

S T O R M ⚡ W ⚡ T C H

Dateline: 2023-11-21



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



[Justice.gov](#) > [U.S. Attorneys](#) > [District of Puerto Rico](#) > [Press Releases](#) > Russian and Moldovan National Pleads Guilty to Operating Illegal Botnet Proxy Service that Infected Tens of Thousands of Internet-Connected Devices Around the World

PRESS RELEASE

Russian and Moldovan National Pleads Guilty to Operating Illegal Botnet Proxy Service that Infected Tens of Thousands of Internet-Connected Devices Around the World

Tuesday, November 14, 2023

For Immediate Release

<https://www.justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service>

SAN JUAN, Puerto Rico – A Russian and Moldovan national pled guilty to three counts of violating 18 U.S.C. § 1030(a)(5)(A) Fraud and Related Activity in Connection with Computers.

The FBI today revealed US law enforcement's dismantlement of a botnet proxy network and its infrastructure associated with the



From at least June 2019 through December 2022, Makinin developed and deployed malicious software to hack thousands of Internet-connected devices around the world, including in Puerto Rico. Makinin controlled these infected devices as part of an extensive botnet, which is a network of compromised devices. The main purpose of the botnet was to turn infected devices into proxies as part of a for-profit scheme, which made access to these proxies available through Makinin's websites, proxx.io and proxx.net. Through those websites, Makinin sold illegitimate access to the infected, controlled devices to customers seeking to hide their Internet activities. A single customer could pay hundreds of dollars a month to route traffic through thousands of infected computers. Makinin's publicly-accessible website advertised that he had over 23,000 "highly anonymous" proxies from all over the world.



“It is no secret that in present times, much criminal activity is conducted or enabled through cybernetic means. Cybercriminals seek to remain anonymous and derive a sense of security because they hide behind keyboards, often thousands of miles away from their victims,” said Joseph González, Special Agent in Charge of the FBI’s San Juan Field Office. “The FBI’s cyber mission has been to impose risk and consequences on our adversaries, ensuring cyberspace is no safe space for criminal activity. This case is one example of how we are doing just that, and I’d like to thank the DOJ’s Computer Crime and Intellectual Property Section, the US Attorney’s Office for the District of Puerto Rico, and the FBI San Juan Cyber Team for their meticulous and relentless work in this case.”

and Related Activity in Connection with Computers.

The FBI today revealed US law enforcement’s dismantlement of a botnet proxy network and its infrastructure associated with the



The background is a vibrant red with a sense of motion, created by several overlapping, curved, and slightly blurred bands of varying shades of red. In the upper right quadrant, there is a large, white, three-dimensional number '3' that appears to be floating or attached to the scene. The text 'BREAKING NEWS' is centered horizontally and vertically. 'BREAKING' is in a white, bold, sans-serif font with a thin black outline. 'NEWS' is in a larger, light blue-grey, bold, sans-serif font with a thin black outline.

BREAKING
NEWS

<https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/>



AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC (2)

Posted on November 15, 2023 by Dissent

SPONSORED OR PAID POSTS

This site doesn't accept sponsored posts and doesn't respond to requests about them.

HAVE A NEWS TIP?

Email:

[Breaches\[at\]Protonmail.ch](mailto:Breaches[at]Protonmail.ch)

[Tips\[at\]DataBreaches.net](mailto:Tips[at]DataBreaches.net)

Signal: +1 516-776-7756

Telegram: [@DissentDoe](https://t.me/DissentDoe)

BROWSE BY NEWS SECTION

Select Category



- General trading practices or pricing issues
- Manipulation of a security
- Insider trading
- Material misstatement or omission in a company's public filings or financial statements, or a failure to file
- Municipal securities transactions or public pension plans
- Specific market event or condition
- Bribery of, or improper payments to, foreign officials (Foreign Corrupt Practices Act Violations)
- Initial coin offerings and cryptocurrencies
- Other

Please select the specific category that best describes your complaint.

Failure to file reports

*** Is this supplemental information to a previous complaint?**

No

*** In your own words, describe the conduct or situation you are complaining about.**

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.



**NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING**



<https://www.bloomberg.com/news/articles/2023-11-15/clorox-cyber-chief-leaves-as-recovery-from-cyberattack-continues?srnd=technology-vp#xj4y7vzkg>

Technology
Cybersecurity

Clorox Cyber Chief Leaves While Company Recovers From Devastating Hack

- Attack disrupted manufacturing operations for several weeks
- Group known as 'Scattered Spider' suspected in security breach



The August breach paralyzed the company's manufacturing operations for weeks and led to nationwide shortages of several products including cleaning sprays, cat litter and Hidden Valley ranch dressing. *Photographer: Gabby Jones/Bloomberg*

By [Ryan Gallagher](#), [Jessica Nix](#), and [Leslie Patton](#)

November 15, 2023 at 2:18 PM EST



Gift this article

Save

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 OR 15(d) of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): September 18, 2023



THE CLOROX COMPANY
(Exact name of registrant as specified in its charter)

Delaware
(State or other jurisdiction of
incorporation)

1-07151
(Commission File Number)

31-0595760
(I.R.S. Employer
Identification No.)

1221 Broadway, Oakland, California 94612-1888
(Address of principal executive offices) (Zip code)

(510) 271-7000
(Registrant's telephone number, including area code)

Not applicable
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- Written communications pursuant to Rule 425 Under the Securities Act (17 CFR 230.425)
- Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock - \$1.00 par value	CLX	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR 230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR 240.12b-2).

Emerging growth company

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

The cybersecurity attack damaged portions of the...IT infrastructure, which caused wide-scale disruption of Clorox's operations. [Clorox] is repairing the infrastructure and is reintegrating the systems that were proactively taken offline. [Clorox] expects to begin the process of transitioning back to normal automated order processing the week of Sept. 25.

Clorox is still evaluating the extent of the financial and business impact. Due to the order processing delays and elevated level of product outages, [Clorox] now believes the impact will be material on Q1 financial results.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-Q

(Mark one)

QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

<https://www.sec.gov/Archives/edgar/data/1810019/000181001923000164/rxt-20230930.htm>

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from _____ to _____.

Commission File Number: 001-39420

RACKSPACE TECHNOLOGY, INC.

(Exact name of registrant as specified in its charter)



Delaware
(State or other jurisdiction of incorporation)

81-3369925
(Employer Identification No.)

CVE-2022-41080 OWASSRF/
Microsoft Exchange
Info Disclosure/RCE

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common stock, par value \$0.01 per share	RXT	The Nasdaq Stock Market LLC

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes No

Indicate by check mark whether the registrant has submitted and posted such files 2 months (or for such shorter period that the

<https://viz.greynoise.io/tag/exchange-owassrf-vuln-attempt?days=30>



We are named in several lawsuits in connection with the December 2022 ransomware incident which caused service disruptions on our Hosted Exchange email business. The pending lawsuits seek, among other things, equitable and compensatory relief. We are vigorously defending these matters. We do not expect any of these claims, individually or in the aggregate, to have a material adverse effect on our consolidated financial position or results of operations. However, at this early stage in the proceedings, we are not able to determine the probability of the outcome of these matters or a range of reasonably expected losses, if any. We maintain insurance, including coverage for cyber-attacks, subject to certain deductibles and policy limitations, in an amount that we believe appropriate. During the three and nine months ended September 30, 2023, we recorded \$0.1 million and \$5.0 million, respectively, of expenses related to the Hosted Exchange incident, including costs to investigate and remediate, legal and other professional services, and supplemental staff resources that were deployed to provide support to customers. We recorded \$5.4 million of loss recovery insurance proceeds received or expected to be received during the three and nine months ended September 30, 2023.

(Ma

Secu

(2) h

regis

nd



https://www.bleepingcomputer.com/news/security/toyota-confirms-breach-after-medusa-ransomware-threatens-to-leak-data/

MEDUSA BLOG

TWITTER TELEGRAM

DAYS: 09
HOURS: 10
MINUTES: 57
SECONDS: 36



Toyota Financial

Toyota Motor Corporation is a Japanese multinational automotive manufacturer headquartered in Toyota City, Aichi, Japan. Toyota is one of the largest automobile manufacturers in the world, producing about 10 million vehicles per year. The leaked data is from Toyota Financial Services in Germany. Toyota Deutschland GmbH is an affiliated company held by Toyota Motor Europe (TME) in Brussels/Belgium and located in Köln (Cologne).

