TwC Next
Marking a Milestone.
Continuing Our Commitment.

Microsoft | Trustworthy Computing

# European Telecom Uses Microsoft Security Data to Remove Botnet Devices from Network

TeliaSonera
www.teliasonera.com

**Country or Region**

Finland

**Industry**

Telecommunications

**Customer Profile**

TeliaSonera, which has nearly 29,000 employees, is one of the largest telecom operators in Europe, serving 164 million customers.

**Business Situation**

As an Internet service provider, TeliaSonera needed an efficient way to identify devices that have been infected by malware and drawn into robotic networks (botnets) to distribute spam, infect other computers, and create damage in other ways.

**Solution**

After the Microsoft Digital Crimes Unit (DCU), working with law enforcement and other parties, took down the Rustock botnet, TeliaSonera used data from the DCU to identify infected devices and block them from its network until they were cleaned.

**Benefits**

- Safer networks with botnet takedowns and cleanup
- Low cost of implementation
- Happier customers – especially businesses
- Better network performance
- A safer Internet

**Hardware**

Intel-based servers

Finland is known as having networks with the fewest malicious software (malware) infections, and within Finland, the telecommunications company TeliaSonera prides itself in being the “cleanest of the clean.” The company earned its reputation for safe computing by creating an automated monitoring and alerting system to identify infected devices, alert their owners, and remove the devices from the network until cleaned. However, TeliaSonera found it difficult to identify computers that had been infected and drawn into a network of compromised systems—or botnet. After the Microsoft Digital Crimes Unit worked with law enforcement to take down the Rustock botnet, TeliaSonera used IP addresses of infected devices found by Microsoft to notify customers their systems had been infected so that action could be taken to resolve the problem. TeliaSonera customers value the enhanced security.

**Situation:**

TeliaSonera, based in Stockholm, Sweden, is the largest telephone company and mobile network operator in Sweden and Finland, and Europe’s largest carrier of Internet Protocol (IP) traffic. Formed by the 2002 merger of the Swedish and Finish telecommunications companies Telia and Sonera, the company focuses on offering its customers a  world-class customer experience across its operations which range from the Nordic and Baltic countries to Nepal, including Russia, Turkey, Spain, and several other nations.

