2022 THREAT BRIEF:

CREDIT UNION AND REGIONAL BANK BRANDS UNDER ATTACK

ALLURE SECURITY

TABLE OF CONTENTS

PREFACE

Allure Security provides brand protection-as-a-service to organizations of all sizes within all types of industries. Recently, more regional banks and credit unions have approached us for help dealing with brand impersonation attacks against their institutions, which signals an increase in fraudsters targeting these organizations.

In this threat brief, we will raise awareness of the growing online brand impersonation threat afflicting regional banks and credit unions.

This report is built on our proprietary data set gathered during our automated daily assessment of tens-of-millions of web pages in Q1 2022.

We've collected and analyzed these data to paint an accurate, up-to-date picture of the problem.

We will also provide evidence that traditional approaches to identifying online brand impersonations — searching for URL permutations or domain monitoring — are ineffective. Such old-fashioned methods leave financial institutions and consumers vulnerable to the myriad repercussions of online fraud.

EXECUTIVE SUMMARY

- Some regional banks and credit unions mistakenly assume that they aren't well-known enough to warrant fraudsters' attention. However, during the first quarter of 2022, **Allure Security found online brand impersonation attacks targeting 1 in 5 regional banks/credit unions in our sample.**

- **Antiquated methods of identifying online brand impersonation attacks** (such as searching for URLs that include use of the brand name or permutations of it) are too time-and-effort-intensive (i.e., costly) and **fail to identify the majority of attacks**, missing 69 percent of attacks detected by modern approaches.

- **Regional banks and credit unions must take action to identify and mitigate online brand impersonation attacks** that harm their institutions and customers/members in multiple ways:

  - Reputation/brand damage
    - Diminished customer/investor trust
    - Increased hiring/retention costs
    - Weakened financial performance metrics (margins, return on equity, earnings, liquidity, market capitalization)
  - Eroded value on digital channel investments
    - Traffic "leaked" to scam sites
    - Changed buyer behaviors due to lack of trust
  - Revenue loss – prospective customers transact with the fraud site and/or forego future purchases
  - Reduced loyalty/satisfaction – negative brand perception sends prospective customers to other institutions
  - Staff opportunity costs – staff could be spending time on tasks more valuable to the business
  - Regulatory and compliance costs

INTRODUCTION

Some regional banks or credit unions mistakenly assume their institution isn't widely known enough to attract fraudsters' attention. We will explode this myth.

The Anti-Phishing Working Group's 1st Quarter 2022 Phishing Activity Trends Report[1] recorded the highest number of unique instances of scam websites ever in March 2022 (and APWG has been tracking these trends for 18 years).

