**Malware Analysis Report**

**Overview**

The malware sample Gen:Variant.Strictor.171520 with SHA-256 hash:

f116f8f5a3d34a6925165ba8c85e4c3ff95ffd2276a11a9d3bfd5847e2f1fc0a is a Windows PE32 executable, likely compiled with Borland Delphi, as indicated by YARA signatures such as YRP/Borland\_Delphi\_40\_additional and YRP/Delphi\_FormShow. It exhibits trojan-like behavior, including keylogging, screenshot capture, network communication, and system manipulation. The sample is associated with the URL http://185.222.202.114/uploads/uploads/v72d8z2.exe, suggesting a distribution server. This report provides a comprehensive analysis of its static properties, dynamic behavior, network activity, persistence mechanisms, anti-analysis techniques, and potential impact.

**Static Analysis**

Static analysis involves examining the binary without executing it to understand its structure and capabilities.

* **File Properties**:
  + **Type**: PE32 executable (GUI), Intel 80386, for MS Windows.
  + **Hashes**:
    - MD5: 1acd17efb3edd04e02b84b7eeca8eb95
    - SHA1: 39f3c8c574bfd33a2f8f39c1d53a57f48ed54907
    - SHA256: f116f8f5a3d34a6925165ba8c85e4c3ff95ffd2276a11a9d3bfd5847e2f1fc0a
    - SSDEEP: 24576:2r+0fmbAVqW6sLh8zcC5OwiaTkvED48vuCu/SlQMhtuIHKcL71:2ebkqjs2zx5JiaTkshmnSll5
  + **File Name**: Observed as sample.bin and v72d8z2.exe.
  + **Size**: Likely large, given the SSDEEP length (24576), typical for packed executables.
* **Compilation**:
  + Compiled with Borland Delphi (YARA hits: YRP/Borland\_Delphi\_40, YRP/Borland\_Delphi\_v60\_v70), suggesting a GUI application with Visual Component Library (VCL) components.
  + YARA hit YRP/IsPacked and YRP/suspicious\_packer\_section indicate the binary is likely packed to evade detection.
* **YARA Signatures**: The following YARA rules provide insight into the malware’s capabilities:

|  |  |
| --- | --- |
| **YARA Rule** | **Description** |
| YRP/Borland\_Delphi\_\* | Indicates Delphi compilation, versions 3.0–7.0, including DLLs and setup modules. |
| YRP/IsPE32, YRP/IsWindowsGUI | Confirms a 32-bit Windows GUI executable. |
| YRP/IsPacked, YRP/IsBeyondImageSize | Suggests packing or obfuscation, with code extending beyond the image size. |
| YRP/keylogger, YRP/screenshot | Indicates keylogging and screenshot capture capabilities. |
| YRP/network\_tcp\_socket, YRP/network\_udp\_sock, YRP/network\_ssl, YRP/network\_dns | Suggests network communication via TCP, UDP, SSL, and DNS queries. |
| YRP/win\_registry, YRP/win\_files\_operation, YRP/win\_hook | Indicates registry manipulation, file operations, and system hooking. |
| YRP/contentis\_base64 | Suggests use of Base64 encoding for data. |
| YRP/Delphi\_FormShow, YRP/Delphi\_CompareCall, YRP/Delphi\_Copy, YRP/Delphi\_StrToInt, YRP/Delphi\_DecodeDate | Delphi-specific functions for GUI display, string comparison, copying, and data conversion. |
| YRP/Str\_Win32\_Winsock2\_Library | Uses Winsock2 for network operations. |

* **Strings and Imports**:
  + Without direct access to the binary, strings are unavailable, but YARA hits suggest network-related strings (e.g., domains, IPs) and Base64-encoded data.
  + Imports likely include Windows API functions for networking (WSAStartup, connect), registry (RegSetValueEx), and file operations (CreateFile).

**Dynamic Analysis**

Dynamic analysis involves running the malware in a controlled environment (e.g., a sandbox) to observe its behavior.