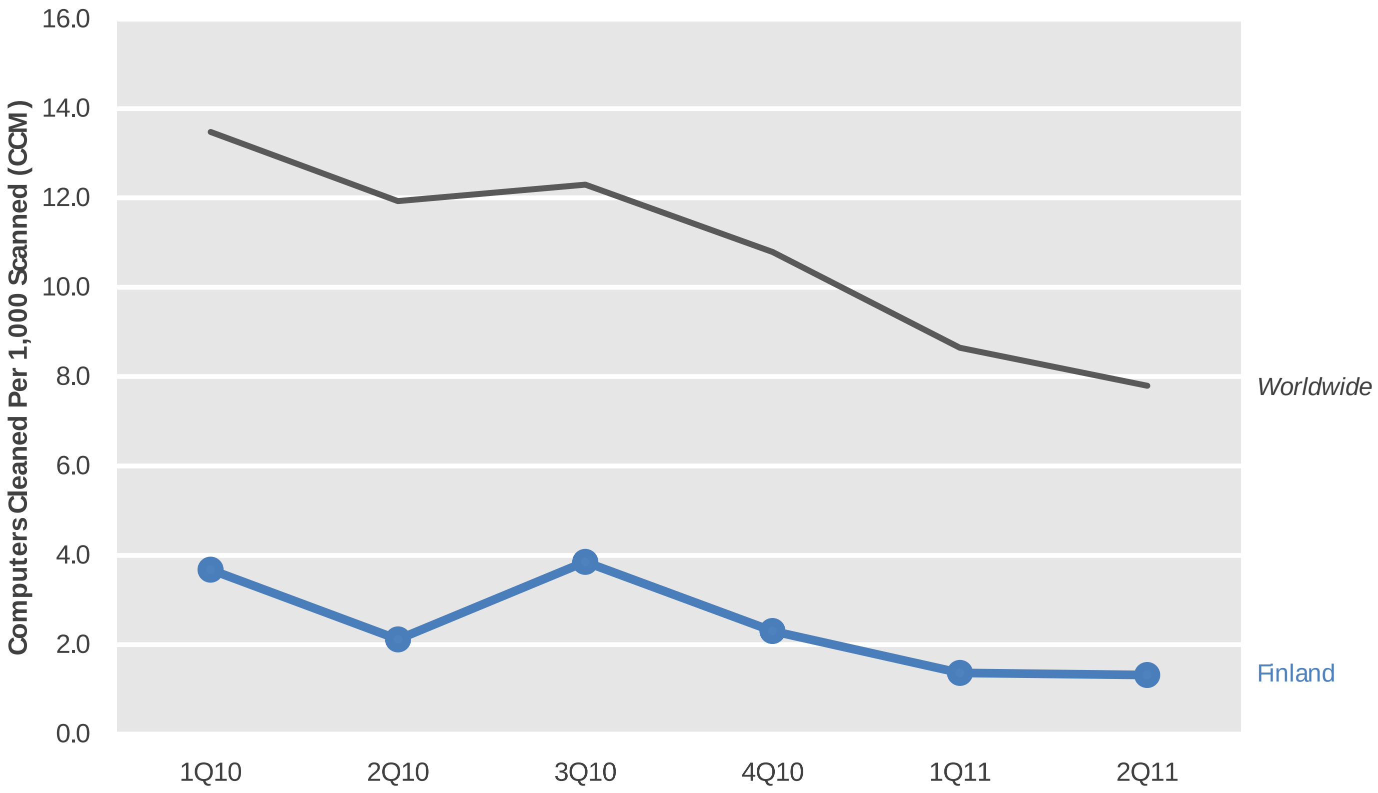
The company, which traces its roots back to 1853, has been a pioneer in the telecom industry, and one of the inventors of mobile communications, including being among the founders of the Global System for Mobile Communications (GSM). Today the company has more than 164 million customers, serviced by nearly 29,000 employees generating revenue of some U.S.$15.5 billion.

The company demonstrated its pioneering leadership by creating its own internal application to automatically monitor the network its customer use for signs of malware, and to automatically alert users of infected devices. TeliaSonera undertook this effort in order to reduce the operational costs it incurred from dealing with infected systems manually, and to slash the time required to identify and respond to malware incidents.

The Microsoft Security Intelligence Report (SIR) identified Finland as the location least infected with computer viruses and other forms of malicious software, referred to as malware. Within Finland, the subject of this case study, TeliaSonera prides itself in providing the cleanest internet service provider (ISP) services, making the company “the cleanest of the clean,” in the words of Arttu Lehmuskallio, Security Manager, Computer Security Incident Response Team, at TeliaSonera. The company keeps its network clean by monitoring traffic for signs of infection, notifying users of infected devices, and isolating their devices from the network until their systems have been cleaned. The company accomplishes its malware scanning without examining message content in order to protect the privacy of its customers.

Microsoft's SIR, which contains data from over 600 million systems worldwide and some of the internet's busiest services, found that Finland has one of the consistently lowest or the lowest percentage of computer's infected with malware when compared to any other location in the world over the past few years. According to the SIR, malware was found on 1.2 out of every 1,000 computers scanned for malware in Finland by the Microsoft Malicious Software Removal Tool (MSRT) in the second quarter of 2011. This was eight times lower than the world wide infection rate average of 9.8 in the same period.

**Figure 1. Infection rates for Finland in 2010 and 2011 by quarter by CCM (Computers Cleaned Per Mille, or Thousand[1])**



TeliaSonera's efforts to reduce the spread of malware are significant because malware can be aimed against a range of targets, including individual users, organizations, and government resources. An especially dangerous form of malware—and a difficult type to detect when not in active mode—is the botnet. A botnet is a network of compromised computers that are controlled by a "command-and-control" computer to execute commands as directed. Computers in a botnet are often called nodes or zombies. Botnets typically are created one node at a time through infecting devices, usually by sending fraudulent e-mails that ask users to open an attachment or click on a link that is infected with malware that converts their computer to a node on a botnet. Once infected the computer may appear to operate normally, but behind the scenes is waiting for orders to help mass distribute spam, participate in denial of service attacks, or in other ways compromise the efficiency and trust of the Internet.

