

Dragon Tails: Preserving Supply-Side Vulnerability Disclosure

Cyber Statecraft Initiative

Atlantic Council

Contributors:

Sara Ann Brackett

Yumi Gambrill

Trey Herr

Emmeline Nettles

Stewart Scott

External Vulnerability Research as a Supply

- What are sources of security?
- Global bug-bounty market size projected to reach **\$5.5 billion by 2027**
- Manifests the 'many eyes' theory of security
- Increasing adoption by government agencies and departments
- Proliferation of bug-bounty platform companies
- Governed by Coordinated Vulnerability Disclosure processes (CVD)

Supply-Side Vulnerability Research

Country of Researcher/Recipient	Total Amount Paid	Percentage of Total Amount Paid by US
United States of America	\$6,718,923	15%
China	\$4,220,302	10%
India	\$4,055,807	9%
Russian Federation	\$2,047,212	5%
United Kingdom of Great Britain and Northern Ireland	\$2,029,512	5%
Germany	\$1,698,018	4%
Canada	\$1,674,918	4%
Netherlands	\$1,190,940	3%
Argentina	\$1,103,724	3%
Australia	\$1,072,930	2%
France	\$1,029,796	2%

Anonymized bug-bounty platform revenue streams by country, from Congressional Testimony—Dakota Cary, February 17, 2022

Supply-Side Vulnerability Research

Can bad policy break this ecosystem, and can we detect those supply shocks?

Good CVD in Log₄Shell

Vulnerability disclosures fall between two extremes:

1. Disclose everything you know about a vulnerability to everyone as soon as you know it.
2. Never disclose anything you know about a vulnerability to anyone.

Good CVD in Log4Shell

Vulnerability disclosures fall between two extremes:

1. Disclose everything you know about a vulnerability to everyone as soon as you know it.
2. Never disclose anything you know about a vulnerability to anyone.

- **November 24, 2021:** Alibaba Cloud researcher discloses log4shell (l4s) to ASF privately.

Good CVD in Log4Shell

Vulnerability disclosures fall between two extremes:

1. Disclose everything you know about a vulnerability to everyone as soon as you know it.
2. Never disclose anything you know about a vulnerability to anyone.

- **November 24, 2021:** Alibaba Cloud researcher discloses log4shell (l4s) to ASF privately.
- **December 8,* 2021:** Researcher follows up with updates for ASF.

*December 8 per Bloomberg, December 9 per the Wall Street Journal

Good CVD in Log4Shell

Vulnerability disclosures fall between two extremes:

1. Disclose everything you know about a vulnerability to everyone as soon as you know it.
2. Never disclose anything you know about a vulnerability to anyone.

- **November 24, 2021:** Alibaba Cloud researcher discloses log4shell (l4s) to ASF privately.
- **December 8,* 2021:** Researcher follows up with updates for ASF.
- **December 10, 2021:** Patching and public announcements of l4s begin.

*December 8 per Bloomberg, December 9 per the Wall Street Journal

Not So Good CVD in Log₄Shell

- **December 22, 2021:** China's MIIT suspends Alibaba Cloud from an information-sharing partnership for failing to disclose I4s to the MIIT prior to DEC9, when they received notice from a 3rd party.
 - Per the Wall Street Journal and an anonymous source: **suspension was a consequence of breach of contract in the info-sharing partnership.**
 - Per other reporting:* **suspension was a consequence of violating *The Regulations on Management of Security Vulnerabilities (RMSV)*.**

*The SCMP and InfoSec Magazine, for example

The RMSV

- Specific enforcement mechanism aside, failure to disclose earlier to the MIIT was the cause of the suspension, and the letter of the RMSV was breached.

vulnerabilities in their products.

Article 7 Network product providers shall perform the following network product security vulnerability management obligations, ensure that their product security vulnerabilities are promptly patched and reasonably released, and guide and support product users to take preventive measures:

(1) After discovering or learning that there are security vulnerabilities in the provided network products, it shall immediately take measures and organize the verification of the security vulnerabilities, and evaluate the degree of harm and the scope of influence of the security vulnerabilities; for the security vulnerabilities existing in its upstream products or components, it shall immediately notify the relevant product provider.

(2) The relevant vulnerability information shall be submitted to the Network Security Threat and Vulnerability Information Sharing Platform of the Ministry of Industry and Information Technology within 2 days. The submitted content shall include the product name, model, version, and technical characteristics, harm, and scope of influence of the vulnerability that have network product security vulnerabilities.

Supply-Side Vulnerability Research

- Very little reporting on the RMSV when it was passed or took effect, big questions about application to multinational companies.
 - Only known (possible) RMSV enforcement is on Alibaba Cloud for I4s.
 - Most coverage concerned with what happens to vulnerabilities after the MIIT gets early access.
 - **Not the focus of this research.**
- **Convenient case study when searching for supply-shocks to international vulnerability research**
 - **Potential for a chilling effect on China's research contributions:**
 - Hesitation to report vulnerabilities until more legal clarity?
 - Internal policy changes regarding accepting vulnerability reports from China?
 - **Clear before and after dates**
 - **Large potential impact :**
 - China is a significant contributor to international vulnerability research

Other CVD and Reporting Laws and Practices

- A lack of clear legal protections for researchers has caused problems globally:
 - German researcher (almost) charged for reporting flaws in campaign app
 - Missouri tried to charge a researcher for reading HTML
- Some good developments here recently:
 - DOJ declining to prosecute good-faith research
 - ENISA push for member governments to develop CVD policies
 - CISA BOD for agencies to develop reporting systems

Research Question

- **Did the RMSV cause a supply shock in China's research contributions?**
 - If so, did that shock trickle into the overall supply of research contributions?
 - Do other shocks occur correlated to unidentified events?

Research Question

- **Added insights:**
 - Better look at external contributions to vulnerability reporting
 - Possible to look at density-distribution of contributors as well
- **Datasets:** Acknowledgements from different CVE and security update databases from Microsoft, Apple, F5, VMWare, and Red Hat
 - Looking across vendors to try to tease out product and ecosystem trends
 - Get variety of internal practices for crediting explicitly or anonymously and for organizing data (by CVE, by update batch, by vulnerability batch, etc.)
 - Open source and proprietary codebases

Key Dates

- **RMSV Timeline:**
 - **July 2020:** Draft law containing RMSV MIIT reporting requirement first reported as known to industry and government in China

Key Dates

- **RMSV Timeline:**
 - **July 2020:** Draft law containing RMSV MIIT reporting requirement first reported as known to industry and government in China
 - **July 2021:** RMSV passed

Key Dates

- **RMSV Timeline:**
 - **July 2020:** Draft law containing RMSV MIIT reporting requirement first reported as known to industry and government in China
 - **July 2021:** RMSV passed
 - **September 2021:** RMSV takes effect

