Tricky Trickbot Runs Campaigns Without Redirection

By Authors & Contributors

Archived: 2026-04-05 20:27:39 UTC

- During June and July, F5 researchers first noticed Trickbot campaigns aimed at a smaller set of geographically oriented targets and did not use redirection attacks—a divergence from previous Trickbot characteristics.
- In this research, we compared two different target configurations, one older, more “traditional” configuration that uses redirection, and a new Trickbot configuration that does not us redirection and exclusively uses dynamic injection.
- The vast majority of all spotted Trickbot campaigns target US financial services institutions; a much smaller percentage target other industries, including cryptocurrencies, credit card companies, and e-commerce.
- Notably, the access pages of financial services institutions, including single sign-on pages, are the most targeted, which indicates that access is still imperative in order to conduct lucrative cybercriminal attacks.

Trickbot, one of today’s most active banking trojans, was first reported on in 2016. It was originally known for its geographically centered campaigns targeting only the financial services industry. But it quickly expanded its targets to include credit card, wealth management, customer relationship management software companies. (For more background on Trickbot, check out the F5 Labs banking malware reference guide (/content/f5-labs-v2/en/archive-pages/education/banking-trojans-a-reference-guide-to-the-malware-family-tree.html).)

Since 2016, Trickbot campaigns have continued to evolve. New campaigns are pivoting to be much more regionally focused, and they exploit using only one type of attack: dynamic Injection (Dinj), also known as server-side injection. The details of these attacks are stored in Dinj files. While the dynamic injection technique isn’t new, it is the first time it has been applied by Trickbot in such a geographically centered campaign.

Over the last few months, F5 researchers have gathered target configuration files from Trickbot campaigns and, for this analysis, compared two of the most different ones. (Note that the traditional Trickbot configuration we analyzed has not been active over the last four months.) Since there is such a stark difference in Trickbot’s current tactics, we used the older configuration as a comparison, which highlights Trickbot’s transition to attacking without redirection, because it is so much more sophisticated. The configurations we compared are v459, composed of new Trickbot tactics of shorter target lists and no redirection, and v420, a more traditional configuration that utilizes both redirection and dynamic injection attacks and has a very long target list.

Active Campaigns Without Redirection

Historically known for using redirection attackA user is forwarded from a trusted site to another, possibly malicious site.s, Trickbot is not using this tactic in some of its latest target configurations. This change, first

noticed by F5 researchers in June and July, continues in August and September 2019. Along with the absence of target lists, redirection is also absent in the encrypted webinject files from the latest campaigns. There is no trace of the previous redirection targets alongside Dinj elements. While this seems to be an intentional shift in tactics, Trickbot continues to target the financial services industry, with 91% of targets on the v459 target list falling into this industry.

