid and similar services are commonly used by organizations for legitimate email marketing and transactional communications, making their domains inherently trusted by both security systems and end users.

Threat actors exploit this trust by registering accounts with these services and using their URL wrapping features to obscure the true destination of malicious links. The wrapped URLs appear as legitimate SendGrid domains (such as u8041948.ct.sendgrid.net) followed by complex tracking parameters that eventually redirect to attacker-controlled infrastructure.

Open Redirect Exploitation

Another tactic involves leveraging open redirect vulnerabilities in legitimate websites. Open redirects occur when web applications accept user-controlled input to determine redirect destinations without proper validation, allowing bad actors to create URLs that appear to point to credible sites but ultimately redirect to malicious destinations.

These vulnerabilities enable threat actors to use well-established domains as launchpads for their attacks, which offers two primary benefits. First, it reduces user suspicion, as recipients see familiar hostnames before any redirection occurs. Second, it can help the attacker sidestep URL reputation systems, which may approve the initial domain without analyzing the final destination.

Cloud Platform Reputation Abuse

A third obfuscation approach involves exploiting the reputation of trusted cloud platforms like Cloudflare Workers, a serverless computing platform that allows developers to run code at the network edge using workers.dev domains. Many security systems automatically whitelist these domains due to Cloudflare's reputation as a legitimate content delivery network and security provider.

Attackers abuse this trust by using Cloudflare Workers to directly host attack infrastructure or deploy malicious applications that serve as intermediaries. This approach offers several advantages: global distribution ensures fast loading times regardless of target location, built-in SSL certificates provide encrypted connections, and sophisticated routing capabilities enable geo-blocking and other evasion techniques.

Base64-Encoded Link Segmentation

One particularly clever technique involves segmenting link anchor text with base64-encoded data. What appears to users as simple text like "Download Statement" is actually constructed with hidden encoded segments:

```
Dow<u><>base64_redacted=3D</u>nlo<u>base64_redacted=3D</u>ad  
St<u>base64_redacted=3D</u>atem<u>base64_redacted=3D</u>ent
```

In the example above, the base64-encoded string "`base64_redacted`" represents the recipient's email address, which is strategically inserted between legitimate text characters. These encoded segments are wrapped in HTML underline tags (`<u></u>`), while the CSS property `text-decoration:none` neutralizes any visual artifacts that would otherwise reveal the obfuscation to users.

The primary purpose is to evade detection mechanisms by breaking up recognizable signatures that security tools typically search for. This method effectively defeats systems that scan for indicators of compromise (IOCs), YARA rules that rely on pattern matching, and regex-based analysis designed to identify suspicious content.

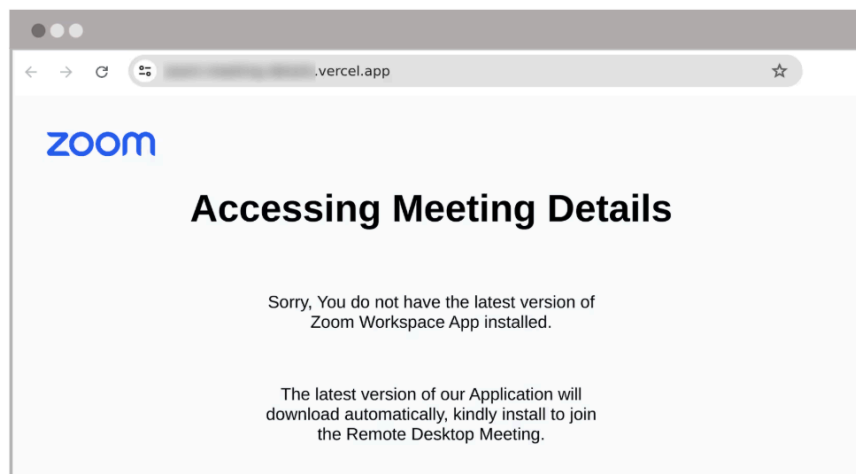
Once targets reach these carefully disguised endpoints, the next phase of the attack begins: deploying ScreenConnect.

