Name : Raj Shedge

Intern_Id:170

Tool Name:

Generated Photos

Description:

Generated Photos is an AI-powered tool that creates entirely fake but realistic human faces. These are synthetic images generated using neural networks and are royalty-free, ideal for UI/UX design, training datasets, and anonymized avatars.

What Is This Tool About?

This tool uses Generative Adversarial Networks (GANs) to create human-like faces that do not belong to real individuals, avoiding privacy issues and enabling safe synthetic data usage.

Key Characteristics / Features:

1. AI-generated, fake but realistic human faces
2. No real person used or represented
3. Royalty-free usage
4. Custom filters: age, gender, ethnicity
5. Expression & emotion control
6. StyleMatch: find similar faces
7. FaceMix: mix two faces
8. High-quality resolution images
9. Random face generator
10. API for automation and apps

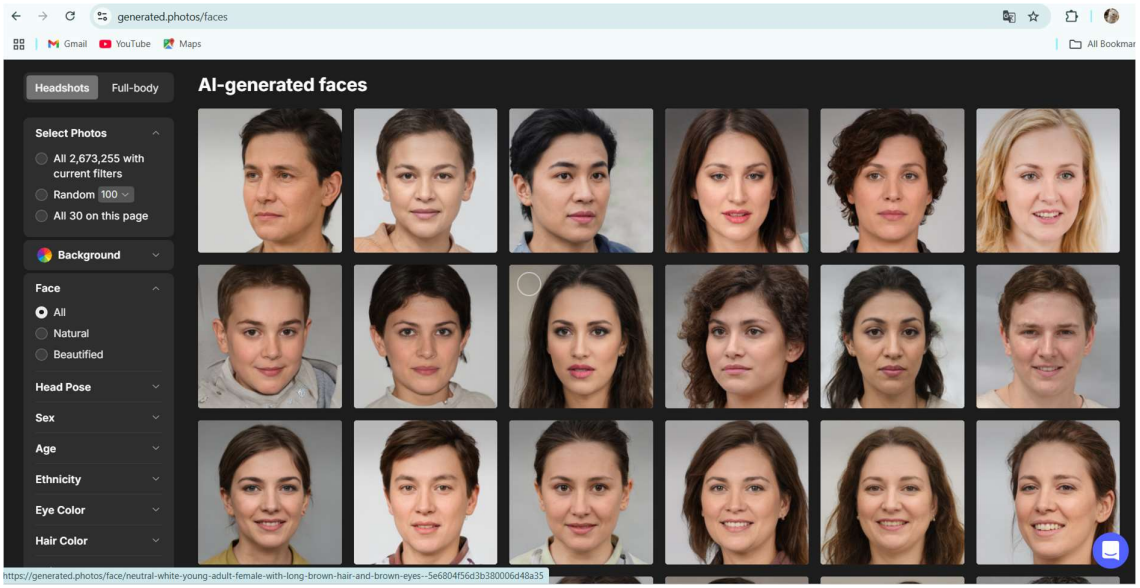
Types / Modules Available:

- Face Generator
- StyleMatch Tool
- FaceMix Tool
- Developer API

How Will This Tool Help?

- Enables UI testing with anonymized faces
- Useful in creating deepfake detection models
- Avoids legal/privacy issues
- Supports diversity testing in face recognition tools

PoC Images:



15-Liner Summary:

1. 100% fake human faces
2. Ethically safe and private
3. AI/GAN based
4. Emotion/age filters
5. API for dev use
6. Style matching available
7. High-res image output
8. Realistic details
9. Consistent lighting and pose
10. No copyright issues
11. Good for deepfake training

12. Good for UI avatars
13. Can be embedded in apps
14. No installation needed
15. Supports diverse datasets

Time to Use / Best Case Scenarios:

- Deepfake dataset preparation
- Privacy-safe design testing
- Face recognition model testing
- Avatar creation

When to Use During Investigation:

- Simulating fake profiles in OSINT
- Forensics model training
- Red teaming for social engineering

Best Person to Use & Required Skills:

- Red teamers, UI designers, researchers
- Basic web and API knowledge

Flaws / Suggestions:

- No dynamic head angle generation
- Requires payment for full access
- Faces can look repetitive in style

Good About the Tool:

- Realistic faces
- Fully synthetic
- Accessible via browser

Tool Name:

ThreatMon Reports (Using CISA Report as Reference)

Description:

ThreatMon offers threat intelligence reports detailing malware campaigns, APT activities, and Indicators of Compromise. Due to access restriction, this PoC uses a public CISA report as a substitute.

