ANY.RUN
INTERACTIVE MALWARE ANALYSIS

# Malware Trends
# Q2 2025

## Q2 2025 REVIEW

BY UPLOADS

**TOTAL SANDBOX SESSIONS: 1,559,930**

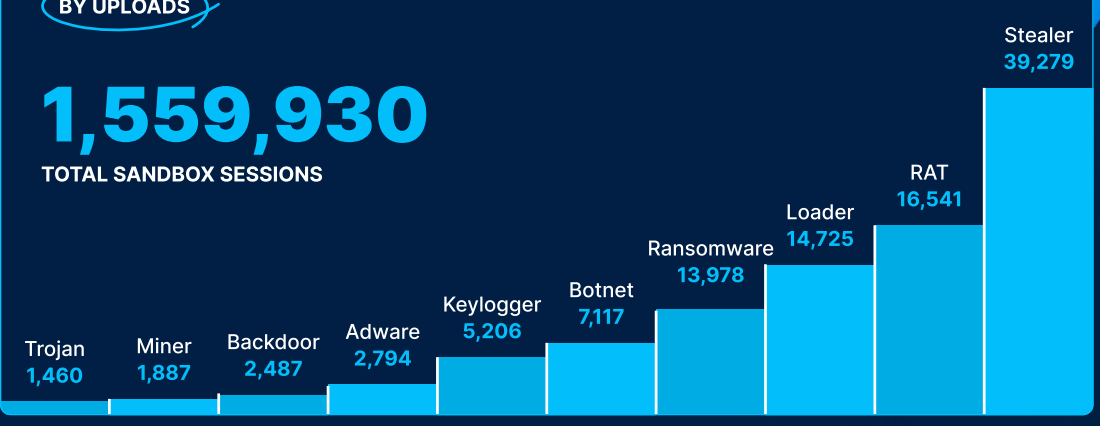
Malicious 336,157 | Suspicious 117,860 | IOCs 842,985,543

## Top malware types from Q2 2025

ANY.RUN

BY UPLOADS

**1,559,930**
TOTAL SANDBOX SESSIONS

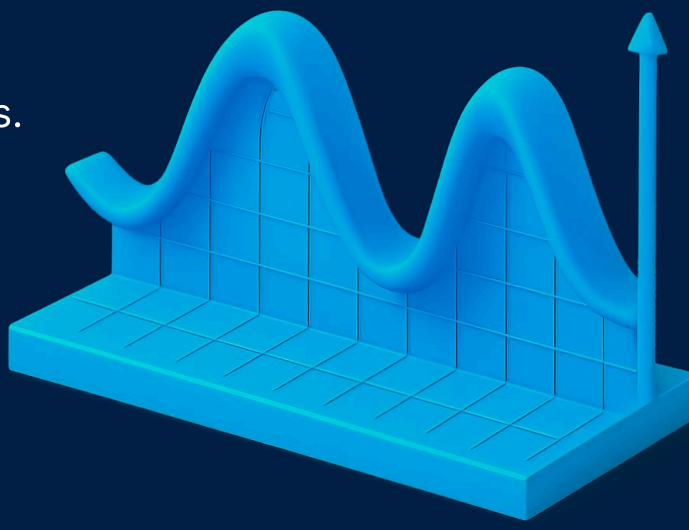


# Table of contents

This report offers essential stats for staying informed about the current threat landscape, covering everything from top malware families to phishing APTs.

The data comes from sandbox analyses in ANY.RUN's Interactive Sandbox run by a global network of 500K analysts and 15K organizations across numerous industries.

Discover the key trends of Q2 2025 and compare them to the Q1 report.



# Summary

*Users launched over 1.5M sandbox sessions in Q2 2025*

## Q2 2025 REVIEW

BY UPLOADS

**TOTAL SANDBOX SESSIONS: 1,559,930**

Malicious 336,157 | Suspicious 117,860 | IOCs 842,985,543

As expected, the scale of threats overall grew. In Q2, users ran over one and half a million sandbox analyses of suspicious files and URLs —1,559,930. The rise compared to the previous quarter equals 9.8%.

