Domain Parking: A Gateway to Attackers Spreading Emotet and Impersonating McAfee

36,813 people reacted

👍 20 11 min. read

SHARE

By Ruian Duan, Zhanhao Chen, Seokkyung Chung, Janos Szurdi and Jingwei Fan

October 29, 2020 at 3:00 AM
Category: Malware, Unit 42
Tags: cybersquatting, domain parking

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

Executive Summary

Domain parking services offer a simple solution for domain owners to monetize their sites' traffic through third-party advertisements. While domain parking might appear harmless at first glance, parked domains pose significant threats, as they can redirect visitors to malicious or unwanted landing pages or turn entirely malicious at any point in time.

We have been detecting parked domains for more than nine years. From March to September 2020, we identified 5 million newly parked domains. In the same time frame, we observed that 6 million parked domains have transitioned to other categories. Out of the transitioned parked domains, 1.0% changed to *malicious* categories (such as phishing or malware); 2.6% changed to *not safe for work* categories (such as adult or gambling); and 30.6% changed to *suspicious* categories (such as questionable or high Risk). Compared to a *benign* domain (such as computer and internet info or

shopping), a parked domain has an eight times higher probability of changing its category to one of the above non-benign categories.

In this blog, we further investigate the domain parking ecosystem and outline different types of abuse, including:

- **Domain registration abuse:** We observed the malicious life cycle of the domain `valleymedicalandsurgicalclinic[.]com`, which is no longer active, as part of a global Emotet campaign. Emotet is one of the most popular malware families distributed via phishing emails. During this campaign, Palo Alto Networks observed attacks against organizations in various industries (such as education, government, energy, manufacturing, construction and telecommunications) all over the world, including the United States, the United Kingdom, France, Japan, Korea and Italy. The attack targeting French organizations also exploited the COVID-19 global pandemic: It used *Covid19* as the phishing email's subject line. None of these attacks were successful.

- **Advertisement abuse (case 1):** We observed attackers abusing the domain `peoplesvote[.]uk` related to the current U.S. presidential election. While visiting `peoplesvote[.]uk`, users are presented with an ad listing page most of the time. However, occasionally, users are first redirected to `0redira[.]com/jr.php`, which hosts an exploit kit script, and subsequently users are redirected to a survey website asking about users' voting preference of Joe Biden or Donald Trump. The exploit kit script hosted on `0redira[.]com/jr.php` fingerprints the browser silently to track users' web activity and hides the landing URLs to prevent security companies and researchers from analyzing and blocking them. Of note, these pages are still active as of this writing.

- **Advertisement abuse (case 2):** Furthermore, we observed a domain, `xifinity[.]com`, mimicking `xfinity[.]com`. When a user attempts to visit the Xfinity website but accidentally types an additional "i," they will go to `xifinity[.]com` and will be redirected to an abusive landing page, `antivirus-protection[.]com-123[.]xyz`. Both domains are active as of this writing. The landing page tries to fool users into believing that their machine is infected and that their McAfee subscription has expired. Clicking on the "Proceed" button will redirect users to a legitimate McAfee download page offering an antivirus subscription. We believe that attackers are abusing McAfee's affiliate program to steal ad revenue.

Security best practice for enterprises is to *keep close track* of parked 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.

Palo Alto Networks Next-Generation Firewall customers can *block* the parked category with the URL Filtering and DNS Security subscriptions.

Domain Parking: Why and How

Individuals and enterprises need to pay registrars (ICANN accredited domain resellers) an annual fee to buy domain names and become domain owners. If domain owners don't have content or service ready to point their domains to, they can leverage parking services to monetize user traffic. Setting up a parking service is simple and only requires domain owners to point their name server (NS) records to the parking service. In return, parking services will either present visitors with a list of advertisements or automatically redirect users to advertisers' webpages. In the first case, domain owners and parking services get paid when a user clicks on an ad, while in the second case, they get paid per user visit. Some domain owners buy large amounts of domain names as an investment to resell them later for a profit or to monetize user traffic. As shown by previous research studies and this blog, parked domains can pose significant threats to end-users. Because of this, along with their questionable utility, it may be best to block parked domains.

Palo Alto Networks has deployed a comprehensive pipeline to track newly parked domains and to publish the detection results to URL Filtering. Recently, we have launched the parked category in DNS Security as well. In particular, our pipeline:

1. Monitors known parked service providers and their infrastructure.
2. Tracks domain registrations and passive DNS queries and performs reverse DNS lookups.
3. Crawls website content.
4. Employs machine learning to combine multiple features to classify whether a domain is parked.

High-Level Statistics

To analyze the current parked domain landscape, we collected the parked domains that were detected from March to September 2020, as well as the ones whose category changed from parked to other categories in the same time span. On average, we found that 27,000 newly parked domains were identified and 35,000 existing parked domains were re-classified daily. In summary, our pipeline has identified 5 million newly parked domains and re-classified 6 million parked domains to other categories in the past six months.

