

Forum: [Hack Forums](#)

Thread: [Researchers Expose Phishing Threats Distributing CountLoader and PureRAT](#)

Stanley - October 6, 2025, 5:20 pm

Researchers Expose Phishing Threats Distributing CountLoader and PureRAT

A new campaign has been observed impersonating Ukrainian government agencies in phishing attacks to deliver CountLoader, which is then used to drop Amatera Stealer and PureMiner.

"The phishing emails contain malicious Scalable Vector Graphics (SVG) files designed to trick recipients into opening harmful attachments," Fortinet FortiGuard Labs researcher Yurren Wan said in a report shared with The

<https://thehackernews.com/2025/09/researchers-expose-svg-and-purerat.html>

JoshAllen - October 6, 2025, 5:31 pm

This campaign shows how phishing tactics are evolving. Fileless malware chains are proving that attackers are becoming more creative.

B3A - October 6, 2025, 11:20 pm

These email threats are getting more and more sneaky.

Its crazy how an SVG could end up on a miner/stealer..

always disable auto-open for ZIP/CHM

DAL-SHA - October 7, 2025, 12:53 am

Phishing attacks getting more clever by using fake government emails and tricky files. People need to be more careful opening stuff online??

Fish - October 7, 2025, 1:44 am

(Oct 6, 2025 05:31 PM)Tyler™ Wrote: [\[CITE\]](#) This campaign shows how phishing tactics are evolving. Fileless malware chains are proving that attackers are becoming more creative.

This is very frightening. AI is probably helping people be even more creative

Vectura - October 7, 2025, 1:45 am

That's another reminder of how creative threat actors are getting with delivery methods. Using SVG files in phishing campaigns is clever because they often bypass traditional email filters—many systems don't treat vector graphics as executable threats. Once CountLoader drops payloads like PureRAT or Amatera Stealer, attackers can exfiltrate credentials, system data, or even hijack computing resources for mining. Targeting Ukrainian agencies also suggests geopolitical motivations behind the operation, not just profit. It's a good case study for why email security needs deeper content inspection beyond just file extensions or signatures.

Aeowulf - October 7, 2025, 3:46 am

People are always the weakest link. Don't skimp out on your user training!

Astaroth - October 7, 2025, 3:55 am

I would not call THN the most reliable news source. Something smells like a pig pen about the whole operation. Almost like the whole thing is setup to back up fake claims from the rotten and corrupt authorities in the US.

But hey, that's just me. You don't have to agree. (It rhymed funnily). ?

Ieste - October 7, 2025, 1:56 pm

Phishing using SVG files? Attackers are getting creative.

Oh_Well - October 9, 2025, 4:07 am

Seems like they're trying to milk infected systems long-term.

Props to Fortinet for catching it, but you know this playbook's gonna get reused fast!

Yanix - October 9, 2025, 4:10 am

That's a serious threat, especially with attackers impersonating government agencies. Using SVG files is a clever but dangerous trick. CountLoader and PureRAT sound like a nasty combo. People really need to be extra cautious with email attachments these days.

Oh_Well - October 9, 2025, 4:13 am

(Oct 9, 2025 04:10 AM)Yanix Wrote: [\[CITE\]](#) That's a serious threat, especially with attackers impersonating government agencies. Using SVG files is a clever but dangerous trick. CountLoader and PureRAT sound like a nasty combo. People really need to be extra cautious with email attachments these days.

Classic social engineering with a... very bad payload chain