Automatically Detecting DNS Hijacking in Passive DNS

Executive Summary

In this article, we explain our process of detecting domain name service (DNS) hijacking and provide some notable examples of this detection from the first half of 2024. DNS hijacking allows cybercriminals to modify DNS records of domain names and redirect users to malicious servers.

Threat actors compromise domains for a variety of different types of attacks, including meddler in the middle (MitM) attacks, drive-by downloads, phishing and scams. Hijackers use a victim domain's reputation to direct victims into malicious campaigns, independent of the expectations of its original visitors. For example, to hijack domains criminals can steal domain owners' credentials at registrars or DNS service providers or alternatively infiltrate these services.

To detect DNS hijacking, we process an average of 167 million new DNS records every day. After initial preprocessing, we take the remaining records that are candidates for detection as DNS hijacking, and we extract 74 features from over 169 terabytes of passive DNS (pDNS) and geolocation data. We then use a machine learning model to predict whether or not these candidate records are truly the result of DNS hijacking.

Between March and September 2024, our detection pipeline processed over 29 billion new records and identified 6,729 as hijacking, with an average daily detection of 38 records. Recently, we deployed a new version of our model that can detect DNS hijacking in our customers' traffic in around 10 minutes.

This article provides some notable examples of DNS hijacking that our pipeline has detected over this period. Examples include:

- The DNS hijacking of a Hungarian political party's domain name
- The defacement of a large utility company and internet service provider (ISP)
- Using the domains of a university and research center to host illicit gambling

Palo Alto Networks Next-Generation Firewall customers receive protection from DNS hijacking via our automated classifier in the Palo Alto Networks Advanced DNS Security subscription service.

Palo Alto Networks Cortex Xpanse and Cortex XSIAM can help customers detect and respond to potential subdomain hijacking risks by identifying susceptible CNAME DNS records on customer-attributed domains.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics	**Cybercrime**, **DNS Hijacking**

Background

DNS hijacking is a pervasive threat that can have catastrophic consequences for domain owners and their customers. An incident on Oct. 22, 2016, is a stark example of this. Cybercriminals seized control of the entire online operation of a major Brazilian bank with over 5 million customers and 500 branches worldwide, as reported by Kaspersky Lab.

The attackers gained control of online banking, mobile, point-of-sale, ATM and investment transactions. During the 5-hour attack, the criminals collected electronic transactions, redirected users to phishing sites to steal their login credentials, and attacked users with malware.

When the malware successfully infected customer's machines, it first disabled antimalware software to avoid detection. It then harvested various credentials and targeted other banks the customer might have used.

The attackers gained control of the bank's online assets by compromising the bank's DNS service provider. While the criminal group's method of compromising the DNS service provider is unclear, the attackers were able to control 36 domains belonging to the bank.

The attackers also abused Let's Encrypt as a free and legitimate certificate authority, establishing certificates to make communication with these domains and subsequent malicious servers look legitimate. In summary, DNS hijacking landed a major bank's entire operation in criminal hands.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product itself is flawed or malicious.

DNS Hijacking in Practice

Threat actors can hijack DNS records using different methods. An attacker can take over the domain owner's account at a domain registrar or a DNS service provider or infiltrate the registrar/DNS service provider.

For example, attackers can use phishing, password guessing or breach another site to take over accounts. In such scenarios, mitigation techniques such as Domain Name System Security Extensions (DNSSEC) or encrypting DNS queries and responses (e.g., DNS over HTTPS and DNS over TLS) are insufficient to prevent attackers from hijacking the records.

Alternatively, attackers can hijack DNS records via DNS cache poisoning or other attacks manipulating DNS responses, such as MitM attacks intercepting communication and modifying the DNS queries on the fly. Cybercriminals hijack DNS records and change the resolution of domains to redirect requests for a domain to a destination they control. DNS hijacking is typically a precursor to other attacks, such as scams or drive-by-downloads.

Automatic Detection of DNS Hijacking

Automatically detecting DNS hijacking is an extreme needle in a haystack challenge. While there are hundreds of billions of DNS records, only a few dozen of them are known cases of DNS hijacking. Figure 1 provides a high-level overview of our machine learning-based detection pipeline consisting of four main steps: preprocessing, feature extraction, machine learning prediction and post-processing.