Stage 2: Deployment of ScreenConnect

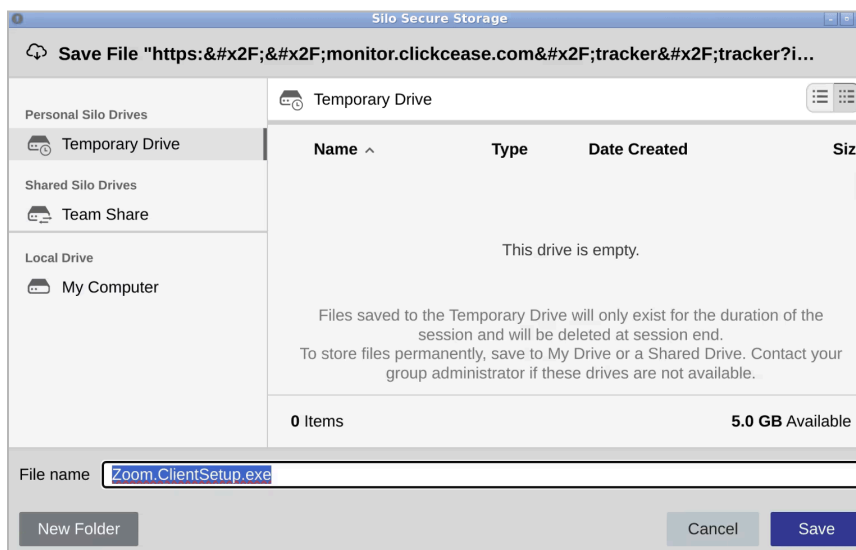
The deployment process reflects a deep understanding of the technical and psychological factors that influence user behavior. Attackers combine legitimate-looking interfaces with urgent messaging, minimizing suspicion while maximizing the likelihood of successful installation.

Automatic Download via AI-Generated Phishing Page

The primary tactic involves redirecting targets to a malicious site hosted at vercel.app. The page, mimicking Zoom's interface, claims the latest version of Zoom isn't installed and that the newest version will automatically download.



Within seconds, the site opens a new browser tab, prompting the download of Zoom.ClientSetup.exe. But this isn't a legitimate Zoom installer. The file is, in fact, ScreenConnect.



The phishing page was likely built using Vercel's v0, an AI-powered tool that helps developers build complete user interfaces from text prompts—essentially functioning as an automated designer and front-end developer. v0 transforms basic ideas into production-ready layouts in minutes, eliminating the need for extensive coding and design expertise.

Embedded Link to Real ScreenConnect Session

The most direct deployment method involves embedding actual ScreenConnect session links directly within phishing emails, creating an immediate pathway to system compromise. This technique exploits the fact that many organizations already have ScreenConnect installed for legitimate remote support purposes, allowing threat actors to bypass the installation process entirely.

Display Text	Link URL
JOIN ZOOM	https://[redacted].screenconnect.com/?Session=[redacted]

When recipients click these links, they are immediately connected to a live ScreenConnect session controlled by the bad actor, assuming the software is already present on the target system. For targets without existing ScreenConnect installations, clicking these links triggers an automatic download prompt for the ScreenConnect client software.

Attack Variations

In addition to the techniques described above, attackers utilize various other social engineering lures to deploy ScreenConnect. Below are additional attack variations observed in this campaign.






Email Theme	Lure	Delivery Method
Zoom/Microsoft Teams Meeting Invitation	Invitation to virtual meeting with link to join call	Links to fake Zoom-like domains or legitimate services (e.g., discordapp[.]com/attachments), where malicious payload is hosted
Event Invitation	Invitation to personal or corporate event with link to RSVP	Links to malicious ScreenConnect instances hosted on fake domains
Shared Document Notification	Notification of shared document (e.g., contract, financial statement, etc.) with link to view document	Links to legitimate services like Dropbox or Github (e.g., raw[.]githubusercontent[.]com), where malicious payload is hosted
Windows Update Notice	Urgent alert regarding system update with link to download and install update	Uses redirects from vk[.]com/google[.]com to fake domain delivering malicious ScreenConnect executable
Impersonation of Authorities	Notification from government agency (such as SSA) regarding important document, with link to download document	Links to legitimate services, where malicious payload is hosted

Stage 3: Account Takeover

The weaponization of ScreenConnect's intended functionality enables threat actors to achieve comprehensive system access equivalent to that of a legitimate IT administrator. This means they can bypass security controls, navigate file systems, and establish a persistent presence across the organization's infrastructure. Because many malicious activities blend seamlessly with legitimate remote administration, threat actors can easily conduct reconnaissance, move laterally, and exfiltrate sensitive data without the organization being immediately alerted.

