Remediating Conficker Via Automated Customer Notifications

Sara Roper, CISSP, GISP
Lead Technical Support Engineer
CenturyLink Managed Security Services, Abuse

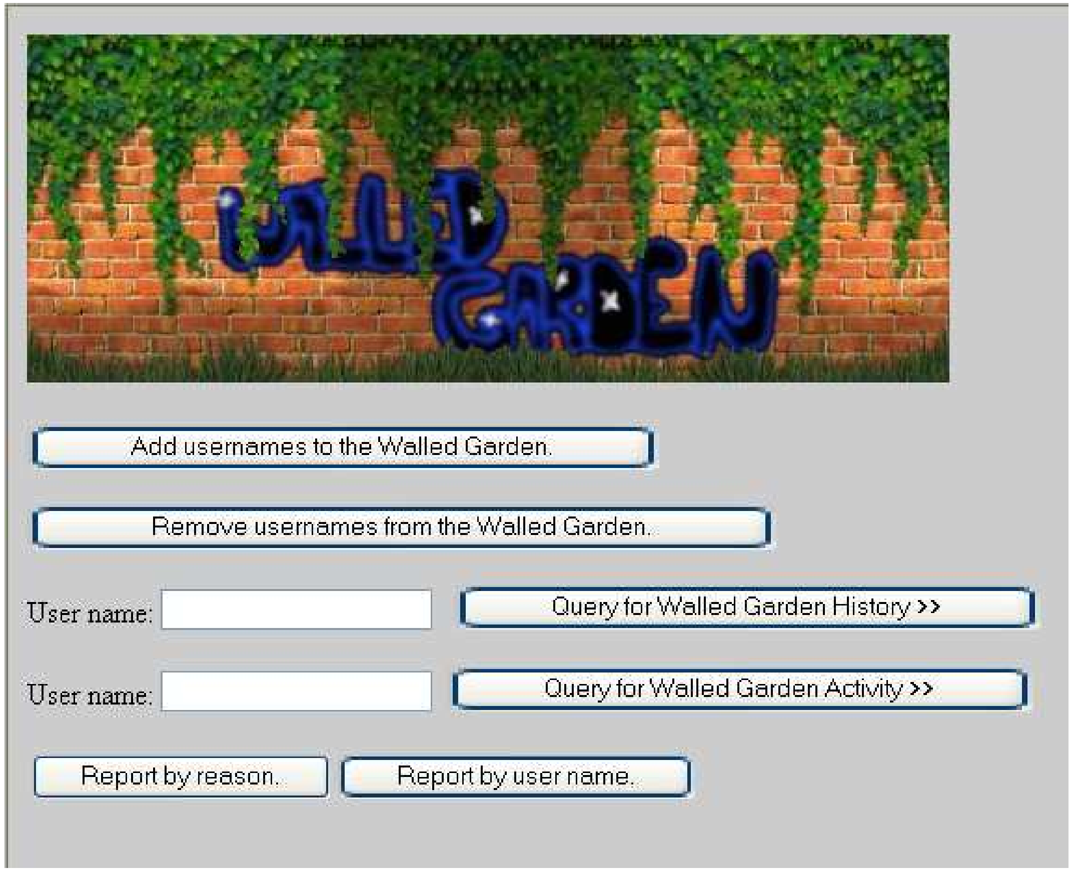
Don Smith, GIAC
Senior Staff Engineer
CenturyLink Technology Management

Prepared by:
Daryl Johnson
Matt McMillon
Don Smith GIAC
Sara Roper CISSP GISP

Agenda

- Walled Garden method and approach
- Walled Garden (WG) trial
- WG usage, analysis and survey results
- Other results
- Conclusion

Walled Garden Method and Approach


WALLED GARDEN
Add usernames to the Walled Garden.
Remove usernames from the Walled Garden.
User name:
Query for Walled Garden History >>
User name:
Query for Walled Garden Activity >>
Report by reason.
Report by user name.