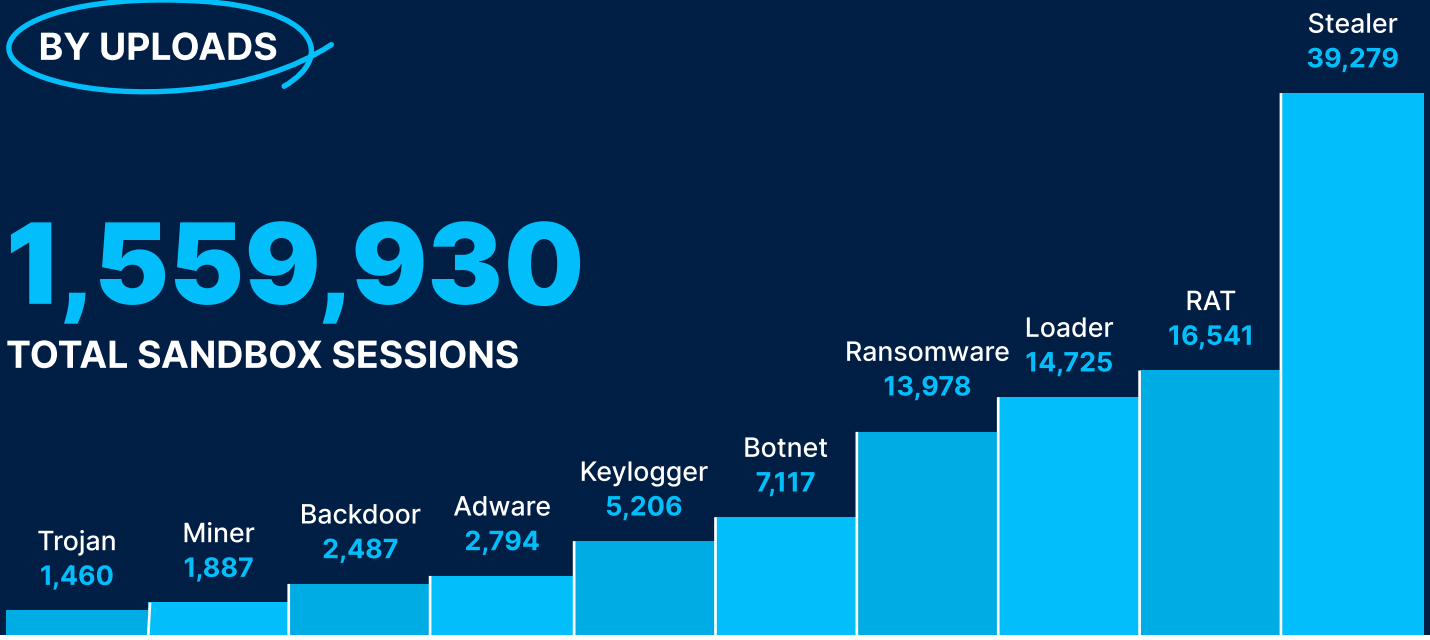
The number of malicious verdicts on these samples significantly increased, too. 336,157 samples were tagged as malicious as compared to 279,515 last quarter.

In total, across these sessions the sandbox extracted 842,985,543 indicators of compromise (IOCs) during Q2 2025, as compared to 829,559,331 in the previous quarter.

# Top Malware Types

BY UPLOADS

**1,559,930**
TOTAL SANDBOX SESSIONS




## Top Malware Types: Highlights

Top four positions remain the same as earlier this year, but their order and activity levels underwent some changes:

### STEALERS

This malware type remains a leader. Its frequency grew by **9%** and reached **39,279** detections.

### LOADERS

Still staying amongst leaders, they were less widespread. The number of detections went from **15,523** to **14,725**.

### RATS

They went from third place in Q1 to second in Q2 with **16,541** detections (**+3,394**).

