

Deadline: 2023-10-24



STORM ⚡ WATCH

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

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://arstechnica.com/security/2023/10/two-ransomware-gangs-knocked-out-of-commission-in-a-single-week/>



**ars** TECHNICA

*BUH-BYE —*

## Feel-good story of the week: Two ransomware gangs meet their demise

One is fatally hacked, the other shut down in international police dragnet.

DAN GOODIN - 10/20/2023, 7:09 PM



GR  
LA

ATCH



Ukrainian Cyber Alliance

<https://www.facebook.com/ruheight/posts/pfbid02nuzurXMLoZEU9qM7kEG3oxECm7aS2Yahi6d5UEAqUPmhZSJRFauqRybTa84Kj9d81>

## Trigona is Gone!

**The servers of the Trigona ransomware gang has been exfiltrated and wiped out**

**Welcome to the world you created for others**

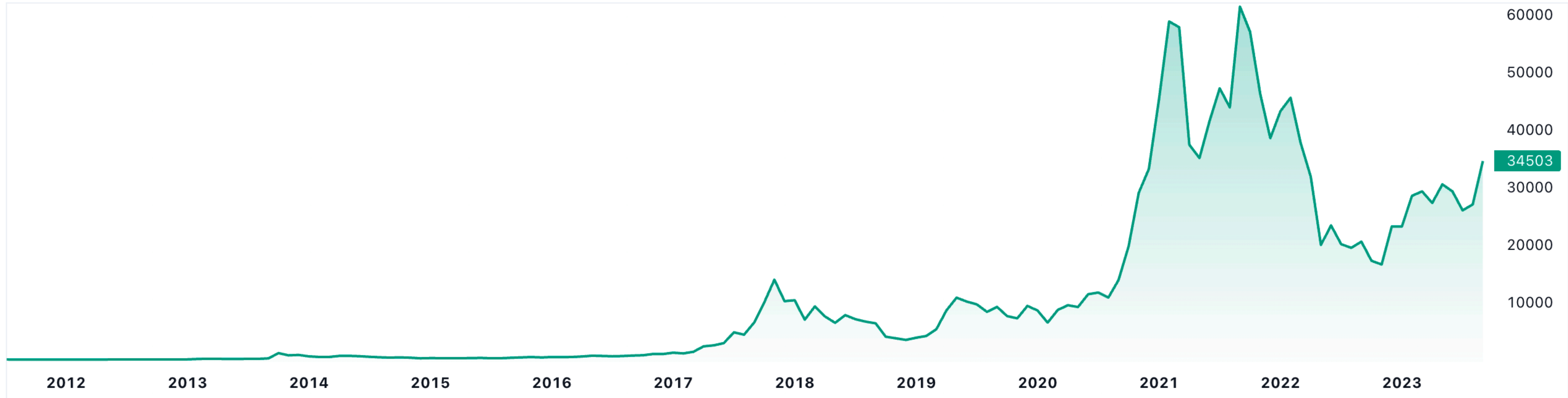
Hacked by  
**Ukrainian Cyber Alliance,**  
disrupting russian criminal enterprises (both public and private)  
since 2014



**This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group**



Guest published on TradingView.com, Oct 24, 2023 11:51 UTC



TradingView

# HOW IT STARTED

CTX579459

## NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967

Security Bulletin | Severity: Critical | 79 found this helpful | Created: 10 Oct 2023 | Modified: 23 Oct 2023 | Status: Final

Applicable Products

Citrix ADC

Description of Vulnerability

Multiple vulnerabilities in NetScaler Gateway (formerly NetScaler Gateway) affect the following supported versions:

Affected Versions

The following supported versions are affected:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

Note: NetScaler Gateway is affected by CVE-2023-4967. For more information, see <https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967>.

This bulletin only applies to on-premises NetScaler Gateway. Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

# HOW IT'S GOING

October 23, 2023 by Anil Shetty

net>scaler.

We now have reports of incidents consistent with session hijacking, and have received credible reports of targeted attacks exploiting this vulnerability.

