Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers

By Zhanhao Chen and Janos Szurdi
September 1, 2020 at 3:00 AM
Category: Malware, Unit 42
Tags: DNS security, Phishing, scam, threat prevention, WildFire

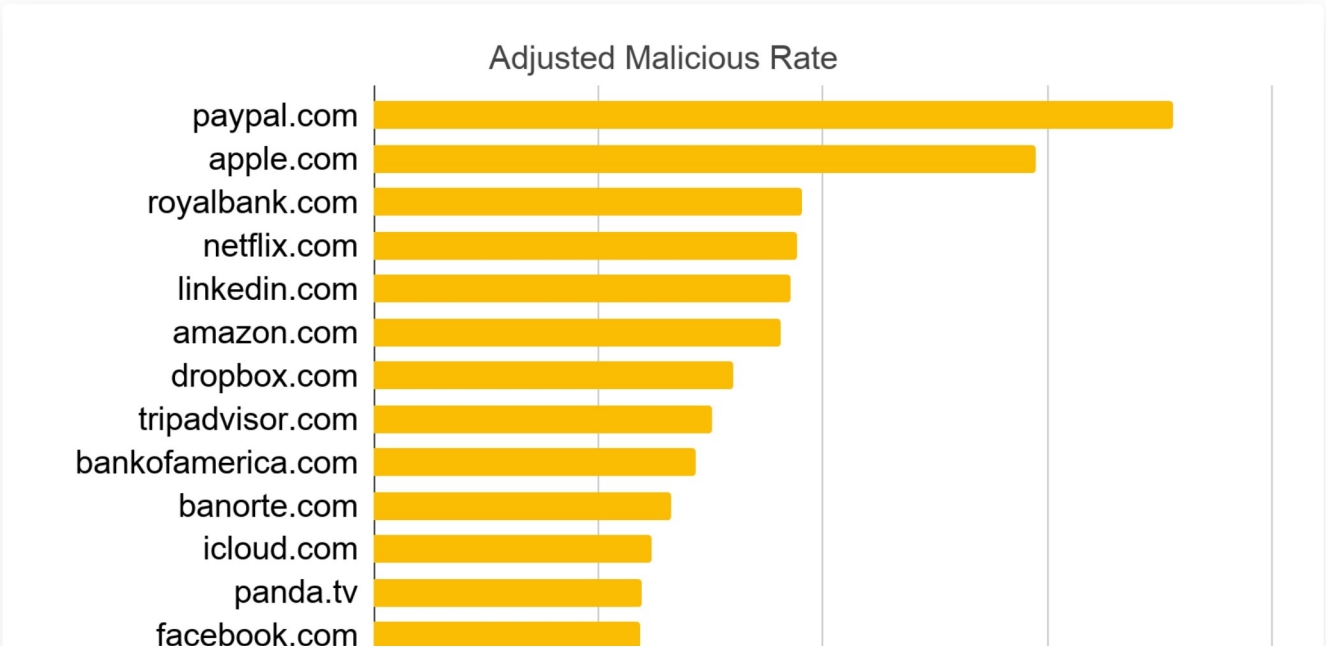
This post is also available in: 日本語 (Japanese)

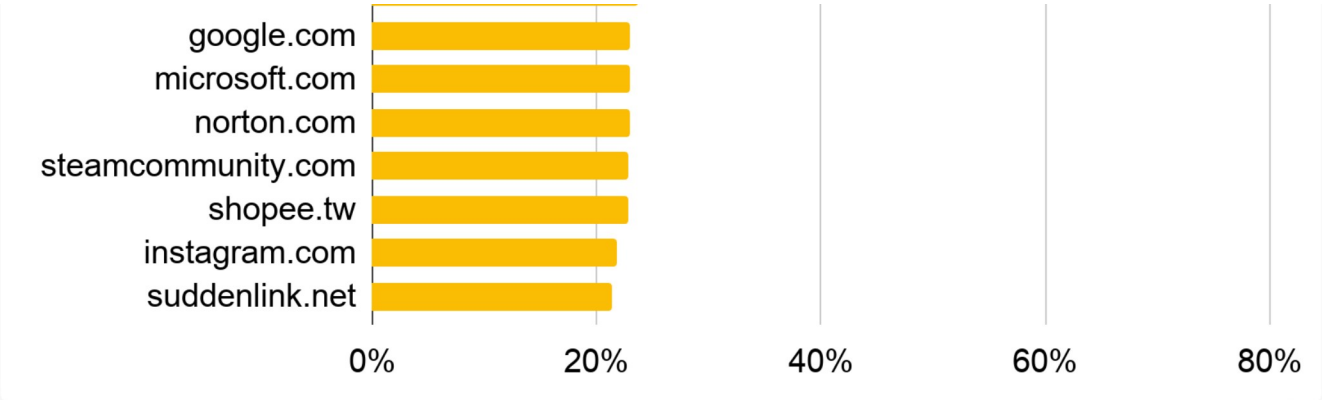
Executive Summary

Users on the internet rely on domain names to find brands, services, professionals and personal websites. Cybercriminals take advantage of the essential role that domain names play on the internet by registering names that appear related to existing domains or brands, with the intent of profiting from user mistakes. This is known as cybersquatting. The purpose of squatting domains is to confuse users into believing that the targeted brands (such as Netflix) own these domain names (such as **`netflix`**`-payments[.]com`) or to profit from users' typing mistakes (such as `whatsa`**`l`**`pp[.]com` for WhatsApp). While cybersquatting is not always malicious toward users, it is illegal in the U.S.,[1] and squatting domains are often used or repurposed for attacks.

The Palo Alto Networks squatting detector system discovered that 13,857 squatting domains were registered in December 2019, an average of 450 per day. We found that 2,595 (18.59%) squatted domain names are malicious, often distributing malware or conducting phishing attacks, and 5,104 (36.57%) squatting domains we studied present a high risk to users visiting them, meaning they have evidence of association with malicious URLs within the domain or are utilizing bulletproof hosting.

We also ranked the Top 20 most abused domains in December 2019 based on adjusted malicious rate, which means that a domain is either a target of many squatting domains or most of these squatting domains are confirmed malicious. We found that domain squatters prefer profitable targets, such as mainstream search engines and social media, financial, shopping and banking websites. When visiting these sites, users are often prepared to share sensitive information, which opens them up to phishing and scams to steal sensitive credentials or money if they can be deceived into visiting a squatting domain instead.





From December 2019 to date, we observed a variety of malicious domains with different objectives:

- **Phishing:** A domain mimicking Wells Fargo (`secure-`**`wellsfargo`**`[.]org`) targeting customers to steal sensitive information, including email credentials and ATM PINs. Also, a domain mimicking Amazon (**`amazon`**`-india[.]online`) set up to steal user credentials, specifically targeting mobile users in India.
- **Malware distribution:** A domain mimicking Samsung (**`samsung`**`eblya`**`iphone`**`[.]com`) hosting Azorult malware to steal credit card information.
- **Command and control (C2):** Domains mimicking Microsoft (`microsoft-store-drm-server[.]com` and `microsoft-sback-server[.]com`) attempting to conduct C2 attacks to compromise an entire network.
- **Re-bill scam:** Several phishing sites mimicking Netflix (such as **`netflix`**`brazilcovid[.]com`) set up to steal victims' money by first offering a small initial payment for a subscription to a product like weight loss pills. However, if users don't cancel the subscription after the promotion period, a much higher cost will be charged to their credit cards, usually $50-100.
- **Potentially unwanted program (PUP):** Domains mimicking Walmart (**`walrmart`**`44[.]com`) and Samsung (**`samsung`**`pr0mo[.]online`) distributing PUP, such as spyware, adware or a browser extension. They usually perform unwanted changes, like changing the browser's default page or hijacking the browser to insert ads. Of note, the Samsung domain looks like a legitimate Australia educational news website.
- **Technical support scam:** Domains mimicking Microsoft (such as **`microsoft`**`-alert[.]club`) trying to scare users into paying for fake customer support.
- **Reward scam:** A domain mimicking Facebook (**`facebook`**`winners2020[.]com`) scamming users with rewards, such as free products or money. To claim the prize, users need to fill out a form with their personal information such as date of birth, phone number, occupation and income.
- **Domain parking:** A domain mimicking RBC Royal Bank (`rby`**`royalbank`**`[.]com`) leveraging a popular parking service, ParkingCrew, to generate profit based on how many users land on the site and click the advertisements.

We studied domain squatting techniques including typosquatting, combosquatting, level-squatting, bitsquatting and homograph-squatting (all defined below). Malicious actors can use these

techniques to distribute malware or to conduct scams and phishing campaigns.

To detect squatting domains, Palo Alto Networks developed an automated system to capture emerging campaigns from newly registered domains, as well as from passive DNS (pDNS) data. We continue to detect currently active cybersquatting domains – we identify malicious and suspicious squatting domains and designate them to the appropriate categories (such as phishing, malware, C2 or grayware). Protections against domains classified in these categories are available in multiple Palo Alto Networks security subscriptions, including URL Filtering and DNS Security.

We recommend that enterprises block and closely monitor traffic from these domains, while consumers should make sure that they type domain names correctly and double-check that the domain owners are trusted before entering any site. More tips can be found in this post on how to protect against cyberattacks.

Squatting Techniques

Typosquatting is one of the most common types of domain registration abuse. Typosquatters intentionally register misspelled variants (such as `whatsa**l**pp[.]com`) of target domain names (`whatsapp[.]com`) to profit from users' typing mistakes or to deceive users into believing that they are visiting the correct target domain. The most frequent typosquatting techniques include registering names one edit distance from the original domain, as these are the most common and overlooked mistakes users make. For more information, readers can refer to academic research papers on the scale and malicious use of typosquatting.

Combosquatting is another widespread registration abuse that combines popular trademarks with words such as "security," "payment" or "verification." Combosquatting domains like `**netflix**-payments[.]com` are often used in phishing emails, by scam websites and for social engineering attacks to convince users that they are visiting web content maintained by the targeted trademark. For more information, readers can refer to this academic paper on a longitudinal study of combosquatting.

Homographsquatting domains take advantage of internationalized domain names (IDNs), where Unicode characters are allowed (such as `microsof**ŧ**[.]com`). Attackers usually replace one or more characters in the target domain with visually similar characters from another language. These domains can be perfectly indistinguishable from their targets, as in the case of apple.com, where the English letter "a" (U+0061) was replaced with the Cyrillic letter "a" (U+0430). For more information, readers can refer to academic research papers on IDNs.

Soundsquatting domains take advantage of homophones, i.e., words that sound alike (for example, *weather* and *whether*). Attackers can register homophone variants of popular domains, such as `**4**ever21[.]com` for `**for**ever21[.]com`. As text-to-speech software like Siri and Google Assistant becomes prevalent, more and more users will become vulnerable to the abuse of soundsquatting domains. For more information, readers can refer to this academic research paper on soundsquatting.

Bitsquatting domains have a character that differs in one bit (such as `micposoft[.]com`) from the same character as the targeted legitimate domain (`microsoft[.]com`). Bitsquatting can benefit attackers because a hardware error can cause a random bit-flip in memory where domain names are stored temporarily. Thus, even though users type the correct domains, they may still be led to malicious ones. Although such hardware errors are usually rare, an academic research paper has shown that bitsquatting is a real threat.

Levelsquatting domains, such as the case of `safety.microsoft.com.mdmfmztwjj.l6kan7uf04p102xmpq[.]bid`, include the targeted brand's domain name as a subdomain. In this example, the victims of the phishing attack might believe they are visiting `safety.microsoft.com`, when instead, they are visiting the attacker's website. This attack is especially worrisome for mobile users because the browser's address bar might not be wide enough to display the entire domain name. For more information, readers can refer to this academic paper for a more comprehensive study of levelsquatting domains.

Detection of Various Squatting Techniques

We leverage lexical analysis to detect candidate squatting domains among the Palo Alto Networks newly registered domain (NRD) and pDNS feeds. Our list of target domains is the combination of popular domains in general and domains popular in specific categories, such as shopping and business. We generate the aforementioned squatting variants of the target domains, and match them against our NRD feed and pDNS hostnames. Additionally, we cluster weekly collections of NRDs to see if registration campaigns target known brands. After the initial discovery step, we leverage WHOIS data to filter out defensive registrations and a heuristic rule-based classifier to identify which domains are true squatting domains.

Figure 1 shows the daily detection statistics for December 2019. During this period, we detected 13,857 squatting domains (~450 per day). Since then, the number of daily detections fluctuate from 200-900. To understand how these domains are leveraged for abuse, we use URL Filtering to categorize them. We label domain names as **malicious** if they are involved in distributing malware or phishing, or if they are being used for command and control (C2) communication. We label domains categorized as grayware, parked, questionable, insufficient content and high-risk as **suspicious**. The average malicious rate of the 13,857 squatting domains is 18.59% (2,595) and the average suspicious rate is 36.57% (5,104).

