ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 09/05/2024 by

What is Account Harvesting?

09/05/2024 13:50

In today's digital world, online security is a primary concern for individuals and businesses. One of the most significant threats is account harvesting, also known as credential or password harvesting.

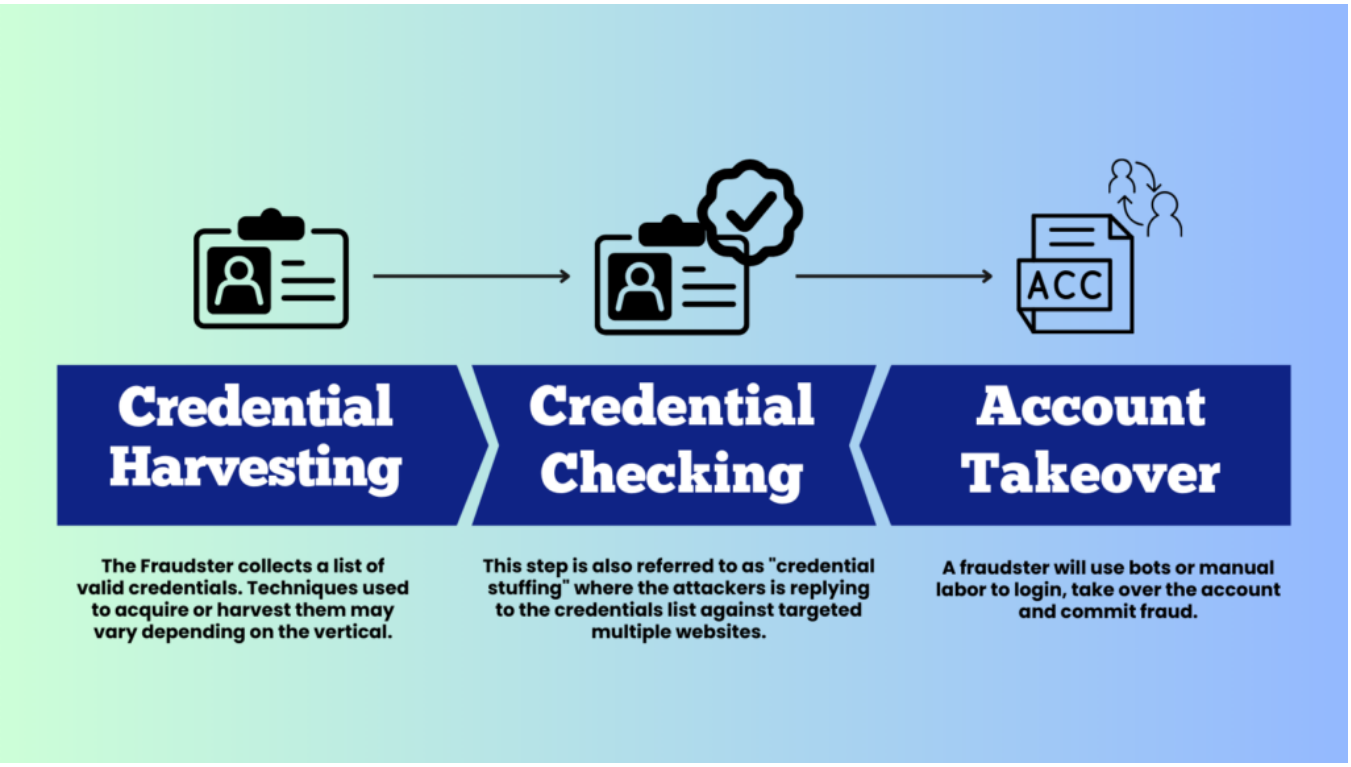
This illegal practice involves collecting sensitive information from unsuspecting victims, such as usernames and passwords. In this article, we will explore account harvesting, how it works, its impact, notable cases, and ways to protect against it.

Basics of Account Harvesting

Account harvesting is a malicious activity where attackers collect login details for various online accounts without authorization. The stolen information can be used for identity theft, financial fraud, and unauthorized personal or business data access.

Attackers use phishing scams, malware, and social engineering to trick people into revealing their

account details. This can happen through fake websites, deceptive emails, or exploiting software vulnerabilities.



What is Account Harvesting?