Post-Compromise Activity: Lateral Phishing

Once initial system access is established through ScreenConnect, cybercriminals frequently pivot to lateral phishing campaigns that leverage the compromised environment to target additional targets within the organization. They analyze communication patterns, identify high-value targets, and craft phishing messages that appear to originate from trusted internal sources.

	 Sent Timestamp	 From Email	 Email Subject	 Recipient Email 
1	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.s. @.edu
2	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.v. @.edu
3	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.m. @.edu
4	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.f. @.edu
5	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.m. @.edu
6	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.d. @.edu
7	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.b. @.edu
8	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.b. @.edu
9	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.b. @.edu
10	2025-03-13 19:17:07	d.j. @.edu	ZOOM Remote Meeting Invitation	a.k. @.edu

Because bad actors can send phishing emails directly from the target's actual account, they can bypass security controls that might flag external phishing attempts. These emails often invite colleagues, partners, and business contacts to join "urgent" video conferences or access "critical" shared documents, ultimately leading to additional ScreenConnect deployments.

Attackers may also use the compromised access to modify existing email threads, inserting malicious links into ongoing legitimate conversations about meetings or document sharing. This technique exploits the natural tendency for users to trust communications that appear to be continuations of established business discussions.

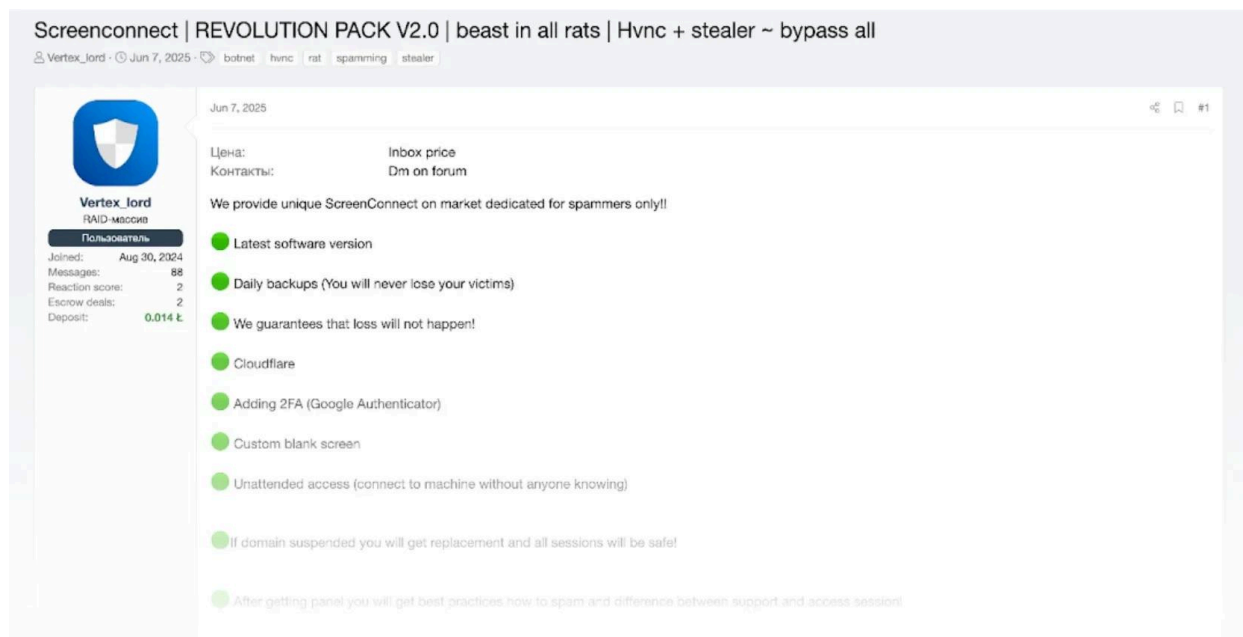
Dark Web Enablement and Tooling

The rise in ScreenConnect-enabled cyberattacks is closely tied to a growing dark web ecosystem that supports the deployment, maintenance, and monetization of the remote management and monitoring (RMM) tool. This underground economy caters to both novice and more advanced threat actors, offering a range of services from pre-packaged kits to fully customized infrastructure that facilitates the weaponization of ScreenConnect.