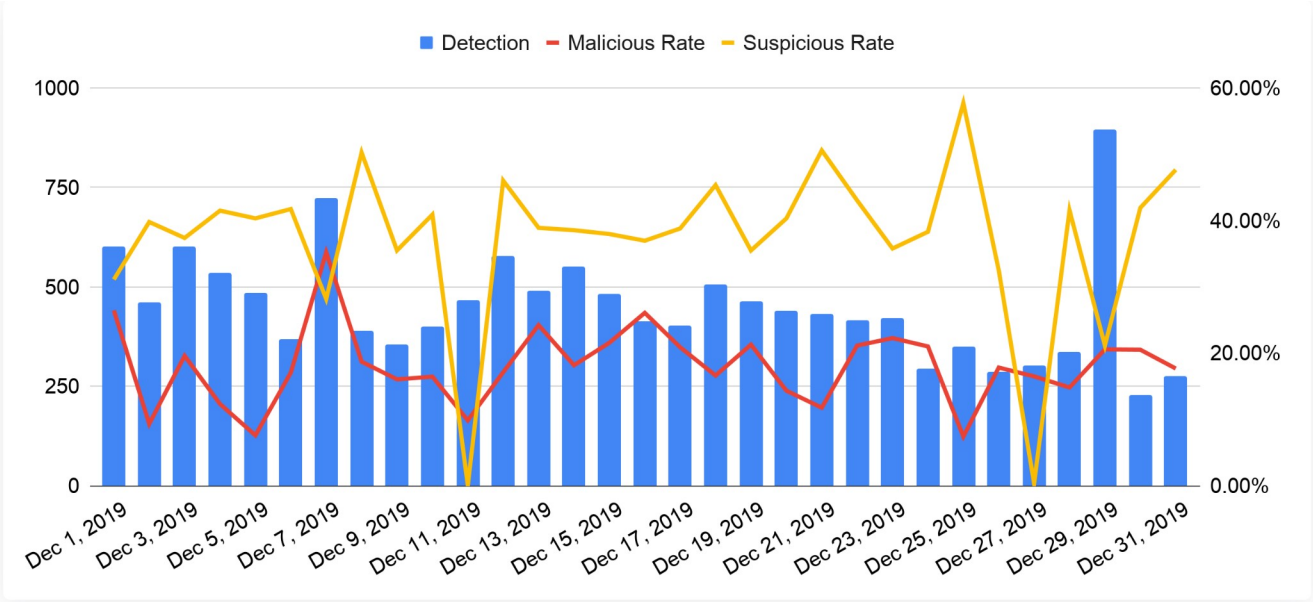


Figure 1. Volume and malicious and suspicious rates of daily domain squatting in December 2019.

Next, we compare our detection of squatting domains to vendors found on VirusTotal. Considering detection delays, we allow a 10-day time window for malicious squatting domains to appear on VirusTotal. Figure 2 shows how well the top 10 vendors detected these malicious and high-risk domains. The best-performing vendor covers about 25% of the malicious or high-risk squatting domains that we detected. Meanwhile, other vendors cover less than 20% of our detections. Lastly, we found that 55% of malicious or high-risk squatting domains are not detected by any vendors.

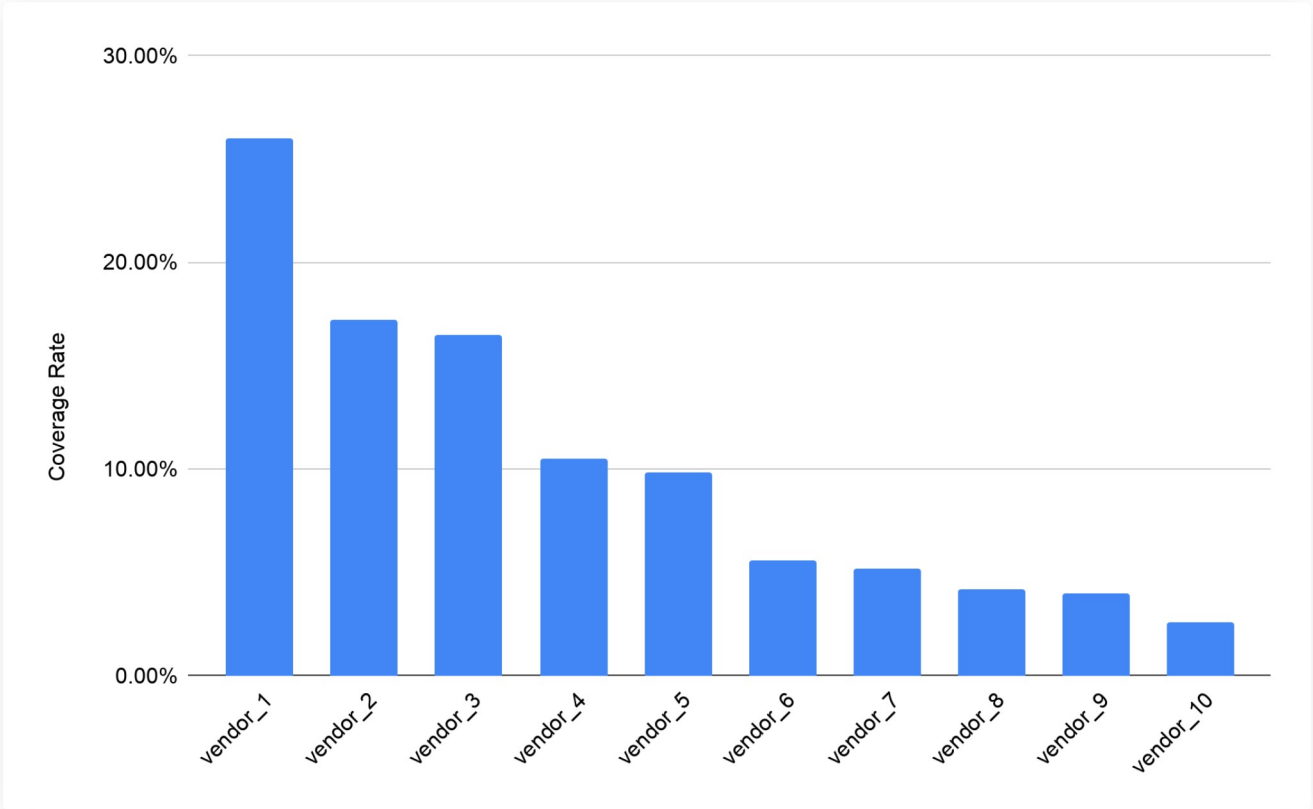


Figure 2. Malicious and high-risk squatting domain detection on VirusTotal in December 2019.

The Domain Squatting Ecosystem

To identify malicious infrastructure hotspots, we studied specific network elements and entities that typosquatters depend on for their operations. Specifically, we studied popular registrars, name services, autonomous systems and certificate authorities used by domain squatters.

For each chart outlined below, we considered the number of squatting detections to reflect their popularity among domain squatters, and the malicious IOC rate to quantify the degree of threat to users. Combining these two metrics, we calculated the adjusted malicious rate of each entity. Thus, a high adjusted malicious rate means that an entity is either targeted by many squatting domains or most of these squatting domains are malicious.

Top 20 Most Abused Domains

Domain squatters prefer popular and thus profitable targets. Figure 3 shows the Top 20 most abused domains. These targets are popular websites, such as mainstream search engines and social media, financial, shopping and banking websites. Squatting domains mimicking these websites benefit from their credibility to attract more users that can be scammed. Therefore, these targets have relatively high squatting detection numbers.

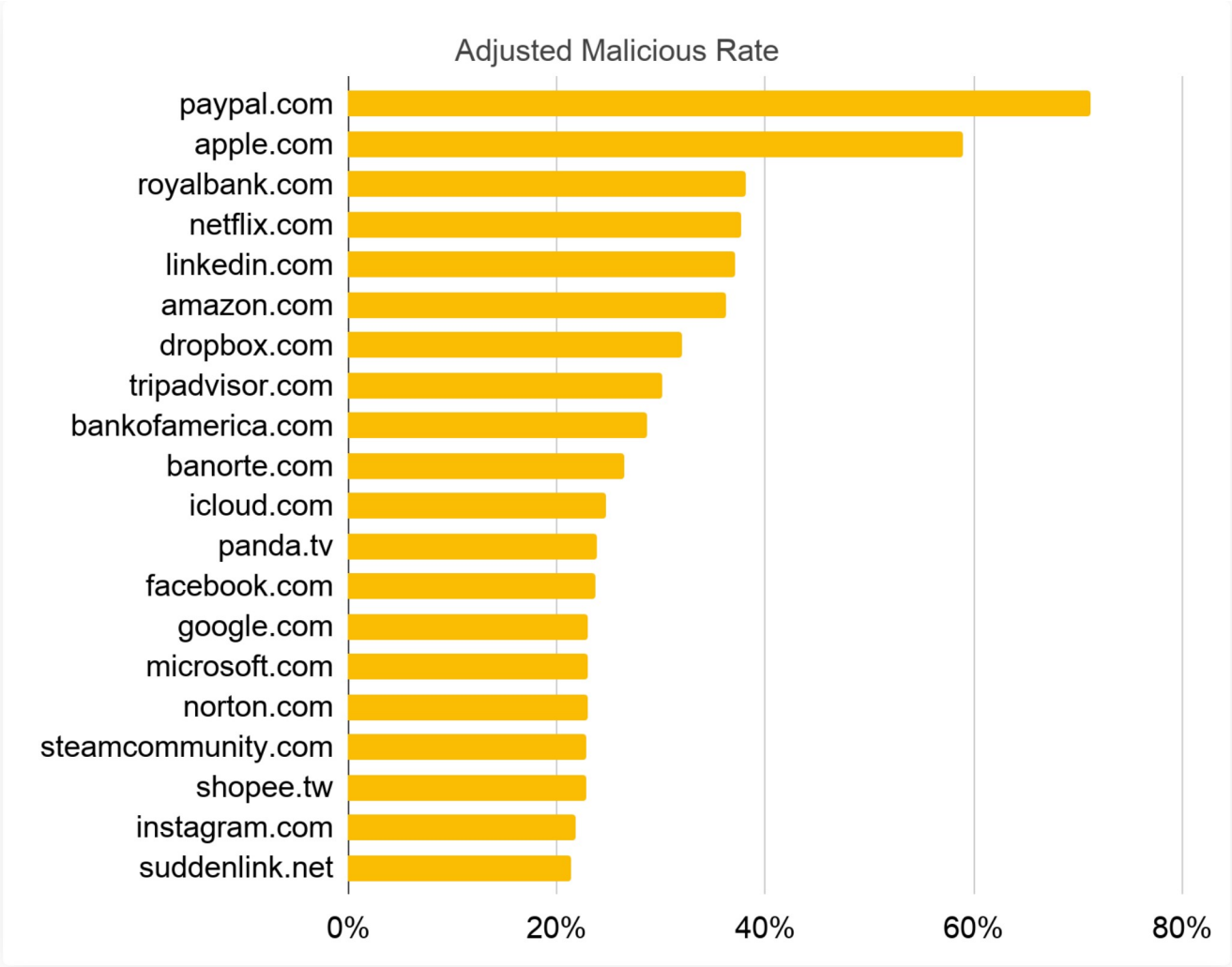


Figure 3. Top 20 most abused domains in December 2019.

Top 10 Most Abused DNS Services and Autonomous Systems

Next, we look at the DNS services and the autonomous systems (AS) used by squatting domains to understand their infrastructure preferences. An AS is a set of IP subnets maintained by one or more network operators.

The name service used by domain squatters often signifies which registrar was used to register the domain, where the squatting web page is hosted or which parking service these domains utilize to profit from user traffic. Figure 4 displays the most abused name services of squatting domains. Freenom.com and dnspod.com are often used by domain squatters, as they provide cheap or free domain registration and domain hosting. DNSPod is known for hosting shady DNS records and for providing services for malicious bulletproof hosting operators. Level-squatters might choose to use registrar.eu as it supports an unlimited number of subdomains and free URL forwarding, which reduces the cost of deploying and scaling attacks.