Add time 1 day

10000\$

Delete All Data

8000000\$

Download data now!

8000000\$

Medusa ransomware gang listed TFS to its data leak site on the dark web, demanding a payment of \$8,000,000 to delete data allegedly stolen from the Japanese company.

The threat actors gave Toyota 10 days to respond, with the option to extend the deadline for \$10,000 per day.



<https://viz.greynoise.io/tag/citrix-adc-netscaler-cve-2023-4966-information-disclosure-attempt?days=30>

3 DAYS

10 DAYS

• 30 DAYS

October 22, 2023 - November 20, 2023

347

UNIQUE IPS OBSERVED BY GREYNOISE

+ TAG CREATED





IRISS

Irish Reporting and
Information Security Service

<https://iriss.ie/irisscon/#speakers>



The skills employed, the hacktivists and other threat actors are not going anywhere. Right now, Russia might be overwhelmingly interested in Ukraine, but their aims and goals remain global.

These skills will be turned in other directions and other targets in the future, they will be shared in threat actor groups online. This is the world you need to be preparing for right now



<https://msrc.microsoft.com/blog/2023/11/reflecting-on-20-years-of-patch-tuesday/>

Reflecting on 20 years of Patch Tuesday

[MSRC](#) / By [MSRC](#) / November 17, 2023 / 3 min read



This year is a landmark moment for Microsoft as we observe the 20th anniversary of Patch Tuesday updates, an initiative that has become a cornerstone of the IT world's approach to cybersecurity. Originating from the [Trustworthy Computing memo](#) by Bill Gates in 2002, our unwavering commitment to protecting customers continues to this day and is reflected in Microsoft's [Secure Future Initiative](#) announced this month. Each month, we deliver security updates on the second Tuesday, underscoring our pledge to cyber defense. As we commemorate this milestone, it's worth exploring the inception of Patch Tuesday and its evolution through the years, demonstrating our adaptability to new technology and emerging cyber threats.

The origin of Patch Tuesday

The concept of Patch Tuesday was conceived and implemented in 2003. Before this unified approach, our security updates were sporadic, posing significant challenges for IT professionals and organizations in deploying critical patches in a timely manner. Senior leaders of the Microsoft Security Response Center (MSRC) at the time spearheaded the idea of a predictable schedule for patch releases, shifting from a "ship when ready" model to a regular weekly, and eventually, monthly cadence.

[Subscribe](#)

Categories >

[MSRC \(1056\)](#)[Japan Security Team \(1015\)](#)[Security Research & Defense \(379\)](#)[BlueHat \(188\)](#)[Microsoft Threat Hunting \(4\)](#)[Bug Bounty Programs \(3\)](#)

Tags >

[セキュリティ情報 \(465\)](#)[脆弱性 \(248\)](#)[アドバイザリ \(172\)](#)[Internet Explorer \(IE\) \(156\)](#)[Security Update \(140\)](#)[Security Advisory \(134\)](#)[Security Bulletin \(133\)](#)[Mitigations \(128\)](#)[Community-based Defense \(107\)](#)[Microsoft Windows \(106\)](#)[View all Tags](#)

Blog /

Re

MSRC /

This year is a landmark moment for Microsoft as we observe the 20th anniversary of Patch Tuesday updates, an initiative that has become a cornerstone of the IT world's approach to cybersecurity. Originating from the Trustworthy Computing memo by Bill Gates in 2002,

(ED: The "Trustworthy Computing" initiative was abandoned in 2014)

our unwavering commitment to protecting customers continues to this day and is reflected in Microsoft's Secure Future Initiative announced this month. Each month, we deliver security updates on the second Tuesday, underscoring our pledge to cyber defense. As we commemorate this milestone, it's worth exploring the inception of Patch Tuesday and its evolution through the years, demonstrating our adaptability to new technology and emerging cyber threats.

This y
has b
Bill G
[Secur](#)
our p
evolu

The

The c
were

manner. Senior leaders of the Microsoft Security Response Center (MSRC) at the time spearheaded the idea of a predictable schedule for patch releases, shifting from a "ship when ready" model to a regular weekly, and eventually, monthly cadence.

[Microsoft Windows \(100\)](#)

[View all Tags](#)

The initial goal was to ensure that security updates were delivered in a predictable and consistent manner, reducing the risk of security vulnerabilities being exploited.