While TeliaSonera has excellent monitoring and alerting tools in place to guard against malware, it lacked the data required to identify computers that had become part of a botnet, but were not yet active. The company needed to find a way to identify infected nodes and remove them from its network until remediated, in order to protect other users and to protect the bandwidth and integrity of its network operations.

[1] The number of computers cleaned for every 1,000 executions of MSRT. For example, if MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 (200 ÷ 50,000 × 1,000).

**Solution:**

TeliaSonera gained the data it required to clean its network of Rustock-infected devices after the Microsoft Digital Crimes Unit (DCU) in March 2011—working in cooperation with law enforcement agencies as well as industry and academic experts—successfully took down the Rustock botnet. At the time of the takedown, Rustock was estimated to have had approximately one million infected computers operating under its control and known to be capable of sending billions of spam email messages every day. Spam ranged from lottery scams to offers for fake —and potentially dangerous —prescription drugs.

The DCU is a worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer and more secure through working with law enforcement, global partnerships, policy, and technology solutions that help:

- Promote a secure Internet
- Defend against fraud and other threats to online safety
- Protect children from technology-facilitated crimes
- Champion a healthy Internet marketplace for advertisers and businesses

The Rustock operation was the second high-profile botnet takedown for Microsoft Active Response for Security (MARS) which combines expertise from Microsoft DCU, Microsoft Malware Protection Center and Trustworthy Computing, as well as Microsoft Customer Support Services-Security to disrupt botnets and begin to undo the damage the botnets have caused by helping victims regain control of their infected computers. Like the earlier takedown of the Waledac botnet, this action relied on legal and technical measures to sever the connection between the command and control structure of the botnet and the malware-infected computers operating under its control to stop the ongoing harm caused by the botnet.

After the Rustock takedown, Microsoft began an ongoing process of providing the IP addresses of infected computers to Computer Emergency Response Teams (CERTs) so that action can be taken in the local regions to clean up infected computers. The Finnish national CERT, immediately delivers to TeliaSonera lists of infected IP addresses that fall within its network.

The IP addresses are loaded into TeliaSonera's internally developed monitoring and alerting application. While TeliaSonera's application is capable of automatically shutting down infected devices, the company includes an additional step to verify the external data before taking action to isolate infected devices. TeliaSonera's monitoring and alerting application automatically assigns flagged IP addresses to the right customers for easy analysis. If the data is proven to be valid, the system then isolates the infected devices from its network and/or dispatches alerts, depending on the customer and case type. In the case of large organizations, TeliaSonera contacts the IT department to initiate the cleanup effort.

Affected customers receive notification text message when a cell phone number is on record for them, which is the case about 90 percent of the time. If the customer isn't heard from within three days of being taken offline, a notification is sent via postal delivery. User devices are then restricted to what TeliaSonera refers to as its walled garden. Within the walled garden users who lack antivirus (AV) protection are offered a trial 3rd party AV application. Users also are provided with a description of the malware detected and suggested cleanup procedures, as well as relevant informational links for resolving the problem.

While TeliaSonera offers its own paid services, it makes clear that it is just one option, and users can make use of any resource they like, including fixing the problem themselves. Users can rejoin the network without a verification test, however systems that haven't been successfully cleaned will be detected again and returned to the walled garden.

"Roughly 20 percent fail the first time, and less than 5 percent fail the second time," Lehmuskallio says. "If they fail repeatedly, our specialist contacts the customer. This happens rarely, maybe once a month. There hasn't been a case where the malware sticks after that. We also use the information we get from our difficult-to resolve cases to find tune our wording or other factors that might have caused confusion."

