

# YOUR GAS METER: THE NEW FRONT LINE IN CYBERWAR

The Stuxnet worm shows how vulnerable your home is to terror attacks. By Mic Wright



**B**y the end of 2020, the government wants every home in the UK to be fitted with a smart meter. The device, as part of a networked system of localised power distribution, allows consumers to control their consumption and – more contentiously – also lets utilities companies monitor real-time usage. The £8 billion scheme is being sold as a way for the average household to cut its energy bills by an estimated £28 per year.

But could such a banal technology in fact be fraught with danger? In July 2009 – five months before the Department of Energy and Climate Change (DECC) announced the initiative – security firm IOActive demonstrated a worm that could rapidly spread through a smart-grid network, disabling meters as it went. The experiment proved what many cybersecurity experts already knew: hackers distributing the right malware could shut down the network. Britain would go dark.

“Before, to destroy a meter, you had to take a sledgehammer to it,” explains John Bumgarner, formerly of the CIA and NSA, and now research director for security technology at think tank the US Cyber Consequences Unit. “That worm could destroy 300,000 [smart meters] in one go. The smart grid is going to be a major target for hackers.” Marc

Maiffret, a former hacker and now chief technology officer at computer-security consultancy eEye Digital Security, says: “If there was a war tomorrow between major powers, the first stages would include cyberattacks with the aim of completely disrupting critical infrastructure. If you have the right combination of factors – power running at full blast and interference that means you cannot redistribute it properly – sabotage can have very serious consequences.”

In May 1997, WIRED US published “A Farewell To Arms” by John Carlin, a feature predicting the future of cyber warfare. It raised the prospect of a “fire sale”: hacker-speak for a co-ordinated strike on a nation’s critical systems – water, energy, emergency services. This frightening vision was optioned for film-script development – and although it didn’t get off the ground in its original form, years later it was incorporated into 2007’s *Die Hard 4.0*. “Every nation in the world is working aggressively to get that kind of capability,” Maiffret says.

And some may already have it.

**In March 2007 an industrial generator at the US Department of Energy’s National Laboratory in Idaho began to malfunction.** First, it shuddered violently; then steam appeared, before vapour billowed from the valves. Within seconds, the machine was hidden by smoke. From outside, the building appeared to be on fire.

This event appeared to be nothing more than a mechanical failure. In fact it was a deliberate attack by the



Stuxnet infection rates: ● Iran (52) ● Indonesia (18) ● India (11) ● Rest of the world (19)  
Countries that the Stuxnet virus has most often attacked, with percentage of total attacks in brackets. Source: *Security Week*



US Department of Homeland Security and its National Cyber Security Division on one of its own facilities, the first demonstration of Project Aurora, a government programme aimed at establishing the potential of cyberattacks to undermine critical infrastructure such as nuclear plants, chemical-treatment centres and water-filtration plants.

The experiment took place in a controlled environment, using a generator unconnected to any national power grid. But it showed that real-world infrastructure can be remotely disabled or even destroyed with only malicious code. The first significant attack of this type came eight years ago. In 2003, the Slammer worm disrupted communication infrastructure in several countries in Asia, Europe and North America, and knocked out 13,000 ATM systems in the US. It also forced a 911 dispatch centre in Seattle to shut down its tracking system. Since then government security agencies have been on alert for the next major, systematic attack.

**L**ast summer their concerns became more pressing. Researchers at a small Belorussian firm, Virus-BlokAda, discovered an advanced piece of targeted malware capable of damaging the programmable logic controls at the heart of nuclear plants and other critical facilities. The worm was found to be targeting an extremely specific configuration of a common Siemens product used in supervisory control and data acquisition (Scada) systems that run amenities such as power plants. By targeting components called programmable logic controllers (PLCs) and altering their function, it could initiate overheating and total destruction of a system, and – potentially – an explosion. It was named Stuxnet.

The worm has a wide range of targets, such as undiscovered vulnerabilities in Windows (known as zero-day exploits), and rootkits (software packages designed to allow undetected but privileged access to systems) for both Windows and the PLCs. It can evade detection by antivirus software, can be updated via peer-to-peer networks, and has an elaborate command-and-control system. Stuxnet is also very difficult to detect – even as it reprograms the Scada system or modifies the way the PLC works, it conceals those changes from operators.