NetScaler ADC and NetScaler Gateway. If exploited, CVE-2023-4966 can result in unauthorized data disclosure. This vulnerability was discovered by our internal team, and at the time of disclosure, we were not aware of any exploits in the wild.

We now have reports of incidents consistent with session hijacking, and have received credible reports of targeted attacks exploiting this vulnerability.

You can find details in the [security bulletin](#).

server, immediately

Here we saw an interesting example of a vulnerability caused by not fully understanding `snprintf`. Even though `snprintf` is recommended as the secure version of `sprintf` it is still important to be careful. A buffer overflow was avoided by using `snprintf` but the subsequent buffer over-read was still an issue.

<https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966>

<https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-4966>



## GREYNOISE TRENDS

CITRIX ADC NETSCALER CVE-  
2023-4966 INFORMATION  
DISCLOSURE ATTEMPT

## TAG INTENT

Malicious

## TAG CATEGORY

Activity

IP addresses with this tag have been observed attempting to exploit CVE-2023-4966, an unauthenticated information disclosure vulnerability in Citrix ADC & NetScaler

> MALICIOUS ISP

152.165.126.141

ORGANIZATION: Sony Network Communications Inc. ACTOR: unknown LAST SEEN: 2023-10-24

SOURCE: Japan DESTINATION: Mexico, Japan, Hong Kong, Finland, India + 22 More

CITRIX ADC NETSCALER CVE-2023-4966 INFORMATION DISCLOSURE ATTEMPT TLS/SSL CRAWLER

WEB CRAWLER

> MALICIOUS HOSTING

64.176.224.56

ORGANIZATION: The Constant Company, LLC ACTOR: unknown LAST SEEN: 2023-10-19

SOURCE: South Korea DESTINATION: France, Germany, Indonesia, China, Canada + 8 More

CITRIX ADC NETSCALER CVE-2023-4966 INFORMATION DISCLOSURE ATTEMPT TLS/SSL CRAWLER

WEB CRAWLER

71.169.48.51

ORGANIZATION: Verizon Business ACTOR: unknown LAST SEEN: 2023-10-19

SOURCE: United States DESTINATION: Poland, Australia, Ghana, India, Israel + 27 More

CITRIX ADC NETSCALER CVE-2023-4966 INFORMATION DISCLOSURE ATTEMPT TLS/SSL CRAWLER

WEB CRAWLER

## CVES:

CVE-2023-4966

CVE-2023-4967



GREYNOISE  
LABS

<https://viz.greynoise.io/query?gnql=tags:'Citrix ADC Netscaler CVE-2023-4966 Information Disclosure Attempt'>

Detected by Snort IDS rule ID 3:50118:2

Proof-of-Concept Known

On October 18th, 2023, PoC remote code execution was demonstrated by VulnCheck in collaboration with GreyNoise. Due to a lack of available public details on the specifics of patches and bypasses, an accurate determination for the related CVE identifier cannot be made. From our best determination, the identified vulnerability is one or multiple of the CVE-2019-XXXXXX vulnerabilities.

**CVE-2019-1862**  
Cisco IOS XE Software Web UI  
Command Injection Vulnerability

**CVE-2019-12650**  
Cisco IOS XE Software Web UI  
Command Injection Vulnerability

**CVE-2019-12651**  
Cisco IOS XE Software Web UI  
Command Injection Vulnerability

**CVE-2021-1435**  
Cisco IOS XE Software Web UI  
Command Injection Vulnerability

**CVE-2023-20273**  
"The attacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to root and write the implant to the file system."

**CVE-2023-20198**  
Cisco IOS XE Software Web UI  
Privilege Escalation Vulnerability

**CVE-????-?????**  
"We have also seen devices fully patched against CVE-2021-1435 getting the implant successfully installed through an as of yet undetermined mechanism."

is now

May 13th, 2019

September 25th, 2019

March 24th, 2021

October 16th, 2023

<https://vulncheck.com/blog/cisco-implants>

<https://censys.com/cve-2023-20198-cisco-ios-xe-zero-day/>

<https://www.greynoise.io/blog/unpacking-cve-2023-20198-a-critical-weakness-in-cisco-ios-xe>





Blog

October 18, 2023

# Qubitstrike - An Emerging Malware Campaign Targeting Jupyter Notebooks

First reported case of Codeberg code hosting platform used to distribute malware

Attackers continue trend of leveraging Discord for Command and Control

Qubitstrike attackers specifically seeking Cloud Service Provider credentials

Cado researchers observed attempts by the attackers to utilize stolen CSP credentials for further exploitation

Jupyter Notebooks exploited for initial access but the malware also supports SSH propagation

October 20, 2020

# Tracking Okta's S...



David Br...

