

## Rise in Active RaaS Groups Parallel Growing Victim Counts: Ransomware in 2H 2023

This data sheet collates relevant information on the ransomware threat landscape for the third and fourth quarters of 2023, obtained from ransomware-as-a-service (RaaS) and extortion groups' leak sites, Trend Micro's open-source intelligence (OSINT) research, and Trend threat intelligence. The data presented here describes ransomware activity in general and the three most prominent ransomware families in the threat landscape during the six-month span.

|                        | JUL              | AUG              | SEP              | OCT              | NOV            | DEC            |
|------------------------|------------------|------------------|------------------|------------------|----------------|----------------|
| Email threats          | 256,371          | 258,155          | 361,162          | 135,242          | 114,629        | 122,068        |
| URL threats            | 167,066          | 149,861          | 120,402          | 130,214          | 132,727        | 135,753        |
| File threats           | 606,886          | 1,420,386        | 995,452          | 1,525,343        | 519,208        | 321,088        |
| <b>Total</b>           | <b>1,030,323</b> | <b>1,828,402</b> | <b>1,477,016</b> | <b>1,790,799</b> | <b>766,564</b> | <b>578,909</b> |
| <b>Total quarterly</b> | <b>4,335,741</b> |                  |                  | <b>3,136,272</b> |                |                |

Table 1. The number of ransomware threats detected and blocked by Trend across email, URL, and file layers per month in the third and fourth quarters of 2023

Source: Trend Research telemetry

|  | 1H 2023 | 2H 2023 |
|--|---------|---------|
| Total active RaaS and extortion groups | 45      | 52      |
| Victim organizations                   | 1,999   | 2,524   |

Table 2. The numbers of active RaaS and extortion groups and victim organizations of successful ransomware attacks in 2023

Sources: RaaS and extortion group leak sites

| Q3                    |              | Q4                    |              |
|-----------------------|--------------|-----------------------|--------------|
| Industry              | Victim count | Industry              | Victim count |
| Manufacturing         | 113          | Manufacturing         | 131          |
| Finance               | 104          | Healthcare            | 101          |
| IT                    | 101          | Finance               | 86           |
| Professional services | 99           | Professional services | 83           |
| Healthcare            | 93           | Construction          | 72           |
| Construction          | 92           | Academe               | 64           |
| Academe               | 72           | IT                    | 64           |
| Legal services        | 66           | Transportation        | 58           |
| Hospitality           | 59           | Legal services        | 49           |
| Materials             | 56           | Materials             | 48           |

Table 3. The top 10 industries affected by successful RaaS and extortion attacks in the third and fourth quarters of 2023

Sources: RaaS and extortion group leak sites and Trend's OSINT research

| Segment    | JUL    | SEP    | OCT    | TOTAL         |
|------------|--------|--------|--------|---------------|
| Enterprise | 13,040 | 14,924 | 13,164 | <b>41,128</b> |
| Consumer   | 2,169  | 2,155  | 2,474  | <b>6,798</b>  |
| SMB        | 1,971  | 1,961  | 1,797  | <b>5,729</b>  |

Table 4. The number of ransomware file detections in machines in each business segment per month in the third quarter of 2023

Source: Trend Research telemetry

| Segment    | OCT    | NOV    | DEC    | TOTAL         | Percentage of increase in Q3 vs. Q4 |
|------------|--------|--------|--------|---------------|-------------------------------------|
| Enterprise | 17,254 | 16,743 | 12,564 | <b>46,561</b> | <b>13.2% increase</b>               |
| Consumer   | 2,354  | 2,602  | 2,461  | <b>7,417</b>  | <b>9.1% increase</b>                |
| SMB        | 1,134  | 1,938  | 1,992  | <b>5,064</b>  | <b>28.7% decrease</b>               |

Table 5. The number of ransomware file detections in machines in each business segment per month in the fourth quarter of 2023

Source: Trend Research telemetry

| Q3             |              | Q4             |              |
|----------------|--------------|----------------|--------------|
| Country        | Victim count | Country        | Victim count |
| United States  | 641          | United States  | 547          |
| United Kingdom | 84           | United Kingdom | 79           |
| Canada         | 54           | Canada         | 58           |
| Germany        | 54           | Germany        | 42           |
| France         | 45           | Italy          | 42           |
| Italy          | 42           | France         | 38           |
| Australia      | 37           | Australia      | 32           |
| Spain          | 22           | Netherlands    | 22           |
| Bulgaria       | 19           | Spain          | 21           |
| Unknown        | 47           | Unknown        | 28           |

