Custom I2P RAT “I2Parcae” Delivered via Pornographic Customer Support Form Spam

Archived: 2026-04-05 19:43:16 UTC

Author: Kahng An

A customer support contact web form spamming campaign delivering a newly distributed Remote Access Trojan (RAT) was seen a few days ago. Cofense Intelligence is tracking this new malware family as “I2Parcae”. This RAT is notable for having several unique tactics, techniques, and procedures (TTPs), such as Secure Email Gateway (SEG) evasion by proxying emails through legitimate infrastructure, fake CAPTCHAs, abusing hardcoded Windows functionality to hide dropped files, and C2 capabilities over Invisible Internet Project (I2P), a peer-to-peer anonymous network with end-to-end encryption. When infected, I2Parcae is capable of disabling Windows Defender, enumerating Windows Security Accounts Manager (SAM) for accounts/groups, stealing browser cookies, and remote access to infected hosts. As of this report, I2Parcae appears to be delivered via automated spam messages targeting customer support contact forms on multiple websites. The messages deliver an embedded link purporting to be pornography.

I2P Overview

This malware sample is notable for many different reasons, but one of them is using I2P for C2 traffic. I2P, like Tor, is an overlay network that provides anonymous connections. However, Tor is far more popular than I2P. On a technical level, I2P is different from Tor because I2P uses peer-to-peer connections between computers running the I2P software. In contrast, Tor relies on dedicated routing nodes that are different from Tor users. This makes it such that every I2P user is contributing their computer as a node on the network, and simply running the I2P software will generate lots of inbound and outbound I2P traffic from other peers connecting to the hosted node. Additionally, all I2P traffic is end-to-end encrypted by the protocol. Both of these properties make network traffic analysis particularly difficult.

I2P provides hidden service website functionality similar to Tor, and these websites (called “eepsites”) can be identified with the .i2p top-level domain. While eepsites can have human-readable domain names, the most basic and likely most common form of domain name uses a Base32 encoding of the eepsite’s public key hash. For example, “2lyi6mgj6tn4eexl6gwnujwfycmq7dcus2x42petanvpwpjlqrhq[.]b32[.]i2p” was an eepsite used by this malware sample.

Campaign Characteristics

The campaign targets various customer support contact forms to deliver an email containing the message submitted in the form. This tactic effectively allows the threat actor to send their message with malicious content using legitimate web or email server infrastructure owned by the potential victim. This tactic will also bypass many SEGs because the email originates from legitimate infrastructure. From the samples analyzed by Cofense Intelligence, this tactic allowed these messages to bypass Cisco IronPort and Proofpoint.

Figure 1 shows an example of one of the emails. The exact structure of the email will vary depending on the contact form system used, but it will generally include a short message and a link to a site purporting to have pornographic material.