What Is This Tool About?

The goal is to give analysts real-time insights into ongoing threat activity, including attacker TTPs, campaign details, and MITRE ATT&CK mapping.

Key Characteristics / Features:

1. Threat activity analysis
2. APT & malware report summaries
3. IOC lists: IPs, domains, hashes
4. Tactics & techniques (MITRE ATT&CK)
5. PDF format with visual aids
6. Indicators useful for blue teams
7. Used in SOC environments
8. Daily/weekly updates
9. Global scope coverage

10. Actionable threat mitigation tips

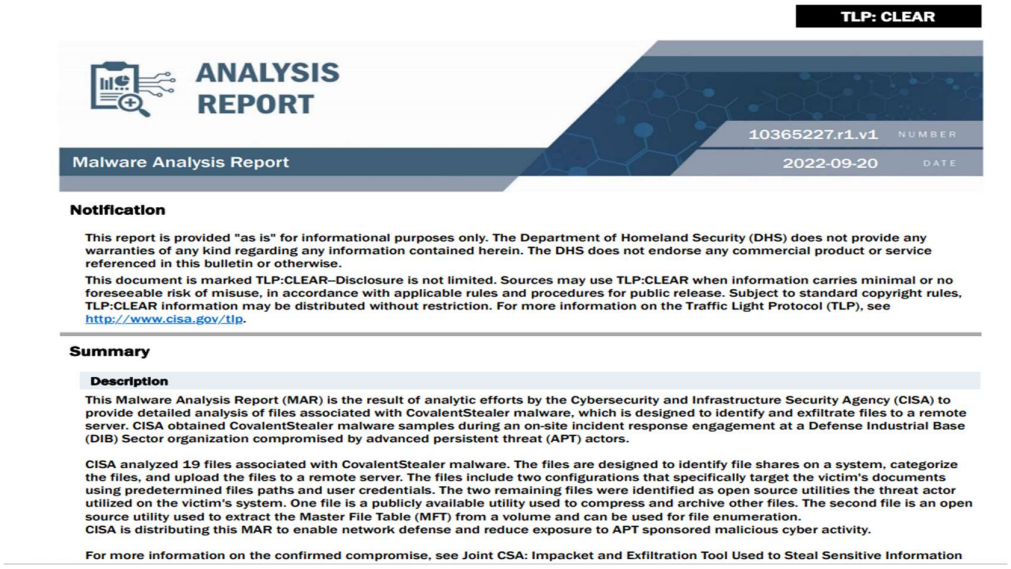
Types / Modules Available:

- Report Feed
- Campaign Analysis
- IOC Section
- MITRE ATT&CK Section

How Will This Tool Help?

- Helps identify active threats
- Maps adversary behavior
- Improves incident response speed
- Helps write detection rules

PoC Images:



TLP: CLEAR

ANALYSIS REPORT

Malware Analysis Report

10365227.r1.v1 NUMBER

2022-09-20 DATE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:CLEAR–Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA) to provide detailed analysis of files associated with CovalentStealer malware, which is designed to identify and exfiltrate files to a remote server. CISA obtained CovalentStealer malware samples during an on-site incident response engagement at a Defense Industrial Base (DIB) Sector organization compromised by advanced persistent threat (APT) actors.

CISA analyzed 19 files associated with CovalentStealer malware. The files are designed to identify file shares on a system, categorize the files, and upload the files to a remote server. The files include two configurations that specifically target the victim's documents using predetermined files paths and user credentials. The two remaining files were identified as open source utilities the threat actor utilized on the victim's system. One file is a publicly available utility used to compress and archive other files. The second file is an open source utility used to extract the Master File Table (MFT) from a volume and can be used for file enumeration.
CISA is distributing this MAR to enable network defense and reduce exposure to APT sponsored malicious cyber activity.