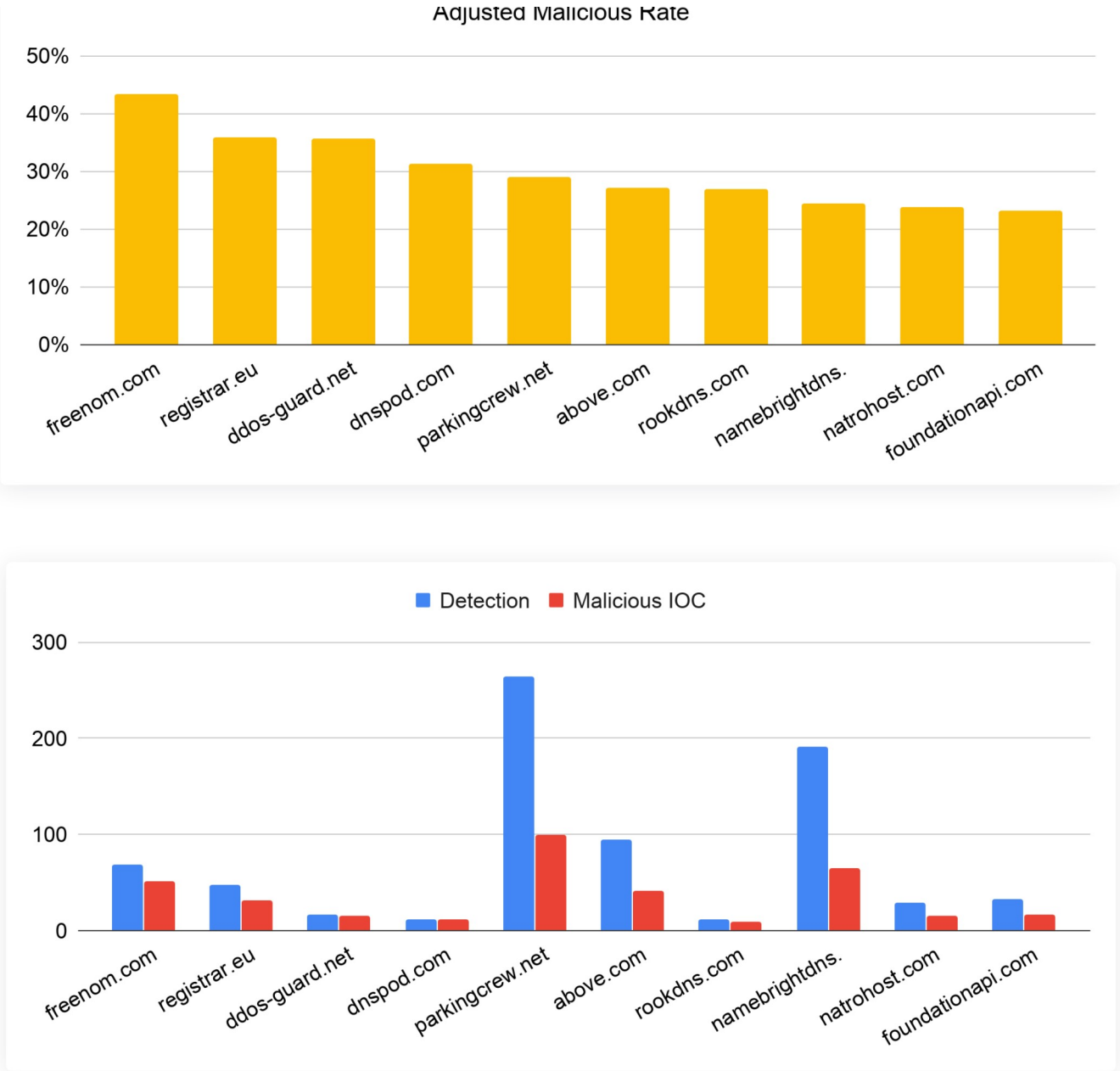
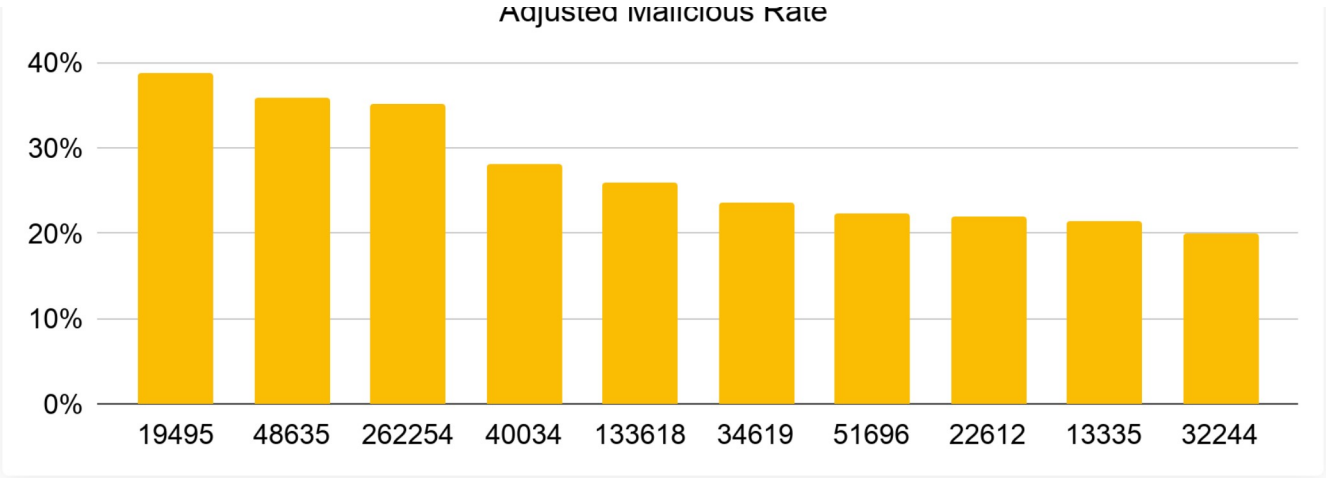


Figure 4. Top 10 most abused DNS services in December 2019.

Additionally, parkingcrew.net and above.com are popular parking services because they provide a simple monetization avenue to domain owners, achieved by pointing domain names' DNS records to their name servers. Parking services usually show users parked pages laden with ads or redirect users to affiliate marketing or malicious websites.

As hosting services often have their own AS, we observed that the AS distribution is somewhat consistent with the name service distribution. The top three most abused AS (19495, 48635, 262254) belong to the three most abused name service providers, respectively (freenom.com, registrar.eu, ddos-guard.net). The fourth most abused AS (40034) is owned by ztomy.com, a service favored for DNS hijacking attacks.



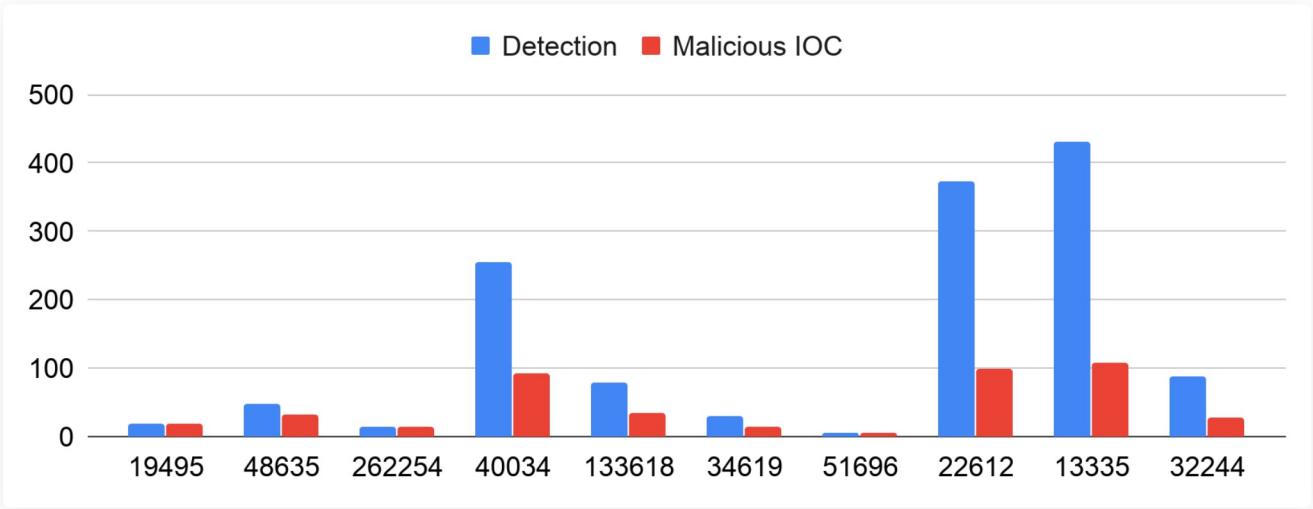
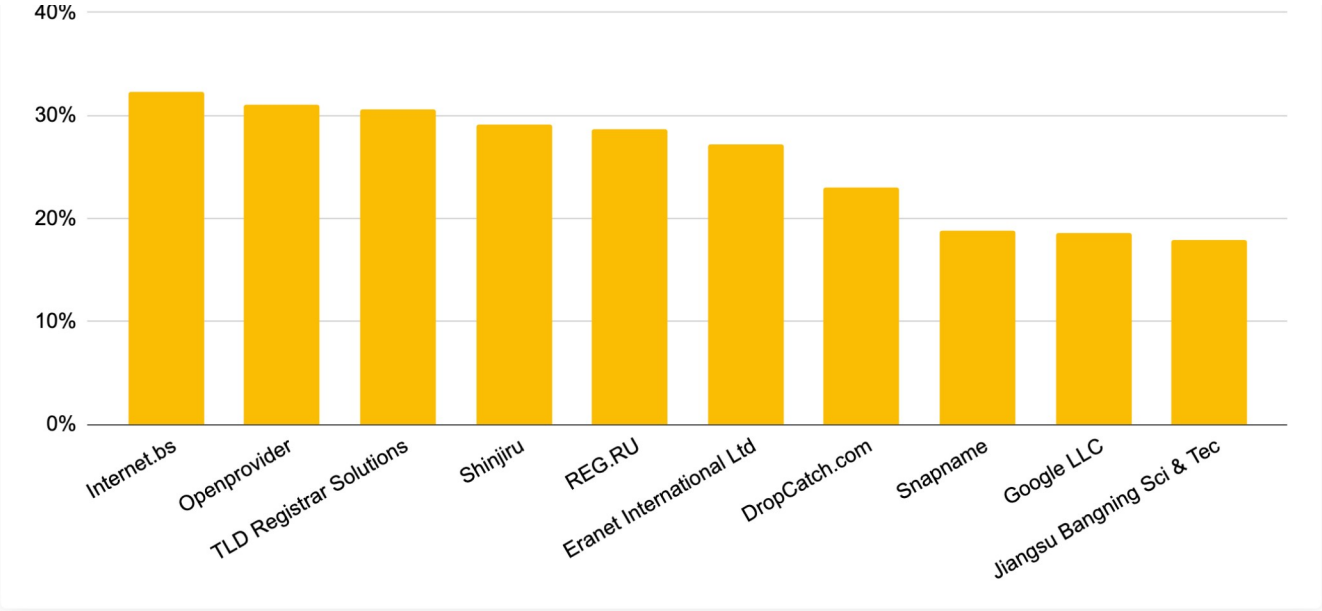


Figure 5. Top 10 most abused autonomous systems in December 2019.

Top 10 Most Abused Registrars

Registrars are entities that sell domain names to users. The most abused registrar, Internet.bs, provides free services preferred by domain squatters, including privacy-protected registration and URL forwarding. We captured several level-squatting campaigns at this registrar. In these campaigns, attackers set up hundreds of subdomains mimicking popular target domains under `com-secure-login[.]info` and `com-finder-me[.]info`. An example level-squatting subdomain is `www.icloud.com-secure-login[.]info`. The second-most abused registrar, Openprovider, offers cheap and easy bulk registrations, attracting many squatting registrations. Additionally, we observed many domains from this registrar having their WHOIS records redacted for privacy. Our system discovered many level-squatting domains registered at TLD Registrar Solutions using the .support TLD (top-level domain), including `icloud.com-iphone[.]support` and `apple.com.recover[.]support`, which users might confuse with legitimate Apple technical support services.