Our analysis of dark web forums, Telegram channels, and underground marketplaces reveals a mature supply chain that significantly lowers the barrier to entry for ScreenConnect-based attacks.

Underground Offerings: Bundled Tools and Custom Builds

Cybercriminals can acquire ScreenConnect in numerous forms across forums, encrypted messaging apps, and anonymous web pages. One of the most popular offerings is the “ScreenConnect REVOLUTION PACK V2.0”, which includes a ScreenConnect agent bundled with hidden virtual network computing (HVNC), wallet checkers, and a suite of security bypasses—such as evasion of Windows Defender, UAC prompts, and even CTRL+ALT+DEL and power options.




This pack also includes a “blank-screen fix” that hides the attacker’s cursor during remote sessions, allowing bad actors to maintain uninterrupted control over compromised systems. It also includes operational resilience features such as daily backups of command-and-control infrastructure and Cloudflare front-end configurations, allowing for quick re-deployment when needed. Perhaps most significantly, the pack offers session restoration capabilities that retain previous connections even if domains are suspended, eliminating the need for re-establishment and ensuring persistent access to compromised systems.


Other sellers offer turnkey deployments, such as full ScreenConnect infrastructure hosted on virtual private servers (VPS) with HTTPS certificates, relay links, asset grouping, and role-based access. One vendor even advertised a \$6,000 custom-branded package with training and after-sales support—effectively a RAT-as-a-Service model that lowers the barrier to entry for non-technical attackers.


Additionally, “lifetime source kits” are being sold for approximately \$3,000, providing buyers with access to the entire source code, silent activation patchers, and server relay configurations. This type of access allows mid-tier actors to host their own persistent infrastructure and bypass traditional hosting limitations.

Access Brokerage and Loader Kits

Not all offerings focus on deployment; some are focused on resale. Vendors offer domain-admin level ScreenConnect access to networks in Germany, the UK, and China, typically including control over 90–345 hosts. These access sales, averaging \$500 to \$2,000 per network, represent a significant escalation from simple tool provision to direct network compromise facilitation.

**I have access for sale**
...\$5MILLION + AV:WD (CAN BE DISABLED) PRIVILEGE: DOMAIN ADMIN 345 PCS IN HOST 500\$ PRICE 2. COMPANY LOCATION: DE REVENUE: \$1.4BILLION+ AV:WD (CAN BE DISABLED) PRIVILEGE: LOCALADMINISTRATOR 90 PCS IN HOST *ITS NOT THE MAIN SERVER OF THE COMPANY BOTH ARE **SCREENCONNECT** ACCESS
Bimarck · Thread · Jan 31, 2024 · Replies: 0 · Forum: ACCESSES: networks, rdp, shells, ftp, sql-inj, DB's


**Buy Access**
I will buy secureconnect access. **screenconnect**.com corp country United Kingdom US And I will also buy KRP access I buy dedicated servers with software: ProSeries21 Lacerte21 Drake21 usually on the desktop icons Pro18Pro19 Pro20 21 Lacerte18 19 20 21
chukkyangel · Thread · Jan 24, 2024 · Replies: 0 · Forum: ACCESSES: networks, rdp, shells, ftp, sql-inj, DB's

**Corp Access**
Geo: China Access Type: **ScreenConnect** Access L:DomainAdmin Industry: Consumer Electronics & Computer Retail Revenue:\$127.5million AV: ESET Pierce:\$700 Do let me know if have any questions
Bimarck · Thread · Jan 22, 2024 · Replies: 1 · Forum: ACCESSES: networks, rdp, shells, ftp, sql-inj, DB's

Loader kits are also available via Telegram, with sellers advertising ScreenConnect installers that silently drop additional payloads and execute post-install scripts. These kits are likely customized per buyer and priced accordingly.