For more information on the confirmed compromise, see Joint CSA: Impacket and Exfiltration Tool Used to Steal Sensitive Information

Product Version 1.0.0.0

PE Sections

MD5	Name	Raw Size	Entropy
6b81a95076cc3d6f6dff7d32afa3b7e2	header	512	2.297287
2d3081eb51c7c393e0a670c8bfcf7c24	.text	788992	7.998126
5569bca67ba8c174f30990c07b585dbe	.rsrc	1536	3.966404

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

84164e1e80...	Used	91a8b31c126a021f5c156742016acdcca7d83 eac4b583bae5d4fd0a85a96813b
84164e1e80...	Created	517faa4a0666ec68842f256f08d987935b6ce 9ef64e33f027e084e8f45b9366d

Description

This file has been identified as CovalentStealer malware. The actor utilized code from several open source projects, including ClientUploader. The retained the internal name "ClientUploader.exe". The program is a file management system that is capable of uploading files to the Internet.

When the program is executed, it will spawn an instance of itself in memory called 'koi'. This instance accesses several embedded resources that it uses to locate and manipulate files on the system. The following is a list of the primary embedded resources:

—Begin Embedded Resources—
BaseNetwork – This resource is used to create sessions and establish connections to the server.
FileContainer – This resource is used to access file shares via Server Message Block (SMB). It is also used to enumerate files and directories and sort them by Message Digest 5 (MD5) hash. It maintains Internet Protocol (IP) addresses, logins, domain names, passwords, and paths for shares on the network.
IFileWorker – This resource is a file management program that is capable of moving and categorizing files. It contains compression libraries for Gzip and Brotli, as well as a file blacklist.
Encryption – This resource handles file encryption, decryption and secure communications. It decrypts the configuration file, onedrv.ini (91a8b31c126a021f5c156742016acdcca7d83eac4b583bae5d4fd0a85a96813b) using the hard-coded Advanced Encryption Standard (AES) key 'M(xcHq88q[s=pc7^+u_Gb_]JC%QQwP:h' and an Initialization Vector (IV) using the first half of the AES key (See Figure 1).
OneDriveClient – This resource targets a user's OneDrive account and creates an upload session to send the files to a remote server. It is able to access files in the victim's OneDrive by unique ID (See Figure 2). Files are uploaded to a Microsoft Azure client identified in the configuration file onedrv.ini by client ID.
—End Embedded Resources—

The program runs a debugging routine and will output debugging data to a file with the same name as the malware and with the .dat extension, e.g. onedrv.dat (517faa4a0666ec68842f256f08d987935b6ce9ef64e33f027e084e8f45b9366d).

Screenshots

Figure 1 - This is the AES encryption routine. The routine uses the hard-coded string 'M(xcHq88q[s=pc7^+u_Gb_]JC%QQwP:h' as the AES key and the first half of the key as the IV.

15-Liner Summary:

1. Real-time threat info
2. Public IOC sharing
3. Adversary behavior breakdown
4. MITRE technique reference
5. Public agency trusted reports
6. Help for SOC teams
7. Malware/trojan analysis
8. C2 infra exposure
9. Report-based threat hunting
10. Good visuals and layout
11. Policy-level input possible
12. Easy to understand
13. Useful for training
14. Works well as reference intel

15. Available freely online

Time to Use / Best Case Scenarios:

- After malware attack
- In threat correlation
- Daily SOC briefings
- For IOC feed to SIEM

When to Use During Investigation:

- To enrich IOC database
- To understand attack patterns
- To trace back threat origin

Best Person to Use & Required Skills:

- SOC Analyst, Threat Hunter, Incident Responder
- Knowledge of MITRE, malware, IOCs

Flaws / Suggestions:

- ThreatMon access limited to business email
- Reports not downloadable for students
- No real-time dashboard on free access

Good About the Tool:

- High quality intel
- Public agency source (CISA)
- Trusted and legal to use
- Covers full threat lifecycle

Note: ThreatMon report access was restricted due to student email limitations. The CISA public threat intelligence report was used as a substitute to demonstrate functionality and structure.

Conclusion:

Both tools assigned in this PoC — *Generated Photos* and *ThreatMon (via CISA)* — offer distinct yet important capabilities in the cybersecurity and digital investigation landscape. Generated Photos provides synthetic, privacy-safe face generation suitable for anonymous testing and red teaming. Meanwhile, ThreatMon (demonstrated via CISA reports) highlights the value of actionable threat intelligence for blue teams, SOC analysts, and digital forensics professionals. Despite access limitations, viable substitutes and open-source resources can be effectively used to showcase and understand tool functionality, preserving the learning and implementation goals of cybersecurity internships and investigations.