From Discussion Forums to Malware Mayhem: The Alarming Rise of Abuse on Google Groups and Usenet

cloudsek.com/blog/from-discussion-forums-to-malware-mayhem-the-alarming-rise-of-abuse-on-google-groups-and-usenet

Pavan Karthick M

Adversary Intelligence

8

mins read

Explore the escalating wave of cyber threats on platforms like Google Groups and Usenet, uncovering the pivotal role of cybersecurity in safeguarding online discussion forums.

Pavan Karthick M

February 3, 2024

Last Update posted on

February 5, 2024

Don't let your brand be used to trap users through fake URLs and phishing pages

Identify and counter malicious links and phishing attempts effectively with CloudSEK XVigil Fake URLs and Phishing module, bolstering your defense against cyber threats

Schedule a Demo

Table of Contents

Author(s)

No items found.

Category: Adversary Intelligence

Motivation: Financial

Region: Global

Source*: B - Mostly Reliable
2 - Probably True

In the fast-paced digital age, online discussion forums have become an integral part of our lives. These platforms provide an avenue for people with similar interests to connect, share ideas, and engage in meaningful conversations. Over time, these discussion forums have evolved, adapting to the changing needs and demands of internet users. However, along with this evolution, there has been a disturbing rise in abuse and malicious activities on platforms like Google Groups and Usenet.

Established in 1980 as a pioneering internet communication system Usenet, experienced a resurgence when integrated with Google Groups. This integration provided a bridge between traditional newsgroup discussions and a broader web audience. However, as Google prepares to end this integration by February 2024 announced in December 2023, a significant shift is occurring in online interactions within Usenet groups.

Particularly, legitimate public groups like 'microsoft.public.platformsdk.security' have witnessed an uptick in malicious activities, including posts related to illegal substance advertisements and malware distribution. While the end of new Usenet content integration is imminent, the accessibility of previously indexed data on Google Groups presents ongoing risks. This impending closure, coupled with the complexities of standalone Usenet clients, indicates a likely decline in Usenet's general accessibility and has become a catalyst for threat actors to maximize their reach in this transitional phase.

Also Read Compromising Google Accounts: Malwares Exploiting Undocumented OAuth2 Functionality for session hijacking

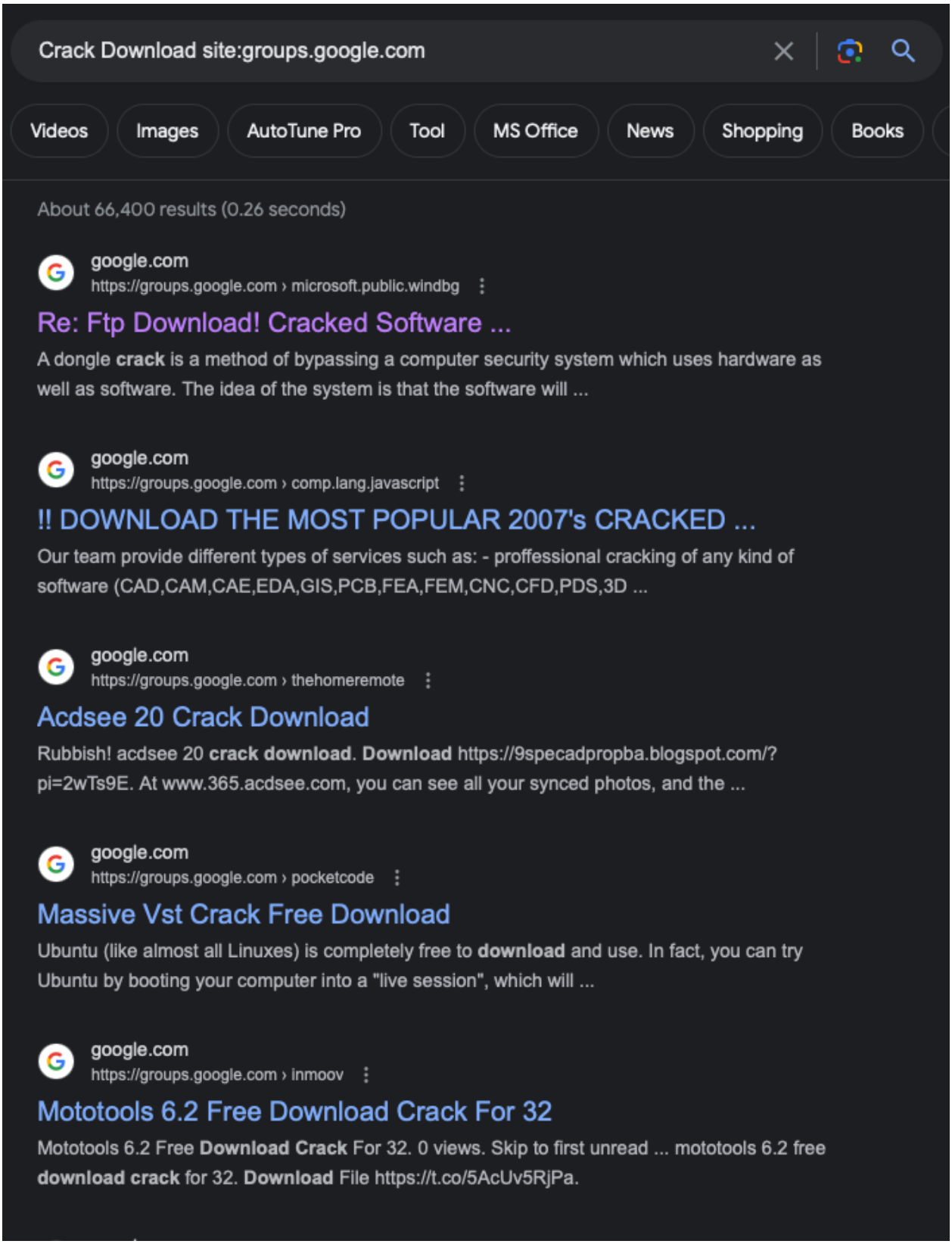
Key Takeaways

- **Exploiting Trust:** Malicious actors are increasingly targeting legitimate Usenet and Google Groups, particularly those focused on security discussions, to spread malware and illegal content disguised as helpful downloads or discussions.
- **Keyword Red Flags:** Be wary of searches using terms like "Crack Download" or "Mod Download" as they often lead to harmful content, even within seemingly legitimate groups.
- **Filtering Limitations**: While platforms like Google implement content filtering, it's not foolproof. Vigilance is crucial as malicious actors employ tactics like URL shorteners and redirects to bypass detection.
- **Threat Actors Exploiting Transition:** Threat actors are exploiting this transition by strategically placing malicious shortener urls which they control within legitimate groups which find their way to search results because of SEO tricks which they play. These placeholders often involve URL shorteners and redirects, ultimately leading users to harmful content even if they start their search innocently.
- **Shared Responsibility:** Both service providers and users must be proactive. Providers need robust filtering and user awareness initiatives, while users require caution and security tools to navigate these platforms safely.

Unmasking the Surge in Malicious Activities

Over the years, the internet has witnessed a surge in malicious activities, with Google Groups and Usenet being no exception. Cybercriminals and malicious actors exploit the open nature of these platforms to spread malware, engage in illegal activities, and manipulate unsuspecting users.

In the highlighted search query you can see 66,400 results. All the Top results which we noticed are having indicators that they spread malicious content.



Google group results - Query used to highlight a number of results with possible malicious intent.