Okta Security has identified  
Okta's support case m...

- Open in Sources panel
- Open in new tab

---

- Clear browser cache
- Clear browser cookies

---

- Copy >

---

- Block request URL
- Block request domain

---

- Sort By >
- Header Options >

---

- Override headers
- Override content
- Show all overrides

---

- Save all as HAR with content**
- Save as...

essential to access





Filter by HTTP status codes.

Group by pages

All entries

[Learn More](#)

- 0       1xx
- 2xx     3xx
- 4xx     5xx



Terms to filter by



[https://toolbox.googleapps.com/apps/har\\_analyzer/](https://toolbox.googleapps.com/apps/har_analyzer/)

- **accept-encoding** gzip, deflate, br
- **accept-language** en-US,en;q=0.9
- **baggage** sentry-environment=production,sentry-release=9a75c2ed5adfaf2855e2f08b16fab43882f61ee0,sentry-public\_key=cbc53af9b3cb4612b135d7ca380a8dca,sentry-trace\_id=e942b3107ad245d0ae0fcb835f0c3a7e,sentry-sample\_rate=0.2,sentry-transaction=trends,sentry-sampled=true
- **cache-control** no-cache
- **cookie** auth.strategy=local
- **dnt** 1

06:17:21.279	GET https://viz.greynoise.io/_nuxt/img/anomalies-graph.9be9b6b.png	200	-	-		70 ms	‡
	GET https://viz.greynoise.io/gn-api/greynoise/v3/summary/tags	0	-	-		6 ms	-

- **dnt** 1
- **pragma** no-cache
- **referer** https://viz.greynoise.io/trends?view=trending
- **sec-ch-ua** "Not=A?Brand";v="99", "Chromium";v="118"
- **sec-ch-ua-mobile** ?0
- **sec-ch-ua-platform** "macOS"



master

3 branches 0 tags

Go to file

Add file

Code



thefunkjunky Flask POST lists test still not working

cc4599d on Mar 1, 2018 32 commits

harsanitizer	POST api tests failing despite confirmation that they work manually	6 years ago
tests/python-tests	Flask POST lists test still not working	5 years ago
.gitignore	Removed ability to load Har() with har_path. Began adding tests	5 years ago
BUILD	Initial Commit <small>This path skips through empty directories</small>	6 years ago
CONTRIBUTING	Initial Commit	6 years ago
LICENSE	Initial Commit	6 years ago
README.md	Modified Garrett's emails	5 years ago
config.json	Fixed additional local/remote static serving issues	6 years ago
requirements.txt	Replace six string_types with basestring	5 years ago

README.md

# HAR Sanitizer

<https://github.com/google/har-sanitizer>

## Description

HAR files are JSON-formatted "recordings" of web traffic activity for a user's browser session, which are often used to troubleshoot web front-ends, REST APIs, authentication issues, etc. However, HAR files will capture everything in a web session, including passwords, sensitive form information, authentication cookies and headers, and any content embedded in HTTP requests. This makes HAR files extremely sensitive, and highly prone to privacy breaches if handled incorrectly.



*But Wait...*  
**There's  
MORE!**

# BeyondTrust Discovers Breach of Okta Support Unit

<https://www.beyondtrust.com/blog/entry/okta-support-unit-breach>

# How Cloudflare mitigated yet another Okta compromise

<https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/>



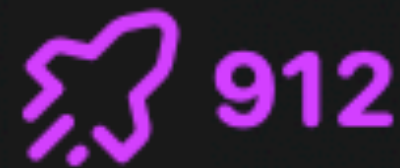
<https://nondeterministic.computer/@mjg59/111270439428001258>



**Matthew Garrett**

@mjg59@nondeterministic.computer

PLEASE check your kids' Halloween candy. Just found an Okta admin access token in a Snickers bar.