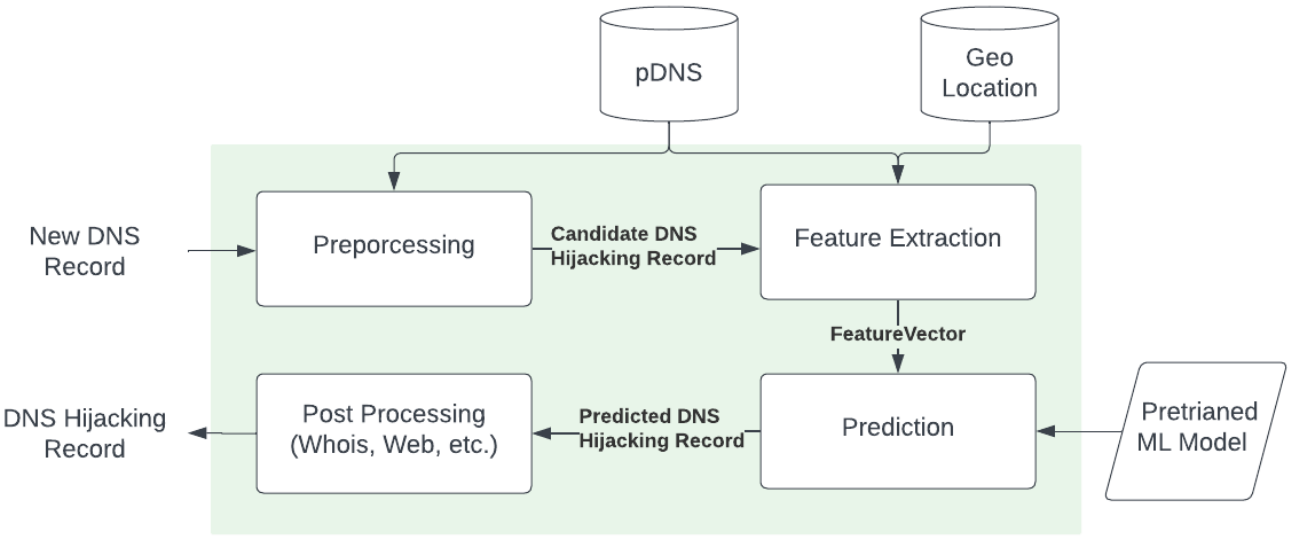

Figure 1. Overview of DNS hijacking detection pipeline.

The pipeline relies mainly on two datasets: pDNS and geolocation data. PDNS is a collection of hundreds of terabytes of historical DNS queries and responses from our customers as well as various global vantage points. Geolocation data maps IP addresses to their geographical location (e.g., country), ISP and Autonomous System Number (ASN).

The first step in our automatic detection of DNS hijacking is preprocessing, which takes new, never-before-seen DNS records as input. DNS hijackers need to create new DNS records to redirect users to their malicious servers, making new records a good starting point.

Preprocessing removes invalid records and records of new domain names. Never-before-seen hostnames are removed as we lack sufficient historical information about them to reliably decide if DNS hijacking were to occur.

We have a separate detector for domain shadowing, which is a special case of DNS hijacking where attackers stealthily create new malicious subdomains under compromised domain names. We also remove records that we observe in the history of the registered/root domain portion (e.g., google.co.uk in the case of www.google.co.uk) of the domain name. We consider the output of this preprocessing as our list of candidate DNS hijacking records.

In the second step, our pipeline extracts 74 features about these candidate DNS records using pDNS and geolocation data. Some features compare the historical usage of the new IP address to the old IP address of the domain name in the new record. For example, we compare the number of domains for which an IP address is a new IP address.

Other features compare the geolocation of the IP address in the new record to the historical IP addresses of the domain name. For example, we compare whether the IP address in the new record has a geolocation never seen before for the domain name.

The detector also considers features that describe the pDNS history of the root domain (e.g., how many IP addresses it has resolved to and in how many countries). Once the detector computes a feature vector for a candidate DNS hijacking record, our pipeline sends it to a pre-trained machine learning model.

Third, our machine learning model provides a probability score indicating the likelihood that the candidate DNS hijacking record is really DNS hijacking. We trained a random forest classifier using DNS hijacking records collected from various reports, and records from our pDNS dataset as our benign dataset.

Our benign dataset might contain a small number of DNS hijacking records, but our training algorithm can tolerate this amount of imperfection in our labeled data. The classifier's outputs are the predicted DNS hijacking records.

In the fourth and final step, we further process the predicted DNS hijacking records to decide if they are truly hijacking. While pDNS allows us to observe and process hundreds of millions of new records, it only provides a limited view about these new records.

To address this issue, we collect additional information about the predicted DNS hijacking records that would have been too expensive at an earlier step. First, we look at WHOIS data of the domain name in the records. WHOIS provides domain registration data and can tell us if a domain was recently reregistered, eliminating potential false positives.

We also conduct active crawls for the domain name's website using the IP address found in the new record as well as using IP addresses the domain previously resolved to, according to pDNS. If the

different web crawls provide identical content or HTTPS certificates, then we don't consider the predicted DNS hijacking record a true DNS hijacking record. We use the final output of our pipeline to block DNS hijacking records for our customers.

Detection Results

Between March 27, 2024, and September 21, 2024, our pipeline has processed over 29 billion new records. It has also selected more than 583 million candidate DNS hijacking records to process further in our machine learning pipeline. After prediction and post-filtering, our pipeline identified 6,729 records as DNS hijacking.

Figure 2 shows that our machine learning pipeline classifies around 3.3 million candidate DNS hijacking records daily (blue line). After post-filtering, we are left with an average of 38 DNS hijacking records a day (red line).