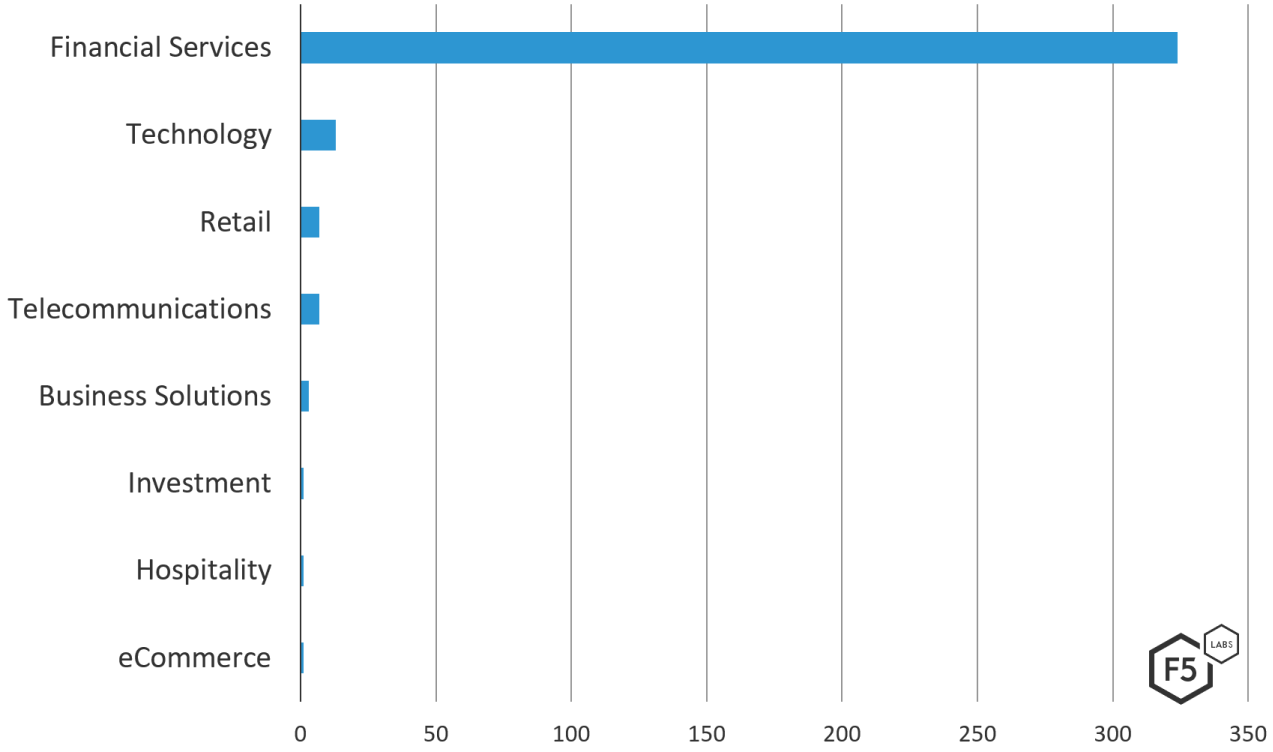

Figure 1. Industries targeted in the Trickbot v459 configuration

Breaking down the financial services industry further, these campaigns using dynamic injection are mostly continuing to target banking institutions and investment arms of banks.