### RANSOMWARE

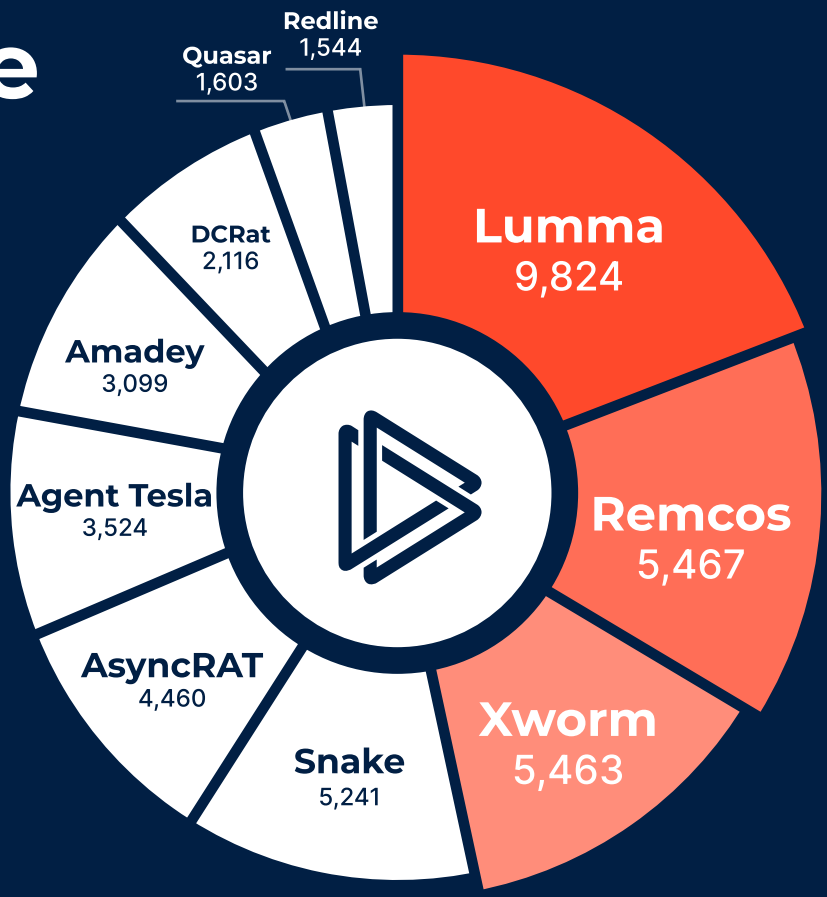
With **13,978** (**+3,593**) detections, it concluded the top four, like in Q1.

Next on the list are Botnets with 7,117 (+1,845) and Keyloggers with 5,206 (+66) detections. They secured their fifth and sixth places with increased activity levels.

The bottom part of the chart changed more noticeably. Adware went from ninth to seventh place with 2,794 detections (+50%). Backdoors went one place lower and took eighth place, although they were detected more often than before (2,487 in Q2 vs 2,089 in Q1).

Miners are a new introduction to the list with 1,887 detections. They conclude the list along with Trojans (1,460 detections).

# Top Malware Families




- Lumma still holds first place with a 19% increase in the number of detections.
- Remcos jumped from fifth to second place: it was detected 5,467 times. In Q1, this number was much lower—3,881.
- Xworm's activity, on the contrary, decreased, but it still holds a place in the top 3. This quarter it was detected 5,463 times (-1,136).

As for other families, their number of detections grew, except for Stealc. It was detected 1,554 times last quarter, but less than that in Q2, as it didn't make it to the top 10 list. Its ninth place was taken by Quasar that went up one place with 1,603 detections.

One malware family that wasn't present in the list in the previous quarter is Redline. In Q2, however, it was detected 1,544 times and concluded the top.

# Top TTPs

Let's move on to tactics, techniques, and procedures used by adversaries. The top 20 list, as usual, indicates significant changes.

| # | MITRE ATT&CK Technique | Detections |
|---|---|---|
| 1 | Impair Defenses: Disable Windows Event Logging, T1562.002 | 95,736 |
| 2 | Virtualization/Sandbox Evasion: Time Based Evasion, T1497.003 | 62,160 |
| 3 | Masquerading: Rename Legitimate Utilities, T1036.003 | 60,520 |
| 4 | Subvert Trust Controls: Install Root Certificate, T1553.004 | 48,575 |
| 5 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, T1547.001 | 45,515 |
| 6 | Virtualization/Sandbox Evasion: System Checks, T1497.001 | 37,446 |
| 7 | Scheduled Task/Job: Scheduled Task, T1053.005 | 35,547 |
| 8 | OS Credential Dumping: /etc/passwd and /etc/shadow, T1003.008 | 29,889 |
| 9 | Unsecured Credentials: Credentials In Files, T1552.001 | 29,817 |
| 10 | System Services: Service Execution, T1569.002 | 24,709 |
| 11 | File and Directory Permissions Modification: Financial Theft, T1222.002 | 24,337 |
| 12 | Credentials from Password Stores: Credentials from Web Browsers, T1555.003 | 23,643 |

