BCG

THE BOSTON CONSULTING GROUP

IT TAKES A COALITION TO PROTECT THE INTERNET OF THINGS

By Greg Boison, Walter Bohmayr, Stefan A. Deutscher, and Michael Bechauf

IT READS LIKE A PLOT out of Hollywood: malicious computer code infects household devices, which then wreak havoc on the world. But no screenwriter crafted this tale. The code exists and has already co-opted hundreds of thousands of products—baby monitors, Wi-Fi routers, security cameras, and more—that sit in homes and on home networks. In the process, it has exposed glaring security weaknesses in the much-touted Internet of Things (IoT).

Many forms of malware leverage these vulnerabilities. Perhaps the most prominent of the breed is Mirai, whose inner workings, published online, are readily adaptable to specific malicious purposes. Taking over connected devices and ordering them to send junk data to targeted servers, Mirai and its brethren can quickly overwhelm sites, businesses, and services, knocking them offline. In October 2016, a Mirai attack on a key internet hub hobbled Amazon.com, Twitter, Reddit, and dozens of other major internet players. Around the same time, press reports implicated the malware in a massive internet outage in Liberia, suggesting that such code could even take an entire country offline.

Shoring up the IoT's defenses is critical for businesses, users, and an economy that increasingly depend on the internet. Current estimates of the global deployment of IoT devices range from 6 billion to 14 billion, and experts anticipate that up to 40 billion more devices will be in place by 2020. It is certainly true that players along the IoT value chain—device manufacturers, internet service providers, and end users—can take steps to close the security gaps. But there is a catch: the players in the best position to act are also the ones that face the least potential harm. This gives them little incentive to make and pay for the fixes.

So how do we tackle this problem? One idea is to work collaboratively to create a coalition of key players along the value (or perhaps more accurately, victim) chain. Using a coordinated approach, they can sort through the complexities, costs, and potential impact of different fixes. They can align incentives to encourage creation of the

most promising fixes. And in the end, they can banish malicious code to where it belongs: on the cinema screen.

A Password Fail

That Mirai works at all is evidence of the insufficient security practices of device manufacturers that use common default passwords across product lines and even across vendors. One manufacturer, for example, uses the same simple password for 80 different camera models. In many cases, users can't change a device's default settings, including any passwords. To be sure, such practices often arise in response to consumer expectations: people want products that are easy to set up and use. And it is unclear how many customers who can change the passwords actually will, to say nothing of maintaining an up-to-date log of all credentials for their devices.

As a result, by using a relatively small set of passwords and a simple process of trial and error, malware can gain access to an enormous array of products. And Mirai has a list of such passwords. Working methodically, it finds and contacts connected devices, attempting to log in by using known credentials. When Mirai gains entry, it issues new instructions to the device. Most users have no idea that anything is amiss, since their camera, router, or other product continues to function. But in the background, the compromised device now monitors the hacker's command-and-control server. When ready to launch an attack, the hacker orders an army of infected devices—known as a botnet—to send data to the target.

By itself, the transmitted data is harmless. It consists of routine requests of the same kinds that uninfected devices send over the internet all the time—for example, a request to establish a connection. But when many thousands of devices send data at the same time to the same destination, the targeted server or site can quickly be overwhelmed. Legitimate traffic can no longer get through.

Knocking a site offline by flooding it with garbage traffic—which in its least sophisticated form is called a *denial of service (DoS) attack*—is not a new phenomenon, and a site under a typical DoS attack can thwart it by identifying and blocking the source of the outsize traffic volume. But Mirai gets around this defense by distributing its traffic across its botnet of hundreds of thousands of devices. In this variant—known as a *distributed denial of service (DDoS) attack*—no single device clogs the network, so the victim of the attack can't respond by shutting down a single obvious offender. There is no way to remove the bad apples, because every apple looks the same.

So far, botnets assembled by Mirai have targeted both individual sites and internet backbone providers. Compounding the problem: the ready availability of Mirai's source code has sparked the emergence of pay-per-use business models in which, for a fee, the proprietor of a botnet army will unleash a DDoS attack on the buyer's online target of choice.