Figure 1 summarizes how we observed parked domains changing during this time period. For simplicity, we group the URL Filtering categories into four classes: *malicious*, *not safe for work*, *suspicious* and *benign*. The *malicious* class consists of malware, command and control (C2), phishing and grayware. Adult, gambling and nudity are represented in the *not safe for work* class. For *suspicious*, we include questionable, insufficient content and high risk domains. Sites are deemed questionable based on suspicious web content, while the insufficient content category is normally applied to a blank website and high risk means the domain displays behavior similar to malicious domains. The *benign* class encompasses all other categories, such as business and economy, computer and internet info and shopping. Figure 1 shows that for parked domains, the *malicious* change rate is 1.0%, the *not safe for work* change rate is 2.6% and the *suspicious* change rate is 30.6%. As a comparison, the non-benign change rate of the parked category is eight times higher than the non-benign change rate of *benign* categories.

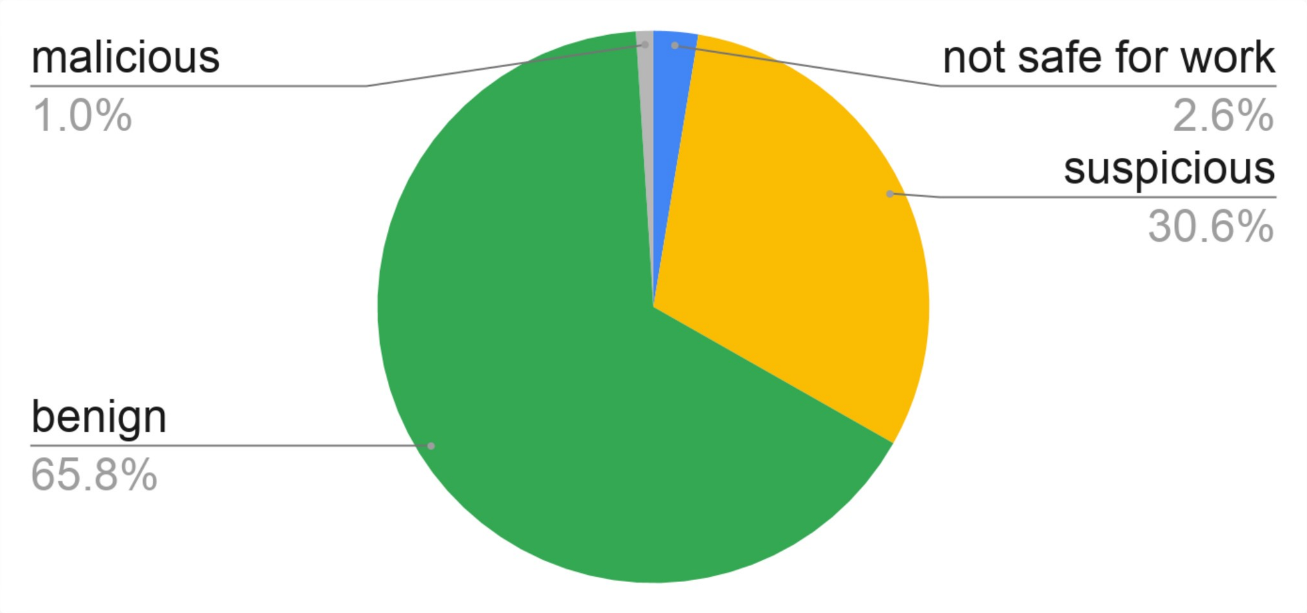


Figure 1. A list of categories that parked domains we observed changed to in the last six months.

Figure 2 presents the distribution of the number of days that domains that we ultimately categorize as *malicious* and *benign* are parked before changing their category. We aggregate the number of category changes from parked for every 10 parked days and normalize by the total number of domains per class. Figure 2 shows that over 25.9% of parked domains that changed to *malicious* categories are parked for less than 10 days, which is significantly different from *benign*, where the majority of them are parked for around 60-69 days. We conjecture that many cybercriminals do not age their domains (a practice used to evade domain lifetime-based detection features) and use them to conduct attacks as soon as possible.