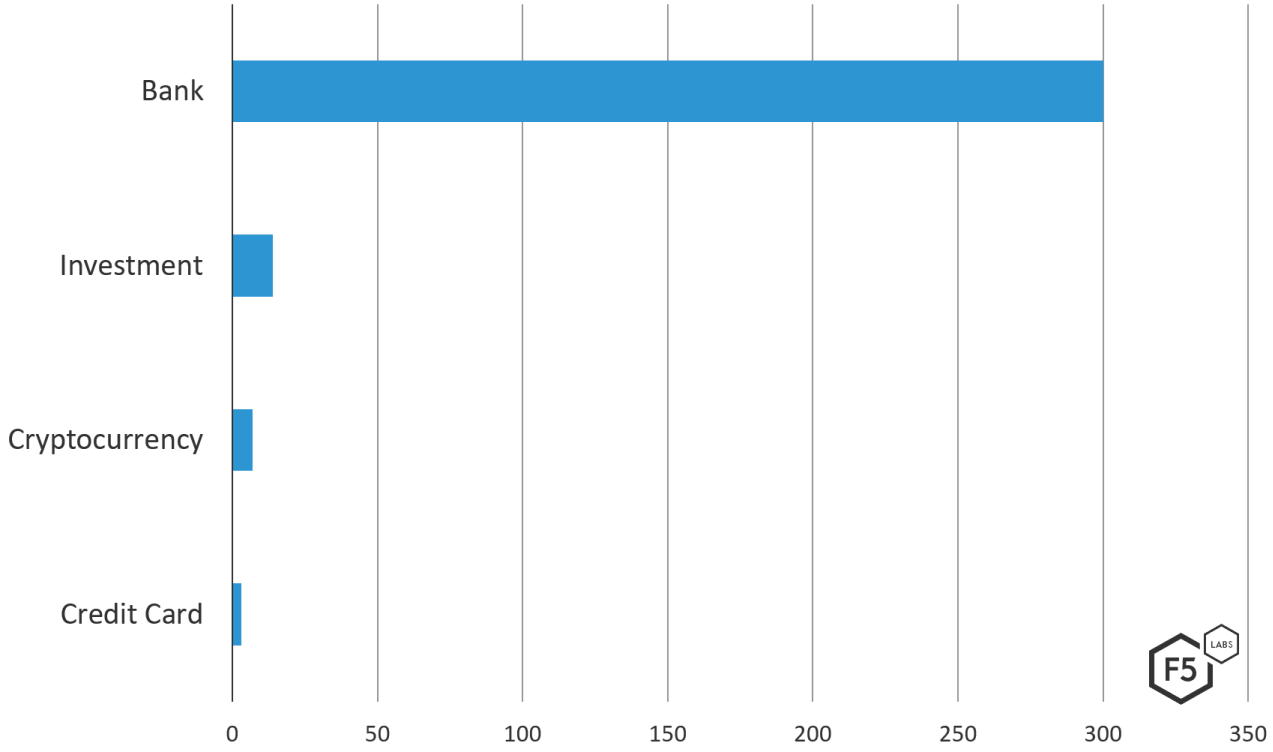

Figure 2. Breakdown of Trickbot v459's dynamic injection targets in the financial services industry

We postulate that Trickbot continues to target financial services with a narrow scope since server-side injection is a dynamic injection technique and needs to be very precise. Dynamic injection needs to make sure the injected content doesn't break legitimate page behavior, and it must take into account that there could be other scripts defending the target page. This is an expensive attack, both in time to set up and insight needed about the target page infrastructure, which helps to explain the whittled down target list for campaigns using only this dynamic injection technique. It is also possible that the v459 target list is under maintenance, with targets that have performed poorly in past campaigns being culled out.

The current campaigns we sampled didn't use redirection attacks. The geographic targeting is clearly against the U.S.