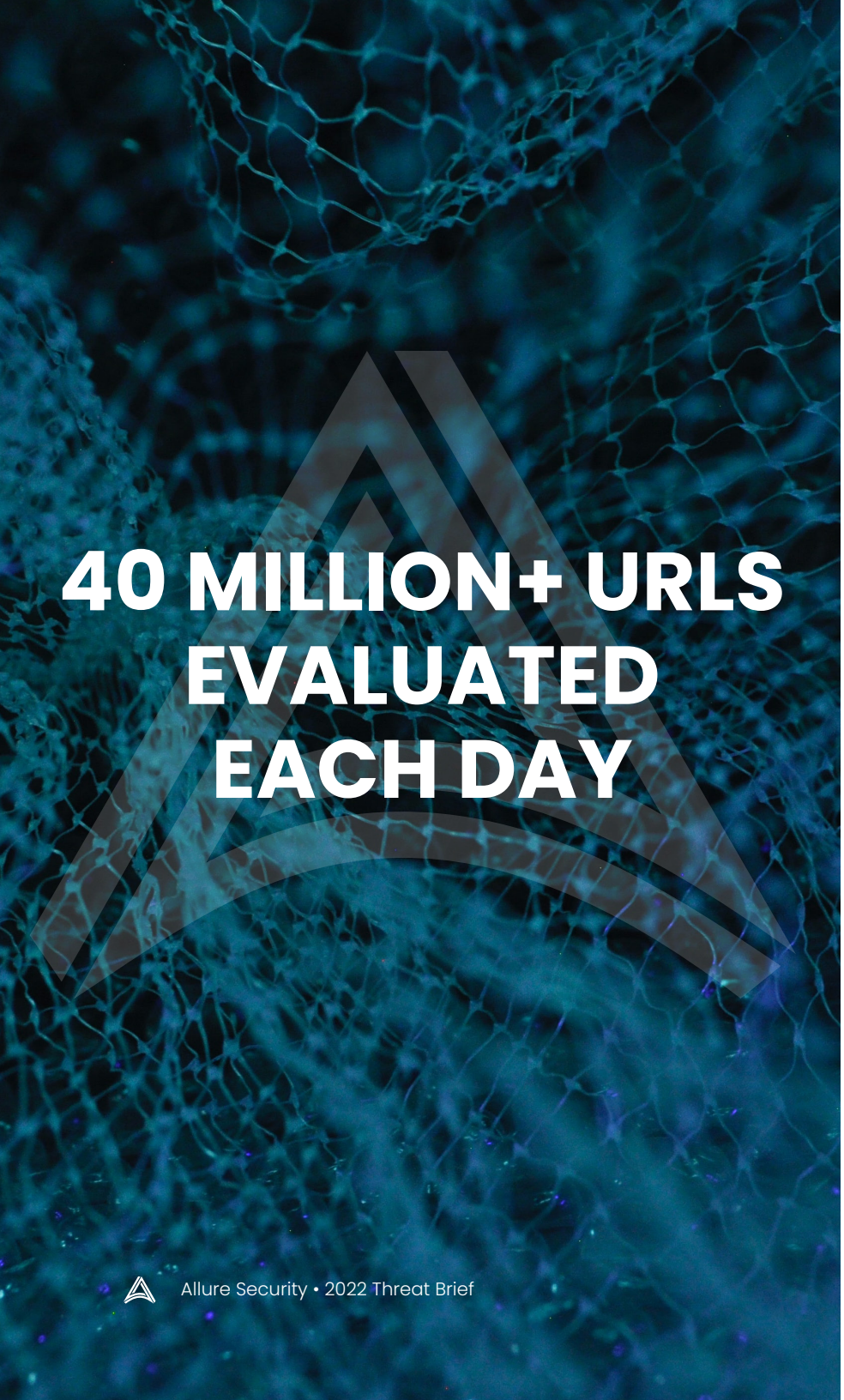
Impersonations of financial services brands made up nearly a quarter of these scam websites making the financial services sector the number one targeted industry. When you also consider that about half of banks in the U.S. manage $300 million or less in assets[2], you start to understand that regional banks and credit unions make up a large population of potential targets for fraudsters.

We've seen numerous examples[3] of scammers targeting[4] credit unions[5] in the first few months of 2022. In March 2022, the National Credit Union Administration warned credit unions of increased risk of social engineering and phishing threats targeting their employees and members.[6] Credit unions and regional banks would be remiss to consider themselves free of the threat of spoof websites, deceptive social media accounts, and phony mobile apps targeting their patrons. Allure Security's analysis of brand impersonation attacks in Q1 2022 proves that the heightened concern of online spoofs of credit union and regional bank brands is warranted. In our data set for Q1 2022, we found 870 instances of online brand impersonations spoofing 164 regional bank and credit union brands.