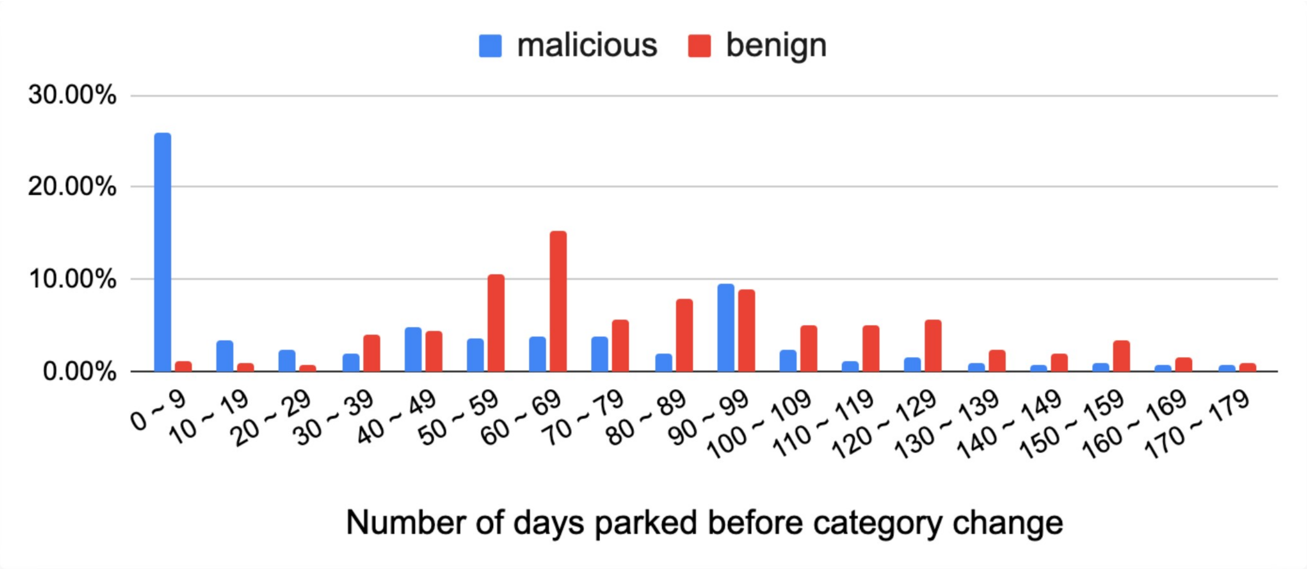


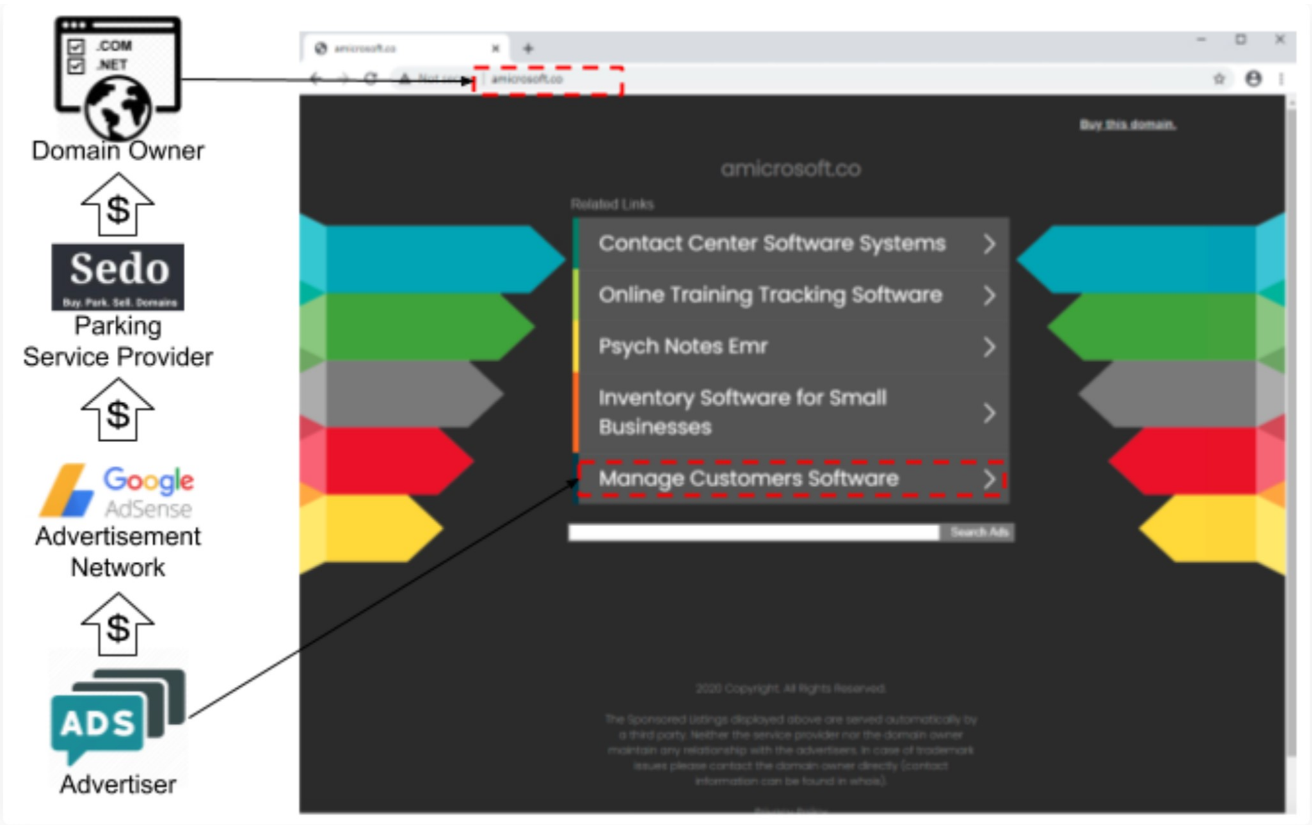
Figure 2. The number of days a domain is parked before a category change occurs, based on observations made during the last six months.

The Ecosystem and Attack Vectors

In this section, we further investigate the benefits of detecting and blocking parked domains. We begin by dissecting the domain parking ecosystem into different stakeholder groups. We then show that the largest attack vector is domain registration, since attackers can register parked domains and turn them malicious at any time. Second, we show that attackers can abuse the lack of advertisement control by some smaller advertisement networks used by parking services, thereby redirecting visitors to malicious or unwanted landing pages. Last, we show that even a parking service itself can pose privacy threats to users.