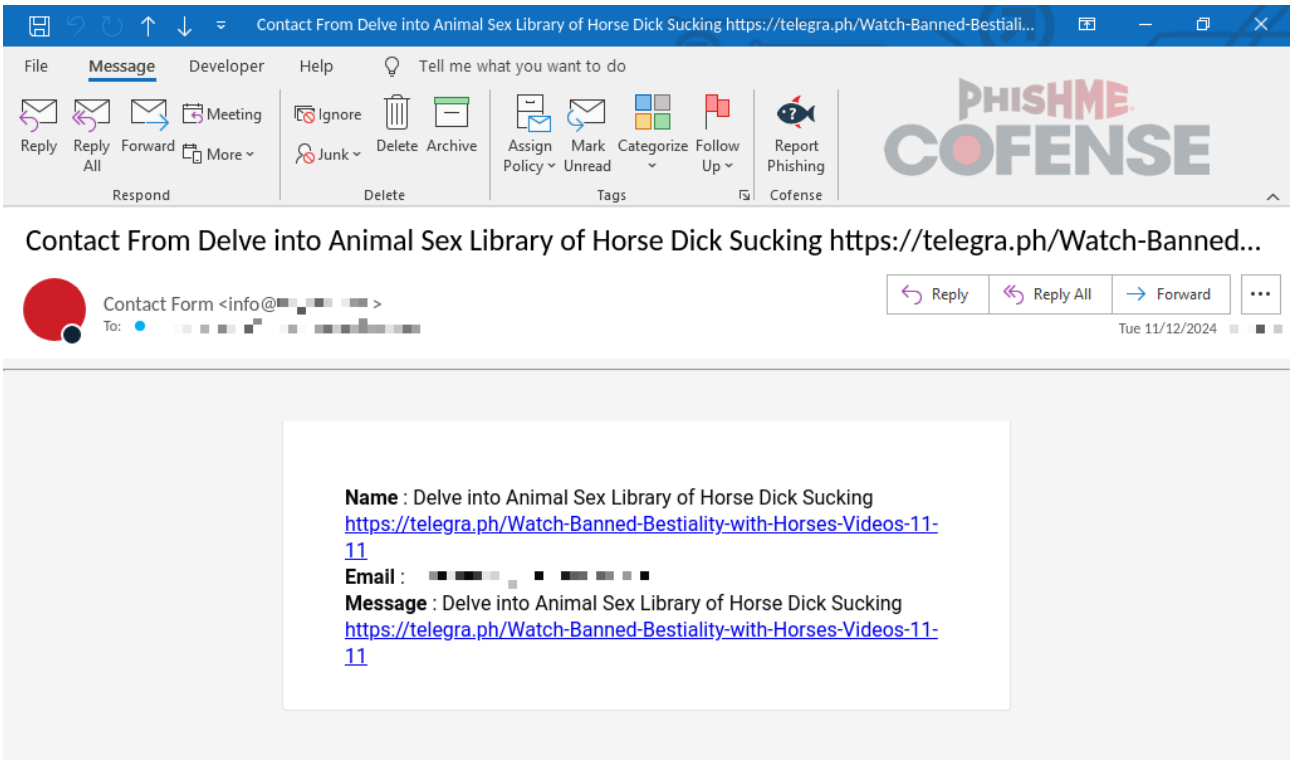

Figure 1: The initial email was sent via a customer support contact form.

Upon clicking on the link, victims are brought to a page purporting to contain a link to the pornography, as shown in Figure 2.

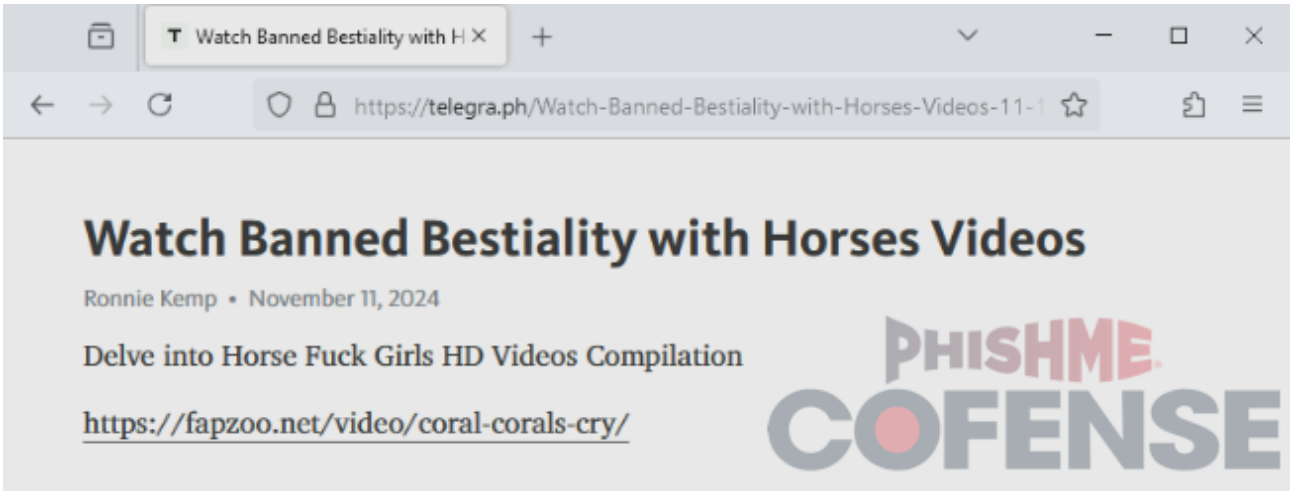

Figure 2: Landing page of the embedded link from the email.

The embedded link on this site is notable because it links to porn-zoo[.]sbs instead of displayed URL. The real embedded link will redirect victims to a fake CAPCHTA page that asks the victim to run a script that has been

copied to their clipboard, which can be seen in Figure 3. This redirect seems to only work on Chromium-based browsers, and users with other browsers will be redirected to a pornographic site.