Reflecting on 20 years of Patch Tuesday

MSRC /

In addition to consolidating patch releases into a monthly schedule, we also organized the security update release notes into a consolidated location. Prior to this change, customers had to navigate through various Knowledge Base articles, making it difficult to find the information they needed to secure themselves. Recognizing the need for clarity and convenience, we provided a comprehensive overview of monthly releases. This change was pivotal at a time when not all updates were delivered through Windows Update, and customers needed a reliable source to find essential updates for various products.

This y
has b
Bill G
[Secur](#)

our pledge to cyber defense. As we commemorate this milestone, it's worth exploring the inception of Patch Tuesday and its evolution through the years, demonstrating our adaptability to new technology and emerging cyber threats.

The origin of Patch Tuesday

The concept of Patch Tuesday was conceived and implemented in 2003. Before this unified approach, our security updates were sporadic, posing significant challenges for IT professionals and organizations in deploying critical patches in a timely manner. Senior leaders of the Microsoft Security Response Center (MSRC) at the time spearheaded the idea of a predictable schedule for patch releases, shifting from a "ship when ready" model to a regular weekly, and eventually, monthly cadence.

[Security Advisory](#) (134)

[Security Bulletin](#) (133)

[Mitigations](#) (128)

[Community-based Defense](#) (107)

[Microsoft Windows](#) (106)

[View all Tags](#)





- CAMLIS 2023**
CAMLIS - 1 / 22
- ▶ **Keynote - Lessons for AI Security Preparedness**
CAMLIS 1:07:58
 - 2 **Threat Detection on Kubernetes Logs Using GNN...**
CAMLIS 27:11
 - 3 **FASER: Binary Code Similarity Search through the use of...**
CAMLIS 23:57
 - 4 **Proxy in a Haystack: Uncovering and Classifying...**
CAMLIS 24:17
 - 5 **SQL Driven Infrastructure for Cybersecurity ML Operations**
CAMLIS 25:54
 - 6 **Small Effect Sizes in Malware Detection? Make Harder...**
CAMLIS 24:25
 - 7 **Adaptive Experimental Design for Intrusion Data Collection**
CAMLIS 25:58
 - 8 **MalDICT: Benchmark Datasets on Malware Behaviors,...**
CAMLIS 25:23

Conference on Applied Machine Learning in Information Security (CAMLIS)

<https://www.youtube.com/watch?v=nFrpJ3tDoJE&list=PL47-BvVz5JMpM6s1UnKTIrQwxKuktRym9>

- Playing Defense: Benchmarking Cybersecurity Capabilities of...**
CAMLIS 16 views · 2 days ago
New 28:11
- Backspace Blackout**
CAMLIS 136 views · 2 days ago
New 26:34
- Don't you forget NLP: prompt injection using repeated...**
CAMLIS 136 views · 2 days ago
New





- CAMLIS 2023**
CAMLIS - 1 / 22
- ▶ **Keynote - Lessons for AI Security Preparedness**
CAMLIS
1:07:58
 - 2 **Threat Detection on Kubernetes Logs Using GNN...**
CAMLIS
27:11
 - 3 **FASER: Binary Code Similarity Search through the use of...**
CAMLIS
23:57
 - 4 **Proxy in a Haystack: Uncovering and Classifying...**
CAMLIS
24:17
 - 5 **SQL Driven Infrastructure for Cybersecurity ML Operations**
CAMLIS
25:54
 - 6 **Small Effect Sizes in Malware Detection? Make Harder...**
CAMLIS
24:25
 - 7 **Adaptive Experimental Design for Intrusion Data Collection**
CAMLIS
25:58
 - 8 **MalDICT: Benchmark Datasets on Malware Behaviors,...**
CAMLIS
25:23

Conference on Applied Machine Learning in Information Security (CAMLIS)

<https://www.youtube.com/watch?v=nFrpJ3tDoJE&list=PL47-BvVz5JMpM6s1UnKTIrQwxKuktRym9>

- Playing Defense: Benchmarking Cybersecurity Capabilities of...**
CAMLIS
16 views · 2 days ago
New
28:11
- Backspace Blackout**
26:34
- Don't you forget NLP: prompt injection using repeated...**
CAMLIS
136 views · 2 days ago
New