THIS REPORT WILL COVER:

- Our data set and methodology for discovering these attacks
- The prevalence of these attacks in our sample
- Why looking for the use of a brand name or permutations of it fails to identify the majority of brand impersonation attacks and requires too much time and effort

[1] https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf
[2] https://sgp.fas.org/crs/misc/R46779.pdf
[3] https://www.khq.com/straight_from_the_source/scam-alert-banks-and-credit-unions-are-seeing-an-increase-of-dangerous-phising-scams/article_da55d7e0-a709-11ec-9f64-df540b1e3ea1.html
[4] https://nbc-2.com/news/crime/2022/04/08/numerous-suncoast-bank-accounts-hacked-in-cape-coral
[5] https://www.cutimes.com/2022/04/15/penfed-hounded-by-multiple-website-spoofings
[6] https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/heightened-risk-social-engineering-and-phishing-attacks



METHODOLOGY AND DATA SOURCES

Allure Security's brand impersonation detection engine collects and automates the evaluation of tens-of-millions of websites, social media accounts, and third-party mobile app listings each day. The data set for this report includes more than 40 million URLs evaluated each day for the 90 days of the first quarter of 2022 or a total pool of 3.6 billion URLs.

ALLURE SECURITY COLLECTS AND ANALYZES URLS FROM NUMEROUS SOURCES INCLUDING:

- Newly published and previously dormant domains and subdomains – our detection engine evaluates these URLs every few hours for the first 0-3 days of the URL's lifespan, daily from days 4 through 30, every other day from days 31 - 60, and weekly from days 61-120
- Potentially deceptively named sites that could be confused for a brand name we protect - currently a pool of approximately 3.8 million URLs evaluated daily
- Allure Security web beacon signals including referrer strings from traffic redirected to sites we protect along with alerts on content containing our beacons or "virtual watermarks"

DATA SOURCES (CONT.)

- Proprietary online advertisement feed which provides URLs contained within online ads that name our customers

- "Lateral crawling" of sites linked to detected brand impersonation attacks to examine other potential scam sites in proximate/related IP address space, under certificates registered by similar company or individual names, with similar WHOIS information, and more

- URLs submitted to the Allure Security API by email security and anti-virus vendor partners

- URLs from commercial threat feeds totaling approximately 12,000 per day

Our AI-powered detection engine then renders each of these URLs in a browser, visiting the site as a human would, to identify impersonations. Our technology automates site analysis using imagery and text — rather than simply URLs — to identify imitations of more than 5,000 brands that we track (a number that continues to grow). The scale and speed we achieve allows us to find more impersonations more quickly than humans or domain monitoring or a combination of the two.

From our total pool of 3.6 billion websites analyzed during the first quarter of 2022, we then separated out credit union and regional bank brands. Please note that this report can't possibly convey the entirety of the problem since our data set is limited to the 864 regional bank or credit union brands we monitored in Q1 2022.

FINDINGS

PREVALENCE OF BRAND IMPERSONATION ATTACKS

For the purposes of this study, we define a brand impersonation attack as a fake website, social media account, or mobile app that impersonates a trusted brand. The scammer's goal is to exploit consumers' trust in the brand to trick them into divulging payment information, credentials, personal data and more.

From January 1 through March 31, 2022 we identified 870 online brand impersonation attacks targeting 164 different regional banks and credit unions. That's about five brand impersonation attacks on each brand in Q1. The top four regional banks and credit unions attacked in our sample experienced more than 100 brand impersonations. The top victim, a regional bank, suffered 154 brand impersonation attacks in the first quarter of 2022.

This volume of attacks proves that scammers have regional banks and credit unions in their crosshairs and these institutions can't afford to consider themselves undeserving of scammers' attention. One recently observed example[7] of a scam targeting regional banks and credit unions involves sending a mass text message to every cell phone in a given area code (typically a geographic area served by a particular credit union or regional bank).