Bulletproof Infrastructure and Persistence Tactics


Criminal actors demonstrate a sophisticated understanding of operational security through their hosting preferences and persistence mechanisms. Underground discussions reveal a preference for “bulletproof” VPS providers that ignore abuse complaints and resist takedown attempts. A notable example involves one user requesting 93 VPS servers from psb-hosting[.]pro specifically for “hosting ScreenConnect services” without triggering reputation blocklists from services like Spamhaus or URLhaus.



Grand_Ceaser
floppy disk
User

Joined: Dec 21, 2024
Messages: 9
Reaction score: 1
Deposit: 0.0054 B

Jun 8, 2025


PSB Offshore said: 



Updating VPN Tariff Plans




<https://psb.hosting/a-vpn>

1 month - 3 \$
3 months - \$8.1 (10% discount)
6 months - \$15.3 (15% discount)
12 months - \$28.8 (20% discount)

i need 93 servers that doesn't get flagged or suspend it i host screen connect service i tried rdpsh and once. they get reports from urlhaus/spamhaus listings they suspendis your service won't do that? I need a clear answer that servers will never be suspended
Can you guarantee that?

 Report

New   #5

 Like +  Quote  Reply

These hosting services advertise low-cost, no-log VPN/VPS setups that support cryptocurrency payments and instant deployment. Many also allow abuse-resistant configurations using Cloudflare to obscure server origins and port forwarding on common ports like 443 or 80 to blend in with regular HTTPS traffic. Some configurations even use TCP ports 8040/8041, the default for ScreenConnect relays. This bulletproof hosting approach directly addresses the operational challenge of maintaining persistent access despite security vendor detection efforts.

Cloud and Self-Hosted Deployment Options

These hosting decisions intersect with the two deployment models offered by ScreenConnect: cloud-hosted and self-hosted. In the cloud-hosted model, infrastructure is maintained by ConnectWise, and URLs typically follow the format of subdomains on screenconnect.com (e.g., example.screenconnect[.]com). In contrast, the self-hosted model allows attackers to configure and deploy ScreenConnect on custom infrastructure using attacker-owned domains (e.g., acme-client-access[.]com).

This reflects the options available on underground markets. Some threat actors purchase access to compromised cloud-hosted ScreenConnect accounts, while others deploy fully customized infrastructure using purchased “RAT-as-a-Service” kits.

From a security operations standpoint, this URL structure represents a deliberate attempt to sidestep IOC-based defenses. Organizations that rely on hardcoded domain lists or static file hashes will struggle to keep pace with dynamic attacker infrastructure. For instance, a basic rule detecting “screenconnect.com” may miss customized domains that host the same payloads or route traffic through trusted intermediaries.

Threat Actor Segmentation

Based on pricing and sophistication, the ScreenConnect underground economy appears to support two main categories of threat actors:

- **Tier 1 – Low Skill:**
 - Use pre-packed kits like ScreenConnect REVOLUTION PACK V2.0.
 - Typically spam or phishing crews with minimal configuration ability.
 - Goal is fast deployment of remote access plus data theft tools.

- **Tier 2 – Mid Skill:**
 - Invest in turnkey deployments or complete source kits.
 - Often Initial Access Brokers or small ransomware affiliates.
 - Require persistence and operational independence without building tools from scratch.

This segmentation reflects the widespread accessibility of ScreenConnect tooling and its ability to enable cybercriminals at all levels to compromise systems at scale.

The evidence suggests that this ecosystem will continue to evolve, with actors increasingly focused on persistence, evasion, and scalability. The combination of legitimate software abuse, bulletproof hosting, and tiered criminal offerings creates a formidable challenge for defensive teams, requiring comprehensive monitoring across network, endpoint, and threat intelligence domains.