Table 6. The top 10 countries affected by successful RaaS and extortion attacks in the third and fourth quarters of 2023

Sources: RaaS and extortion group leak sites and Trend's OSINT research

| Q3                |                                | Q4                |                                |
|-------------------|--------------------------------|-------------------|--------------------------------|
| Ransomware family | Number of victim organizations | Ransomware family | Number of victim organizations |
| LockBit           | 252                            | LockBit           | 266                            |
| Clop              | 175                            | Play              | 112                            |
| BlackCat          | 110                            | BlackCat          | 95                             |

Table 7. The top three ransomware families used in successful RaaS and extortion attacks in terms of victim organizations in the third and fourth quarters of 2023

Sources: RaaS and extortion group leak sites

| Organization size                 | LockBit |     | BlackCat |    | Clop |    |
|-----------------------------------|---------|-----|----------|----|------|----|
|                                   | Q3      | Q4  | Q3       | Q4 | Q3   | Q4 |
| Small (1 to 200 employees)        | 167     | 153 | 52       | 52 | 110  | 4  |
| Medium (201 to 1,000 employees)   | 41      | 62  | 33       | 23 | 33   | 3  |
| Large (more than 1,001 employees) | 12      | 20  | 19       | 13 | 31   | 0  |
| Unknown                           | 32      | 31  | 6        | 7  | 1    | 1  |

Table 8. The distribution by organization size of LockBit, BlackCat, and Clop's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Sources: LockBit, BlackCat, and Clop's leak sites and Trend's OSINT research

| JUL        |     | AUG       |     | SEP          |     |
|------------|-----|-----------|-----|--------------|-----|
| LOCKBIT    | 423 | EGOGEN    | 495 | BLACKCAT     | 388 |
| STOPCRYPT  | 405 | LOCKBIT   | 350 | EGOGEN       | 350 |
| BLACKCAT   | 307 | BLACKCAT  | 322 | CONTI        | 348 |
| EGOGEN     | 249 | CONTI     | 312 | STOPCRYPT    | 280 |
| CONTI      | 179 | STOPCRYPT | 249 | LOCKBIT      | 270 |
| SODINOKIBI | 150 | AKIRA     | 239 | RHYSIDA      | 124 |
| TARGETCOMP | 132 | RHYSIDA   | 164 | RAGNAR       | 118 |
| CLOP       | 124 | CRYPTESLA | 133 | RAGNARLOCKER | 118 |
| CRYPTESLA  | 122 | CLOP      | 129 | CRYPTESLA    | 117 |
| CRYSIS     | 102 | PHOBOS    | 120 | PHOBOS       | 113 |

Table 9. The top 10 ransomware families in terms of ransomware file detections in machines in the third quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| OCT       |     | NOV        |     | DEC        |     |
|-----------|-----|------------|-----|------------|-----|
| GWZICHA   | 460 | BLACKCAT   | 586 | LOCKBIT    | 518 |
| LOCKBIT   | 441 | LOCKBIT    | 360 | TARGETCOMP | 267 |
| STOPCRYPT | 326 | STOPCRYPT  | 266 | STOPCRYPT  | 217 |
| CONTI     | 318 | CONTI      | 250 | BLACKCAT   | 186 |
| BLACKCAT  | 226 | AKIRA      | 221 | AKIRA      | 166 |
| ENCODER   | 208 | AVOSLOCKER | 176 | CONTI      | 158 |
| AKIRA     | 198 | CYCLOPS    | 166 | AVOSLOCKER | 152 |
| BLACKSUIT | 175 | GWZICHA    | 163 | PHOBOS     | 146 |
| CRYPTESLA | 172 | CRYPTESLA  | 159 | CRYPTESLA  | 120 |
| CONVAGENT | 164 | CRILOCK    | 150 | GWZICHA    | 107 |