Stakeholders

We show the major stakeholder groups in the domain parking ecosystem and their relationships in Figure 3, namely *domain owners*, *parking service providers*, *advertisement networks* and *advertisers*. Note that the term *stakeholders* as used here represents roles and can refer to the same entity or multiple entities. Domain owners own parked domains and have the incentive to monetize through parking service providers. Parking service providers incorporate and organize feeds from advertisement networks to monetize user traffic. Advertisement networks characterize user traffic from parked domains and present ads to users from interested advertisers.



amicrosoft.co

Related Links

- Contact Center Software Systems
- Online Training Tracking Software
- Psych Notes Emr
- Inventory Software for Small Businesses
- Manage Customers Software

2020 Copyright. All Rights Reserved.

The Sponsored Listings displayed above are served automatically by a third party. Neither the service provider nor the domain owner maintain any relationship with the advertisers. In case of trademark issues please contact the domain owner directly (contact information can be found in whois).

Privacy Policy

Figure 3. Stakeholders in the domain parking ecosystem and their relationships.

As mentioned previously, domain owners need to point their NS records to the parking service's name server to "park" their domains. We measured the popularity of service providers by checking the DNS NS records of parked domains detected from March to September 2020. Figure 4 presents the top 15 most popular NS domains. The majority of parked domains are resolved by the NS of large registrars, including GoDaddy (`domaincontrol[.]com`) and NameBright (`namebrightdns[.]com`). Besides the large registrars and hosting providers, we identified several dedicated parking service providers. The most popular dedicated provider is Sedo (`sedoparking[.]com`), which is used by 19.5% of parked domains.

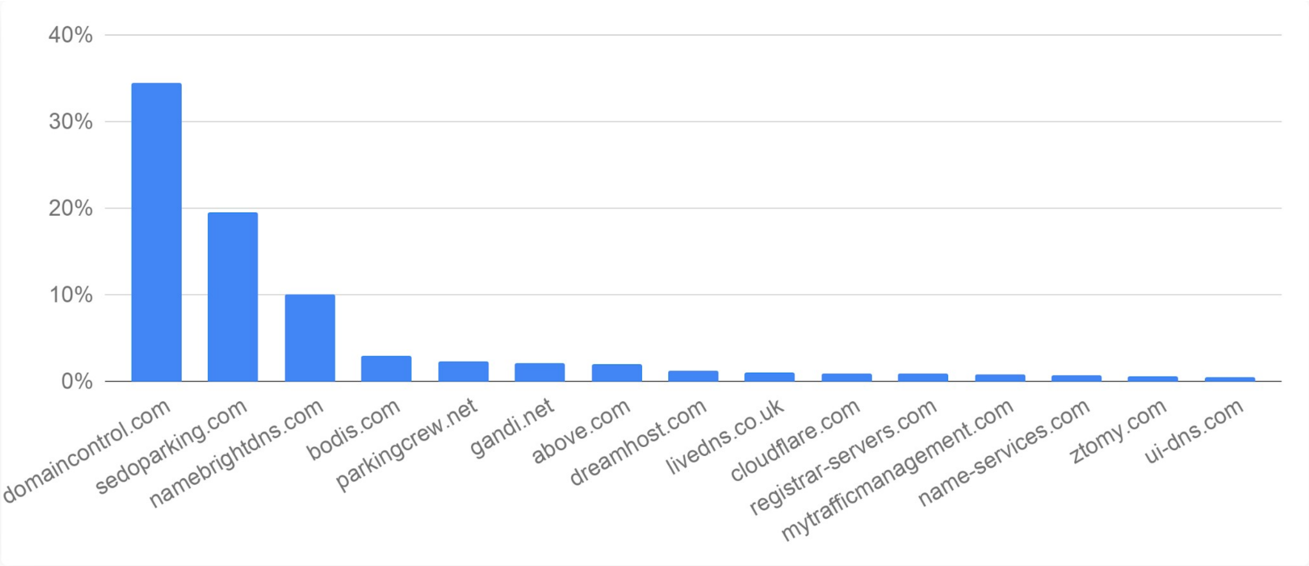


Figure 4. A list of parking service providers including registrars, hosting providers and dedicated parking providers.

Domain Registration Abuse

Parked domains could present threats to users when they turn malicious. Figure 1 shows that 1.0% of parked domains eventually changed to malicious categories such as C2 and malware. Some attackers appear to host parked pages on their domains before deploying malicious content, potentially to amortize their costs.

For example, we observed the malicious life cycle of the domain `valleymedicalandsurgicalclinic[.]com`. This domain was registered on July 8, 2020. Our newly registered domain detector found this domain, and our parking detector pipeline classified it as parked based on the website content. Two months later, our malware analysis engine, WildFire, captured multiple malware instances, such as SHA256: `a9fe73484674696be756808e93f839be7157cd65995d8de9e67e40bf77c9b229` and `54ac560845b09ce00a48b604ac7c440331cbde4362839a3dbf14c378230bee21` hosted on the URL `valleymedicalandsurgicalclinic[.]com/ujftb/statement/wr7hoba7i9hz` since Sept. 14, 2020. Furthermore, we discovered that it's part of a global Emotet campaign (refer to our recent Emotet blog for more information). Emotet is one of the most popular malware families distributed via phishing emails. The documents attached to the phishing emails contain macro scripts that call back to the C2 servers from victims' machines. Emotet further downloads Trojan payloads that steal victims' credential information or even compromises their machines. We can see many suspicious behaviors from these files, including incorrect file extensions and communication with multiple C2 servers, such as `50.91.114[.]38` and `51.38.124[.]206`. We sketch the phases of the Emotet campaign in Figure 5.

