## Abstract

To discuss and explore the theoretical viewpoint of Malvertising, its displacement to devices and defense tactics end users can implement.  This paper will walk through an exhibition of two devices communicating over a network with access to a centralized website containing a malicious advertisement.  A presentation of the laboratory experiment consisting of a virtual environment impersonating a remote user, website, and a command-and-control server (C2C) will be presented.  A technical overview will explore the characteristics of code used during Malvertising attacks.  I will elaborate on special code functions, and how it's utilized to achieve an attack.  Finally, user awareness principles are examined to educate end users of bad actors' mischievous techniques and simple adaptable defense tactics to minimize malignant behavior related to Malvertising.

**Malvertising**

One popular form of growing and marketing business since 1980 is online advertising.  After rapidly taking off in the 1990's, online advertising became popular with mobile phones and social platforms. Revenue from advertisements in 2024 is expected to grow by 13.2% and gross $302.77 billion forQ3 of 2024. (Yoram Wurmser, August 2024, "Ad Spending Benchmarks: Q3 2024, https://www.emarketer.com/content/ad-spending-benchmarks-q3-2024 ) (Cramer-Flood, "Worldwide Digital Ad Spending Forecast 2024", https://www.emarketer.com/content/worldwide-digital-ad-spending-forecast-2024, January 2024)

Current benchmarks from Q2 of 2024 reveal revenue from google ads gross $ 48.51 billion. (Konstantinovic and Goldman, "Earnings Report: How Is Digital Advertising Spending Performing Halfway Through 2024?" https://www.emarketer.com/content/earnings-report-how-is-digital-advertising-spending-performing-halfway-through-2024 , August 2024)

Unfortunately, the same technique is applicable for adverse actors to spread malware and infect remote systems.  The popularity of Malvertising has influenced various bad actors to redefine their techniques and execute activities ranging from gathering system information to Ransomware.

A distinct concept of Malvertising is its ability to infiltrate legitimate online advertisements (ads) within websites.  Initially, ads are embedded within a website with no intent of deploying malicious code. Once a site is compromised by a bad actor, an injection of malicious code such as spyware or malware is distributed throughout legitimate code.  Malicious code is deployed to a mass number of visitors naïve to its immoral behavior.  The final step of the bad actor is to remove any trace of malicious code. (Wikipedia Contributors, "Malvertising", Wikipedia, The Free Encyclopedia, December 2023)

Removing malicious code from a site intensify the ability of tracking who, what and where the code originated. Tracking the depth of damage throughout the network becomes invincible. ~~A malicious actors' intentions for injecting code into a legitimate site is never to remain on the original site.~~

Any end user who interacts with a malicious ad is susceptible to a number of outcomes. For malicious code to execute and function as intended, the end user must interact and allow the code to download or install on their device. This task is predicated on the user downloading the code one of two ways, automatic download which happens by design of code or the user clicking the malicious advertisement. Several results may occur from a single click of a malicious link. Two results include "redirecting traffic" and "executing code".

Redirection is a common term used to establish communication between two websites. A natural characteristic of the World Wide Web is the process of routing network traffic from one location to another. To efficiently communicate between two destinations, several sub sites are traversed before reaching the final destination. Similar to traveling across any Country or territorial body of land. Directly traveling through the common body(s) of land from a current location to destination is more efficient than routing around the common body(s) of land to reach an intended destination. To establish a successful connection to a remote site, website traffic is like traveling across bodies of land, direct communication yields greater speed and protection, therefore sub networks are connected between source and destination.

In communication between two sites, a malicious advertisement will redirect an end user to its own malicious website with no intent of connecting to the intended destination. While the end user has no indication or knowledge of this involuntary redirect, activity between user and the website persists as normal. To access a site, the following details may be required but not limited to providing a name and password credentials; banking transactions; medical records; proprietary information; network details;

device details; or any other details the bad actor can use to infiltrate the end user system. All activity is susceptible to being recorded and stored for the bad actors to utilize in a malicious manner for future endeavors.

A second intent of bad actors is to successfully execute the code and transfer data directly from the targeted device in an effort to not being discovered or prevented by the antivirus software. While the success rate of completing this process remains difficult, it yields profitable and persistent information over time.

## Methodology

To understand the process of executing a successful Malvertising campaign, both the technical and psychological approach is analyzed. Redirecting traffic traversed online includes an in-depth understanding of code development and networking.

In the area of networking, bad actors configure website traffic to route back to their C2C server. Traffic redirected by a malicious ad, terminates a server managed by the bad actor. Bad actors acquire skills in these areas including system administration, networking and security administrators. Skillful techniques are necessary to export data related to credentials, passwords, credit card details, addresses, phone number, banking, medical and other privilege details applicable to the individual or network. Two cases will be reviewed to analyze the process and methodology to gain this particular information.

