STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-04-30

LIKE

SUBSCRIBE

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://StormWatch.ing

LEAVE A COMMENT

SHARE

STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

https://www.orangecyberdefense.com/be/blog/unveiling-the-depths-of-residential-proxies-providers

RESIdential Proxies

https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/
https://sec.okta.com/blockanonymizers

From March 18, 2024 through to April 16, 2024, Duo Security and Cisco Talos observed large-scale brute force attacks on multiple models of VPN devices.

From April 19, 2024 through to April 26, 2024, Okta's Identity Threat Research team observed a spike in credential stuffing activity against user accounts from what appears to be similar infrastructure.

Credential Stuffing

Attempts to sign-in to online services using large lists of usernames and passwords obtained from previous data breaches of unrelated entities, or from phishing or malware campaigns.

All recent attacks share one feature in common: they rely on requests being routed through anonymizing services such as TOR.

Millions of the requests were also routed through a variety of residential proxies including NSOCKS, Luminati and DataImpulse.

RESIP providers leverage real users' devices like computers, smartphones, and IoT devices to create large pools of residential IP addresses, which are more effective at evading detection than datacenter or VPN IPs.

GreyNoise Trends

SQUELDA MSSQL BRUTE FORCE ATTEMPT

INTENTION
MALICIOUS

CATEGORY
Activity

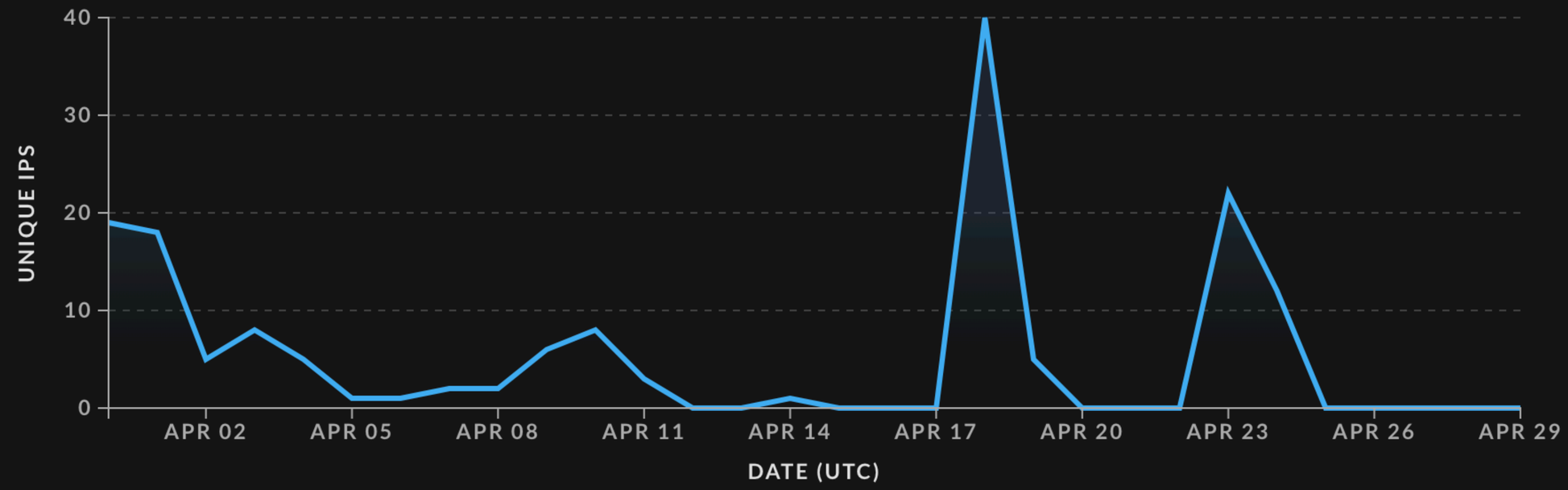
CVES
No associated CVEs

IP addresses with this tag have been observed using the SQLDict tool which utilizes squelda 1.0 to conduct a MSSQL brute force attempt via dictionary attack.