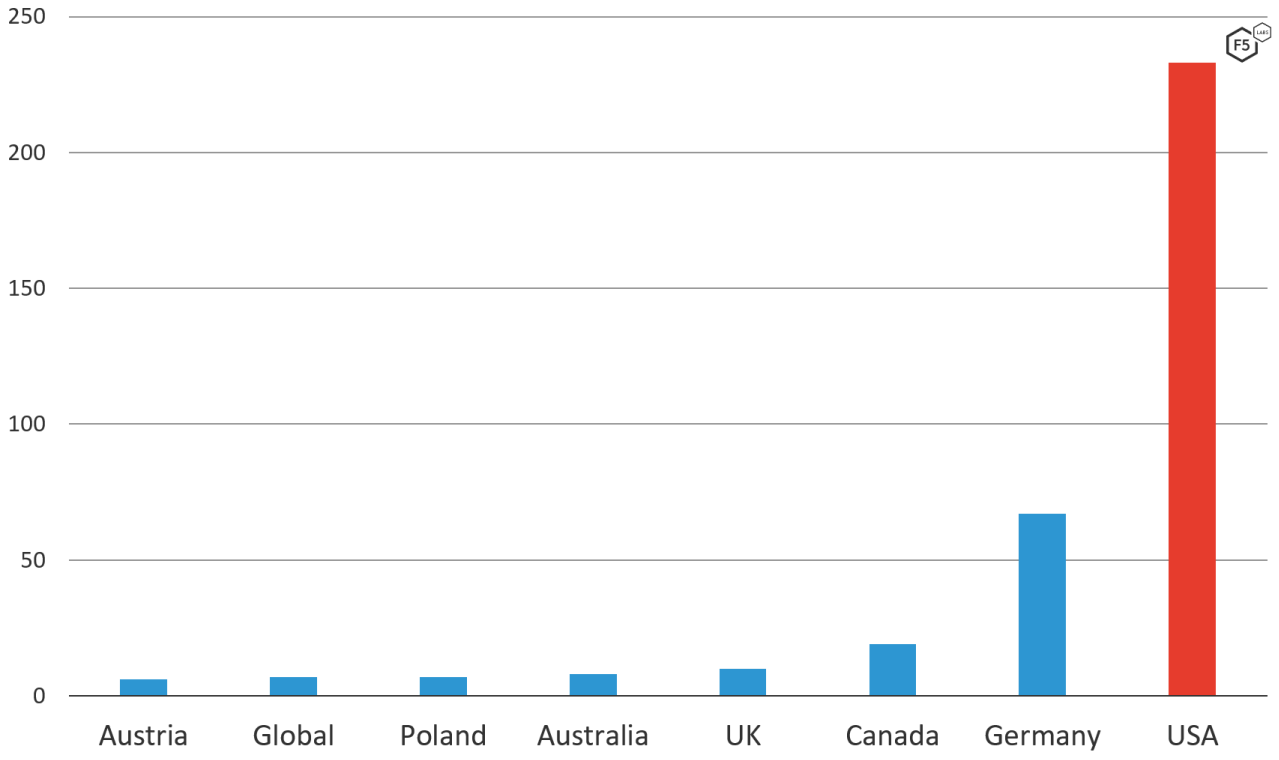

Figure 3. Trickbot v459 target list by geolocation, broken out by country

Active Campaigns With Redirection

As stated earlier, the v420 Trickbot campaign utilizes traditional Trickbot tactics. Geographically, the top targeted countries are similar, but the v420 campaign has a broader reach, attempting to target users either logging into banks around the world or users based in certain locations for global institutions. Further, v420 has a much longer target list with 1,135 unique URIs, compared with v459's 360 unique URIs. Along with that, the v420 target list casts a larger net. There are more smaller financial services institutions that are geographically dispersed. Along with the clear industry targeting included in the target list are a number of general extensions, redirection attempts, or URLs that do not resolve.

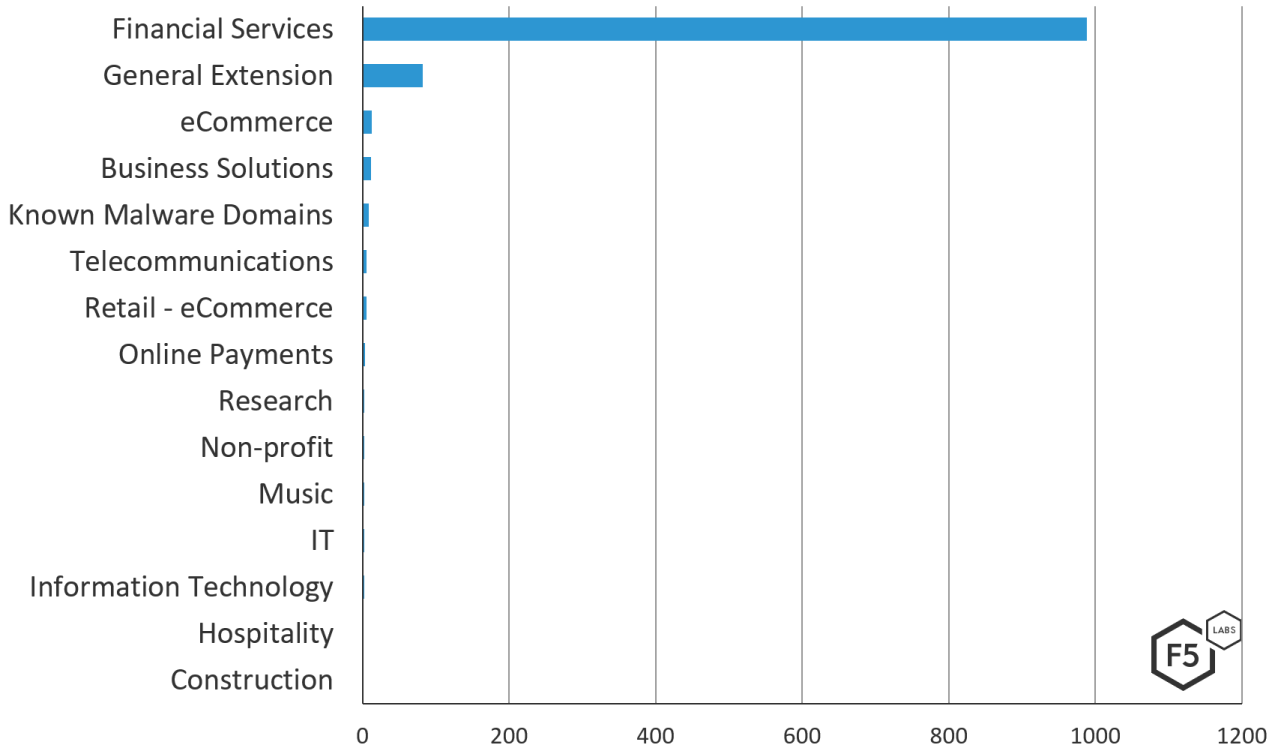

Figure 4. Trickbot v420's targeted industries by unique URL targeted

Similar to the v459 target configuration, when the financial services industry is broken out by segment, banks and investment banks are heavily targeted. Cryptocurrency exchanges also make up a portion of this list, which makes sense, due to their anonymity. Notably, due to the larger list size and the focus on Italy and Italian financial consulting firms, there is a broader spread in subindustry across the financial services industry.