**Architectural Overview**

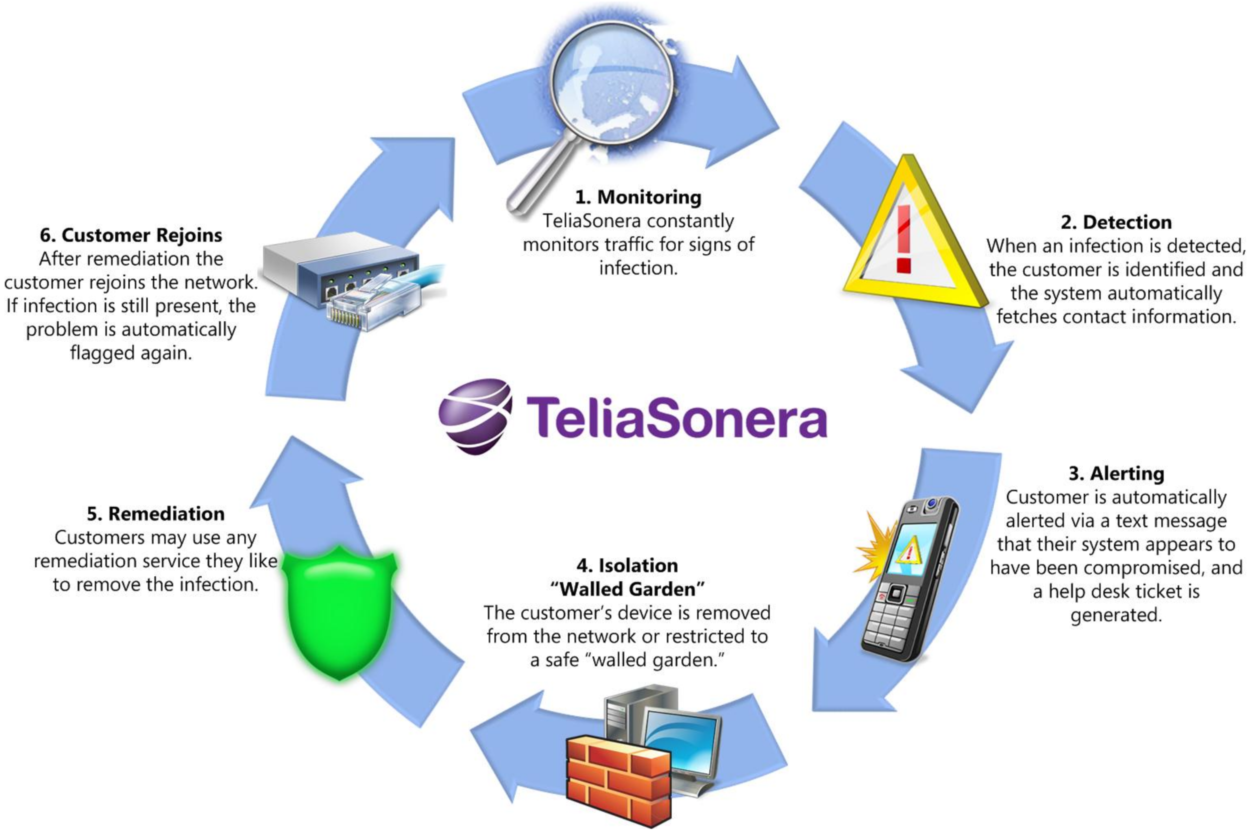
One reason that TeliaSonera is able to make such rapid and efficient use of the IP addresses discovered in the Rustock takedown is that Lehmuskallio's team has done such an effective job of creating their own monitoring and alerting tool for acting upon the news of infected IP addresses.

“We created our own custom application, and the cost to do so was essentially nothing,” Lehmuskallio says. “We have one developer focusing on creating our automated system. Others contribute at times, but it is essentially one person working part time. Our first version was up and running within a couple of months."

TeliaSonera’s automated system performs a range of functions when malware is detected, including:

- Identify the customer based on the IP-address and timestamp
- Fetch the customer’s contact information
- Read internal and external alerts and move them to a database, from which they are automatically assigned to the relevant customer
- Remove end users from the network, limiting their access to a “walled garden”
- Notify customers that their systems have apparently been compromised
- Generate a ticket for TeliaSonera customer service
- Provide customer service with access to relevant information on why a user’s access was shut down
- Provide ability for customer service to reopen the connection
- Collect an audit trail

**Figure 2. TeliaSonera provides a complete cycle of protection for its users.**



**1. Monitoring**
TeliaSonera constantly monitors traffic for signs of infection.

**2. Detection**
When an infection is detected, the customer is identified and the system automatically fetches contact information.