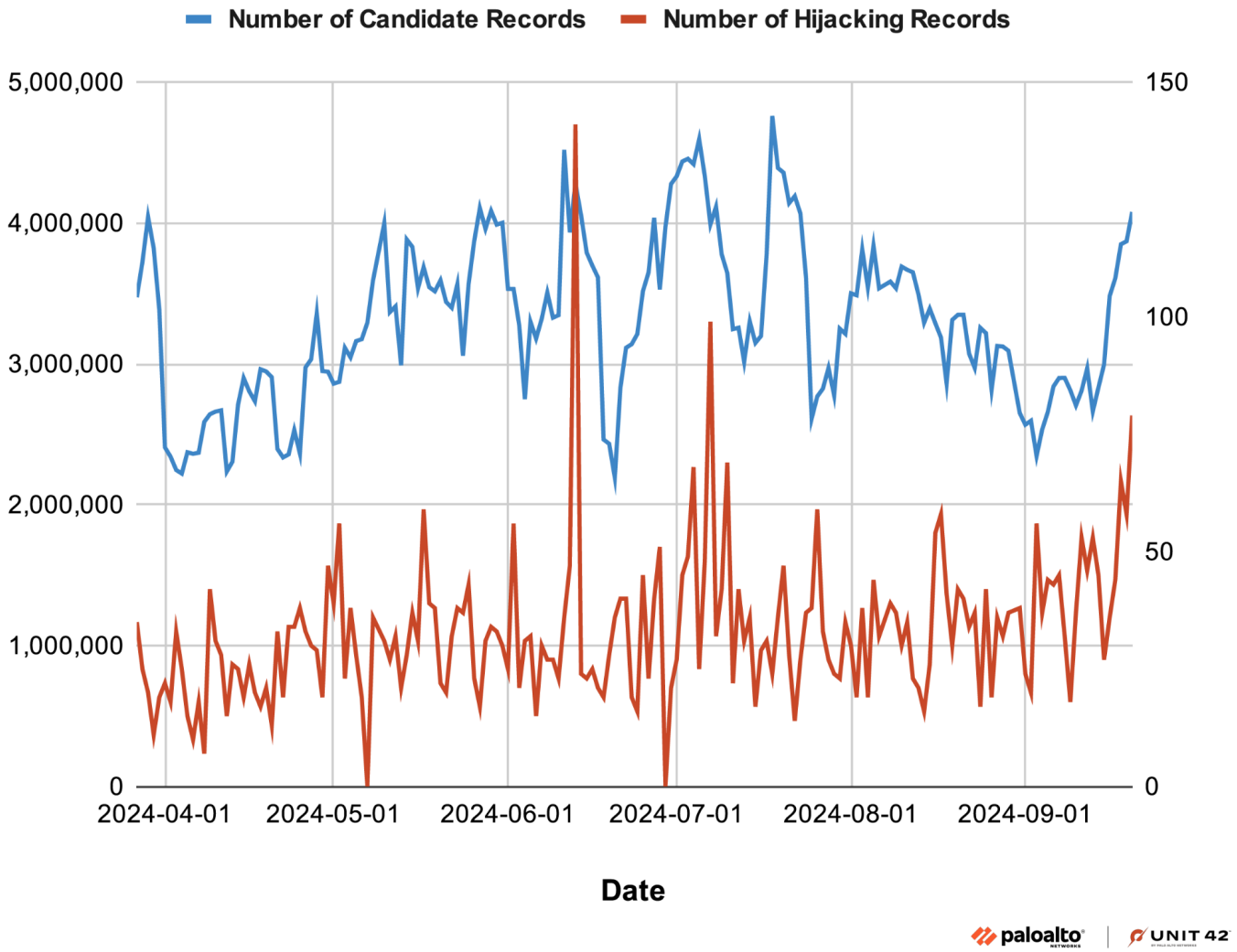

Figure 2. Daily counts of candidates and predicted DNS hijacking records.

DNS Hijacking in the Wild

DNS Hijacking of Two Companies by Same Group

On May 8, we detected two domains of one of the largest utility management companies in the U.S. pointing to a new IP address at `176.9.24[.]28`. The FTP service of the website was particularly suspicious, because it had been previously hosted on a different IP address since 2014, as shown in Figure 3.