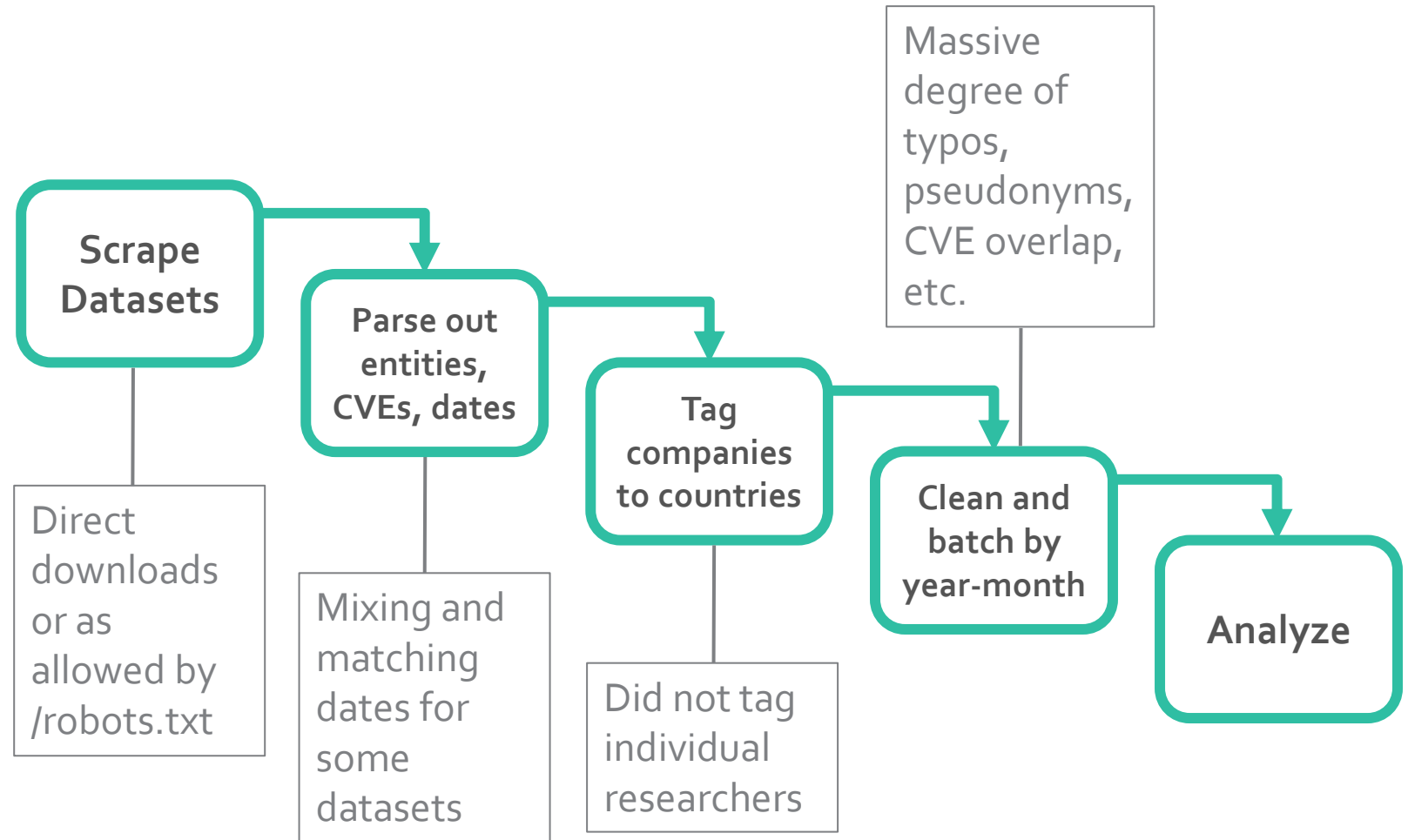
Key Dates

- **RMSV Timeline:**
 - **July 2020:** Draft law containing RMSV MIIT reporting requirement first reported as known to industry and government in China
 - **July 2021:** RMSV passed
 - **September 2021:** RMSV takes effect
 - **December 2021:** RMSV enforced publicly for first time (maybe)

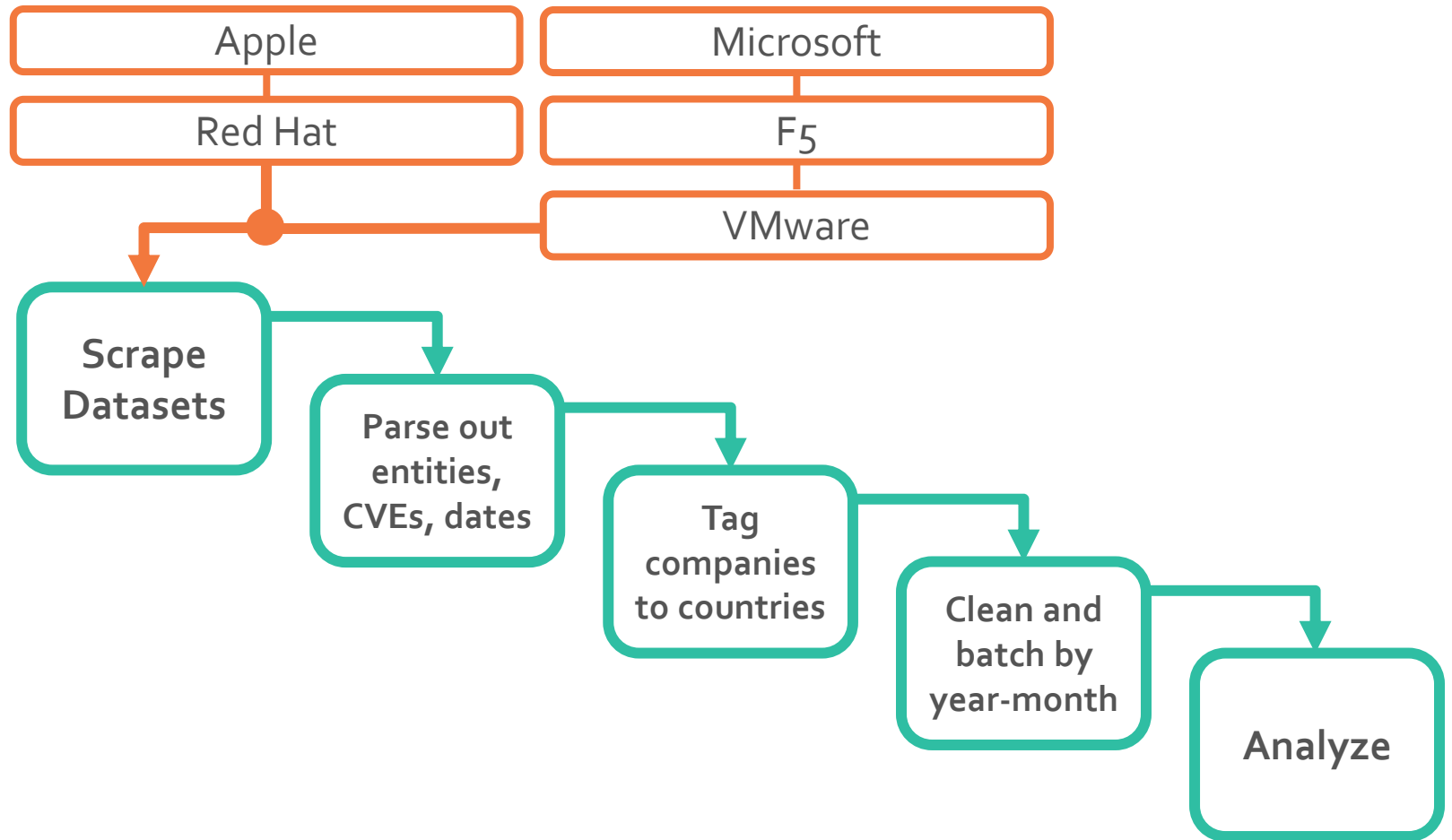
Key Dates

- **RMSV Timeline:**
 - **July 2020:** Draft law containing RMSV MIIT reporting requirement first reported as known to industry and government in China
 - **July 2021:** RMSV passed
 - **September 2021:** RMSV takes effect
 - **December 2021:** RMSV enforced publicly for first time (maybe)
- **Some confounding events:**
 - Summer 2020: Flurry of cyber regulations in China
 - Summer 2020: US blacklisting of companies in China accelerates
 - Summer 2021: More blacklisting

Methodology



Methodology



Methodology 3

- **Some quirks:**
 - Can't compare between datasets directly because of overlap in CVEs.
 - Apple security updates often predate listed dates for CVEs found on NVD, Tenable, etc., and are organized by software update.
 - Unclear where credits are all for vulnerability discovery or demonstration of vulnerability application of a specific product.
 - Batching by month adds noise.
 - Not clear how the delay between private reporting and public patching and acknowledgement plays out.