TOOL TIME



imjasonh update readme d6c1302 · last week History

Preview Code Blame 48 lines (31 loc) · 2.68 KB Raw

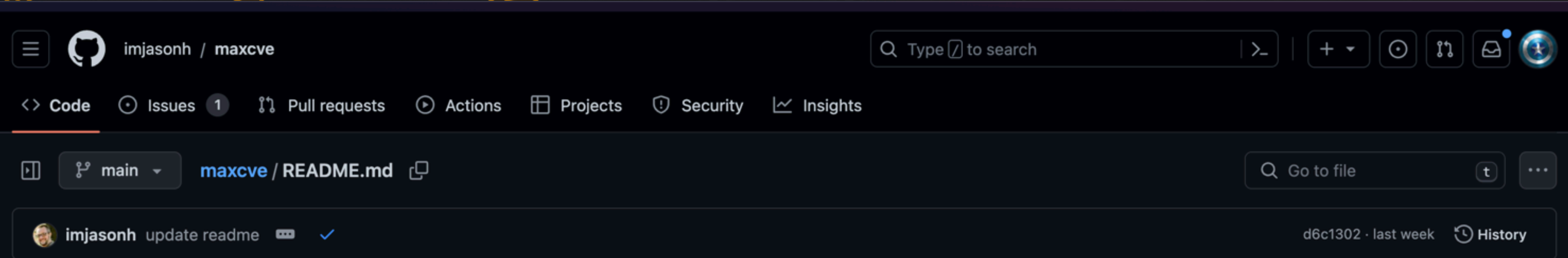
MAXIMUM CVEs

This repo generates a container image that maximizes the number of CVEs in the image, while minimizing the size of the image. The result is a 148 KB image that reports as having almost 30,000 CVEs. That's roughly one CVE for every 5 bytes of image data!

```
$ time gype $(go run .) > /dev/null
2023/11/12 11:07:09 wrote /lib/apk/db/installed
2023/11/12 11:07:09 wrote /etc/os-release
2023/11/12 11:07:09 wrote ttl.sh/maxcve@sha256:c43609f71b0bf2d3f317d6347291bc070c09aab40cdcae5a16b723ea596620ab
  ✓ Vulnerability DB [no update available]
  ✓ Loaded image ttl.sh/maxcve@sha256:c43609f71b0bf2d3:
  ✓ Parsed image sha256:9ccc9244966be8bcl
  ✓ Cataloged packages [26573 packages]
  ✓ Scanned for vulnerabilities [29345 vulnerability matches]
    └─ by severity: 1925 critical, 17158 high, 8845 medium, 400 low, 0 negligible (1017 unknown)
    └─ by status: 24759 fixed, 4586 not-fixed, 0 ignored
```

Or, if you prefer to consume data visually:

<https://github.com/imjasonh/maxcve>



Aside from being fun, this image demonstrates how scanners work -- and importantly, how they don't work.

At their most basic, scanners require images (1) tell them what OS they are, and (2) tell them what packages they contain. This image does both, but it does so in a way that is misleading.

Or, if you prefer to consume data visually:



Premium

Search



Malicious Compliance: Reflections on Trusting Container Scanners

Ian Coldwater, Independent; Duffie Cooley, Isovalent; Brad Geesaman, Ghost Security; Rory McCune, Datadog



Malicious Compliance: Reflections on Trusting Container... - Coldwater, Cooley, Geesaman, McCune



CNCF [Cloud Native Computing Foundation]
107K subscribers

Subscribe

66



Share

Download

Clip

Save



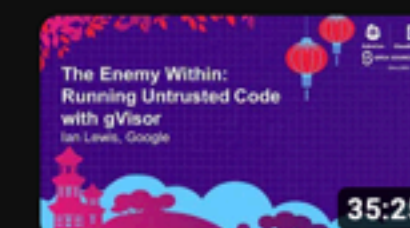
3,243 views May 1, 2023

Malicious Compliance: Reflections on Trusting Container Scanners - Ian Coldwater, Independent; Duffie Cooley, Isovalent; Brad Geesaman, Ghost Security; Rory McCune, Datadog

<https://www.youtube.com/watch?v=9weGi0csBZM>

McCune will demonstrate some creative ways to intentionally bypass container image analysis and admission control detection. Attendees will walk away with a greater understanding of the limitations of tooling used to validate images, and learn how to create better security policies in their own environments. The results may surprise you!

