NEWSLETTER

RJ2 Technologies Monthly Newsletter
November 2024

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

(847) 380-1194

www.rj2t.com

In this newsletter:

Unmasking Fileless Malware: How Hackers Attack Without a Trace

The techniques cybercriminals use to hack into systems are not any simpler. Today, there's a glut of malware types that don't rely on traditional methods for infiltration. Fileless malware, in particular, is an incredibly elusive and dangerous threat that can bypass even the most sophisticated security measures.

What is Fileless Malware?

Fileless malware is a type of malicious program that operates without using executable files to infect a computer like how traditional malware does. Instead, it operates within the system's memory (RAM) or uses legitimate programs already running on your machine to covertly infect your systems.

The initial exploit, or intrusion point, can vary, but the most common method used by cybercriminals is through phishing emails containing malicious links or attachments. Once clicked or opened, the malware will execute its code and spread quickly by escalating its privileges and exploiting vulnerabilities in the operating system or applications. It typically leverages built-in system tools such as PowerShell and WMI (Windows Management Instrumentation) to carry out its malicious activities without ever leaving a single file or detectable footprint on the hard drive.

Although fileless malware doesn’t install itself permanently on a system, it can establish a persistent foothold by modifying system configurations or scheduling tasks to run malicious scripts every time the system boots up. Its ability to adapt and mimic legitimate processes means it can avoid detection for longer periods, leading to greater damage over time.

How to Mitigate Fileless Malware Threats

To protect against fileless malware, businesses need to take a proactive approach and implement multiple layers of security measures. Here are key strategies for mitigating the risk of fileless malware attacks:

Implement advanced endpoint protection
Rather than relying solely on basic antivirus software, which may not detect fileless threats, it's crucial to deploy advanced endpoint protection solutions that can monitor system behavior. These tools can identify suspicious activity in real time, even if no files are involved, by recognizing patterns of abnormal memory usage or unexpected behaviors in trusted programs.

Utilize application whitelisting
Application whitelisting is the practice of allowing only approved programs to run on a system. It can be accessed through the operating system's security settings or through third-party software, where you can determine which applications and scripts are allowed to run based on their digital signatures, publisher, or file paths. By implementing a strict whitelist, businesses can prevent unauthorized programs from running and stop fileless malware in its tracks.

Regularly update software
Exploiting software vulnerabilities is a common entry point for fileless malware. To prevent this, it's critical to ensure that all your software, operating systems, and third-party applications are up to date with the latest patches. Regular patching closes known vulnerabilities that attackers could use to compromise your system.

Train employees on phishing awareness
Many fileless malware attacks begin with a phishing email that tricks the user into clicking a malicious link or opening an infected document. Providing regular cybersecurity training to your employees on how to recognize phishing attempts, suspicious links, and unexpected attachments can significantly reduce the chances of malware gaining initial access to your network.

Segment networks
If a fileless malware attack successfully infiltrates one part of your network, segmentation can contain the threat, prevent it from spreading, and reduce the overall impact of fileless malware. To segment your network, you can create separate subnets or VLANs and implement strict access control policies that prevent unauthorized communication between different parts of the network.

Monitor and analyze network traffic
Network traffic monitoring can identify anomalies or unusual communication patterns that might indicate a fileless malware infection. For instance, if a system suddenly starts communicating with unknown or suspicious IP addresses, it could be a sign of malware activity. Early detection of any unusual network behavior can help organizations respond quickly and mitigate potential damage.

Fileless malware is incredibly sophisticated, and your technical expertise must match its stealthy and evasive nature. If you don't have cybersecurity experts on your team, working with a managed IT services provider like us, RJ2 Technologies, can help you implement the necessary security measures and continuously monitor your systems for any signs of fileless malware. **Contact us today at marketing@rj2t.com or 847-303-1194** to protect your business from this growing threat.

Enjoying Getting the Most Recent IT News from RJ2 Technologies?