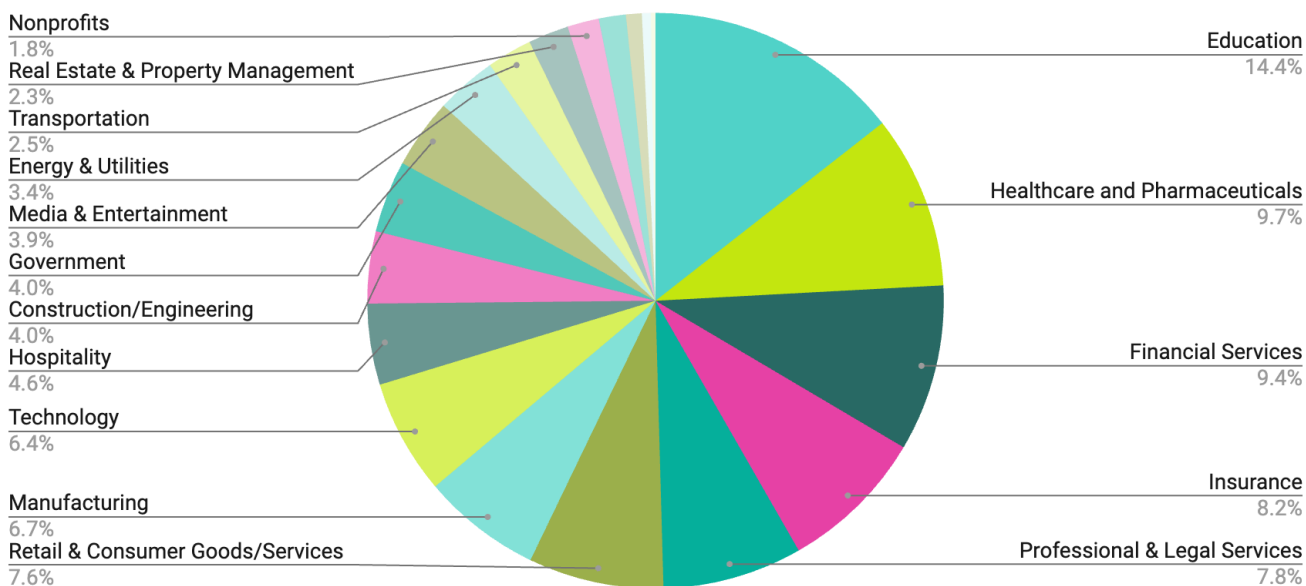
Victimology

Abnormal researchers discovered that this phishing campaign has targeted over 900 organizations across a broad spectrum of industries and geographic regions. The campaign's wide-reaching nature reflects the universal appeal of videoconferencing impersonation tactics and the accessibility of ScreenConnect deployment tools in underground markets.

Of the targeted organizations identified by Abnormal researchers, education and religious organizations represent the largest segment at 14.4% of targets, followed by healthcare and pharmaceuticals at 9.7%, and financial services at 9.4%. This relatively even distribution across sectors—with no single industry representing more than 15% of targets—suggests attackers are prioritizing broad coverage over specialized targeting.

The distribution across other business sectors is notably even, with insurance (8.2%), professional and legal services (7.8%), retail and consumer goods (7.6%), manufacturing (6.7%), and technology (6.5%) all representing significant portions of the attack surface, reflecting the campaign's extensive reach across the economy.

Target Distribution, by Industry



Given the diverse social engineering techniques employed, the emphasis on lateral phishing post-compromise, and the commoditized nature of ScreenConnect tools in criminal marketplaces, this activity appears primarily focused on establishing widespread network access for potential resale or follow-on monetization rather than targeted espionage or sector-specific data theft.

Geographically, most affected organizations were based in the United States, with notable presence from Canadian (.ca domains), Australian (.com.au, .edu.au, .gov.au domains), and UK organizations (.co.uk domains), demonstrating the global scope of this threat campaign.

Conclusion

ScreenConnect-enabled compromises exploit legitimate remote administration capabilities, leaving minimal forensic evidence and significantly complicating detection and response efforts. The psychological sophistication of these attacks—leveraging familiar videoconferencing contexts and established relationships—exploits fundamental human vulnerabilities to deceive targets into granting attackers access to their devices.

The maturity of the supporting criminal ecosystem—evidenced by tiered service offerings, bulletproof hosting solutions, and comprehensive evasion techniques—indicates that ScreenConnect abuse is not an isolated phenomenon but rather a systematic exploitation of trust in modern business communications.

This campaign serves as a critical reminder that modern threats increasingly weaponize trusted systems rather than circumvent them. As a result, defenders must fundamentally reconsider their approach to threat detection and response.

Security leaders must adopt a multi-layered defense strategy that encompasses advanced behavioral analytics, zero-trust network architecture, enhanced security awareness programs, and continuous threat intelligence research.