Images, OCR, and Logos:
Seeing the Full Picture

As the saying goes, "an image is worth a thousand words." Screenshots and photos of internal systems, phishing kits, stolen credit cards and IDs wallpaper underground forums and marketplaces as threat actors seek to verify their wares or boast about their successes.

Images are rich with information that can be leveraged to protect your organization from threats such as fraud, phishing, access for sale, stolen data, and PII. That's where Intel 471's Images, OCR, and Logos functionality (IOL) comes in, ensuring you see the full picture. All you need to do is turn it on!

Use IOL to Identify Images of:

- Stolen credit cards
- Compromised accounts
- Checks
- Phishing kits
- Screenshots of internal systems
- Access badges
- Scans of IDs such as passports, driving licenses
- Exploit code

…..And much more

What Does IOL Deliver?

Each part of the IOL functionality enhances the detection and mitigation of threats such as fraud, phishing and stolen data.

Images – TITAN displays the invaluable images that we've collected from forums and Instant Messages. Gain further contextualization of the image and insight into the mind of the threat actor sharing it.

Optical Character Recognition (OCR) – Any text present within the image will be recognised and stored alongside the image to be returned in watchers and searches. This means you can instantly inspect and identify images of relevance, such as screenshots of a compromised system bearing your organization's name etc, to enhance research or take action to alleviate risk.

Logos – Going beyond text, our AI-based logo recognition will identify your logo within an image, even if it's rotated, distorted. These results will also be stored with the image and returned in watchers and searches. Receive near real-time alerts to track and disrupt where your logo's been used without your knowledge.

sales@intel471.com

How will it help me?

- Detect and mitigate against threats including fraud, phishing, access for sale, stolen data, PII.
- The threat actor shared the image for a reason. Access this enriched contextualization of image and actor for your own research and escalation processes.
- Get ahead of threat actors by setting up watchers to be alerted in near real-time upon the discovery of images relevant to your organization.
- Search for logos and text within images on TITAN, and pivot to related data to enhance research.
- Track where your logo is being used without your knowledge to prevent it from legitimizing fraud and impairing your brand's hard earned reputation.

Opt In and Don't Miss Out

- This IOL functionality is not enabled by default. To opt in, all you need to do is accept the terms within TITAN.
- Intel 471 strives to keep our stakeholders safe, so we've developed an extensive filtering process to help remove any objectionable material (nudity, violence, et al) before it reaches you. We also allow you to flag any potentially objectionable images for review.
- Share your logos with your Intel 471 contact, and these will be added to our solution to train our logo recognition function to deliver the most accurate alerts of potentially nefarious use of your brand.

Turn on IOL in 4 Simple Steps

1. When logged into TITAN, click your user name.
2. Select 'Profile' from the dropdown menu.
3. Read the agreement, and click 'I Agree'.
4. Select 'Home' to return to the dashboard.

sales@intel471.com