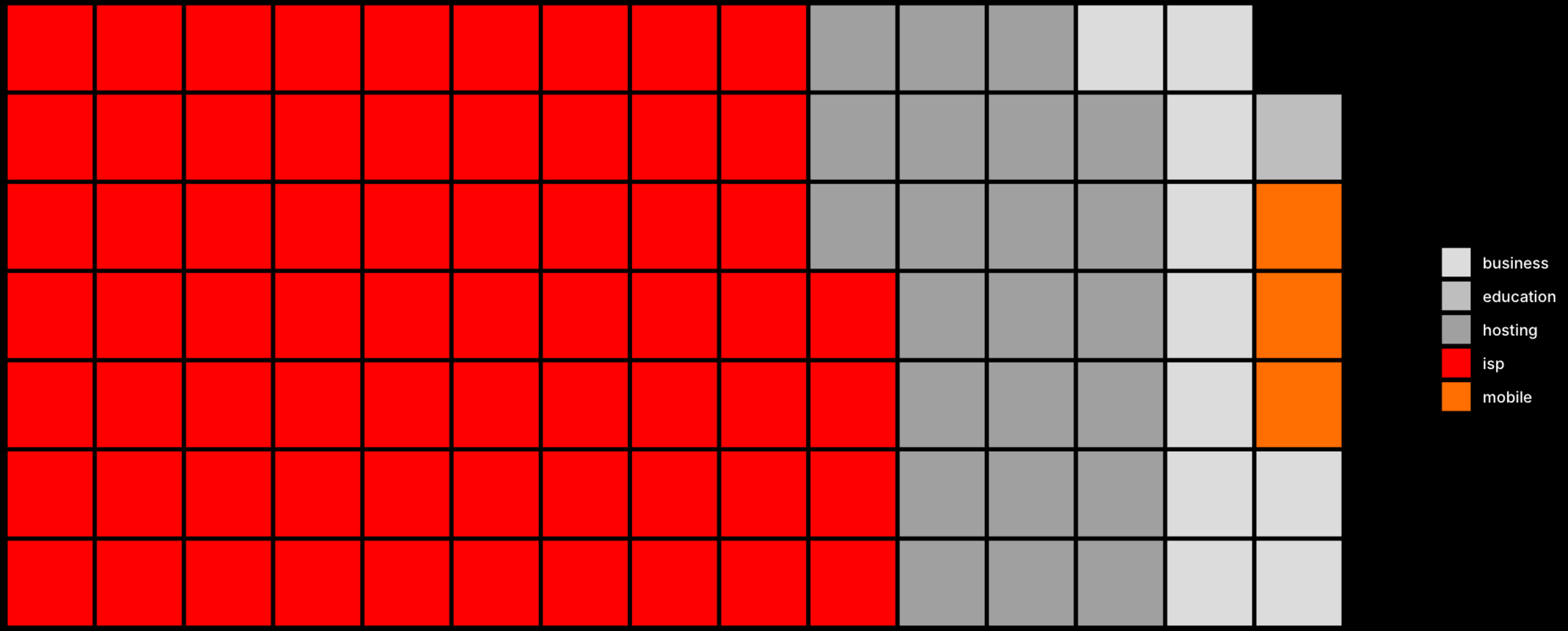
24 HOURS | 10 DAYS | •30 DAYS | March 31, 2024 - April 29, 2024 (UTC)

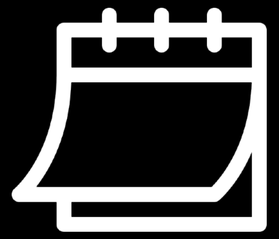
Unique IPs Observed

Last 30 days



squelda MSSQL Brute Force Attempts IP Categories





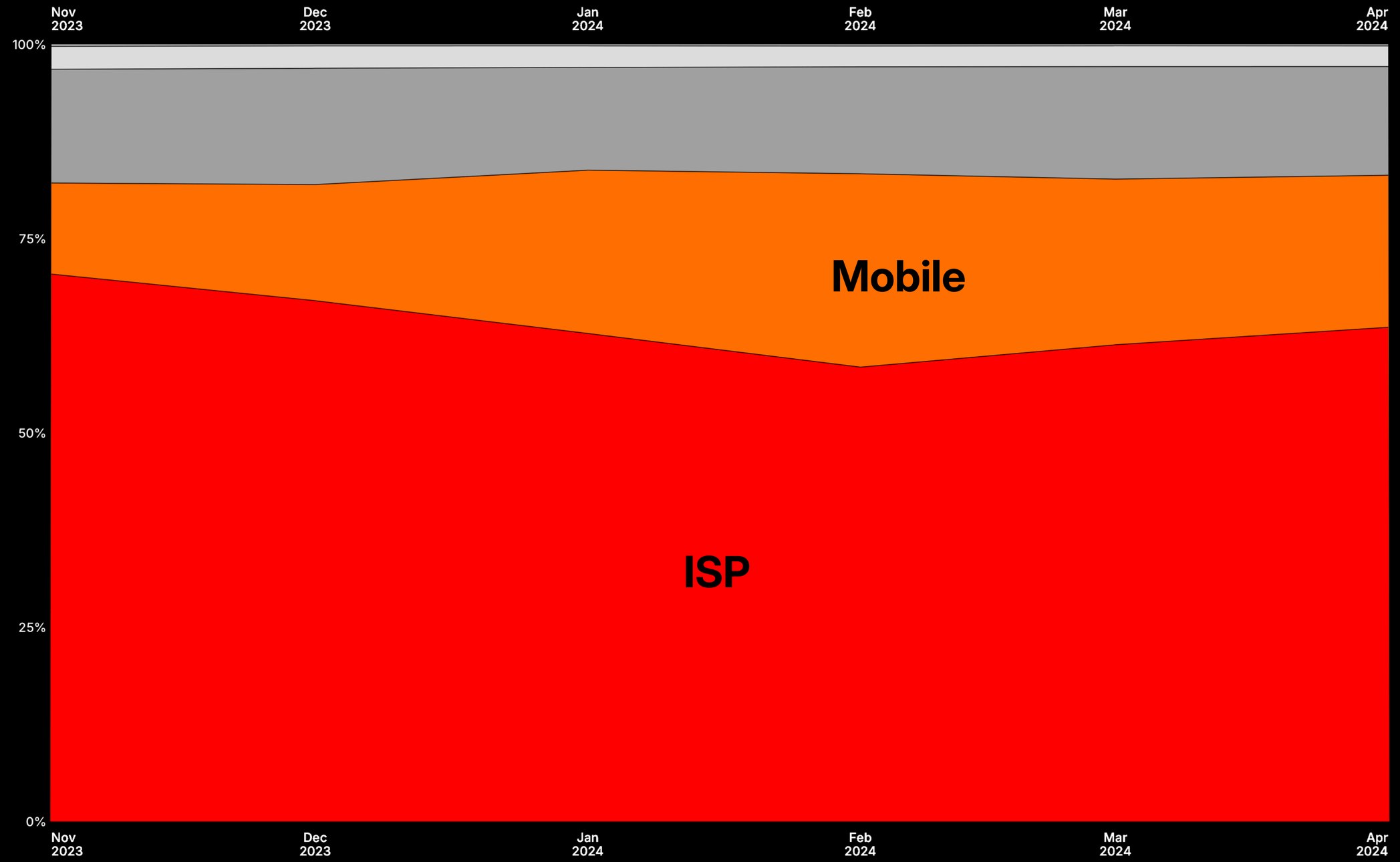
Mar-Apr 2024

60% ISP

~2 Million IPv4s

20% Mobile

~700K IPv4s


Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
100%
75%
50%
25%
0%
Mobile
ISP

How to Use Machine Learning to Detect Residential Proxies

https://datadome.co/bot-management-protection/how-to-use-machine-learning-to-detect-residential-proxies/

Table of Contents

Machine learning (ML) is an important tool for scaling sophisticated bot and online fraud protection. One way we apply ML at DataDome is to identify residential proxies.

