Monthly Cybersecurity Newsletter

March 2023
Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Carly Sherrod

Malware Hidden in Google Search Ads

Google has recently discovered malicious software suppressed within some of its ads that have appeared in its search results. This software, otherwise known as Malware, is designed to exploit the weaknesses in the search engine's system.

Malware is the term used to describe any computer program or other code designed to harm or exploit a computer system. It is often used by hackers to steal sensitive information or to spread viruses and other malicious software. Recently, an especially destructive form of malware has been found in Google search ads. Google has outlined ways for users to identify and protect themselves from falling victim to Malware attacks. [Protect yourself from malware - Google Ads Help]

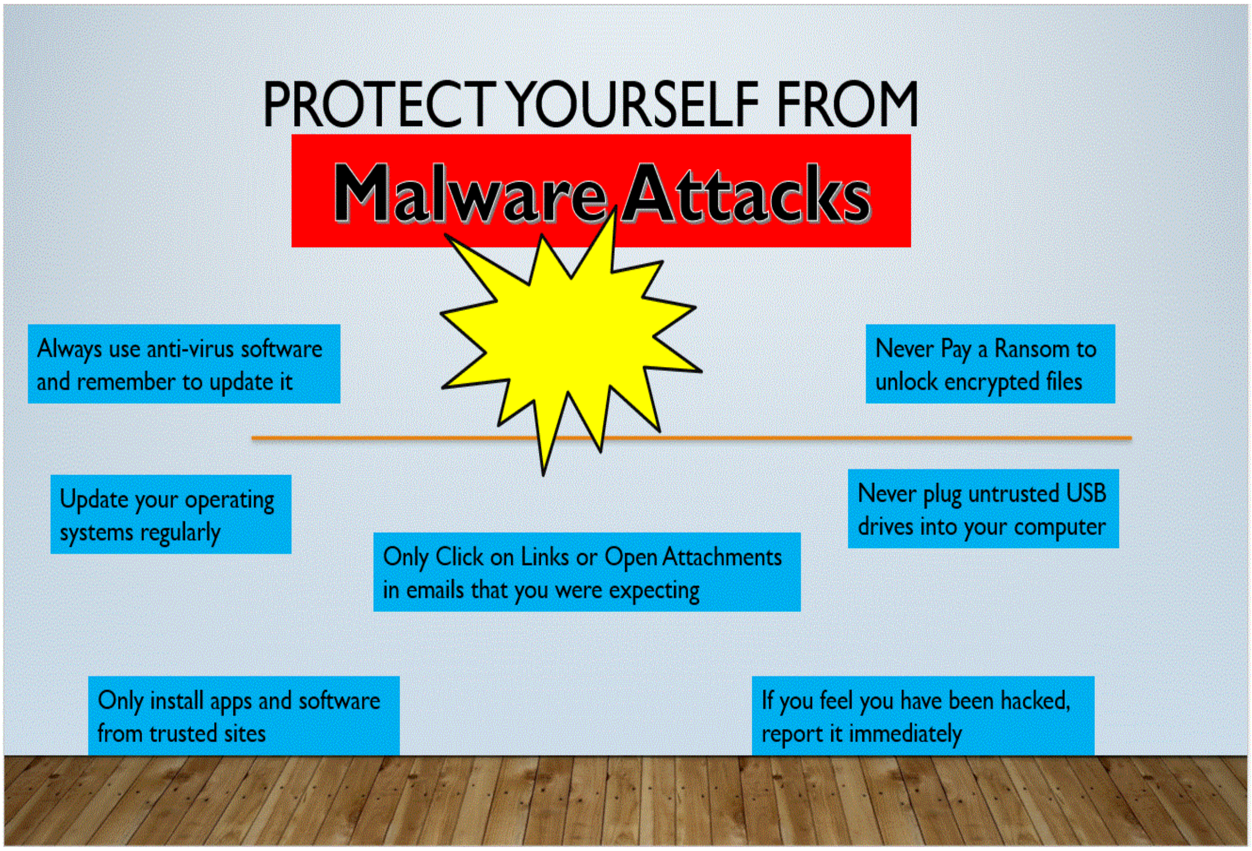
Google search ads are intended to help businesses and individuals promote their services, products and websites. Unfortunately, hackers have started creating malicious Google search ads in an effort to fool unsuspecting users into clicking on them. These ads contain malicious links that, if clicked on, will install malware on the user's system. The malware may be designed to steal personal information, launch distributed denial-of-service attacks, or even take control of the user's computer.

