Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 5-JULY-2024, 2:00 IST

Title	**AdsExhaust: New Adware Masquerading as Oculus Installer Wreaks Havoc**
Summary	• Hackers often attack the users who are searching for the Meta Quest app is due to they tend to be willing to install and download it as soon as possible, which exposes them to downloading harmful versions. • This group has discovered significant attacks, including the Kaseya MSP breach and the more_eggs malware. • The TRU Positives reports are issued by the TRU team that share synopses of recent threat investigations revealing new cyber security challenges. • In June of 2024, the eSentire Threat Response Unit detected AdsExhaust, an adware disguised as an installation software for Oculus. • This malicious software steals screenshots from internet users and manipulates their browsing activity to generate income through advertising.
Severity	Medium
Attack Vectors	• The Infection chain starts with downloading a ZIP file that contains batch scripts that fetch additional malicious components and establish scheduled tasks for persistence. • A PowerShell script iterates, getting system details, taking screenshots, and transferring information to a C2 server. • The well-developed persistence techniques and data exporting capacities of the adware underscore the dynamic nature of unthreatening downloads of common programs. • AdsExhaust adware is created using a malicious PowerShell payload that utilizes a mutex to make sure only one instance of the malware runs and it targets Microsoft Edge. • In its idle state, it simulates user interaction with ads by injecting clicks, opening tabs, and navigating to embedded URLs. This adware takes screenshots and overlays them in order to hide itself. • Once open ads are detected, they interact with "Sponsored" content on the pages to generate false revenue from advertising. Additionally, AdsExhaust uses Google searches to fetch keywords from a remote server. • This highly advanced adware deploys diverse methodologies like C2 communication, keystroke simulation, and screen manipulation to evade detection while making unauthorized money via artificial ad engagement.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	Hashes	• 04c74048c5be59ceb2e35d5538b72f3328a268953dfbe1f287285f1dbb7e1dfa • 1818a0062898b94dfccada9127d7d6af44bf663cb298759bef4447c43798e082 • 30b32288db0cde0156fe1e43db15b87ee71d14f2e9610180f27886e1ef20f9f1 • 351fa3e33d607ff77548ba6422ac0a5264fb3e847e65996d3ef4faefc2a738c5 • 52c81cc2729ee702ed3803bbb94213a42fe4632f61abd4300ba8157f512be1df • 6cba1871dcf173af8c031a543b4ac561 • 70364ea952ea4e7d60bbe0e87f288528f22e2f780179ac36ee101e1b335ea622 • 79e8beff1589349e078b88496c469a84ccaeb00e176bdf39dc14811bb4c1a8c7 • 7c97c864aceff6ad7df548882a57165655c72f682313f3c59c5d8be37cea24fc • 84af73ad559d67741eeba4b7b0b286a223bb5137d8edae11673d37a4c068c62e • 95133896517b80620f4c81af332d258da5b7d50413b30eac1cf3808e511210a1 • 962024ea6f85ca97adbd7ec55686579185f1cb5ce7dd7e722edd2a91d6872e91 • ef2666d085fc1d8897b58935637c308e • f089c37110f17041640910b0d49bfc5a • f2f850b85a72fa3bbf7ca45cd29e25439f04ba1955bc404ca0a4311b54395f61
	URLs	• http[:]//oculus-app.com • http[:]//us11.org/in.php • http[:]//us5.co/downloading.php • http[:]//us99.org/keywords.txt • https[:]//life2vec.io/ • https[:]//life2vec.io/ai-predicting-business-risks/ • https[:]//life2vec.io/auto-insurance-guide/ • https[:]//life2vec.io/benefits-life-insurance-beyond-death-benefit/ • https[:]//life2vec.io/best-accidental-insurance-america/