Residential proxies are increasingly popular among attackers because their IP addresses resemble those of regular, human users. So, the ability to detect whether or not a request originates from a residential proxy significantly improves the quality of detection.

In this guide, we present one of the ML models used by DataDome to classify whether or not a residential IP address was recently used as a residential proxy by malicious bots. But before we dive into ML, we'll begin with a run-through of the basics.

What is an IP address?

An IP (Internet Protocol) address is a set of numbers that can be seen as a device's

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

[Submitted on 26 Apr 2024]

Merchants of Vulnerabilities: How Bug Bounty Programs Benefit Software Vendors

Esther Gal-Or, Muhammad Zia Hydari, Rahul Telang

Software vulnerabilities enable exploitation by malicious hackers, compromising systems and data security. This paper examines bug bounty programs (BBPs) that incentivize ethical hackers to discover and responsibly disclose vulnerabilities to software vendors. Using game-theoretic models, we capture the strategic interactions between software vendors, ethical hackers, and malicious hackers. First, our analysis shows that software vendors can increase expected profits by participating in BBPs, explaining their growing adoption and the success of BBP platforms. Second, we find that vendors with BBPs will release software earlier, albeit with more potential vulnerabilities, as BBPs enable coordinated vulnerability disclosure and mitigation. Third, the optimal number of ethical hackers to invite to a BBP depends solely on the expected number of malicious hackers seeking exploitation. This optimal number of ethical hackers is lower than but increases with the expected malicious hacker count. Finally, higher bounties incentivize ethical hackers to exert more effort, thereby increasing the probability that they will discover severe vulnerabilities first while reducing the success probability of malicious hackers. These findings highlight BBPs' potential benefits for vendors beyond profitability. Earlier software releases are enabled by managing risks through coordinated disclosure. As cybersecurity threats evolve, BBP adoption will likely gain momentum, providing vendors with a valuable tool for enhancing security posture and stakeholder trust. Moreover, BBPs envelop vulnerability identification and disclosure into new market relationships and transactions, impacting software vendors' incentives regarding product security choices like release timing.

Subjects: **Cryptography and Security (cs.CR)**; Computer Science and Game Theory (cs.GT); General Economics (econ.GN)

Cite as: arXiv:2404.17497 **[cs.CR]**

(or arXiv:2404.17497v1 **[cs.CR]** for this version)

Computer Science > Cryptography and Security

[Submitted on 26 Apr 2024]

Merchants of Vulnerabilities: How Bug Bounty Programs Benefit Software Vendors

Esther Gal-Or, Muhammad Zia Hydari, Rahul Telang

Software vulnerabilities enable exploitation by malicious hackers, compromising systems and data security. This paper examines bug bounty programs (BBPs) that incentivize ethical hackers to discover and responsibly disclose vulnerabilities to software vendors. Using game-theoretic models, we capture the strategic interactions between software vendors, ethical hackers, and malicious hackers. First, our analysis shows that software vendors can increase expected profits by participating in BBPs, explaining their growing adoption and the success of BBP platforms. Second, we find that vendors with BBPs will release software earlier, albeit with more potential vulnerabilities, as BBPs enable coordinated vulnerability disclosure and mitigation. Third, the optimal number of ethical hackers to invite to a BBP depends solely on the expected number of malicious hackers seeking exploitation. This optimal number of ethical hackers is lower than but increases with the expected malicious hacker count. Finally, higher bounties incentivize ethical hackers to exert more effort, thereby increasing the probability that they will discover severe vulnerabilities first while reducing the success probability of malicious hackers. These findings highlight BBPs' potential benefits for vendors beyond profitability. Earlier software releases are enabled by managing risks through coordinated disclosure. As cybersecurity threats evolve, BBP adoption will likely gain momentum, providing vendors with a valuable tool for enhancing security posture and stakeholder trust. Moreover, BBPs envelop vulnerability identification and disclosure into new market relationships and transactions, impacting software vendors' incentives regarding product security choices like release timing.

Subjects: **Cryptography and Security (cs.CR)**; Computer Science and Game Theory (cs.GT); General Economics (econ.GN)

Cite as: arXiv:2404.17497 **[cs.CR]**

(or arXiv:2404.17497v1 **[cs.CR]** for this version)

❌ No specific program

❌ Theoretical Analysis (Game Theory)

Computer Science > Cryptography and Security

[Submitted on 26 Apr 2024]