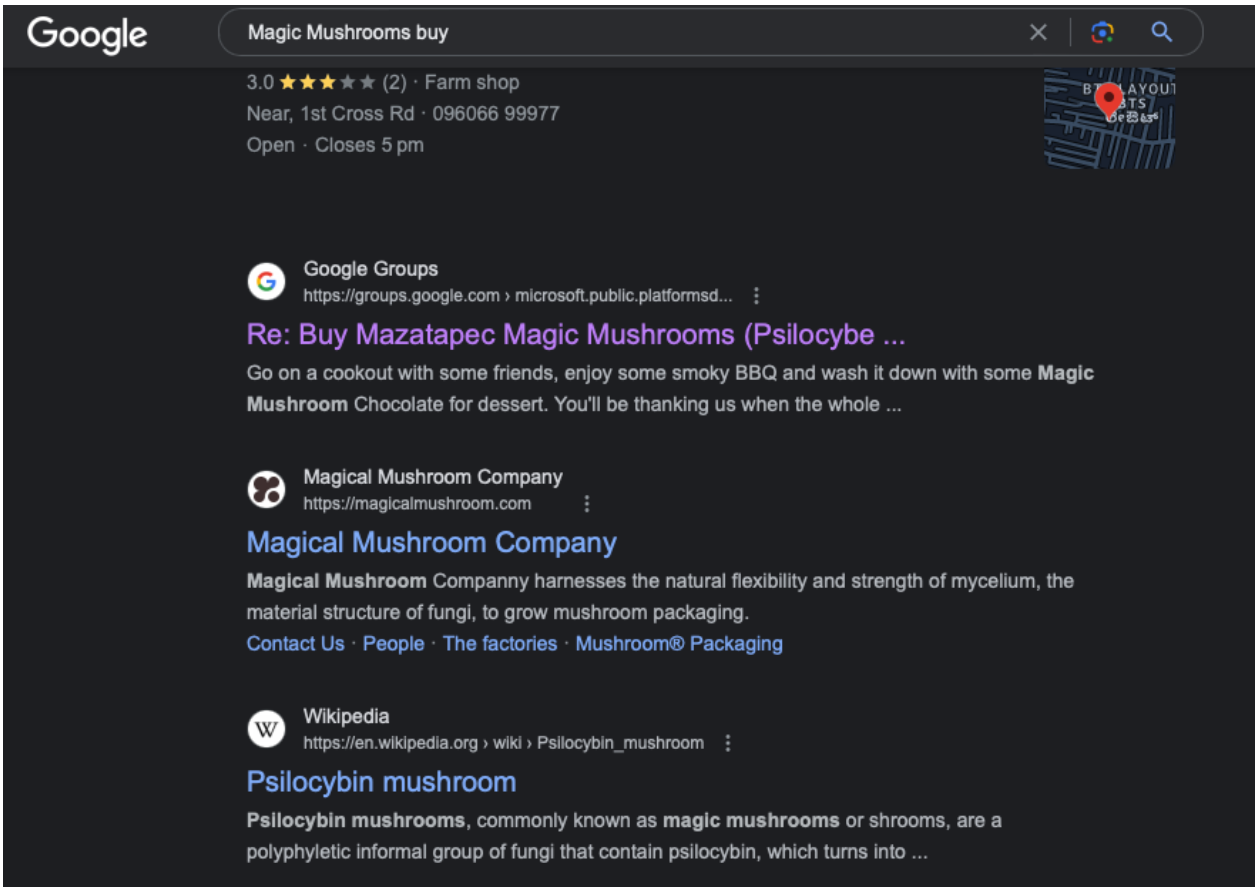
The Enduring Challenge of Indexed Data

- Usenet groups - microsoft.public.windbg a legitimate conversation was replied with malicious links to ahmadpc[.]org gullible users might try checking everything out in turn infecting themselves.
- Usenet group - comp.lang.javascript a legitimate usenet group was sent a message with redirection to www[.]prosoftstore[.]com a malicious site according to virustotal.
- Google Groups - thehomeremote a legitimate google group used by users of “The Home Remote” users for asking feature requests abused to spread malware using hxxps://9specadpropba[.]blogspot[.]com/?pi=2wTs9E
- Google Groups - Pocket Code / Catrobat User Forum a user group which was likely created by malicious actors was banned for spreading malware
- Google Groups - InMoov a legitimate google group for discussions about design software maintained their group and removed the message spreading the malware.

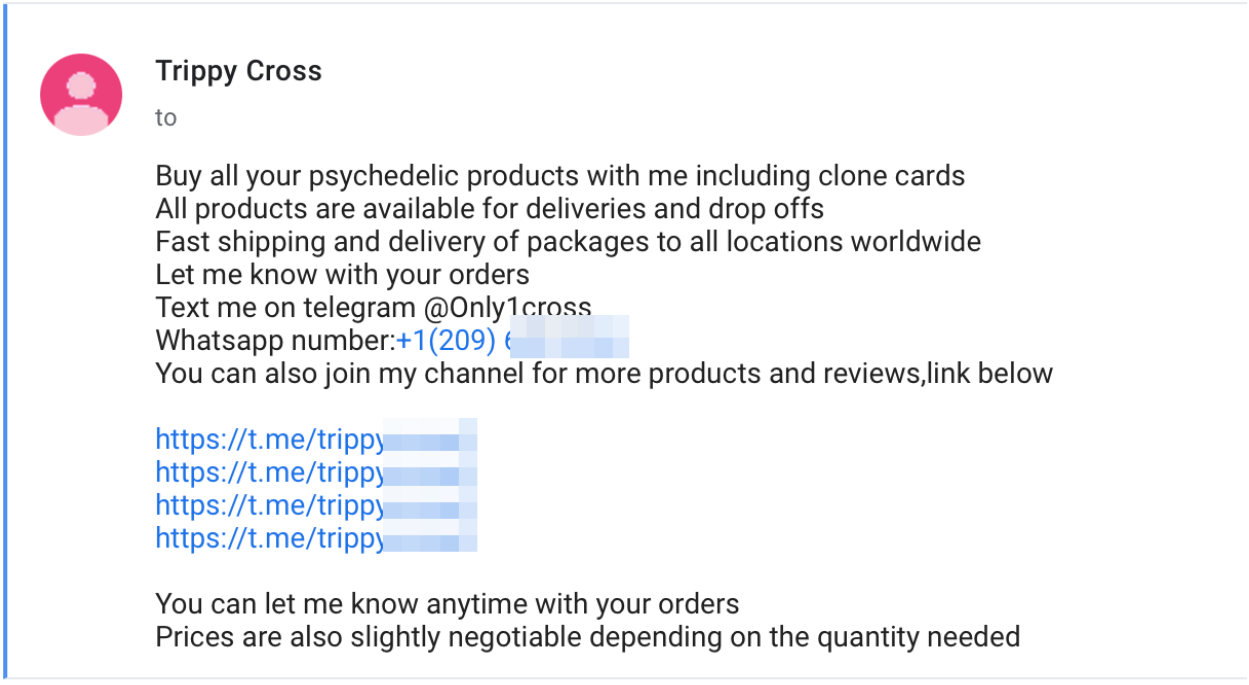
As seen actions are taken at certain times, but it doesn’t guarantee the malware free search results, so action from Group owners, Usenet owners, Users who browse are accountable on what they do to keep themselves malware free.