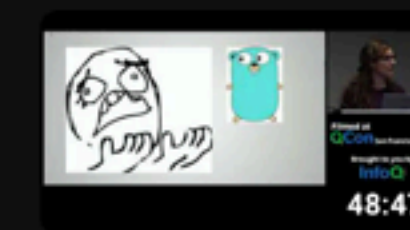
Cloud Native Co... Related Recently uploaded



The Enemy Within: Running Untrusted Code with gVisor -...
CNCF [Cloud Native Computing Fou...
1.9K views · 4 years ago



Collaboratively Building App Manifests at Scale in Complex...
CNCF [Cloud Native Computing Fou...
461 views · 6 months ago



The Why of Go
InfoQ
171K views · 5 years ago



Breakpoints in Your Pod: Interactively Debugging...
CNCF [Cloud Native Computing Fou...
984 views · 6 months ago



4 JavaScript Projects under 4 Hours | JavaScript Tutorial For...
Simplilearn
164K views · Streamed 9 months...



Orchestrating Multi-Tenancy Kubernetes Environments with...
CNCF [Cloud Native Computing Fou...
589 views · 6 days ago



Debugging Under Fire: Keep your Head when Systems have...
GOTO Conferences
87K views · 6 years ago



Demystifying IPv6 Kubernetes -
Antonio Jose Ojea Garcia,...



Tuning PostgreSQL for High-Write Workloads
Grant Wulder
40K views · 6 years ago



A commonly recommended best practice for security and compliance is to scan container images for vulnerabilities before allowing them to run inside a cluster. Many organizations codify allow/deny policies based on the results of these scans, using this policy-as-code approach to form the basis of trust. But what exactly are container scanners looking for? And can you always trust the results? Let's break this down layer by layer, from an attacker perspective. Why do certain changes in the way images are built produce wildly varying results? Can the flexibility in how container images are built and distributed be used to alter or prevent scanning tools from being able to fully understand what's in a container? How might clever image builders use these tricks to avoid scrutiny from these tools?

McCune will demonstrate some creative ways to intentionally bypass container image analysis and admission control detection. Attendees will walk away with a greater understanding of the limitations of tooling used to validate images, and learn how to create better security policies in their own environments. The results may surprise you!

Tuesday, February 14, 2018

42:33

45K views · 6 years ago





Shameless Self-Promotion



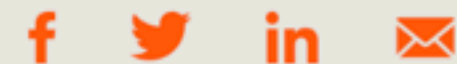
Request a Demo

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

BLOG

Introducing Censys Search Teams

SHARE



NOVEMBER 14, 2023

Tags: [Censys Search](#)

Unlocking Industry-Leading Internet Intelligence for Small Security Teams

In today's ever-evolving threat landscape, staying a step

✕ Want to learn more about what this means for your org or is there something else I can help with?





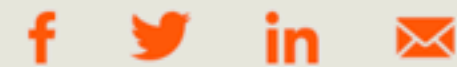
Request a Demo

<https://censys.com/discovery-of-ntc-vulkan-infrastructure/>

BLOG

Discovery of NTC Vulkan Infrastructure

SHARE



NOVEMBER 15, 2023

Tags: [Federal](#), [Research](#)

Executive Summary

In March 2023, various media outlets published details from documents received in February of 2022 from a former NTC Vulkan employee who opposed Russia's invasion of Ukraine. Moscow-based NTC Vulkan, the

ABOUT THE AUTHOR



Matt Lembright
Director of Federal Applications





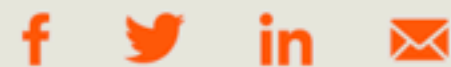
Request a Demo

<https://censys.com/unleash-the-power-of-censys-search-discovering-more-with-historical-data/>

BLOG

Unleash the Power of Censys Search: Exploring More with Historical Data

SHARE



NOVEMBER 16, 2023

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

Welcome back to Part III of our "Unleash the Power of Censys Search"

