

# Threat Actors use Google Ads to Deploy VIDAR Stealer

---

 [kroll.com/en/insights/publications/cyber/threat-actors-google-ads-deploy-vidar-stealer](https://kroll.com/en/insights/publications/cyber/threat-actors-google-ads-deploy-vidar-stealer)



Kroll has observed threat actors abusing Google Ads to deploy malware masquerading as legitimate downloads or software that has been “cracked” or modified to remove or disable features such as copy protection or adware. As part of our analysis of this trend and threat, we have identified specifically that VIDAR malware, an information-stealing trojan, is using Google Ads to advertise spoofed domains and redirect users to fraudulent sites or malware downloads. Kroll is currently tracking the use of this tactic by ransomware groups globally, particularly groups that are assessed with medium confidence to be associated with former Conti ransomware affiliates such as Royal, Black Basta, and Hive ransomware operators. While the infection vector is the same, Zloader is typically used to deploy further malicious tooling to gain a foothold within the network during the Intrusion Lifecycle.

As an example of Kroll's findings and analysis into this trend, we discovered a particular Google Ad that, while displaying the legitimate domain of the opensource image editing product GIMP, ultimately redirected the user to a typo-squatted domain, hosting a cloned website containing malicious downloads. This is particularly interesting as the format of the advert is controlled through Google's Ad framework. The display domain highlighted below is extracted by Google from the target URL provided by the advertiser.

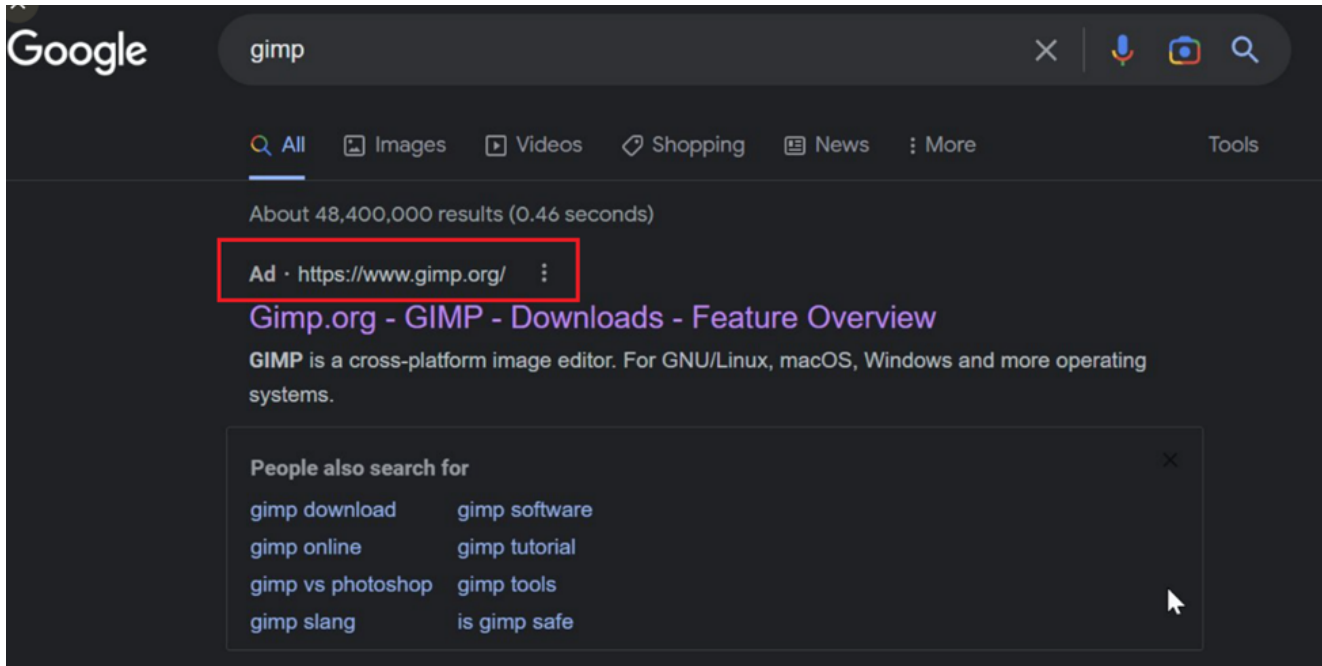


Figure 1: Screenshot of Malicious Ad (Source: Kroll)