**3. Alerting**
Customer is automatically alerted via a text message that their system appears to have been compromised, and a help desk ticket is generated.

**4. Isolation “Walled Garden”**
The customer’s device is removed from the network or restricted to a safe “walled garden.”

**5. Remediation**
Customers may use any remediation service they like to remove the infection.

**6. Customer Rejoins**
After remediation the customer rejoins the network. If infection is still present, the problem is automatically flagged again.

The automation makes the malware monitoring and alerting solution nearly cost free to administer, as well. "Just as we had one person create the application, it takes only one person to manage the monitoring and alerts," Lehmuskallio says. "A process that required 45 minutes to handle manually in the past was automated so that one person could handle the same procedure at the rate of 500 an hour."

The company is hopeful that more ISPs will adopt similar programs. "The benefits of an ISP monitoring their network are so great, and the costs are so small, that I'm surprised more ISPs have not already implemented a similar solution," Lehmuskallio says. "The more ISPs who monitor and alert, the safer the Internet will be."

**Best Practices**

Lehmuskallio has been invited to speak in several countries and to European agencies about how it implemented its monitoring and alerting system. TeliaSonera is eager to help other ISPs create their own solutions. Lehmuskallio notes, "We share our best practices and learnings freely with other ISPs who want to make their own networks safer."

Here are a few of TeliaSonera's suggested best practices:

- **Create your own solution**. While TeliaSonera freely shares its solution with others, it suggests that organizations create their own internal application so that it specifically meets their needs.
- **Monitor.** As a first step the application should provide automated monitoring of network activity and other elements to detect the presence of malicious code.
- **Alert**. TeliaSonera believes it is essential that users be notified when an infection is detected so they can take actions to safeguard their own resources, as well as remediate the problem to protect the health of the network. The company has found that the alerts also serve an educational purpose, making users more cautious about opening attachments or clicking on unknown links.
- **Contain.** The company advises others to adopt its practice of isolating infected devices from the network until they have been remediated to protect other network users and to enhance the overall health of the Internet.
- **Encourage third-party remediation.** TeliaSonera has consciously decided to leave plenty of room for third-party resources to provide remediation services. Once TeliaSonera alerts a device owner, the company doesn't care who provides the disinfecting services. "We didn't want to be in the position of alerting a device owner to a problem and then charging them to fix it," Lehmuskallio says. "The customer can work with whomever they like to resolve the issue."
- **Verify Remediation.** After remediation, device health should be verified either before the device being allowed network access, or through re-detection of the problem when a still-infected device rejoins the network.
- **It's a Journey, Not a Destination.** As long as the threat landscape continues to evolve, so will the need to continue refining how to keep networks clean. But taking that first step on the journey is essential. TeliaSonera started its monitoring activities with manual methods some years earlier. When the company decided to automate, it simply looked at what tasks required the most time to do manually and then created the code to automate the processes.

**Benefits:**

After the Microsoft Digital Crimes Unit, working with law enforcement and other parties, succeeded in its efforts to takedown the Rustock botnet, and supplied the infected IP addresses to the Finnish national CERT, TeliaSonera was able to use the information to remove the devices from its network and alert the owners. The efficiency with which TeliaSonera's automated systems were able to respond to this and other malware threats, has helped the company to create a safer computing environment, at a low cost of implementation. The enhanced security makes for happier customers—especially businesses. The company believes its customers are also benefitting from better network performance and that its efforts are helping to create a safer Internet, even beyond its own network.

***Safer Networks with Botnet Takedowns and Cleanup***

TeliaSonera is able to provide a safer computing environment for its customers because of the work Microsoft DCU and other parties have played in tracking down and closing botnets used to cause malicious activity.

"We could not find devices connected to botnets on our network without the IP addresses and other information that Microsoft supplies," Lehmuskallio says. "Our team at TeliaSonera is dedicated to protecting the Internet and we greatly appreciate the investment Microsoft puts into security. Because of the collective efforts, criminals are getting caught and this helps make the Internet safer."

