1. Các công cụ, môi trường scan phổ biến

|  |  |
| --- | --- |
|  | ransomeware.exe |
| BKAV | pass |
| Antivirus | pass |
| Window Defender | pass |
| Virustotal | 9/73 security vendors flagged   * Trojan.Win32.Save.a * Static AI - Suspicious PE * W64.AIDetectMalware * Malicious * BehavesLike.Win64.Downloader.vc * Malicious (high Confidence) * RiskWare/Win32.Kryptik.a * Win/malicious\_confidence\_90% (D) * Trojan.Agent.Win32.3991781 |

* Ransomeware.exe (Python + PyInstaller):
  + Đây là mã độc Python đã được đóng gói thành tệp thực thi bằng PyInstaller.
  + Phần lớn các phần mềm diệt virus như VirusTotal phát hiện ra tệp này dựa trên dấu hiệu của mã độc và dấu hiệu nhận biết của PyInstaller. Nó được nhận diện với các tên như Gen.Giant.Mikey.28, RiskWare/Win32.Kryptik.a, và Trojan.Giant.Mikey.28.
  + Điều này cho thấy rằng mã độc này đã bị phát hiện bởi các công cụ diệt virus dưới nhiều biến thể khác nhau, nhưng không có yếu tố bổ sung nào để lừa người dùng ngoài việc là một mã độc đơn giản.

Dưới đây là nhận xét chi tiết về từng loại mã độc được phát hiện và lý do tại sao chúng bị phát hiện:

* Nhận xét về các mã độc sau: Trojan.Win32.Save.a, Static AI - Suspicious PE, W64.AIDetectMalware, Malicious, BehavesLike.Win64.Downloader.vc, Malicious (high Confidence)

Nguyên nhân xuất hiện các flag này là sử dụng PyInstall đóng gói file python. Một hành động đóng 1 file thành file thực thi được coi là một dấu hiệu bất thường. Các công cụ scan đã xếp nó vào false positive.

**Dương tính giả** (hay còn được viết là *false positive* hoặc F/P) là một thuật ngữ thường được sử dụng trong an ninh mạng để chỉ việc một tập tin hoặc cài đặt bị phát hiện là mã độc khi thực tế nó không phải.

Trong thống kê, dương tính giả được gọi là **lỗi loại I**, do hệ thống kiểm tra một điều kiện cụ thể và đưa ra quyết định dương tính sai (khẳng định sai). Ngược lại với dương tính giả là **âm tính giả** (lỗi loại II), khi hệ thống kiểm tra một điều kiện không đúng trong khi thực tế nó lại đúng. Trong bài viết này, chúng ta sẽ tập trung vào dương tính giả trong lĩnh vực an ninh mạng. Tuy nhiên, cần lưu ý rằng âm tính giả trong lĩnh vực này thường được gọi là “bỏ sót” (*misses*), tức là những tập tin hoặc hành vi mã độc mà phần mềm bảo vệ không phát hiện ra.

**Các nguyên nhân có thể gây ra dương tính giả**

Những nguyên nhân phổ biến nhất của dương tính giả bao gồm:

1. **Heuristic**: Các quyết định được đưa ra dựa trên những mảnh thông tin tối thiểu.
2. **Phân tích hành vi**: Các quyết định dựa trên hành vi, và tập tin hợp pháp thể hiện hành vi mà thường được coi là độc hại.
3. **Học máy**: Đôi khi ta gặp tình huống “rác vào thì rác ra” (*garbage in, garbage out*), hay nói một cách lịch sự hơn, “quá trình huấn luyện không tính đến một số tình huống nhất định.”

**Học máy** được thực hiện bằng cách cung cấp cho hệ thống một lượng lớn dữ liệu huấn luyện. Những sai sót hoặc không rõ ràng trong dữ liệu huấn luyện có thể dẫn đến các lỗi phát hiện.

Việc thiết kế các quy tắc phát hiện cho những tập tin hoặc hành vi mã độc chưa biết luôn là sự cân bằng giữa việc cố gắng bao phủ kết quả đúng càng nhiều càng tốt mà không kích hoạt bất kỳ dương tính giả nào. Tuy nhiên, việc này đôi khi có thể xảy ra sai sót.