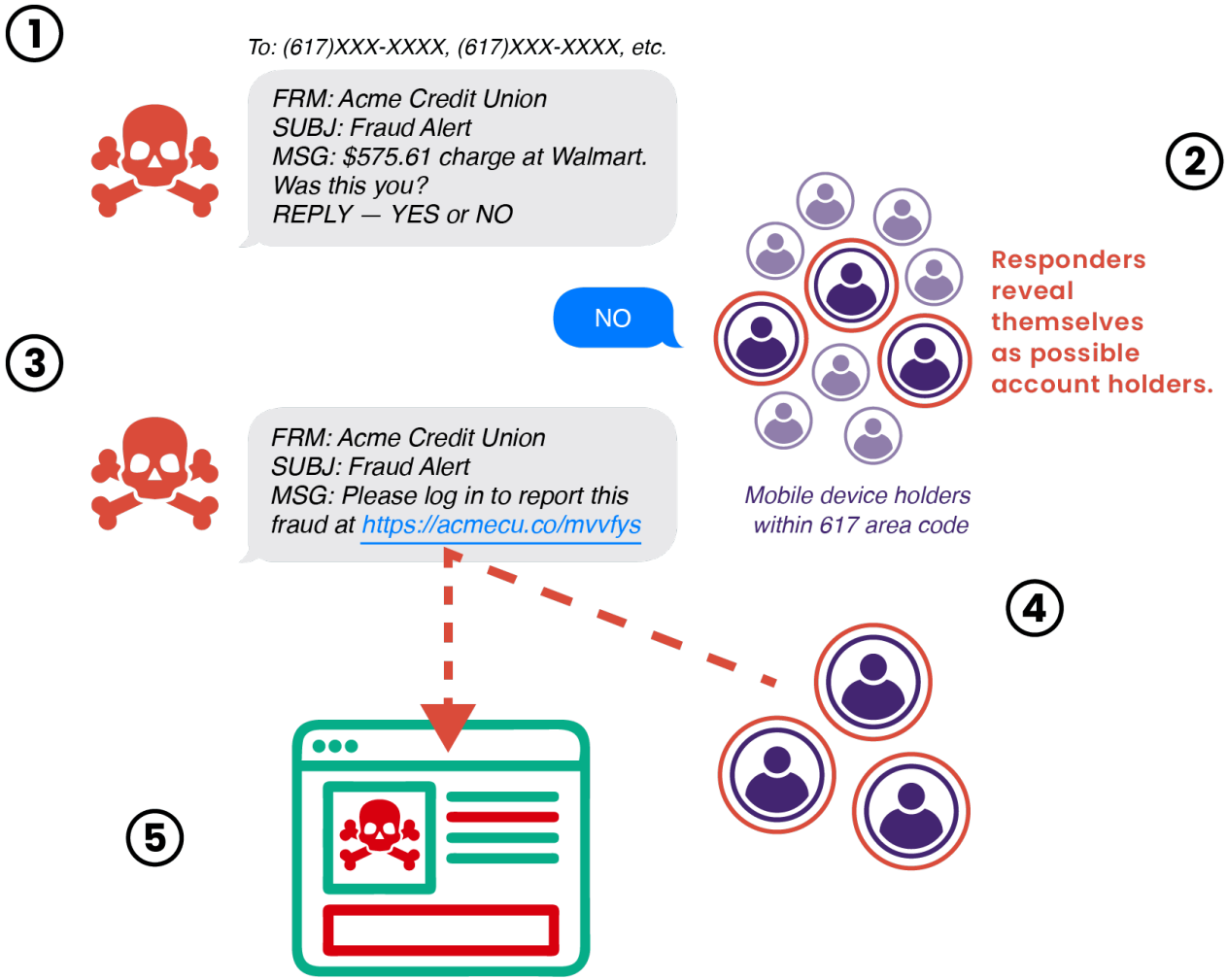
That SMS message will ask for confirmation of an alleged fraudulent transaction on the recipient's account at a financial institution in the area. The real purpose of the text message is to confirm who has an account at the regional bank or credit union. Anyone that responds identifies themselves as an account holder at the institution. The scammer will then follow up with a link asking them to log-in to report the fraud. That link directs the victim to a fake website that impersonates the brand's log-in page and the flustered victim has then given up their credentials and more to a thief.