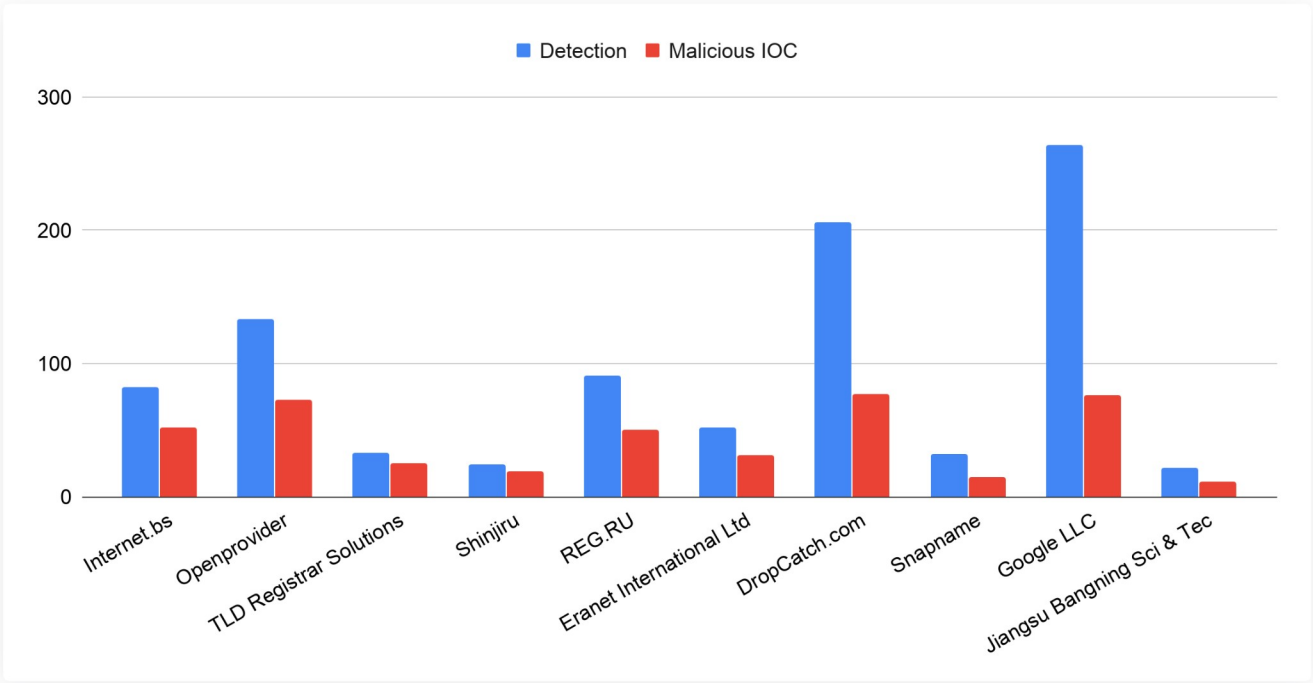
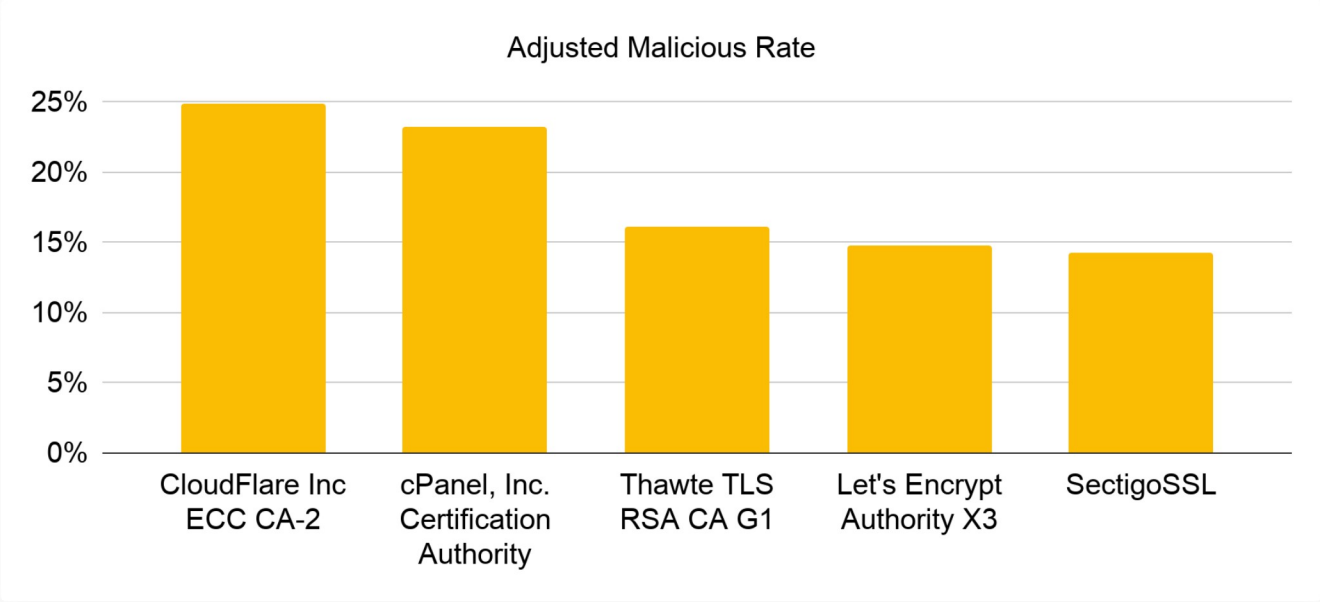


Figure 6. Top 10 most abused registrars in December 2019.

Top 5 Most Abused Certificate Authorities

As HTTPS became common, cybercriminals increased the use of certificates to make their websites appear legitimate. Figure 7 provides an overview of the certificate authorities (CAs) preferred by squatting sites. The most popular CA is Cloudflare, as it offers a bundle, including free SSL encryption. The second most popular CA, cPanel Inc CA, is preferred by domain squatters because of the convenience and the ease of its AutoSSL services. Through cPanel's management interface, their customers are able to finish all steps of SSL encryption, including certificate purchase, automatic installation and renewal. Thawte CA is not a trusted CA anymore, and browsers will label

their certificate as suspicious, but squatting domains are still using it.



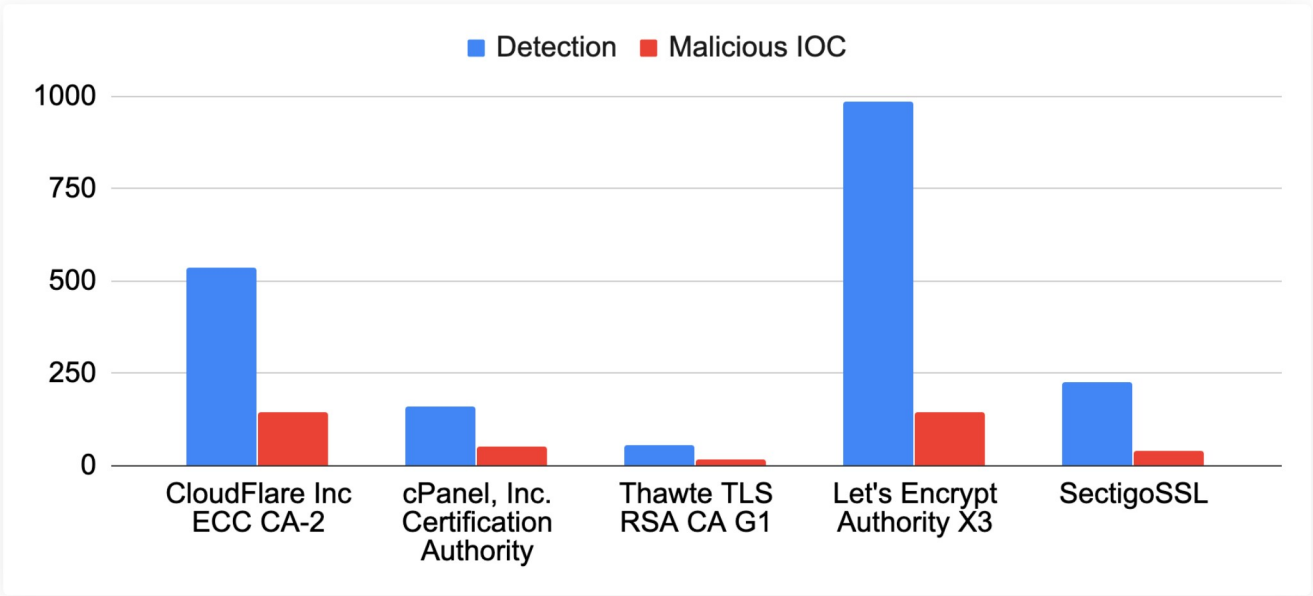


Figure 7. Top 5 most abused certificate authorities in December 2019.

Malicious Usages and Threats

In this section, we discuss in detail different types of abuse leveraging squatting domains. It includes malware distribution, phishing, C2 communication, potentially unwanted programs (PUPs), scams, ad-laden sites and affiliate marketing.

Phishing

Phishing is one of the most popular threats leveraging squatting domains. All of the different squatting techniques we discussed can be used to lure users into believing that a squatting domain is owned by the legitimate brand and to increase the efficiency of phishing and scam campaigns.

One example is a combosquatting domain, `secure-`**`wellsfargo`**`[.]org`, which targets Wells Fargo's customers. This domain hosts a copy of Wells Fargo's official site, as illustrated in Figure 8.a. However, this site is only the front-end portion of the original site, redirecting all clicks to the same login page (shown in Figure 8.b) to steal customers' sensitive information, including email credentials and ATM PINs.