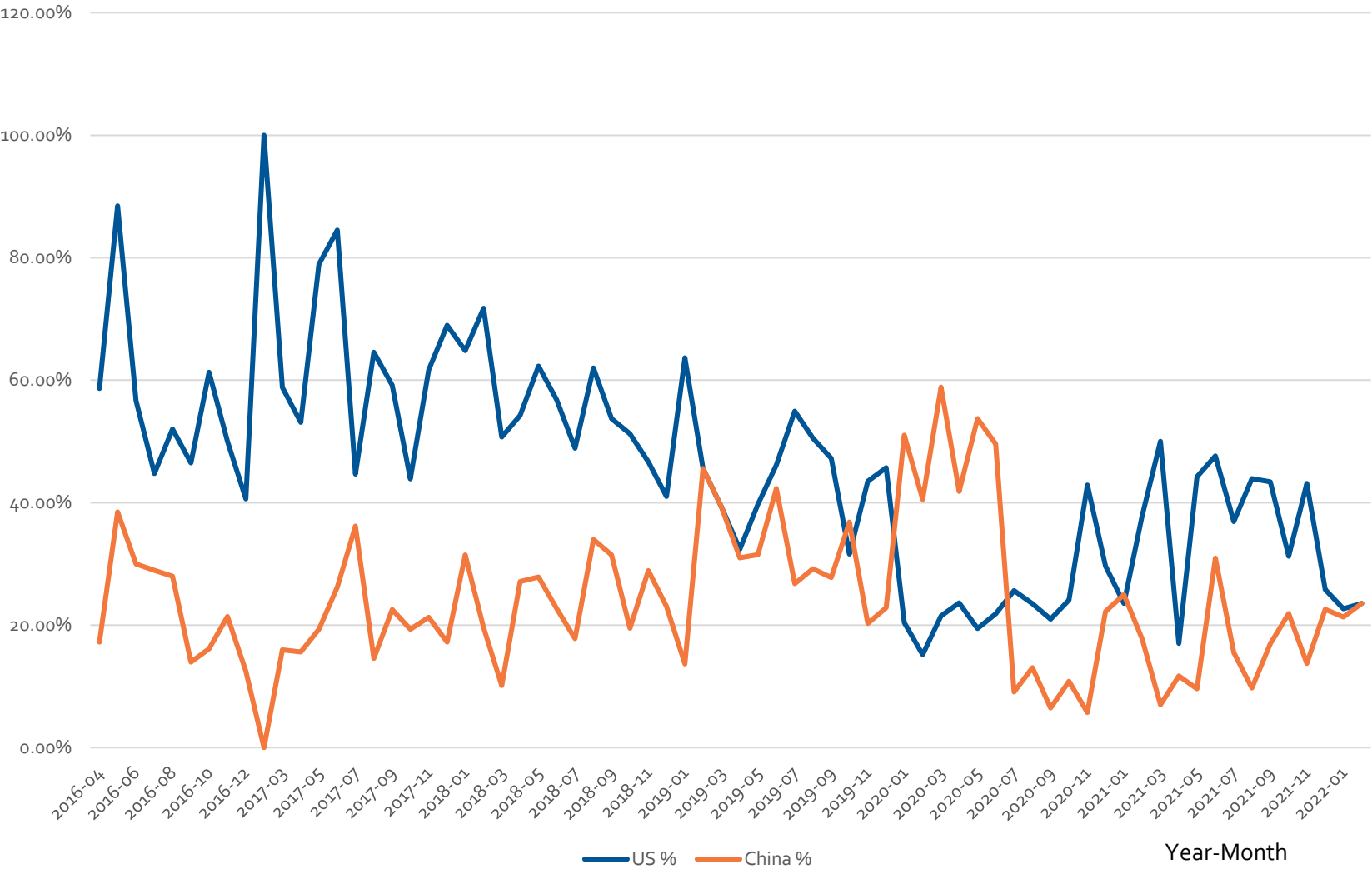
Datasets

- **Microsoft: n = 4355**
- Apple: n = 14740
- VMWare: n = 1363
- F5: n = 335
- **Red Hat: n = 3307**