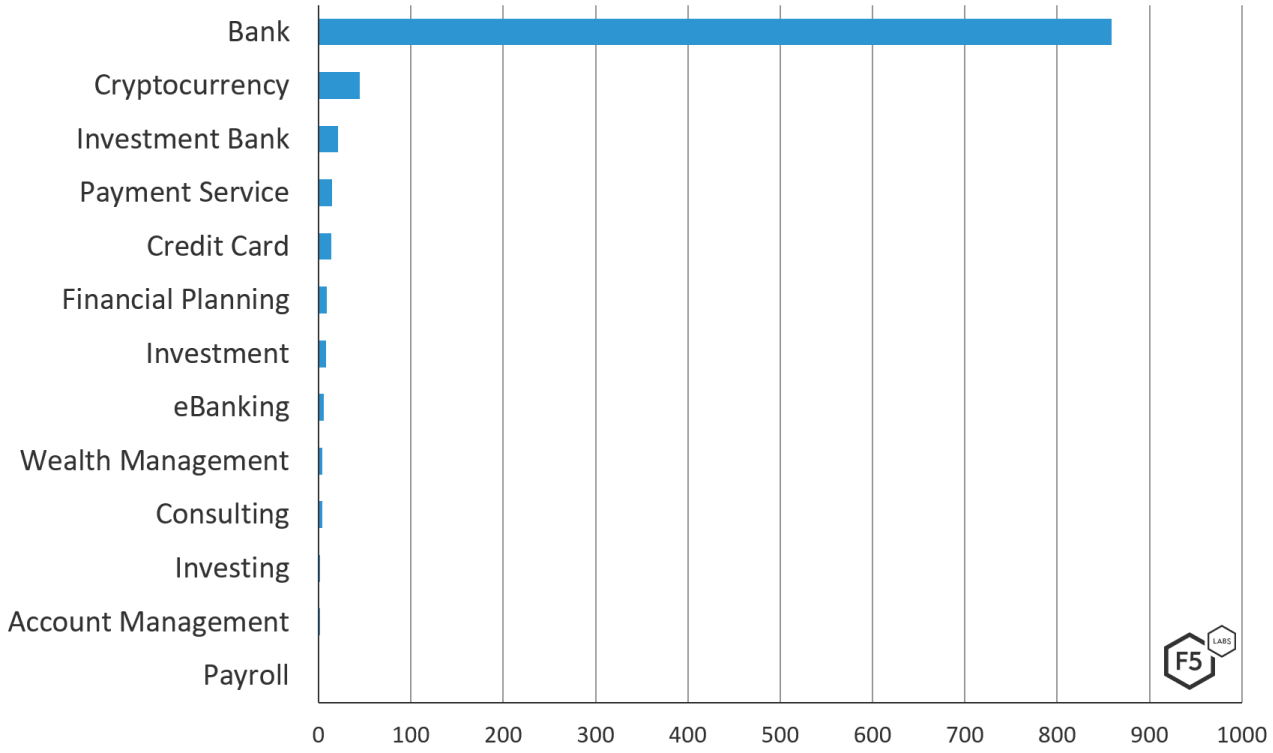

Figure 5. Trickbot v420 breakdown of the financial services industry by unique URL targeted

Geographically, the Trickbot v420 target file is more scattered than the v459 target file—not really targeting regionally, but targeting wealthy countries or countries known for their relaxed banking laws. Notably, Russia and China do not appear on this list at all. As of this analysis, Trickbot does not have official attribution to either a country or a group, and the list of nations not on this list may be telling.