Table 10. The top 10 ransomware families in terms of ransomware file detections in machines in the fourth quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| JUL                |                 | AUG                        |                 | SEP                        |                 |
|--------------------|-----------------|----------------------------|-----------------|----------------------------|-----------------|
| Industry           | File detections | Industry                   | File detections | Industry                   | File detections |
| Banking            | 1,658           | Banking                    | 1,558           | Banking                    | 1,519           |
| Government         | 501             | Government                 | 1,557           | Fast-moving consumer goods | 674             |
| Telecommunications | 243             | Fast-moving consumer goods | 698             | Government                 | 309             |

Table 11. The top three industries in terms of ransomware file detections in machines per month in the third quarter of 2023

Source: Trend Research telemetry

| OCT                        |                 | NOV                        |                 | DEC        |                 |
|----------------------------|-----------------|----------------------------|-----------------|------------|-----------------|
| Industry                   | File detections | Industry                   | File detections | Industry   | File detections |
| Technology                 | 1,579           | Technology                 | 2,193           | Banking    | 1,343           |
| Banking                    | 1,509           | Banking                    | 1,470           | Technology | 726             |
| Fast-moving consumer goods | 1,388           | Fast-moving consumer goods | 591             | Financial  | 394             |

Table 12. The top three industries in terms of ransomware file detections in machines per month in the fourth quarter of 2023

Source: Trend Research telemetry

| JUL               |                   |            | AUG                        |                   |            | SEP        |                   |            |
|-------------------|-------------------|------------|----------------------------|-------------------|------------|------------|-------------------|------------|
| Industry          | Ransomware family | Detections | Industry                   | Ransomware family | Detections | Industry   | Ransomware family | Detections |
| Banking           | BLACKCAT          | 39         | Banking                    | EGOGEN            | 70         | Banking    | CONTI             | 50         |
|                   | LOCKBIT           | 32         |                            | CONTI             | 44         |            | EGOGEN            | 29         |
|                   | CRYPTESLA         | 29         |                            | AKIRA             | 30         |            | LOCKBIT           | 26         |
| Government        | LOCKBIT           | 16         | Government                 | LOCKBIT           | 48         | Technology | CONTI             | 17         |
|                   | CONTI             | 15         |                            | CONTI             | 46         |            | LOCKBIT           | 15         |
|                   | BLACKCAT          | 14         |                            | EGOGEN            | 36         |            | CRYPTESLA         | 13         |
| Telecommunication | LOCKBIT           | 8          | Fast-moving consumer goods | CONTI             | 19         | Financial  | EGOGEN            | 19         |
|                   | CLOP              | 5          |                            | LOCKBIT           | 16         |            | CONTI             | 10         |
|                   | CRYPTESLA         | 4          |                            | CRYPTESLA         | 14         |            | CRILOCK           | 6          |

Table 13. The top three industries in terms of ransomware file detections in machines in the top affected industries per month in the third quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| OCT                        |                   |            | NOV                        |                   |            | DEC        |                   |            |
|----------------------------|-------------------|------------|----------------------------|-------------------|------------|------------|-------------------|------------|
| Industry                   | Ransomware family | Detections | Industry                   | Ransomware family | Detections | Industry   | Ransomware family | Detections |
| Technology                 | LOCKBIT           | 39         | Technology                 | LOCKBIT           | 59         | Banking    | TARGETCOMP        | 34         |
|                            | CONTI             | 38         |                            | CONTI             | 58         |            | LOCKBIT           | 26         |
|                            | BLACKCAT          | 28         |                            | BLACKCAT          | 50         |            | CRYPTESLA         | 24         |
| Banking                    | CONTI             | 50         | Banking                    | CRYPTESLA         | 28         | Technology | LOCKBIT           | 21         |
|                            | AKIRA             | 35         |                            | LOCKBIT           | 27         |            | SODINOKIBI        | 15         |
|                            | CRYPTESLA         | 28         |                            | CONTI             | 26         |            | CONTI             | 14         |
| Fast-moving consumer goods | CONTI             | 35         | Fast-moving consumer goods | CRILOCK           | 11         | Financial  | LOCKBIT           | 18         |
|                            | LOCKBIT           | 30         |                            | CONTI             | 10         |            | TARGETCOMP        | 17         |
|                            | CRYPTESLA         | 28         |                            | LOCKBIT           | 10         |            | AVOSLOCKER        | 17         |

