



# NEW REVIL VERSION IDENTIFIED

**ZEROFOX INTELLIGENCE**

F-2022-05-13a

Classification: WHITE

Criticality: HIGH

Intelligence Requirements: DEEP DARK WEB & CRIMINAL UNDERGROUND

May 13, 2022



### Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 2:00 PM (EDT) on May 13, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# New REvil Version Identified

## Key Findings

- Updated samples indicate REvil or someone close to the group has resumed operations.
- REvil joins a growing list of ransom families requiring predetermined command line arguments to function.
- REvil no longer refuses to run based on an infected systems' language.
- An unused configuration element introduced previously is now populated with credentials.

## Analyst Commentary

REvil—also sometimes referred to as Sodinokibi—is a ransomware family that first appeared in April 2019 and is thought to be a rebrand of the GandCrab ransomware. The group has been attributed to high-profile attacks, such as the ones against JBS Foods and Kaseya in 2021. Although several members of the group were arrested in January 2022<sup>1</sup>, that does not appear to have deterred the remaining members.

After halting all public activity in October 2021, REvil appears to have resumed operations in April 2022. ZeroFox has observed multiple updates to REvil's leak site since then, with five new victims appearing since the site came back online, including Unicity International, U.S.-based manufacturer of wellness supplements, and Ludwig Freytag Group, a Germany-based construction company.

Researchers for Secureworks Counter Threat Unit (CTU) analyzed new samples found on VirusTotal in late March 2022. Analysis of these recently discovered samples indicated that the developer making modifications had access to the original REvil source code, adding to the likelihood of the group's return.<sup>2</sup>

---

<sup>1</sup> <https://www.bbc.com/news/technology-59998925>

<sup>2</sup>

<https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence>



Changes to REvil's string decryption logic were found that now require a predetermined value to be passed via the command line to successfully run. This value is used to calculate the RC4 decryption key length and the encrypted data offset within the binary. Without this value, REvil samples will no longer be able to execute successfully.

Many malware and ransomware families have language checks that prohibit infecting systems in The Commonwealth of Independent States (CIS) and outright ban clients or affiliates from targeting countries in the region. The REvil sample analyzed by SecureWorks CTU has removed this check, allowing the ransomware to run on any system, regardless of language or location. The significance of this removal has yet to be determined.

An "accs" element was added to REvil's configuration in October 2021, but it was not used for anything at the time. The new sample populates this field with what appears to be targeted accounts from the victim's network.

Hardcoded public keys have also been updated, though the reason for this is currently unknown. Other minor changes have been made as well, including changing the location of the configuration and using globally unique identifiers (GUID) to format affiliate IDs.

A second, near-identical REvil sample was discovered with a newer timestamp in April 2022. The only major difference from the version analyzed in March is that the April 2022 build does not contain the changes to string decryption that require the command line argument. This version also contains a bug when renaming files that prevents it from encrypting files afterwards, which is likely to be quickly fixed.

## Recommendations

- Ensure antivirus and intrusion detection software is up to date with all patches and rule sets.
- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Avoid opening unsolicited attachments and never click suspicious links.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Review network logs for potential signs of compromise and data egress.



- If not already enabled, engage with ZeroFox for ongoing compromised credential monitoring. Immediate password changes should be implemented for any affected account.

## Appendix 1: IOCs

| Indicator                                                        | Type        | Description             |
|------------------------------------------------------------------|-------------|-------------------------|
| 861e2544ddb9739d79b265aabe327d11617bc9d9c94bc5b35282c33fcb419bc  | SHA256 hash | March 2022 REvil sample |
| 0c10cf1b1640c9c845080f460ee69392bfaac981a4407b607e8e30d2ddf903e8 | SHA256 hash | April 2022 REvil sample |



## Appendix 2: Traffic Light Protocol for Information Dissemination

### Red

#### WHEN SHOULD IT BE USED?

##### Sources may use TLP:

**RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

#### HOW MAY IT BE SHARED?

##### Recipients may NOT share TLP:

**RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

### Amber

##### Sources may use TLP:

**AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

##### Recipients may ONLY share TLP:

**AMBER** information with members of their own organization and only as widely as necessary to act on that information.

### Green

#### WHEN SHOULD IT BE USED?

##### Sources may use TLP:

**GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

#### HOW MAY IT BE SHARED?

##### Recipients may share TLP:

**GREEN** information with peers & partner organizations within their sector or community but not via publicly accessible channels.

### White

##### Sources may use TLP:

**WHITE** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

##### Recipients may share TLP:

**WHITE** information without restriction, subject to copyright controls.