The Google Search Gateway

Manipulated Queries, Illicit Results

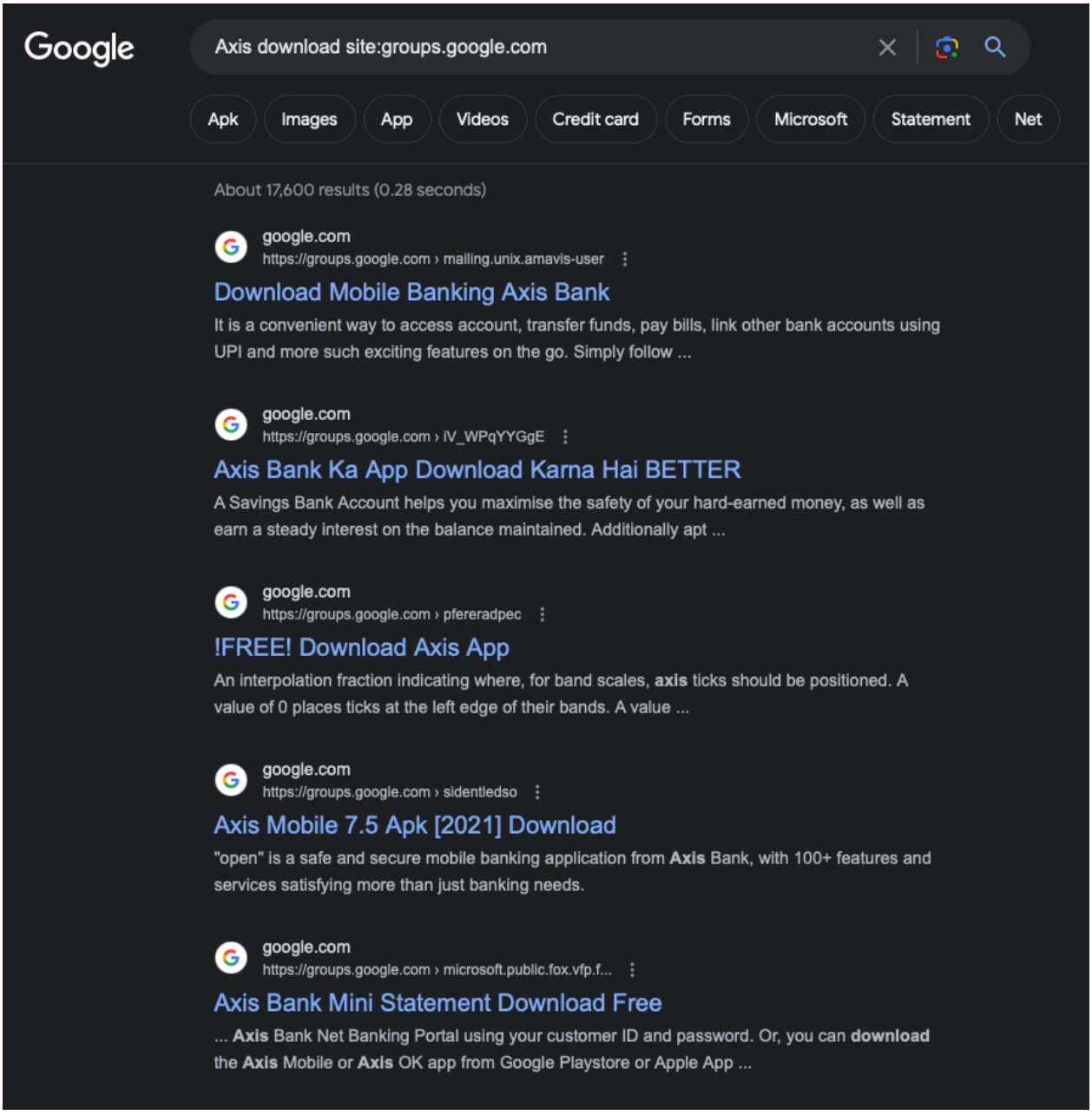


Search Query



Illicit result redirect sharing telegram marketplace for Controlled substances.

Brands targeted to spread malware



Search Results highlighting Brand name Abuse on Google Groups

A striking instance involves the misuse of prominent brand names, such as 'Axis Bank,' a well-known Indian banking institution. Malicious actors have leveraged these trusted brands to disseminate malware through various channels, including Google Groups, Usenet Groups, and User groups. This tactic not only capitalizes on the reputation and recognition associated

with established brands but also provides SEO benefits by attracting users searching for legitimate brand-related content, ultimately deceiving unsuspecting users into engaging with content that conceals malware threats.

Case Studies: Google Groups as a Vector for Illicit activity

Two existing activities shed light on the exploitation of these platforms for the propagation of malware and malicious content.

Case Study 1: "CrackedCantil: A Malware Symphony Breakdown"

- A blog post by AnyRun titled "CrackedCantil: A Malware Symphony Breakdown" provides a complete technical breakdown of the malware and how it found its way into the digital ecosystem using Google Groups as a delivery mechanism.
- In this scenario, unsuspecting users encountered the malware when they attempted to download what appeared to be a cracked version of IDA Pro. The unsuspecting victims were directed to a Google Groups conversation that linked to a fake website offering the cracked software. Unbeknownst to them, they were downloading malware that had infiltrated this seemingly legitimate platform.

Case Study 2: Twitter User Revelation

> Another alarming incident comes from a vigilant Twitter user who raised concerns about the state of online security. This user's discovery was nothing short of unsettling. It highlighted the persistent issue of top search results, particularly for COVID, illegal drug, and NSFW-related queries, being riddled with spam, explicit content, and malware.

These case studies collectively underscore the vulnerabilities within Google Groups and Usenet, emphasizing the urgent need for enhanced security measures and user awareness to combat the abuse and misuse of these platforms.

Recommendations

- Service Providers: Implement robust content filtering and monitoring mechanisms, particularly focusing on keywords and redirection attempts associated with illicit activities.
- Users: Maintain a critical eye towards online content, especially on unregulated platforms. Utilize security tools and practice safe browsing habits.
- Law Enforcement: Enhance collaboration with online platforms to identify and apprehend malicious actors behind these operations.

- Threat Intelligence Sharing: Foster continuous information sharing between threat intelligence communities, security researchers, and service providers to stay ahead of evolving tactics.

Conclusion

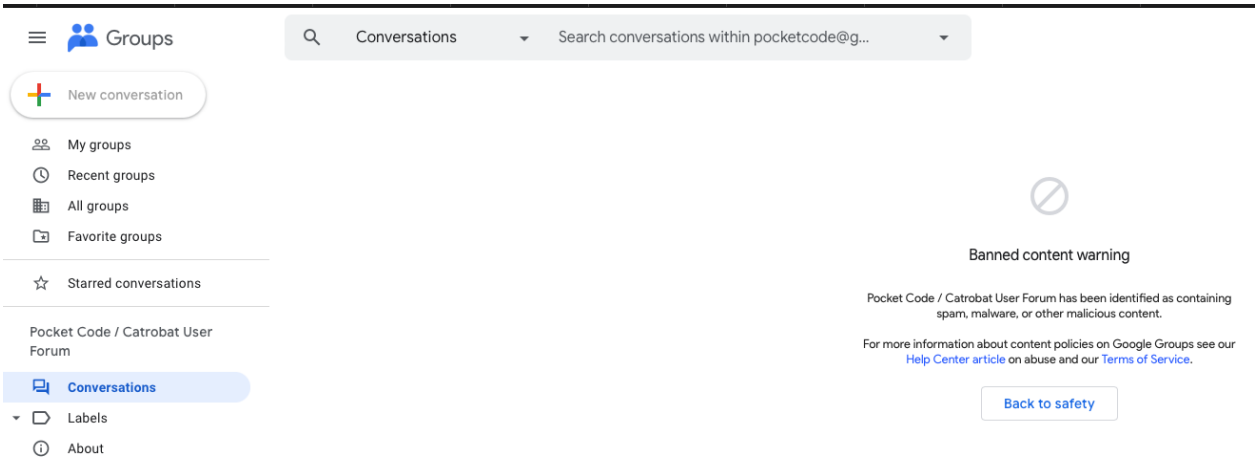
The surge in Usenet abuse serves as a stark reminder of the dark undercurrents of the internet, demanding a collaborative approach from all stakeholders. Group administrators are urged to maintain the cleanliness of their groups by promptly removing spam, enforcing posting restrictions, and managing group join requests. Similarly, Usenet administrators should employ similar measures to protect their communities. It is crucial to educate users about these issues, fostering a culture of awareness and vigilance. Google, as a leading platform, should continue its efforts in content filtering and banning malicious content by using focus words. Collectively, these actions are essential for mitigating the risks posed by malicious actors and for fostering a safer digital environment for all.