Table 14. The top three industries in terms of ransomware file detections in machines in the top affected industries per month in the fourth quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| JUL        |                   |            | AUG        |                   |            | SEP        |                   |            |
|------------|-------------------|------------|------------|-------------------|------------|------------|-------------------|------------|
| Industry   | Ransomware family | Detections | Industry   | Ransomware family | Detections | Industry   | Ransomware family | Detections |
| Enterprise | LOCKBIT           | 372        | Enterprise | EGOGEN            | 495        | Enterprise | EGOGEN            | 343        |
|            | STOPCRYPT         | 250        |            | BLACKCAT          | 309        |            | CONTI             | 317        |
|            | EGOGEN            | 243        |            | CONTI             | 300        |            | BLACKCAT          | 296        |
|            | BLACKCAT          | 242        |            | LOCKBIT           | 288        |            | LOCKBIT           | 182        |
|            | CONTI             | 175        |            | AKIRA             | 237        |            | STOPCRYPT         | 159        |
| Consumer   | STOPCRYPT         | 123        | Consumer   | STOPCRYPT         | 73         | Consumer   | STOPCRYPT         | 82         |
|            | LOCKBIT           | 42         |            | LOCKBIT           | 57         |            | LOCKBIT           | 55         |
|            | PHOBOS            | 31         |            | PHOBOS            | 34         |            | DRODZP            | 35         |
|            | CRYPTOLOAD        | 21         |            | MAGNIBER          | 25         |            | CRYPTOLOAD        | 26         |
|            | TARGETCOMP        | 19         |            | CRYPTOLOAD        | 24         |            | DWNLDR            | 22         |
| SMB        | BLACKCAT          | 57         | SMB        | STOPCRYPT         | 26         | SMB        | BLACKCAT          | 90         |
|            | STOPCRYPT         | 25         |            | BLACKCAT          | 7          |            | LOCKBIT           | 28         |
|            | RYUK              | 14         |            | CRYPTESLA         | 6          |            | STOPCRYPT         | 25         |
|            | PHOBOS            | 11         |            | LOCKBIT           | 5          |            | CONTI             | 20         |
|            | TARGETCOMP        | 10         |            | PHOBOS            | 5          |            | SPORA             | 10         |

Table 15. The top five ransomware families in terms of ransomware file detections in machines per business segment and per month in the third quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| OCT        |                   |            | NOV        |                   |            | DEC        |                   |            |
|------------|-------------------|------------|------------|-------------------|------------|------------|-------------------|------------|
| Industry   | Ransomware family | Detections | Industry   | Ransomware family | Detections | Industry   | Ransomware family | Detections |
| Enterprise | GWZICHA           | 460        | Enterprise | BLACKCAT          | 558        | Enterprise | LOCKBIT           | 395        |
|            | LOCKBIT           | 382        |            | LOCKBIT           | 272        |            | TARGETCOMP        | 231        |
|            | CONTI             | 305        |            | CONTI             | 214        |            | BLACKCAT          | 160        |
|            | BLACKCAT          | 204        |            | AKIRA             | 210        |            | AKIRA             | 153        |
|            | AKIRA             | 195        |            | AVOSLOCKER        | 167        |            | AVOSLOCKER        | 144        |
| Consumer   | STOPCRYPT         | 126        | Consumer   | STOPCRYPT         | 94         | Consumer   | STOPCRYPT         | 122        |
|            | LOCKBIT           | 44         |            | LOCKBIT           | 53         |            | LOCKBIT           | 61         |
|            | DRODZP            | 29         |            | DRODZP            | 52         |            | DRODZP            | 44         |
|            | CRYPTOLOAD        | 21         |            | CRYPTOLOAD        | 34         |            | CRYPTOLOAD        | 32         |
|            | DWNLDR            | 19         |            | EXMAS             | 29         |            | PHOBOS            | 24         |
| SMB        | PLAYDE            | 47         | SMB        | PLAYDE            | 71         | SMB        | LOCKBIT           | 52         |
|            | STOPCRYPT         | 36         |            | LOCKBIT           | 28         |            | CONTI             | 23         |
|            | BLACKCAT          | 14         |            | BLACKCAT          | 22         |            | STOPCRYPT         | 21         |
|            | LOCKBIT           | 14         |            | STOPCRYPT         | 21         |            | PHOBOS            | 16         |
|            | ISHTAR            | 8          |            | CONTI             | 21         |            | CRILOCK           | 16         |