### ***Case Study I***

Google experienced Malvertising during a couple of attacks between November - December 2020. Approximately eighty-eight domains were discovered by Guardio Labs. These sites hosted or contaminated malicious ads. Guardio accepted the challenge to investigate and research the incident during the last week of December 2022. (Banyan Security Research Labs, 2023, “Malvertising and

Vermux – Cybercrime Goes Mad Men”  https://www.banyansecurity.io/blog/malvertising-and-vermux-cybercrime-goes-mad-men/ )

Guardio Labs discovered Russian domains primarily targeting US endpoints.  Graphic Processing Units (GPU) were targeted by one attack which was named Vermux by Guardio Labs.  The attack originated as an effort to power crypto wallets. Ads generated on legitimate sites which redirect users to a malicious domain afterbern[.]live.  The ads impersonated an MSI Afterburner graphics card tool. (Guardio Labs, 2022, https://labs.guard.io/masquerads-googles-ad-words-massively-abused-by-threat-actors-targeting-organizations-gpus-42ae73ee8a1e )

The Vermux attack is a great example of the psychological perspective discussed above in the Methodology section.  There must be an ability to develop advertisements to entice a specific community of end users. The attacker must present relative content attractive to various audiences, society, and communities at the current point in time.  Ads must intrigue an end user's appetite to psych ally capture the eyesight and coerce the decision to click an ad without rehearsing normal security tactics to prevent such behavior.  Time affects end user decisions.  The quicker an ad captivates the attention of an end user, the greater opportunity for marginal error such as not recognizing a misspelled domain.

Users targeted during the Vermux attack often searched and shopped for ways to overclock processors.  Overclocking employs the opportunity for gamers to increase voltage in graphical processing units and take advantage of faster game speeds and enriched graphics.

MSI Afterburner is a popular tool downloaded and used by many gamers to increase speeds in their GPU.  As users search the word “Afterburner” google analytics (discussed later) recognized the keyword search and presented the malicious website as a solution to download “Afterburner”.  (google analytics select a site based on popularity of website and a trust relationship established with google before site can be manipulated and utilized in a malicious manner) However, the actual website domain embedded in some options returned redirect to *afterbern.live,* a malicious site. The end user must choose the malicious site by clicking on the advertised option as an option to download MSI Afterburner. Once the user interacts with this malicious site, involuntary payload(s) are downloaded to the user and once executed it will establish access to the user's internal processes. Once an established connection is established, files are installed to allow the user to maintain a binding connection in memory and access to processor locations. The goal is to access GPU processor power and remotely consume processors on the attacker's side, resulting in increasing crypto mining production.

Second research conducted by Guardio Labs discovered impersonating websites and ads mimicking Grammarly registered domains. Based on keyword searches related to Grammarly, google analytics returned websites matching the keyword searched. Each time a user naively selects a URL impersonating a Grammarly site, a trust relationship is established between the malicious ads and Google services, security and policy. Each official google ad is assigned a unique number known as Google Click ID (gclid). Websites embedded ads to promote other services and products. These ads contain a unique identification number to identify a legitimate google ad with its parent website (domain). The unique id is identical to its parent website where the end user is redirected too after clicking on the ad. In this case study the domain grammarly[.]org. (original site: grammarly[.]com) is one of the eighty-eight discovered domains trusted by google ads analytics over time.

The transition from a legitimate website to a malicious website occurs when the end user naively clicks an ad resembling grammarly[.]com. The user is re-directed to a malicious website impersonating Grammarly such as grammarly[.]org or grammmartly[.]org. Very subtle name differences route network traffic in different paths. One path leads to a benign website grammarly.org which functions normal with no malicious intent, however, it is not the official grammerly[.]com site, whereas grammartly[.]org route traffic to a malicious site and traverse traffic to a C2C server. User activity is then monitored and recorded to entrap useful information such as passwords, usernames, pin codes, etc.

How is traffic dynamically routed?  Based on its gclid.  If the unique id matches an impersonated Grammarly domain, the user is redirected to a malicious site.  Whereas, if the gclid does not match an impersonated malicious Grammarly domain, the user is redirected to a benign site.

Google Analytics determine which site is returned based on a keyword typed into a search engine (Google help topics, https://support.google.com/searchads/answer/7342044?hl=en ) In this case study a search query's related to Grammarly such as "download Grammarly" will return a popular list of sites related to Grammarly.

Once interaction with a malicious ad is established, the end user is routed to either a malicious or benign site.   Several parameters influence how a user is routed across the network including but not limited to the end user geo-location, user-agent, gclid, etc.  Meeting a pre-determined characteristic(s) result in the end user routed to links resembling numerous iterations of *gramm-arly.com*.  Network traffic communication is masked from the end user viewpoint.  Redirection is controlled by the bad actor's C2C server.  The process and switching of networks are oblivious to the end user.