1 IN 5 Regional banks & credit unions experienced a brand impersonation attack	**164** Brands impersonated
154 Maximum attacks on any one brand	**870** Total brand impersonation attacks
5 Attacks per brand on average	

*For the quarter ending March 31, 2022

[7] https://roanoke.com/news/local/crime-and-courts/casey-couple-loses-55-000-after-fake-text-purportedly-from-their-bank/article_34ad4184-7586-11ec-8269-0b74736de763.html

EXAMPLE OF BRAND IMPERSONATION SCAM DISTRIBUTED VIA SMS



DETECTION EFFICACY

OUTMODED DETECTION METHODS

Businesses have attempted to detect brand impersonation attacks in a number of ways (including but not limited to):

1. **Customer complaints** - Scam victims contact the targeted brand's customer support team to complain of fraud
2. **Google Alerts** - Configure Google Alerts to notify a business of the use of their brand name online
3. **Manual search** - Periodically search the internet manually for their brand name or use Google Images to perform an image search for their logo
4. **String-based detection & domain monitoring** - Iterating on permutations of a brand's URL and visiting those sites to identify anything suspicious

Maybe the above methods are better than absolutely nothing, but they leave much to be desired. Customers acting as a business's detection system does nothing to protect the brand – the fraud has occurred, the customer is angry and may churn, the sale is lost, and the brand/ reputation is damaged. It's a lose-lose situation.

Google Alerts or manual search or a combination of the two has limited coverage. For example, scammers will slightly alter logos to circumvent detection via image search. In addition, manually reviewing alerts and examining associated websites borders on drudgery. Not to mention that the number of websites a human can review in an hour or day is a pittance compared to the number of new websites launched each day. Some studies estimate that as many as 175 new websites are created every minute[8].

Domain monitoring consists of creating permutations of your URL to identify potential look-alike URLs and visiting those URLs looking for malicious intent. Like Google Alerts and manual searches, domain monitoring requires a lot of work and fails to find a majority of brand impersonation attacks. Below we'll prove how ineffective, and how much work, domain monitoring can be exploring our same data set.

[8] https://siteefy.com/how-many-websites-are-there/#:~:text=As%20per%20our%20calculations%2C%20approximately,are%20created%20every%20day%20worldwide

DOMAIN MONITORING DETECTION EFFICACY

The majority of domain monitoring's detection capability relies on analysis of strings. For the purposes of our discussion we'll define a string as a series of characters. For example, the fictional brand name "acme" is a string. Unfortunately, our data shows that relying strictly on string detection fails to identify the majority, 69 percent, of online brand impersonation attacks.

ONLY 31%	69%
of attack URLs contained strings similar to the victim organization's brand name (e.g, "look-a-like" URLs or typosquatting)	of attacks went undetected by string-based detection methods

*For the quarter ending March 31, 2022

Let's look deeper into the mere 31 percent of brand impersonation attacks detected with a string-based method such as domain monitoring.

Attack Methods Identified with Domain Monitoring

17%	Attacks used a recognizable brand string at the beginning of the domain name or as a subdomain	**acmebank.com** vs. acmebankonline.com vs. acmebank.devsite.com
7%	Attacks used look-a-like strings	**acmebank.com** vs. acrnebank.com vs. acmcbank.com
5%	Attacks used a recognizable brand string somewhere within the domain/subdomain	**acmebank.com** vs. nowacmebank.com vs. onlineacmebank.now.com
1.5%	Attacks used a different top-level domain (e.g., .biz, .net, .xyz) with the same recognizable brand string	**acmebank.com** vs. acmebank.online vs. acmebank.site

What readers should take away from this exploration is that **detecting online brand impersonations based solely on looking for the brand name, or deceptive misspellings of it, addresses less than a third of the problem.** Domain monitoring, which uses this method, is inadequate.