Table 16. The top five ransomware families in terms of ransomware file detections in machines per business segment and per month in the fourth quarter of 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| JUL               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| Turkey            |            | Kuwait            |            | Germany           |            | India             |            | UAE               |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| LOCKBIT           | 87         | CRYPTESLA         | 28         | EGOGEN            | 28         | LOCKBIT           | 53         | LOCKBIT           | 16         |
| CONTI             | 82         | LOCKBIT           | 26         | STOPCRYPT         | 23         | STOPCRYPT         | 44         | CONTI             | 15         |
| SODINOKIBI        | 75         | CRILOCK           | 24         | LOCKBIT           | 22         | EGOGEN            | 40         | BLACKCAT          | 11         |
| CLOP              | 44         | CONTI             | 23         | MATSNU            | 17         | BLACKCAT          | 29         | ISHTAR            | 8          |
| BLACKCAT          | 42         | SPORA             | 22         | CONTI             | 15         | TARGETCOMP        | 17         | CRYPCTB           | 8          |
| VENUSLOCK         | 41         | CRYPTLOCK         | 20         | TARGETCOMP        | 15         | CELANCYC          | 15         | CLOP              | 7          |
| EGOGEN            | 39         | ISHTAR            | 18         | CRYPTESLA         | 14         | CLOP              | 15         | EGOGEN            | 7          |
| BLACKBYTE         | 38         | CRYPHYDRA         | 18         | CRILOCK           | 12         | RYUK              | 14         | CRYPHYDRA         | 7          |
| AKIRA             | 35         | SODINOKIBI        | 16         | SPORA             | 11         | SODINOKIBI        | 14         | SODINOKIBI        | 7          |
| CRYSIS            | 32         | CRYPMIC           | 16         | BLACKCAT          | 11         | AKIRA             | 13         | CRILOCK           | 7          |

Table 17. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in July 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| AUG               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| Brazil            |            | Turkey            |            | Kuwait            |            | Germany           |            | Saudi Arabia      |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| EGOGEN            | 101        | LOCKBIT           | 48         | CRYPTESLA         | 28         | EGOGEN            | 52         | LOCKBIT           | 19         |
| CONTI             | 59         | CONTI             | 47         | CRILOCK           | 24         | CONTI             | 39         | CONTI             | 18         |
| LOCKBIT           | 52         | CLOP              | 36         | LOCKBIT           | 23         | AKIRA             | 21         | CRYPTESLA         | 14         |
| AKIRA             | 43         | BLACKCAT          | 33         | SPORA             | 22         | LOCKBIT           | 19         | CRILOCK           | 12         |
| RHYSIDA           | 35         | SODINOKIBI        | 27         | CONTI             | 20         | RHYSIDA           | 17         | BLACKCAT          | 11         |
| BLACKCAT          | 33         | CRYPTESLA         | 27         | CRYPTLOCK         | 18         | STOPCRYPT         | 15         | SPORA             | 11         |
| SODINOKIBI        | 23         | EGOGEN            | 24         | CRYPHYDRA         | 17         | CRYPTESLA         | 15         | CRYPTLOCK         | 10         |
| CRILOCK           | 22         | RYUK              | 21         | ISHTAR            | 16         | RAGNARLOCKER      | 13         | CRYPHYDRA         | 9          |
| CLOP              | 21         | BACUCRYPT         | 19         | SODINOKIBI        | 16         | CRILOCK           | 12         | CRYPMIC           | 9          |
| ARCRYPTER         | 21         | CRYPMIC           | 19         | CRYPCTB           | 16         | TARGETCOMP        | 12         | CLOP              | 9          |