Research by US antivirus firm Symantec suggests that Stuxnet initially spread via USB thumb drives, which are frequently used by infrastructure engineers to transfer data and to patch systems. Now it roams online, searching for systems

employing the Siemens PLC configuration that it targets. Whereas recent cyberattacks, such as the Conficker worm and the assault on Google by Chinese hackers in early 2010, were relatively unsophisticated (attacking the ageing Internet Explorer 6 browser), security researchers believe Stuxnet represents a new level of complexity. None of the experts who have studied Stuxnet can identify a definite culprit. And no one has been able yet to determine its exact target.

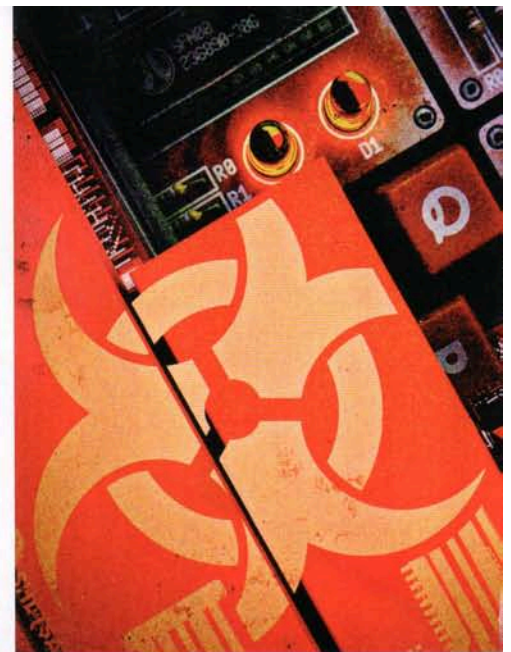
According to Ralph Langner, a German specialist in infrastructure security who has analysed Stuxnet's code, "It is the first real cyberwar operation in history – everything before this was kids' stuff." As the first worm with the ability physically to disrupt critical infrastructure, Stuxnet is seen by many security experts as a warning of what a worm could do to power plants more widely.

The worm's complexity has led to suggestions that Stuxnet was created by a state agency. That theory is supported by analysis from Symantec and Siemens detailing infection numbers. Out of more than 45,000 cases worldwide, more than half have been in Iran.

A recent report in *The New York Times* claimed that the worm was a joint US-Israeli project to disrupt Iran's nuclear programme: either the plant at Bushehr or the Natanz uranium-enrichment facility. In October, Reza Taghipour, the minister of communications, told Iranian state TV that the virus had been introduced inadvertently on infected USB sticks by "foreign experts" from the state-backed Russian contractor Atomstroyexport, who were working at the plants. Atomstroyexport declined to comment.

Thus far, researchers have failed to identify the specific process attacked by Stuxnet but have discovered that it injects a segment of code called Organisational Block 35 into the controller. This code is related to processes that are fast or occur in high-temperature or high-pressure situations. Interfering with them could create the same result as seen in the Project Aurora demonstration – the components tearing themselves apart.

Langner believes the virus was created by a coalition of states intent on disrupting the Iranian nuclear programme and forcing Iran's hand in talks with the US, the



UK, France, China, Russia and Germany. (In late November 2010, Iran returned to the negotiating table.)

He explains the spread of Stuxnet elsewhere as collateral damage, and identifies the worm as a blueprint for future cyberattacks using malware: "Stuxnet was developed to attack one specific site and process," he says. "But now the weapon is in the public domain it can be modified and will not be limited to attacking high-value targets [using] insider knowledge."

Jeffrey Carr disagrees with Langner's belief that the worm originated in Israel and proposes an alternative theory – that Stuxnet is part of an ongoing space race between China and India, where the prize is domination of the satellite communications market. In such a ruthlessly competitive arena, a worm that could cripple a rival's technology – or transmit back data from it – would be very desirable. "[Langner's] technical work is fine. It's the part that follows that I have a problem with," he says. "Multiple countries were attacked. The argument that infections in 150 other countries are blowback is wildly overblown."

Whatever the origin of the virus, Bumgarner thinks that limited state-sponsored attacks on infrastructure are likely in the short term – Chinese hackers have already been identified as the source of interference with the US power grid during outages in 2009 – but foresees larger

Subscribe to WIRED now  
at just £2 an issue:  
[www.magazineboutique.co.uk/  
wired/W173](http://www.magazineboutique.co.uk/wired/W173)  
or call 0844 848 5202





ILLUSTRATION: ALEX VARANESE

attacks by extremist organisations in the future. "They'll get that kind of capability, but the big question is whether they could launch multiple attacks at one time," he says.