Common Methods Used

- **Phishing Scams**: Attackers send fake emails or messages that look like they come from trusted sources, such as banks or online services. These messages often contain links to bogus websites that mimic real ones. When users enter their login details, attackers capture the information.
- **Malware**: Malicious software can be installed on a victim's device without knowledge. This software can record keystrokes, capture screenshots, or monitor network traffic to gather login credentials.
- **Social Engineering**: Attackers use psychological tricks to manipulate individuals into revealing their account details. They might impersonate trusted individuals or use persuasive tactics to gain trust.

The Evolution of Account Harvesting

Account harvesting is not new, but it has evolved with technology. In the past, attackers used methods like shoulder surfing (watching someone enter their login details) or dumpster diving

(searching through trash for sensitive information).

With the internet's growth, attackers now have more sophisticated tools to target more people and organizations.

Over the years, several high-profile incidents have highlighted the dangers of account harvesting.

For example, in 2013, hackers infiltrated a central social media platform, compromising millions of users' login details. This incident led to financial losses and exposed sensitive personal information, such as private messages and photos.

How Account Harvesting Works

Account harvesting involves several steps designed to exploit vulnerabilities and acquire login credentials. Attackers first identify potential targets, often through data breaches, social media mining, or purchasing information on the dark web.

Techniques Employed

They then use phishing emails, fake websites, or malware to trick victims into revealing their account information. Once obtained, the attackers may use the credentials for malicious purposes

or sell them on the dark web.

Techniques Employed

- **Phishing**: Sending deceptive emails or messages to trick users into clicking on malicious links or providing their credentials.
- **Malware**: Using software like keyloggers or credential-stealing Trojans to capture login details without the user's knowledge.
- **Social Engineering**: Employing psychological tactics to convince individuals to disclose their account information willingly.
- **Password Guessing**: Using automated tools to guess weak passwords and gain unauthorized access.

The Impact of Account Harvesting

Effects on Individuals:

- Account harvesting can lead to severe consequences for individuals, such as identity theft, financial loss, and reputational damage.
- If a compromised account is linked to other services, like email or social media, the effects can be widespread, impacting various aspects of an individual's digital life.

Effects on Businesses:

- The impact on businesses can be equally devastating. Breached accounts can expose sensitive corporate information, customer data, or financial records, leading to financial loss, legal issues, and reputational damage.
- Such incidents often result in a loss of customer trust, which is critical in today's competitive market.

Several notable account harvesting incidents have made headlines and served as cautionary tales. For instance, a large social media platform once fell victim to a sophisticated phishing attack.

Attackers sent convincing emails that looked like official notifications, prompting users to click on a malicious link and enter their credentials. Thousands of accounts were compromised, resulting in reputational damage and a loss of user confidence.

Lessons Learned

Past incidents have taught valuable lessons for both individuals and businesses:

- **Be Wary of Unsolicited Communications**: Exercise caution when responding to emails or

messages, especially those requesting personal information.
- **Use Strong, Unique Passwords**: Choose complex passwords and avoid reusing them across multiple accounts.
- **Enable Multi-Factor Authentication**: Add an extra layer of security by requiring additional verification beyond a username and password.
- **Monitor Account Activity Regularly**: Quickly identify and address any suspicious activity.

Protecting Yourself from Account Harvesting

To protect against account harvesting, adopt these best practices:

- **Keep Software and Devices Updated**: Regularly update software and devices with the latest security patches to protect against vulnerabilities.
- **Use Reputable Security Software**: Utilize trusted antivirus and antimalware solutions to detect and prevent attacks.
- **Stay Informed About Threats**: Be aware of the latest phishing techniques and malware trends to recognize and avoid risks.
- **Educate Yourself and Others**: Educate yourself, friends, family, and colleagues about the risks and preventive measures for account harvesting.

Tools and Resources

Many tools and resources can help protect against account harvesting. Password managers generate and securely store unique passwords, while cybersecurity awareness training programs educate individuals and businesses about the latest threats and prevention techniques.