In conclusion, the rise in abuse and malicious activities on Google Groups and Usenet is a cause for concern. As these platforms continue to evolve, it is imperative to address these issues to ensure a safe and secure online environment. By harnessing the power of technology and promoting responsible participation, we can combat abuse and foster a thriving community within online discussion forums.

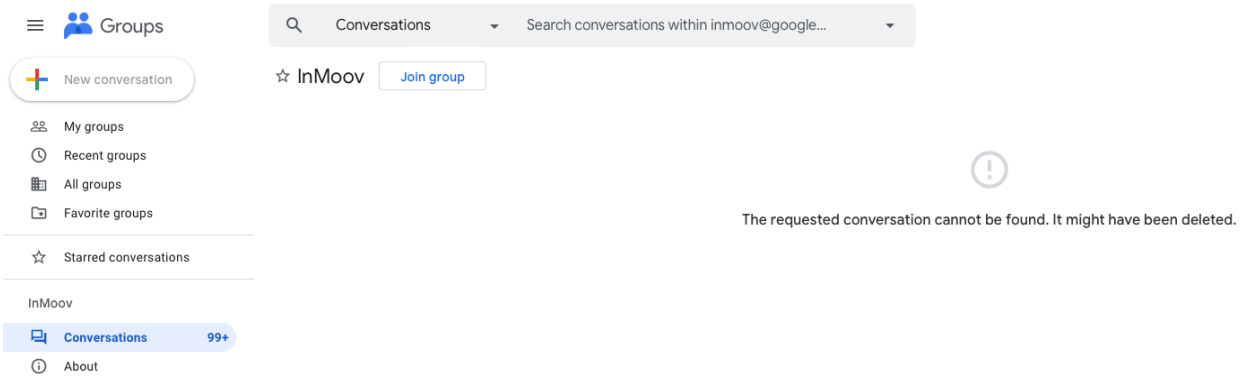
References

- CrackedCantil: Malware Work Together
- https://twitter.com/lilyraynyc/status/1738266748422365446

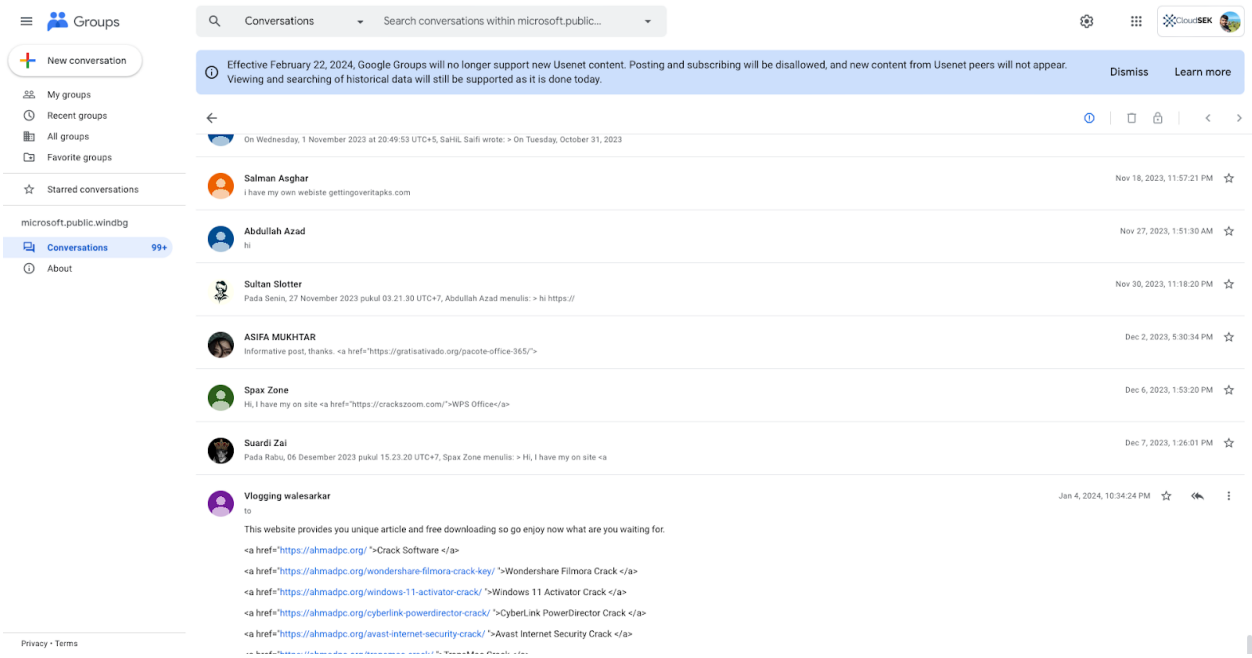
Appendix



https://groups.google.com/g/pocketcode - Banned content due to google's content filtering.



https://groups.google.com/g/inmoov/c/khPrj358HIY - Removed content, Group admin monitoring and keeping Group clean



Latest message from the group - Malicious link to ahmadpc[.]org a known malicious site

Author

Pavan Karthick M

Threat Intelligence Researcher at CloudSEK

Predict Cyber threats against your organization

Schedule a Demo

Adversary Intelligence

8

min read

Explore the escalating wave of cyber threats on platforms like Google Groups and Usenet, uncovering the pivotal role of cybersecurity in safeguarding online discussion forums.