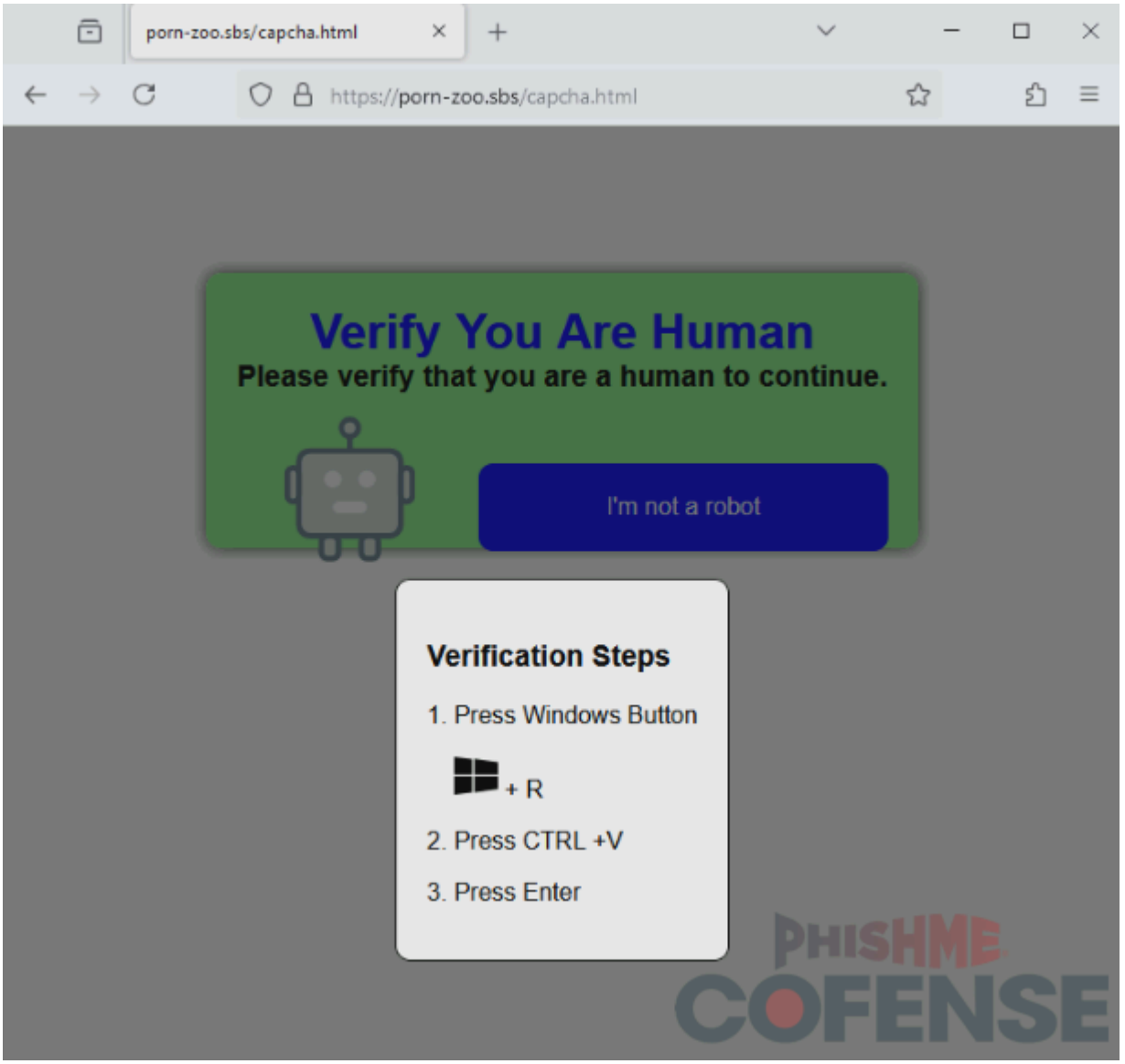

Figure 3: A fake CAPTCHA site that automatically copies a malicious script into the victim's clipboard for the victim to run.

I2Parcae is downloaded and executed on the victim's machine upon running the malicious script. After the malware is installed, the script will open a browser window to a pornographic site, misleading victims into thinking the script was a legitimate CAPTCHA to access the site.

Malware Capabilities

I2Parcae is particularly stealthy with its capabilities. After the malicious script is run by the victim, I2Parcae will disable Windows Defender, create a Windows Defender exclusion for "%HOMEDRIVE%\Users\", and create a folder named "Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}" in C:\Users\Public\. This is notable because "{20d04fe0-3aea-1069-a2d8-08002b30309d}" is a hardcoded link to the "My PC" page in the built-in Windows File Explorer. Attempting to navigate to a folder named that using Windows File Explorer will simply

direct the user to the “My PC” page. However, I2Parcae uses this folder to drop various malicious DLLs, configuration files, scheduled tasks, and an I2P installation package.

I2Parcae creates two scheduled tasks, coomgr and sesctl, that run correspondingly named executables at system start. The exact capabilities and purpose of these two executables are unknown, but the debug logs suggest that coomgr.exe is used for accessing web browser data and sesctl.exe is used for accessing system information.

I2Parcae’s main payload is simply named main.exe and appears to use various DLL modules, all of which generate robust and in-depth logs. The most notable module, and the one that provides the most logging, is cnccli.dll, which appears to be the C2 module. Its corresponding configuration file appears to contain two C2 addresses: an I2P address and a regular IPv4 address and port. Other modules appear to include capabilities to enumerate Microsoft SAM accounts and groups (samctl.dll), enumerate installed programs (prgmgr.log), and make connections to other hosts via Windows Remote Desktop Services (rdpctl.log). The main payload listens on localhost over port 41673, which is used by the various modules for communication.