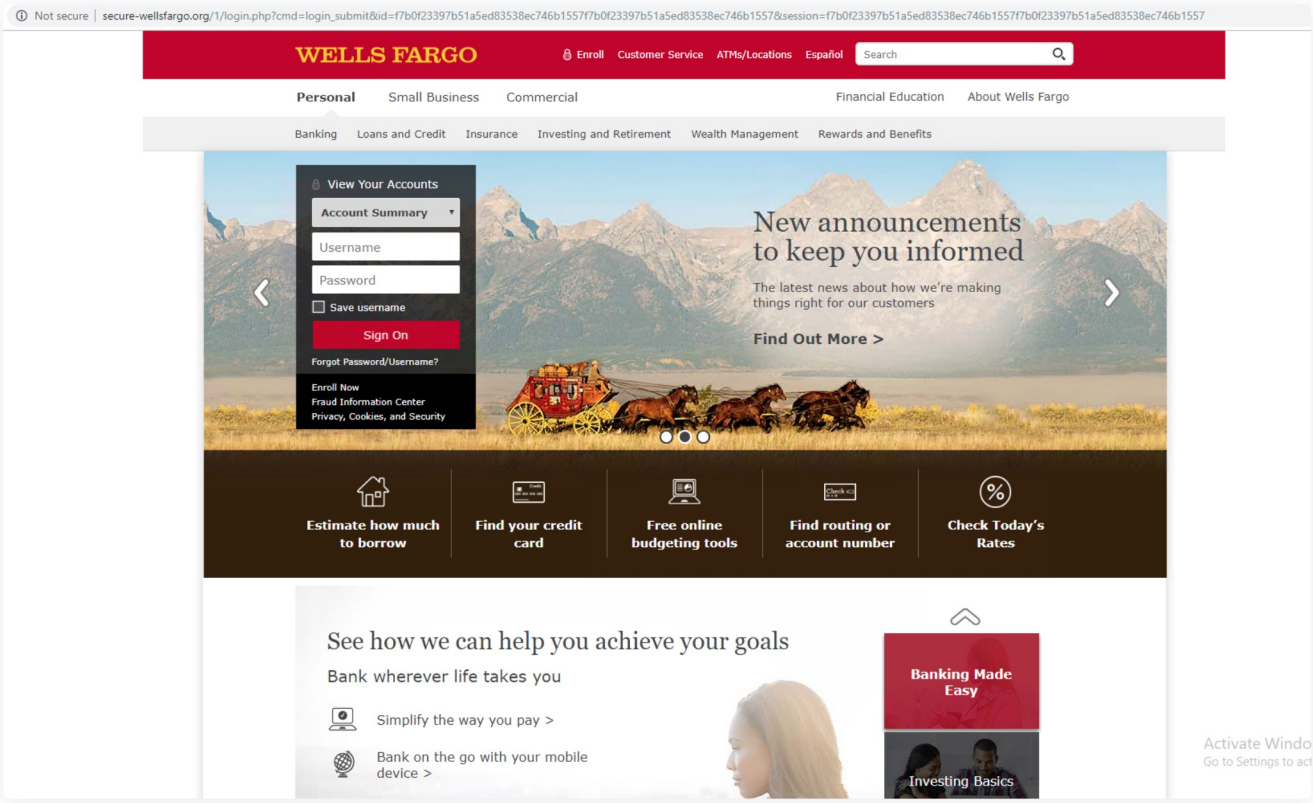


Figure 8.a. Fake Wells Fargo website: secure-wellsfargo[.]org

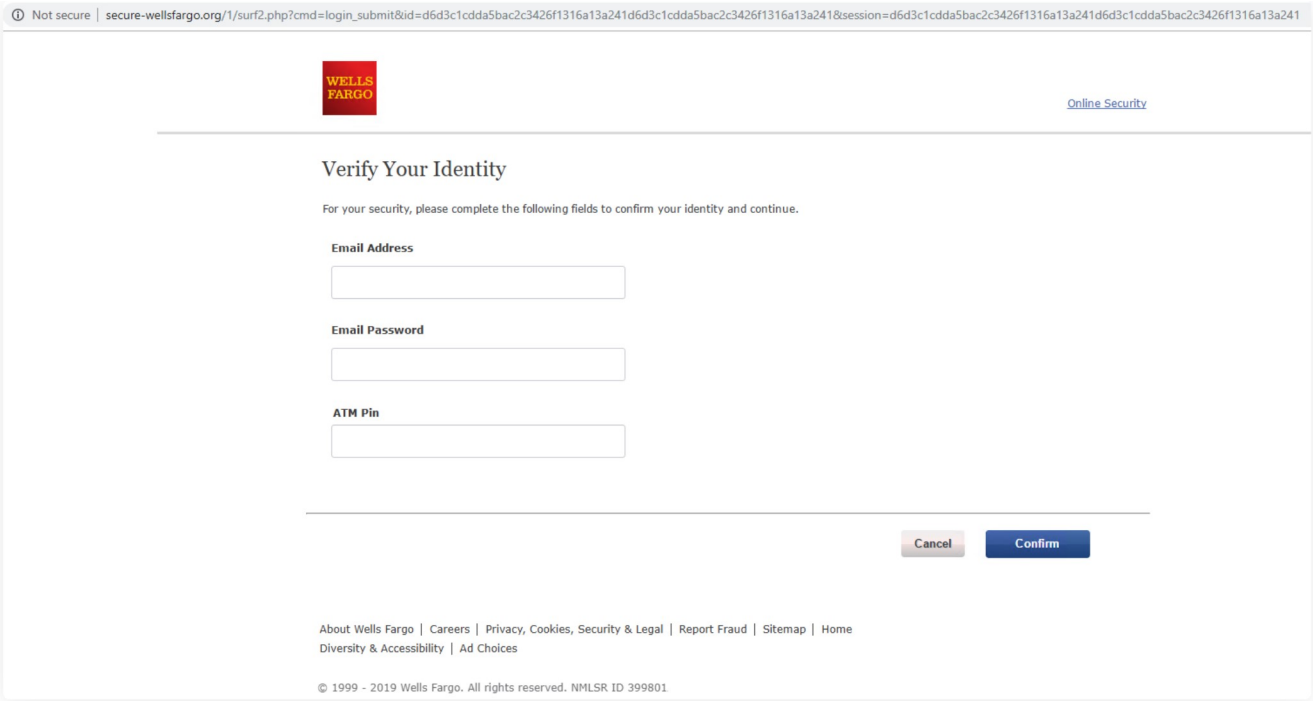


Figure 8.b. Phishing login page for secure-wellsfargo[.]org

Figure 9 demonstrates how another combosquatting domain, **amazon**-india[.]online, mimicking Amazon, is set up to steal user credentials, specifically targeting mobile users in India. As a common strategy, all links on this site first redirect users to the same product page (the middle screenshot in Figure 9) and then to the payment page. In this particular case, the perpetrators did not even go through the trouble of optimizing the phishing page for desktop users.

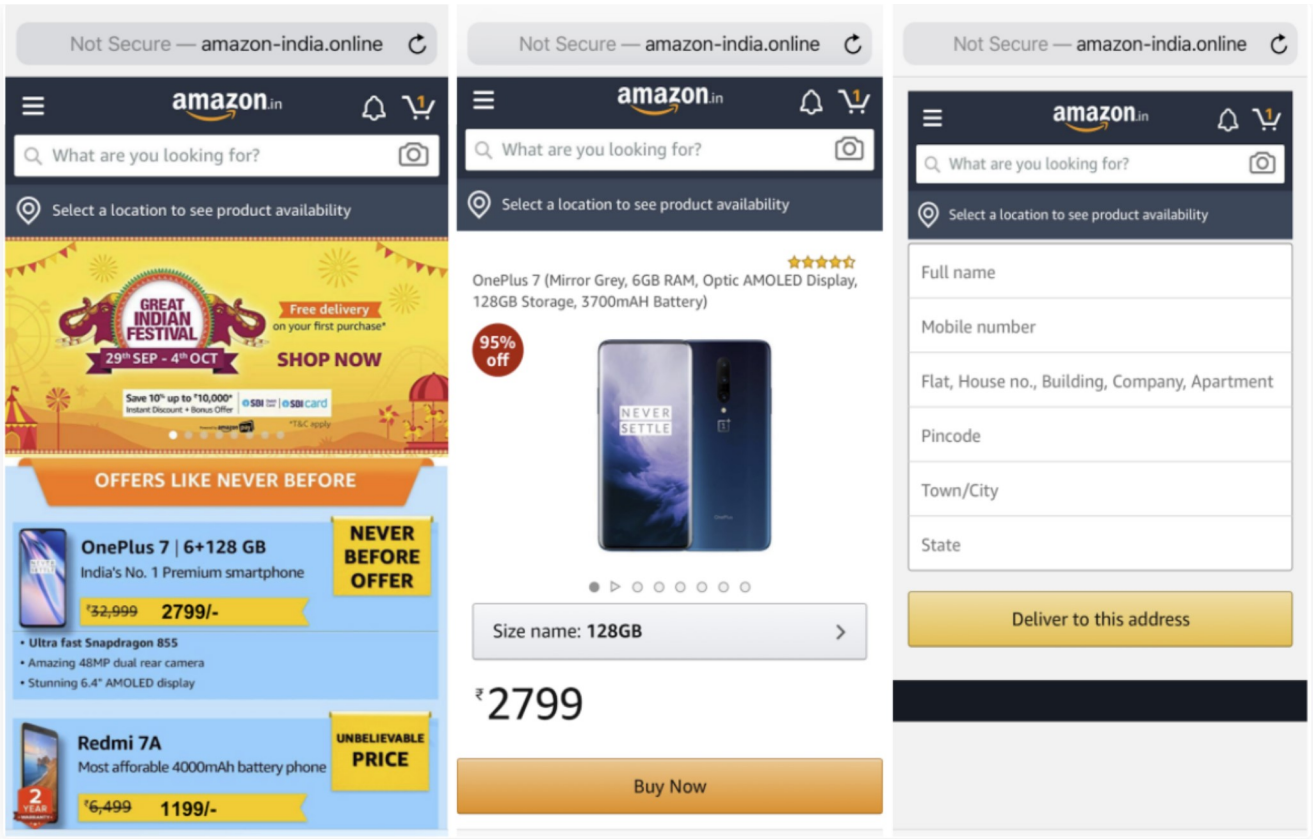


Figure 9. Fake Amazon website: amazon-india[.]online

Malware Distribution

Squatting domains are also often used to distribute malware. A combosquatting domain mimicking Samsung (**samsung**eblya**iphone**[.]com) hosts Azorult malware `5acd6d9ac235104f90f9a39c11807c37cdfb103d6c151cc1a2e4e38bf3dbe41f` on the URL **samsung**eblya**iphone**[.]com/dolce.exe. Azorult malware is a credential and payment card information stealer, usually spread by phishing emails. It has been an active threat since 2016 and is one of the top malware families. Once the malware executes, it will generate a unique identifier for the compromised machine based on the machine's globally unique identifier and username. Then the malware will contact the C2 server with this identifier, and it will retrieve the configuration of the infected machine, including the running processes and services. Additionally, Azorult malware often downloads payload from other compromised servers. The new payload can collect and send out sensitive data such as cookies, browser credentials and cryptocurrency information.

Analyzing the malware sample downloaded from **samsung**eblya**iphone**[.]com, we found that it attempted to send a POST request to **samsung**eblya**iphone**[.]com/index.php, which is consistent with this malware family's known behavior to exfiltrate data. Besides the observed network activity, the malware also displayed suspicious behaviors such as changing the settings of Internet Explorer.

Command & Control (C2)

Malware instances on infected machines typically need to "phone home" to a C2 server for further commands to execute, to download new payloads or to perform data exfiltration. Malware often relies on domain names to locate C2 servers, and these domains are called C2 domains. While using squatting domains for C2 is uncommon, we speculate that the intention of those who do so is to evade automated detection (such as Domain Generation Algorithm detection) and manual analysis.

Our squatting detection system captured squatting domains mimicking Microsoft, **microsoft**-store-drm-server[.]com on January 30, 2020, and **microsoft**-sback-server[.]com on February 3, 2020. From the Palo Alto Networks WildFire Malware Analysis Engine, we retrieved similar malware samples, including fa28b59eb0ccd21d3994b0778946679497399b72c2e256ebf2434553cb7bf373 and e7fb436bf7d8784da092315bce1d3511a6055da41fe67362bad7a4c5d3f0294e, connecting to them. These two domain names used the previously mentioned DNSPod for name resolution, which is infamous for being slow in responding to abuse investigations. First, the malware resolved these domains to the same IP address 217.182.227[.]117. Then, it communicated through SSL traffic with the same JA3 (SSL fingerprint): 6312930a139fa3ed22b87abb75c16afa on client-side and 4192c0a946c5bd9b544b4656d9f624a4 on server-side. Observing the same behavior, we conclude they were using the identical SSL application and were part of the same campaign.

Similar to most C2 domains, these two squatting domains were short-lived. They were only used for one to two days after registration and were then abandoned by attackers. Tracking 217.182.227[.]117, we are able to find other C2 domains used by this campaign: store-in-box[.]com from Jan. 27-28, stt-box[.]com from Jan. 29-31, **microsoft**-store-drm-server[.]com from Jan. 31-Feb. 2, and **microsoft**-sback-server[.]com on February 3.

Potentially Unwanted Program (PUP)

A PUP could be either standalone software, like spyware or adware, or a browser extension. PUPs usually perform unwanted changes, like changing the browser's default page or hijacking the browser to insert ads. Researchers have shown that some PUP downloaders are also repurposed for malware campaigns. Websites hosting PUPs usually try to scare users by showing them warning messages like "Your computer is infected!" or "Your license has expired!" to convince them to download the advertised software.

Figure 10 shows a combosquatting domain mimicking Walmart (**walrmart**44[.]com) that distributes PUP. Depending on the browser used, it redirects users to landing pages offering different types of PUPs for download. When we visit this domain in Safari, it tells us that our Flash player might be outdated and offers us the chance to download the newest version from their site, as illustrated in Figure 10.a. While using Chrome, we get a "click continue and install extension" page, as shown in Figure 10.b, which redirects users to the Chrome store for the "Security for Chrome" extension. Alternatively, this website will occasionally redirect users to various legitimate ecommerce websites, including Walmart, Amazon and Aliexpress. After repeated visits, it will remember the source IP address and reject further visits even if we use different browsers (Figure 10.c).