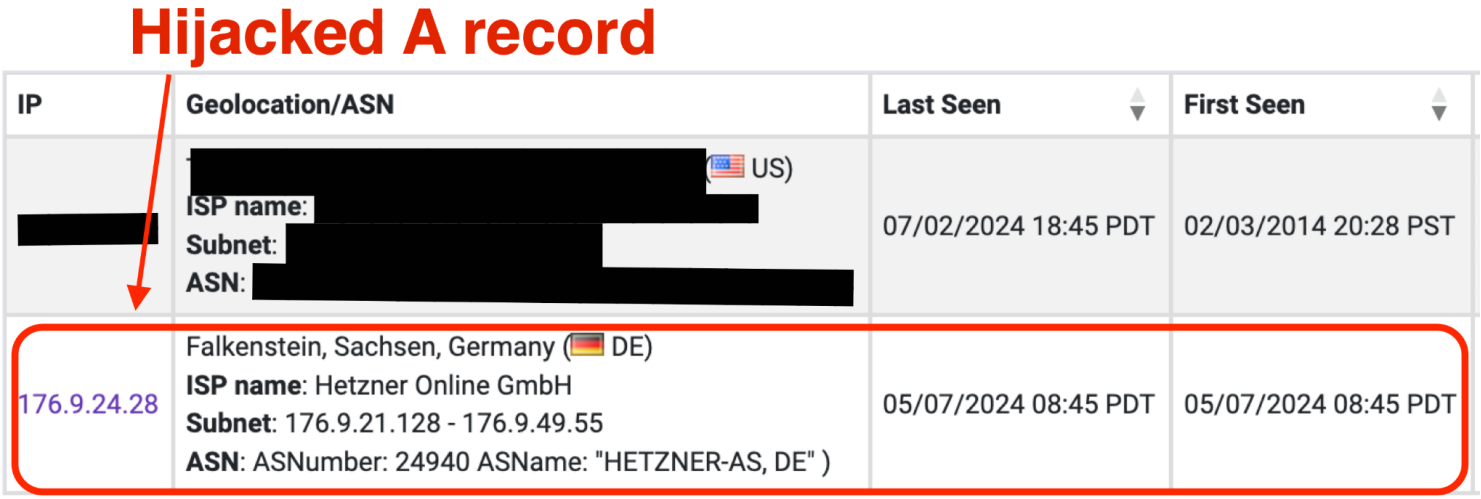

Figure 3. The detected hijacked record for the FTP service. This record was also detected as hijacking for the main domain.

Apart from the new IP address, there were no other IP addresses associated with this service in the pDNS records. When we examined the screenshot of the FTP service captured by our crawler that's shown in Figure 4, we noticed that the hijacked IP address hosted a defaced page by a group called Garuda Security.

Figure 4. The screenshot of the defaced FTP service captured by our crawler.

We further investigated other DNS records associated with the main website and found that hours before the IP address changed, its nameservers (i.e., NS records) were hijacked to `ns1[.]csit-host[.]com` and `ns2[.]csit-host[.]com`. Both of the nameservers resolved to the same hijacked IP address `176.9.24[.]28`.

On May 25, we detected a similar DNS hijacking incident on one of the largest ISPs. Its A record was hijacked to `176.9.24[.]28`, the same IP address used in the DNS hijacking attack against the utility management company, shown in Figure 5.

Hijacked A record

IP	Geolocation/ASN	Last Seen	First Seen
176.9.24.28	Falkenstein, Sachsen, Germany (DE) **ISP name**: Hetzner Online GmbH **Subnet**: 176.9.21.128 - 176.9.49.55 **ASN**: ASNumber: 24940 ASName: "HETZNER-AS, DE")	05/26/2024 12:13 PDT	05/24/2024 11:35 PDT

Figure 5. The detected hijacked record for the ISP website.

The pDNS data also shows that minutes before observing the hijacked record, the nameservers were hijacked to `ns1[.]csit-host[.]com` and `ns2[.]csit-host[.]com` as shown in Figure 6. Based on the attack similarity, we speculate that the same group conducted both attacks.

Name Server	Last Seen	First Seen
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
ns1.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT
ns2.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT

Name server hijacked

Figure 6. The change in NS record in the pDNS data.

We looked into recent hacking incidents for this IP address using `Zone-H[.]org`. Figure 7 shows two instances of web page defacement involving the same IP address in 2017 and 2023.