CONTINUED

| | | |
|---|---|---|
| 13 | Masquerading: Match Legitimate Resource Name or Location, T1036.005 | 22,145 |
| 14 | Phishing: Spearphishing Link, T1566.002 | 21,063 |
| 15 | Impair Defenses: Disable or Modify Tools, T1562.001 | 20,871 |
| 16 | System Binary Proxy Execution: Rundll32, T1218.011 | 16,996 |
| 17 | Software Discovery: Security Software Discovery, T1518.001 | 12,054 |
| 18 | Hide Artifacts: Hidden Window, T1564.003 | 11,023 |
| 19 | File and Directory Permissions Modification: Windows File and Directory Permissions Modification, T1222.001 | 8,858 |
| 20 | Indicator Removal: File Deletion, T1070.004 | 8,349 |

## Top TTPs: Q2 2025 vs Q1 2025

Among TTPs, the leaders of the list were:

- **T1562.002** - Impair Defenses: Disable Windows Event Logging. This TTP holds first place with 95,736 detections.
- **T1497.003** - Virtualization/Sandbox Evasion: Time Based Evasion. It took second place. ANY.RUN detected it 62,160 times.
- **T1036.003** - Masquerading: Rename Legitimate Utilities. Concluding the top 3 list of most widespread TTPs, this technique had 60,520 detections.

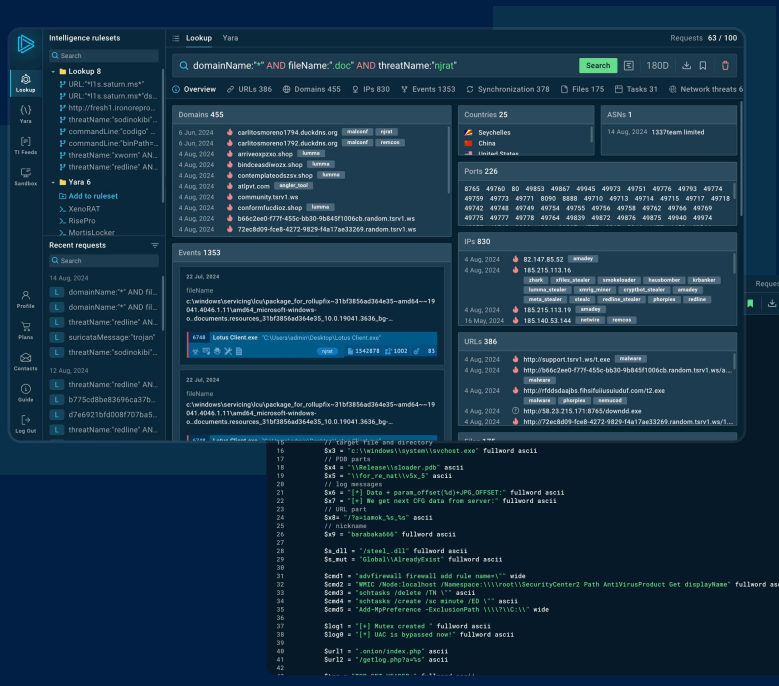
# Other notable changes

- **T1547.001** – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder jumped from twelfth place to fifth. Compared to Q1, it was detected 3.5 times more often (45,515 detections).
- A total of 15 out of 20 top TTPs were not mentioned in the Q1 report. This highlights the fact that threat actors constantly switch between tactics, techniques, and procedures.
- To ensure proactive security of your infrastructure against evolving threats, use ANY.RUN's TI Lookup to observe TTPs in fresh, real-world malware samples.

# Collect Fresh Threat Intelligence with TI Lookup

TI Lookup offers a searchable database of fresh Indicators of Compromise (IOCs), Attack (IOAs), and Behavior (IOBs) belonging to the latest cyber attacks on 15,000 companies.