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532

6 Shopping Scams and How to Avoid Them

It's November, which means the biggest online shopping day of the YEAR is just weeks away: Cyber Monday, occuring on Monday, December 2nd, 2024. Unfortunately, it's also open season for cybercriminals. Because preparation is the best prevention, we're covering the six most common shopping scams this time of year and how to avoid them.

It's Open Season For Shopping Scams

Thanks to cybercriminals, what should be a season of festive shopping is now dangerous for consumers. According to the Federal Trade Commission, shopping scams were the second-worst type of scam in the US in 2023. And online scams are at their worst during the holidays. According to TransUnion's 2022 Global Digital Fraud Trends report, there was a 127% increase in daily fraud attempts between November 24 and 28 compared to January 1 through November 23.

Due to the high volume of shopping activity during the holiday season, cybercriminals don't have to work hard to find potential victims. But it's not simply volume that contributes to the rise in attacks; consumers take more risks during the holiday season. According to Norton's 2022 Cyber Safety Insights Report, nearly one in three adults (32%) worldwide admitted to taking more risks with online shopping closer to the holidays. Last-minute shopping pressure or excitement around scoring big deals results in common mistakes, including clicking on unverified links, using public WiFi for transactions and ignoring website security red flags.

Cybercriminals expect shoppers to make mistakes, and they have tried-and-true tactics for stealing your money. During this time of year, everyone should be extra cautious with their online purchases to protect themselves from cybercrime. Watch out for the six scams on the following page that appear this time of year, and protect yourself this holiday season.

GADGET OF THE MONTH

Portable Charger Power Bank

The Portable Charger Power Bank 40000mAh is a powerful solution for travelers who need reliable, fast charging on the go. Its 30W PD and QC 4.0 quick-charging capabilities can charge an iPhone 13 from 20% to 80% in just 30 minutes! Charging three devices simultaneously through its Type-C and dual USB ports is ideal for multitasking professionals. Its large 40000mAh capacity ensures a week's worth of power, eliminating battery anxiety during travel. The built-in LED display and practical bright flashlight bonus feature make this power bank a dependable tool for every traveler.

6 Common Scams During Black Friday And Cyber Monday And How to Avoid Them

1. Fake Coupons: Scammers distribute fake coupons promising steep discounts. These coupons are often shared via e-mail, social media and fake websites designed to mimic legitimate retailers. Remember: if it feels too good to be true, it probably is.
How to avoid: Always verify a coupon by checking the retailer's official website or app, and avoid clicking on links in unsolicited e-mails.

2. Phony Websites: To steal personal information, fake websites mimic legitimate online stores using similar logos, branding and URLs that are only slightly different from the official sites.
How to avoid: Check for secure website indicators such as HTTPS and a padlock icon in the address bar. Read reviews and quickly search the website's legitimacy before making any purchases. Pay attention to the URL for any unusual characters or misspellings.

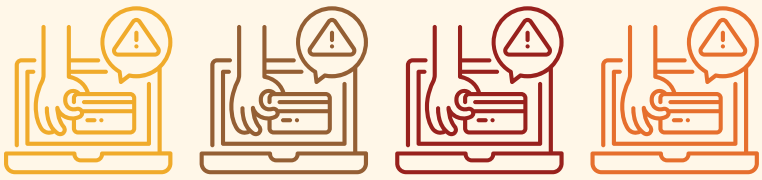
3. Fake Delivery And Nondelivery Scams: Scammers send fake delivery notifications or claim a package is undeliverable to trick you into providing personal information.
How to avoid: Track orders directly through the retailer's website or app. Avoid clicking on links in suspicious messages, and be cautious of unsolicited delivery notifications.

4. Fake "Order Issue" Scams: E-mails claiming a problem with your order and asking for personal details are common. These messages often look like they come from well-known retailers.
How to avoid: Contact customer service directly through the retailer's official channels to verify any issues, and avoid providing personal details through links in unsolicited messages.