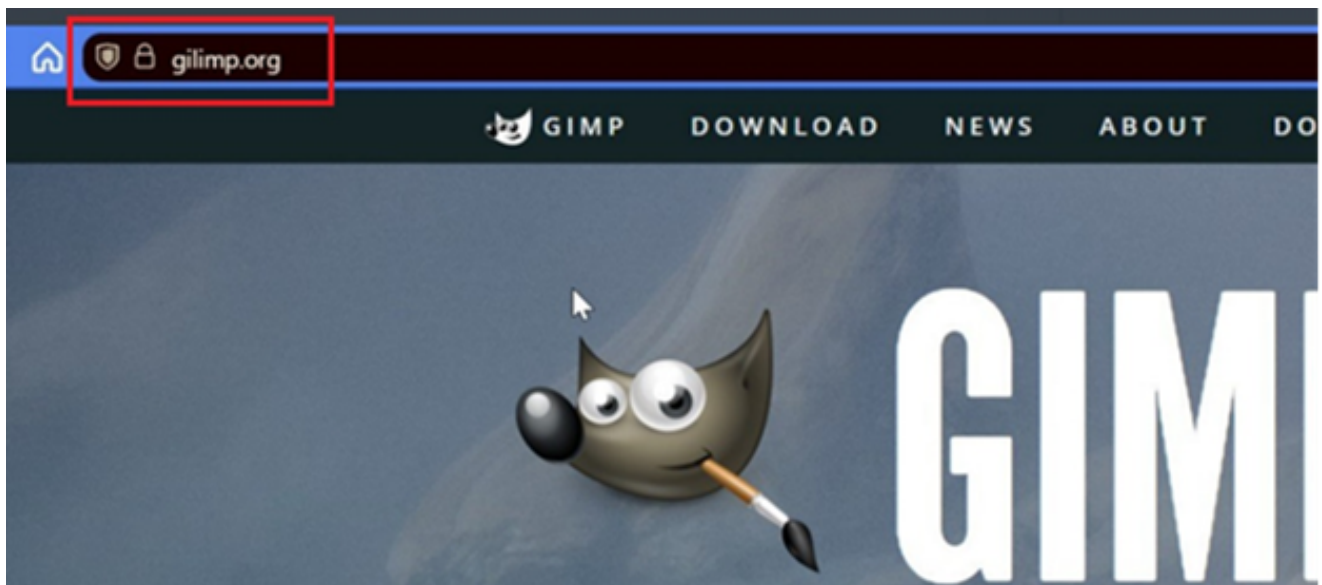


Figure 2: Screenshot of the Typo-Squatted Domain (Source: Kroll)

The malicious domain gilimp[.]org appears to have been registered on October 17, 2022, indicating that this advert could have been live for up to 16 days at the time of our analysis.

# Whois Record for GiLimp.org

## — Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	PrivacyGuardian.org llc
Registrant Country	us
Registrar	Namesilo, LLC IANA ID: 1479 URL: <a href="http://www.namesilo.com">http://www.namesilo.com</a> Whois Server: <a href="http://whois.namesilo.com">http://whois.namesilo.com</a> <a href="mailto:abuse@namesilo.com">abuse@namesilo.com</a> (p) 14805240066
Registrar Status	clientHold, clientTransferProhibited
Dates	16 days old Created on 2022-10-17 Expires on 2023-10-17 Updated on 2022-10-29
Name Servers	HOUSTON.NS.CLOUDFLARE.COM (has 26,286,142 domains) KATJA.NS.CLOUDFLARE.COM (has 26,286,142 domains)

Figure 3: Whois Record for Typo-Squatted Domain (Source: Kroll)



At the time of the investigation, it was no longer possible to access the advertisement (“advert”), and the screenshots available online no longer showed the destination URL of the advert when hovered over to see the first step in the request chain, making it more difficult for Kroll to definitively determine exactly how the threat actor achieved this.

