From SEO Poisoning to Malware Deployment: Malvertising campaign uncovered

⋮ 9/26/2025

Blog

Modern malvertising is faster and stealthier than ever. Discover how attackers abused SEO, Cloudflare, and short-lived certificates—and how our MDR stopped them.

5 minutes read

September 26, 2025

David Kasabji

Principal Threat Intelligence Analyst

Our Managed Detection and Response (MDR) team recently investigated a sophisticated malvertising campaign that attempted to compromise an enterprise endpoint through a fake Microsoft Teams installer. The attack was initially detected when Microsoft Defender's Attack Surface Reduction (ASR) rules blocked suspicious outbound connections, triggering our investigation.

Through detailed forensic analysis, we uncovered **a multi-stage attack leveraging SEO poisoning and certificate abuse**. What makes this campaign particularly noteworthy is the threat actor's abuse of legitimate code-signing services to evade detection, specifically exploiting short-lived certificates that expire within three days. Thanks to properly configured ASR rules, the malware was prevented from establishing command and control communication, effectively neutralizing the threat before any damage could occur.

Initial detection and alert

The ASR Block that started it all

On September 25, 2025, Microsoft Defender's Attack Surface Reduction rules triggered an alert by blocking suspicious outbound connections from a newly executed file. This preventive action initiated our investigation, which revealed a sophisticated attack attempt that had bypassed traditional signature-based detections through the use of valid code signing.

Timeline of events

Our forensic analysis reconstructed the following sequence of events:

Time	Event	Significance
13:42:28	Navigation to www.bing.com	Search initiated
13:42:39	Redirection to teams-install.icu	**11 seconds after search – indicating automated redirect**
13:42:55	HTTPS connection established to malicious domain	Payload download initiated
14:20:21	cleanmgr.exe creates DismHost.exe in Temp folders	Suspicious living-off-the-land activity
14:39:00	MSTeamsSetup.exe execution attempted	Signed malware execution
14:39:15	**ASR blocks C2 connection attempt**	**Attack prevented – Alert triggered**

The remarkably short 11-second gap between the Bing search and the malicious site visit immediately stood out—this timing is far too rapid for manual user interaction, strongly suggesting an automated redirect mechanism, likely through malvertising or a poisoned search result.

Technical analysis

Stage 1: The malvertising vector

Our investigation revealed a sophisticated redirect chain that led the user from a legitimate search to malware delivery:

Bing Search → team.frywow.com → teams-install.icu

The threat actors employed multiple deception techniques:

1. **SEO Poisoning/Malvertising**: Malicious sites positioned in search results for Teams-related queries
2. **Domain Spoofing**: The domain “teams-install.icu” crafted to appear as a legitimate Microsoft property
3. **Infrastructure Masquerading**: All malicious domains hosted on Cloudflare (IP ranges: 104.21.x.x, 172.67.x.x), leveraging the CDN’s reputation

teams-install[.]icu Infrastructure Details:

- **IP Addresses**: 172.67.154.95, 104.21.72.190
- **Hosting**: Cloudflare CDN
- **SSL Certificate**: Google Trust Services (WE1)
- **Certificate Validity**: September 24-26, 2025 (2 days only)
- **Domain Age**: Newly registered (typical of malicious campaigns)

Stage 2: Signed malware – the certificate abuse

The most sophisticated aspect of this campaign was how the malware evaded initial detection:

MSTeamsSetup.exe Analysis:

- **Digital Signature**: Valid and trusted
- **Signer**: “KUTTANADAN CREATIONS INC.”
- **Certificate Chain**: Microsoft ID Verified CS EOC CA 01
- **Certificate Lifespan**: 2 days (September 24-26, 2025)

This represents an emerging threat pattern where actors obtain legitimate short-lived certificates to:

- Bypass signature-based security controls
- Minimize the window for certificate revocation
- Automate the signing process for multiple campaigns
- Exploit trust in signed executables

Our research identified similar certificates being used in related campaigns, including signers such as “Shanxi Yanghua HOME Furnishings Ltd,” suggesting a broader operation.