Oct 20, 2023 at 21:36

3 DAYS

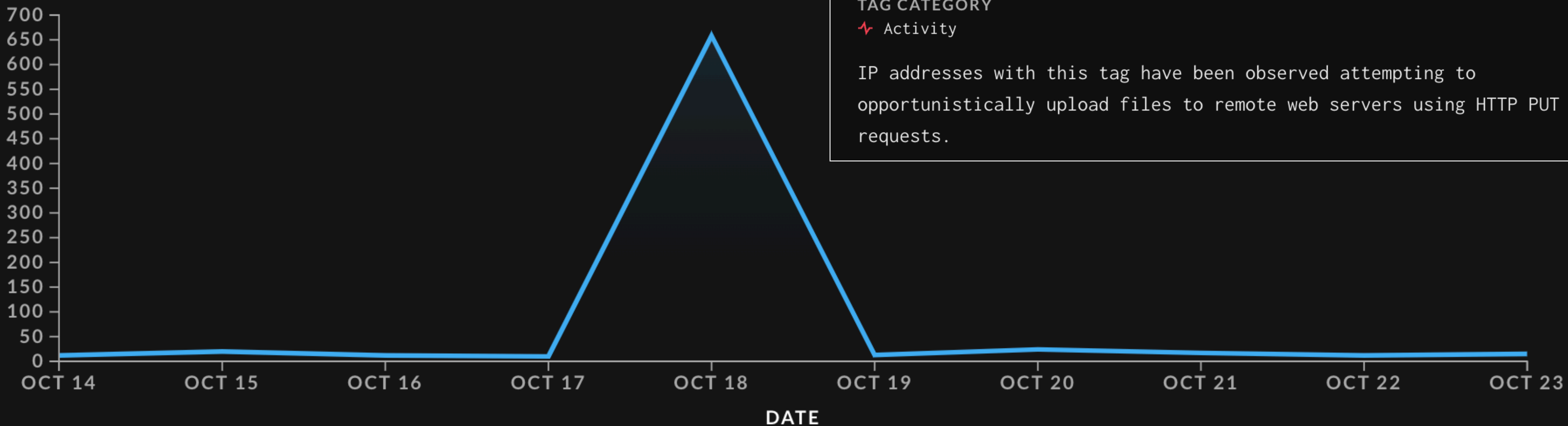
• 10 DAYS

30 DAYS

October 14, 2023 - October 24, 2023

# 732

UNIQUE IPS OBSERVED BY GREYNOISE



### GREYNOISE TRENDS

↗ HTTP PUT UPLOADER

### TAG INTENT

Malicious

### TAG CATEGORY

↗ Activity

IP addresses with this tag have been observed attempting to opportunistically upload files to remote web servers using HTTP PUT requests.

<https://viz.greynoise.io/tag/http-put-uploader-scanner?days=10>

jre版本: openjdk:8-jre

elasticsearch版本: v1.6.0

影响版本: 1.6.1以下

## 原理 [🔗](#)

### 参考文章

- <https://www.exploit-db.com/exploits/38383/>
- <http://www.freebuf.com/vuls/99942.html>

说明:

elasticsearch 1.5.1及以前, 无需任何配置即可触发该漏洞。之后的新版, 配置文件elasticsearch.yml中必须存在 `path.repo`, 该配置值为一个目录, 且该目录必须可写, 等于限制了备份仓库的根位置。不配置该值, 默认不启动这个功能。

## 漏洞复现 [🔗](#)




### 1. 新建一个仓库 [🔗](#)

```
PUT /_snapshot/test HTTP/1.1
Host: your-ip:9200
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0
Connection: close
```





**Brianna Goldstein**  
to blin...@chromium.org

Oct 19, 2023, 4:52:53 PM (4 days ago)   

[https://groups.google.com/a/chromium.org/g/blink-dev/c/9s8ojrooa\\_Q](https://groups.google.com/a/chromium.org/g/blink-dev/c/9s8ojrooa_Q)

**Explainer**

[IP Protection form](#) <https://github.com/GoogleChrome/ip-protection>

**Specification**

None

**Summary**

[IP Protection](#) is a feature that sends third-party traffic for a set of domains through proxies for the purpose of protecting the user by masking their IP address from those domains.