Walled Garden Notification

- Special Conficker instance of the Walled Garden
- Locally hosted MSRT
- “Quick Out” -> remove virus later

Conficker Walled Garden Trial

- Trial run 3/11/09 to 3/25/09
- Version of Conficker infection unknown variable
- Data set of 455 unique users were used to identify initial repeat infection rate
- 71 others were added at the end of the trial but we could not collect the data on them regarding repeat infections because the trial ended before there was a two-week period since they were put in the WG

Initial Repeat Infection Rate

- 13% of the users were put into the Walled Garden twice
  - During the trial 31 users entered 2 times out of 455 total WG users
  - Users who entered twice were noted and identified as having repeat infections

Two Week Repeat Infection Rate

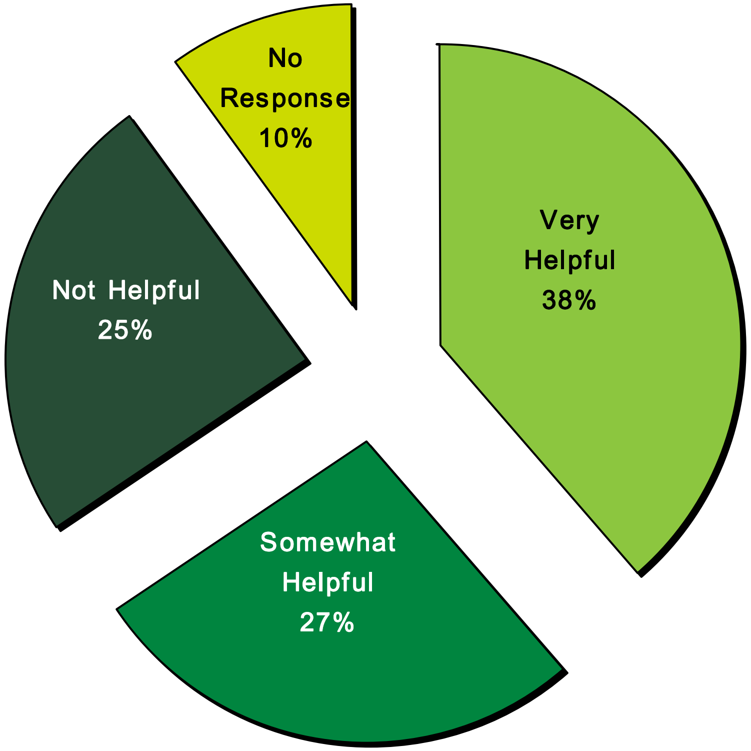
- Repeat infection query performed from data obtained through 4/10/09
- Most users did not appear as having repeat infections

Survey Results

- Survey submissions are optional
- People tend to take surveys when they're upset

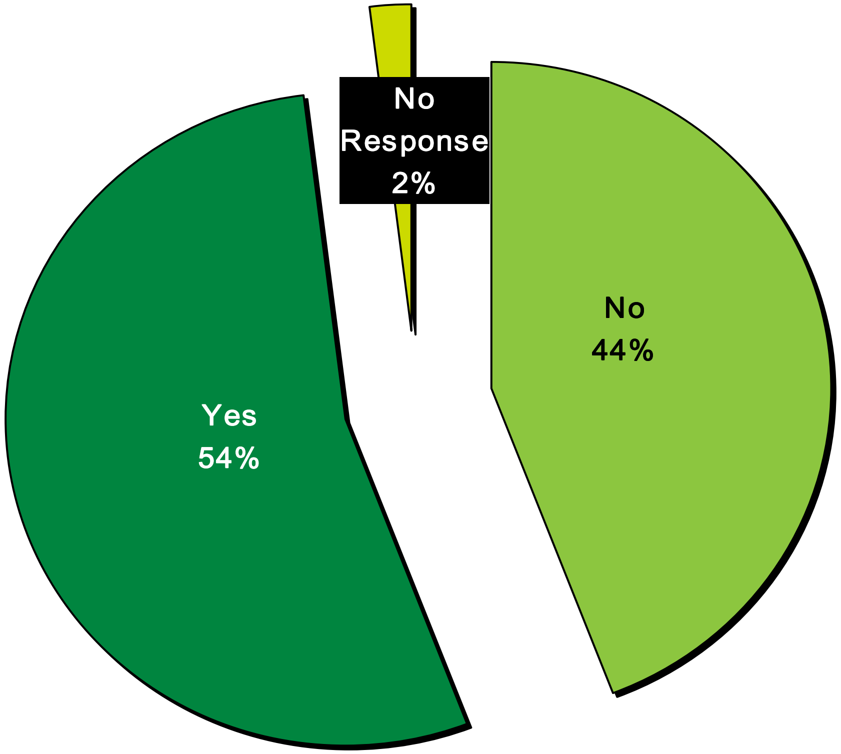
Survey Analysis

- Overall, how helpful was the notification?