This image is redistributed with permission from KnowBe4.

Thankfully, Google is actively working to combat malware within its ads. The search engine's engineers are creating safeguards to ensure that ads are safe and are of high quality. Additionally, Google is blocking malicious domains and ads that contain malicious content. [Prevent malware in ad content - Google Ad Manager Help]

Even with these safeguards in place, users must be on the lookout for malicious search ads. It is important to recognize the signs of a bad ad, such as suspicious domain names, deceptive offers or shortened URL links. If you suspect that a malicious ad is being used, it is best to report it to Google immediately so that it can be removed from the search engine's system. It is also important to be vigilant when clicking on unknown sources as they can also be malicious.

Ultimately, it is essential for Google users to be aware of the threat imposed by malicious search ads. Understanding the dangers of such malicious software can help us stay safe with using the Google search engine.



PROTECT YOURSELF FROM

Malware Attacks

Always use anti-virus software and remember to update it

Never Pay a Ransom to unlock encrypted files

Update your operating systems regularly

Never plug untrusted USB drives into your computer

Only Click on Links or Open Attachments in emails that you were expecting

Only install apps and software from trusted sites

If you feel you have been hacked, report it immediately

Be Wary of Survey Scams

Online surveys are too often scams designed to steal personal or financial information, warns Phil Muncaster at ESET. Muncaster explains that these surveys are usually distributed via phishing or by ads on websites, impersonating trusted brands and offering phony rewards:

- “The scam often begins with an unsolicited email or text/message likely spammed out to countless other victims. This is basically a phishing message designed to lure the recipient into participating by clicking through.
- “It often features a well-known brand to add a sense of legitimacy and encourage the victim to participate. In December 2022, a popular survey scam abused the brand of chocolate-maker Cadbury to do this – promising recipients the chance to win ‘an exclusive Christmas Chocolate Magic Basket’ if they took a short quiz.
- “The scam may feature a thematic lure – such as the Christmas Cadbury one, or the supposed ‘40th anniversary’ of wholesaler Costco which was used in a June 2022 campaign in South America.”

These scams can cause varying degrees of damage. Many are focused on collecting information, and others attempt to trick the user into installing malware or transferring money. Muncaster offers the following recommendations to help users avoid falling for these scams.

- “Look out for any offers that seem too good to be true. It could be a large cash prize for just a few minutes work, or an expensive gift.
- “Watch out for typos or poor grammar – it could be a sign that things aren’t quite right.
- “Shortened URLs might also indicate fraud.
- “Time-limited offers are another way for scammers to turn up the pressure on their victims.
- “Some senders may be vague about who’s running the survey – with no ‘contact us’ link to follow.
- “If the sender uses a free webmail account, then the survey is likely to be a scam.”

It’s worth noting that such scam surveys represent a business as well as a personal risk. Many of them are cast as business-to-business surveys to take the temperature of a market, or to gauge the climate of opinion among customers.

This article is redistributed with permission from KnowBe4.

[HEADS UP] Russian Hacker Group Launches New Spear Phishing Campaign with Targets in US and Europe

DON'T GET HOOKED BY PHISHING SCAMS!
THINK BEFORE YOU CLICK.
REPORT SUSPICIOUS EMAILS.
WHEN IN DOUBT, DELETE.

The Russian-based hacking group, Seaborgium, is at it again with increased spear phishing attacks targeting US and European countries in the last year.