Kroll analyzed a binary on the malicious domain that was presented to appear as the GIMP software. The analysis showed that it was in fact VIDAR malware. Our experts were able to determine that the malware was stealing browser cookies and passwords, along with detailed system information, before sending these to a C2 IP address.

The IP information for this IP address shows its geolocation as St. Petersburg in the Russian Federation.

## IP Information for 91.213.50.70

### — Quick Stats

IP Location	 Russian Federation Sankt-peterburg It Resheniya Llc
ASN	 AS49943 (registered Feb 02, 2022)
Whois Server	whois.ripe.net
IP Address	91.213.50.70

```
% Abuse contact for '91.213.50.0 - 91.213.50.255' is ' abuse@ren
```

```
inetnum:          91.213.50.0 - 91.213.50.255
descr:            3304776
netname:          RU-ITRESHENIYA
country:          RU
org:              ORG-ITR1-RIPE
admin-c:          ITR30-RIPE
tech-c:           ITR30-RIPE
status:           ASSIGNED PA
mnt-by:           IP-RIPE
created:          2020-09-07T16:45:21Z
last-modified:    2022-06-16T15:28:52Z
source:           RIPE
```

Figure 4: C2 IP Address Information (Source: Kroll)

## Most Likely Methodologies

The Kroll Cyber Threat Intelligence team tested a number of theories leveraging the Google Ad workflow for how “malvertising” could lead to the deployment of the VIDAR Stealer. Kroll proposed with high confidence the below two most likely scenarios based on completed research to date:

1. A homoglyph attack utilizing international domain name scheme
2. Via manipulation of the tracking template URL option

## Homoglyph Attack

This attack method is documented by others within the Security and Incident Response communities and seems to be a favorite hypothesis shared by many to include Kroll's researchers.

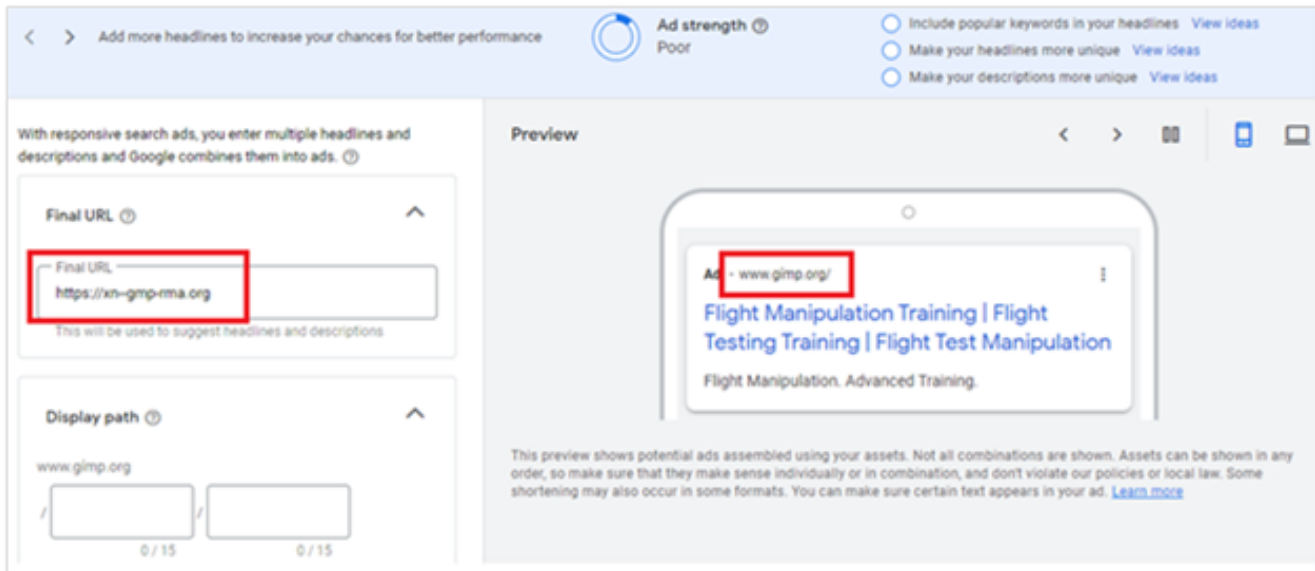


Figure 5: Screenshot Showing the Setting Up of Homoglyph Attack in Google Ads (Source: Kroll)

As detailed in Figure 5, Kroll's threat intelligence team would be able to set up an advert utilizing an international domain name that would pass most viewer's initial inspection of the domain. If a homoglyph attack was used, it is an exceptionally effective approach with no obviously out-of-place characters.

