

Found by NSS 9 of 9 indicators on no list NSS holds

Fake Zoom update page installs a self-hosted ScreenConnect client: technical analysis

A page made to look like a Zoom meeting tells the visitor their app is out of date and offers an update. The update is a ScreenConnect remote-access client set to call a server its sender runs; whoever runs it hands over control of their computer. NSS took the page from the day's new registrations, captured it, read the installer and traced it to that server within 23 hours of the page's registration. The server's domain was registered 63 days before the lure. None of the nine indicators was on any list NSS holds on 12 November 2026.

PUBLISHED 12 Nov 2026
LAST UPDATED 12 Nov 2026
READING TIME 8 min
MARKING TLP:CLEAR

0 of the 9 indicators on any list NSS holds

23 h from lure registration to its

1 server behind the download portal and the relay

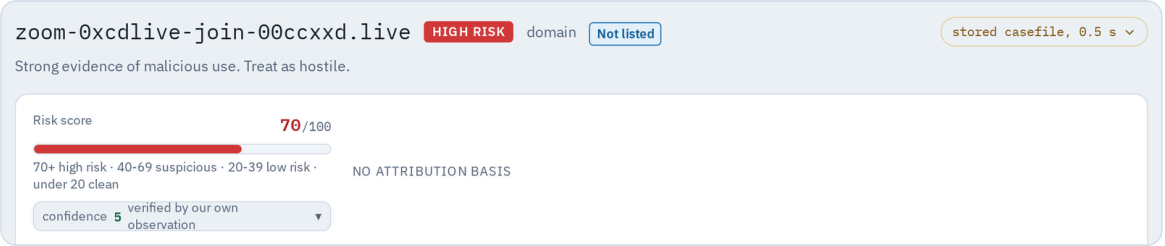
63 days

	server and file hash		by which the connect-back domain is older than the lure

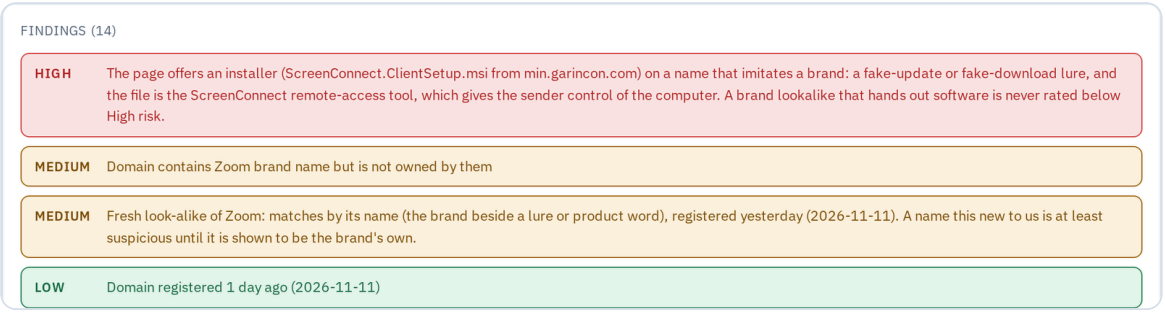
Key findings

1. The page zoom-0xcdlive-join-00ccxxd[.]live, registered on 11 November 2026 at 14:31 UTC, shows a fake "Zoom Cloud Meetings" window: "Update Required. Your app version needs to be 5.3.0 or higher to join this meeting." It served the same page to a desktop, a phone and a crawler.
2. The Update button downloads ScreenConnect.ClientSetup.msi from min[.]garincon[.]com. The file is a ScreenConnect remote-access client: 15,216,640 bytes, SHA-256 c98e783442a4ca72244f3bb1d5f8ad28bc1f3f94db8a5afac9597a7c870ca590. Two fetches gave the same file.
3. The client is set to connect back to 524ff283-2094-4f98-b68d-f24f61c5f8fa[.]dotinicon[.]com on port 8041. Anyone who runs it hands remote control of their computer to whoever runs that server.
4. One server sits behind both names. The connect-back host resolves to 45[.]87[.]61[.]155, which had ports 8041, 443 and 80 open on 12 November. Asked by address on port 443, it serves the same portal page as min[.]garincon[.]com, behind a content-delivery origin certificate issued on 13 October, the day garincon[.]com got its first certificate.
5. min[.]garincon[.]com is not a file store. It is a self-hosted remote-access portal ("Welcome to our online remote support and collaboration portal"). The sender runs their own instance of the product rather than borrowing anyone's account.
6. The two operator domains were bought at the same registrar a month apart: dotinicon[.]com on 9 September and garincon[.]com on 12 October 2026. The lure page was bought on 11 November, at a different registrar, and placed on a shared hosting platform.