ABOUT THE AUTHOR



Rachel Hannenberg
Content Marketing



PRODUCT INSIGHTS

Getting A Leg Up On Initial Access Ransomware With CISA KEV and GreyNoise Tags

The Cybersecurity and Infrastructure Security Agency (CISA) has added a field to their Known Exploited Vulnerabilities (KEV) catalog that denotes if a KEV CVE has been used in ransomware attacks. 35% of those have a corresponding GreyNoise tag. See how together CISA and GreyNoise can help you stay even further ahead of our combined adversaries

boB Rudis | Nov 16, 2023



<https://www.greynoise.io/blog/getting-a-leg-up-on-initial-access-ransomware-with-cisa-kev-and-greynoise-tags>



Triage

Explore

About Sift

November 2023

2023-11-14 (34)

2023-11-13 (84)

2023-11-12 (85)

2023-11-11 (165)

2023-11-10 (87)

2023-11-09 (65)

2023-11-08 (84)

2023-11-07 (124)

2023-11-06 (121)

2023-11-05 (124)

2023-11-04 (85)

2023-11-03 (129)

2023-11-02 (308)

2023-11-01 (116)

October 2023

2023-11-14

< 5 / 34 records >

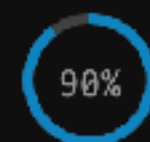
EXPORT

Potential Shellshock Exploit Detected

THREAT



CONFIDENCE



ATTACK TYPE

REMOTE CODE EXECUTION

Existing Tags For This Event

- Web Crawler
- Shell Shock CVE-2014-6271

Payload Examples

```
GET / HTTP/1.1
Accept-Encoding: gzip
Accept: */*
Host: <ip>:443
User-Agent: () { :; }; echo; echo; /bin/bash -c 'expr <random_num_len_9> + <random_num_len_9>'
```



Using math operations as a test payload? I guess it's better than 'Hello, World!'

- 🏷️ rConfig SQL Injection Attempt (CVE-2020-10546, CVE-2020-10547, CVE-2020-10548, CVE-2020-10549)
- 🏷️ Zemra Botnet CnC Web Panel RCE Attempt
- 🏷️ Oracle WebLogic CVE-2014-4210 SSRF Attempt (CVE-2014-4210)
- 🏷️ CrushFTP RCE Attempt (CVE-2023-4177)
- 🏷️ FSMLabs TimeKeeper RCE Attempt (CVE-2023-31465)

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

**WE NEED
TO TALK
ABOUT
KEY**




It Has Been

5

Days Since The
Last KEV Release

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

- ❌ CVE-2023-36033: Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability
- ❌ CVE-2023-36025: Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
- ❌ CVE-2023-36036: Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability
- ❌ CVE-2023-36584: Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability
- ❌ CVE-2023-1671: Sophos Web Appliance Command Injection Vulnerability 
- ❌ CVE-2020-2551: Oracle Fusion Middleware Unspecified Vulnerability



