



**| Flash |**

# ShinyHunters Attacks Cl0p Ransomware Leak Site

F-2026-09-22a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Dark Web, Threat Actor, Ransomware

**September 22, 2026**

## 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 10:00 AM (EDT) on September 22, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# | Flash | ShinyHunters Attacks CI0p Ransomware Leak Site

## | Key Findings

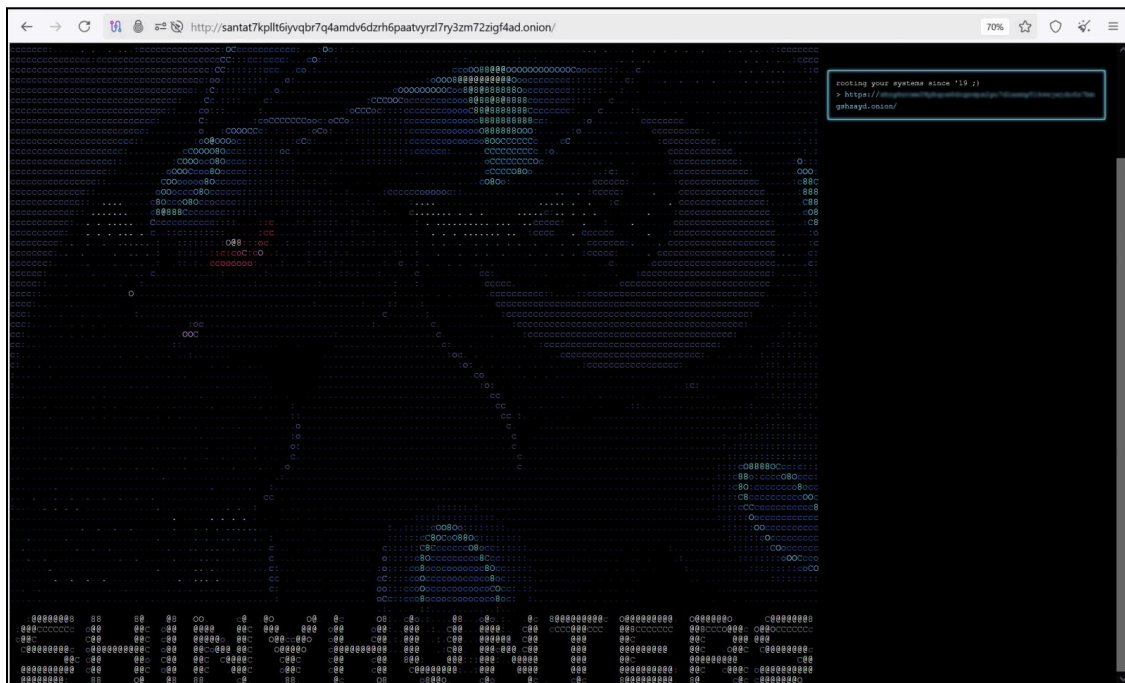
- On September 18, 2026, ransomware and digital extortion (R&DE) collective ShinyHunters gained unauthorized access to the dark web leak site belonging to fellow R&DE threat collective CI0p.
- ShinyHunters claims to have stolen significant amounts of data from CI0p, including the group's source code—likely meaning the source code for CI0p's ransomware-as-a-service (RaaS) software and tools. There is a roughly even chance that ShinyHunters gained access to the IP addresses of individuals connected to CI0p.
- Unless CI0p comes to a rapid agreement for ShinyHunters to release the stolen data—and assuming ShinyHunters will actually return data and source code—ZeroFox assesses that CI0p is unlikely to have the capability to conduct successful R&DE operations, causing a tangible, if temporary, degradation of the threat actor group's ability to impact organizations.
- Additionally, ZeroFox assesses that rivalries and attacks between R&DE collectives will very likely lead to greater fragmentation across the threat landscape. Such fragmentation will almost certainly see new threat actors and splinter groups,

creating a more crowded R&DE ecosystem and almost certainly leading to an increase in incidents.

## Details

On September 18, 2026, R&DE collective ShinyHunters gained unauthorized access to the dark web leak site belonging to fellow R&DE threat collective CI0p. The attack began when ShinyHunters exploited what the group claims was an unauthenticated file upload vulnerability on CI0p's site; ShinyHunters allegedly exploited the vulnerability to upload a small text file that contained a note warning CI0p not to threaten the group.<sup>1</sup>

Several hours later, ShinyHunters reportedly told a journalist that it had defaced CI0p's leak site.<sup>2</sup> The defaced leak site now includes a link to ShinyHunters' own dark web leak site, as well as a message taunting CI0p.