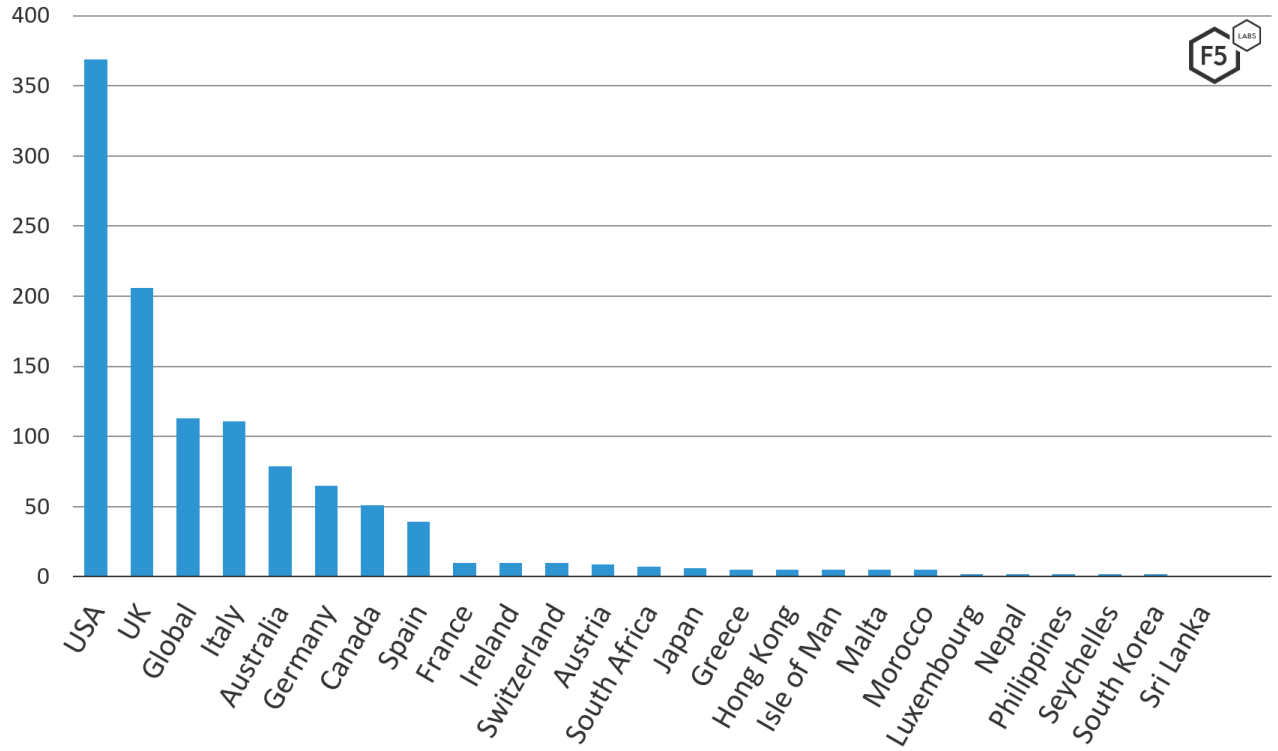

Figure 6. Trickbot v420 target list geographic distribution showing unique URLs targeted by country

Further breaking down the “global” category of the geographic distribution from the v420 configuration, there were a number of URLs. Most URLs are general extensions/redirection attempts, which mean that they do not target one website specifically; instead, they are meant as a catchall. These were not seen in the same volume in the v420 configuration. Along with that, cryptocurrency exchanges are categorized as targeting a global market instead of an individual country anyone in the world can access them.