- **Speed up investigations:** Pin 40 types of indicators to actual threats in seconds.
- **Respond faster:** Get actionable threat info to streamline containment.
- **Adapt to evolving threats:** Enrich your detection capabilities with fresh data.




Try now. It's free →

# Phishing Activity in Q2 2025

The phishing threats saw a slight decline in activity. In Q1 2025, their total number was 107,793. In the second quarter of 2025 it decreased by 2.5% to 104,704 detections.

**107,793** OVERALL ACTIVITY BY UPLOADS

**ACTIVITY OF CYBERCRIMINAL GROUPS**

| | |
|---|---|
| STORM-1747 | 14,017 |
| TA569 | 1,781 |
| TA558 | 363 |
| STORM-1575 | 103 |
| TA582 | 70 |

## Activity by cyber criminal groups

### STORM-1747

This group continued to dominate the list. Although its number of detections decreased by 13%, still, it was detected a significant number of times—14,017.

### TA569

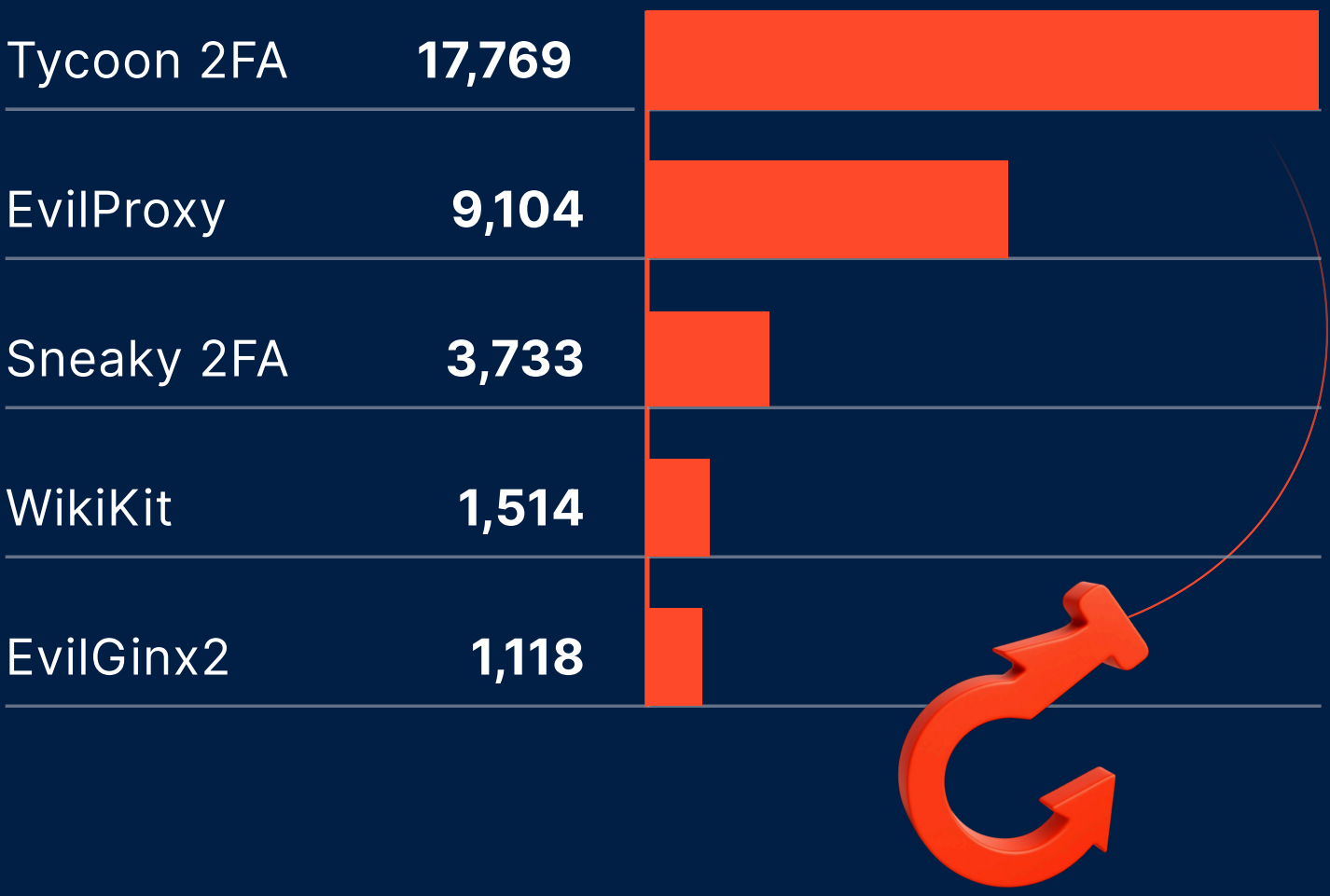
Second place is also taken by the same group as in Q1. It was detected 1,781 times (+776).