Merchants of Vulnerabilities: How Bug Bounty Programs Benefit Software Vendors

Esther Gal-Or, Muhammad Zia Hydari, Rahul Telang

Software vulnerabilities enable exploitation by malicious hackers, compromising systems and data security. This paper examines bug bounty programs (BBPs) that incentivize ethical hackers to discover and responsibly disclose vulnerabilities to software vendors. Using game-theoretic models, we capture the strategic interactions between software vendors, ethical hackers, and malicious hackers. First, our analysis shows that software vendors can increase expected profits by participating in BBPs, explaining their growing adoption and the success of BBP platforms. Second, we find that vendors with BBPs will release software earlier, albeit with more potential vulnerabilities, as BBPs enable coordinated vulnerability disclosure and mitigation. Third, the optimal number of ethical hackers to invite to a BBP depends solely on the expected number of malicious hackers seeking exploitation. This optimal number of ethical hackers is lower than but increases with the expected malicious hacker count. Finally, higher bounties incentivize ethical hackers to exert more effort, thereby increasing the probability that they will discover severe vulnerabilities first while reducing the success probability of malicious hackers. These findings highlight BBPs' potential benefits for vendors beyond profitability. Earlier software releases are enabled by managing risks through coordinated disclosure. As cybersecurity threats evolve, BBP adoption will likely gain momentum, providing vendors with a valuable tool for enhancing security posture and stakeholder trust. Moreover, BBPs envelop vulnerability identification and disclosure into new market relationships and transactions, impacting software vendors' incentives regarding product security choices like release timing.

Subjects: **Cryptography and Security (cs.CR)**; Computer Science and Game Theory (cs.GT); General Economics (econ.GN)

Cite as: arXiv:2404.17497 **[cs.CR]**

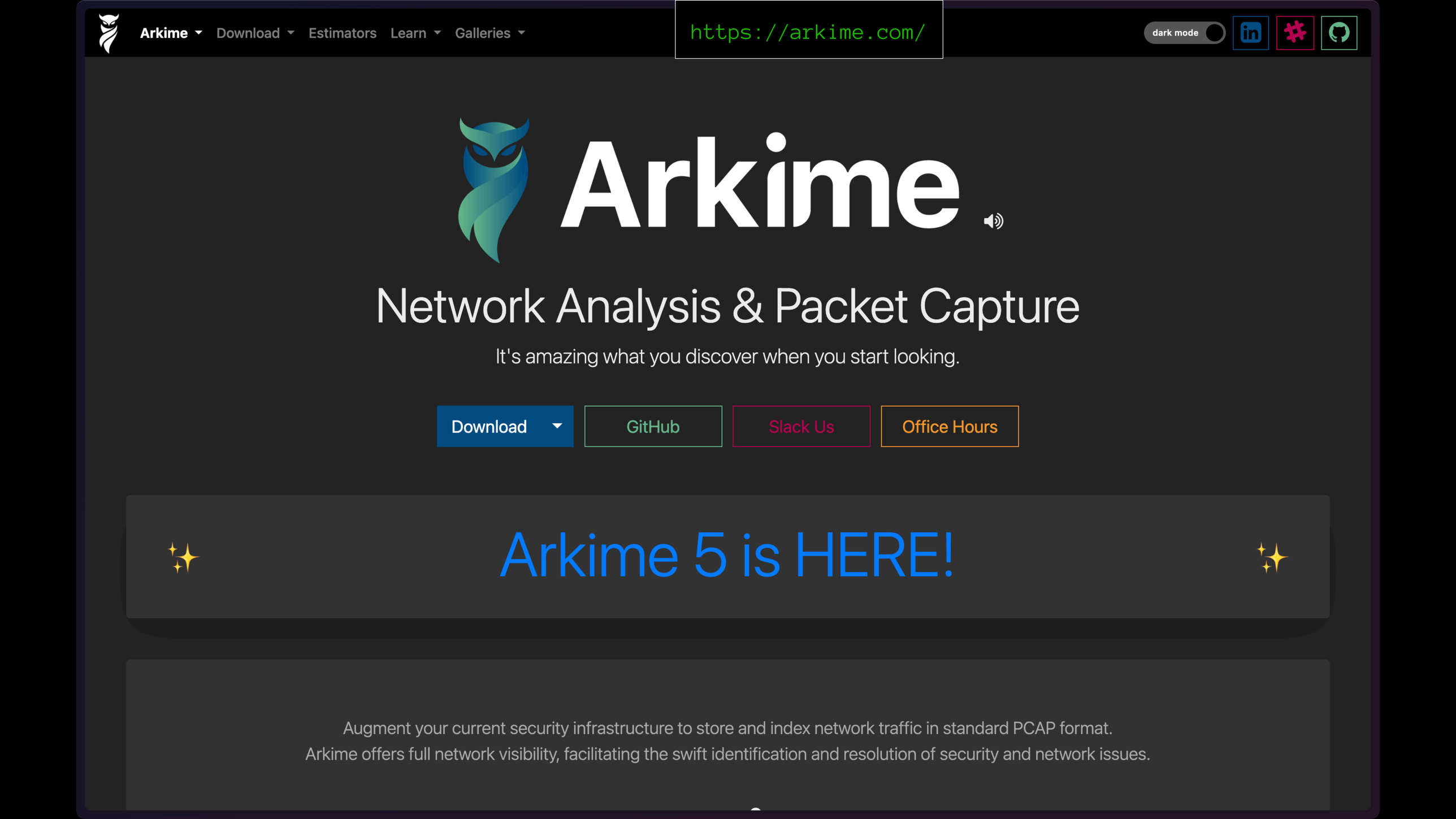
(or arXiv:2404.17497v1 **[cs.CR]** for this version)

The study's primary aim is to understand how BBPs can influence software vendors' decisions regarding software release timing, the setting of bounty amounts, and the selection of ethical hackers to participate in these programs.

It investigates the potential benefits of BBPs for software vendors, including increased expected profits, earlier software releases, and the optimal number of ethical hackers to involve in a BBP *based on the expected number of malicious hackers*.

