WhoisXMLAPI

Scoping the Domain Asset Surface of Today’s Most-Impersonated Brand (Hint: That’s a Bank)

Posted on August 26, 2021

Microsoft often lands at the top of global lists of most-impersonated brands over time. But that’s not always the case as per this research by Vade in which Crédit Agricole was identified as phishers’ favorite.

Building on this finding, we took a closer look at look-alike DNS Internet assets to check if they could be possible contributors to Crédit Agricole becoming a favored phishing target. By scoping part of its DNS attack surface, we hope to shed more light on the subject from a domain registration perspective. Could the volume of typosquatting domains have anything to do with the occurrence?

Crédit Agricole Domain Registration Trend

Using Domains & Subdomains Discovery, we obtained a sample of the domains and subdomains that contain various combinations of the strings “credit” and “agricole” to determine how big the bank’s potential attack surface might be.

Our data set comprised 3,159 domains and 2,602 subdomains registered as early as 1995 up to the present.

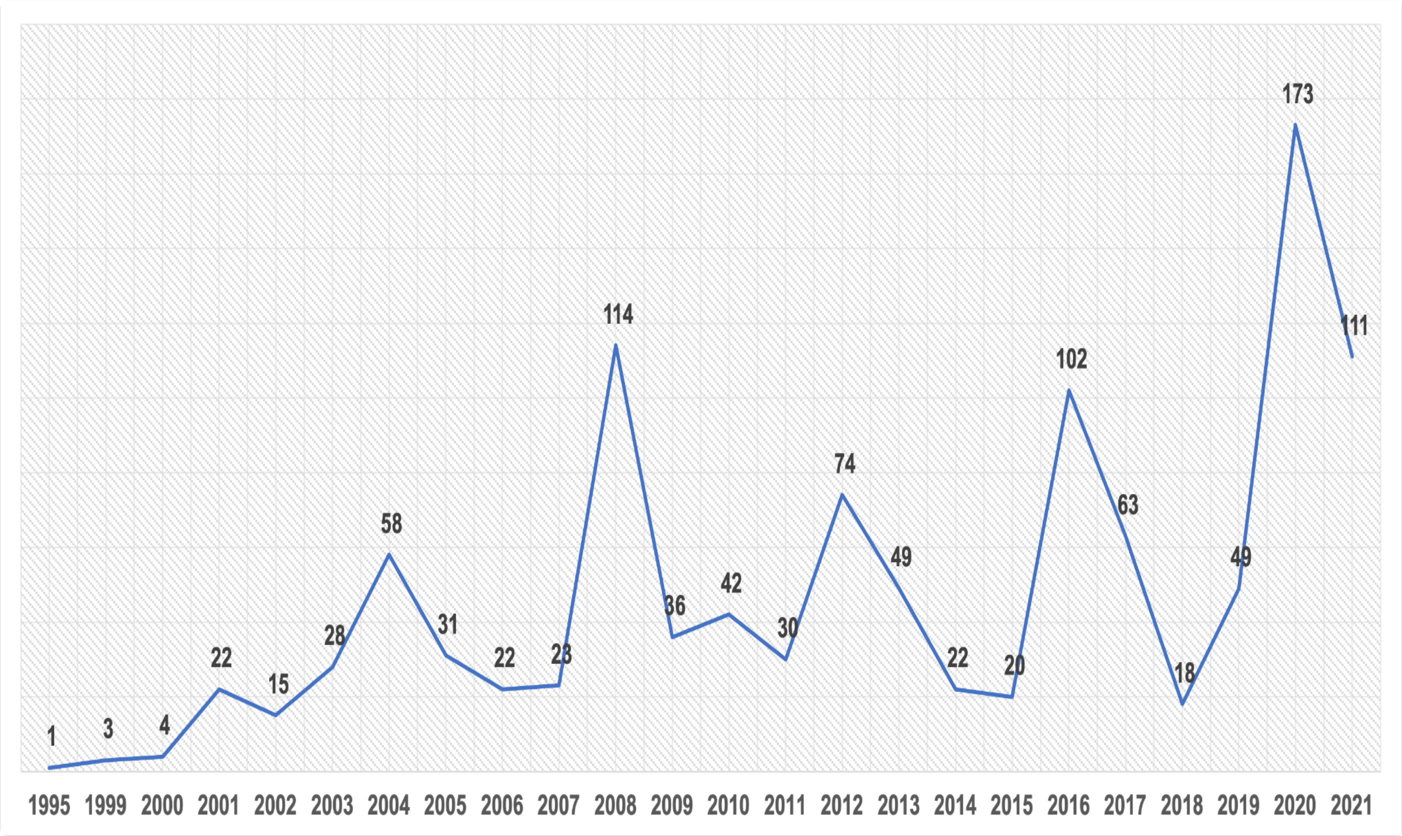

***Chart 1:** Domain registration volume distribution by creation year*

The Crédit Agricole domain registration peaked in 2020, but since 2021 isn't over yet, there is a chance for this year's volume to beat 2020's. To determine if the domains could be considered a culprit behind the volume of phishing attacks targeting the bank and its customers, we looked at how many of them could be publicly attributed to the financial service provider.

We first obtained the WHOIS record of the bank's domain credit-agricole[.]fr to collect identifiable details. We then compared these with information contained in the WHOIS records of the 3,159 domains we initially gathered and subjected to a bulk WHOIS lookup.