After receiving much feedback from the ecosystem, the design of the broader proposal is as follows:

- **IP Protection will be opt-in initially.** This will help ensure that there is user control over privacy decisions and that Google can monitor behavior.
- **It will roll out in a phased manner.** Like all of our privacy proposals, we want to ensure that we learn as we go and we recognize that there may be unintended consequences.
- **We are using a list based approach and only domains on the list in a third-party context will be impacted.** We are conscious that these proposals may impact some third-party services.

We plan to test and roll out the feature in multiple phases. To start, Phase 0 will use a single Google-owned proxy and will only proxy requests to domains owned by Google. This first phase will allow us to test our infrastructure while preventing impact to other companies and gives us more time to refine the list of domains that will be proxied. For simplicity, only clients with US-based IP addresses will be granted access to the proxies for phase 0.

A small percentage of clients will be automatically enrolled in this initial test, though the architecture and design will evolve between this test and future launches. To access the proxy, a user must be logged in to Chrome. To prevent abuse, a Google-run authentication server will grant access tokens to the Google run proxy based on a per-user quota.

In future phases we plan to use a 2-hop proxy, as had previously been indicated in the IP Protection explainer.



draft-ietf-masque-quic-proxy-00

MASQUE

Internet-Draft

Intended status: Experimental

Expires: 18 February 2024

T. Pauly

E. Rosenberg

Apple Inc.

D. Schinazi

Google LLC

<https://datatracker.ietf.org/doc/draft-ietf-masque-quic-proxy/> 23

QUIC-Aware Proxying Using HTTP  
draft-ietf-masque-quic-proxy-00

## Abstract

This document defines an extension to UDP Proxying over HTTP that adds specific optimizations for proxied QUIC connections. This extension allows a proxy to reuse UDP 4-tuples for multiple connections. It also defines a mode of proxying in which QUIC short header packets can be forwarded using an HTTP/3 proxy rather than being re-encapsulated and re-encrypted.



<https://seacoastcurrent.com/ixp/488/p/40000-maine-residents-may-have-had-ids-stolen-in-massive-hack/>