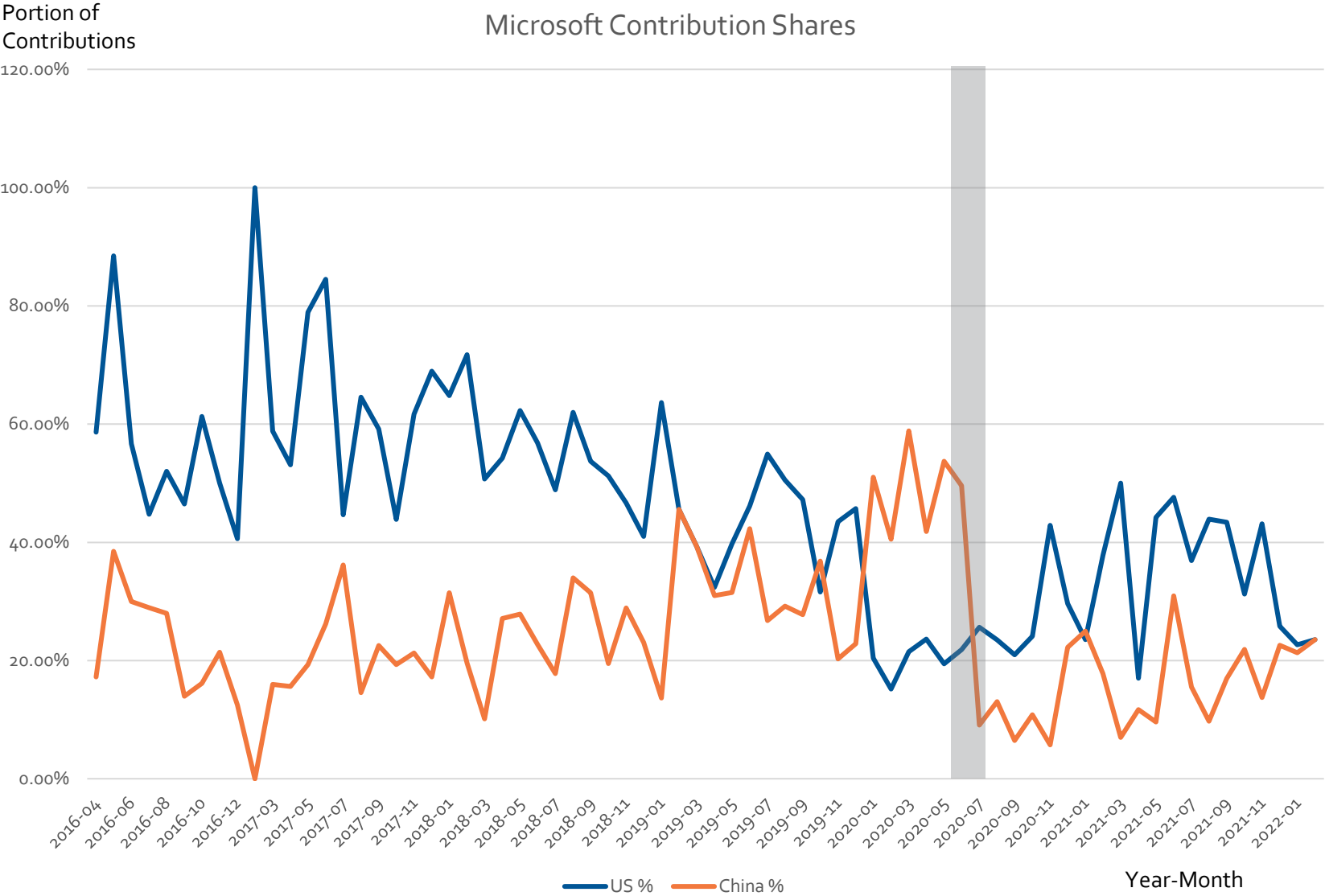
Microsoft Contributions

Portion of Contributions

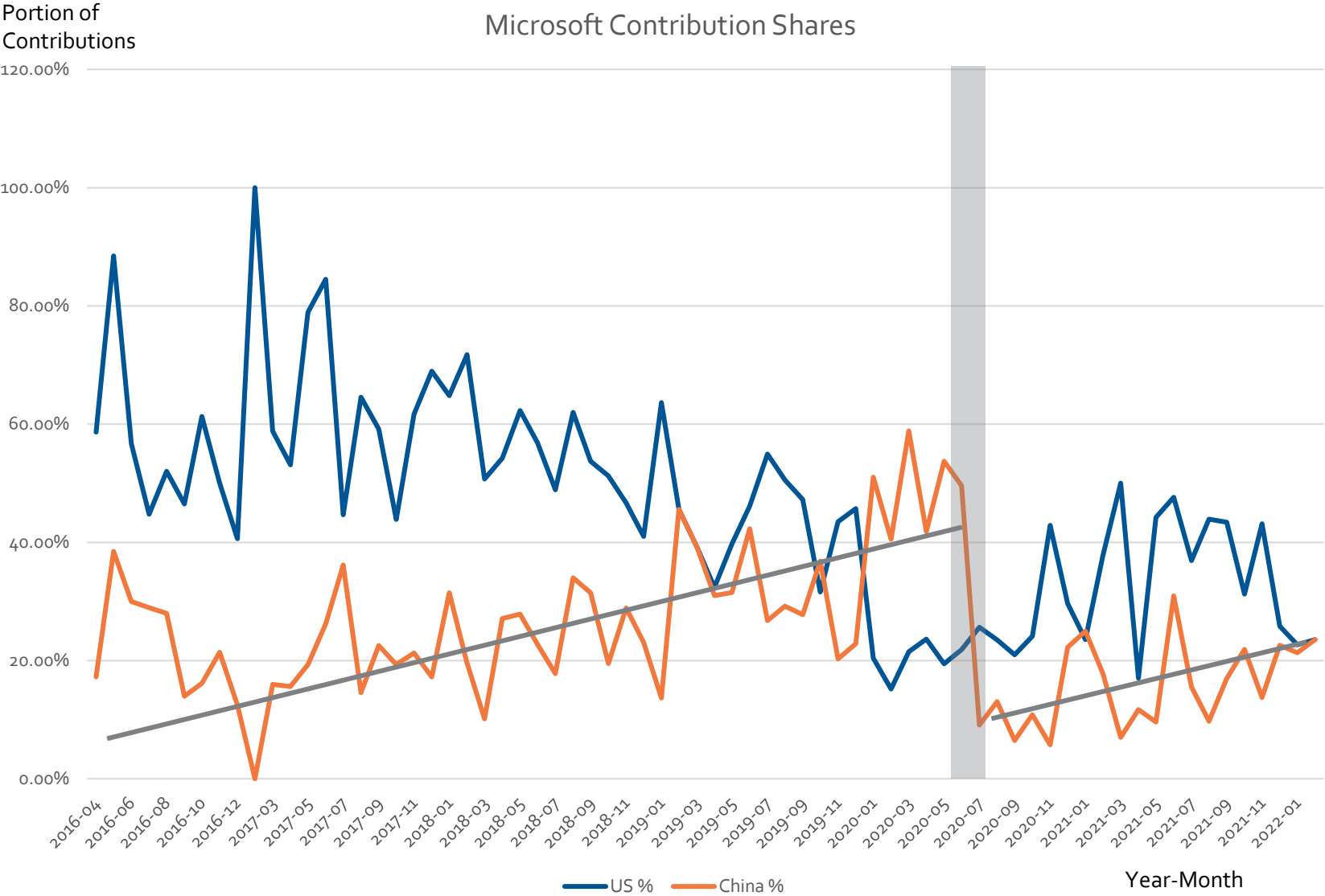
Microsoft Contribution Shares



Microsoft Contributions

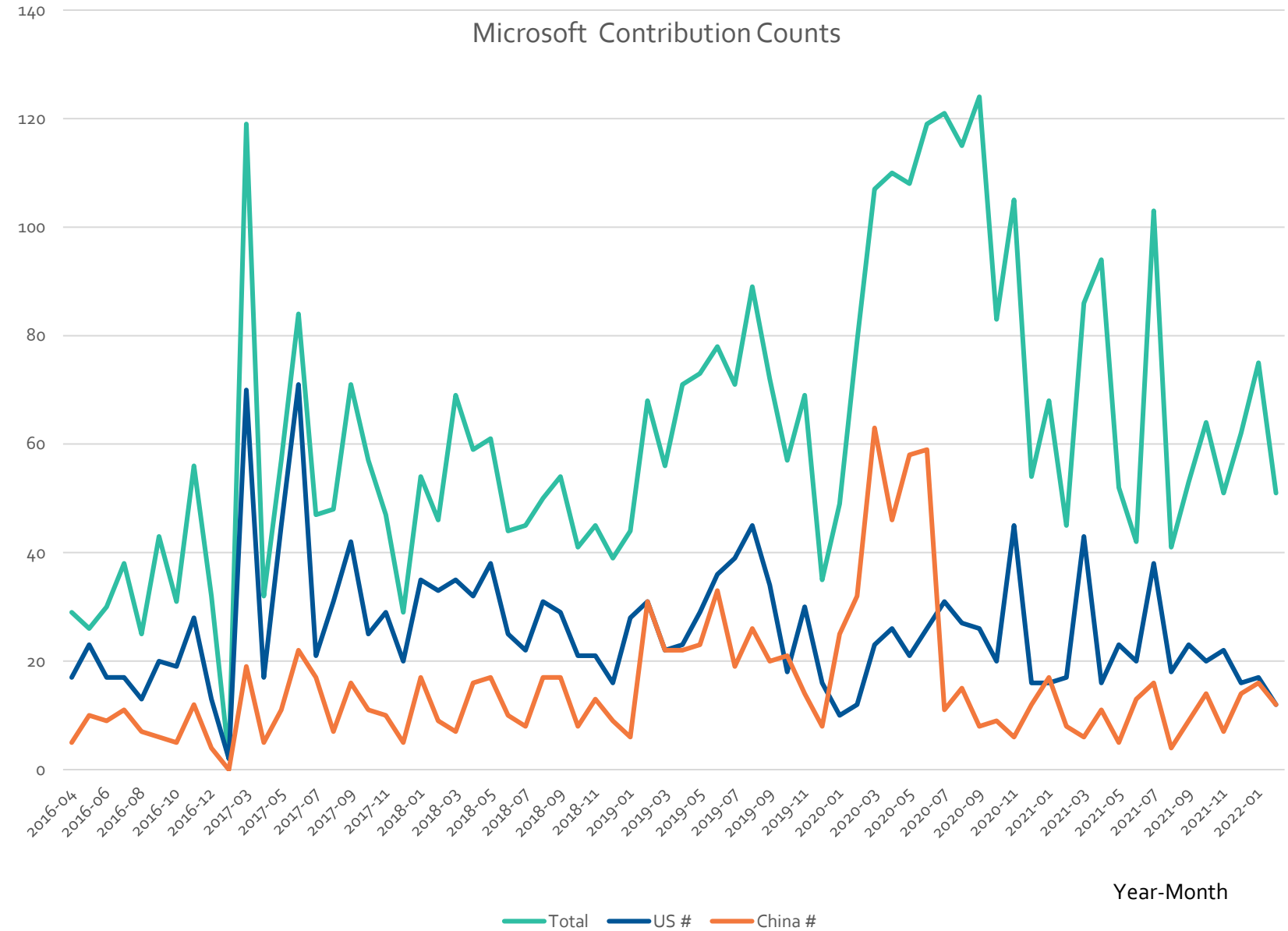


Microsoft Contributions



Microsoft Contributions

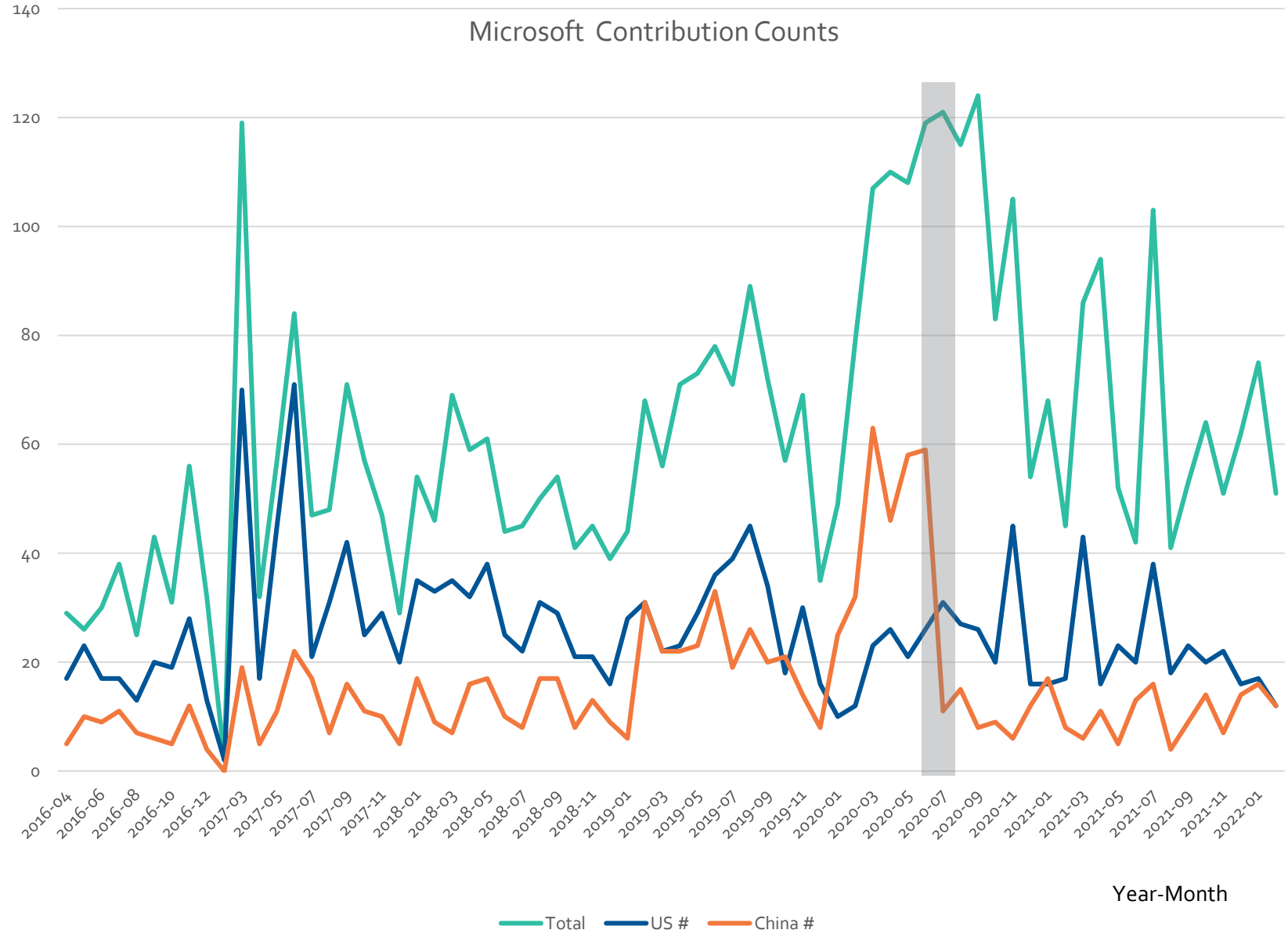
Contributions



Year-Month

Microsoft Contributions

Contributions

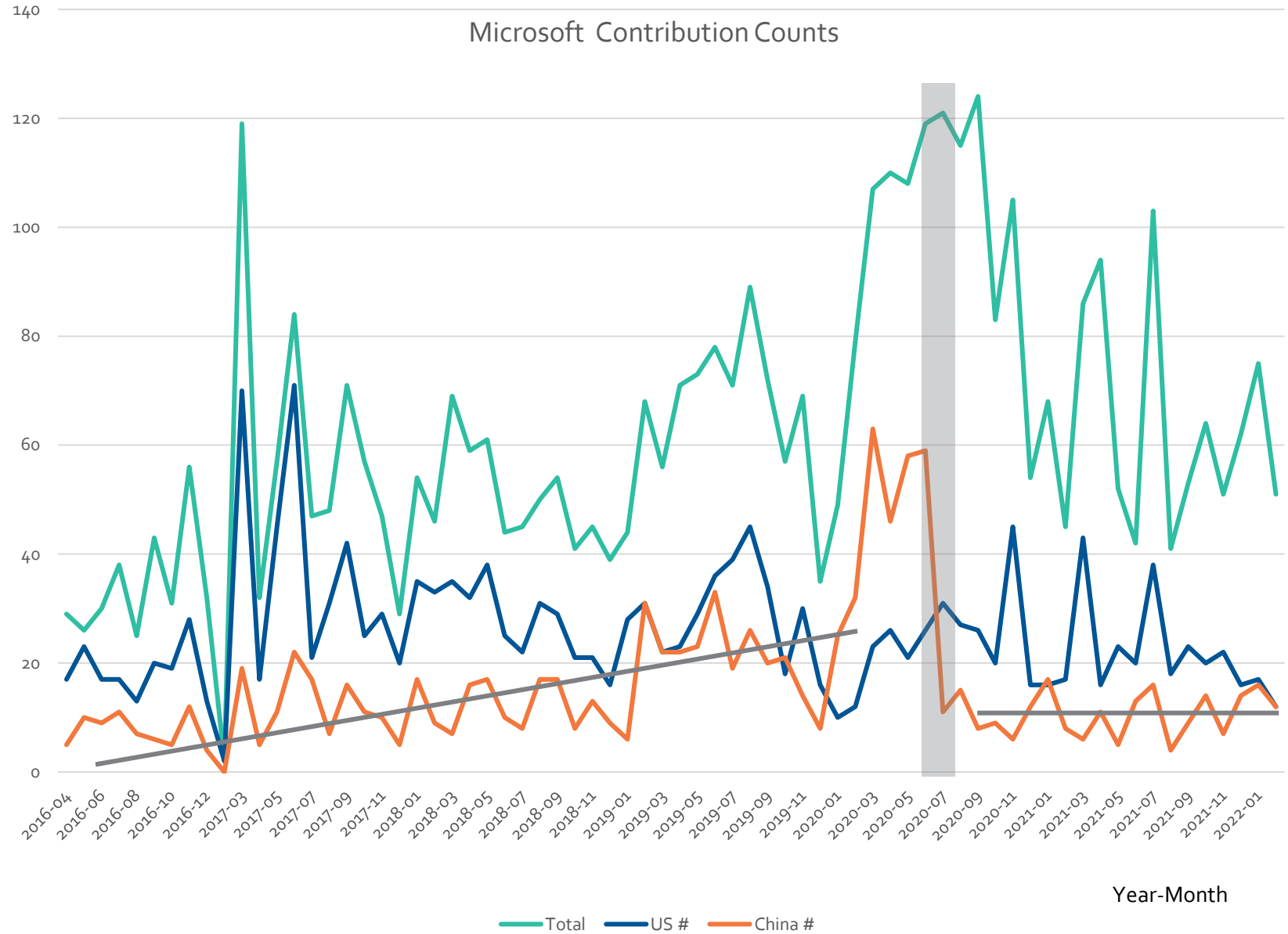


Year-Month

— Total — US # — China #

Microsoft Contributions

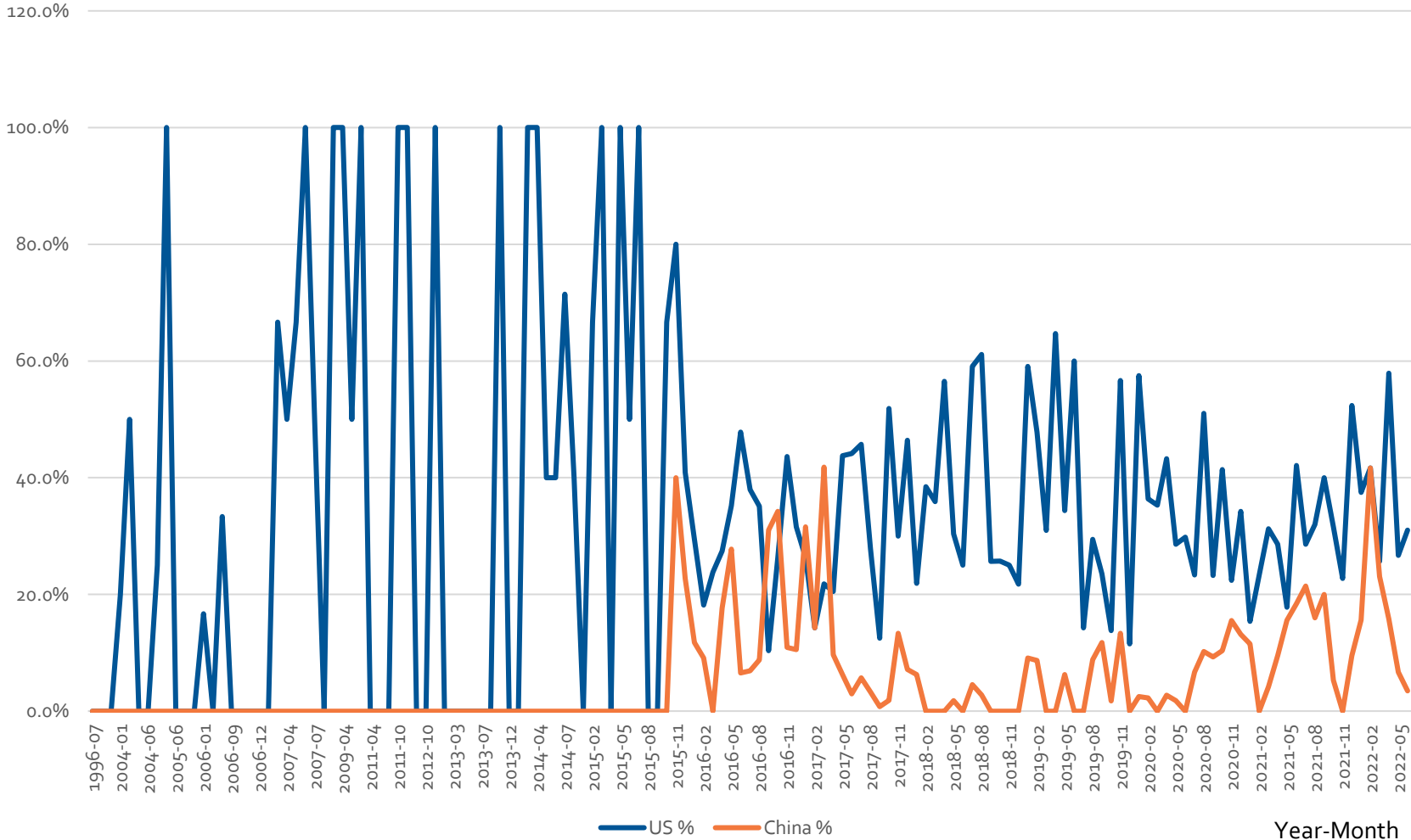
Contributions



Red Hat Contributions

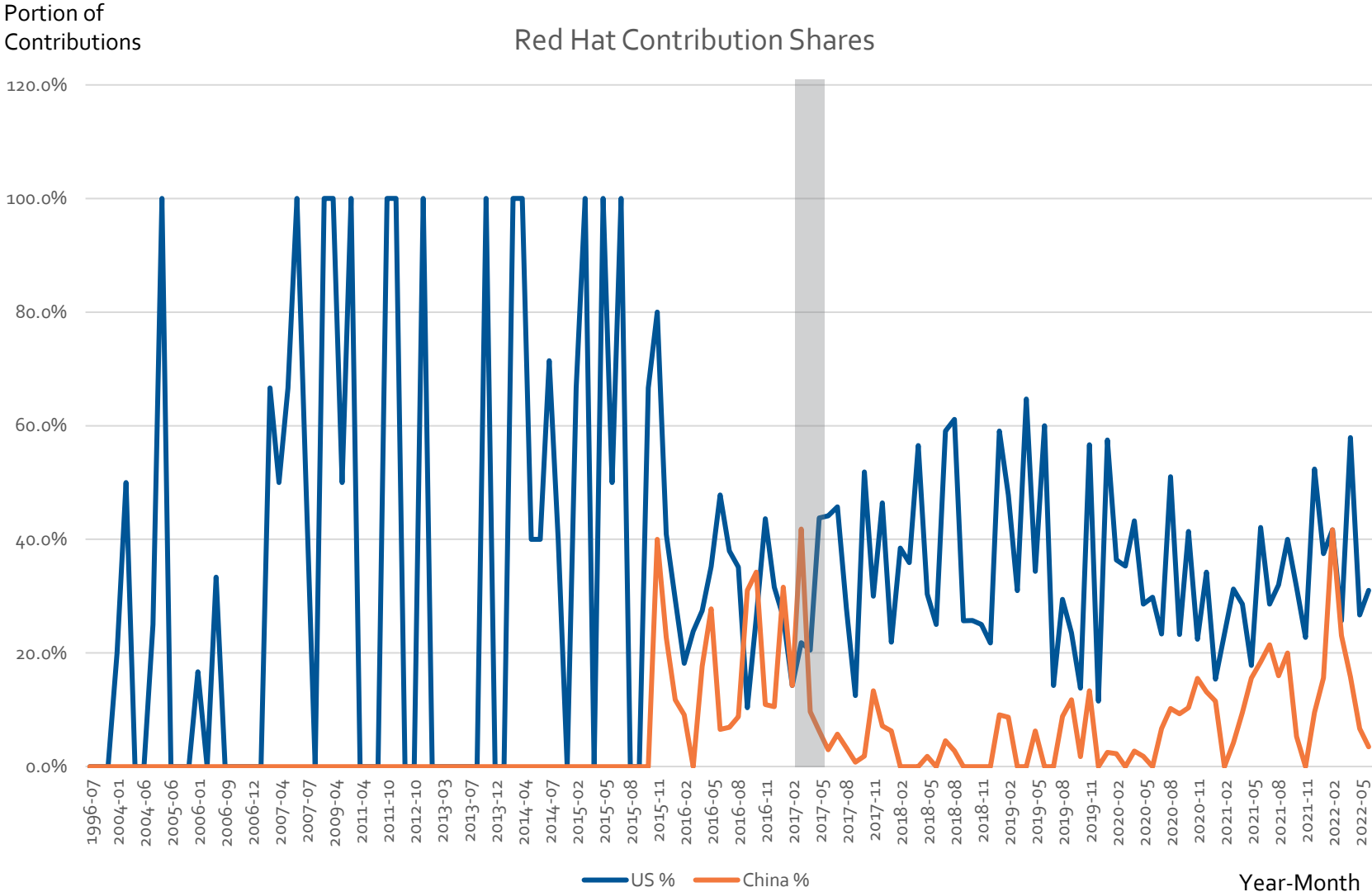