STORM WATCH

CYBERSECURITY NEWS

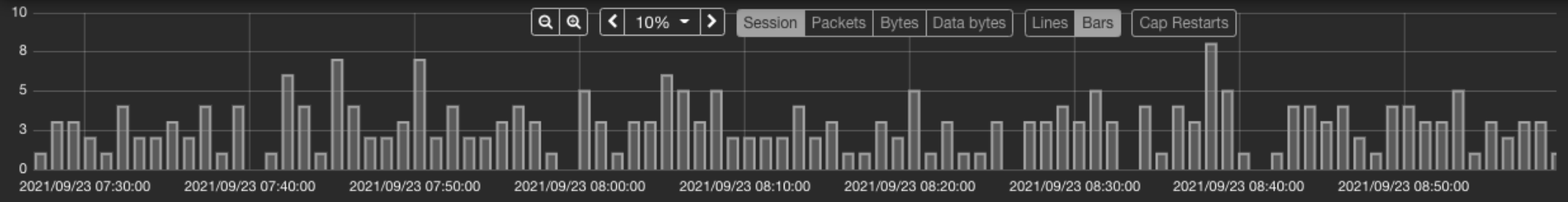

Arkime
Download
Estimators
Learn
Galleries
https://arkime.com/
dark mode
Arkime
Network Analysis & Packet Capture
It's amazing what you discover when you start looking.
Download
GitHub
Slack Us
Office Hours
Arkime 5 is HERE!
Augment your current security infrastructure to store and index network traffic in standard PCAP format.
Arkime offers full network visibility, facilitating the swift identification and resolution of security and network issues.

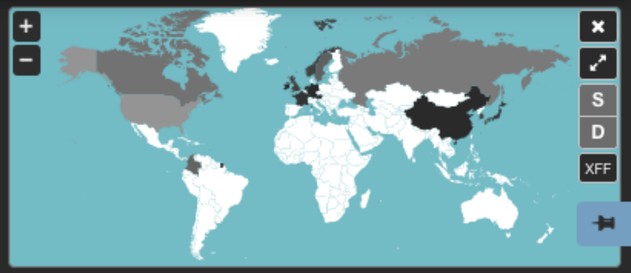
Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings Users v5.0.0

Search Search

Custom Start 2021/09/23 07:26:51 End 2021/09/23 08:59:15 Bounding Last Packet Interval Auto 01:32:24

50 per page « ‹ 1 2 3 4 5 › » Showing 1 - 50 of 260 entries





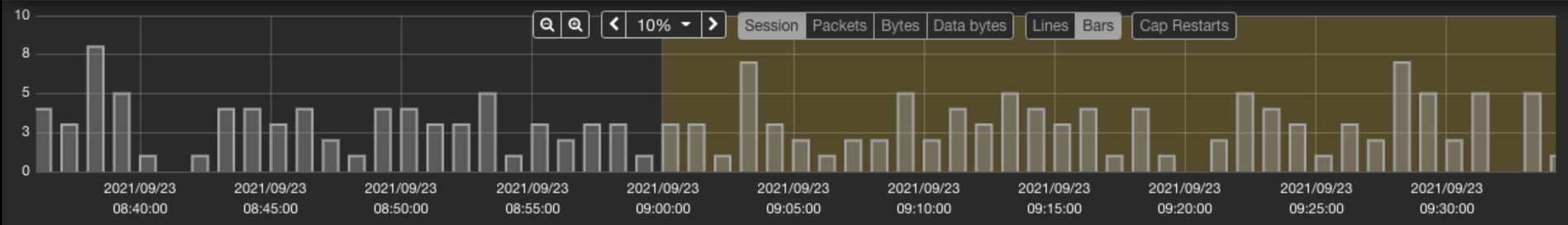
	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Info
+	tcp	2021/09/23 08:57:31	2021/09/23 08:58:47	190.0.0.2	45188	10.176.192.13	80	6,443	3,245,118 3,605,688	test	URI wooden.com/detail/whenever.cgi wooden.com/guest/clue wooden.com/philosophy/climate.jpg more...
+	tcp	2021/09/23 08:53:02	2021/09/23 08:53:54	172.16.0.1	19142	192.168.177.160	80	10,394	8,422,064 9,357,850	test	URI miracle.com/because/crop.jpg miracle.com/military/barrel.gif
+	tcp	2021/09/23 08:52:25	2021/09/23 08:59:10	172.5.5.113	44482	10.11.12.13	80	9,800	4,585,731 5,095,258	test	URI employer.com/package/lawsuit.php employer.com/valuable/daughter.gif
+	tcp	2021/09/23 08:51:31	2021/09/23 08:58:30	104.16.125.34	17015	192.168.1.111	80	8,325	6,440,536 7,156,152	test	URI white.com/submit/nor.cgi white.com/cultural/far.cgi white.com/topic/mystery.php more...
+	tcp	2021/09/23 08:51:27	2021/09/23 08:55:41	64.12.21.3	25755	224.0.0.22	80	6,596	3,340,475 3,711,640	test	URI president.com/repeatedly/ship.jpg
+	tcp	2021/09/23 08:50:49	2021/09/23 08:55:31	10.0.2.15	1039	10.10.10.19	80	4,836	774,734 860,817	test	URI fall.com/band/example.jpg fall.com/substantial/virtue.cgi fall.com/impossible/avoid.jpg more...
+	tcp	2021/09/23 08:50:09	2021/09/23 08:53:44	204.62.14.153	63884	10.156.206.202	80	8,167	4,855,979 5,395,533	test	URI voice.com/adolescent/critic.gif voice.com/hour/historical.php voice.com/before/empty.gif more...
+	tcp	2021/09/23 08:49:44	2021/09/23 08:57:49	10.44.100.22	6316	10.0.0.4	80	11,861	7,050,194 7,833,550	test	URI ancient.com/attention/temperature.html ancient.com/particular/continued.php ancient.com/drag/customer.gif more...
+	tcp	2021/09/23 08:49:28	2021/09/23 08:58:11	155.230.24.155	8888	10.180.156.141	80	7,767	5,880,874 6,534,305	test	URI color.com/and/unable.cgi color.com/broad/monitor.cgi
+	tcp	2021/09/23 08:47:44	2021/09/23 08:51:50	139.162.123.134	37560	10.180.156.141	80	10,779	5,422,082 6,024,537	test	URI modern.com/im/in/crisis.php