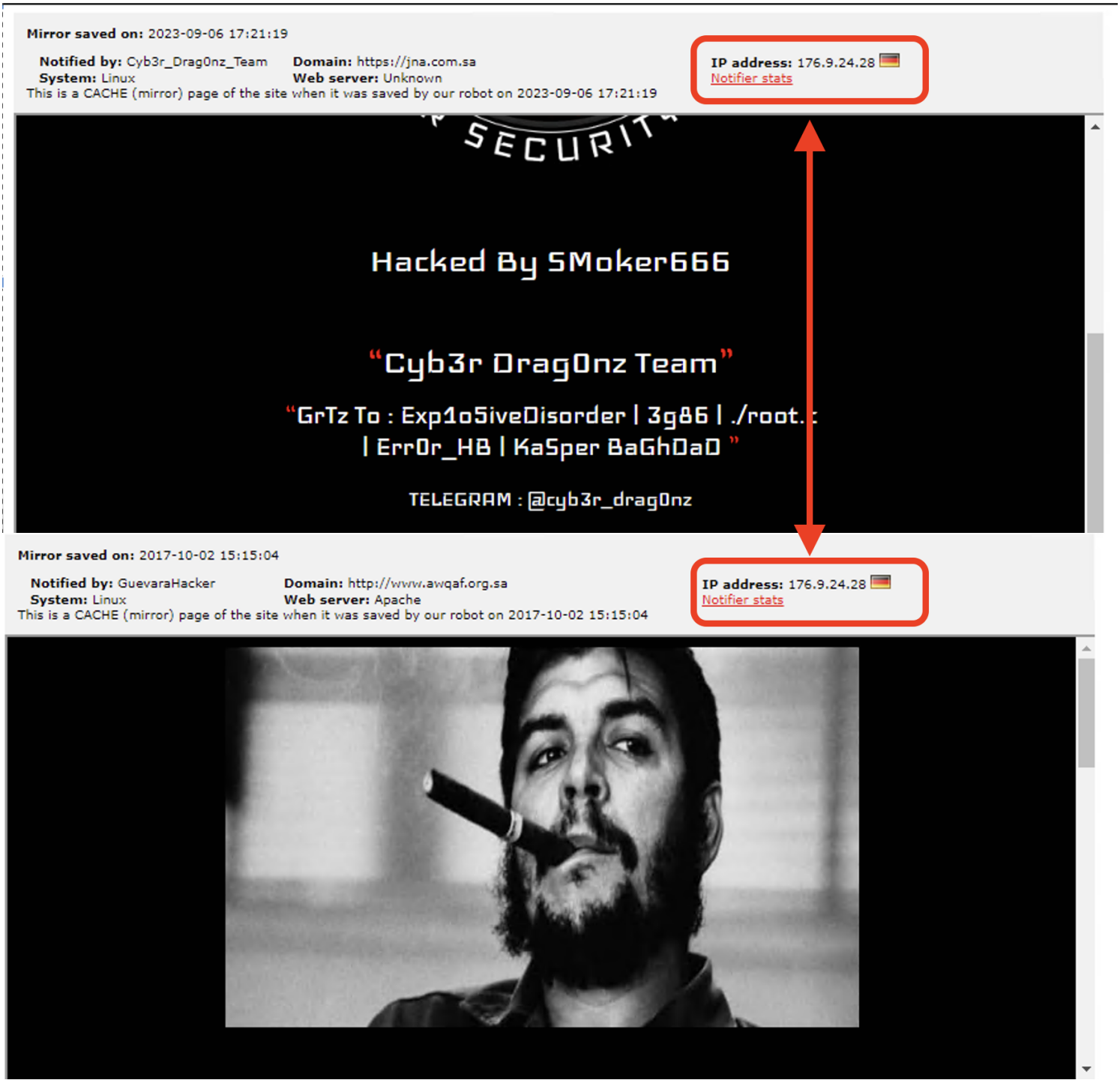

Figure 7. The screenshots taken from `Zone-H[.]org` show that the hijacked IP address was also involved in past incidents.

A Domain Name of a Hungarian Political Party Hijacked

The Democratic Coalition (DK), until recently the largest political opposition to the Hungarian government, owns the domain `dkujpest[.]hu`. This domain has been using IP addresses from the `37.9.175[.]0/24` subnet since 2017.

A web hosting company in Bratislava, Slovakia called WebSupport S.R.O. manages this IP subnet. The nameservers for the domain for several years were:

- `Ns1.gyumolcstarhely[.]hu`
- `Ns2.gyumolcstarhely[.]hu`
- `Ns3.gyumolcstarhely[.]hu`
- `Ns1.webonic[.]hu, ns2.webonic[.]hu`
- `Ns3.webonic[.]hu`

These nameserver domains also seem to be operated by WebSupport S.R.O. After the attack, the domain operators switched the nameservers to:

- `Ns1.websupport[.]hu`
- `Ns1.websupport[.]hu`
- `Ns1.websupport[.]hu`

We hypothesize that WebSupport S.R.O. changed the nameservers after the attack to increase security or control. Upon reporting this to representatives for WebSupport, they replied that only administrators of the domain can change DNS records, indicating that WebSupport is not the domain administrator.

On Jan. 28, 2024, our model detected that `dkujpest[.]hu` suddenly resolved to a new German IP address `152.70.176[.]210`. We also found that the domain briefly resolved to `135.148.57[.]147`, another German IP address.

These IP addresses are in a different ISP and ASN that we have never seen before for `dkujpest[.]hu`. Our web crawler found that the original web content shown in Figure 8 was changed to a phishing login page spoofing Microsoft shown in Figure 9. We confirmed with the maintainer of `dkujpest[.]hu` and its hosting provider WebSupport S.R.O. that these hijacking IP addresses and the spoofed Microsoft login page are not part of their infrastructure.