Portion of Contributions

Red Hat Contribution Shares

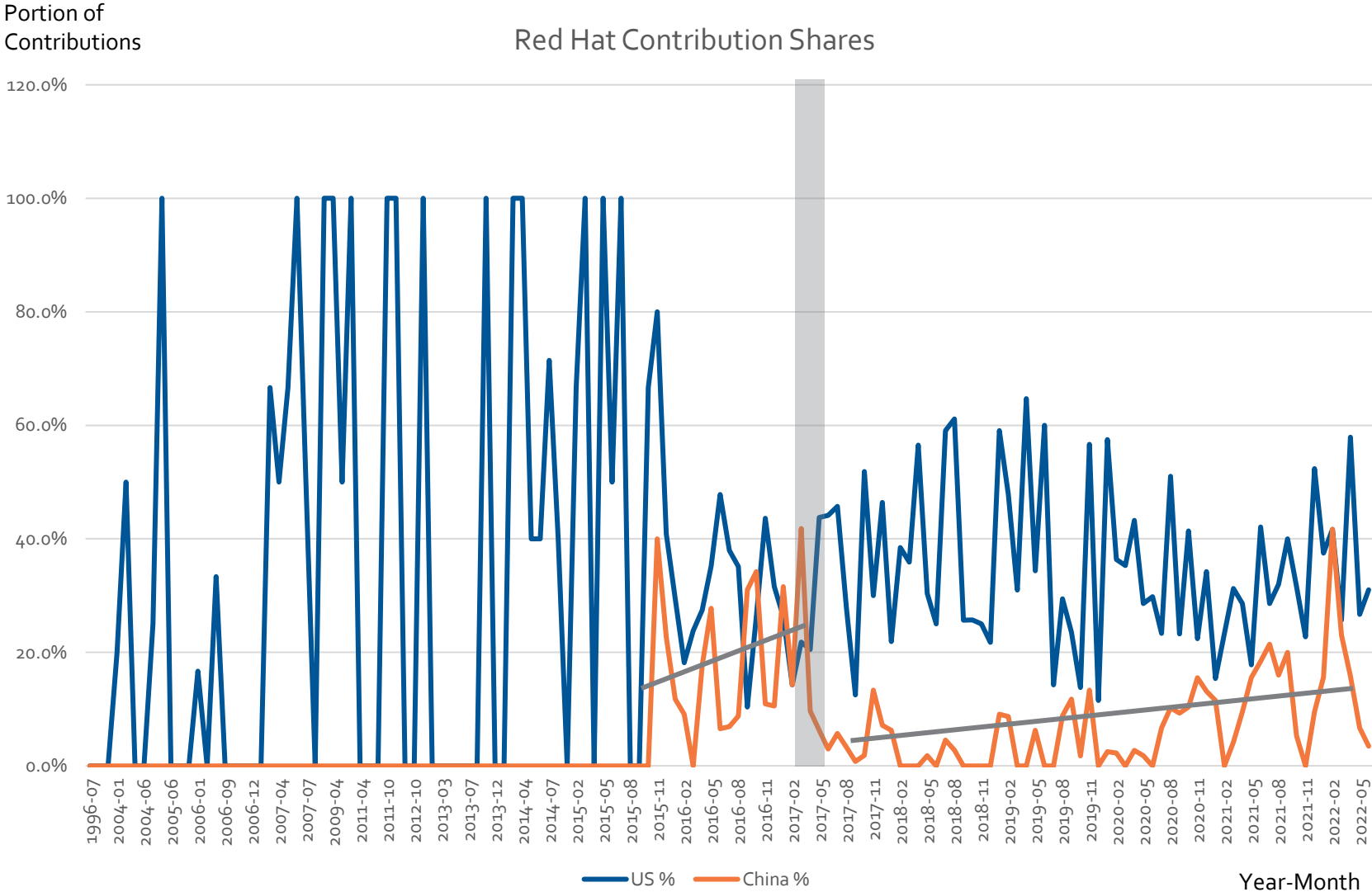


Year-Month

Red Hat Contributions



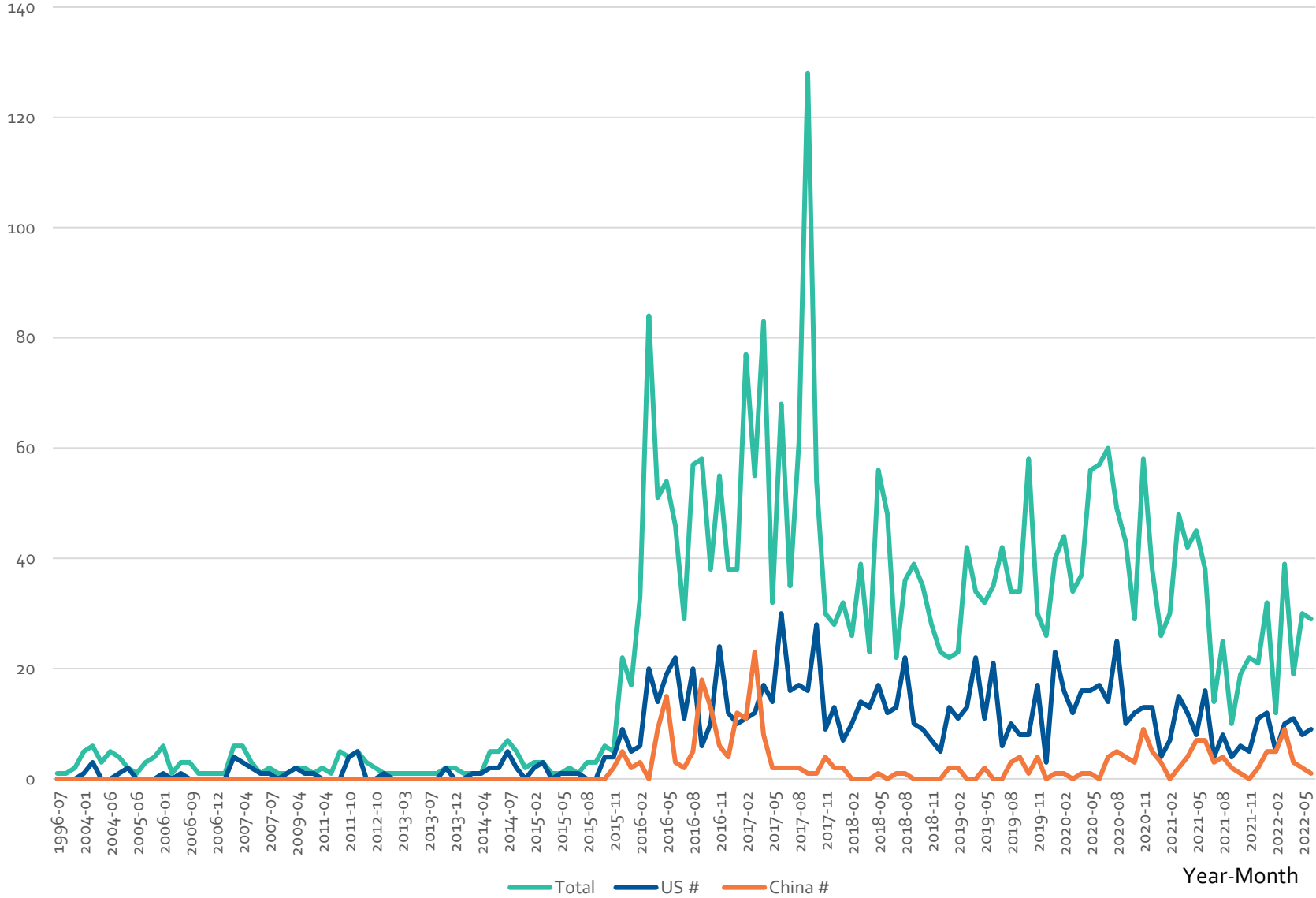
Red Hat Contributions



Red Hat Contributions

Contributions

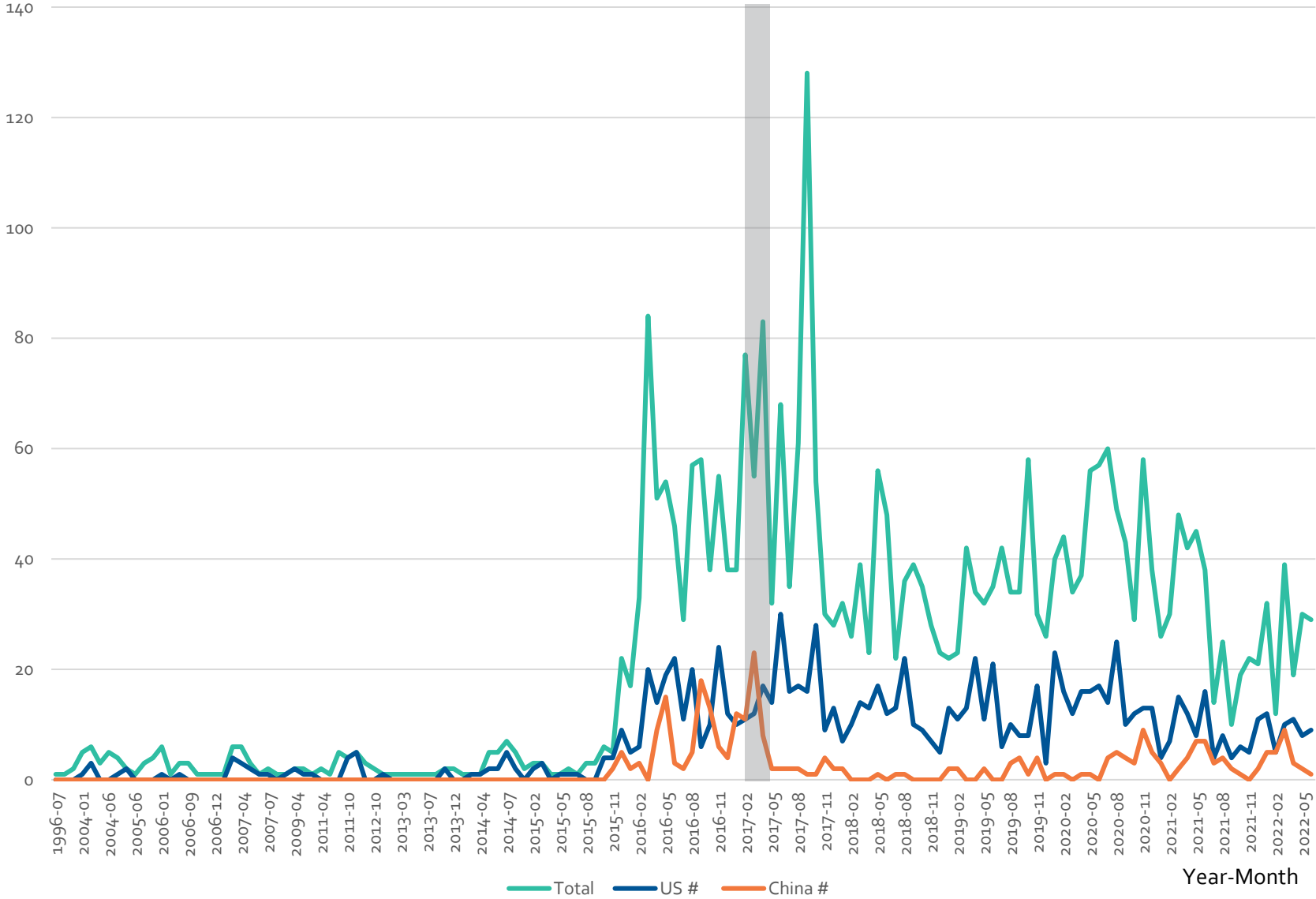
Red Hat Contribution Counts



Red Hat Contributions

Contributions

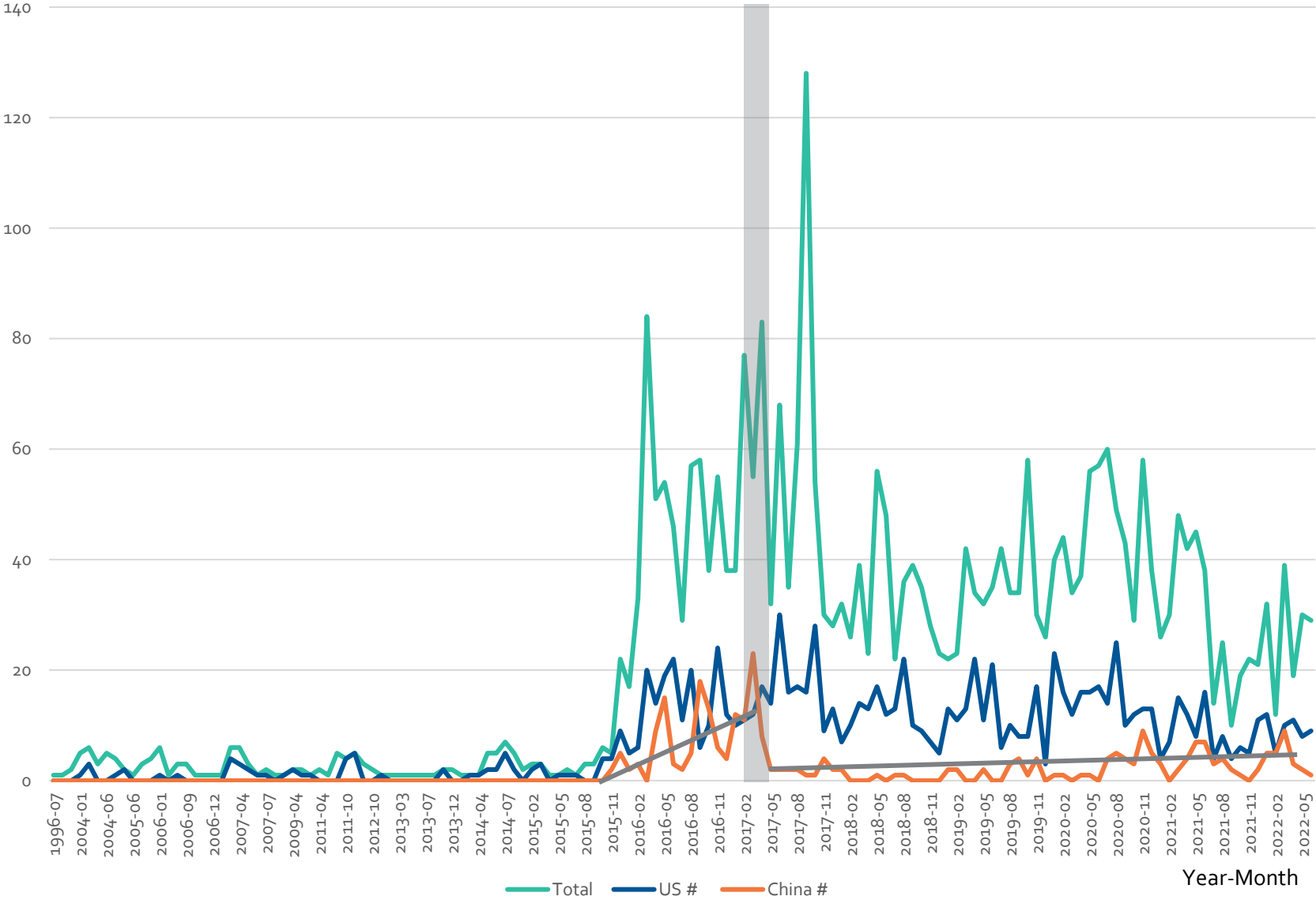
Red Hat Contribution Counts



Contributions

Red Hat Contribution Counts

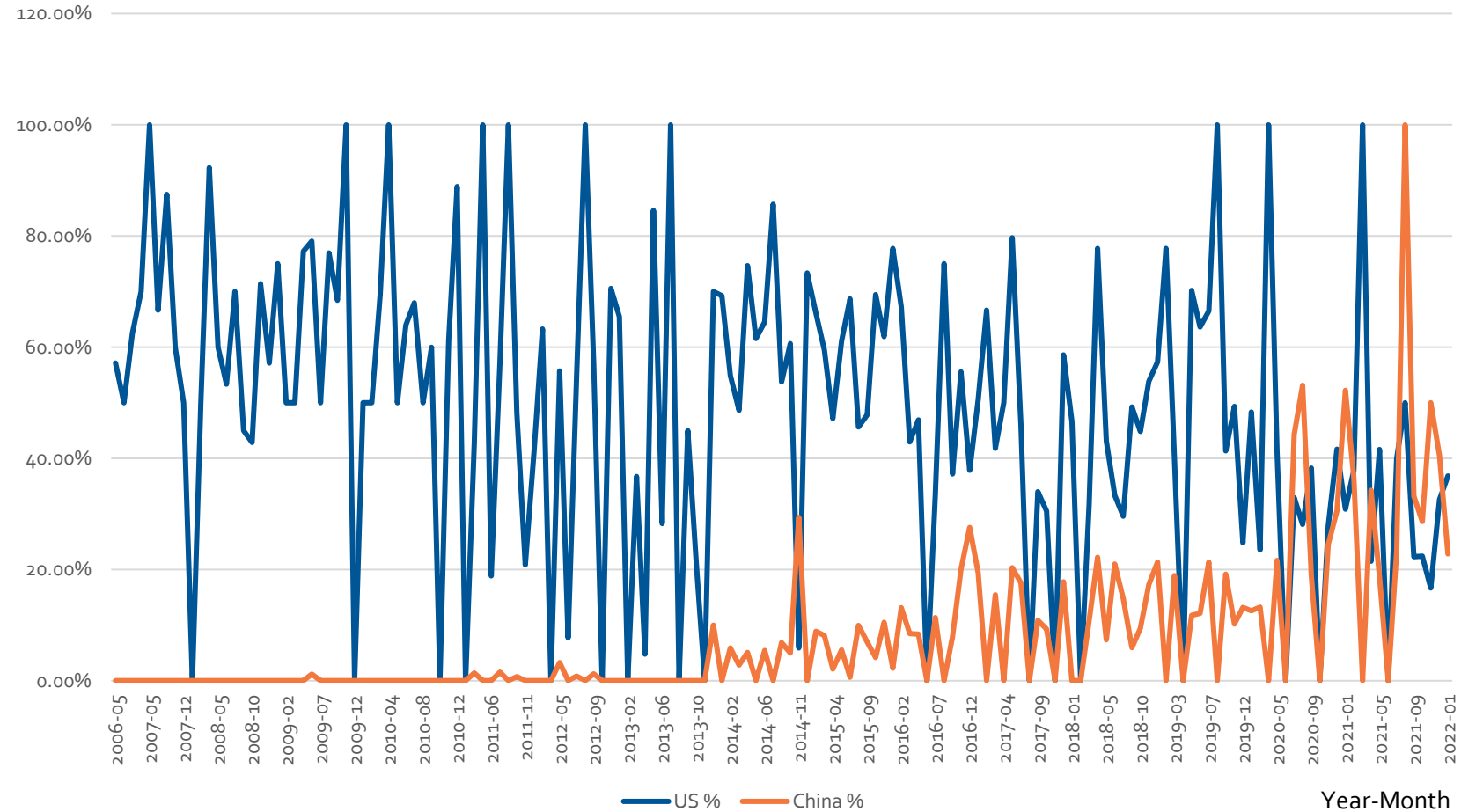
Red Hat Contributions



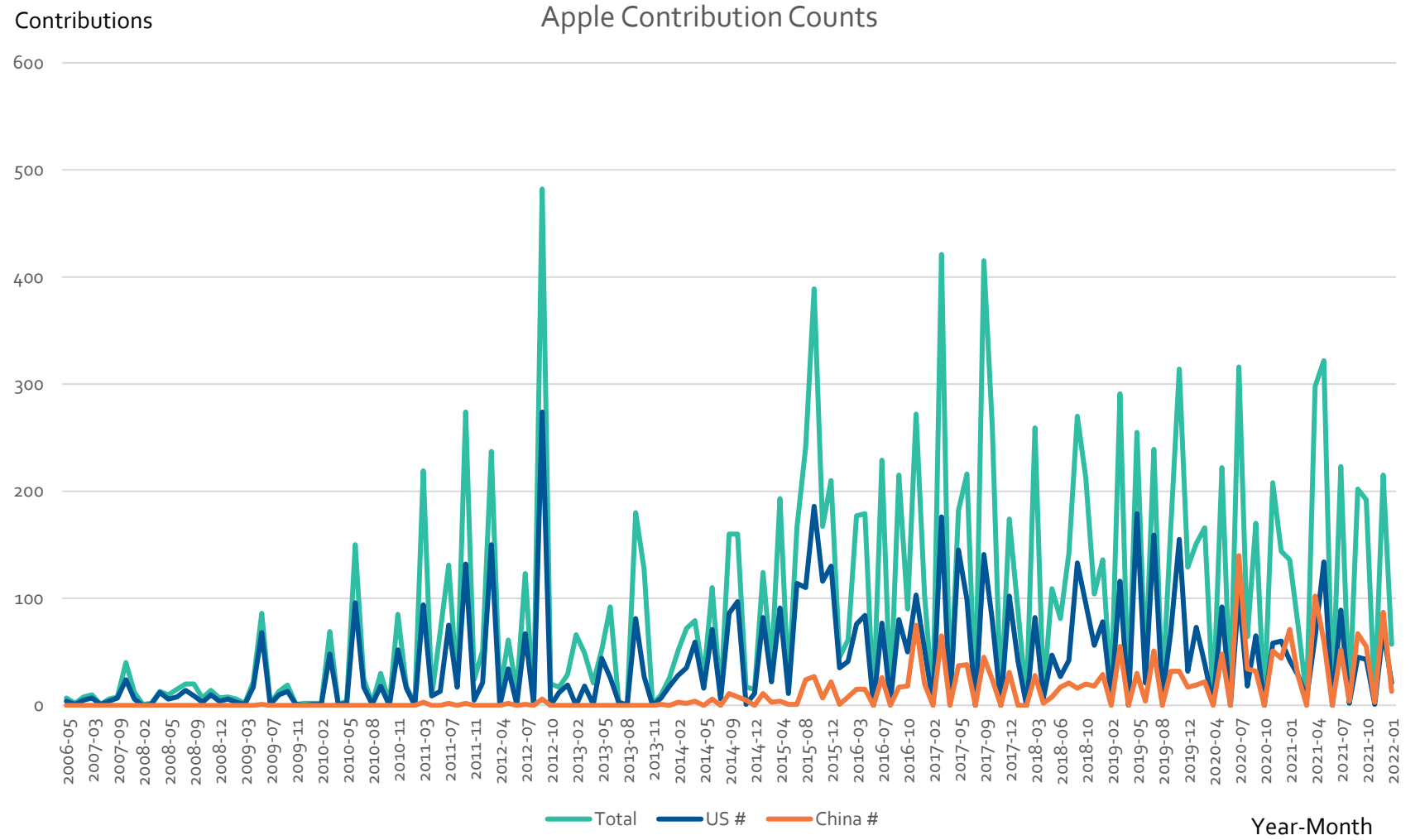
Apple Portions