***Low Cost of Implementation***

TeliaSonera encourages ISPs to start a monitoring and alerting program as soon as possible, especially because it is so easy to do. "Don't buy a solution, just make your own," Lehmuskallio says. "The costs are negligible. One person crated ours in just a few months."

***Happier Customers—Especially Businesses***

TeliaSonera says that creating a malware monitoring and alerting program is a great way to build customer loyalty. "They absolutely appreciate our alerting them," Lehmuskallio says. "Individual customers are aware that we are helping them, but when it comes to businesses, they are extremely thankful for our monitoring and alerting efforts because they know what the consequences could be of infections remaining undiscovered. We prevent a lot of potential catastrophes for them."

The company does not specifically market its monitoring and alerting as a security service, but rather considers it something that is a part of any Internet service bought from them. "Security is one good reason to choose us instead of someone else in the market," Lehmuskallio says. "Once a customer ends up getting their workstation or server hacked or infected, they'll see our service in action. Our monitoring and alerting program is an important element to building trust with our customers and helps to foster customer loyalty."

***Better Network Performance***

Though the company hasn't performed tests to quantify the benefit, TeliaSonera has seen better network performance because of its efforts to monitor for malware and remove infected nodes from its system until they are cleaned. "We don't get as many phone calls about interrupted service or bad performance as we would were we not protecting our resources from malware," Lehmuskallio says. "All of the spam and other traffic caused by malware can soak up a lot of bandwidth as well as crowd out TCP ports."

***A Safer Internet***

TeliaSonera enjoys the satisfaction of knowing it is helping to create a safer computing experience for its customers, while also helping to enhance the overall health of the Internet. By monitoring for malware and alerting users when they have an infected device, TeliaSonera is helping the customer prevent loss of data and privacy, while also helping to ensure the infected computer doesn't survive undetected to infect other computers inside or outside of its network.

Along the way, it is educating users. Individuals who learn their computer has been infected by malware are more likely to be cautious in opening attachments and clicking on spam-delivered links. "Our customers learn," Lehmuskallio says. "We see fewer repeats for infections. They learn from their mistakes. They also learn that we are serious about requiring them to clean their devices before trying to reconnect to our network. If a device is still infected, it simply gets bounced back off the network."

While the company takes pride in helping to protect its individual and business customers from losing data, intellectual property, trade secrets, and other resources, it also feels good about protecting customers from the embarrassments that can come from malware-driven breaches of social media. "We don't want our customers to have to explain to friends and business associates that someone had hijacked their identity in social media and sent out the pleas for money, or other scams," Lehmuskallio says. "It's very embarrassing for an individual when something like that happens."

TeliaSonera's efforts as an ISP protecting users from malware represents an innovative step toward creating a safer, more trusted Internet. In 2010, Scott Charney, corporate vice president of Trustworthy Computing at Microsoft, proposed a collective defense approach to building an Internet Health model via a white paper entitled Collective Defense – Applying Global Health Models to the Internet.

The Internet could be a lot safer if more companies adopted monitoring and alerting programs such as TeliaSonera. "TeliaSonera has more than 30 percent marketshare in Finland, yet only 8 percent of the malware," Lehmuskallio says. "If every ISP had a monitoring and alerting system like ours to automatically act upon botnet identity information provided by trusted sources such as Microsoft, botnets would have a much shorter life expectancy."

## Summary

In summary, TeliaSonera is using data generated by the Microsoft Digital Crimes Unit with its own internally developed monitoring and alerting solution to create a safer environment for its users. The company has found it easy to develop and inexpensive to operate automated monitoring and alerting systems that protect network resources, while providing value to its customers. TeliaSonera believes the values are so great that ISPs everywhere should consider adopting similar programs. The efforts of TeliaSonera exemplify how important device health is both to customers within its network and those outside the network. As more ISPs adopt monitoring and alerting solutions, their combined efforts will help to create the kind of collective defense that will provide a safer more trusted computing experience for everyone.

## Resources:

For more information about the threat landscape, please see: www.microsoft.com/sir

For more information about how to protect against botnets, please see: http://support.microsoft.com/botnets

For more information about how users can get daily updates on their network from the Microsoft SNDS service, please see: https://postmaster.live.com/snds/index.aspx

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.