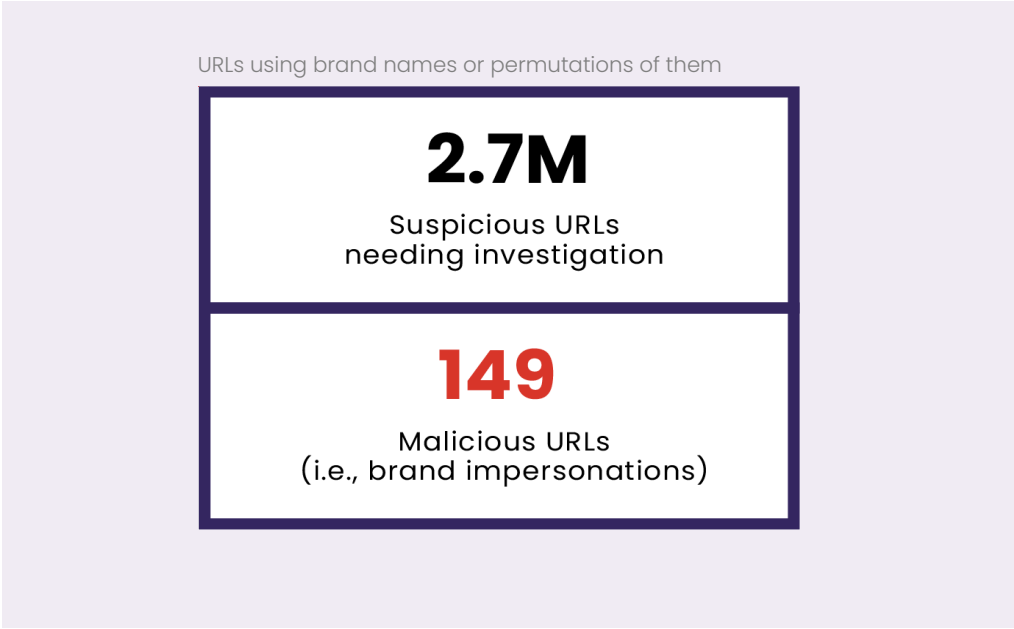
DOMAIN MONITORING DETECTION COSTS

Domain monitoring and/or string-based detection failed to identify almost 70 percent of the online brand impersonation attacks in our sample. Domain monitoring requires an impractical amount of time and effort for an insufficient result. To support the case for automating this process, below we elaborate on what string-based detection of scam websites costs a regional bank or credit union in terms of person hours.

To give an idea of the volume of work necessary to find and then confirm an online brand impersonation using string-based methods, we carved out a subset of 79 brands. Those 79 brands experienced suspicious URLs that were direct or close permutations of their brand name string. Keep in mind though that identifying a domain that uses a brand name, or a close iteration of it, is only the beginning.