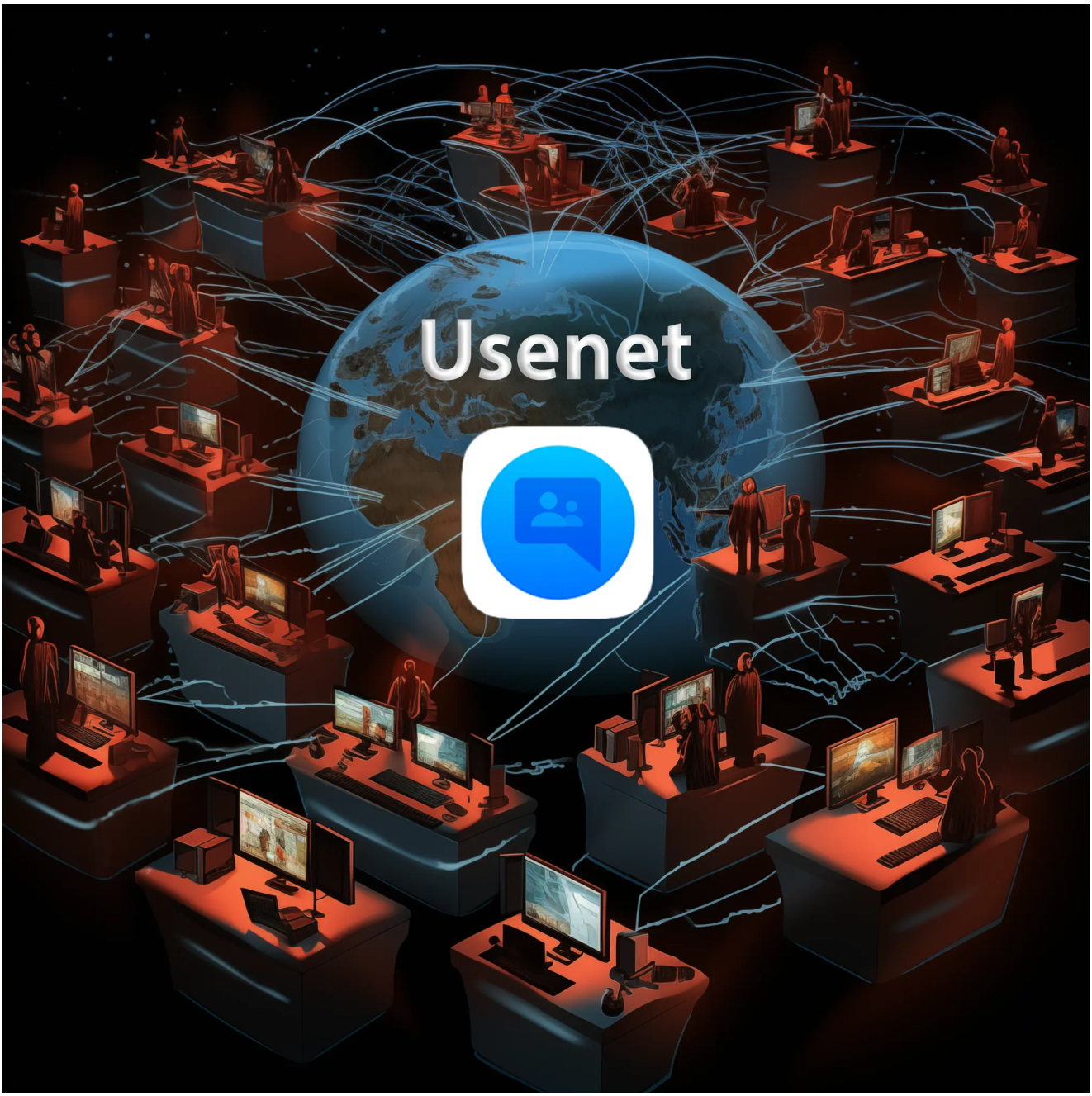
Authors

Pavan Karthick M

Threat Intelligence Researcher at CloudSEK

Co-Authors

No items found.



Category: Adversary Intelligence

Motivation: Financial

Region: Global

Source*: B - Mostly Reliable
2 - Probably True

In the fast-paced digital age, online discussion forums have become an integral part of our lives. These platforms provide an avenue for people with similar interests to connect, share ideas, and engage in meaningful conversations. Over time, these discussion forums have

evolved, adapting to the changing needs and demands of internet users. However, along with this evolution, there has been a disturbing rise in abuse and malicious activities on platforms like Google Groups and Usenet.

Established in 1980 as a pioneering internet communication system Usenet, experienced a resurgence when integrated with Google Groups. This integration provided a bridge between traditional newsgroup discussions and a broader web audience. However, as Google prepares to end this integration by February 2024 announced in December 2023, a significant shift is occurring in online interactions within Usenet groups.

Particularly, legitimate public groups like 'microsoft.public.platformsdk.security' have witnessed an uptick in malicious activities, including posts related to illegal substance advertisements and malware distribution. While the end of new Usenet content integration is imminent, the accessibility of previously indexed data on Google Groups presents ongoing risks. This impending closure, coupled with the complexities of standalone Usenet clients, indicates a likely decline in Usenet's general accessibility and has become a catalyst for threat actors to maximize their reach in this transitional phase.

Also Read Compromising Google Accounts: Malwares Exploiting Undocumented OAuth2 Functionality for session hijacking