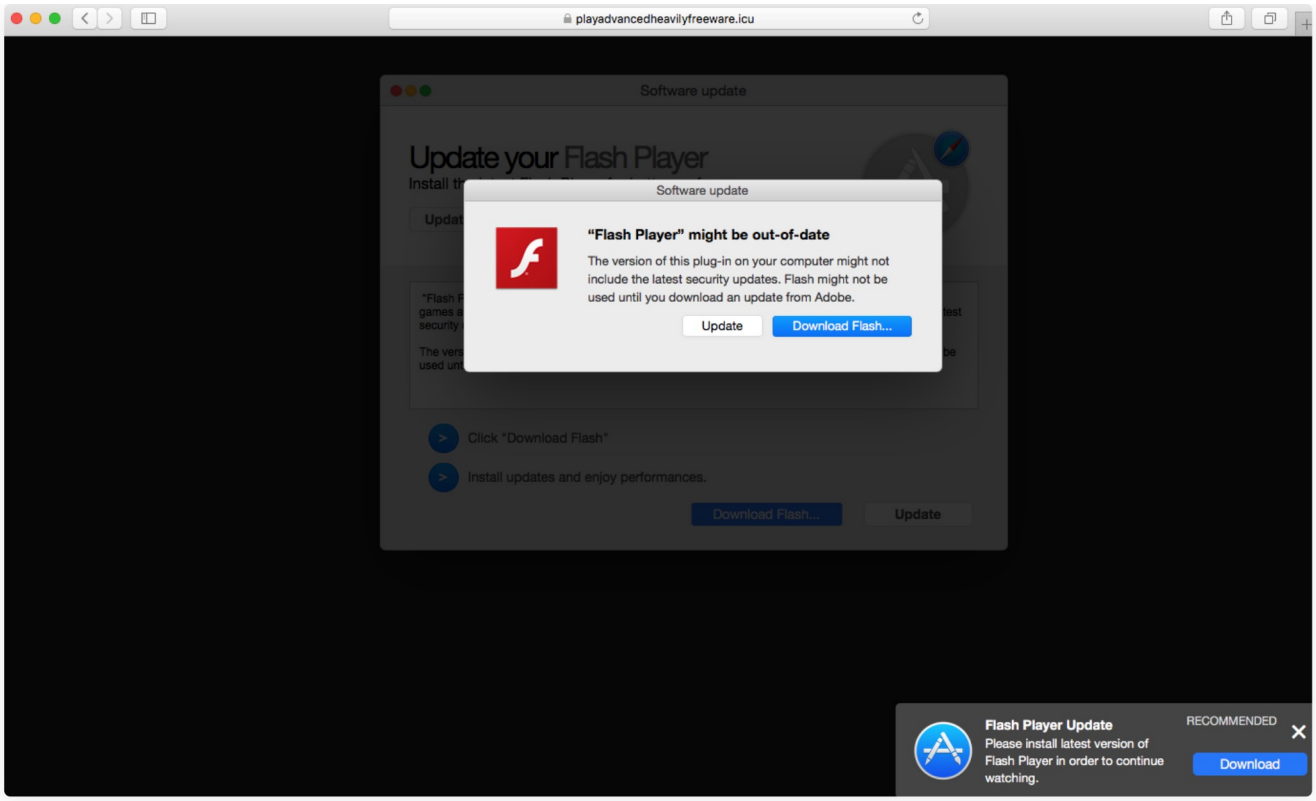


Figure 10.a. Redirection to PUP installation in Safari from walrmart44[.]com

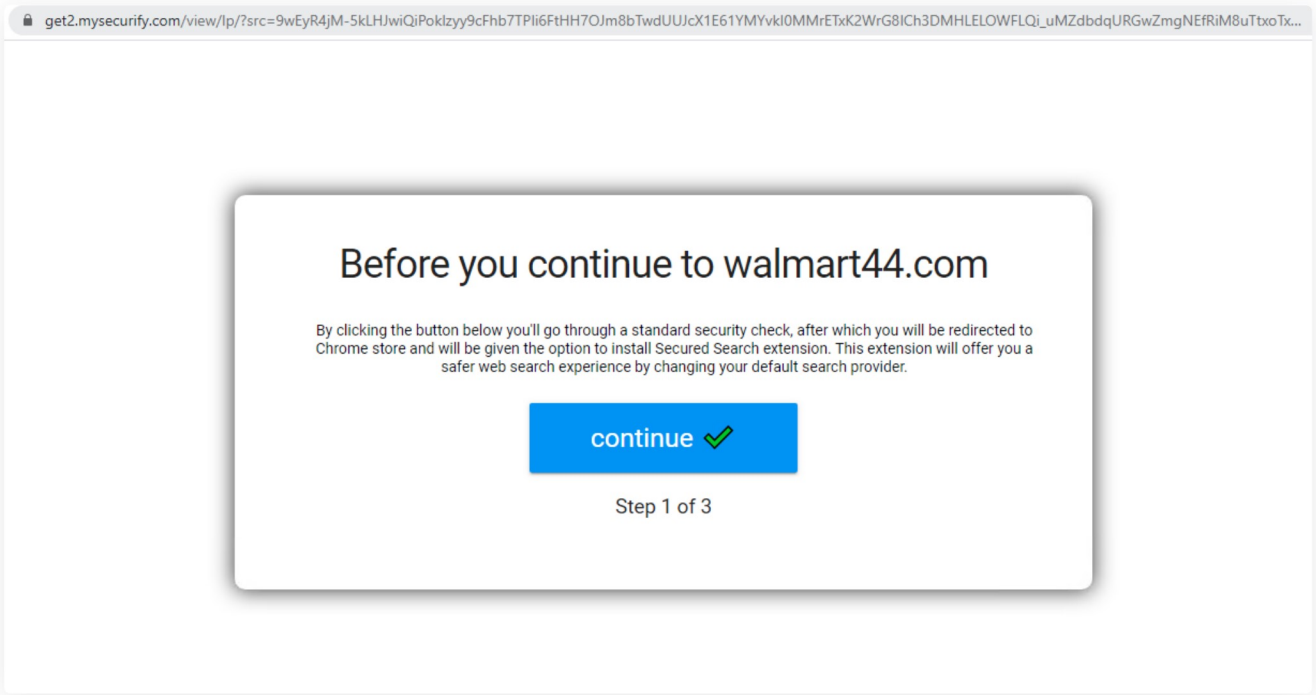


Figure 10.b. Redirection to PUP installation in Chrome from walrmart44[.]com

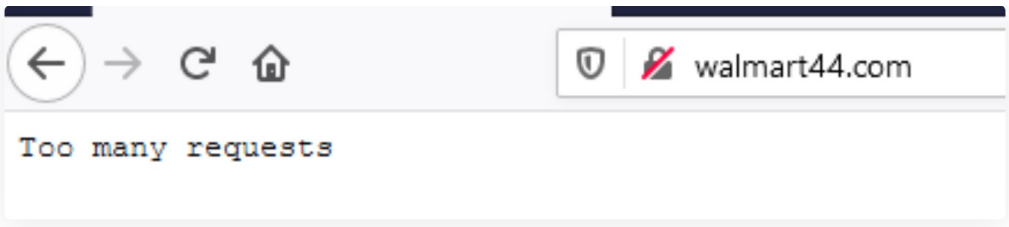


Figure 10.c. walrmart44[.]com blocks crawlers when visited too frequently.

A combosquatting domain mimicking Samsung (**samsung**`pr0mo[.]online`) looks like a legitimate Australian educational news website with a valid SSL certificate. However, visiting this site, users are faced with popup windows, warning them about security flaws (Figure 11.a). Clicking on the warnings, users are redirected to a fake virus scanning page, which recognizes their operating system to increase credibility but will always display the same list of detected viruses (Figure 11.b). Finally, clicking the "Proceed" button takes users to a download page for a system repair tool, which is legitimate but potentially unwanted.

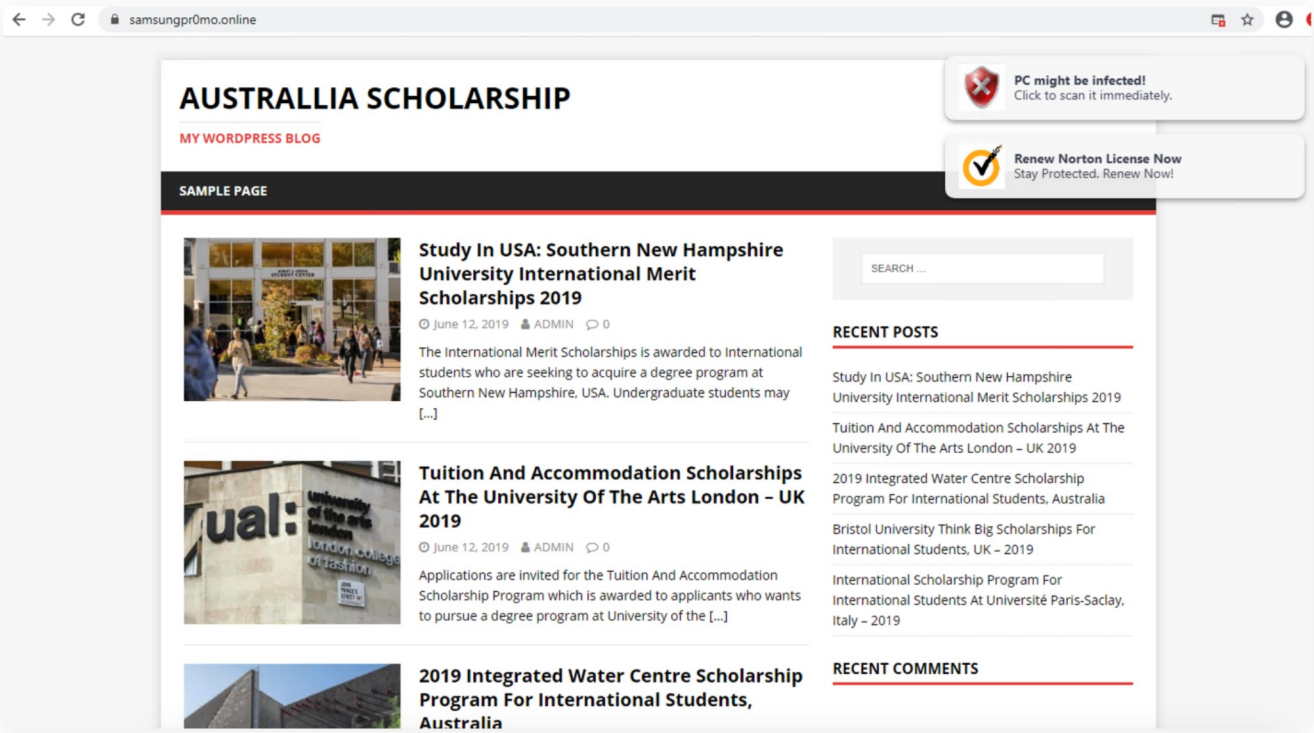


Figure 11.a. samsungpr0mo[.]online displaying warning messages in the top right corner.

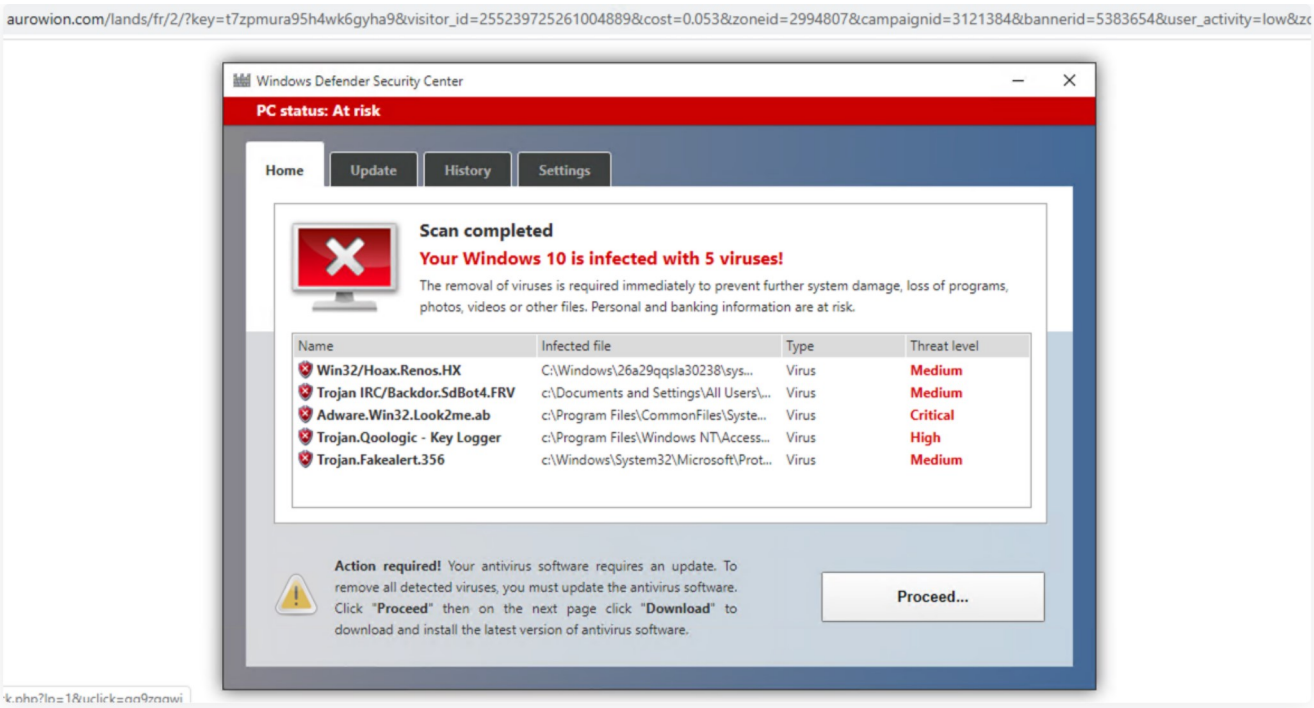


Figure 11.b. A fake virus scanning page displays after clicking on a warning message from samsungpr0mo[.]online

Technical Support Scam

Technical support scams are social engineering attacks. An associated website's purpose is to scare people with audio and visual warnings into believing that their machine is compromised. It prompts people to call the displayed fake technical support center's phone number. When people call the number, scammers will try to persuade them that the only way to save their machine is by paying for the fraudulent support service. In the case of combosquatting, the domain name often contains keywords like "security," "alert" and "warning." An example domain mimicking Microsoft (**`microsoft`**`-alert[.]club`) shown in Figure 12.a was registered on June 11, 2020. This website presents warning messages in Japanese (translated to English in Figure 12.b), renders dynamic content, such as a running command line window, and plays audio alerts.