The observed campaign was launched using multiple domains around the world. During this campaign, Palo Alto Networks observed attacks against organizations in various industries (such as education, government, energy, manufacturing, construction and telecommunications) all over the world, including the United States, the United Kingdom, France, Japan, Korea and Italy. The attack targeting French organizations also exploited the COVID-19 global pandemic: It used *Covid19* as the phishing email's subject line (refer to our COVID-19 scams blog for similar cases). None of the attacks were successful.

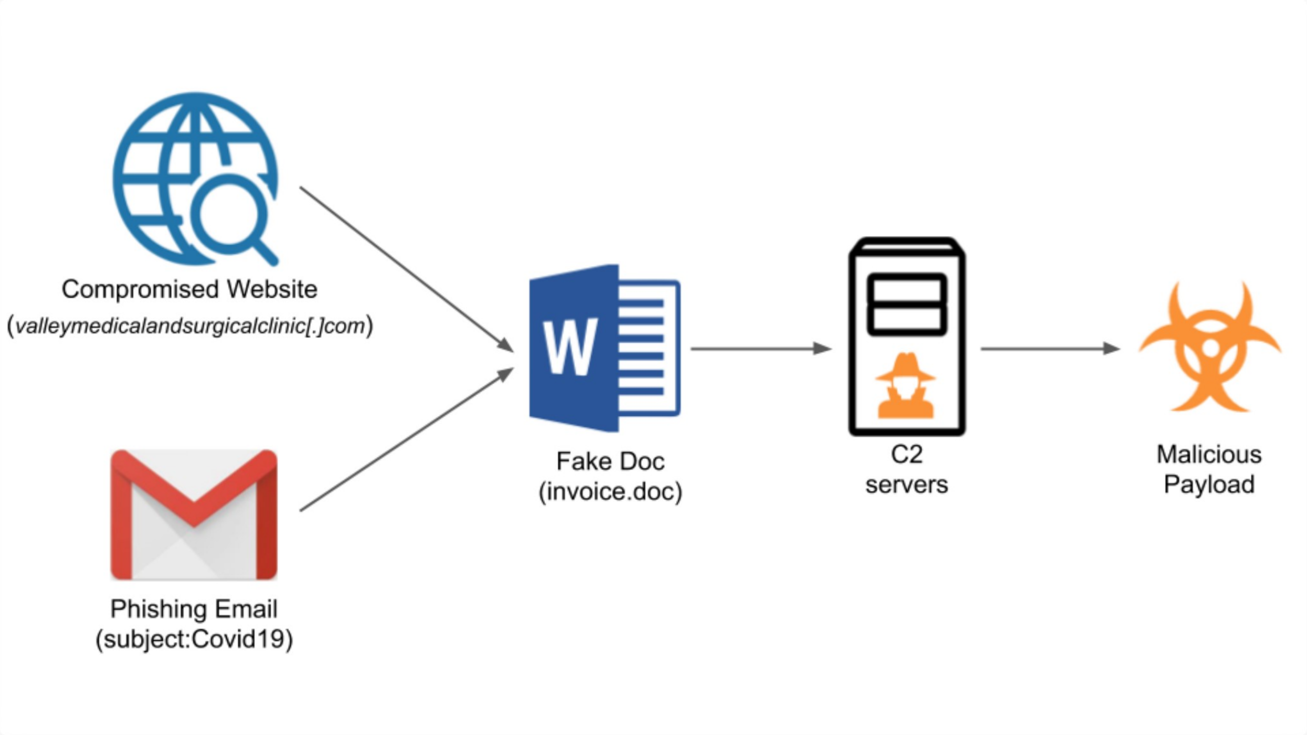
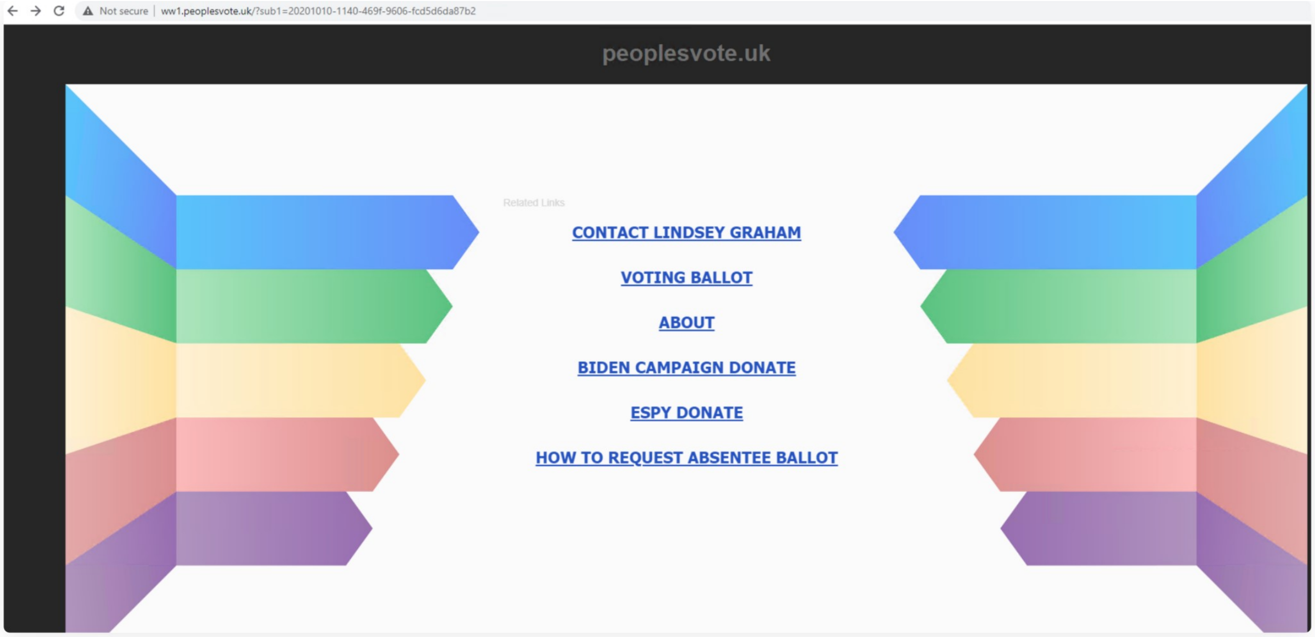