Using the bulk WHOIS lookup results, we found that only 2% of the total number of domains that contained the company's name could be publicly attributed to Crédit Agricole based on their identified registrant organization. The rest didn’t share that particular WHOIS record detail or left the field blank.

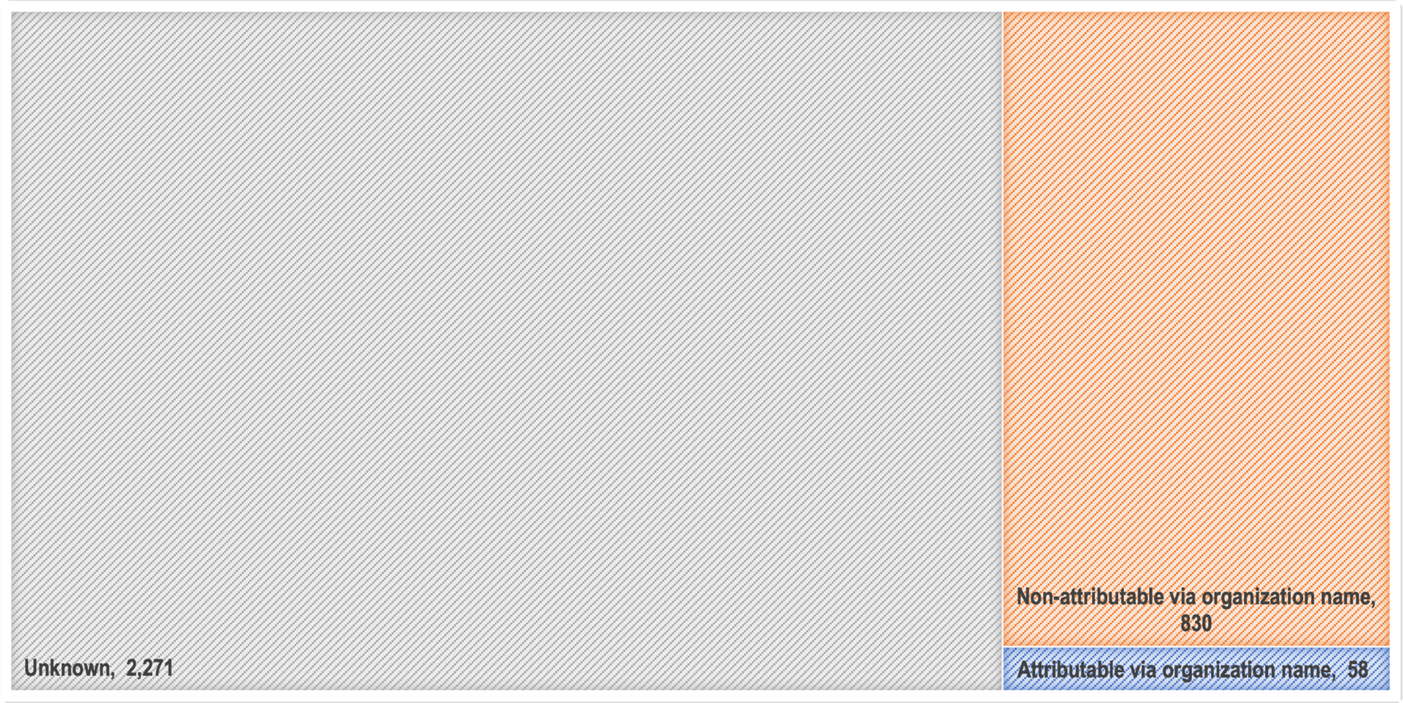

***Chart 2**: Percentage of the total number of domains containing Crédit Agricole owned but were not owned by the bank*

Malicious Domain and Subdomain Volume

Subjecting the 5,671 domains and subdomains to a bulk malware check using Threat Intelligence Platform (TIP), we found that 17% were dubbed “dangerous.” Examples of the malicious domains are:

- gcreditagricole[.]com
- xn--crditagricoles-ckb[.]com

- www-credit-agricole-fr[.]fr
- fr-credit-agricole-support[.]com
- creditagricole-activatation[.]com
- credit-agricole[.]midwayhotelservicesllc[.]com
- credit-agricole[.]fr[.]applecart[.]com[.]my
- mail[.]creditagricole[.]services-securipass[.]fr
- webdisk[.]creditagricole[.]services-securipass[.]fr
- cpanel[.]credit-agricolee[.]bounceme[.]net

There were more than twice as many malicious subdomains (372) than domains (150). Closer scrutiny of the subdomains showed that their root domains weren't under Crédit Agricole's control.

Companies that are often phished could benefit from regular monitoring of what could be considered typosquatting domains and subdomains. Warning customers about these at the very least or taking that a step further (taking action to have the offending web properties taken down) could be an effective protection measure.

Prioritizing the domains and subdomains for malware checks could be guided by the top TLDs used, which are:

- .com (35%)
- .ru (25%)
- .fr (9%)

The TLDs the malicious domains and subdomains used were almost evenly divided among ccTLDs (51%) and gTLDs (49%).

Any company is at risk of becoming the subject of cyber attacks. Monitoring domains that use their brand and company names, however, can be one of the first steps in identifying web properties that could be used as part of brand impersonation and related phishing campaigns.

If you are a security researcher and wish to obtain a copy of the list of domains and subdomains mentioned in this post, feel free to contact us.