Table 18. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in August 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| SEP               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| Germany           |            | Kuwait            |            | Turkey            |            | Algeria           |            | Taiwan            |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| CONTI             | 53         | LOCKBIT           | 26         | CONTI             | 26         | CONTI             | 17         | MAGNIBER          | 23         |
| EGOGEN            | 46         | CRYPTESLA         | 26         | CRYPTESLA         | 16         | LOCKBIT           | 15         | STOPCRYPT         | 15         |
| LOCKBIT           | 40         | CONTI             | 26         | LOCKBIT           | 16         | CRYPTESLA         | 13         | PHOBOS            | 11         |
| AKIRA             | 25         | CRILOCK           | 24         | STOPCRYPT         | 15         | CRILOCK           | 12         | SCARAB            | 9          |
| BLACKCAT          | 24         | SPORA             | 22         | BABUK             | 12         | SPORA             | 11         | RODUK             | 8          |
| STOPCRYPT         | 21         | CRYPTLOCK         | 20         | CRILOCK           | 12         | BLACKCAT          | 11         | LOCKBIT           | 8          |
| SPORA             | 21         | CLOP              | 19         | MOUNTLOCKER       | 11         | CRYPTLOCK         | 10         | CRYPZXAS          | 7          |
| CRILOCK           | 20         | CRYPHYDRA         | 18         | BLACKCAT          | 11         | SODINOKIBI        | 9          | ENCODER           | 7          |
| CRYPTESLA         | 19         | ISHTAR            | 16         | SPORA             | 11         | STOPCRYPT         | 8          | CRYPTOLOCKER      | 6          |
| CRYPHYDRA         | 18         | SODINOKIBI        | 16         | CRYPTLOCK         | 10         | CRYPHYDRA         | 8          | CRYPAURA          | 9          |

Table 19. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in September 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| OCT               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| Turkey            |            | Kuwait            |            | Japan             |            | UAE               |            | Germany           |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| LOCKBIT           | 68         | CRYPTESLA         | 25         | ENCODER           | 150        | CONTI             | 29         | CONTI             | 36         |
| CONTI             | 67         | LOCKBIT           | 21         | LOCKBIT           | 43         | CRILOCK           | 18         | LOCKBIT           | 25         |
| CRYPTESLA         | 56         | CONTI             | 21         | DRODZP            | 29         | LOCKBIT           | 18         | BLACKCAT          | 23         |
| CRILOCK           | 52         | CRILOCK           | 20         | CRYPTOLOAD        | 21         | CRYPTESLA         | 16         | RHYSIDA           | 13         |
| SPORA             | 46         | SPORA             | 19         | LOCKYDOWNLOADER   | 17         | SPORA             | 14         | CRYPTESLA         | 13         |
| CRYPTLOCK         | 41         | CLOP              | 17         | DWNLDR            | 16         | CLOP              | 14         | STOPCRYPT         | 13         |
| CRYPHYDRA         | 41         | ISHTAR            | 16         | INJECT            | 15         | CRYPTLOCK         | 13         | SODINOKIBI        | 12         |
| SODINOKIBI        | 38         | CRYPHYDRA         | 15         | STOPCRYPT         | 11         | MATRIX            | 11         | CHAOS             | 12         |
| BLACKCAT          | 37         | SODINOKIBI        | 15         | SCHOPETS          | 8          | BLACKCAT          | 11         | CRILOCK           | 12         |
| CRYPMIC           | 36         | EGOGEN            | 15         | SCARAB            | 8          | CRYPCTB           | 11         | SPORA             | 11         |

Table 20. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in October 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

| NOV               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| Turkey            |            | Germany           |            | Kuwait            |            | Japan             |            | US                |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| CONTI             | 68         | CONTI             | 49         | CRYPTESLA         | 28         | DRODZP            | 51         | PLAYDE            | 42         |
| LOCKBIT           | 67         | LOCKBIT           | 47         | LOCKBIT           | 26         | LOCKBIT           | 34         | LOCKBIT           | 38         |
| CRILOCK           | 46         | CRYPTESLA         | 40         | CONTI             | 25         | EXMAS             | 29         | BLACKCAT          | 25         |
| CRYPTESLA         | 45         | CRILOCK           | 38         | CRILOCK           | 24         | CRYPTOLOAD        | 28         | CONTI             | 22         |
| BLACKCAT          | 44         | SPORA             | 33         | SPORA             | 22         | DWNLDR            | 25         | AKIRA             | 17         |
| SPORA             | 42         | STOPCRYPT         | 31         | CRYPTLOCK         | 20         | INJECT            | 21         | RYUK              | 17         |
| CRYPTLOCK         | 38         | CRYPTLOCK         | 30         | CLOP              | 18         | LOCKYDOWNLOADER   | 21         | SODINOKIBI        | 15         |
| CRYPHYDRA         | 36         | SODINOKIBI        | 28         | CRYPHYDRA         | 18         | SMALL             | 14         | PHOBOS            | 15         |
| CLOP              | 36         | AKIRA             | 28         | BLACKCAT          | 16         | NEMUCOD           | 14         | STOPCRYPT         | 15         |
| ISHTAR            | 34         | CRYPCTB           | 27         | SODINOKIBI        | 16         | NETWALKER         | 12         | ROYAL             | 14         |