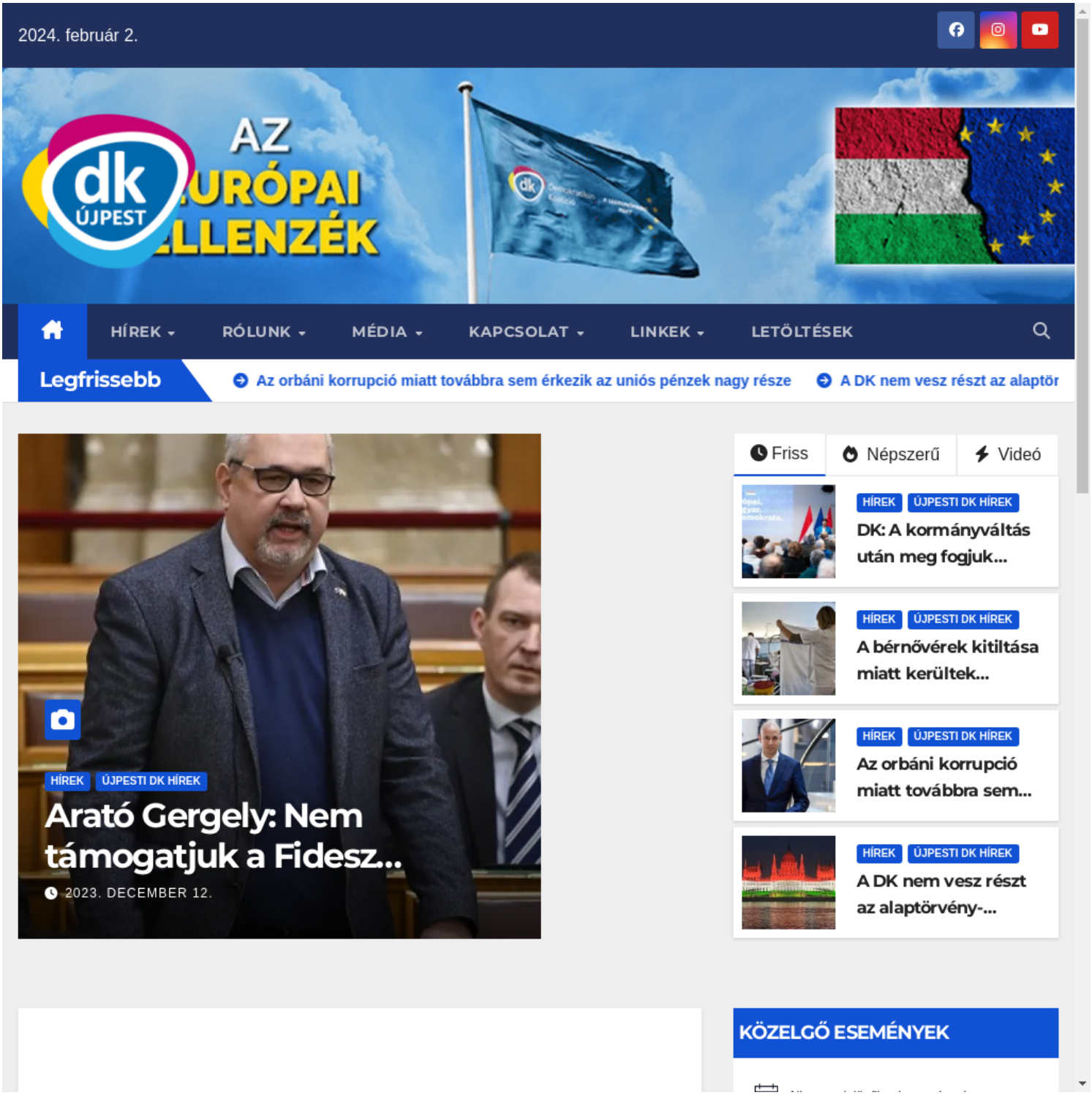

Figure 8. The webpage of domain `dkujpest[.]hu` before DNS hijacking.