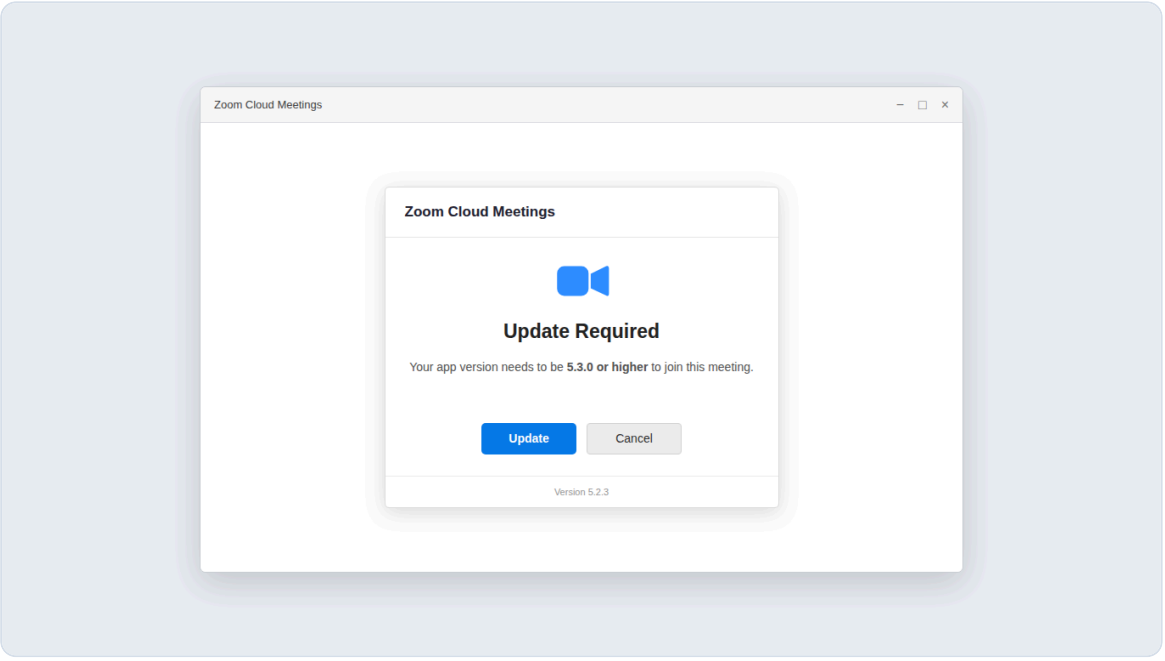
7. None of the nine indicators was on any list NSS holds when this paper was written. NSS now rates the page, both download names, both connect-back names and the server address High risk 70.



NSS Investigate, 12 November 2026: the stored casefile for the lure page reads High risk 70/100, confidence 5 (verified by our own observation), Not listed.



Why: the top findings in the same casefile. The score rests on what the page offers for download, not on its address.



What a visitor sees: NSS capture of zoom-0xcdlive-join-00ccxxd[.]live, 12 November 2026, 09:59 UTC. The Update button links to the installer on min[.]garincon[.]com.

Timeline

9 Sep 2026, 14:52
dotinicon[.]com is registered. It will hold the connect-back host.

12 Oct 2026, 17:51
garincon[.]com is registered at the same registrar.

13 Oct 2026
Certificates for garincon[.]com (12:28) and an origin certificate on the server 45[.]87[.]61[.]155 (16:14).

11 Nov 2026, 14:31
The lure page zoom-0xcdlive-join-00ccxxd[.]live is registered. Its first certificate follows 23 minutes later.

12 Nov, 04:08
The name arrives in NSS's next daily list of new registrations. NSS resolves it, and the brand rule matches Zoom beside "join".