Sessions | SPIView | SPIGraph | Connections | Hunt | Files | Stats | History | Settings | Users — v5.0.0

Search | Search

Custom | Start 2021/09/23 08:36:01 | End 2021/09/23 09:34:11 | Bounding Last Packet | Interval Auto | 00:58:10

Showing 177 entries filtered from 4,969 total entries



general

tcp (177) | Unload All | Load All

Search for fields to display in this category | Dst IP | Protocols | Src IP | Arkime Node | Arkime Root ID | Asset | Asset Cnt | Bytes | Community Id | Data bytes | Dst ASN | Dst ASN Name | Dst ASN Number | Dst Bytes

Dst IP 10.180.156.141 (18) 10.0.0.3 (4) 216.58.194.195 (4) 10.0.0.4 (3) 10.0.0.7 (3) 10.10.10.1 (3) 10.10.10.13 (3) 10.64.11.49 (3) 10.156.206.202 (3) 10.176.171.11 (3) 74.125.24.95 (3) 192.168.0.1 (3) 10.0.0.12 (2) 10.10.10.2 (2) 10.10.10.12 (2) 10.10.10.14 (2) 10.10.10.16 (2) 10.11.12.13 (2)
10.172.10.172 (2) 31.13.74.1 (2) 38.229.70.20 (2) 64.236.64.226 (2) 66.59.111.190 (2) 74.125.228.103 (2) 104.16.125.34 (2) 118.215.80.242 (2) 172.16.0.2 (2) 172.16.0.4 (2) 172.17.96.77 (2) 172.17.96.143 (2) 188.40.206.23 (2) 190.0.0.1 (2) 190.0.0.23 (2) 192.30.252.131 (2) 192.168.65.3 (2)
192.168.177.160 (2) 192.168.178.20 (2) 204.62.14.153 (2) 216.58.208.195 (2) 217.13.4.24 (2) 224.0.0.1 (2) 224.0.0.22 (2) 10.0.0.1 (1) 10.0.0.5 (1) 10.0.0.8 (1) 10.0.0.11 (1) 10.0.0.33 (1) 10.2.95.39 (1) 10.9.8.7 (1) 10.10.10.11 (1) 10.10.10.19 (1) 10.10.10.20 (1) 10.10.10.30 (1) 10.11.11.11 (1)
10.13.13.13 (1) 10.34.0.1 (1) 10.89.85.15 (1) 10.150.10.150 (1) 10.176.192.13 (1) 10.180.121.109 (1) 10.180.156.249 (1) 13.12.11.10 (1) 14.17.32.211 (1) 23.0.0.2 (1) 23.0.0.3 (1) 52.43.228.156 (1) 54.226.182.138 (1) 64.15.116.182 (1) 66.59.111.182 (1) 68.178.213.61 (1) 74.125.24.100 (1)
74.125.24.149 (1) 74.125.228.226 (1) 74.125.228.238 (1) 104.89.119.175 (1) 129.21.171.72 (1) 129.170.17.4 (1) 155.230.24.155 (1) 172.16.0.3 (1) 172.16.44.3 (1) 172.130.128.76 (1) 173.194.68.26 (1) 190.0.0.3 (1) 190.0.0.4 (1) 190.0.0.5 (1) 190.0.0.13 (1) 190.0.0.15 (1) 190.0.0.25 (1)
192.30.252.130 (1) 192.168.0.10 (1) 192.168.1.111 (1) 192.168.8.97 (1) 192.168.25.150 (1) 192.168.40.178 (1) 192.168.56.11 (1) 192.168.56.12 (1) 192.168.65.1 (1) 192.168.168.1 (1) 192.168.170.8 (1) 192.168.170.20 (1) more...

Protocols http (177) tcp (177)