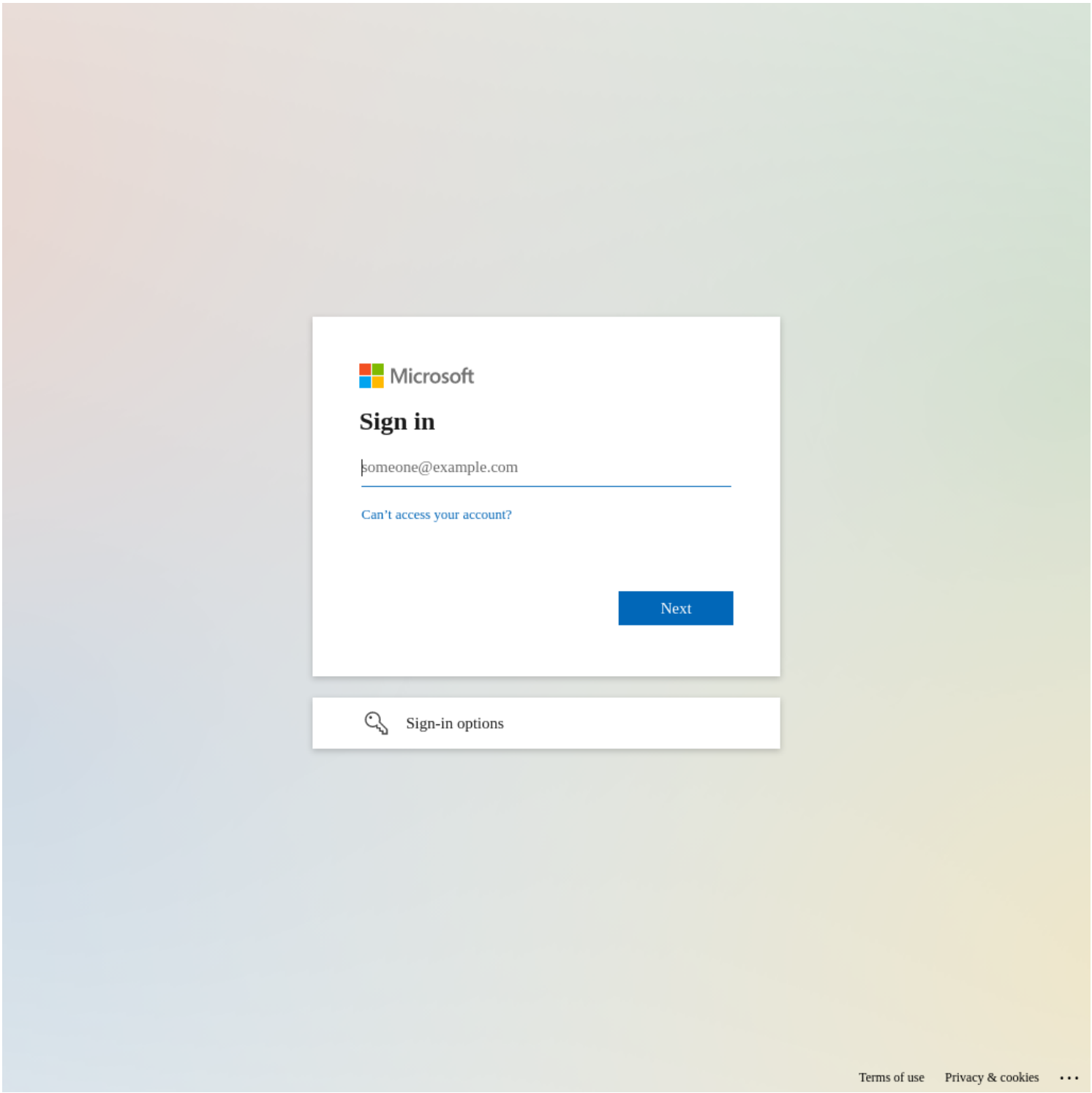

Figure 9. The webpage of domain `dkujpest[.]hu` after DNS hijacking.

Two of the biggest Hungarian news portals, HVG and Telex, covered the hacking of `dkujpest[.]hu` two days after our model detected it.

Ongoing Illicit Gambling Campaign: A Research Center’s and a University’s Domains Hijacked

On the second of April 2024, we detected a new IP address `139.59.255[.]10` from Singapore for a research center’s domain `c-sharp[.]in`. This new IP address was suspicious because `c-sharp[.]in` had been using a U.S.-based IP address `208.91.198[.]24` since 2014.

Our web crawler found that DNS hijackers changed the original website hosted on `208.91.198[.]24` shown in Figure 10 to an illicit gambling website hosted on `139.59.255[.]10`, shown in Figure 11.

Figure 10. The webpage of `domain c-sharp[.]in` hosted on `208.91.198[.]24` before DNS hijacking.

Figure 11. The webpage of `domain c-sharp[.]in` hosted on `139.59.255[.]10` after DNS hijacking.

Additionally, we detected `ccdc[.]org[.]do`, which also resolved to `139.59.255[.]10` on June 28, indicating that this group of cybercriminals continuously look for potential domains to hijack.

In a similar case, we found that `uts[.]ac[.]id` (a university's domain) started resolving to a Singaporean IP address `159.223.92[.]200` on Jan. 13, 2024. However, the domain has exclusively used an Indonesian IP address `103.84.194[.]81` since 2017.

We also observed that the hijacker added many new subdomains, two new nameserver domains and one mail server DNS record:

- `Ns5.uts.ac[.]id`
- `Ns6.uts.ac[.]id`
- `Mail.uts.ac[.]id`

We found that these new subdomains and the original nameservers resolved to the hijacker's IP address (`159.223.92[.]20`) during the attack. Like in the previous case, our web crawler found that DNS hijackers changed the original website hosted on `103.84.194[.]81` (Figure 12) to an illicit gambling website hosted on `159.223.92[.]200` (Figure 13).