		• https[:]//life2vec.io/best-insurance-self-driving-cars/ • https[:]//life2vec.io/business-insurance-myths/ • https[:]//life2vec.io/business-owners-policy-bop-small-businesses/ • https[:]//life2vec.io/cash-value-component-whole-life-insurance/ • https[:]//life2vec.io/choose-right-business-attorney-startup/ • https[:]//life2vec.io/cost-of-pet-insurance-is-it-worth-it/ • https[:]//life2vec.io/dental-insurance-guide/ • https[:]//life2vec.io/disability-insurance-essential-working-adult/ • https[:]//life2vec.io/emerging-trends-in-small-business-insurance/ • https[:]//life2vec.io/general-liability-insurance-guide/ • https[:]//life2vec.io/getting-a-car-accident-insurance-claim-online/ • https[:]//life2vec.io/guide-individual-and-family-health-insurance-plans/ • https[:]//life2vec.io/health-insurance/ • https[:]//life2vec.io/home-owners-insurance-guide/ • https[:]//life2vec.io/houston-maritime-attorney/ • https[:]//life2vec.io/impact-autonomous-vehicles-auto-insurance/ • https[:]//life2vec.io/innovation-rising-need-business-insurance/ • https[:]//life2vec.io/intellectual-property-protection/ • https[:]//life2vec.io/life2vec-ai-death-calculator/ • https[:]//life2vec.io/life-insurance-different-life-stages/ • https[:]//life2vec.io/life-insurance-estate-planning/ • https[:]//life2vec.io/life-insurance-for-small-business-owners/ • https[:]//life2vec.io/maximize-dental-insurance-benefits/ • https[:]//life2vec.io/mistakes-term-life-insurance/ • https[:]//life2vec.io/professional-liability-insurance-life2vec-io/ • https[:]//life2vec.io/professional-liability-insurance-save-business/ • https[:]//life2vec.io/reduce-workers-compensation-insurance-costs-tips/ • https[:]//life2vec.io/renters-insurance-vs-homeowners-insurance-key-differences/ • https[:]//life2vec.io/retirement-planning-in-the-usa-life2vec-io/ • https[:]//life2vec.io/selecting-a-maritime-attorney-in-houston/ • https[:]//life2vec.io/selecting-the-right-life-insurance-policy-a-guide/ • https[:]//life2vec.io/small-business-insurance-guide/ • https[:]//life2vec.io/tax-benefits-whole-life-insurance/ • https[:]//life2vec.io/technology-modern-workers-compensation-insurance/ • https[:]//life2vec.io/telematics-usage-based-insurance-auto/ • https[:]//life2vec.io/term-life-insurance-in-the-usa/ • https[:]//life2vec.io/term-life-insurance-vs-life-insurance-policy/ • https[:]//life2vec.io/top-10-car-accident-attorneys-in-the-usa/ • https[:]//life2vec.io/top-10-dental-insurance-plans-2024/ • https[:]//life2vec.io/top-10-houston-maritime-attorneys-leading-the-way-in-maritime-law/ • https[:]//life2vec.io/top-10-loan-lenders-in-the-usa-life2vec-io/ • https[:]//life2vec.io/top-10-renters-insurance-providers/ • https[:]//life2vec.io/top-10-term-insurance-plans-usa/ • https[:]//life2vec.io/top-10-truck-accident-attorneys-in-the-usa/ • https[:]//life2vec.io/top-20-accident-attorneys-usa/ • https[:]//life2vec.io/top-7-insurance-providers-in-the-usa/ • https[:]//life2vec.io/top-workers-compensation-insurance-policies/ • https[:]//life2vec.io/travel-insurance-guide/ • https[:]//life2vec.io/truck-accidents-hiring-the-right-attorney/ • https[:]//life2vec.io/types-of-insurance/ • https[:]//life2vec.io/understanding-life-insurance-policies-offer-returns/ • https[:]//life2vec.io/whole-life-insurance-for-high-net-worth-individuals/ • https[:]//life2vec.io/workers-compensation-insurance-protecting-your-workforce-life2vec-io/

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Never trust or open links and attachments received from unknown sources/senders. • Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. • Deploy EDR solutions on all devices. • Confirm that all devices are protected with Endpoint Detection and Response (EDR) solutions. • Implement a Phishing and Security Awareness Training (PSAT) Program that educates and informs your employees on emerging threats in the threat landscape. • We recommend modifying the default 'open-with' settings for script files, ensuring they open with a basic text editor like Notepad instead of executing. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**
References	• https://cybersecuritynews.com/dware-meta-quest/ • https://www.esentire.com/blog/adsexhaust-a-newly-discovered-adware-masquerading-oculus-installer