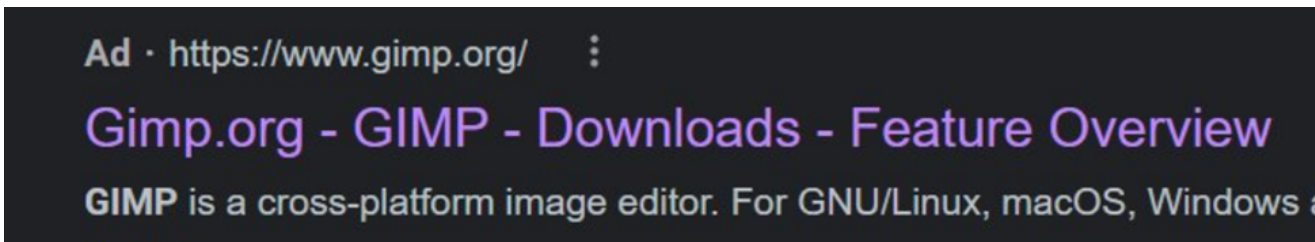


Figure 6: Zoomed In View of Ad (Source: Kroll)

Kroll observed that the ultimate page reached by clicking on the link was not an international domain, but a second, different typo-squatting domain. This inconsistency makes this method appear less probable since the threat actor would need to link to 2 domains via a redirect chain.

However, there is a possibility that the threat actor did this to protect their homoglyph domain or they were aware that some web browsers will show the ascii format domain name in the address bar (for example: xn--gmp2ub[.]org instead of gimp[.]org), making the website

appear more suspicious. Kroll's testing of this process also identified Google's automated domain checking processes which would normally frustrate a threat actor's usage of this methodology.

## Tracking Template URL

Google Ads allow for the use of a tracking link that would be the first link connected too, in order to store various parameters for your advertising campaign before forwarding on to the target page. With this tracking link set, the display domain remains the domain of the target URL.