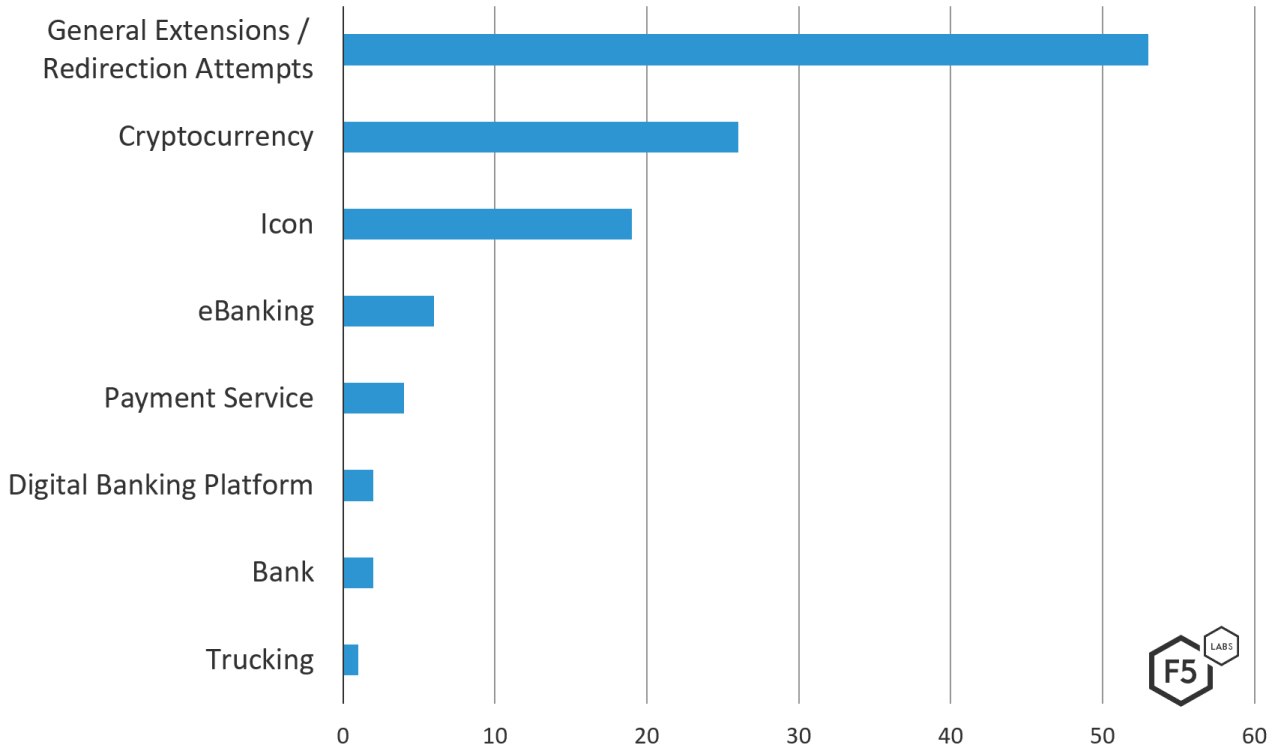

Figure 7. Breakdown of Trickbot v420 global targets by specific industry

Overall, the Trickbot v420 and the v459 target files are similar in that they both heavily target financial services institutions and are geographically centered around the US. Digging a little deeper, the Trickbot v459 target list seems to be a more focused version of the v420 target file.

The behavior exhibited from the v420 target list is much more of a traditional Trickbot campaign and is more representative of the direction, based on previous behaviors, in which analysts thought Trickbot seemed to be going. F5 threat researchers speculate that the recent change could be in defense of some action taken against the malware's authors or supporting infrastructure.

How Banks React

Targeting users is not uncommon. Banks have known from inception of the Internet that they would be an obvious target for attackers. In response, banks have hardened their websites to the point where the best way in is through a human. So instead of attacking the bank's website, malicious actors go after users. On the target files analyzed, many of the targets are specific access points to the institution. Notably, some banks that were on the v420 target list have acknowledged this publicly and warn users about this danger.