Last month, I previously wrote about Seaborgium launching a phishing campaign with targets in the UK. Now these threat actors have taken one step further with fake personas, social media accounts, and academic papers to lure their victims into replying to their phishing emails. They have also widened their net to multiple regions across the globe with a new focus on the US and additional regions within Europe. Each successful attack means the threat actor is able to refine their fake profiles to be more convincing and lure future victims.

Journalists are also becoming a target for multiple Russian hacking groups. Since journalists hold sensitive information, it could serve as high value to execute cyber espionage for the Russian state-sponsored groups.

While spear phishing campaigns continue to increase in sophistication, the root cause stems from social engineering. Whether it was specific language in the email or a convincing fake profile, threat actors are refining commonly used social engineering tactics to ensure your users fall victim to their attack. Thankfully, there are ways to identify if your organization is being targeted. We have several tips for preventing a spear phishing attack from targeting your users:

- First of all, you need all your defense-in-depth layers in place. Defending against attacks like this is a multi-layer approach. The trick is to make it as hard as possible for the attacker to get through and to not rely on any single security measure to keep your organization safe.
- Do not have a list of all email addresses of all employees on your website, use a web form instead.

- Regularly scan the Internet for exposed email addresses and/or credentials, you would not be the first one to find one of your user's username and password on a crime or porn site.
- Never send out sensitive personal information via email. Be wary if you get an email asking you for this info and when in doubt, go directly to the source.
- Enlighten your users about the dangers of oversharing their personal information on social media sites. The more cybercriminals know, the more convincing they can be when crafting spear phishing emails.
- Users are your last line of defense! They need to be trained using new-school security awareness training and receive frequent simulated phishing emails to keep them on their toes with security top of mind.

This article is redistributed with permission from KnowBe4.

Reddit is the Latest Victim of a Spear Phishing Attack Resulting in a Data Breach

There is a lot to learn from Reddit's recent data breach, which was the result of an employee falling for a "sophisticated and highly-targeted" spear phishing attack.

I spend a lot of time talking about phishing attacks and the specifics that closely surround that pivotal action taken by the user once they are duped into believing the phishing email was legitimate.

However, there are additional details about the attack we can analyze to see what kind of access the attacker was able to garner from this attack. But first, here are the basics:

According to Reddit, an attacker set up a website that impersonated the company's intranet gateway, then sent targeted phishing emails to Reddit employees. The site was designed to steal credentials and two-factor authentication tokens.

There are only a few details from the breach, but the notification does mention that the threat actor was able to access "some internal docs, code, as well as some internal dashboards and business systems."

Since the notice does imply that only a single employee fell victim, we have to make a few assumptions about this attack:

- **The attacker had some knowledge of Reddit's internal workings** – The fact that the attacker can spoof an intranet gateway shows they had some familiarity with the gateway's look and feel, and its use by Reddit employees.

- **The targeting of victims was limited to users with specific desired access** – Given the knowledge about the intranet, it's reasonable to believe that the attacker(s) targeted users with specific roles within Reddit. From the use of the term "code," I'm going to assume the target was developers or someone on the product side of Reddit.

- **The attacker may have been an Initial Access Broker** – Despite the access gained that Reddit is making out to be not a big deal, they do also mention that no production systems were accessed. This makes me believe that this attack may have been focused on gaining a foothold within Reddit versus penetrating more sensitive systems and data.

There are also a few takeaways from this attack that you can learn from:

1. **2FA is an important security measure** – Despite the fact that the threat actor collected and (I'm guessing) passed the credentials and 2FA details onto the legitimate Intranet gateway—a classic man-in-the middle attack—it's far better to have MFA in place than to have no additional authentication factors in place.

2. **Employees play a major role in organizational cybersecurity** – Reddit mentions that "soon after being phished, the affected employee self-reported, and the security team responded quickly, removing the infiltrator's access and commencing an internal investigation."

This article is redistributed with permission from KnowBe4.

Should You Click on Unsubscribe?