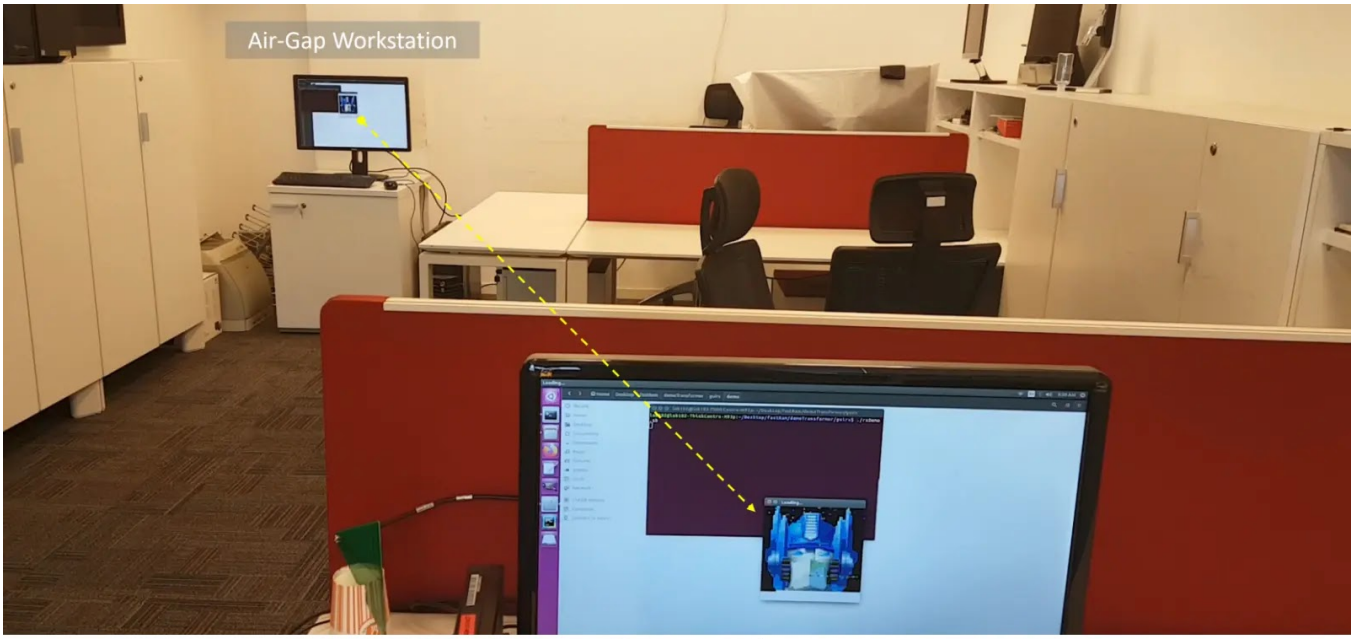
Investing in these resources can significantly enhance account security. Account harvesting is a significant threat in today's digital landscape, with the potential to cause immense damage and disruption.

Individuals and businesses can better protect themselves by understanding account harvesting, recognizing the techniques used, and implementing robust security measures.

Vigilance, education, and preventive strategies are crucial for creating a safer online environment for everyone.