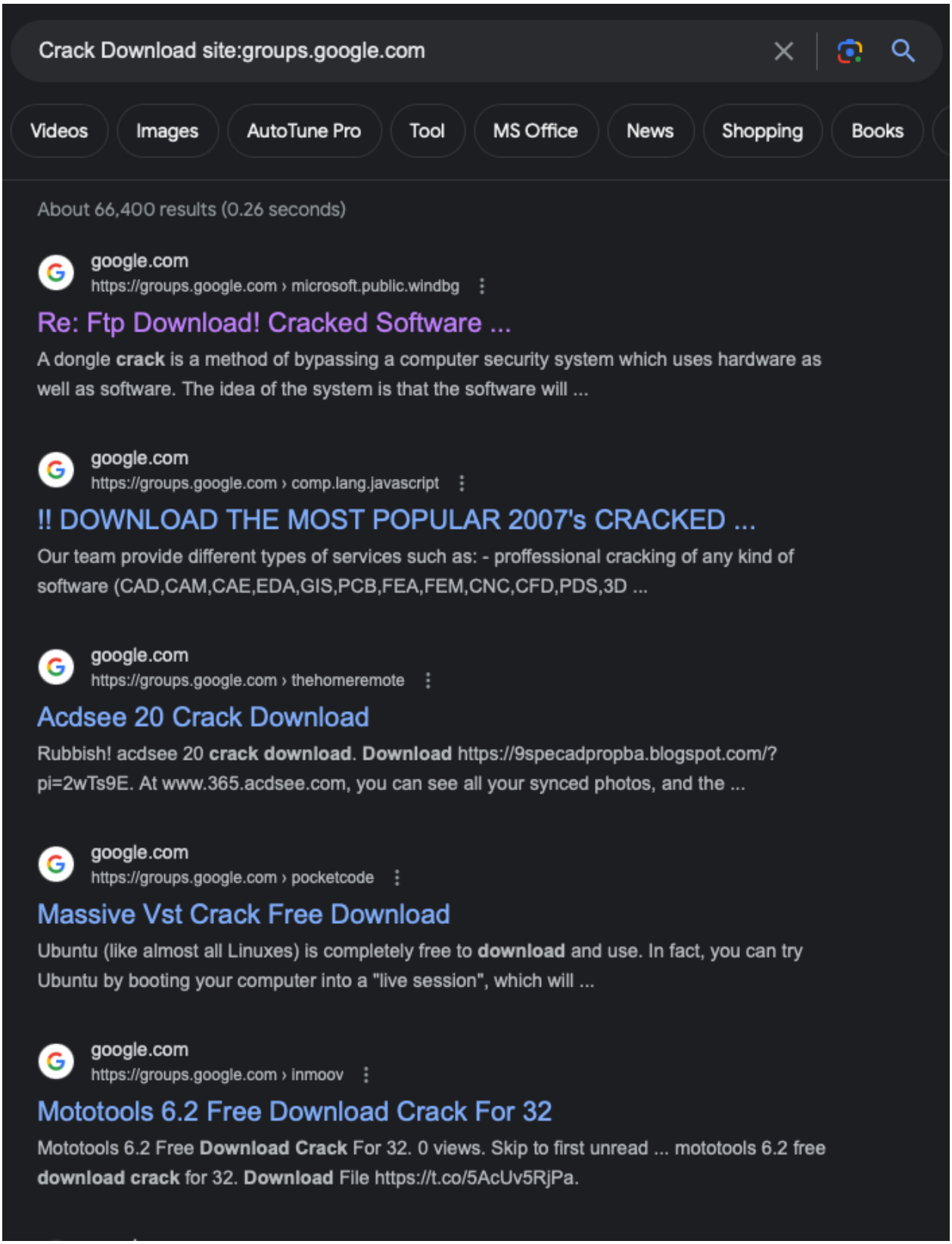
Key Takeaways

- **Exploiting Trust:** Malicious actors are increasingly targeting legitimate Usenet and Google Groups, particularly those focused on security discussions, to spread malware and illegal content disguised as helpful downloads or discussions.
- **Keyword Red Flags:** Be wary of searches using terms like "Crack Download" or "Mod Download" as they often lead to harmful content, even within seemingly legitimate groups.
- **Filtering Limitations**: While platforms like Google implement content filtering, it's not foolproof. Vigilance is crucial as malicious actors employ tactics like URL shorteners and redirects to bypass detection.
- **Threat Actors Exploiting Transition:** Threat actors are exploiting this transition by strategically placing malicious shortener urls which they control within legitimate groups which find their way to search results because of SEO tricks which they play. These placeholders often involve URL shorteners and redirects, ultimately leading users to harmful content even if they start their search innocently.
- **Shared Responsibility:** Both service providers and users must be proactive. Providers need robust filtering and user awareness initiatives, while users require caution and security tools to navigate these platforms safely.

Unmasking the Surge in Malicious Activities

Over the years, the internet has witnessed a surge in malicious activities, with Google Groups and Usenet being no exception. Cybercriminals and malicious actors exploit the open nature of these platforms to spread malware, engage in illegal activities, and manipulate unsuspecting users.

In the highlighted search query you can see 66,400 results. All the Top results which we noticed are having indicators that they spread malicious content.



Google group results - Query used to highlight a number of results with possible malicious intent.

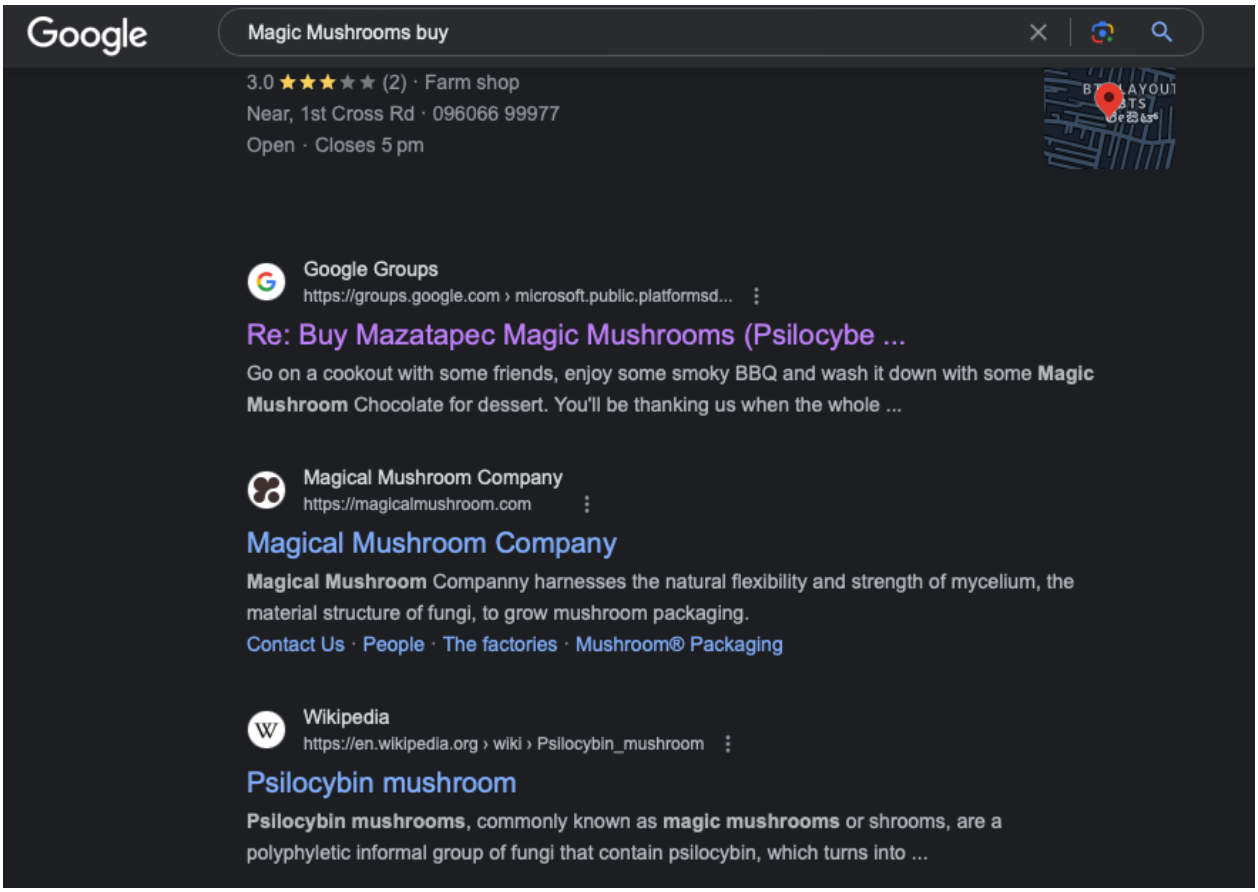
The Enduring Challenge of Indexed Data

- Usenet groups - microsoft.public.windbg a legitimate conversation was replied with malicious links to ahmadpc[.]org gullible users might try checking everything out in turn infecting themselves.
- Usenet group - comp.lang.javascript a legitimate usenet group was sent a message with redirection to www[.]prosoftstore[.]com a malicious site according to virustotal.
- Google Groups - thehomeremote a legitimate google group used by users of “The Home Remote” users for asking feature requests abused to spread malware using hxxps://9specadpropba[.]blogspot[.]com/?pi=2wTs9E
- Google Groups - Pocket Code / Catrobat User Forum a user group which was likely created by malicious actors was banned for spreading malware
- Google Groups - InMoov a legitimate google group for discussions about design software maintained their group and removed the message spreading the malware.

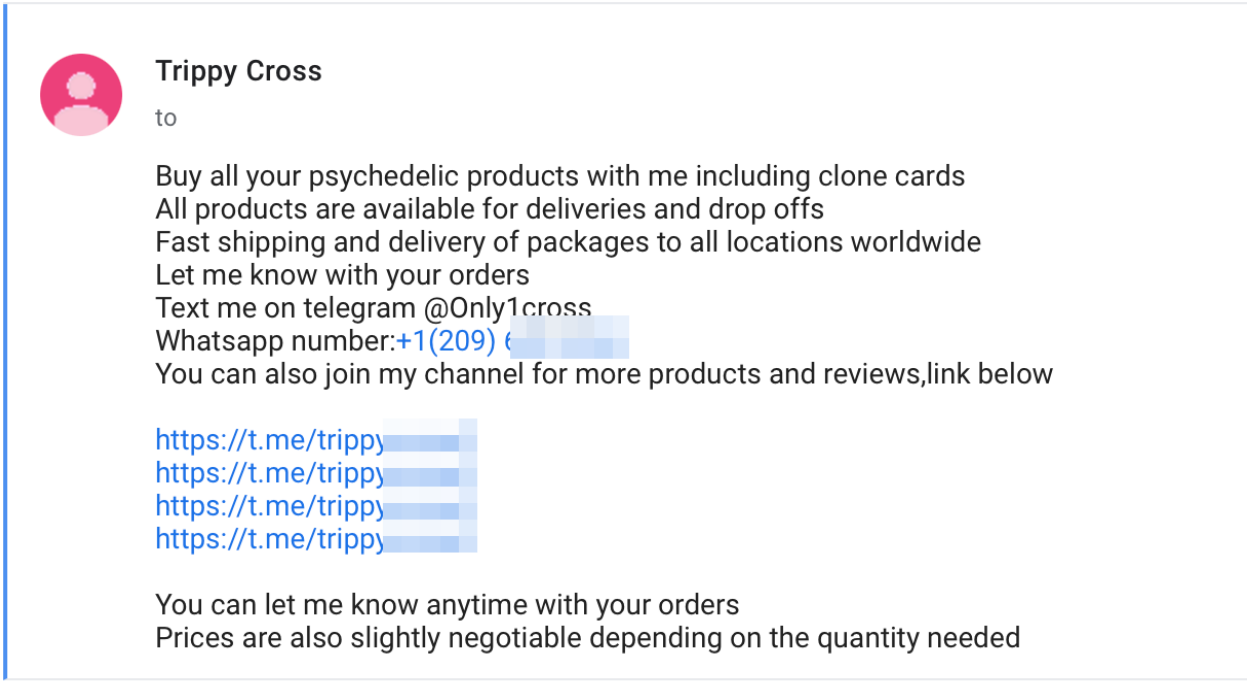
As seen actions are taken at certain times, but it doesn’t guarantee the malware free search results, so action from Group owners, Usenet owners, Users who browse are accountable on what they do to keep themselves malware free.

