Issued 3/18/17

Samsung Leaking Customer Information via Shipper's Website

The website of a company handling the shipment of Samsung products is currently leaking data about Samsung customers in an appalling manner. The issue came to light yesterday when application security engineer Matt Metzger published a Medium article detailing his attempts to notify Samsung of the problem.

Even if the issue is present in the systems of AGS, a company Samsung collaborates to handle product shipments, Metzger places the blame on Samsung. "I entrusted Samsung with my data, and that is who I hold solely responsible for safeguarding it," Metzger says. "If Samsung’s business partner is leaking that information, Samsung needs to remedy the situation.”

According to Metzger, there are a multitude of problems with the AGS shipment tracking system:
✭ The tracking ID is included in the URL and anyone can easily edit it to access details for other customers
✭ The tracking ID is sequential, and details about Samsung customers can be scraped en masse
✭ Anyone can search for other people's orders via a publicly-accessible search form
✭ The search form visibly hints the order ID is a seven-digit number
✭ AGS recycles order tracking numbers every year, meaning users will see order details from different customers when searching for their order ID

✭ Some orders have been indexed by Google and show up in search results, meaning you don't need to order a Samsung product to discover internal AGS order links

✭ At a first stage, leaked data included orderer's last name, orderer's city, ordered item, and order number

✭After the product was delivered, the order would be updated with proof-of-delivery, such as the orderer's signature, full name, and full address

Issue reported months ago

Metzger says he reported the issue to Samsung months ago, but in a reply from Samsung's security team, the company told him to contact AGS. As previously stated, Metzger thought this issue was Samsung's concern and went public with his findings.

The researcher argues that this data could be easily scraped and used in phone scams to extract payment card details from Samsung customers, as scammers could very easily pose as Samsung employees by mentioning seemingly secret order details.