RAMBO Attack Steals Data From Air-gapped Systems

09/05/2024 14:40

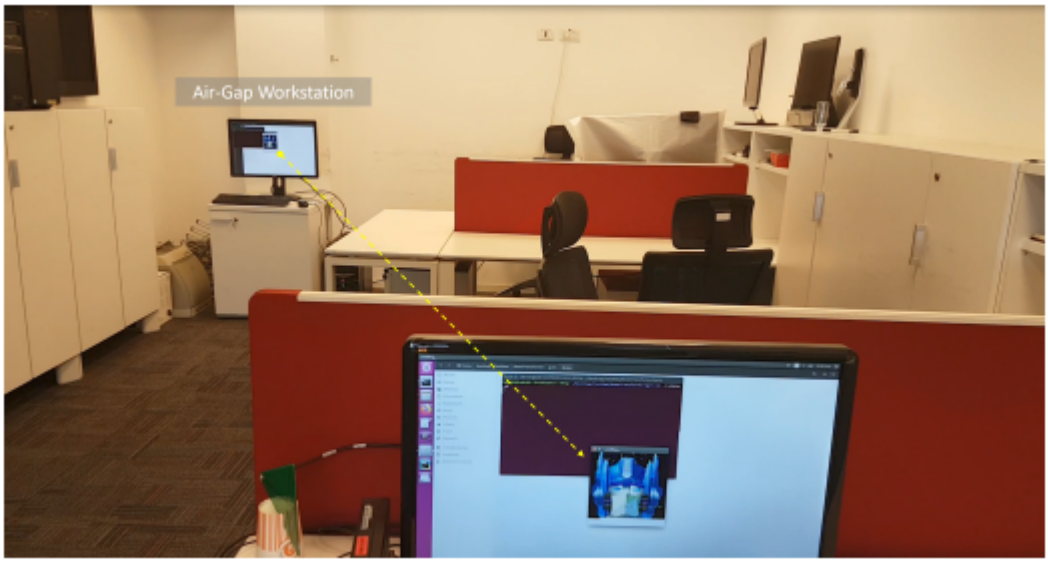


RAMBO Attack Steals Data From Air-gapped Systems

Researchers explore the vulnerability of air-gapped networks to malicious attacks. Despite their physical isolation, these networks can be compromised through covert channels, such as electromagnetic emissions.

The attack model involves malware manipulating RAM to generate radio signals that can be encoded with sensitive information and exfiltrated from a distance. It presents the design and implementation of a transmitter and receiver capable of transmitting and receiving these signals.

Experimental results demonstrate the feasibility of the attack, highlighting the need for robust countermeasures to protect air-gapped networks from such threats.



Attack demonstration

The study presents a novel covert channel based on electromagnetic emissions from the RAM bus. The transmitter modulates memory access patterns to encode data, which is then demodulated by the receiver.

Utilizing Manchester encoding for faster transmission ensures clock synchronization and error detection, which increases bandwidth requirements.

The transmitter employs the MOVNTI instruction to maintain RAM bus activity and uses a preamble sequence for synchronization. The demodulator frames the received data based on an alternating bit sequence.

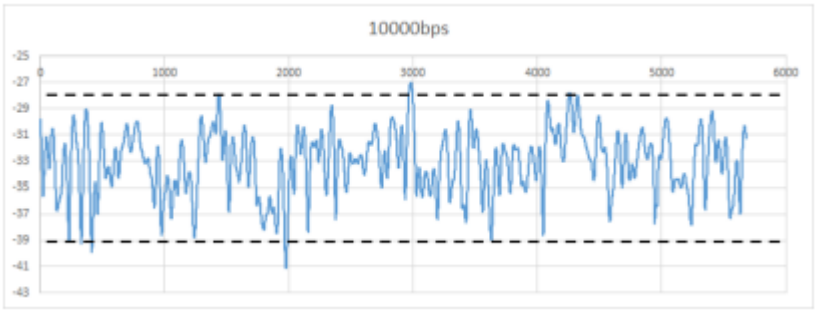
A comparison between Manchester encoding and OOK modulation concluded that Manchester encoding is more suitable for this covert channel due to its synchronization and error detection benefits.

. Ettus B210 Universal Software Radio Peripheral (USRP)

The evaluation of the RAMBO covert channel demonstrates its effectiveness in exfiltrating data through electromagnetic emissions from DDR RAM. Despite varying distances and bit rates, the channel maintained a high signal-to-noise ratio and low bit error rates.

Low SNR levels limited high-speed transmissions. Faraday shielding and virtualization were shown to be effective countermeasures, but they are not widely deployable.

The DDR RAM clock frequency influences the covert channel's frequency range and can be affected by spread spectrum clocking. Overall, the RAMBO covert channel presents a significant security risk, requiring careful consideration of countermeasures.



The transmission with 10000 bps.

Several countermeasures can be employed to mitigate the RAMBO attack. Physical separation using zone restrictions and Faraday enclosures can prevent information leakage.

Host-based intrusion detection systems and hypervisor-level monitoring can detect suspicious memory access patterns. External spectrum analyzers and radio jammers can identify and disrupt covert radio transmissions.

Internal memory jamming can interfere with the covert channel and may also impact legitimate operations. While these countermeasures offer varying levels of protection, a combination of approaches is often necessary to effectively defend against the RAMBO attack.

The paper demonstrated a novel air gap covert channel attack that exploits memory operations in isolated computers to exfiltrate sensitive data. By manipulating memory-related instructions, attackers can encode and modulate information on electromagnetic waves emitted from the memory buses.

A nearby receiver equipped with a software-defined radio can then intercept, demodulate, and decode the transmitted data, which enables attackers to leak various types of information, including keystrokes, files, images, and biometric data, at a rate of hundreds of bits per second.

We Hunted Hidden Police Signals at the DNC

09/05/2024 10:30