# HACKED

## 40,000 MAINE RESIDENTS MAY HAVE HAD IDS STOLEN IN MASSIVE HACK

 Cooper Fox | Published: October 21, 2023

Luca Bravo / Unsplash / Canva

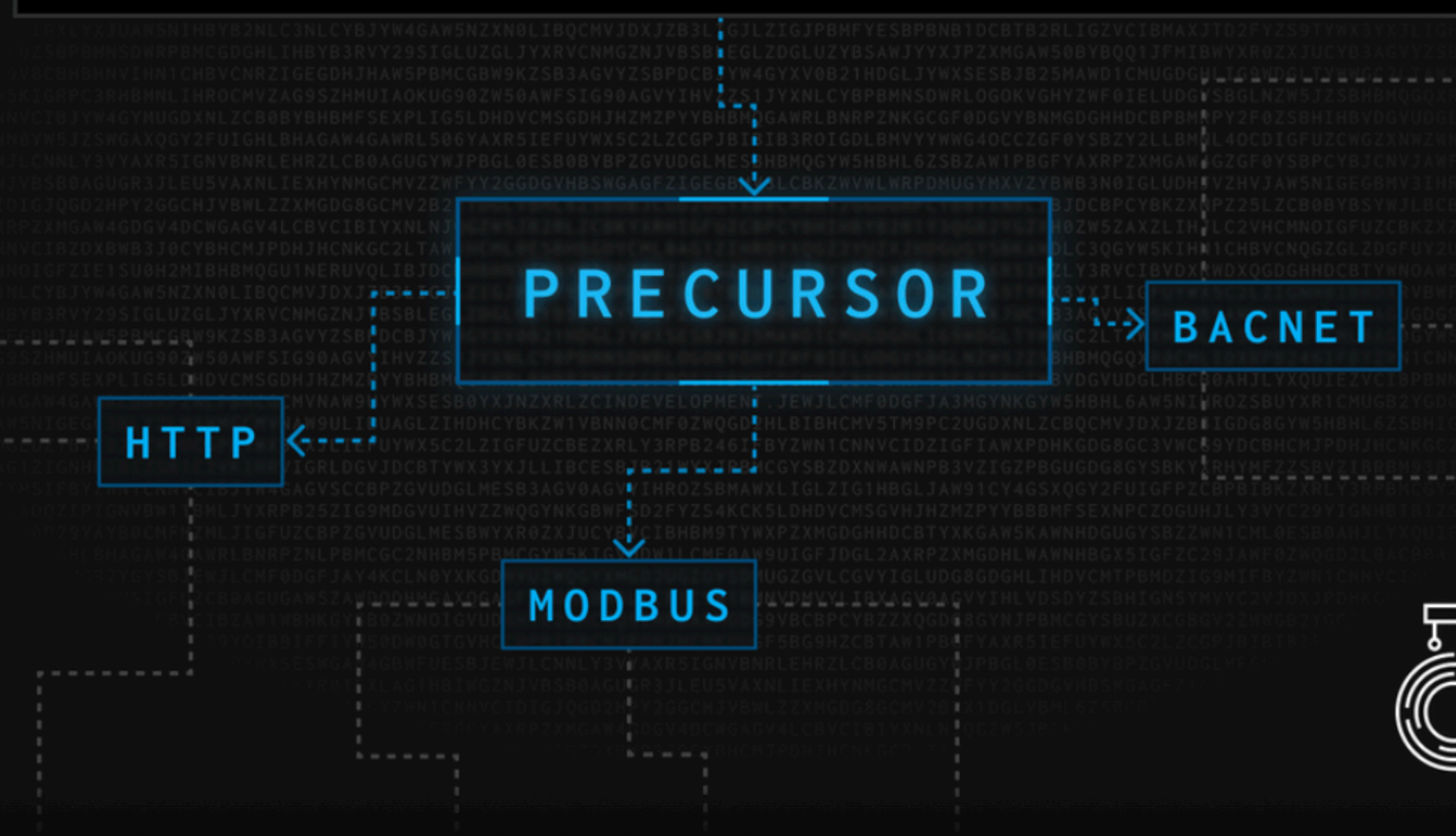
LABS

# Precursor: A Quantum Leap in Arbitrary Payload Similarity Analysis

Matt Lehman | October 17, 2023



```
SFRUUDFNT0RCVVMYQKFDSD05FVDJNT0RCVVMZSFRUUDNCQUNLTKVUMUHUVFAYQKFDSD05FVDNNT0RCVVMXCG==
```



<https://www.greynoise.io/blog/precursor-a-quantum-leap-in-arbitrary-payload-similarity-analysis>

- 🏷️ Citrix ADC Netscaler CVE-2023-4966 Information Disclosure Attempt
- 🏷️ ZenTao CMS SQL Injection Attempt
- 🏷️ Cisco IOS XE Privilege Escalation Attempt
- 🏷️ Atlassian Jira Path Traversal Attempt
- 🏷️ Cisco IOS XE RCE Attempt
- 🏷️ V2 Catalog Scanner
- 🏷️ Zimbra Collaboration Suite Directory Traversal Attempt
- 🏷️ Oracle WebLogic CVE-2018-2894 File Upload Attempt
- 🏷️ MLFlow Directory Traversal Attempt
- 🏷️ Microsoft Exchange Server Scanner
- 🏷️ Yii Framework Information Disclosure Scanner





It Has Been

1

Days Since The  
Last KEV Release

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

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

Cisco IOS XE Web UI Unspecified Vulnerability

Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability



# Storm ⚡ Watch