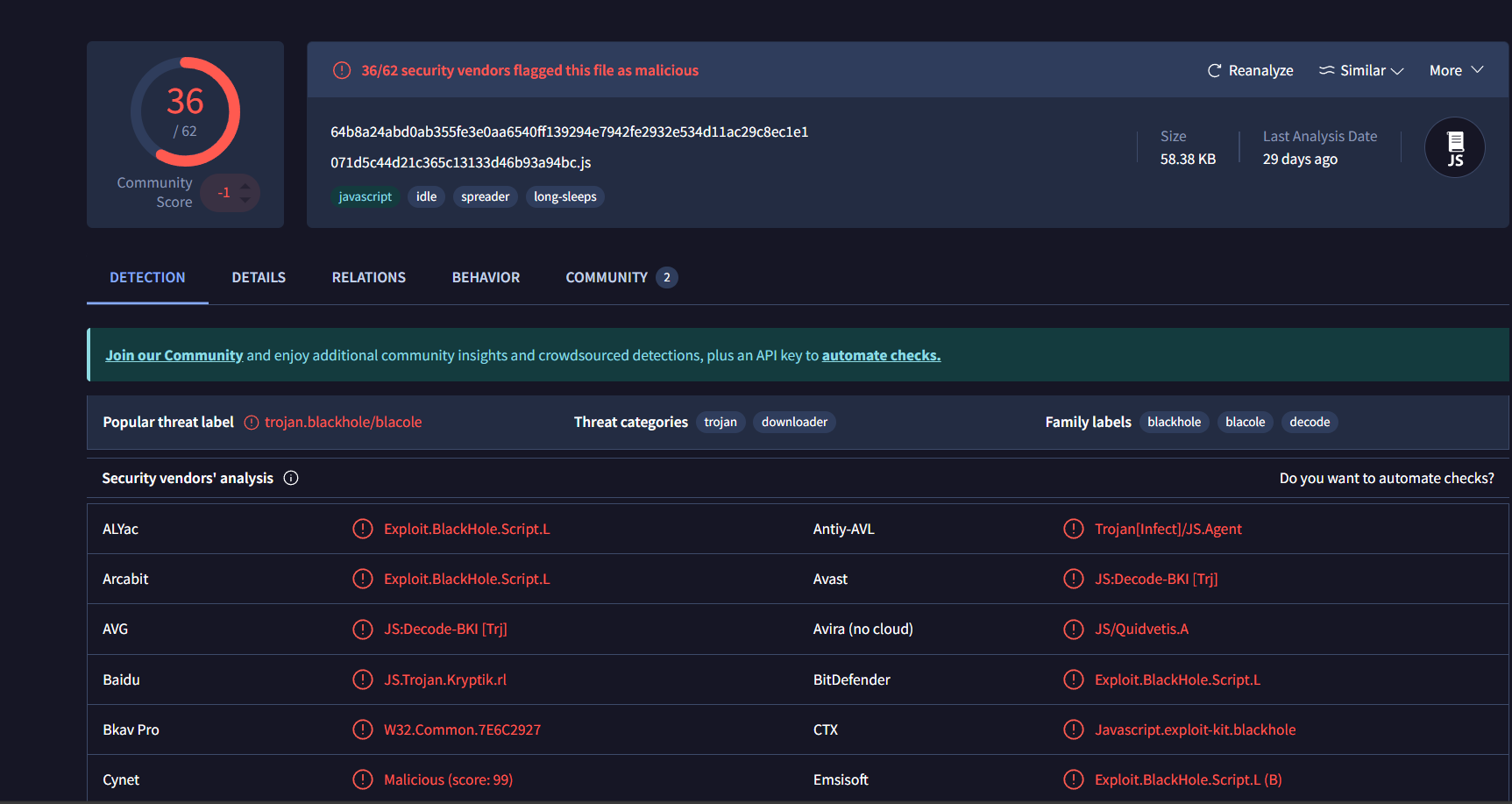
* RiskWare/Win32.Kryptik.a

Kryptik (còn được gọi là Win32 / Kryptik.BGIS) là một trojan cửa hậu, thường được cài đặt mà người dùng không biết. Do đó, mọi người không cố tình cài đặt các chương trình loại này. Khi cài đặt, Kryptik có thể được điều khiển từ xa.

Sử dụng tính năng này, tội phạm mạng cố gắng lừa mọi người cài đặt Kryptik để họ có thể đánh cắp thông tin và sau đó sử dụng nó để tạo doanh thu. Nếu có bất kỳ lý do nào để tin rằng Kryptik được cài đặt trên hệ điều hành, hãy xóa nó ngay lập tức.