Table 21. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in November 2023, with notable ransomware families highlighted

Source: Trend Research telemetry



| DEC               |            |                   |            |                   |            |                   |            |                   |            |
|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|-------------------|------------|
| US                |            | Germany           |            | Kuwait            |            | Turkey            |            | Ukraine           |            |
| Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections | Ransomware family | Detections |
| LOCKBIT           | 109        | AKIRA             | 35         | CONTI             | 24         | CATAKA            | 32         | CONTI             | 18         |
| BLACKCAT          | 32         | CONTI             | 34         | LOCKBIT           | 24         | LOCKBIT           | 21         | LOCKBIT           | 16         |
| PHOBOS            | 27         | LOCKBIT           | 30         | CRYPTESLA         | 24         | BLACKKINGDOM      | 16         | BLACKCAT          | 11         |
| SCARAB            | 24         | CRYPTESLA         | 25         | SPORA             | 22         | CONTI             | 16         | CRILOCK           | 11         |
| BLACKMATTER       | 23         | TARGETCOMP        | 24         | CRILOCK           | 21         | SODINOKIBI        | 15         | SPORA             | 10         |
| CRYPTEAR          | 23         | CRILOCK           | 24         | CRYPTLOCK         | 20         | ISHTAR            | 13         | CLOP              | 9          |
| CONTI             | 20         | SPORA             | 22         | CRYPHYDRA         | 17         | STOPCRYPT         | 13         | CRYPTLOCK         | 9          |
| CLOP              | 20         | AVOSLOCKER        | 21         | SODINOKIBI        | 16         | CRILOCK           | 12         | CRYPTESLA         | 9          |
| SODINOKIBI        | 19         | CRYPTLOCK         | 19         | CLOP              | 16         | SPORA             | 12         | CRYPHYDRA         | 9          |
| PLAYDE            | 17         | CRYPHYDRA         | 17         | CRYPCTB           | 16         | CRYPTESLA         | 10         | SODINOKIBI        | 8          |

Table 22. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in December 2023, with notable ransomware families highlighted

Source: Trend Research telemetry

## LockBit

| Q3                    |              | Q4                    |              |
|-----------------------|--------------|-----------------------|--------------|
| Industry              | Victim count | Industry              | Victim count |
| Construction          | 25           | Manufacturing         | 38           |
| Professional services | 22           | Finance               | 22           |
| Academe               | 20           | Healthcare            | 22           |
| Healthcare            | 20           | Construction          | 18           |
| Manufacturing         | 20           | Professional services | 17           |
| Others                | 145          | Others                | 149          |
| <b>Total</b>          | <b>252</b>   | <b>Total</b>          | <b>246</b>   |

Table 23. The distribution by industry of LockBit's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: LockBit's leak site

| Q3                              |              | Q4                              |              |
|---------------------------------|--------------|---------------------------------|--------------|
| Region                          | Victim count | Region                          | Victim count |
| North America                   | 114          | North America                   | 119          |
| Europe                          | 66           | Europe                          | 73           |
| Asia-Pacific                    | 24           | Asia-Pacific                    | 40           |
| Middle East                     | 19           | Latin America and the Caribbean | 14           |
| Latin America and the Caribbean | 17           | Africa                          | 8            |
| Africa                          | 9            | Middle East                     | 8            |
| Eastern Europe                  | 1            | Eastern Europe                  | 4            |
| Unknown                         | 2            |                                 |              |
| <b>Total</b>                    | <b>252</b>   | <b>Total</b>                    | <b>266</b>   |

Table 24. The distribution by region of LockBit's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: LockBit's leak site

| Q3             |              | Q4             |              |
|----------------|--------------|----------------|--------------|
| Country        | Victim count | Country        | Victim count |
| United States  | 105          | United States  | 110          |
| France         | 17           | United Kingdom | 19           |
| United Kingdom | 13           | Italy          | 12           |
| Germany        | 12           | France         | 11           |
| Canada         | 9            | Germany        | 10           |
| Others         | 96           | Others         | 104          |
| <b>Total</b>   | <b>252</b>   | <b>Total</b>   | <b>266</b>   |