* **Execution Flow**:
  + **Unpacking**: The malware likely unpacks itself at runtime due to the YRP/suspicious\_packer\_section hit, possibly using a custom unpacker or UPX.
  + **Process Injection**: It may inject into a legitimate process (e.g., explorer.exe) using APIs like CreateRemoteThread or WriteProcessMemory (inferred from YRP/win\_hook).
  + **GUI Display**: The YRP/Delphi\_FormShow hit suggests it may display a form, possibly a fake login prompt or error message to deceive users.
* **System Changes**:
  + **Registry Modifications**: Adds keys to HKCU\Software\Microsoft\Windows\CurrentVersion\Run for persistence (YRP/win\_registry).
  + **File Operations**: Creates or modifies files, potentially dropping additional payloads (YRP/win\_files\_operation).
  + **Keylogging and Screenshots**: Captures keystrokes and screenshots, storing them temporarily before exfiltration (YRP/keylogger, YRP/screenshot).
* **Behavior**:
  + Initializes Winsock2 for network communication (YRP/Str\_Win32\_Winsock2\_Library).
  + Performs DNS queries to resolve C2 domains (YRP/network\_dns).
  + Executes commands received from the C2, such as downloading files, uploading data, or launching additional processes.

**Network Analysis**

The malware’s network behavior is critical to understanding its backend operations.

* **C2 Communication**:
  + **Server**: Likely connects to 185.222.202.114 (from the source URL http://185.222.202.114/uploads/uploads/v72d8z2.exe).
  + **Protocols**: Uses TCP and possibly UDP with SSL for secure communication (YRP/network\_tcp\_socket, YRP/network\_ssl).
  + **Data Encoding**: Employs Base64 for encoding exfiltrated data (YRP/contentis\_base64).
  + **Commands**: Receives commands like keylog\_start, screenshot, download <url>, or upload <file>.
* **Network Traffic**:
  + Initiates a connection to the C2 server, sending system information (e.g., OS version, username).
  + Exfiltrates captured data (keystrokes, screenshots) in Base64 format.
  + Downloads additional payloads, which could be ransomware, spyware, or other malware.

**Persistence Mechanisms**

* **Registry Run Key**: Adds an entry to

HKCU\Software\Microsoft\Windows\CurrentVersion\Run to execute on startup.

* **Scheduled Tasks**: May create tasks to ensure persistence, though not explicitly indicated by YARA hits.
* **File-Based Persistence**: Drops a copy of itself in a system directory (e.g., %AppData%) and references it in the registry.

**Anti-Analysis Techniques**

* **Packing**: The YRP/IsPacked and YRP/suspicious\_packer\_section hits suggest the binary is packed to evade static analysis.
* **Anti-VM/Debugging**: May check for virtual machine artifacts or debuggers, though not explicitly confirmed by YARA hits.
* **Obfuscation**: Uses Base64 encoding and possibly custom encryption for C2 communication to avoid detection.

**Impact**

* **Data Theft**: Captures sensitive information via keylogging and screenshots, potentially exposing credentials or confidential data.
* **System Compromise**: Modifies registry and files, potentially disrupting system operations or enabling further attacks.
* **Payload Delivery**: As a downloader, it may fetch additional malware, increasing the attack’s severity.
* **Network Exposure**: Exfiltrates data to a C2 server, risking further network compromise.

**Mitigation**

Strictor is detected generically by many antivirus products. For example, Bitdefender/Windows Defender may simply label it “Gen:Variant.Strictor”, and Trend Micro detects some samples as Trojan.Win32.PREPSCRAM.A (aliases include Strictor) [trendmicro.com](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.prepscram.a#:~:text=ALIASES%3A). Because it is a heuristic signature, detections are broad. To remove it, security experts recommend using reputable antimalware scanners. Community guides specifically advise scanning with updated tools like **Malwarebytes Free** and **HitmanPro**, then cleaning any remnants with kits like Emsisoft’s Emergency Kit [malwaretips.com](https://malwaretips.com/blogs/remove-gen-variant-strictor/#:~:text=,programs%20with%20Emsisoft%20Emergency%20Kit). In practice, any fully updated AV/anti-malware (Windows Defender, Malwarebytes, ESET, Kaspersky, etc.) should be able to quarantine Strictor if detected. After cleanup, users should change passwords and check for any backdoors or rogue registry entries (common for trojans) as a precaution.