Some common questions we get are "Should I click on an unwanted email's 'Unsubscribe' link? Will that lead to more or less unwanted email?"

The short answer is that, in general, it is OK to click on a legitimate vendor's unsubscribe link. But if you think the email is sketchy or coming from a source you would not want to validate your email address as valid and active, or are unsure, do not take the chance, skip the unsubscribe action.

In many countries, legitimate vendors are bound by law to offer (free) unsubscribe functionality and abide by a user's preferences. For example, in the U.S., the 2003 CAN-SPAM Act states that businesses must offer clear instructions on how the recipient can remove themselves from the involved mailing list and that request must be honored within 10 days.

Note: Many countries have laws similar to the CAN-SPAM Act, although with privacy protection ranging the privacy spectrum from very little to a lot more protection.

The unsubscribe feature does not have to be a URL link, but it does have to be an "internet-based way". The most popular alternative method besides a URL link is an email address to use. In some cases, there are specific instructions you have to follow, such as put "Unsubscribe" in the subject of the email. Other times you are expected to craft your own message. Luckily, most of the time simply sending any email to the listed unsubscribe email address is enough to remove your email address from the mailing list.

In rare cases, in violation of the law, some vendors only provide a mailing address or phone number. A minority of legitimate vendors do not include an unsubscribe feature in their email or obscure it so much (e.g., in a tiny font mixed up in other tiny text at the end of the email) that it might as well be missing. But in general, most legitimate business emails include an unsubscribe link (although it is not always obvious), and if you follow the link, you can get taken off that business's email list.

Unfortunately, unsubscribing does not mean that the company has to remove you from any mailing lists they already gave or sold to other third parties, only that they cannot include your email address going forward from the moment you completed the unsubscribe action. Sometimes the resale of your email address happens so fast that unsubscribing does not prevent your email address from being used by dozens of other third parties.

It is also not unheard of for a legitimate vendor to ignore your unsubscribe request, even if they appear to give you a way to do it. Some obviously have broken processes or a poorly performing third party that supposedly handles it for them, but other vendors seem to knowingly skirt the law by claiming ignorance. There is a huge loophole in the CAN-SPAM Act that says that a vendor can continue to reach out to you if the email is "transactional or relationship", meaning the vendor is responding to a recipient's invited transaction or ongoing relationship. It is amazing how many vendors I have never done business with think their uninvited email is "transactional" or a continuation of our "relationship".

Violations of the CAN-SPAM Act can cost senders up to $50,120 per violation. If you cannot get the vendor to stop sending you unwanted emails, go here.

But if you know or suspect the email is coming from a non-legitimate vendor, clicking on any unsubscribe feature is hit or miss. Some of the spam senders consider themselves legitimate businesses and will offer and abide by the unsubscribing rule of their (or their recipient's home) country. Most will not. Most of the time, clicking on a fraudster's unsubscribe feature will simply confirm your email address is valid and active and this will likely result in your email appearing for sale in cybercriminal forums for years.

In summary, yes, click on those unsubscribe features when included in legitimate emails from legitimate vendors, but not if the email appears to be from a spam marketer or phishing scam artist.

This article is redistributed with permission from KnowBe4.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note**: You must have a valid state employee Microsoft 365 account*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Mar. 2: SANS Webinar: The State of DDOS Attacks: A Look Back at 2022

Mar. 8: SANS Webinar: Attack Surfaces Management Solutions Forum 2023

Mar. 14: SANS Webinar: Building Better Cloud Detections…By Hacking? |AWS Edition

Mar. 14: SANS Webinar: Streamline and Eliminate Audit Procedures

Mar. 15: SANS Webinar: Designing Access to Shared Datasets in the Cloud

Mar. 15: SANS Webinar: 2023 SANS Report: Become Timeless: The Present and Future Skills Needed for Cyber Security Job Success at Any Level

Mar. 16: SANS Webinar: The New OSINT Cheat Code: ChatGPT

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember … Stop. Think. Connect.*

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*