The Google Search Gateway

Manipulated Queries, Illicit Results

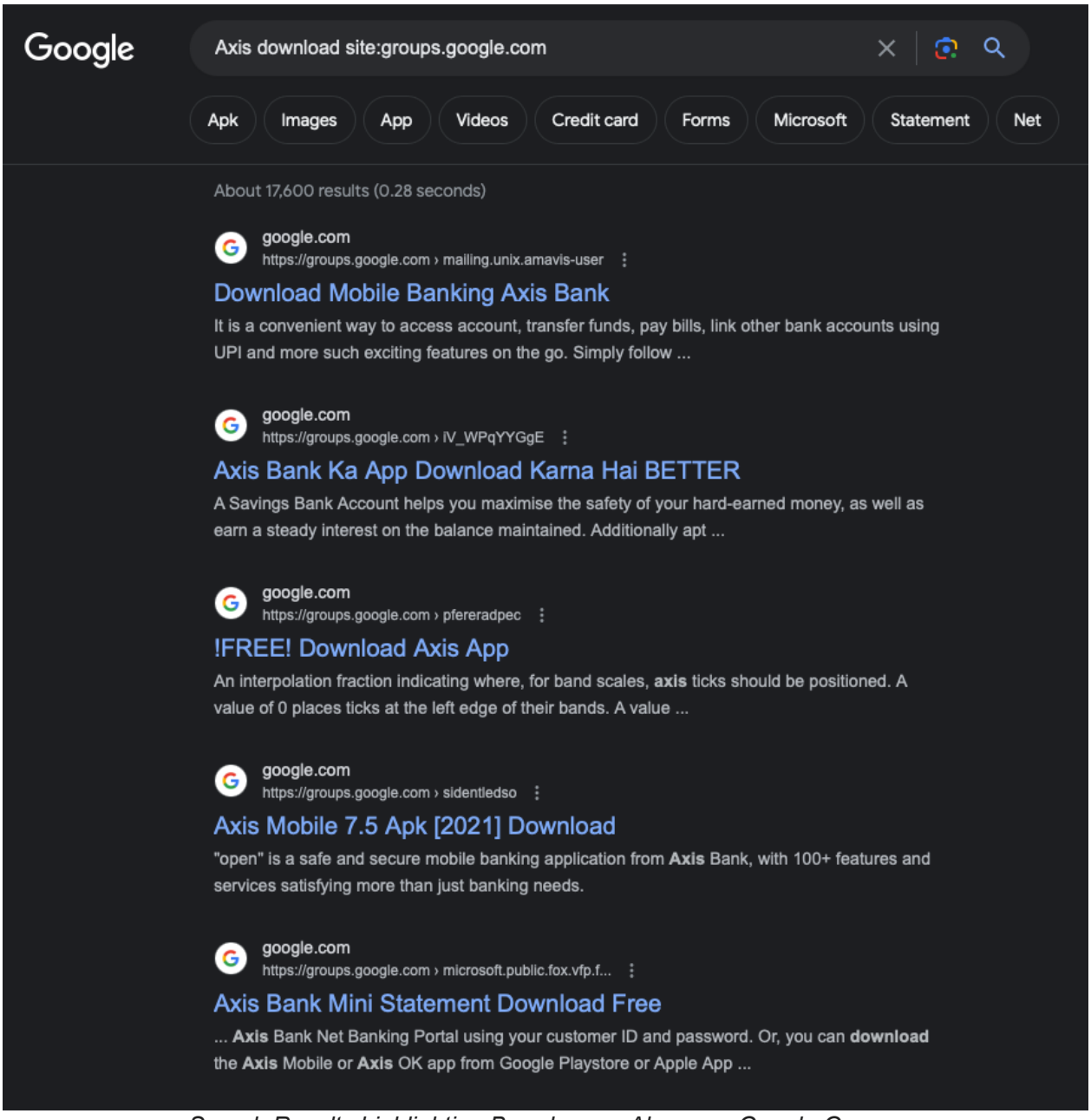


Search Query



Illicit result redirect sharing telegram marketplace for Controlled substances.

Brands targeted to spread malware



Search Results highlighting Brand name Abuse on Google Groups

A striking instance involves the misuse of prominent brand names, such as 'Axis Bank,' a well-known Indian banking institution. Malicious actors have leveraged these trusted brands to disseminate malware through various channels, including Google Groups, Usenet Groups, and User groups. This tactic not only capitalizes on the reputation and recognition associated

with established brands but also provides SEO benefits by attracting users searching for legitimate brand-related content, ultimately deceiving unsuspecting users into engaging with content that conceals malware threats.

Case Studies: Google Groups as a Vector for Illicit activity

Two existing activities shed light on the exploitation of these platforms for the propagation of malware and malicious content.

Case Study 1: "CrackedCantil: A Malware Symphony Breakdown"

- A blog post by AnyRun titled "CrackedCantil: A Malware Symphony Breakdown" provides a complete technical breakdown of the malware and how it found its way into the digital ecosystem using Google Groups as a delivery mechanism.
- In this scenario, unsuspecting users encountered the malware when they attempted to download what appeared to be a cracked version of IDA Pro. The unsuspecting victims were directed to a Google Groups conversation that linked to a fake website offering the cracked software. Unbeknownst to them, they were downloading malware that had infiltrated this seemingly legitimate platform.

Case Study 2: Twitter User Revelation

> Another alarming incident comes from a vigilant Twitter user who raised concerns about the state of online security. This user's discovery was nothing short of unsettling. It highlighted the persistent issue of top search results, particularly for COVID, illegal drug, and NSFW-related queries, being riddled with spam, explicit content, and malware.

These case studies collectively underscore the vulnerabilities within Google Groups and Usenet, emphasizing the urgent need for enhanced security measures and user awareness to combat the abuse and misuse of these platforms.

Recommendations

- Service Providers: Implement robust content filtering and monitoring mechanisms, particularly focusing on keywords and redirection attempts associated with illicit activities.
- Users: Maintain a critical eye towards online content, especially on unregulated platforms. Utilize security tools and practice safe browsing habits.
- Law Enforcement: Enhance collaboration with online platforms to identify and apprehend malicious actors behind these operations.