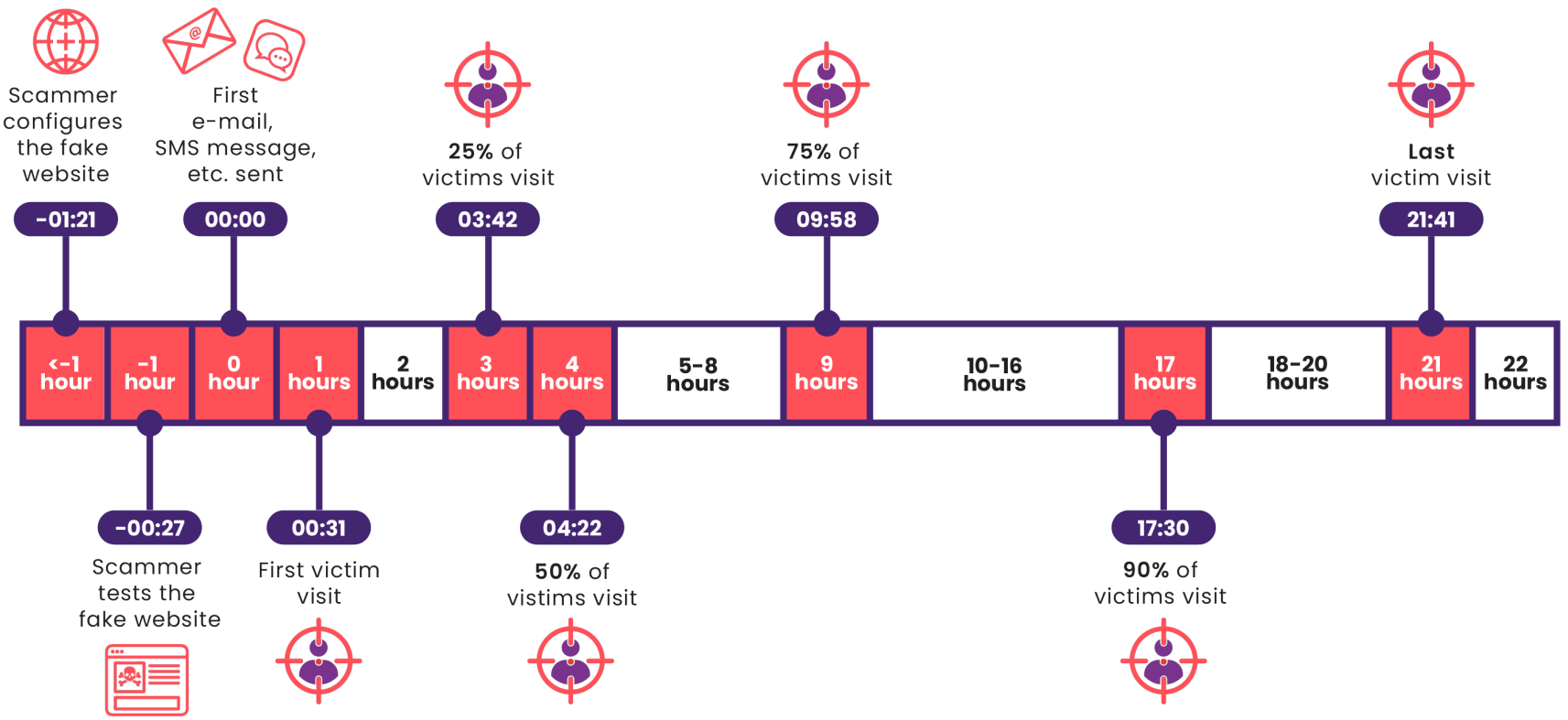
A human also needs to visit the suspicious URL to verify whether or not the site has malicious intent. In our work for this study, it took us 20 to 60 seconds to visit any one URL and make a decision about whether or not it was malicious.

Using only domain monitoring or string-based analysis, these 79 brands would need to spend between 20 and 60 seconds reviewing each suspicious URL – a total of 15,000 to 45,000 hours. That's an astonishing amount of time, and many regional banks and credit unions lack even a single dedicated cybersecurity resource, let alone a team with time to handle such a task. The 15,000 to 45,000 hours estimate also assumes that an analyst would only need to review any given URL once (which is a recipe for failure).



Seventy-five percent of victims visit a scam website within 10 hours of the attacker distributing the scam to the targeted brand's customers (i.e., "inviting" people to the scam website via e-mails, SMS messages, QR codes, online ads, etc.).[9] So, to make any considerable impact on reducing fraud resulting from these scams, the sites need to be detected closer to the beginning of their lifespan. Scammers regularly update scam website content requiring that brands evaluate these URLs on an ongoing basis – adding even more time and effort. From our data sample, 9 institutions would have needed to evaluate 100,000 URLs. Estimating this review to take between 20 seconds to 1 minute per URL we come to a total of 556 to 1,667 hours. And if you hope to detect an attack within the first 24 hours or so, an institution might need to perform this operation daily! It cannot be done.