12 Nov, 04:34
NSS captures the page and records the installer link. The first casefile reads Suspicious 40.

12 Nov, about 10:07
NSS adds a rule: a brand look-alike that offers an installer is rated malware delivery. The page and the download host move from Suspicious 40 to High risk 70.

12 Nov, 13:11
NSS fetches the installer once through its probe and reads where it connects. The connect-back host, its domain and the server move to High risk 70: 22 hours 40 minutes after the lure was registered.

How the lure works

The page draws a desktop window titled "Zoom Cloud Meetings" inside the browser, with the Zoom camera icon and a version line, "Version 5.2.3". It says the visitor's app must be 5.3.0 or higher to join the meeting. There are

two buttons. Update is a plain link to the installer. Cancel only shows a message.

The page needs no script to do harm, asks for no password and sets no cookie. It is 8,912 bytes and was the same for a desktop, a phone and a crawler, so it does not hide from scanners. Its harm is the file.

How visitors reach it NSS did not see. A name like this, with "join" and a meeting-style code in it, is made to sit in a meeting invitation sent by email or message.

The installer

NSS fetched the file once on 12 November at 13:11 UTC through its probe, took its hashes, read its settings and deleted it. It was never run.

PROPERTY	VALUE
File name	ScreenConnect.ClientSetup.msi
Size	15,216,640 bytes
SHA-256	c98e783442a4ca72244f3bb1d5f8ad28bc1f3f94db8a5afac9597a7c870ca590
MD5	e6142c9c458795d1fea5e18288c1adfb
Kind	Windows Installer package, author "ScreenConnect Software"
Client id	230f9b38c3c088fe, installed as the service "ScreenConnect Client (230f9b38c3c088fe)"
Connects to	524ff283-2094-4f98-b68d-f24f61c5f8fa[.]dotinicon[.]com, port 8041

ScreenConnect is a legitimate remote-support product. Here it is used as the payload: once installed, the client calls the sender's server and waits to be controlled. No exploit is needed, and security tools that trust remote-support software may let it run.

One server behind the names

Three records tie the download host and the connect-back host to one server, 45[.]87[.]61[.]155:

- The connect-back host resolves to it, and its relay port 8041 was open on 12 November.
- Asked by address on port 443, it serves the same portal page that min[.]garincon[.]com serves through a content-delivery network, with the same page title.
- It presents that network's origin certificate, issued on 13 October 2026, the day garincon[.]com received its first public certificate.

So the sender runs one self-hosted instance of the product. Its web portal is reached as min[.]garincon[.]com behind the delivery network, and its relay is reached directly as a long random host name under dotinicon[.]com. The two operator domains were bought at the same registrar, a month apart, and both use the delivery network's name servers.

Seen before: the same method in public reporting

NSS Hunt searched NSS's library of past reporting for the same lure and the same tool. The method is not new. These public reports describe it, closest first:

REPORTED	WHO, AS REPORTED	LURE	PAYLOAD	HOW CLOSE
Aug 2026	SMOKE#SCREEN campaign, no named group	Fake Zoom updates, then business documents	Legitimate ScreenConnect client for remote control, on Windows and macOS	Same lure, same tool
Sep to Oct 2026	Several criminal	Event invitations, fake meeting	Rogue ScreenConnect clients, one	Same tool, other lures

	campaigns, no named group	invitations, payment notices, shared dashboards	paired with a second remote-management tool	
2026	Sapphire Sleet, reported as North Korean	A fake Zoom SDK update on macOS	AppleScript that fetches further stages	Same lure, other payloa
May 2026	Nimbus Manticore (UNC1549), reported as Iranian	Trojanized Zoom installers and job lures	MiniJunk and MiniFast backdoors	Same lure, other payloa

NSS found none of this paper's names, addresses, file hash or client id in any of these reports, or anywhere else in its records. The match is in method only, so this paper does not link the operator to any group above. What the reports do show is that a fake Zoom update handing out a remote-support client is an established playbook, used by criminal crews for months, and that state groups use the Zoom update lure too.

Lure or test?

The Cancel button on the lure shows the message "You cancelled the demonstration." NSS cannot tell whether this page is a lure kit or an authorised phishing test. Either way, a remote-access client calling an instance you do not own is an incident.