Figure 5. Illustration of the phases of the Emotet campaign.

Advertisement Abuse

The domain parking ecosystem depends on advertisers to profit from user traffic. As discussed earlier, parking services either show users a list of ads (and get paid based on the number of user clicks on these ads) or redirect users automatically to the advertisers' webpages (and get paid based on the number of user visits). Often the parking services and the advertisement networks do not have the means or willingness to filter abusive advertisers (i.e. attackers). Therefore, users are exposed to various threats, such as malware distribution, potentially unwanted program (PUP) distribution and phishing scams. In our experience, we most frequently observe the distribution of grayware.

We observed attackers abusing the domain `peoplesvote[.]uk` related to the current U.S. presidential election, which was allowed by the lack of control by `above[.]com`, the seventh-most popular domain parking service, as shown in Figure 4. While visiting `peoplesvote[.]uk`, users are presented with an ad listing page most of the time, as shown in Figure 6. However, occasionally, users are first redirected to `0redira[.]com/jr.php`, which hosts an exploit kit script, and subsequently redirected to a survey website asking about users' voting preference, as shown in Figure 7. The exploit kit script hosted on `0redira[.]com/jr.php` fingerprints the browser silently to track users' web activity and hides the landing URLs. Of note, these pages are still active as of this writing.



Not secure | ww1.peoplesvote.uk/?sub1=20201010-1140-469f-9606-fcd5d6da87b2

peoplesvote.uk

Related Links

CONTACT LINDSEY GRAHAM

VOTING BALLOT

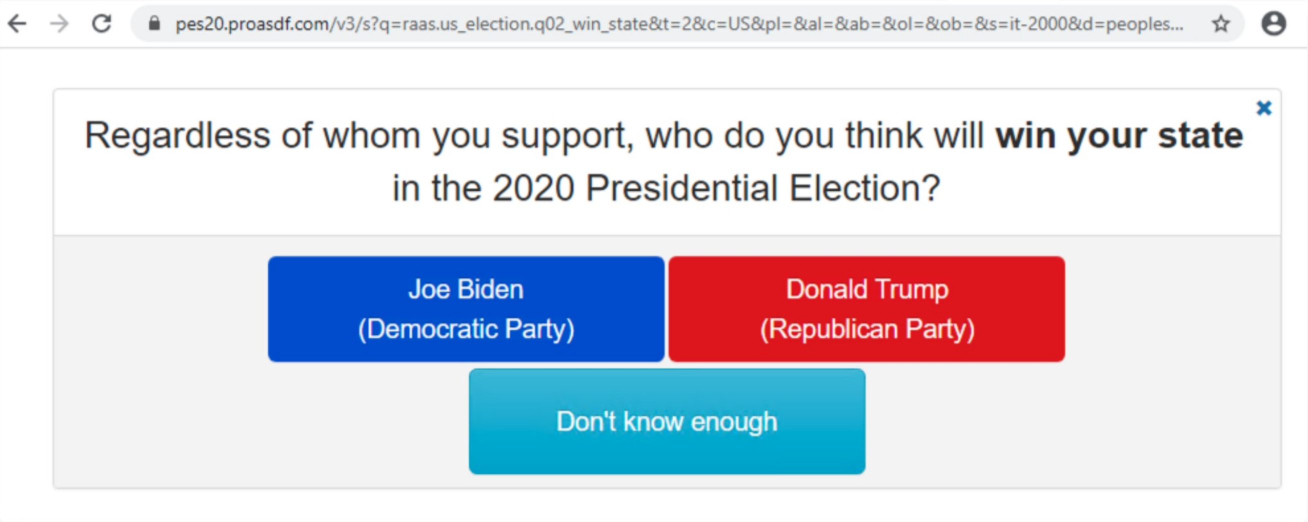
ABOUT

BIDEN CAMPAIGN DONATE

ESPY DONATE

HOW TO REQUEST ABSENTEE BALLOT

Figure 6. The ad listing page often seen while visiting peoplesvote[.]uk.



pes20.proasdf.com/v3/s?q=raas.us_election.q02_win_state&t=2&c=US&pl=&al=&ab=&ol=&ob=&s=it-2000&d=peoples...

Regardless of whom you support, who do you think will **win your state** in the 2020 Presidential Election?