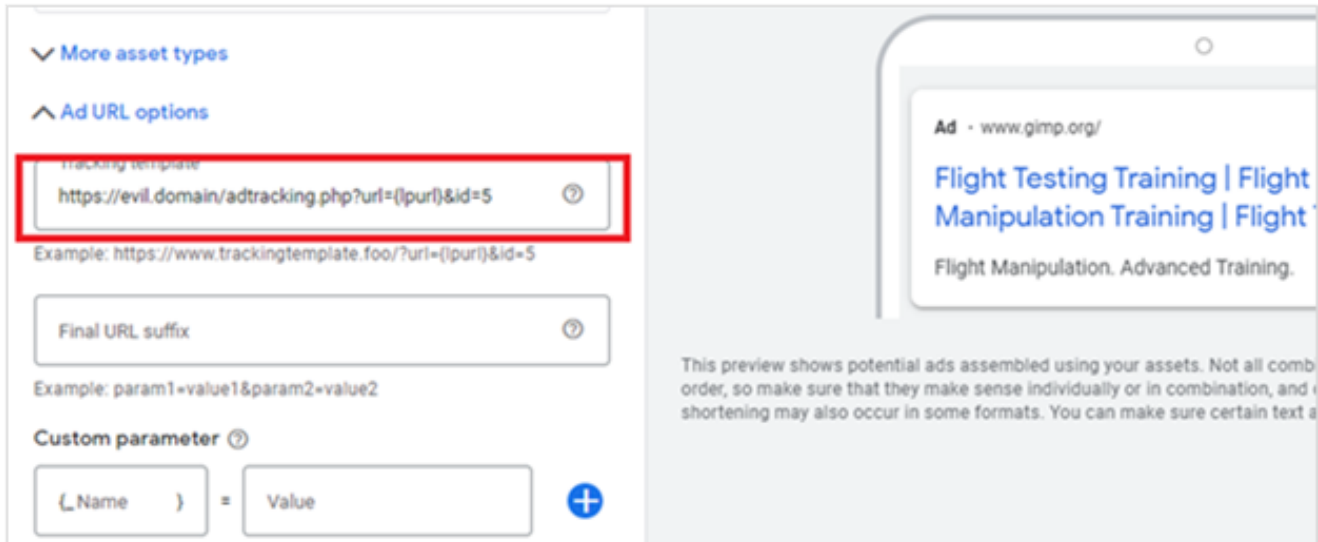


Figure 7: Screenshot Showing the Setting Up of a Cross domain Tracking Template in Google Ads (Source: Kroll)

It is possible that, by using a malicious tracking link, a threat actor could set up an advert for the legitimate gimp.org and redirect to their malicious page instead of the real page. This is currently the method Kroll assesses has been leveraged by Threat Actors in prior Intrusion Lifecycles.

Kroll tested this methodology using a malicious tracking template hosted on a separate domain and successfully redirected an advert click to a third domain - the video of which can be viewed here. The setup used the process described in the official Google documentation for cross-domain redirects.

Ad	Campaign	Ad group	Status	Ad strength	Final URL	Tracking template
<input type="checkbox"/> Best   Spring Loaded   Self Sealing +1 more <a href="http://www.spring-loaded-stem-boits.xyz">www.spring-loaded-stem-boits.xyz</a> Spring Loaded Self Sealing Stem Boits. A description of the page. <a href="#">View assets details</a>	StemBoits	Ad group 1	Eligible	Poor	<a href="https://www.spring-loaded-stem-boits.xyz">https://www.spring-loaded-stem-boits.xyz</a>	<a href="https://meta-nym.net/adv_tracking.php?url={ipuri}&amp;name=stemboits">https://meta-nym.net/adv_tracking.php?url={ipuri}&amp;name=stemboits</a>

Figure 8: Screenshot of Active Advert Setup using Cross domain Tracking Template (Source: Kroll)

By utilizing a custom PHP script on the tracking domain, we were then able to redirect traffic to a proof-of-concept domain instead of the legitimate website. There is some automated checking performed by Google to detect incorrect redirecting; however, this was circumvented with minimal effort. It is likely this automated checking is designed to detect mistakes rather than this specific methodology.

## Additional Methodologies

Our team also explored a series of less likely scenarios:

1. A configuration setting within the Google Ads system allowing the ability to specify a different target domain to display domain either legitimately allowed or via a bug
2. Use of an open redirect on the gimp.org site
3. A bug in URL validation processes allowing for manipulation of display

## Configuration Setting

To date, our team have been unable to produce a combination of settings in the Google Ads interface that would allow a different display domain from the target domain.

## Use of Open Redirect

The Google Ads system extracts the domain it displays in the advert from the Final URL field. If an open redirect were present on the gimp.org website and being used as the Final URL, “gimp.org” would be displayed. It is not possible to test whether Google Ads would detect this without an open redirect vulnerability being present to use in the test.