Average Online Brand Impersonation Attack Timeline (victim traffic to scam websites relative to first e-mail sent in hours:minutes)



[9] https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise

Not only are string-based methods such as domain monitoring more expensive, and not only do they miss the majority of attacks – they also don't catch these scams before people have already fallen victim. Catching these scams during configuration or testing reduces (or eliminates) the number of victims, making ongoing analysis of suspicious URLs crucial. Pre-launch detection stops the scam before it starts.

Suspicious URLs flagged using string-based detection and estimated review time

Suspicious URLs	**100K** (9 institutions would review 100K+ URLs)	**10K** (33 institutions would review 10K+ URLs)	**3K** (median, 40 institutions would review 3K+ URLs)
Time to Review	**556 - 1,667 hours**	**56 - 167 hours**	**17 - 50 hours**

Consider the task set forth for a cybersecurity analyst taking this challenge on. They receive a list of hundreds of URLs in the morning and must visit each and every one. As you might imagine, the work becomes tedious quickly. In one case, a customer of Allure Security reported spending two hours everyday from 9 a.m. to 11 a.m. clicking through a list of 40 - 100 URLs. By choosing an AI-based solution to do the work instead, this particular individual reduced their workload from 2 hours to five minutes. As a result they also found more online brand impersonations and found them closer to their genesis, before fraud campaigns were launched against their customers.

This also speaks to the opportunity costs inherent in these legacy approaches. Cybersecurity staff spend time reviewing a substantial list of URLs, the majority of which are not a threat (though this fact absolutely must be validated). They could be bringing more value to the organization for example by helping reinforce defenses against ransomware, training employees in best security practices, or enabling the product team to mitigate vulnerabilities and deliver a secure user experience.

In the end, domain monitoring requires an impossible amount of time and even then fails to catch most brand impersonation attacks.

CONCLUSION

Regional banks and credit unions are increasingly under attack by fraudsters taking advantage of their trusted brands to swindle their customers. The impact of this problem can't be overstated – a strong brand attracts and retains customers and employees. It's one of a financial institution's most valuable assets – valued by the institution and its customers or members.

Outmoded methods for solving the problem give the impression that the problem is unsolvable and futile at worst or thankless at best. However, with modern AI-powered online brand protection solutions, it can actually be much more effective and easy. Regional banks and credit unions need to proactively gain visibility into the use of their brand online (whether authorized or not) and respond to misuse as quickly as possible. Fortunately, online brand protection providers such as Allure Security can take the majority of this work onto their shoulders, which frees your staff to engage in more stimulating, gratifying, and valuable work.

ABOUT ALLURE SECURITY

Allure Security protects brands by finding and stopping online scams before customers fall victim. Scam websites, phony social media profiles, and rogue mobile apps impersonate trusted brands to mislead people and steal their money, credentials, and personally identifiable information. Our patented, artificial intelligence-powered engine finds more of these online brand impersonations more quickly and with greater accuracy than legacy approaches. In addition, our unique, multi-pronged approach to response – blocklisting, decoy data injection, and takedown – significantly reduces the lifespan of a scam and the damage it can do.

- Allure Security discovers deceptive online content that impersonates your brand and targets your customers.
- Allure Security arms your brand protection, legal, cybersecurity, and fraud teams to defend your brand and your customers.
- Allure Security shortens scams' lifecycles reducing related online fraud, minimizing brand damage, and limiting revenue loss.

Our customers include leading financial institutions, apparel brands, cryptocurrency exchanges and wallets, investment advisors, state governments, and media conglomerates.

PHONE
(877) 669-8883

E-MAIL
info@alluresecurity.com

LINKEDIN
https://www.linkedin.com/company/alluresecurity

TWITTER
https://twitter.com/alluresecurity


2022
ALLURE
SECURITY
2022