Hơn nữa, thuật ngữ "Kryptik" (còn được gọi là Krypt, Cryptic, Crypt và Packed) được sử dụng bởi các cơ sở dữ liệu phần mềm độc hại khác nhau để mô tả các tệp "đóng gói" (nén).

Tên phát hiện:



[VirusTotal - File - 64b8a24abd0ab355fe3e0aa6540ff139294e7942fe2932e534d11ac29c8ec1e1](https://www.virustotal.com/gui/file/64b8a24abd0ab355fe3e0aa6540ff139294e7942fe2932e534d11ac29c8ec1e1/detection)

- Win/malicious\_confidence\_90% (D)

Được phát hiện bởi CrowdStrike.

Điểm đặc biệt của công nghệ này là thay vì đưa ra câu trả lời có/không như các phần mềm diệt virus truyền thống, nó trả về điểm tin cậy từ 60 đến 100. Điểm số càng cao, khả năng tệp tin là phần mềm độc hại càng chắc chắn. Engine này không phụ thuộc vào chữ ký (signatures) nên có khả năng phát hiện phần mềm độc hại mới mà các engine khác có thể bỏ qua.

Thay vì dựa vào các chuỗi byte cụ thể như cách truyền thống, CrowdStrike sử dụng học máy để phân tích các đặc điểm tổng quan của tệp tin, từ đó tạo ra các "đặc trưng" mô tả cấu trúc của tệp. Điều này bao gồm việc đánh giá mức độ ngẫu nhiên trong tệp hoặc phân tích các tài nguyên nhúng (như hình ảnh, biểu tượng, mẫu giao diện, v.v.). Hàng triệu giá trị số được trích xuất và phân tích, giúp engine đưa ra quyết định chính xác về việc tệp có phải là phần mềm độc hại hay không.

CrowdStrike cũng giải thích rằng học máy vượt trội trong việc nhận diện phần mềm độc hại mới mà không cần cập nhật thường xuyên, nhờ khả năng "tổng quát hóa" (generalization) – tức là hiểu sâu về phần mềm độc hại thay vì chỉ học các dấu hiệu nhận diện tạm thời.

Ngoài ra, CrowdStrike nhấn mạnh rằng trong Falcon Host, engine này là lớp bảo vệ đầu tiên trước khi các kỹ thuật theo dõi hành vi (behavioral techniques) phát huy tác dụng, đặc biệt quan trọng khi đối phó với các mối đe dọa từ quốc gia hoặc tội phạm có tổ chức.

* Trojan.Agent.Win32.3991781

Là một phân nhóm của họ "Agent", bao gồm nhiều loại phần mềm độc hại khác nhau không thuộc về các nhóm đã biết khác. Họ Agent bao gồm trojan, sâu (worms), virus, backdoor và các chương trình độc hại khác.

Một số ví dụ đại diện của các phân nhóm khác bao gồm:

* Backdoor/Agent.AMB
* Rootkit/Agent.EA
* Trojan/Agent.AFB
* Trojan-Downloader/Agent.BRK
* Trojan-Downloader/Agent.EYA
* Trojan-Dropper/Agent.PR
* Worm/Agent.T

**Nhận xét chung**  
Hầu hết các phát hiện đều là một **Phát hiện Heuristic**. Điều này cho biết một tệp tin đã được xác định là mối đe dọa tiềm ẩn do hành vi đáng ngờ của nó. Phát hiện này thường được kích hoạt bởi phần mềm độc hại cố gắng hoạt động như hoặc giả mạo các ứng dụng hợp pháp.

Những cờ này cho thấy file bị nghi ngờ có chứa mã độc hại với mức độ cảnh báo cao từ nhiều công cụ diệt virus khác nhau. Các công cụ đều sử dụng những kỹ thuật phát hiện khác nhau như chữ ký (signature), phát hiện heuristic, và đặc biệt là học máy (machine learning), để xác định rằng file có dấu hiệu của các loại mã độc tiềm ẩn. Nhìn chung, các cờ này đều chỉ ra rằng file có khả năng chứa mã độc, bao gồm trojan, malware hoặc phần mềm có hành vi tải về mã độc khác. Điều này đặc biệt đáng chú ý khi các engine học máy (machine learning) và phát hiện heuristic đều đồng thuận về khả năng file này gây nguy hiểm.