**CI0p's dark web leak site after ShinyHunters' defacement**

Source: ZeroFox Intelligence

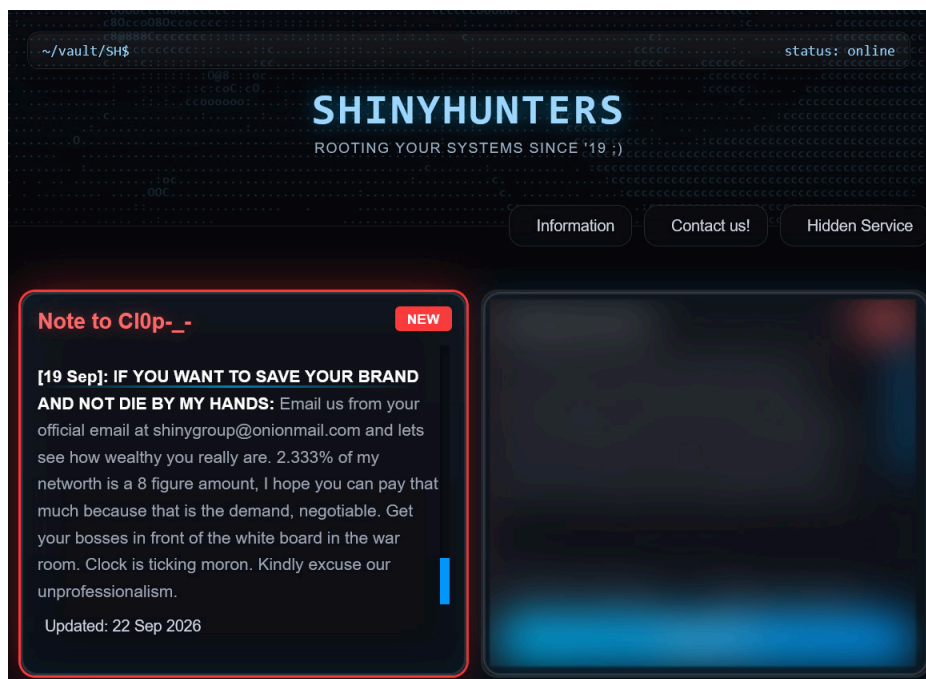
<sup>1</sup> [hXxps://www.bleepingcomputer\[.\]com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/](https://www.bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/)

<sup>2</sup> *Ibid.*

ShinyHunters claims to have stolen significant amounts of data from CI0p, including its source code<sup>3</sup>—likely meaning the source code for CI0p’s RaaS software and tools.

- It is also likely that ShinyHunters obtained system activity indicators and authentication logs.
- There is a roughly even chance that ShinyHunters gained access to the IP addresses of individuals connected to CI0p.

On September 22, 2026, ShinyHunters added CI0p as a victim on its dark web leak site. In the post, the collective threatened to destroy CI0p’s brand unless an eight-figure ransom is paid, with the amount increasing every 24 hours that CI0p fails to respond or negotiate.<sup>4</sup>



## CI0p added to ShinyHunters’ dark web leak site

Source: ZeroFox Intelligence

ZeroFox assesses that this incident will likely have a significant impact on CI0p’s R&DE activity over the next six months. ShinyHunters exploiting CI0p’s leak site, stealing data, and very likely gaining access to CI0p’s source code will likely have more consequences

<sup>3</sup> Ibid.

<sup>4</sup> Ibid.

than just reputational damage. Unless CI0p comes to a rapid agreement for ShinyHunters to release the stolen data—and assuming ShinyHunters will actually return data and source code—ZeroFox assesses that CI0p is unlikely to have the capability to conduct successful R&DE operations, causing a tangible, if temporary, degradation of the threat actor group’s ability to impact organizations.

Additionally, ZeroFox assesses that rivalries and attacks between R&DE collectives will very likely lead to greater fragmentation across the threat landscape. Such fragmentation will almost certainly see new threat actors and splinter groups, creating a more crowded R&DE ecosystem and almost certainly leading to an increase in incidents.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## **| Appendix B: ZeroFox Intelligence Probability Scale**

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |