RomCom and TransferLoader IoCs in the Spotlight

By By WhoisXML API (Sponsored Post)

Archived: 2026-04-05 13:40:58 UTC

Proofpoint released "10 Things I Hate about Attribution: RomCom vs. TransferLoader" detailing connections between RomCom and TransferLoader. While the researchers said the backdoors were typically used by different groups—RomCom by TA829 and TransferLoader by UNK_GreenSec, they did see similarities between the threat actors' campaigns.

WhoisXML API further analyzed the campaign infrastructures, specifically the domains used in the attacks, to spot even more similarities and uncover new artifacts. Our analysis comprises two parts.

The first part covered our search for typosquatting domains and unraveling similarities between them and the 109 domains identified as indicators of compromise (IoCs)—20 for RomCom and 89 for TransferLoader. Our search led to these findings:

- Four domain IoCs appeared in five typosquatting groups
- Each typosquatting group had 3—8 domains, including one IoC
- Typosquatting domain groups were spotted between 650 days before and one day after their current WHOIS record creation dates

The second part, meanwhile, covered our search for more insights on the 109 domains identified as IoCs along with new connected artifacts. Our investigation led to these discoveries:

- 19 domain IoCs were deemed likely to turn malicious upon registration 77-271 days prior to reporting date
- 3,051 email-connected domains, 28 were malicious
- 28 IP addresses, 27 were malicious
- 17 IP-connected domains
- 1,682 string-connected domains, 24 were malicious

A sample of the additional artifacts obtained from our analysis is available for download from our website.

Part 1: Uncovering Typosquatting Domains

We began our analysis by looking for domains that not only looked similar to those tagged as IoCs but were also registered in bulk along with the IoCs on Typosquatting Data Feed. We discovered that four domains tagged as IoCs, all tied to TransferLoader, were part of five typosquatting groups. They were included in feed files from June 2023 to April 2025.

DOMAIN IoC	MALWARE	TYPOSQUATTING DATA FEED FILE DATE
1day[.]live	TransferLoader	23 June 2023

1day[.]live	TransferLoader	29 September 2023
1drive[.]expert	TransferLoader	14 February 2025
dr365[.]live	TransferLoader	21 February 2025
livestorage[.]click	TransferLoader	15 April 2025

Upon closer scrutiny, we discovered that each group of domains had 3-8 domains each with one being an IoC. Take a look at a sample typosquatting group below with the IoC 1day[.]live.

date	group_number	group_member_number	total_no_of_grp_members	domain	registrant_country	registrarName	nameServers	IPs
9/29/23	237	1	8	1day[.]one	UNITED STATES	GoDaddy.com, LLC	pdns04.domaincontrol.com|pdns03.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	2	8	1day[.]fyi	UNITED STATES	GoDaddy.com, LLC	pdns09.domaincontrol.com|pdns10.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	3	8	1day[.]live	UNITED STATES	GoDaddy.com, LLC	pdns05.domaincontrol.com|pdns06.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	4	8	1day[.]zone	UNITED STATES	GoDaddy.com, LLC	pdns03.domaincontrol.com|pdns04.domaincontrol.com|	15.197.148.33 3.33.130.190
9/29/23	237	5	8	1day[.]ltd	UNITED STATES	GoDaddy.com, LLC	pdns11.domaincontrol.com|pdns12.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	6	8	1day[.]ventures	UNITED STATES	GoDaddy.com, LLC	pdns05.domaincontrol.com|pdns06.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	7	8	1day[.]support	UNITED STATES	GoDaddy.com, LLC	pdns13.domaincontrol.com|pdns14.domaincontrol.com|	3.33.130.190 15.197.148.33
9/29/23	237	8	8	1day[.]biz	UNITED STATES	GoDaddy.com, LLC	pdns12.domaincontrol.com|pdns11.domaincontrol.com|	3.33.130.190 15.197.148.33

Note similarities between the IoC (i.e., highlighted in yellow) and the seven look-alike domains in terms of registrant country, registrar, and NS provider. All eight domains in the group also shared two IP addresses.

An even deeper dive into the typosquatting results showed a number of similarities between the 28 domains (i.e., four IoCs and 24 look-alikes). Note that the IoC 1day[.]live was mentioned twice because it was bulk-registered with two groups—one on 23 June 2023 and the other on 29 September that same year.

CREATION DATE	**REGISTRAR**	**REGISTRANT COUNTRY**
23 June 2023	Google	Canada
29 September 2023	GoDaddy	U.S.

We summed up details for the four domains tagged as IoCs and the five typosquatting groups they belonged to below.

- 1day[.]live appeared in two groups. The first group comprising three domains was created on 23 June 2023 in Canada under Google. All of their NSs were also provided by Google. The second group, meanwhile, comprised eight domains created on 29 September 2023 in the U.S. under GoDaddy. All of their NSs were provided by Domain Control. Interestingly, the domains in the second group also shared two IP addresses —3[.]33[.]130[.]190 and 15[.]197[.]148[.]33—for around 13 months (i.e., September 2023—October 2024) based on the results of an additional DNS history lookup.
- 1drive[.]expert appeared in a group comprising six domains created on 14 February 2025. While one domain did not have a registrant country on record, the remaining five were split into two countries. Three were registered in the U.S. and one in China. The six domains were also administered by three registrars—three under Tucows, two under Alibaba, and one under Shanghai Fuhu Information Technology. Lastly, they were split across three NS providers—three under System DNS, two under HiChina, and one under DNS.com. Note that two other look-alike domains shared the IoC's registrant country, registrar, and NS providers. Also, two look-alike domains shared the IoC's IP address—52[.]72[.]49[.]79—for around five months (i.e., May—October 2021) according to an additional historical DNS lookup.

- Dr365[.]live appeared in a group with four domains created on 21 February 2025. While one domain did not have a registrant country on record, the remaining three domains were split among three countries. One each was registered in China, Iceland, and the U.S. The four domains were administered by three registrars—two by Spaceship and one each by Tucows and Snapnames 94. They were split across three NS providers—two under Cloudflare and one each under Juming and System DNS.
- Livestorage[.]click appeared in a group comprising seven domains created on 15 April 2025 in three countries. Four were registered in Japan, two in the U.S., and one in China. The seven domains were administered by four registrars—four by GMO Internet Group and one each by DNSPod, Tucows, and Wix. They were split across five NS providers—three under Onamae and one each under AfterNIC, DNSPod, System DNS, and Wix.

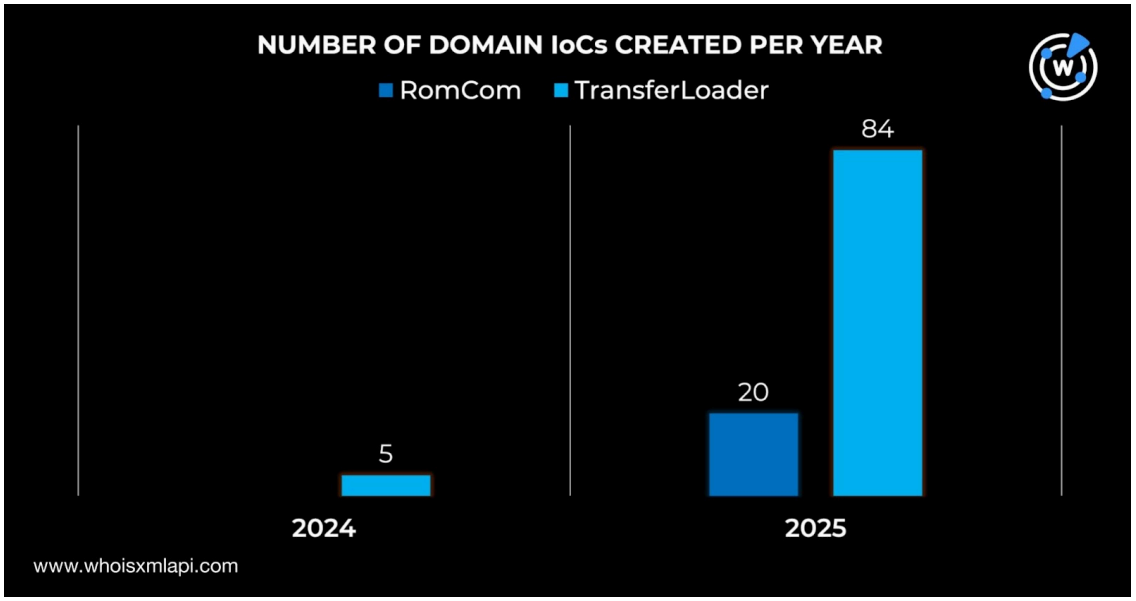
It is also worth noting that three typosquatting groups related to the IoCs 1drive[.]expert, dr365[.]live, and livestorage[.]click shared the U.S. as registrant country, Tucows as registrar, and System DNS as NS provider, hinting at a shared infrastructure.

Finally, we obtained the current WHOIS records of the four domains tagged as IoCs that appeared in typosquatting data feed files via Bulk WHOIS API and found out that three of them—1drive[.]expert, dr365[.]live, and livestorage[.]click—appeared on the feed a day after their current WHOIS record creation date. 1day[.]live, meanwhile, appeared 650 and 552 days before its current creation date.

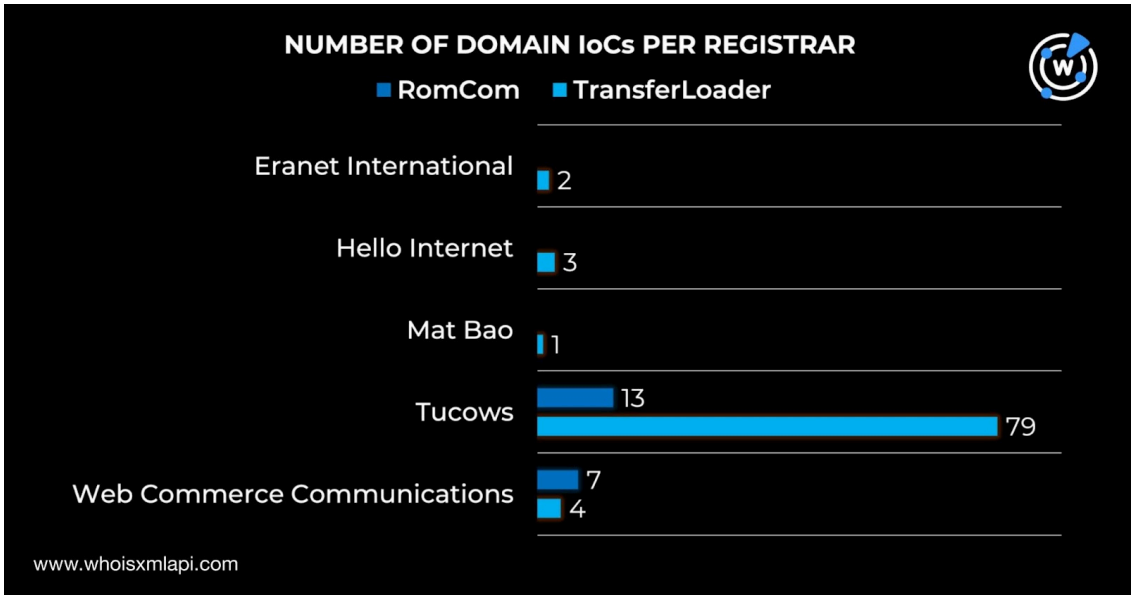
DOMAIN IoC	TYPOSQUATTING DATE	CURRENT WHOIS RECORD DATE
1day[.]live	23 June 2023	3 April 2025
1day[.]live	29 September 2023	3 April 2025
1drive[.]expert	14 February 2025	13 February 2025
dr365[.]live	21 February 2025	20 February 2025
livestorage[.]click	15 April 2025	14 April 2025

Part 2: Discovering Connected Artifacts

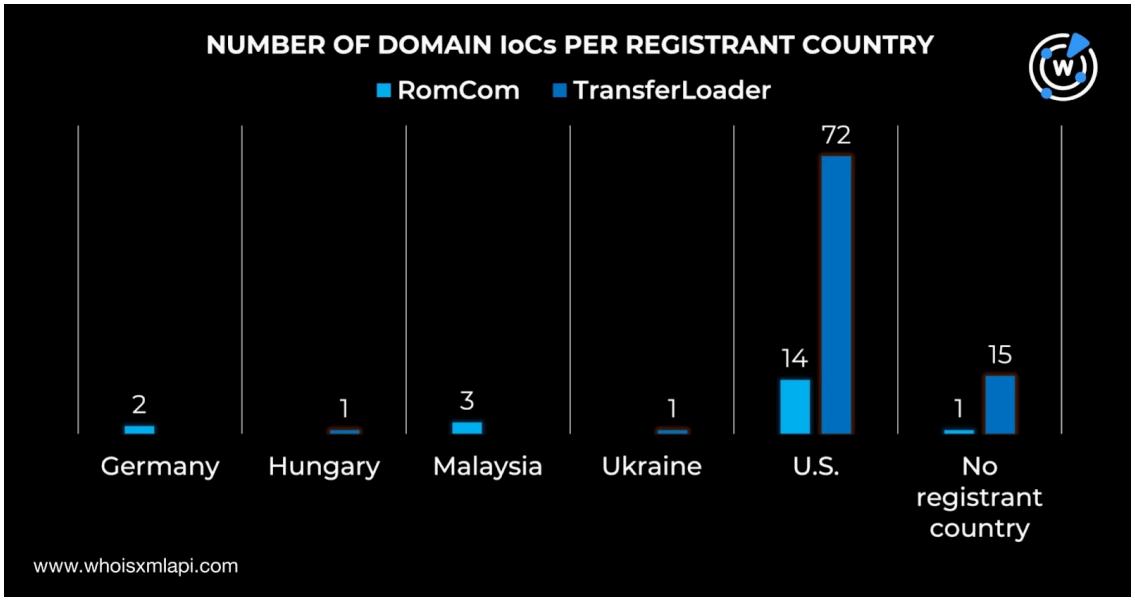
We started our search for connected artifacts by querying the 109 domains tagged as IoCs on Bulk WHOIS API and found out that they all had current WHOIS records. Upon closer examination, we discovered that they were likely fairly newly registered when they figured in attacks. Specifically, all of the 20 RomCom domains were created in 2025, specifically between 20 January and 11 June 2025. The 89 TransferLoader domains, meanwhile, were created between 2024 and 2025, particularly between 2 October 2024 and 14 April 2025.



The 20 RomCom domains tagged as IoCs were split across two registrars—13 under Tucows and seven under Web Commerce Communications. The 89 TransferLoader IoCs, meanwhile, were administered by five registrars—79 by Tucows, four by Web Commerce Communications, three by Hello Internet, two by Eranet International, and one by Mat Bao.



While one RomCom IoC did not have a registrant country on record, the remaining 19 were registered in three countries—14 in the U.S., three in Malaysia, and two in Germany. Fifteen TransferLoader IoCs did not have registrant countries on record as well. The remaining 74 were registered in three countries—72 in the U.S. and one each in Hungary and Ukraine.



We then checked if any of the 109 domains tagged as IoCs appeared on First Watch Malicious Domains Data Feed. We discovered that 27 domains—24 for TransferLoader and three for RomCom—were deemed likely to turn malicious upon registration. Specifically, they appeared on the feeds 77—271 days prior to being reported as IoCs on 30 June 2025.

This post only contains a snapshot of the full research. Download the complete findings and a sample of the additional artifacts on our website or contact us to discuss your intelligence needs for threat detection and response or other cybersecurity use cases.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*