Src IP 192.168.0.10 (5) 18.26.4.105 (4) 74.125.228.37 (4) 104.16.125.34 (4) 10.0.0.2 (3) 10.34.0.1 (3) 23.0.0.3 (3) 52.43.228.156 (3) 74.125.228.226 (3) 192.168.168.1 (3) 193.242.192.43 (3) 216.58.208.195 (3) 10.0.0.4 (2) 10.0.0.6 (2) 10.0.0.7 (2) 10.0.2.15 (2) 10.5.4.3 (2) 10.9.8.7 (2) 10.10.10.11 (2)
10.10.10.18 (2) 10.23.46.37 (2) 10.150.10.150 (2) 10.176.176.11 (2) 10.180.121.109 (2) 10.180.121.151 (2) 13.115.50.210 (2) 64.12.168.40 (2) 64.236.64.225 (2) 66.59.111.182 (2) 74.217.87.13 (2) 139.162.123.134 (2) 155.230.24.155 (2) 172.5.5.113 (2) 172.28.2.3 (2) 172.202.246.57 (2)
192.168.25.150 (2) 192.168.40.178 (2) 192.168.57.14 (2) 192.168.65.1 (2) 192.168.65.3 (2) 204.62.14.153 (2) 216.58.194.195 (2) 224.0.0.1 (2) 224.0.0.13 (2) 8.8.8.8 (1) 10.0.0.1 (1) 10.0.0.3 (1) 10.0.0.8 (1) 10.0.0.12 (1) 10.0.0.16 (1) 10.0.0.17 (1) 10.0.13.120 (1) 10.1.2.1 (1) 10.10.0.3 (1) 10.10.10.1 (1)
10.10.10.2 (1) 10.10.10.10 (1) 10.10.10.14 (1) 10.10.10.15 (1) 10.10.10.16 (1) 10.10.10.19 (1) 10.10.30.26 (1) 10.11.12.13 (1) 10.12.12.12 (1) 10.44.100.22 (1) 10.176.192.13 (1) 10.180.156.141 (1) 10.180.156.185 (1) 10.180.156.249 (1) 13.12.11.10 (1) 14.17.32.211 (1) 23.0.0.2 (1) 31.13.74.1 (1)
35.174.150.168 (1) 38.229.70.20 (1) 54.226.182.138 (1) 64.12.21.3 (1) 64.236.55.18 (1) 64.236.64.226 (1) 68.178.213.61 (1) 74.125.24.95 (1) 74.125.24.149 (1) 74.125.228.39 (1) 74.125.228.103 (1) 104.89.119.175 (1) 127.0.0.1 (1) 172.16.0.1 (1) 172.16.0.2 (1) 172.16.0.3 (1) 172.16.0.4 (1)
172.130.128.76 (1) 173.194.68.26 (1) 190.0.0.1 (1) 190.0.0.2 (1) 190.0.0.5 (1) 190.0.0.12 (1) 190.0.0.13 (1) 190.0.0.15 (1) 192.30.252.131 (1) 192.168.1.3 (1) more...