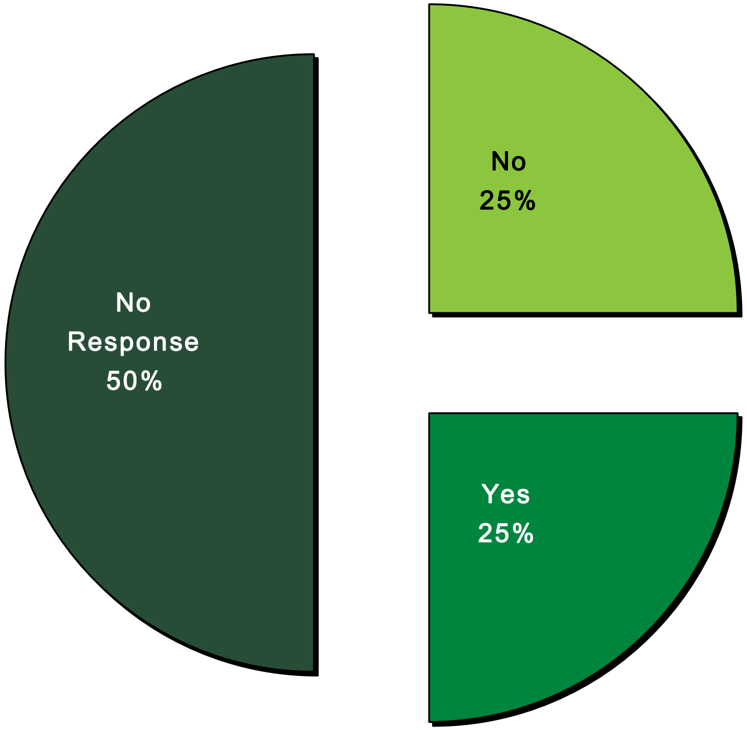
Survey Analysis

- Did you use the recommended tools and do a complete scan of your computer?



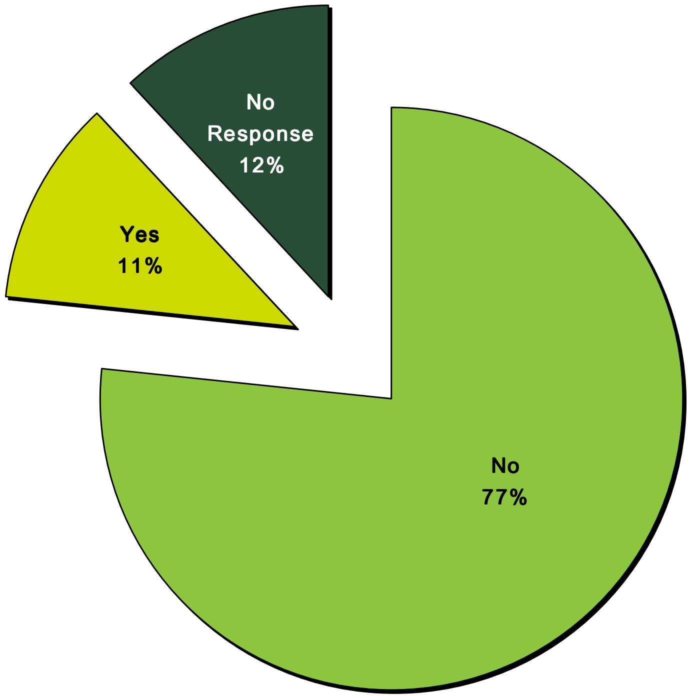
Survey Analysis

- Did you find a virus or other type of malicious software on your computer as a result of this notification?

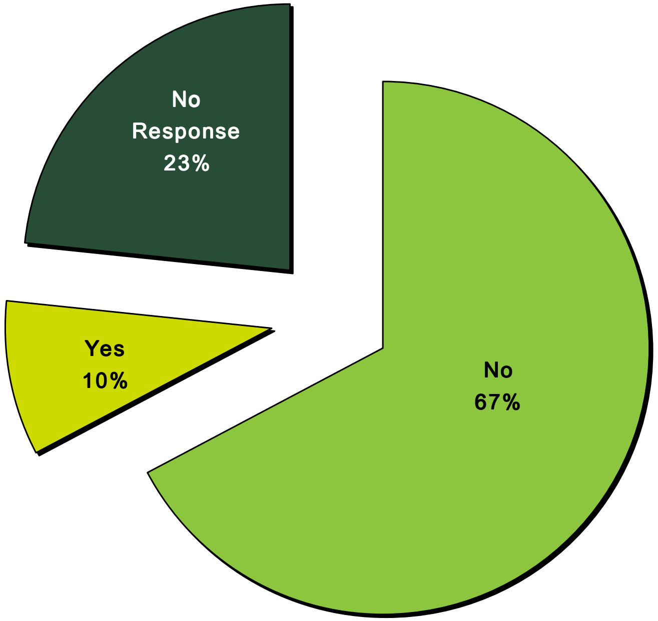


Survey Analysis

- Did you have to call us for support to guide you through this process?