### TA558

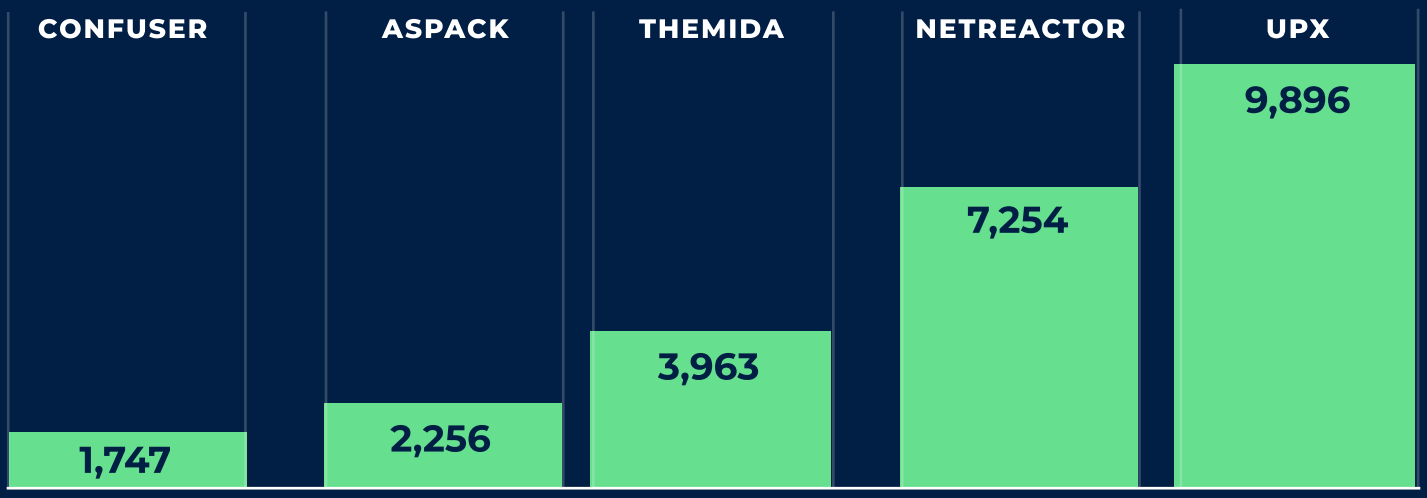
A new leader on the list. It showed no noticeable activity in the previous quarter, but in Q2 was detected 363 times, ending up in third place.

# Activity by phishing kits

- Tycoon 2FA experienced a drop in activity by 17% and yet remained at the top of the list. It was detected 17,769 times, which is still a staggering number compared to other phishing kits.
- Keeping its second place, EvilProxy demonstrated strong growth: its number of detections almost doubled (9,104 vs last quarter's 4,743).
- Third place remained occupied by Sneaky2FA, just like in Q1 2025. Its detections number is 3,733, which is 2.5 times higher than before.
- **WikiKit** with 1,514 detections went one step higher than previously and ended up in fourth place.
- **EvilGinx2** concludes the top with 1,118 detections (+27).