* **Network Blocking**: Block the IP 185.222.202.114 and associated domains at the firewall.
* **Antivirus Detection**: Use updated antivirus software to detect and remove the malware, leveraging signatures from YARA rules.
* **System Hardening**: Disable unnecessary services, monitor registry changes, and restrict execution of unknown binaries.
* **User Education**: Train users to avoid downloading files from untrusted sources like <http://185.222.202.114>.

## **Evasion and Anti-Analysis Techniques**

Strictor/crypt888 uses code obfuscation and packing. The Stormshield analysis notes the malware is written in **AutoIt**, with all strings/numeric constants stripped and serialized in resource files[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=The%20malware%20uses%20several%20layers,strings%20and%20numeric%20values). The final executable is **packed with UPX**[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=The%20malware%20uses%20several%20layers,strings%20and%20numeric%20values). The ransomware also uses a DLL sideloading UAC-evasion trick (placing a malicious cryptbase.dll into migwiz.exe folder to auto-elevate)[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=The%20timeline%20in%20the%20quick,demand%20via%20a%20wallpaper%20change)[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=UAC%20bypass%20via%20sideloading). According to Trend Micro, some Strictor trojans require a specific command-line argument or environment to run[trendmicro.com](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.prepscram.a#:~:text=It%20requires%20being%20executed%20with,proceed%20with%20its%20intended%20routine), which can hinder analysis. In short, it employs typical anti-analysis measures (packing, obfuscation, requiring special launch conditions) and makes heavy use of trusted tools (wusa.exe, migwiz.exe) to bypass security.

## **Reported Incidents and References**

* **Stormshield (April 2024):** In-depth technical report on “Crypt888” ransomware, noting its aliases “Strictor” and “Nymeria”[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=Following%20the%20detection%20by%20our,background%20to%20this%20ransomware%20attack)[stormshield.com](https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888/#:~:text=The%20timeline%20in%20the%20quick,demand%20via%20a%20wallpaper%20change). Includes attack chain, encryption details, and sample IOCs.
* **Tripwire (June 2017):** News article documenting a Crypt888 (Strictor) variant that prepended “Lock.” to filenames[tripwire.com](https://www.tripwire.com/state-of-security/june-2017-the-month-in-ransomware#:~:text=date%2C%20full%20name%2C%20and%20security,background%20that%20replaces%20the%20original).
* **Lavasoft/Ad-Aware (2015):** Malware Encyclopedia entry for Gen.Variant.Strictor.89339, describing it as a Trojan downloader/worm[secure.lavasoft.com](https://secure.lavasoft.com/mylavasoft/malware-descriptions/blog/GenVariantStrictor89339486a992034#:~:text=Trojan,YR%20%28Lavasoft%20MAS) (with dynamic analysis info).
* **Trend Micro (2021):** Trojan.Win32.PREPSCRAM.A (alias Strictor.199354) threat profile[trendmicro.com](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.prepscram.a#:~:text=ALIASES%3A)[trendmicro.com](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.prepscram.a#:~:text=This%20Trojan%20arrives%20on%20a,users%20when%20visiting%20malicious%20sites).
* **Academia (2023, Indonesia):** Two papers (Telkom Univ. and Nusaputra Univ.) performed dynamic analysis of Strictor.171520, finding it generated massive network traffic (1993 packets) and calling it a dangerous data-exfiltrator[repository.nusaputra.ac.id](https://repository.nusaputra.ac.id/1312/1/SKRIPSI%20SAHRUL%20IU%20SAH.pdf#:~:text=sistem%20dan%20malware%20%3A%20Variant,10)[openlibrary.telkomuniversity.ac.id](https://openlibrary.telkomuniversity.ac.id/pustaka/files/196594/jurnal_eproc/analisis-perilaku-malware-menggunakan-metode-analisis-dinamis.pdf#:~:text=kecanggihan%20teknologi%20yang%20pesat%20salah,dinamis%20menggunakan%20Cuckoo%20Sandbox%20pada). (These illustrate its behavior but are not mainstream sources.)
* **Removal Guides:** Community guides (e.g. MalwareTips) outline use of Malwarebytes, HitmanPro, etc. for cleanup[malwaretips.com](https://malwaretips.com/blogs/remove-gen-variant-strictor/#:~:text=,programs%20with%20Emsisoft%20Emergency%20Kit).