The prevention success

Microsoft Defender’s ASR rules successfully blocked the malware’s attempt to establish C2 communication with:

- nickbush24.com (primary C2)

This timely intervention prevented:

- Establishment of persistent backdoor access
- Potential data exfiltration
- Deployment of additional payloads
- Possible ransomware deployment

What could have happened

Based on the indicators and our threat intelligence correlation, this malware appears to be a variant of the Oyster backdoor (also known as Broomstick or CleanUpLoader). For those interested in understanding the full capabilities of this malware family and what could have occurred without the ASR intervention, we recommend reviewing Rapid7’s detailed analysis: Malvertising Campaign Leads to Execution of Oyster Backdoor.

Their research documents the complete attack chain including persistence mechanisms, data collection capabilities, and post-exploitation activities that our client was fortunately spared from experiencing.

Detection recommendations

Based on our investigation, organizations should implement the following detection strategies:

Critical detection points

1. **Certificate Anomaly Detection**
    - Alert on executables signed with certificates valid for ≤ 7 days
    - Monitor for first-seen signers, especially for software installers
    - Track certificates issued by “Microsoft ID Verified CS EOC CA 01”
2. **Network-Based Detection**
    - Flag rapid redirects from search engines to newly registered domains
    - Alert on downloads from domains with .icu TLDs
    - Monitor connections to Cloudflare IPs immediately after search engine queries

Key lessons learned

1. **Living-off-the-Land Evolution**: Attackers continue finding creative ways to abuse legitimate Windows utilities
2. **ASR Rules Save the Day**: A properly configured Attack Surface Reduction policy can stop sophisticated attacks that bypass traditional antivirus
3. **Certificate Trust Is Not Absolute**: Short-lived certificates are being weaponized to evade security controls
4. **Speed of Attack**: Modern malvertising can compromise users in under 15 seconds from search to infection

Indicators of Compromise (IOCs)

Network Indicators:

Indicator	Description
teams-install[.]icu	Malicious payload delivery site
team[.]frywow[.]com	Redirect/gate infrastructure
witherspoon-law[.]com	Redirect/gate infrastructure
Nickbush24[.]com	C2 Server

File Indicators:

Indicator	Description
MSTeamsSetup.exe	The name of malicious executable
bd6ad2e1b62b2d0994adf322011f2a3afbb14f097efa3cbe741bc4c963e48889	SHA256 of malicious file
KUTTANADAN CREATIONS INC.	Certificate signer

Microsoft XDR advanced hunting queries

```
// Search for files signed by known malicious signers
DeviceFileCertificateInfo
| where Timestamp > ago(30d)
| where Signer has_any ("KUTTANADAN CREATIONS INC.", "Shanxi Yanghua HOME
Furnishings Ltd",
                       "Shanghai Ruikang Decoration Co")
| join kind=inner (DeviceFileEvents) on SHA1
| project Timestamp, DeviceName, FileName, FolderPath, Signer, SHA256,
InitiatingProcessFileName
| sort by Timestamp desc

// Detect connections to known malicious domains
DeviceNetworkEvents
| where Timestamp > ago(30d)
| where RemoteUrl has_any ("teams-install.icu", "nickbush24.com",
"team.frywow.com")
| project Timestamp, DeviceName, InitiatingProcessFileName, RemoteUrl,
          InitiatingProcessCommandLine
| sort by Timestamp desc
```

Conclusion

This investigation highlights both the sophistication of modern malvertising campaigns and the effectiveness of properly configured endpoint protection. While the threat actors successfully bypassed traditional signature-based detection through certificate abuse, Microsoft Defender's behavioral-based ASR rules prevented the attack from achieving its objectives.

Organizations should take this as a reminder to:

- Review and optimize ASR rule configurations
- Implement detection for certificate abuse patterns
- Educate users about malvertising threats
- Maintain defense-in-depth strategies

The rapid evolution of these techniques—from SEO poisoning to certificate abuse to living-off-the-land tactics—demonstrates that security teams must continuously adapt their detection and prevention strategies.

About the author

David Kasabji

Principal Threat Intelligence Analyst

David Kasabji is a Principal Threat Intelligence Analyst at the Conscia Group. His main responsibility is to deliver actionable intelligence in different formats according to target audiences, ranging from Conscia's own cyberdefense, all the way to the public media platforms. His work includes collecting, analyzing, and disseminating intelligence, reverse engineering obtained malware samples, crafting TTPs […]

David Kasabji

Principal Threat Intelligence Analyst

Join our Threat Intelligence newsletter

Stay ahead of cyber threats with Conscia ThreatInsights—the only European-focused threat intelligence newsletter.

Sign up here

Related

Resources