ClickFix report: 2026-11-02 – 2026-11-05

What the organization's browsers met on attack pages. Sites count once. Versions are as the sites report them; vulnerabilities are possible, not proven.

What was seen	Sites
A ClickFix lure on the page	
A command put on the clipboard	
The lure read from a smart contract	
A newly registered domain	
A device-code sign-in lure	

Commands, by form

Form	Sites
PowerShell: download and run	12
Reports the visitor, then downloads	9
Obfuscated PowerShell	4
Program to Temp, started	1
ZIP unpacked, program started	1
Network drive over WebDAV	1
Installer to Temp, installed silently	1

Smart contracts behind the lures

Contract	Chain	Sites
0xf70730a4e5b89b6c6e02edaed582ba…	polygon	10
0xb6bc9e1d0b2fb96ab7c47e04cb0be4…	polygon	6
0xb29927b7d854b232d5e58cfc20186…	polygon	4
0xdf132e2893824e26ec8ae8014b4f4f…	bsc	3
0x46790e2ac7f3ca5a7d1bfce312d11e…	bsc	3
0xf4a32588b50a59a82fba148d43608…	bsc	1
0xa1decfb75c8c0ca28c10517ce56b71…	bsc	1
0xb909956b9d716ddfdf6935115a8d6f…	polygon	1

What to do: tell people that no real website asks them to press Windows + R, open Terminal or paste something to prove they are human; stop commands at the paste (ByteMantle replaces a dangerous command on the clipboard); keep the websites you run up to date.