Communication between the end user and malicious site is now established.  The connection creates a conduit to deliver malicious payload(s)transferred from the bad actor C2C server to the end user device. A payload entails a variety of variations designed to extract or destroy relevant information essential to the bad actor from its victim device.   Guardio Labs noted three unique characteristics:

1. **Bundled with legit software** – a legitimate version of Grammarly is installed along with an executable file silently detonated in the victim's device extracting information.
2. **Bloated Files** – inflating the executable file with zeroes and expanding larger than automated malware analysis systems' max size allowed.

3. **Changing Payloads Periodically** – Altering the behavior of payloads.

**Mobile Devices**

Malvertising gained public exposure to both Android and iPhone devices.

*Android*

One area where malware continues to rise is mobile devices. Threats for mobile device applications increased approximately 30% between the first half of 2022 to 2023. This affects not only corporations and large organizations but also personal devices. (Verizon, 2023, “2023 Mobile Security”) Kaspersky protected personal devices processed over 5 million cyber-attacks attempted during Quarter 2 of 2022. (Maserve, “Mobile Malware”, https://www.techtarget.com/searchmobilecomputing/definition/mobile-malware, 2023)

Android devices are popular for using the redirect method to coerce individuals in interacting with hidden malicious sites. An example of this technique is an advertisement for an Amazon gift card or a sale item recently viewed on a different website. Bad actors take advantage of cookies to identify browser history and most common sites visited. Replications of these sites are developed and inserted into legitimate sites as ads and google applications. The replicas contain embedded code utilized by the bad actor to redirect user or transfer malicious code through an open session to the endpoint.

*iPhone*

Most popular method used to attack iPhone devices include but not limited to injecting malicious applications such as Apple Pay sessions. The code infects the application by inserting functions intelligent enough to interact with native Apple code. The code is able to make routing decisions based on what outcome is returned after a function executes.

A function grouped with various methods to create code to interact between memory, hardware, and software. The method “canMakePayments” is a payment authorization request that probes the user device for a valid Apple wallet payment method. Based on the outcome returned by a Boolean function of true or false, it determines where the application redirect the user. When a user does not have Apple Wallet setup and is active on their device, the code will remain dormant and not interact with the mobile device. If the function returns true, the code will redirect the user to a malicious C2C server managed by the bad actor. After verification of payment is complete a three-step process is required to accomplish this task:

1. User receives two popups:

   i) device update

   ii) install Apple Pay update

2. A screen overlay presents the end user with a credit card details page where the end user must enter card information
3. Malware logs the following data and sends back to C2C server:
   a. credit card information
   b. iOS version
   c. IP

(Fiscutean, “What is Malvertising? When Malicious ads attack”, CSO, December 2020)

Mobile security company Wandera vice president Michael Covington categorized three characteristics of Malvertising in mobile devices:

1. In-App Phishing attack – attacks distributed inside malicious application

2. Cryptojacking – utilizing resources from an unauthorized remote computer to mine cryptocurrency (see Vermux Case Stud I above)
3. Deliver Payloads to device – least successful

Malvertising will continue to threaten mobile device security. Attacks like cryptocurrency empower an attacker with access to unauthorized power and computer processor resources directly from the attacked computer. Resources are used to verify cryptocurrency transactions. Resources compromised from these devices are dispersed as power and processor speed to accelerate the attacker's local system performance. In addition to consuming power resources, gaining access to various third-party exchange institution networks to convert crypto to legally traded currency, is a successful outcome. Commonly known as "Money laundering", a criminal case trial prosecuted the exchange of virtual currency for legally recognized trading currency. (Hayes, "Convertible Virtual Currency: Meaning, Types, and Example", https://www.investopedia.com/terms/c/convertible-virtual-currency.asp, March 2024)

Malvertising can present a long-term footprint in compromised environments. This tactic has proven to be more destructive and less exposable, due to careful planning and attack methods. An incentive for gaining unapproved persistent access to a remote system to yield success in gaining confidential or proprietary information to leverage future attacks. A successful attack will return confidential information relevant to the targeted victim including user online activity, device and network information, or confidential private information applicable to:

- Is device in motion or at rest
- Position of device
- Browser platform: Linux x86_64, Win32, or MacIntel
- Antivirus presence
- Is device Android or iPhone

Mobile devices can be twice as difficult to sift out malicious activity due to several uncontrollable reasons including but not limited to:

- screen size present difficulty identifying URL
- excessive usage may cause relax in trusting unknown sources
- links in emails erroneously clicked

For the majority of common end users, they’re not trained in cybersecurity defense tactics. Therefore, security is achieved from a cohesive approach. End user awareness in harmony with overarching governance ordinances must be leveraged to manage the evolving threat to offensive cyber-attacks.

Vigilant observation, patched devices and virus protectors are three main defenses an end user can practice combatting such attacks. An indispensable factor of malvertising entails the psychological concept of enticing end users’ attention and coercing them to provide sensitive data. Don’t easily be misled into taking the bait of advertisements and misspelled domains. Take the extra steps by googling an advertisement, locating the secure link, hovering over the link with the mouse, and manually verifying the URL is correct before clicking the link. Malvertising offers no returns. Click Safely!!!