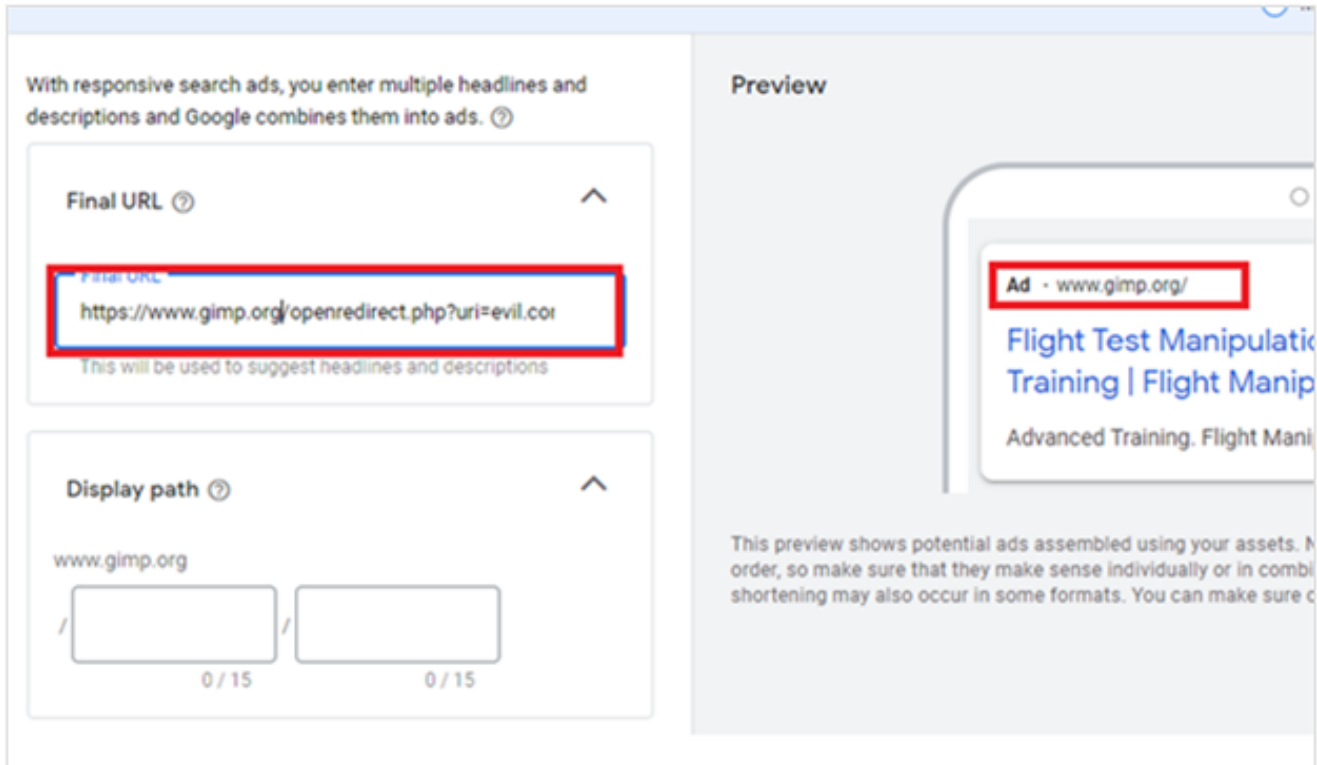


Figure 9: Screenshot Showing Hypothetical Setup of Attack Using an Open Redirect (Source: Kroll)

For this to work, there would have to be an open redirect vulnerability on the gimp.org website; additionally, the aforementioned redirection validation checks performed by google would need bypassing.

## Validation Bug

It is conceivable that a bug in the validation of inputs might have allowed the manipulation of the advert and target domain. Our team tried a numerous strategies to see what resulted as controlled tests. All tests were caught by server-side validation. However, they were successful in changing the display of the preview advert to not reflect the target domain.