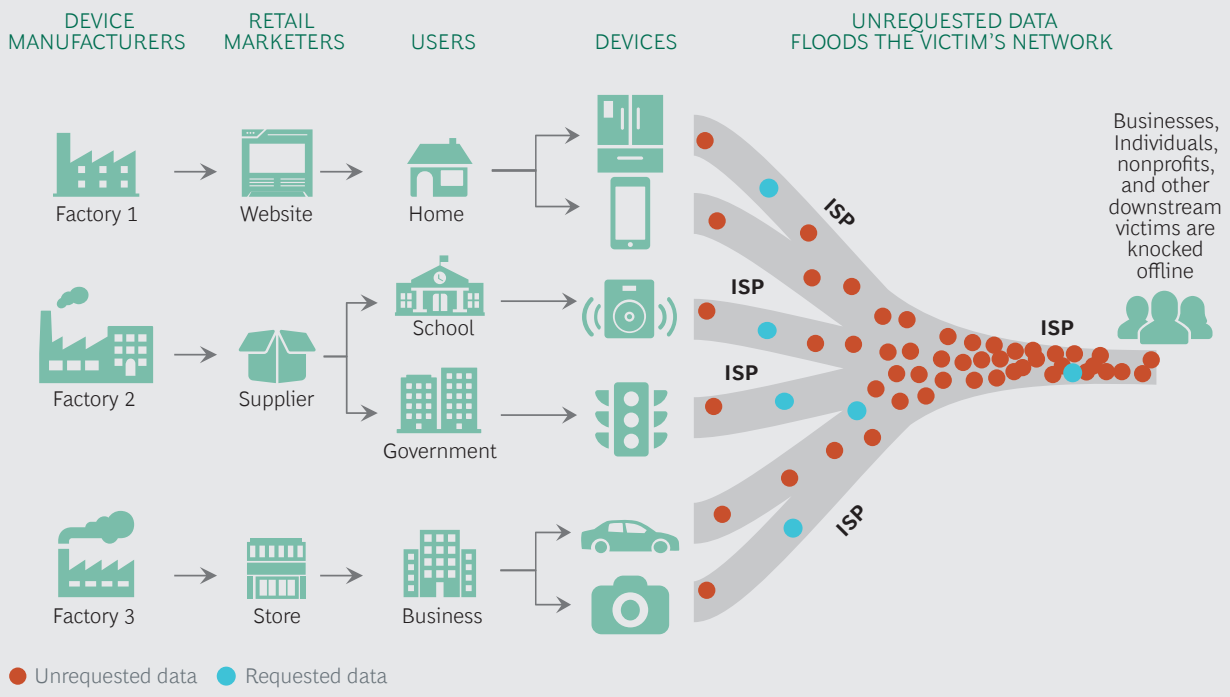
The Victim Chain

One of the most problematic aspects of a Mirai attack is that the point of greatest vulnerability is not the point of greatest harm. The weak spot is the IoT device and its poor security. The attack starts there. But little or no damage occurs at this entry point. At worst, users might notice that their baby monitor or connected doorbell seems to be working a bit sluggishly.

The real harm occurs farther down the chain. An ISP may see a flood of junk traffic clogging its network. Businesses, individuals, and entities relying on that ISP may find themselves knocked offline. (See the exhibit.) Typically, these end-of-the-chain actors bear the brunt of the damage. But they are also the actors in the worst position to do anything about it, because the key vulnerability that makes the damage possible lies far upstream, at the poorly secured IoT devices.

So why not secure those devices? If the manufacturers of IoT products adopted stronger password protection and security practices, code like Mirai wouldn't be able

When Infected Devices Go Rogue: The Victim Chain in a DDoS Attack



Source: BCG analysis.

to pick so many locks. Unfortunately, manufacturers have little incentive to take this step—and plenty of reasons not to.

In a hypercompetitive marketplace, speed and convenience are everything. Measures that boost security can make products more cumbersome to use, less interoperable, and slower to market. Any of these shortcomings can put a vendor at a disadvantage against its peers, particularly the thousands of low-end manufacturers that are unlikely to prioritize security no matter what their competitors do. Taking an economic hit in the name of better security might be worth it if the vendor gained something tangible in return, but the benefits generally arise only downstream, to the advantage of players other than the vendor and its customer.