Portion of Contributions

Apple Contribution Shares



Apple Contributions



Takeaways

1. **No clear, universal supply shock from the RMSV in China, though maybe a local one** in the Microsoft data.
2. Something that looks like a supply shock happened in the Red Hat data but not at a time with a clear correlated event.
3. Contribution trends differ greatly among company, code, and product environments.
4. A supply shock in a specific legal context doesn't necessarily trickle into the whole ecosystem, though loss of growth is difficult to assess.
5. **Companies and government can better protect research communities and insure against shocks—can't assume their absence.**

Recommendations

- Opportunity for a policymaking reset to invest in research community and increase its resilience
- **Harmonized vulnerability disclosure practices across the US and allies and partners**
- **Improve support for vulnerability discovery tools**
- **Better track vulnerability disclosure flows and incentivize research in areas where contributions fall off**

Summary

- Consider vulnerability research as a source of security, a supply and a community to be invested in and protected.
- Is the research community vulnerable to supply shocks? Probably, but the mechanisms are still unclear, especially over long timeframes.
- There is some limited evidence for local supply shocks, though they did not seem to spread from one set of researcher entities to the larger ecosystem or even between code and product environments.
- There are ways to invest in the research community and build in resilience. Fragmenting it is also possible and would hurt overall security.

Thank you!

Full Draft Report: <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>

Questions?

sscott@atlanticcouncil.org

therr@atlanticcouncil.org