Joe Biden (Democratic Party)

Donald Trump (Republican Party)

Don't know enough

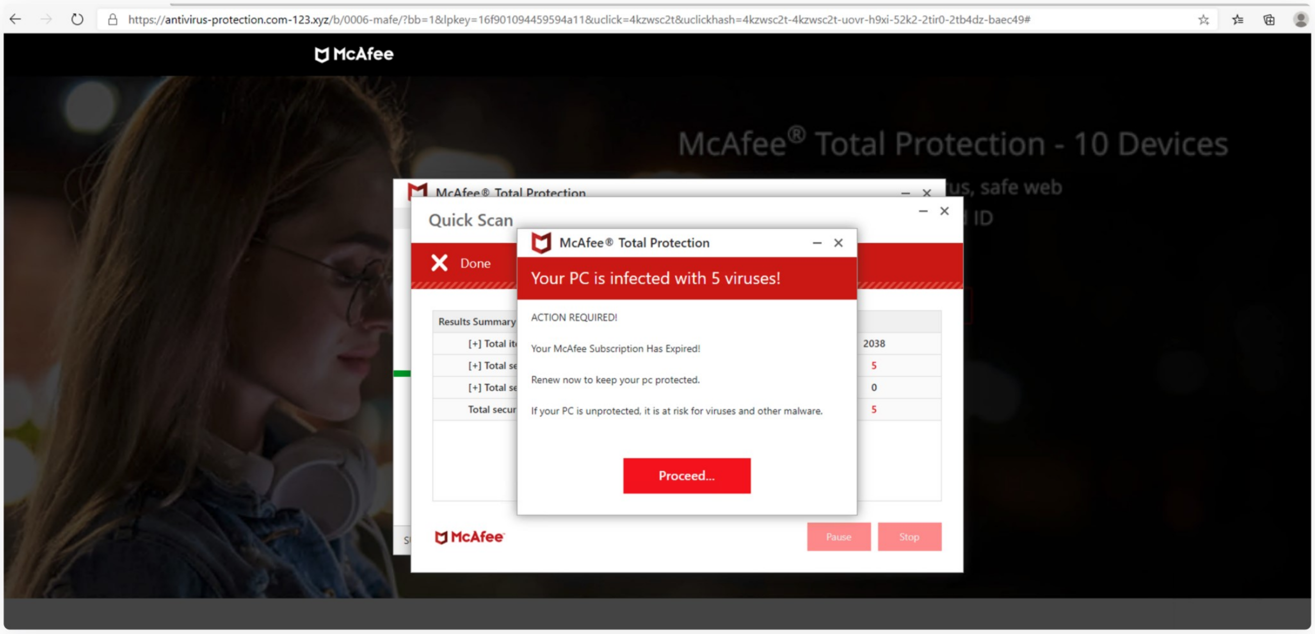
Figure 7. The voting preference landing page that is sometimes seen after visiting peoplesvote[.]uk and being redirected to a survey website.

Furthermore, we observed attackers abusing the largest dedicated parking service provider, Sedo. We found a parked domain, `xifinity[.]com`, that is a typosquatting domain mimicking `xfinity[.]com` (refer to our cybersquatting blog or this academic paper for more information). When a user attempts to visit the Xfinity website but accidentally types an additional "i," they will go to `xifinity[.]com` and will be redirected to an advertiser page. We identified that the traffic to this domain is sold to multiple advertisers. One of the advertisers, `softonic[.]com`, presents users with a software download page.

Besides legitimate advertisers, we also captured multiple redirections to PUPs from attackers. Figure 8 shows one of the abusive landing pages, the level-squatting domain `antivirus-`

protection[.]com-123[.]xyz. The landing page tries to trick users into believing that their machine is infected and that their McAfee subscription has expired. Clicking on the "Proceed" button will redirect users to a legitimate McAfee download page offering an antivirus subscription. We believe that attackers are abusing McAfee's affiliate program to steal ad revenue.

As a squatting domain, xifinity[.]com receives a high visit volume compared to other parked domains. We observed over 1,000 DNS requests for xifinity[.]com in our passive DNS dataset from June to September 2020, and the domain is still active as of this writing – as is antivirus-protection[.]com-123[.]xyz. From a domain owner's perspective, using a parking service is a convenient way to monetize user traffic. However, as abusive advertisers (i.e. attackers) are not filtered, users are exposed to various threats.



https://antivirus-protection.com-123.xyz/b/0006-mafe/?bb=1&lpkey=16f901094459594a11&uclick=4kzwsc2t&uclickhash=4kzwsc2t-4kzwsc2t-uovr-h9xi-52k2-2tir0-2tb4dz-baec49#

Your PC is infected with 5 viruses!

ACTION REQUIRED!

Your McAfee Subscription Has Expired!