bgp

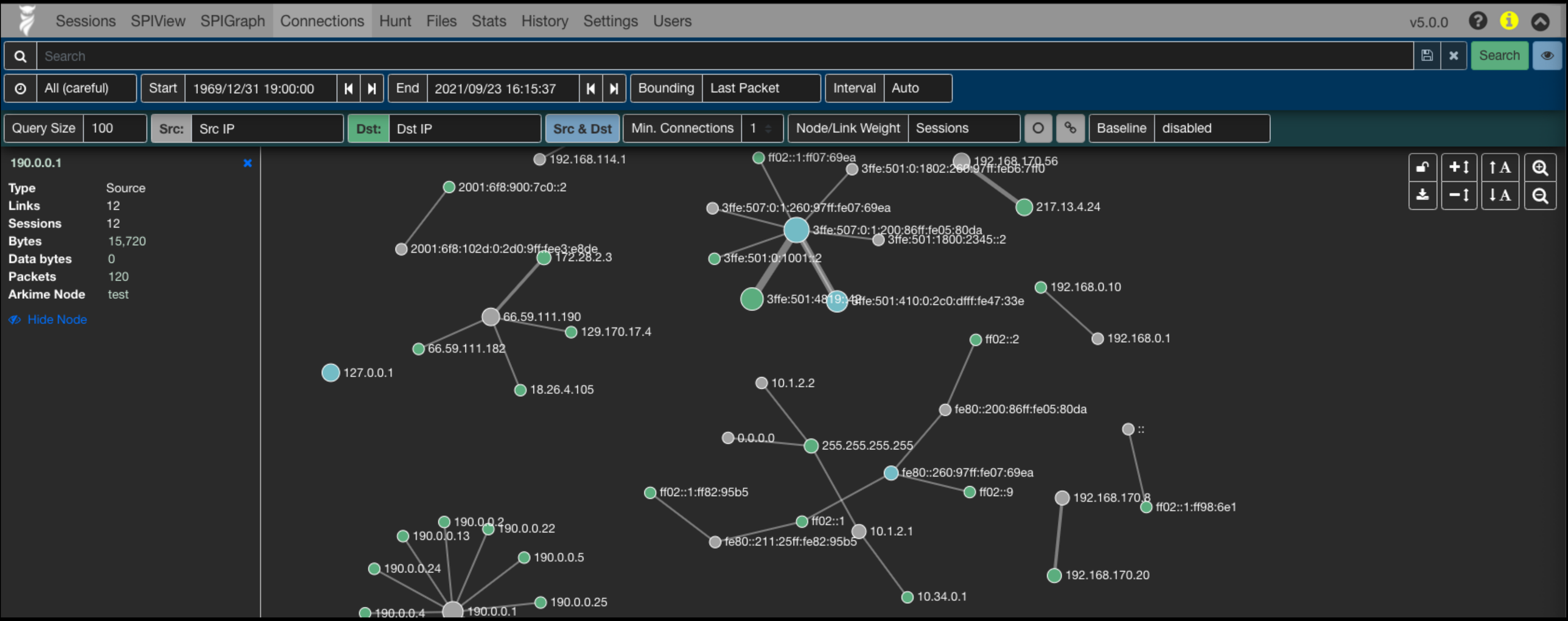
Unload All | Load All

cert

Unload All | Load All

cloud

Unload All | Load All


Sessions
SPIView
SPIGraph
Connections
Hunt
Files
Stats
History
Settings
Users
v5.0.0
Search
Search
All (careful)
Start
1969/12/31 19:00:00
End
2021/09/23 16:15:37
Bounding
Last Packet
Interval
Auto
Query Size
100
Src:
Src IP
Dst:
Dst IP
Src & Dst
Min. Connections
1
Node/Link Weight
Sessions
Baseline
disabled
190.0.0.1
Type
Source
Links
12
Sessions
12
Bytes
15,720
Data bytes
0
Packets
120
Arkime Node
test
Hide Node
192.168.114.1
2001:6f8:900:7c0::2
2001:6f8:102d:0:2d0:9ff:fee3:e8de
172.28.2.3
66.59.111.190
129.170.17.4
66.59.111.182
127.0.0.1
18.26.4.105
ff02::1:ff07:69ea
192.168.170.56
3ffe:501:0:1802:260:97ff:feb6:7ff0
217.13.4.24
3ffe:507:0:1:260:97ff:fe07:69ea
3ffe:507:0:1:200:86ff:fe05:80da
3ffe:501:1800:2345::2
3ffe:501:0:1001::2
3ffe:501:4819:
3ffe:501:410:0:2c0:dfff:fe47:33e
192.168.0.10
192.168.0.1
ff02::2
10.1.2.2
fe80::200:86ff:fe05:80da
0.0.0.0
255.255.255.255
::
fe80::260:97ff:fe07:69ea
ff02::1:ff82:95b5
ff02::9
192.168.170.8
ff02::1:ff98:6e1
ff02::1
10.1.2.1
fe80::211:25ff:fe82:95b5
192.168.170.20
10.34.0.1
190.0.0.2
190.0.0.22
190.0.0.13
190.0.0.5
190.0.0.24
190.0.0.25
190.0.0.4
190.0.0.1

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

censys

https://censys.com/crushftp-cve-2024-4040-crushed-expectations/

Products Solutions Federal Resources Company Search Now

BLOGS

CrushFTP CVE-2024-4040: Crushed Expectations

LABS

Decrypting Fortinet's FortiOS 7.0.x

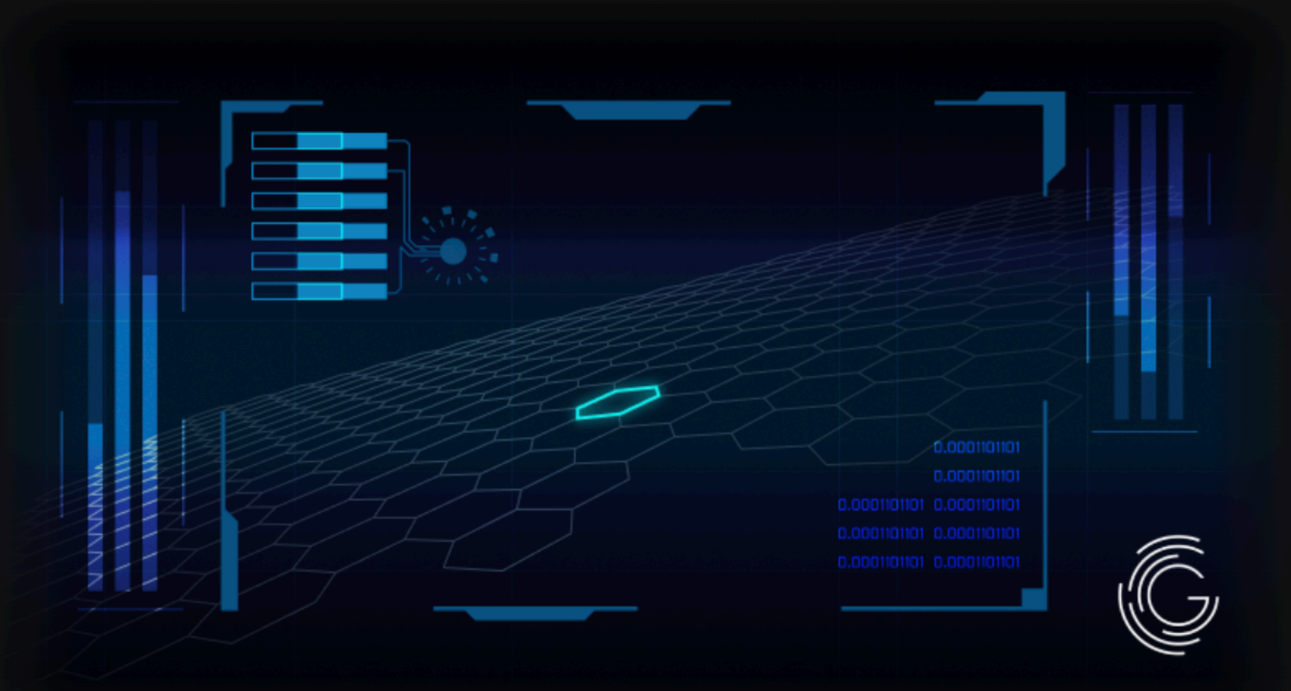
The GreyNoise Labs Team | April 23, 2024

https://www.greynoise.io/blog/decrypting-fortinets-fortios-7-0-x

PRODUCT

Exploring GreyNoise: The User-Centric Design Approach in Cybersecurity

Donna Becerra | April 24, 2024



https://www.greynoise.io/blog/exploring-greynoise-the-user-centric-design-approach-in-cybersecurity

STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP

- WordPress LayerSlider CVE-2024-2879 SQL Injection Attempt (CVE-2024-2879)
- Progress Flowmon CVE-2024-2389 Command Injection RCE Attempt (CVE-2024-2389)
- Yongyou NC Cloud Arbitrary File Upload Attempt ()

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

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

6

Days Since The
Last KEV Release

https://kev.hrbrmstr.app

CVE-2022-38028: Microsoft Windows Print Spooler Privilege Escalation Vulnerability

CVE-2024-4040: CrushFTP VFS Sandbox Escape Vulnerability

CVE-2024-20359: Cisco ASA and FTD Privilege Escalation Vulnerability

CVE-2024-20353: Cisco ASA and FTD Denial of Service Vulnerability