3 DAYS

10 DAYS

• 30 DAYS

GREYNOISE TRENDS

~ SOPHOS WEB APPLIANCE RCE ATTEMPT

TAG INTENT

Malicious

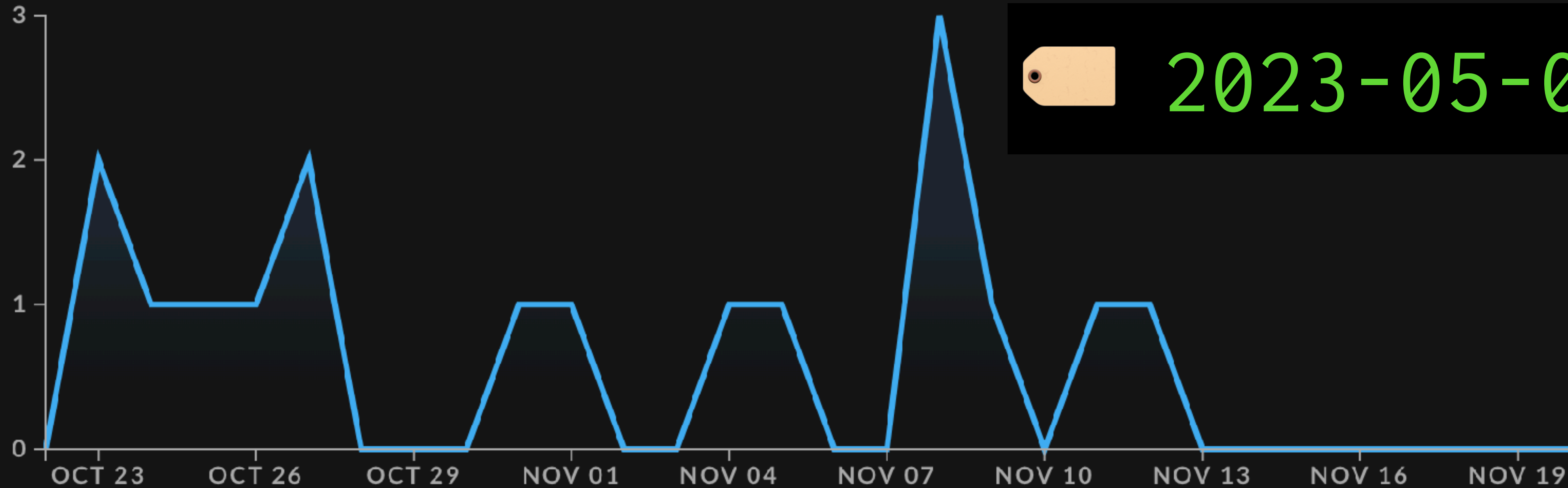
TAG CATEGORY

~ Activity

IP addresses with this tag have been observed attempting to exploit CVE-2023-1671, a remote command execution vulnerability in Sophos Web Appliance.

10

UNIQUE IPS OBSERVED BY GREYNOISE



 2023-05-01

<https://viz.greynoise.io/tag/sophos-web-appliance-rce-attempt?days=30>



<https://www.cisa.gov/news-events/news/piloting-new-ground-expanding-scalable-cybersecurity-services-protect-broader-critical>

BLOG

Piloting New Ground: Expanding Scalable Cybersecurity Services to Protect the Broader Critical Infrastructure Community

Released: November 17, 2023

By Eric Goldstein, Executive Assistant Director for Cybersecurity

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE](#)



In recent years, cyber attacks have intensified in both volume and impact—affecting the day-to-day operations of organizations across our nation’s critical infrastructure sectors. When most Americans consider the cyber-physical impact of attacks on critical infrastructure, they may recall when a ransomware attack on Colonial Pipeline’s corporate network led to a disruption of fuel supplies to gas stations along the East Coast. More recently, advanced actors such as [Volt Typhoon](#) have demonstrated the intent and technical ability to disrupt our critical infrastructure





Top

Home

Blog

Partners

Contacts

Resources

Rel

By

REL

In r

org

CISA is excited to announce a pilot program designed to deliver cutting-edge cybersecurity shared services on a voluntary basis to critical infrastructure entities that are most in need of support. CISA has acted as a managed service provider to the federal civilian government for years and observed significant risk reduction along with the benefits of cost-savings and standardization. Leveraging a new authority provided by Congress, we are eager to extend our support and enterprise cybersecurity expertise with non-federal organizations that require additional assistance to effectively address cybersecurity risks.

impact of attacks on critical infrastructure, they may recall when a ransomware attack on Colonial Pipeline's corporate network led to a disruption of fuel supplies to gas stations along the East Coast. More recently, advanced actors such as [Volt Typhoon](#) have demonstrated the intent and technical ability to disrupt our critical infrastructure





TLP:CLEAR



Mitigation Guide: Healthcare and Public Health (HPH) Sector

November 2023
Cybersecurity and Infrastructure Security Agency

https://www.cisa.gov/sites/default/files/2023-11/HPH-Sector-Mitigation-Guide-TLP-CLEAR_508c.pdf

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see <http://www.cisa.gov/tlp>.

TLP:CLEAR

This vulnerability mitigation guidance maps CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) to Health and Human Services (HHS) and the Health Sector Coordinating Council's (HSCC) joint publication: 405(d) Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients which is detailed in the CPG HICP Crosswalk guide. This mitigation guide evaluates the most common vulnerabilities exposed in the HPH Sector and provides tailored recommendations and best practices for HPH organizations of all sizes. In addition to CPGs, HICPs, and the HPH Sector Cybersecurity Framework Implementation Guide, CISA recommends manufacturers of HPH technology products take actions in line with CISA's Principles and Approaches for Security-by-Design and -Default in order to reduce the burden of cybersecurity on their customers.



Storm ⚡ Watch