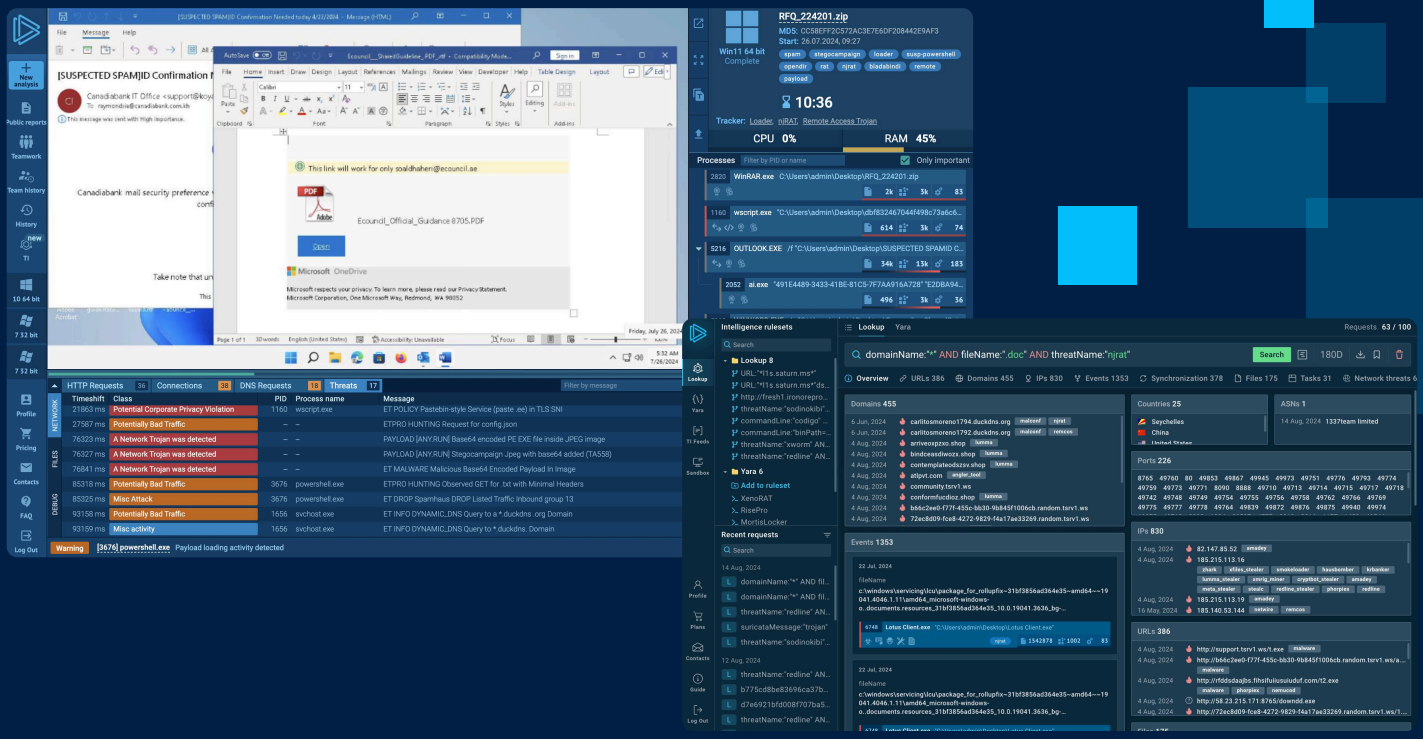
# Top Protectors and Packers




The list of top protectors and packers used by threat actors to evade malware detection in Q2 2025 includes:

| | |
|---|---|
| **UPX** | Still leading the chart, it was detected more often: 9,896 times (15% growth). |
| **NETReactor** | Also secured its place with an increased detection number: 7,254 as compared to just 4,917 last quarter. |
| **Themida** | Like in Q1, it concludes the top three. ANY.RUN detected it 3,963 times. |
| **ASPack** | With a doubled activity (2,256 detections vs 1,092), it moved from fifth to fourth place. |
| **Confuser** | The only new addition to this list. It was detected 1,747 times. |

# Build Better Security with ANY.RUN



ANY.RUN's services are used by more than 500,000 cybersecurity professionals and SOC teams at over 15,000 companies across different industries, including finance, manufacturing, healthcare, and technology.

The Interactive Sandbox helps businesses ensure fast and accurate analysis of threats targeting Windows, Linux, & Android systems. It provides capabilities for hands-on and in-depth investigations of complex malware and phishing scenarios.

Threat Intelligence Lookup enables organizations to enrich their knowledge on active cyber attacks, while TI Feeds allow businesses to expand threat coverage and detection.

Integrate ANY.RUN to stay ahead of threats →