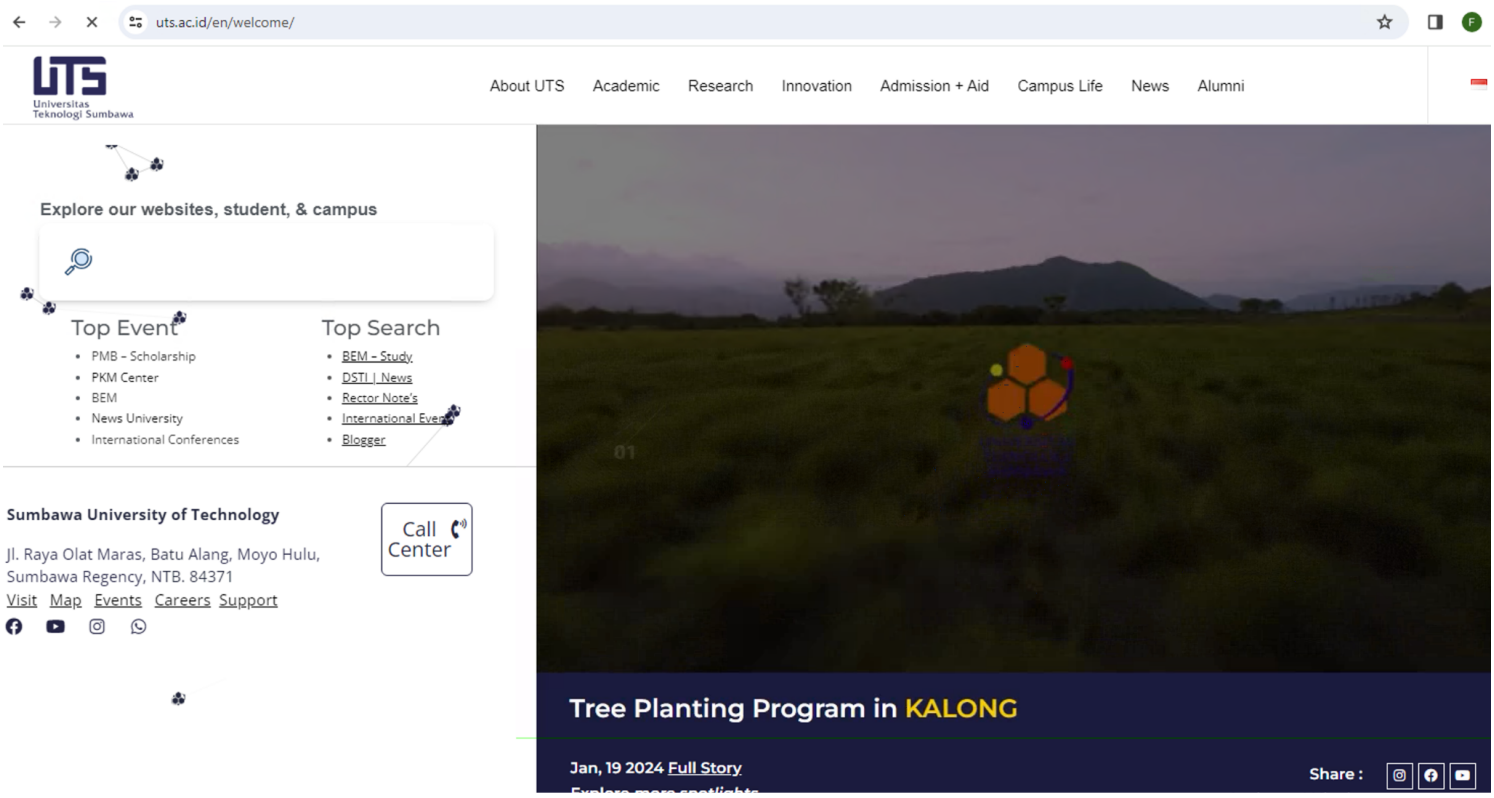

Figure 12. The webpage of domain `uts.ac[.]id` before DNS hijacking.

Figure 13. The webpage of domain `uts.ac[.]id` after DNS hijacking.

The two IP addresses share the same ISP and ASN. Furthermore, they use the hijacked domains to promote similar illicit gambling sites, indicating these two hijacking cases are likely part of the same campaign.

Conclusion

Our machine learning-based pipeline processes an average of 167 million new DNS records daily and leverages hundreds of terabytes of pDNS and geolocation data to detect DNS hijacking. Every day, our detector flags dozens of records as hijacking to protect our customers. Recently, we deployed a new version of our model that can detect DNS hijacking in our customers' traffic in around 10 minutes.

We observe that cybercriminals use compromised domains to host phishing content, to deface websites, or to spread illicit content. In this post, we selected examples of DNS hijacking that our automatic pipeline has found, including the following:

- One of the largest utility companies in the U.S.
- A large ISP
- A major political party in Hungary
- A university
- A research center

Palo Alto Networks Next-Generation Firewall customers receive protection from DNS hijacking via our automated classifier in the Palo Alto Networks Advanced DNS Security subscription service.

Palo Alto Networks Cortex Xpanse and Cortex XSIAM can help customers detect and respond to potential subdomain hijacking risks by identifying susceptible CNAME DNS records on customer-attributed domains.

Acknowledgments

We want to thank Reethika Ramesh, Bradley Duncan, Lysa Myers, and Arun Kumar for their invaluable input on this article.

Indicators of Compromise

DNS hijacking records

- c-sharp[.]in A 139.59.255[.]10
- ccdc.org[.]do A 139.59.255[.]10
- dkujpest[.]hu A 135.148.57[.]147
- dkujpest[.]hu A 152.70.176[.]210
- mail.uts.ac[.]id A 159.223.92[.]200
- ns1.uts.ac[.]id A 159.223.92[.]200
- ns2.uts.ac[.]id A 159.223.92[.]200
- ns3.uts.ac[.]id A 159.223.92[.]200
- ns4.uts.ac[.]id A 159.223.92[.]200
- ns5.uts.ac[.]id A 159.223.92[.]200
- ns6.uts.ac[.]id A 159.223.92[.]200
- uts.ac[.]id A 159.223.92[.]200
- uts.ac[.]id NS ns5.uts.ac[.]id
- uts.ac[.]id NS ns6.uts.ac[.]id
- uts.ac[.]id MAIL mail.uts.ac[.]id

IP addresses used by attackers

- 135.148.57[.]147
- 139.59.255[.]10
- 152.70.176[.]210
- 159.223.92[.]200
- 176.9.24[.]28

Nameservers used by attackers

- ns1[.]csit-host[.]com
- ns2[.]csit-host[.]com