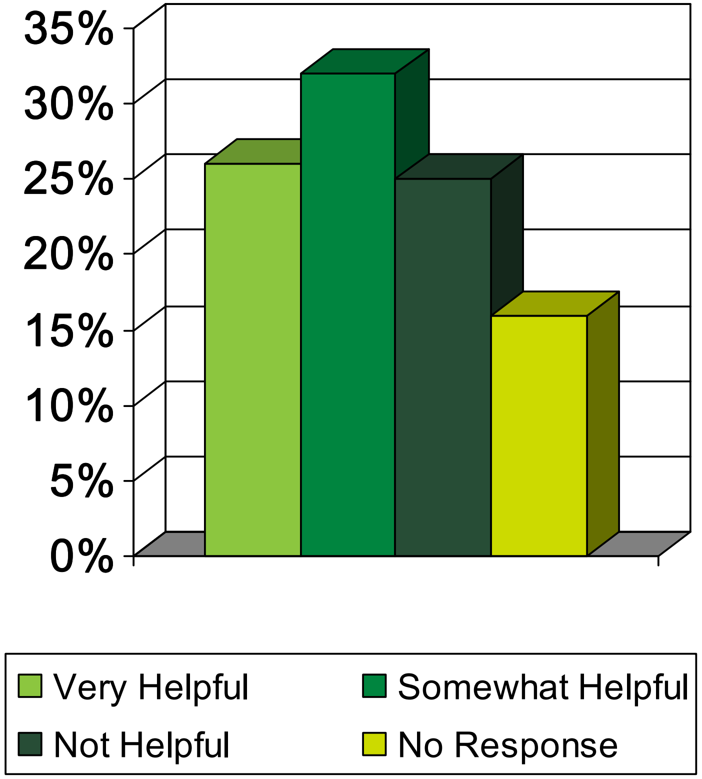


- Did you have to call your antivirus software provider or a local helpdesk for support?



Survey Analysis

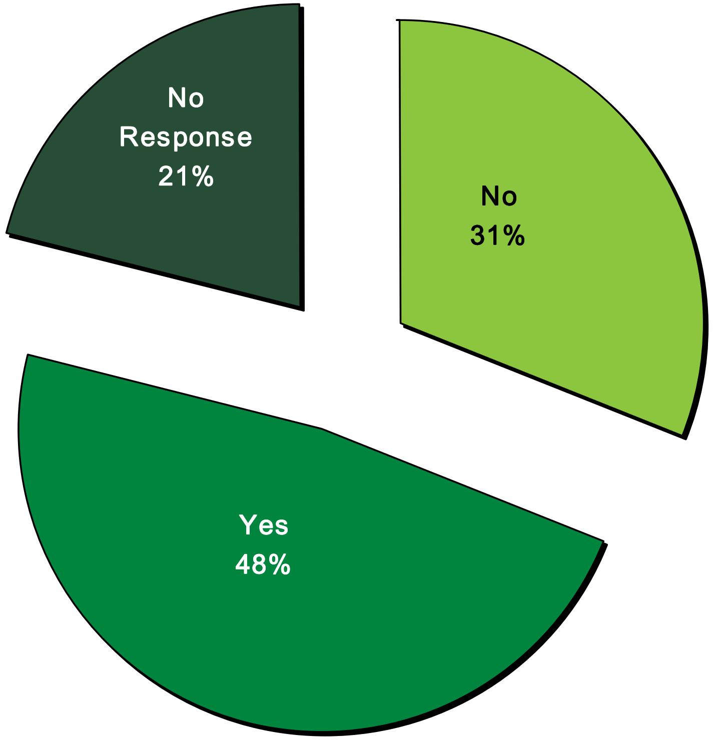
- How helpful was the information and links that were provided in removing the virus infection?