How it maps to ATT&CK

TECHNIQUE	WHAT NSS SAW
T1583.001 Acquire Infrastructure: Domains	Three domains bought between September and November 2026
T1608.001 Stage Capabilities: Upload Malware	The installer staged on the sender's own portal

T1036 Masquerading	A web page drawn as a Zoom desktop window and a fake update
T1204.002 User Execution: Malicious File	The visitor must download and run the installer
T1219.002 Remote Access Tools: Remote Desktop Software	A remote-support client set to connect to the sender's relay

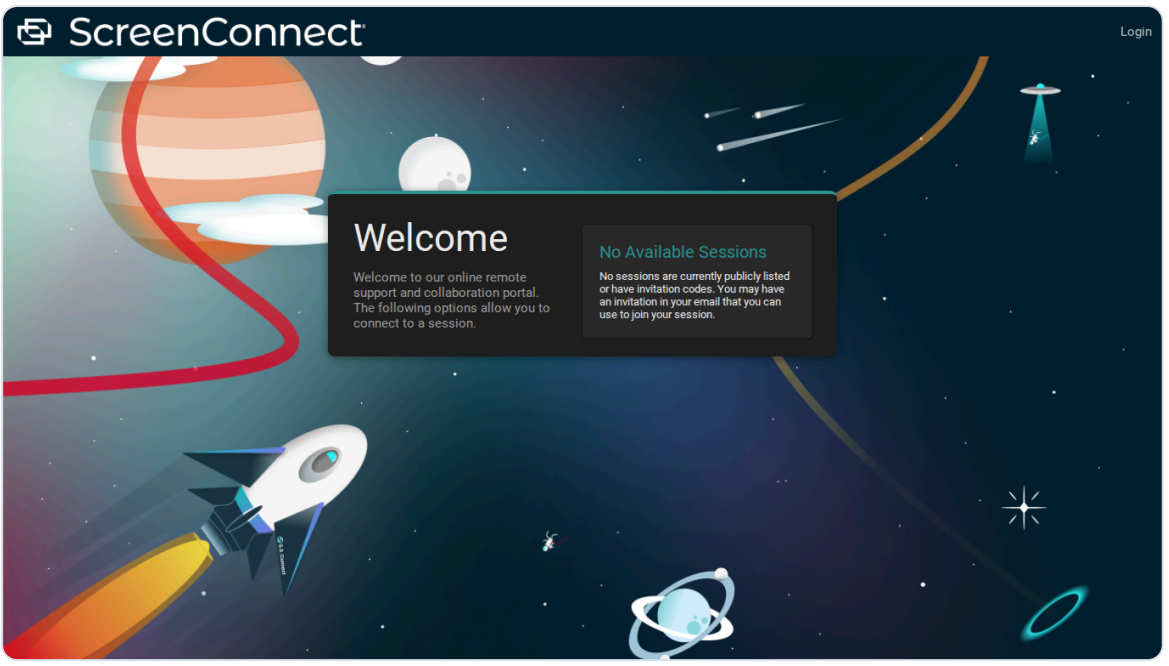
What a defender can look for

In order of how much each one catches:

1. Hunt endpoint records for the SHA-256 above, and for a service named "ScreenConnect Client (230f9b38c3c088fe)".
2. Allow only the remote-support instances your organisation runs. A remote-support client that calls an instance you do not own is the finding, whatever the lure.
3. Alert on outbound connections to port 8041, and to 45[.]87[.]61[.]155 on any port.
4. Block the five names and the installer address in the indicator list at DNS and web proxy.
5. Tell staff that Zoom updates come from the Zoom app or zoom[.]us, never from a page that opens from a meeting link.

Do not block the lure page's own address. It belongs to a shared hosting platform that serves unrelated sites.

All nine indicators are in the CSV and JSON files below, and each one opens as a casefile in NSS Investigate.



The download host is the sender's own remote-access portal: NSS capture of min[.]garincon[.]com, 12 November 2026, 10:01 UTC.