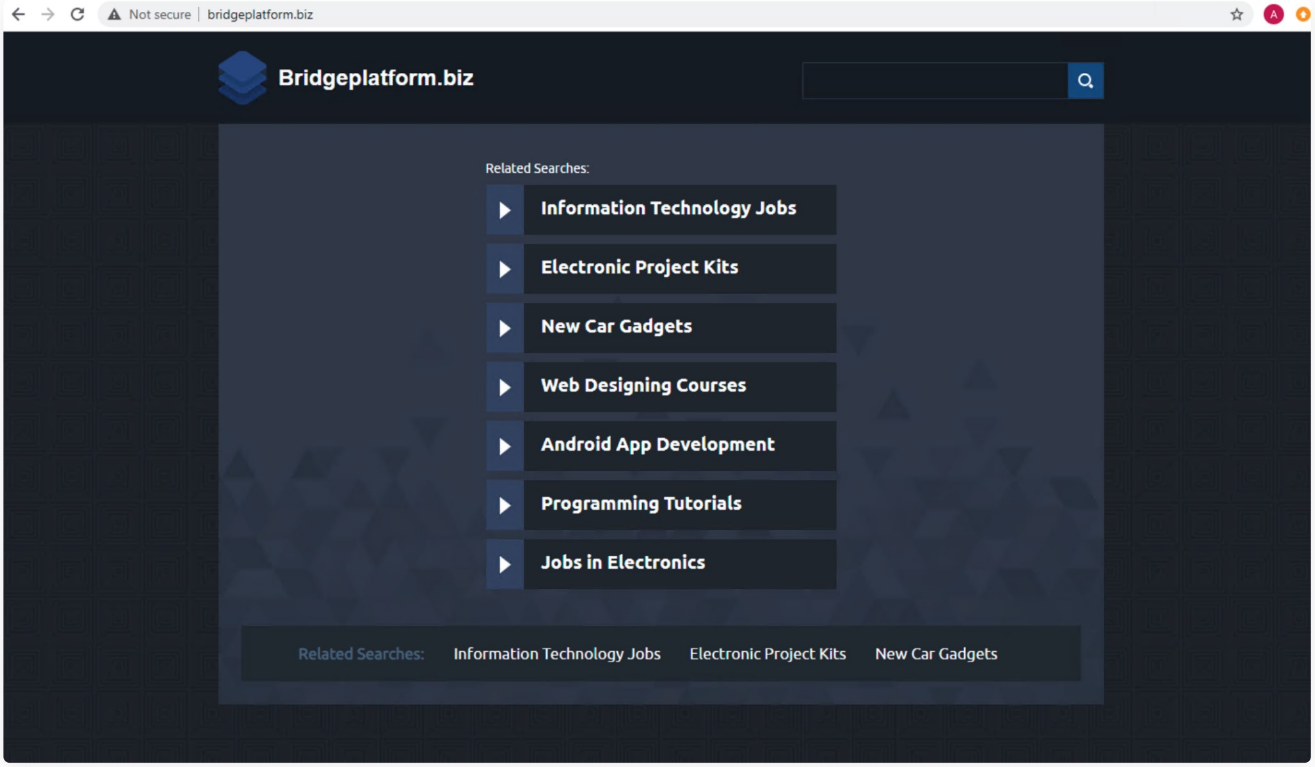
Renew now to keep your pc protected.

If your PC is unprotected, it is at risk for viruses and other malware.

Figure 8. The landing page impersonating McAfee while visiting xifinity[.]com.

Parking Service Abuse

We observed several parked pages using ztomy[.]com, the 14th-most popular parking service provider (shown in Figure 4), harvesting visitors' personal information. We observed that these pages generate fingerprints of users' browsers and send them back to the parked domain. The parked pages are using the browser fingerprinting script from pxlgnpgecom-a.akamaihd[.]net/javascripts/browserfp.min.js, which collects various private information and tracks user behavior. These browser fingerprints could be leveraged to track visitors' online activities, allowing advertisement networks to target visitors with ads tailored to them. Additionally, domain owners complained online that their domains' NS records were configured to ztomy NS servers without their awareness, which could be considered a form of domain hijacking.



Not secure | bridgeplatform.biz

Bridgeplatform.biz

Related Searches:

- Information Technology Jobs
- Electronic Project Kits
- New Car Gadgets
- Web Designing Courses
- Android App Development
- Programming Tutorials
- Jobs in Electronics

Related Searches: Information Technology Jobs Electronic Project Kits New Car Gadgets

Figure 9. An example of a parked domain, bridgeplatform[.]biz, using ztomy[.]com as the parking service provider.

Conclusion

In summary, parked domains can expose users to threats as they can redirect visitors to malicious or unwanted landing pages or turn entirely malicious in the future. Due to their questionable utility and the fact that our system can quickly re-classify parked domains when they merit new categories, we suggest that Palo Alto Networks Next-Generation Firewall customers *block* the parked category with URL Filtering or DNS Security. While this may be deemed a bit overly cautious by some due to potential false positives, we suggest alerts be set up for additional visibility at the bare minimum.

Palo Alto Networks Next-Generation Firewall customers are protected against malicious indicators (domain, IP, URL, SHA256) mentioned in this blog via URL Filtering, DNS Security and Threat Prevention subscription services.

Acknowledgements

We would like to thank Wei Wang and Ryan Nangong for their help with providing some of the data sources necessary for our analysis. We would also like to extend our gratitude to Jimmy Chen and Jun Javier Wang for their advice and help with improving the blog.

IOCs

Emotet campaign:

```
valleymedicalandsurgicalclinic[.]com
```

```
valleymedicalandsurgicalclinic[.]com/ujftb/statement/wr7hoba7i9hz
```

```
a9fe73484674696be756808e93f839be7157cd65995d8de9e67e40bf77c9b229
54ac560845b09ce00a48b604ac7c440331cbde4362839a3dbf14c378230bee21
```

```
50.91.114[.]38
```

```
51.38.124[.]206
```

Fingerprinting:

```
0redira[.]com/jr.php
```

```
bridgeplatform[.]biz
```

```
peoplesvote[.]uk
```

Cybersquatting:

```
xifinity[.]com
```

```
antivirus-protection[.]com-123[.]xyz
```