CenturyLink™

Survey Analysis

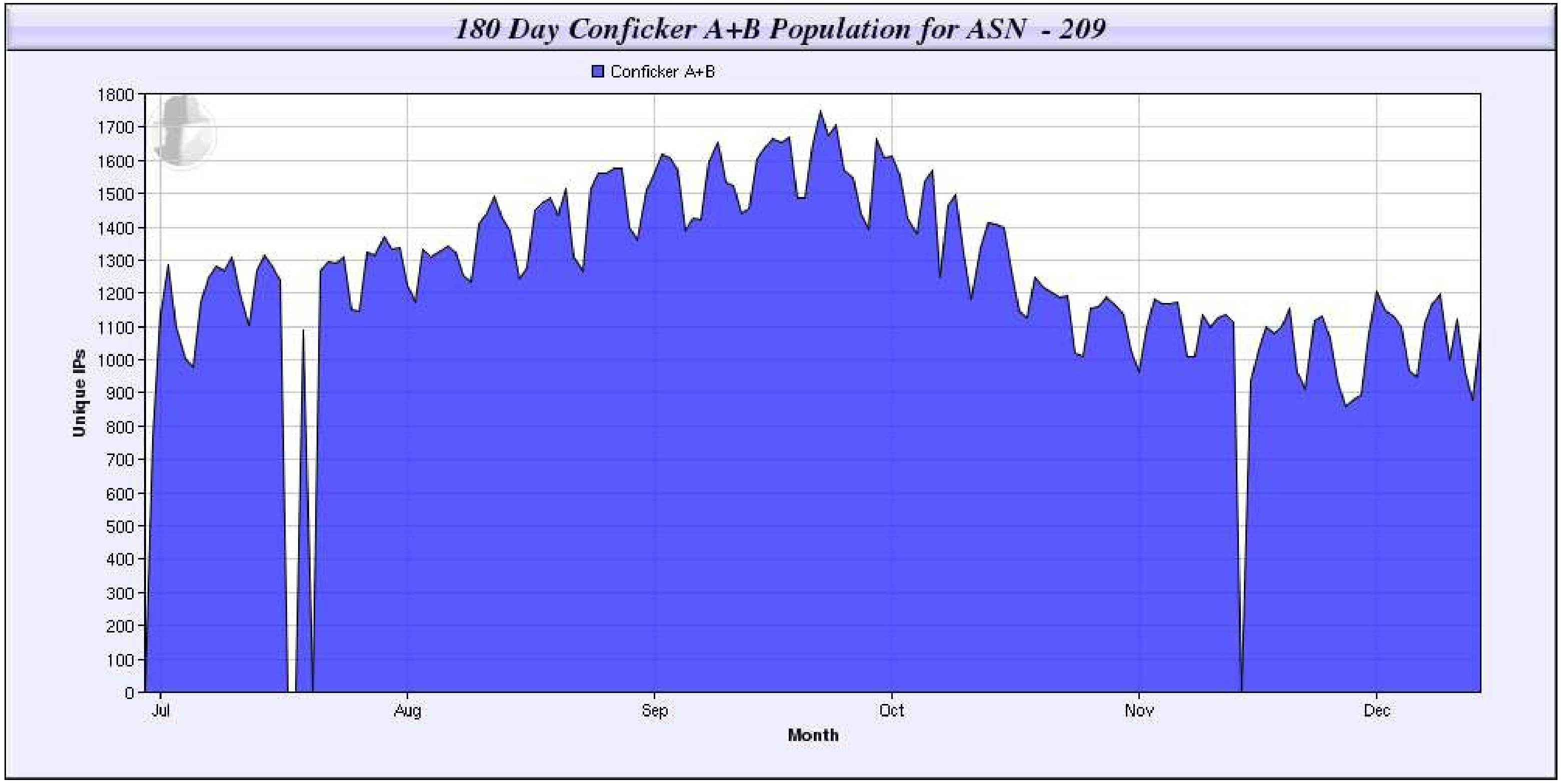
- Do you view (your provider) in a more positive manner as a result of this notification?



Survey Analysis

- Did you use the recommended tools and do a complete scan of your computer?
  - Only the customers that reported using the tools found a virus or malicious software.
- “Overall, how helpful was the notification?” 63% of the people that reported “Very Helpful” to this question used the recommended tools.
- 46% of those who used the recommended tools found a virus.
- 56% of the respondents that reported finding a virus reported "Very helpful" on the “overall” question.
- 22% of the total respondents reported finding a virus.