- Threat Intelligence Sharing: Foster continuous information sharing between threat intelligence communities, security researchers, and service providers to stay ahead of evolving tactics.

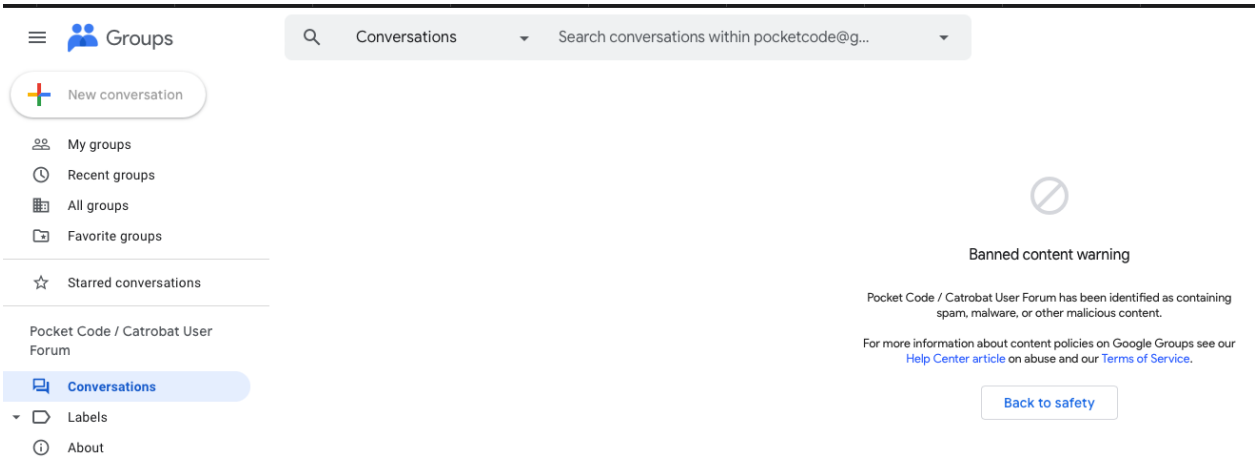
Conclusion

The surge in Usenet abuse serves as a stark reminder of the dark undercurrents of the internet, demanding a collaborative approach from all stakeholders. Group administrators are urged to maintain the cleanliness of their groups by promptly removing spam, enforcing posting restrictions, and managing group join requests. Similarly, Usenet administrators should employ similar measures to protect their communities. It is crucial to educate users about these issues, fostering a culture of awareness and vigilance. Google, as a leading platform, should continue its efforts in content filtering and banning malicious content by using focus words. Collectively, these actions are essential for mitigating the risks posed by malicious actors and for fostering a safer digital environment for all.

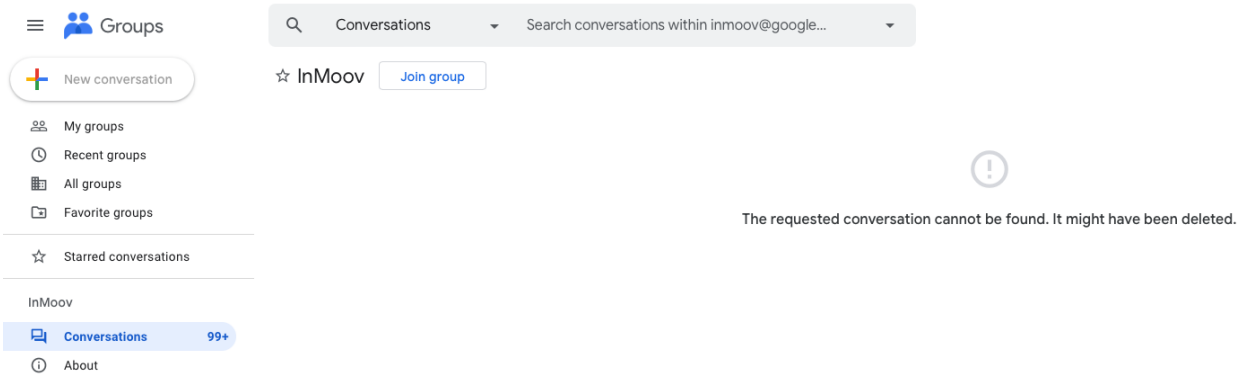
In conclusion, the rise in abuse and malicious activities on Google Groups and Usenet is a cause for concern. As these platforms continue to evolve, it is imperative to address these issues to ensure a safe and secure online environment. By harnessing the power of technology and promoting responsible participation, we can combat abuse and foster a thriving community within online discussion forums.

References

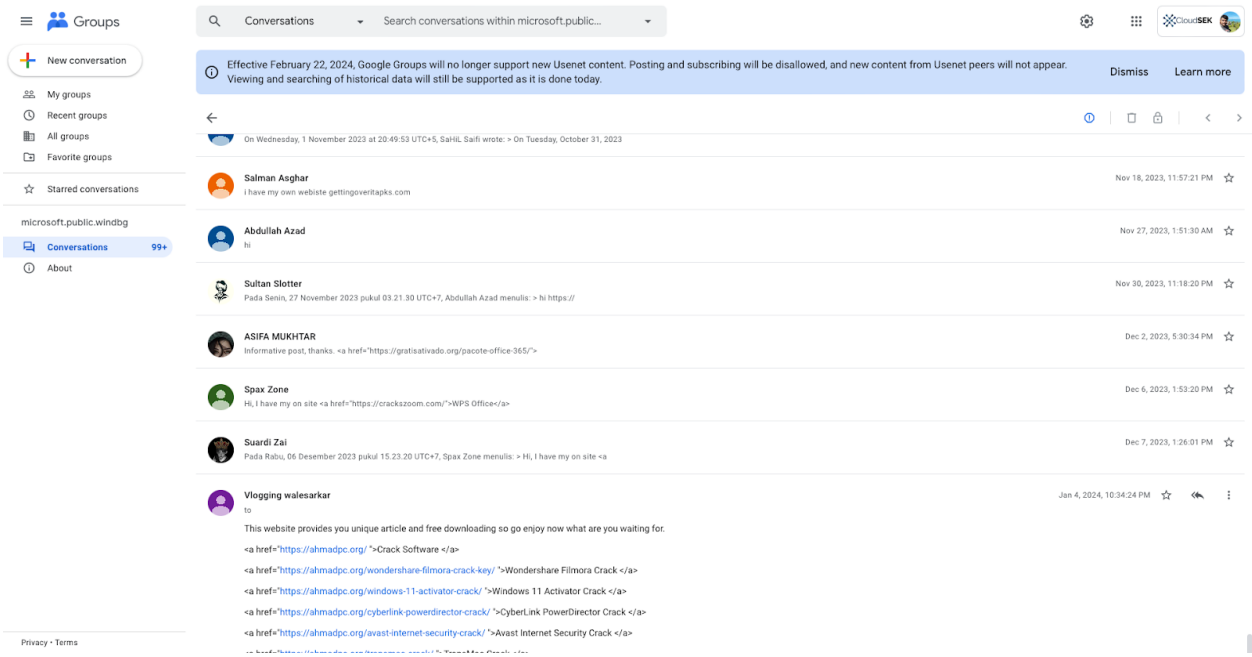
Appendix



https://groups.google.com/g/pocketcode - Banned content due to google's content filtering.



https://groups.google.com/g/inmoov/c/khPrj358HIY - Removed content, Group admin monitoring and keeping Group clean



Latest message from the group - Malicious link to ahmadpc[.]org a known malicious site