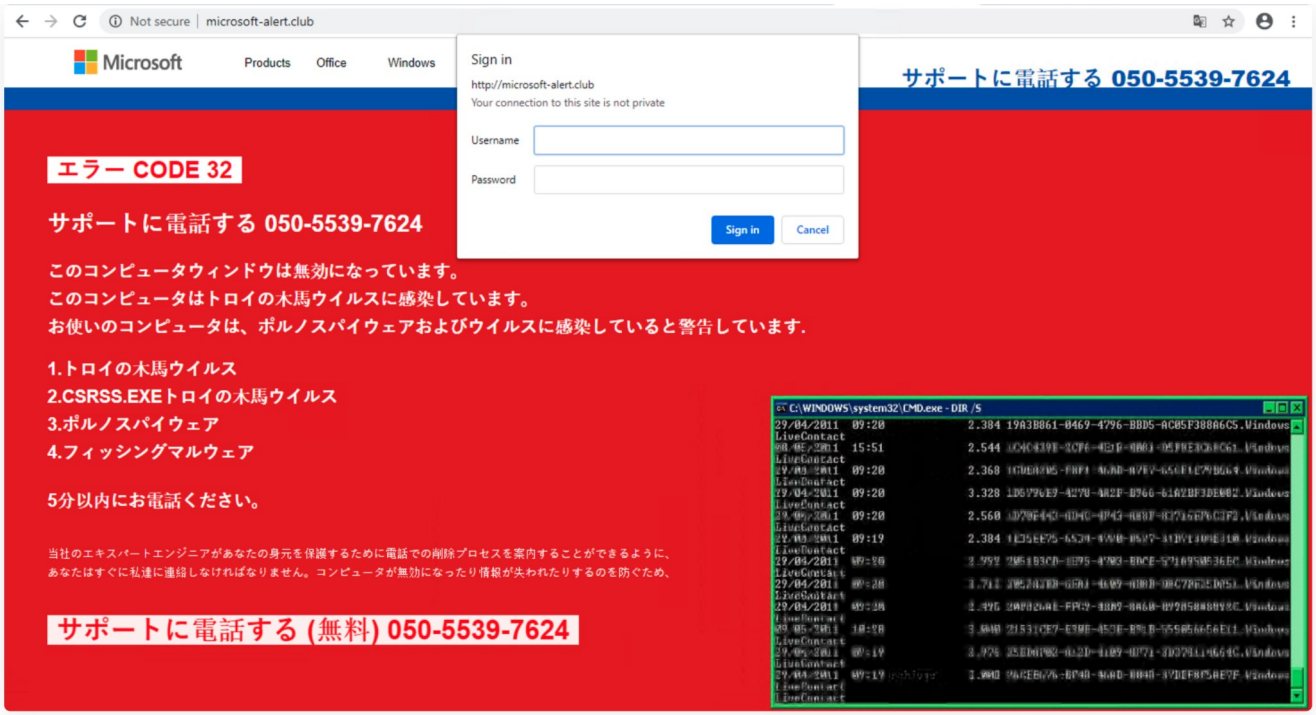


Figure 12.a. A technical support scam page hosted on microsoft-alert[.]club

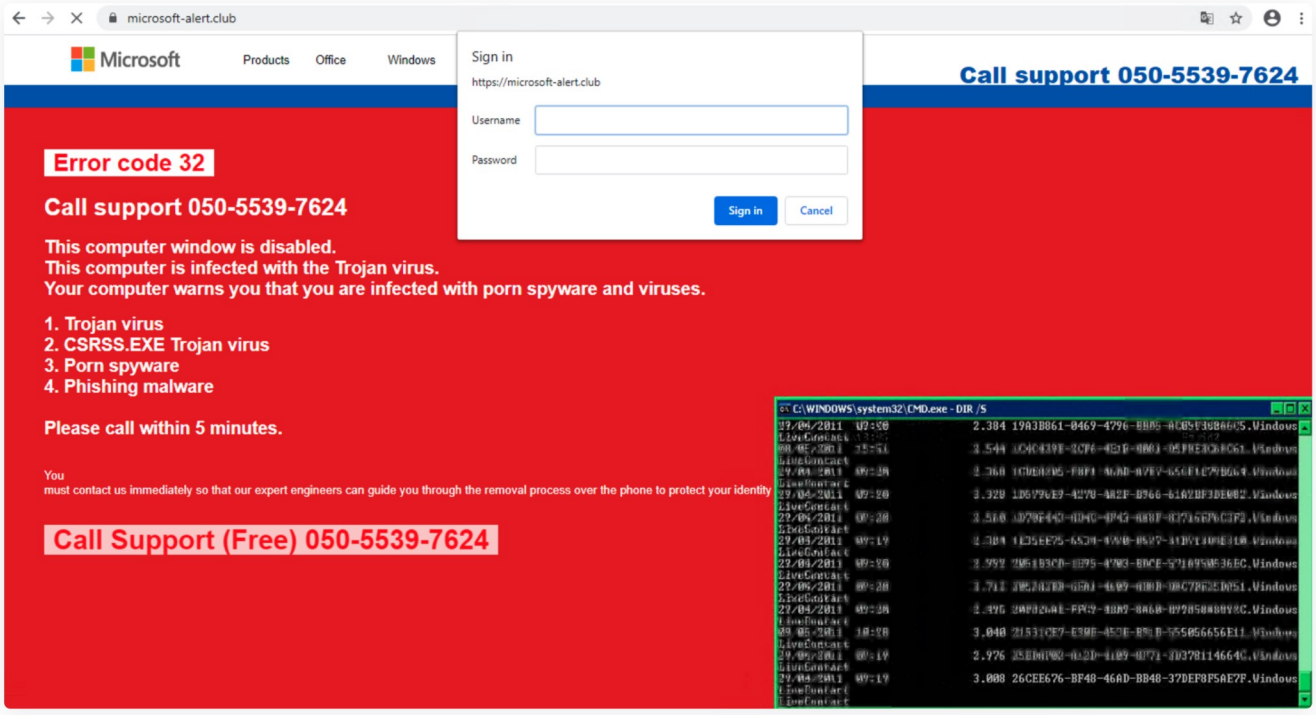


Figure 12.b. Translated to English.

Re-bill Scam

Re-bill scammers first offer a subscription to products such as weight loss pills in exchange for a small initial payment. However, if users don't cancel the subscription after the promotion period, a

much higher cost will be charged to their credit cards, usually $50-100. Additional information on this type of scam can be found in Unit 42's previous research on deceptive affiliate marketing. The combosquatting domain **`netflix`**`brazilcovid[.]com` leverages both Netflix and the COVID-19 pandemic. The main page looks like the Portuguese Netflix site (Figure 13.a), and has the purpose of obtaining user email addresses. (It is shown translated to English in Figure 13.b.) A deceptive reward message (Figure 13.c) is then shown to potential victims. Finally, users are redirected to a survey and then to a re-bill scam page (Figure 13.d).

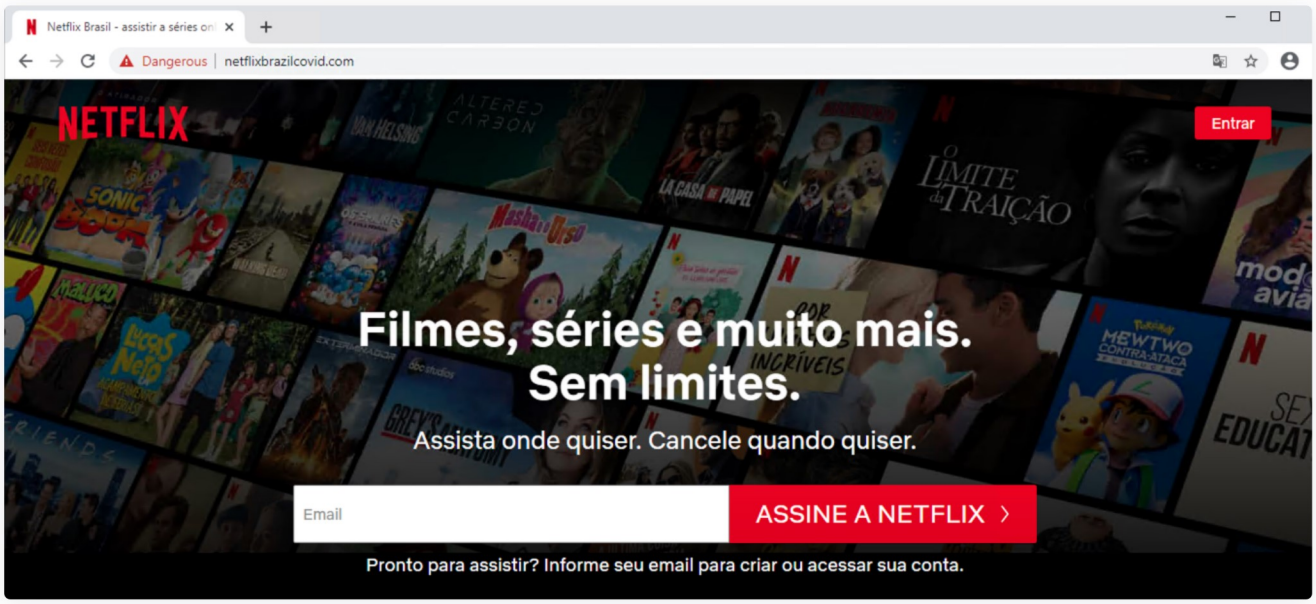


Figure 13.a. A fake Netflix main page hosted on netflixbrazilcovid[.]com

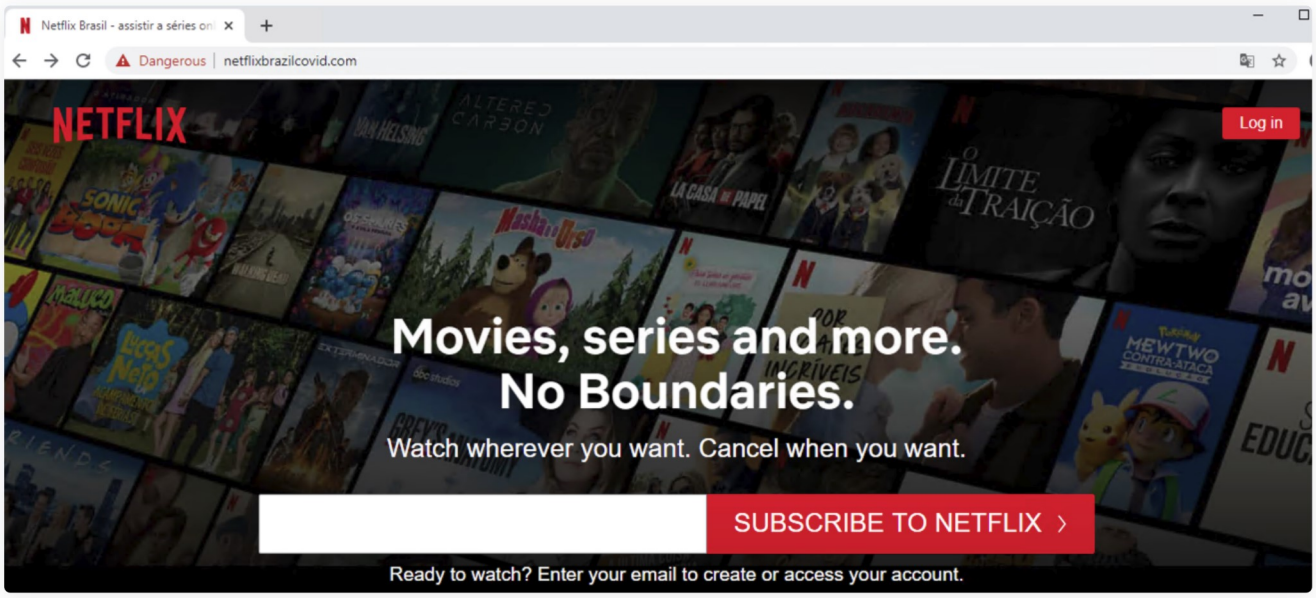


Figure 13.b. Translated to English.