Table 25. The distribution by country of LockBit's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: LockBit's leak site

## BlackCat

| Q3                    |              | Q4                    |              |
|-----------------------|--------------|-----------------------|--------------|
| Industry              | Victim count | Industry              | Victim count |
| Legal services        | 16           | Finance               | 11           |
| Finance               | 12           | Healthcare            | 10           |
| Healthcare            | 12           | IT                    | 10           |
| Manufacturing         | 10           | Manufacturing         | 6            |
| Professional services | 6            | Professional services | 6            |
| Others                | 52           | Others                | 52           |
| <b>Total</b>          | <b>110</b>   | <b>Total</b>          | <b>95</b>    |

Table 26. The distribution by industry of BlackCat's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: BlackCat's leak site

| Q3                              |              | Q4                              |              |
|---------------------------------|--------------|---------------------------------|--------------|
| Region                          | Victim count | Region                          | Victim count |
| North America                   | 57           | North America                   | 62           |
| Europe                          | 23           | Asia-Pacific                    | 12           |
| Asia-Pacific                    | 17           | Europe                          | 12           |
| Latin America and the Caribbean | 5            | Latin America and the Caribbean | 5            |
| Africa                          | 4            | Eastern Europe                  | 2            |
| Middle East                     | 3            | Africa                          | 1            |
| Eastern Europe                  | 1            | Middle East                     | 1            |
| <b>Total</b>                    | <b>110</b>   | <b>Total</b>                    | <b>95</b>    |

Table 27. The distribution by region of BlackCat's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: BlackCat's leak site

| Q3             |              | Q4             |              |
|----------------|--------------|----------------|--------------|
| Country        | Victim count | Country        | Victim count |
| United States  | 54           | United States  | 57           |
| Germany        | 6            | Canada         | 5            |
| United Kingdom | 6            | Australia      | 4            |
| Australia      | 5            | Brazil         | 4            |
| Italy          | 4            | United Kingdom | 3            |
| Others         | 35           | Others         | 22           |
| <b>Total</b>   | <b>110</b>   | <b>Total</b>   | <b>95</b>    |

Table 28. The distribution by country of BlackCat's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: BlackCat's leak site

## Clop

| Q3                    |              | Q4           |              |
|-----------------------|--------------|--------------|--------------|
| Industry              | Victim count | Industry     | Victim count |
| IT                    | 34           | Academe      | 2            |
| Finance               | 29           | Construction | 1            |
| Manufacturing         | 14           | Healthcare   | 1            |
| Professional services | 14           | Hospitality  | 1            |
| Healthcare            | 10           | IT           | 1            |
| Others                | 74           | Others       | 2            |
| <b>Total</b>          | <b>175</b>   | <b>Total</b> | <b>8</b>     |

Table 29. The distribution by industry of Clop's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: Clop's leak site

| Q3                              |              | Q4            |              |
|---------------------------------|--------------|---------------|--------------|
| Region                          | Victim count | Region        | Victim count |
| North America                   | 119          | North America | 8            |
| Europe                          | 42           |               |              |
| Asia-Pacific                    | 9            |               |              |
| Middle East                     | 4            |               |              |
| Latin America and the Caribbean | 1            |               |              |
| <b>Total</b>                    | <b>175</b>   | <b>Total</b>  | <b>8</b>     |

Table 30. The distribution by region of Clop's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: Clop's leak site

| Q3             |              | Q4            |              |
|----------------|--------------|---------------|--------------|
| Country        | Victim count | Country       | Victim count |
| United States  | 114          | United States | 7            |
| United Kingdom | 12           | Canada        | 1            |
| Germany        | 9            |               |              |
| Netherlands    | 7            |               |              |
| Canada         | 5            |               |              |
| Others         | 28           |               |              |
| <b>Total</b>   | <b>175</b>   | <b>Total</b>  | <b>8</b>     |

Table 31. The distribution by country of Clop's successful attacks in terms of victim organizations in the third and fourth quarters of 2023

Source: Clop's leak site



Trend Micro, a global cybersecurity leader, leverages decades of security expertise, research, and innovation to help make the world safe for exchanging digital information.

[TrendMicro.com](https://www.trendmicro.com)

Trend Micro  
Research 