In addition, boosting security can raise the cost of a product, which may be a deal breaker for some prospective buyers. For example, companies that integrate IoT devices into their own products can see and (if they choose to do so) prioritize a short-term benefit by buying a less secure device that may be 20% cheaper than a more locked-down alternative.

Similarly, consumers usually don't have much incentive to batten down the IoT hatches. Maintaining firewalls—which prevent malicious code from communicating with networked devices—requires continuing effort and, often, skill that a user may not possess. On the other hand, although failing to implement a firewall may lead to the infection of a device, the consumer may experience no adverse effects beyond a slowdown in the compromised device's operating speed.

It's the same story with ISPs. Theoretically they might be able to add enough bandwidth to prevent any harm when thousands of devices send junk data at once. But more bandwidth costs more money, and ISPs are far enough upstream that the negative consequences they might suffer from a DDoS attack are unlikely to justify the expense of providing an extra layer of bandwidth as a safeguard. Furthermore, Mirai-like malware could conceivably attack devices inside an ISP (such as the em-

bedded computers found in routers and switches), in which case added bandwidth would be of no use.

The Way Forward: Cooperation and a Coalition

Unfortunately, the player that is most at risk—the business, individual, or organization at the end of the chain—can't fix the problem on its own. Someone else's device, made by yet another party and compromised without the owner's knowledge, is the source of all the grief.

If you look at any single player along the victim chain, either the incentive or the capability to plug the security hole is missing. The only way to shut down code like Mirai is through collaboration: multiple parties taking steps together. The idea is to create incentives—and eliminate disincentives—so that those who can take action will do so.

A collaborative approach would bring many of the key stakeholders—including, potentially, government players such as (in the US) the Department of Homeland Security and the Federal Communications Commission—face to face to plan a joint strategy. Together, this coalition would examine every possible mitigating step, analyzing its effectiveness in shutting down malicious code and its cost. The group would identify where the cost burden lies, whether the step is worth taking, and how incentives might be aligned to trigger it.

The stakeholders might determine, for example, that adoption of an incentive program in which ISPs provide rebates to consumers who secure their IoT devices (such as by deploying and managing firewalls on their home networks) is a promising step. Programs offering similar discounts have achieved good results in other contexts. For instance, US utilities may provide rebates to customers who install energy-efficient lighting or smart meters in their homes. Right now, ISPs don't have much incentive to take this step. But sitting together in a room, the stakeholders can assess the situation from outside the ISP silo. What could other players do to spur the ISPs to action? Perhaps the government could agree to subsidize IoT security rebates through a program similar to the FCC's Universal Service Fund—subscriber fees that the agency uses to promote access to telecommunications services in the US. Then ISPs could offer the rebates without taking a financial hit from the extra costs involved.

Or perhaps governments could act to hold providers liable if their devices participate in an attack. Or government regulation or a certification program along the lines of the Energy Star program for energy efficiency could spur merchants to sell devices that comply with robust security standards. Such standards take time to develop, and attackers will inevitably tweak and hone their tactics in the interim. But in the longer term, higher standards could provide a strong defense. The key point is that a coalition can identify and help implement some of the many practical possibilities that exist.

Homing in on the optimal fixes—layered solutions with aligned incentives—calls for complicated cost-benefit analysis. And bringing together the different players creates intricacies and challenges in stakeholder management. This is not a simple approach. Still, with proper orchestration, coalitions can solve difficult problems. And given that code like Mirai currently has too easy a time infiltrating and infecting IoT devices, we need to tackle the problem today. At risk are not just networks and sites, but the value and promise of the internet.

About the Authors

Greg Boison is an associate director in the Washington, DC, office of The Boston Consulting Group. You may contact him by email at boison.gregory@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office. You may contact him by email at bohmayr.walter@bcg.com.

Stefan A. Deutscher is an associate director in BCG's Berlin office. You may contact him by email at deutscher.stefan@bcg.com.

Michael Bechauf is an associate director in the firm's San Francisco office. You may contact him by email at bechauf.michael@bcg.com.

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with more than 90 offices in 50 countries. For more information, please visit bcg.com.