524ff283-2094-4f98-b68d-f24f61c5f8fa.dotinicon.com HIGH RISK verdict stands domain

NSS FOUND THIS OPERATOR ITSELF CONFIRMED NSS-ZM-01

Fake Zoom update page, a separate download portal and a self-hosted remote-access server

found 2026-11-11 1 host 4 domains Hyonix (AS931) fake-software-update, remote-access-delivery, brand-impersonation Not on any list NSS held when it was found.

siblings 45.87.61.155

Watch the whole operator Reports

the platform's own infrastructure register: this host was found and confirmed by NSS analysis

The end of the chain: NSS Investigate on the host the installer connects back to, 12 November 2026. It joins the confirmed operator entry NSS-ZM-01 with its server 45[.]87[.]61[.]155.

FINDINGS (7)

CRITICAL NSS found this itself via 45.87.61.155: confirmed operator NSS-ZM-01 (1 host, 4 domains), first found 2026-11-11 by new-registration hunting, Investigate and capture. Fake Zoom update page, a separate download portal and a self-hosted remote-access server

HIGH The remote-access installer handed out by a page that imitates a brand is set to connect back here (524ff283-2094-4f98-b68d-f24f61c5f8fa.dotinicon.com:8041, called by ScreenConnect.ClientSetup.msi from zoom-0xcdlive-join-00ccxxd.live). Whoever runs this host takes control of each computer that runs the installer, so it is never rated below High risk.

Why: the connect-back host is rated on what the installer does, read from the file itself.

The NSS tools used

> Discovery

> Capture

Took the name from the day's new registrations, resolved it and matched it as a Zoom look-alike with a meeting word beside the brand.

Loaded the page as a desktop, a phone and a crawler, kept the screenshots and the page source, and recorded the installer link.

> Investigate
Built the casefiles: the registry record, certificates and page for each name, and the verdict High risk 70 for the page, both download names, both connect-back names and the server address.

> Probe
Fetched the installer once, took its hashes, read its connect-back setting and deleted it; then checked which ports the server answers on.

> Hunt
Searched NSS's library of past reporting for the same lure and tool: four earlier patterns, and no shared name, address or file.

> Register
Holds the operation as one entry with its names, server and file, so new names that call the same server join it.

Indicators

All 9 indicators. Each is written defanged so it cannot be opened by accident.

INDICATOR	TYPE
`zoom-0xcdlive-join-00ccxxd[.]live`	Domain
`hxxps://min[.]garincon[.]com/Bin/ScreenConnect.ClientSetup.msi`	URL
`min[.]garincon[.]com`	Domain
`garincon[.]com`	Domain

524ff283-2094-4f98-b68d-f24f61c5f8fa[.]dotinicon[.]com	Domain
dotinicon[.]com	Domain
45[.]87[.]61[.]155	IP addre
c98e783442a4ca72244f3bb1d5f8ad28bc1f3f94db8a5afac9597a7c870ca590	File hash
e6142c9c458795d1fea5e18288c1adfb	File hash

DOWNLOAD CSV JSON

How we know

What this rests on

- The page text, link and screenshots are from NSS captures on 12 November 2026 at 04:34 and 09:59 UTC; the portal capture is from 10:01 UTC.
- Registration dates and registrars are public registration records. Certificate dates are from the certificates the servers presented and from public certificate logs.

- The file facts are from one fetch on 12 November 2026 at 13:11 UTC, repeated once with the same hash. The file was read, not run.
- "On no list NSS holds" was checked on 12 November 2026 against every list NSS takes in.

What we cannot say

- NSS did not see how visitors are sent to the page, who received it, or whether anyone ran the installer.
- NSS did not run the installer or watch a session. What it does after it connects is from the product's known behaviour, not observation.
- The page's own wording calls it a demonstration. NSS cannot tell a criminal lure from an authorised test.
- "On no list NSS holds" is not "on no list anywhere".
- This paper is not attributed to any named group.

Use and citation

This paper is marked TLP:CLEAR: it may be shared without restriction. Cite as:

```
Nexus Sentinel Station (NSS), "Fake Zoom update page installs a self-hosted ScreenConnect client: technical analysis", NSS-ZM-01, 12 Nov 2026. https://nsshq.com/research/fake-zoom-update-remote-access
```

See something wrong? corrections@nsshq.com

NSS is not affiliated with Zoom, ScreenConnect, or any registrar, hosting platform or network named in this paper. They are named because the page, the file and the public records name them; nothing here says they knew of or took part in the activity.