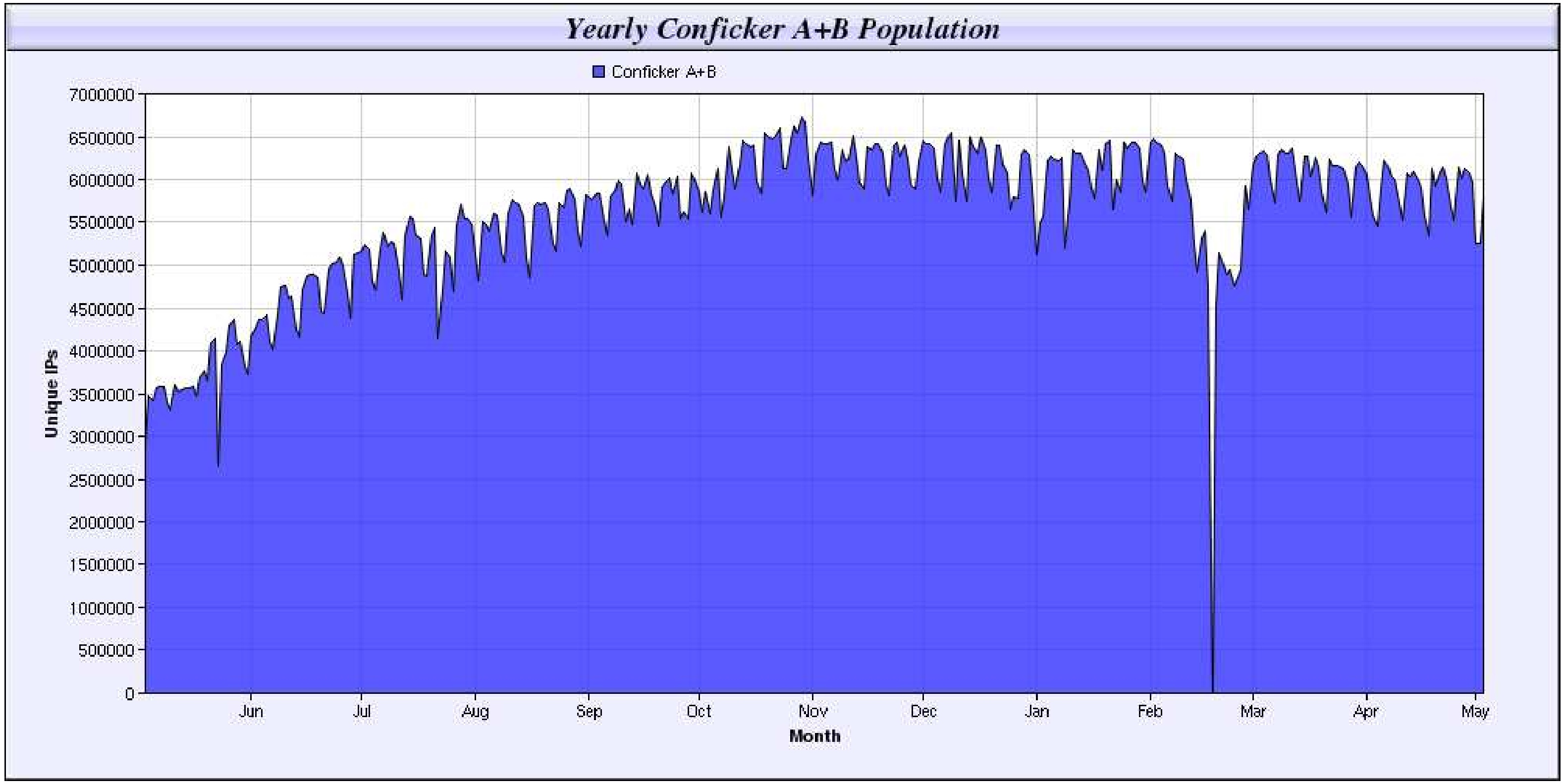
Shadow Server’s Conficker Graph, AS 209



http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

Shadow Server's Conficker Graph

Worldwide, Conficker infection rates were still increasing



- Note the large valleys in the graphs are due to missing sinkhole data.

http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

Walled Garden Notification Conclusion

- We believe locally hosting MSRT assisted our customers in malware detection and removal for this malware family.
- Only the customers that ran the offered tools found a virus.
- Since Conficker blocked nearly all antivirus and removal tool sites, the locally hosted MSRT tool would have been nearly the only way that Conficker infected users would be able to remove the malware effectively.

Questions?