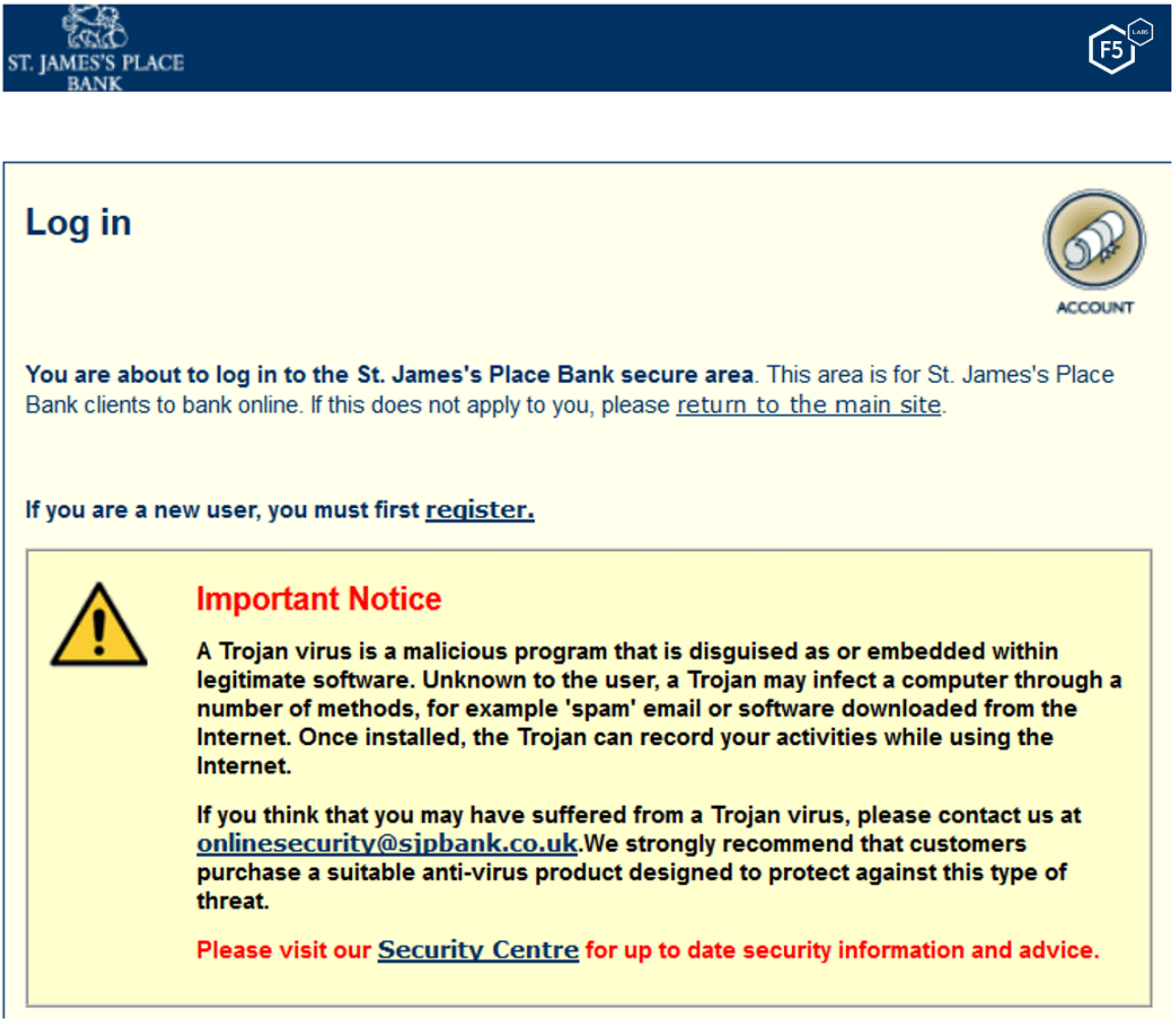

Figure 8. Example of a bank warning users about Trickbot and other banking trojans

The example shown in Figure 8 is from a bank only seen in the v420 target list, but these warnings are not only put out by smaller institutions. Banks need to find ways to let users know who to trust and make them aware of the resources available to them. Making sure this information is on the page of Google search results helps them to try to keep users safe.

Conclusion

Researchers can only speculate why Trickbot has dropped the redirection attack vector in some of its newest, active campaigns. The v459 target list is much more focused and may be under maintenance, to just fixate on the top preforming targets. Researchers hypothesize that this may be due to the need for a lot of computing power and servers to support the large waves of spam campaigns—and to keep steady pressure on infected users in order to steal money. Whatever the reason for the change, Trickbot remains an active and engaged threat to financial services institutions and their users.

Security Controls

The following security controls (/content/f5-labs-v2/en/archive-pages/education/what-are-security-controls.html) are recommended in order to mitigate these malware attacks.