5. Account Verification Scams: Scammers send e-mails or texts asking you to verify your account information. These messages often include links to fake login pages.
How to avoid: Never provide personal details through links in unsolicited messages; instead, log in directly to your account through the official website.

6. Gift Card Scams: Scammers offer discounted gift cards or request payment via gift cards. Once the card numbers are provided, the scammer uses the balance, leaving the victim with a worthless card.
How to avoid: Purchase gift cards directly from reputable retailers and never use them as a form of payment to unknown individuals.

Avoid Scams and Create a Safer Shopping Experience



Nothing will kill the holiday shopping spirit like $1,000 worth of fraudulent charges on your credit card or gifts from phony sites that never arrive. Cybercriminals take advantage of the festive shopping rush, and consumers' tendency to take more risks during this time only amplifies the danger. By verifying sources, checking website security and avoiding unsolicited links, you can enjoy a safer shopping experience this season!

If you would like to learn more about other techniques cyber criminals use to hack into your company's important data, **contact RJ2 Technologies at 847-303-1194** to protect your data.

Vendor Partner Highlight -

Duo Security, a partner of Cisco since 2018, is a user-friendly zero trust security solution that safeguards data, devices, and applications for teams of all sizes. This platform specializes in multi-factor authentication (MFA) and zero-trust security making it easier for companies to adopt best cybersecurity practices. Some of their products include features like adaptive access policies, device health checks, and phishing-resistant authentication. Duo aims to protect organizations against data breaches by verifying only legitimate users and appropriate devices have access to sensitive data and applications.

RJ2 Technologies partners with Duo to offer more secure access to your business applications with MFA and single sign-on (SSO). By adding this extra layer of protection against unauthorized access, this complements our managed IT services as our goal is to help companies have robust, scalable security measures in place to protect important data, business devices, and other applications. To learn more about this partnership, **call RJ2 Technologies at 847-303-1194.**

Tech Gifts to Avoid Buying

While a playful robot that uses facial recognition to analyze a child's moods might seem like an awesome gift for your nephew, it's not so great when you learn that data can be hacked by cybercriminals or shared for third-party advertising. At the 2023 CES electronics exhibition, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, told the Washington Post that most tech companies address safety problems when they happen rather than developing safety features proactively. Companies are "really focused on cost, capability, performance and speed to market, not on basic safety," she said.

No matter how well they promise to clean your floors or entertain your children, some tech products are not worth the security risks. Here are a few tech gifts to avoid and tips for wiser tech shopping.

Beware These Tech Gifts

Camera-Enabled Devices With Bad Privacy Policies
Doorbell cams have one purpose: to see and hear everything around your home and neighborhood. Then it sends that data to the cloud. Poorly secured cameras could allow hackers to access live feeds, potentially giving them insight into when you're home and when you're away. Always choose devices with end-to-end encryption and transparent privacy policies.

Genetic Testing Kits
In 2023, nearly 7 million 23andMe users had their ancestry data hacked – a stark reminder of the risks of genetic testing. Criminals are drawn to this highly sensitive data, and companies like Veritas and Ancestry.com have also faced breaches. Beyond theft, there's the issue of law enforcement's ability to access this information. Remember, once you spit into a test tube, you give away your genetic information, that of your close relatives and even future generations.

AI-Integrated Devices
In 2022, images from iRobot's AI-enabled Roomba were leaked online. Although the company claimed test users consented to share data, it underscores the risk of AI devices collecting extensive information about you. Read the privacy policy closely. If you can't customize data settings or companies aren't clear about how they use your data, shop elsewhere.

Tracking Devices For Kids
Tracking devices for children might seem like a thoughtful gift for families, but these devices can expose children's real-time location to hackers, stalkers or third parties. In 2021, the popular family safety app Life360 was found to be selling user location data to data brokers, according to reporting by The Markup. A safer approach is to discuss location sharing openly with your kids and use built-in features like Google's Family Link or Apple's end-to-end encrypted location sharing.