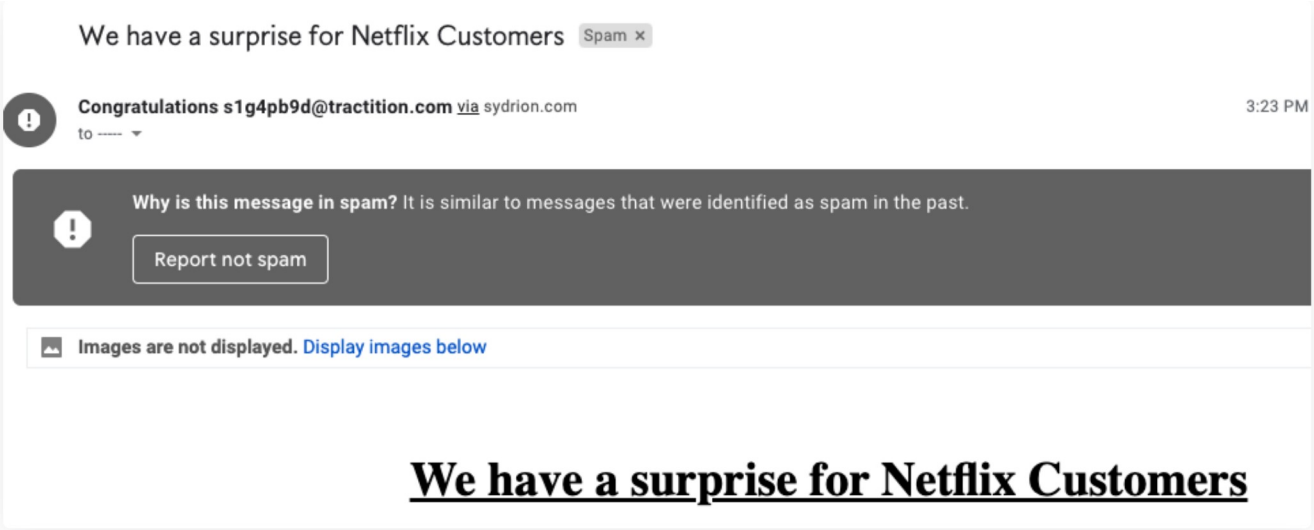


Figure 13.c. Deceptive social engineering reward email.

Figure 13.d. A re-bill scam page distributed by deceptive reward email.

Reward Scam

Another popular scam offers users rewards such as free products or money. When we initially captured **`facebook`**`winners2020[.]com`, it was under development with placeholder images and texts, as shown in Figure 14.a. However, the perpetrators recently replaced placeholders with

meaningful content. From the screenshot, we could tell the page mimics a free lottery related to Facebook. To claim the prize, users need to fill out a form with their personal information such as date of birth, phone number, occupation and income (Figure 14.b).

Figure 14.a. Reward scam page under development: facebookwinners2020[.]com

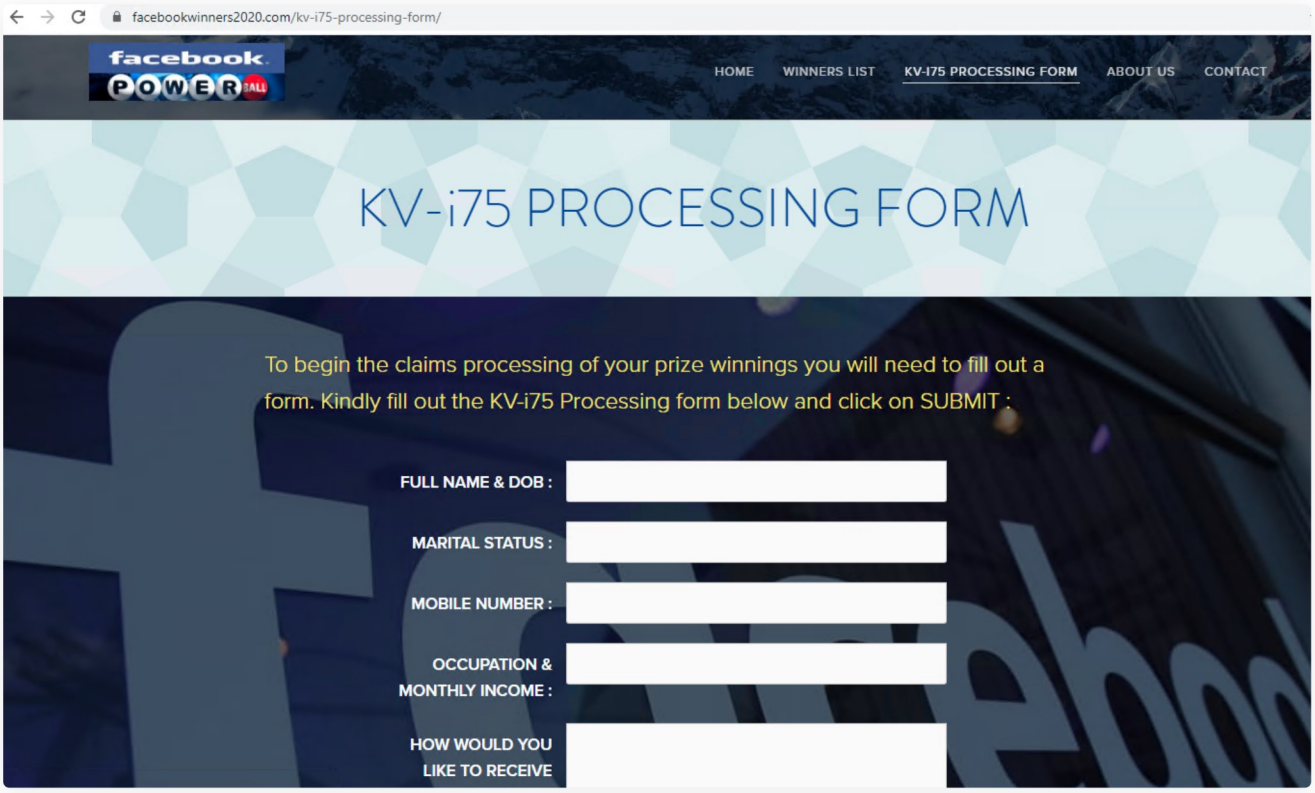


Figure 14.b. An application form on facebookwinners2020[.]com requesting personal information.

Domain Parking

A common and easy way to monetize user traffic is to use a parking service by pointing the squatting domain's IP address or NS record to the parking service's servers. Figure 15 provides an example of a parked domain mimicking RBC Royal Bank, `rby`**`royalbank`**`[.]com`, leveraging a popular parking service, ParkingCrew, to generate profit based on how many users land on the site and click the advertisements. In some cases, parking services also redirect users to scam and phishing pages. As the hostname in the certificate is different from the squatting domain, the browser will label it as "Not secure." Parked pages usually show users a list of advertisements related to the parked domain. In our example, the ads shown are related to financial services.

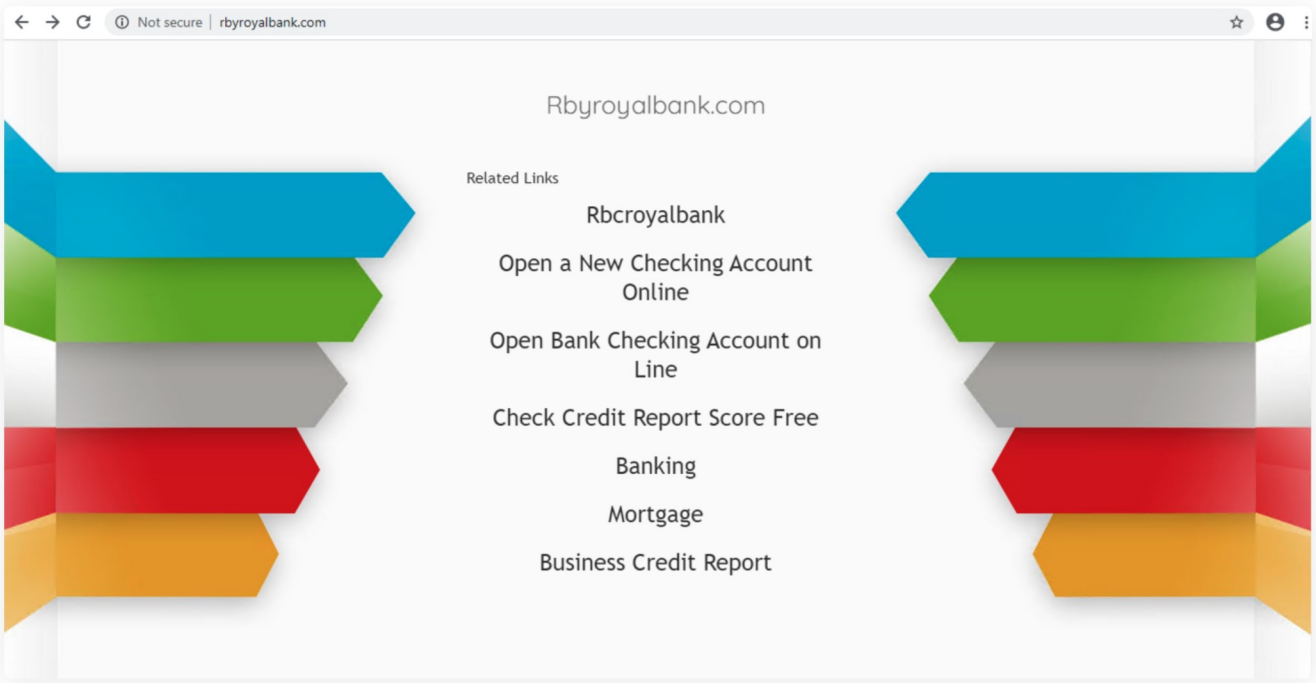


Figure 15. A parked page for rbyroyalbank[.]com

Conclusion

In summary, domain squatting techniques leverage the fact that users rely on domain names to identify brands and services on the Internet. These squatting domains are often used for nefarious activities, including phishing, malware and PUP distribution, C2 and various scams. A high rate of malicious and suspicious usage among squatting domains was observed. Therefore, continuous monitoring and analysis of these domains are necessary to protect users.

Palo Alto Networks monitors newly registered domains and newly observed hostnames from pDNS and Zone files to capture emerging squatting campaigns. Our automatic pipeline publishes the

domains it detects to URL Filtering and DNS Security using the appropriate category, including malware, phishing, C2 or grayware.

Analyzing the squatting ecosystem, we found that domain squatters prefer certain types of target domains, registrars, hosting services and certificate authorities. The following attributes are common in cases of malicious squatted domains:

- Domain names that are targeting known financial, shopping and banking domains.
- Domains that use frequently abused registrars and hosting services.
- Domains that do not have completely validated SSL certificates.

Therefore, we advise everyone to be more careful when encountering these domains.

Palo Alto Networks customers using URL Filtering, DNS Security, WildFire and Threat Prevention are protected from the threats related to squatting domains mentioned in this blog. Using AutoFocus, our customers can further study the malware mentioned in this blog by using the tag AzoRult.

Acknowledgements

Special thanks to Daiping Liu, Kelvin Kwan, Laura Novak, Jun Javier Wang, Vicky Ray, Eddy Rivera, Erica Naone and Arun Kumar for their help with improving the blog.

IOCs

Sha256

5acd6d9ac235104f90f9a39c11807c37cdfb103d6c151cc1a2e4e38bf3dbe41f

fa28b59eb0ccd21d3994b0778946679497399b72c2e256ebf2434553cb7bf373

e7fb436bf7d8784da092315bce1d3511a6055da41fe67362bad7a4c5d3f0294e

JA3 Pair

Client JA3: 6312930a139fa3ed22b87abb75c16afa

Sever JA3: 4192c0a946c5bd9b544b4656d9f624a4

Malware/Phishing Squatting Hostname

amazon-india[.]online

apple.com.recover[.]support

com-finder-me[.]info

com-secure-login[.]info

facebook.com-account-login-manage.yourfiresale[.]com

icloud.com-iphone[.]support

microsoft-alert[.]club

microsoft-sback-server[.]com

microsoft-store-drm-server[.]com

microsoft[.]com (xn--microsof-wyb[.]com)

netflix-payments[.]com

netflixbrazilcovid[.]com

rbyroyalbank[.]com

safety.microsoft.com.mdmfmztwjj.l6kan7uf04p102xmpq[.]bid

samsungeblyaiphone[.]com

samsungpr0mo[.]online

secure-wellsfargo[.]org

store-in-box[.]com

stt-box[.]com

www.icloud.com-secure-login[.]info

Grayware Hostname

4ever21[.]com

facebookwinners2020[.]com

micposoft[.]com

walrmart44[.]com

whatsalpp[.]com

URL

samsungeblyaiphone[.]com/dolce.exe

samsungeblyaiphone[.]com/index.php

IP

217.182.227[.]117

1. Anti-cybersquatting Consumer Protection Act (ACPA) (15 USC §1125(d)) ↑