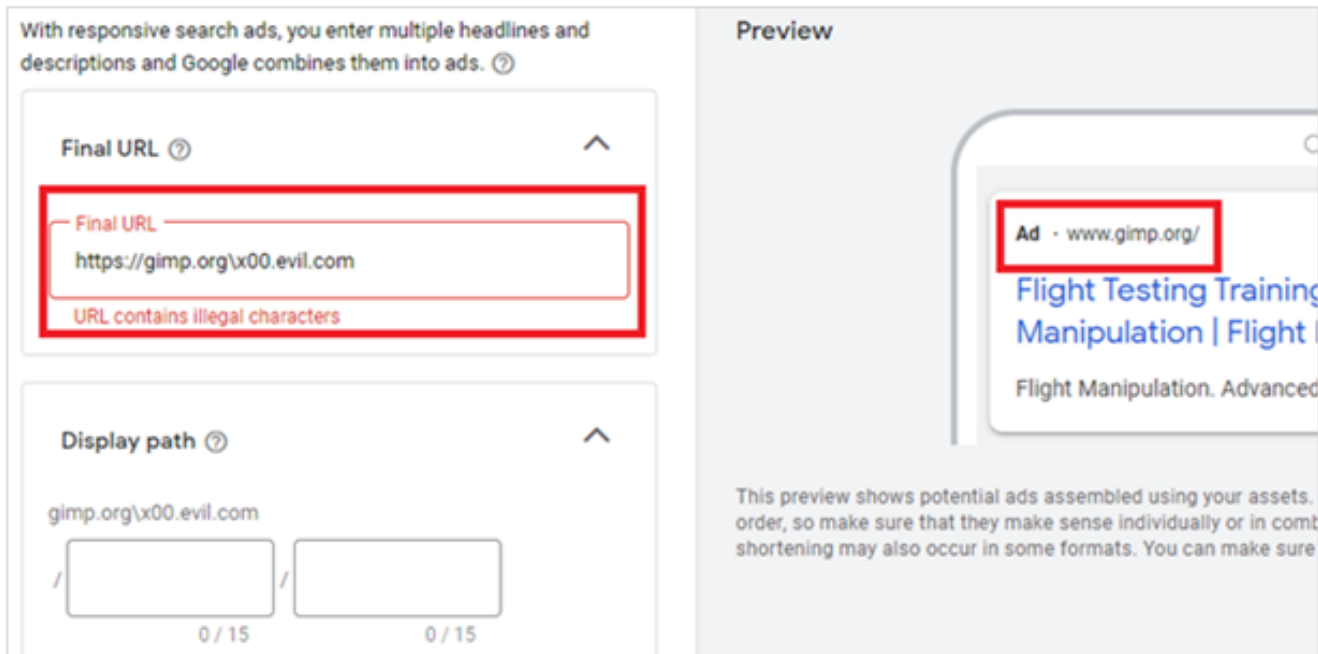


Figure 10: Screenshot Showing an Attempt to Manipulate the URL to Display Incorrectly (Source: Kroll)

## Google Review

---

As mentioned earlier, Google has a review process for adverts. Changes to the advert, including changing domain or tracking link will take the advert offline and require further review.

## Impact

---

Now that this attack has been documented on various websites, it is very likely that other actors will attempt this technique because it can effectively turn any website into a watering hole attack, conveniently placing their malicious website at the top of the Google Search results.

While it is particularly dangerous for sites that provide software for download, it could easily be expanded for other purposes. For example, a clone of a login page of a legitimate domain could be hosted for credential harvesting.

## Kroll Recommendations

---

- Inform and educate personnel of this current attack methodology, making them aware of the dangers of downloading executables from websites that have not been verified as legitimate, particularly in relation to executables found after clicking through any form of online advertising.
- Where possible, restrict staff from downloading executables, a feature of many web filtering capable proxy servers.

- Require all installs to be performed by information technology staff from vetted binary repositories.
- Employ [endpoint detection and response](#) (EDR) and next-generation anti-virus (NGAV) tools across all endpoints within the environment.

Learn more about [Kroll's end-to-end cyber security services](#) or call our [Cyber Incident Response Hotline](#) to request immediate assistance.

## Stay Ahead with Kroll

---

### Cyber Risk

---

Incident response, digital forensics, breach notification, managed detection services, penetration testing, cyber assessments and advisory.

### 24x7 Incident Response

---

Enlist experienced responders to handle the entire security incident lifecycle.

### Computer Forensics

---

Kroll's computer forensics experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or location of data sources.

### Cyber Risk Retainer

---

Kroll delivers more than a typical incident response retainer—secure a true cyber risk retainer with elite digital forensics and incident response capabilities and maximum flexibility for proactive and notification services.

### Ransomware Preparedness Assessment

---

Kroll's ransomware preparedness assessment helps your organization avoid ransomware attacks by examining 14 crucial security areas and attack vectors.

### Malware Analysis and Reverse Engineering

---

Kroll's Malware Analysis and Reverse Engineering team draws from decades of private and public-sector experience, across all industries, to deliver actionable findings through in-depth technical analysis of benign and malicious code.

### Cloud Security Services

---

Kroll's multi-layered approach to cloud security consulting services merges our industry-leading team of AWS and Azure-certified architects, cloud security experts and unrivaled incident expertise.

## **Assessments and Testing**

---

Kroll's field-proven cyber security assessment and testing solutions help identify, evaluate and prioritize risks to people, data, operations and technologies worldwide.

[Return to top](#)