In October last year, the UK government published a Strategic Defence and Security Review, which addressed the threat of cyber attacks from states, criminals and terrorists. This has given birth to Britain's National Cyber Security Programme, which will receive £650 million in funding during the next four years.

Rex Hughes, the codirector of the Cyber Security Project at the Royal Institute of International Affairs, believes the UK is among the best-prepared nations against cyberattacks. "Britain is definitely in the big league," he says. "GCHQ and the NSA in the US work closely and there's no reason Britain shouldn't remain in the top tier. Despite a slow start the Cyber Security Operations Centre in GCHQ and the Office of Cyber Security in the Cabinet Office mean that the UK has a pretty robust response prepared."

Still, strategists foresee future risks of terrorists attacking critical infrastructure using malware. "I don't think Islami[st] terror cells are there yet," Carr says. "The old guys in the leadership won't sanction cyberattacks either. They prefer an old-fashioned physical explosion. But once you have internet-savvy terrorists in control, they will understand the benefit of a cyberattack. The tricky element is finding an engineer with the right skills who is also a religious radical."

For the time being, it seems that major cyberattacks remain the domain of state intelligence services and skilled non-state teams for hire. Sir John Sawers (aka "C"), chief of Britain's Secret Intelligence Service (SIS), has highlighted concerns about threats to Britain from such attacks. "Electricity grids, our banking system, anything controlled by computers could be threatened," he said during a public speech (the first ever by a serving head of MI6) in October 2010. "Cyber is becoming an instrument of policy as much as diplomacy or military force. Even technology threats have a crucial human element. SIS will be launching operations to counteract nations launching cyberattacks against us."

But are the utilities companies aware of how serious a potential threat their systems face from digital assault? Bumgarner

offers up an unsettling example to suggest otherwise. "One night I was talking to someone from a large electric company," he says. "They said the company had no systems on the public internet. I was mapping its network using my laptop. I turned it around and showed them where the firm had portals on the network for Scada controls. If you took all the electric companies out there and accessed just their IP addresses, which are easy to find, I guarantee you'd find a hole in their networks."

Although creating a piece of malware as sophisticated as Stuxnet may demand complex skills, it's simple to discover where vulnerabilities lie within critical infrastructure. "Google is a phenomenal tool for figuring out how to compromise industrial control systems," Bumgarner says. "It allows you to map the vulnerable systems. Someone misconfigures a system and it gets indexed - and then it shows up in Google's cache."

**T**he EU dictates that the UK must install 50 million smart meters by 2017. To reach this target, in January British Gas created a Smart Homes division and promised to install two million meters by the end of 2012. Already 47,000 homes have taken part in a large-scale trial overseen

by Ofgem and run by E.On, EDF Energy, Scottish Power and Scottish and Southern Energy. Smart meters will have four components, according to British Gas's specifications: an electricity meter; a gas meter; an in-home display; and a communications hub. The four components will communicate with each other using a low-power (2.4Ghz) wireless technology called Zigbee. The meters will pass data to the central hub and that will send the data to the energy provider via GPRS, allowing exact calculation of bills. The comms hub also backs up information in case of the GPRS link going down. But how secure those SIM-enabled meters are, and how easily hackers might be able to infiltrate those wireless networks, is still not clear.

The US is bracing itself for a serious attack on its energy infrastructure from Stuxnet-style malware along the lines of the exercise in Idaho. "It is going to happen," says Patrick Ciganer, director of the US Department of Energy's Transparency Initiative. "We have to avoid the obvious scenarios and mitigate the consequences."

*Mic Wright wrote about producing viral videos in 01.11*

## % THE WIRED INDEX

# 1,760

Number of PS3 consoles used by the US Air Force to create a \$2 million supercomputer

# 35.8%

Proportion of mammals declared extinct in scientific papers since 1500 that are in fact still alive

# \$43

Amount spent per voter by or on behalf of candidates in the 2010 US midterm elections

# £0.47

Amount spent per voter by or on behalf of candidates in the UK 2010 general election

# 1 BILLION

Estimated number of birds killed annually by window panes

# 28%

Phone users who suffer damage from their use, according to telecoms-funded studies

# 63%

Phone users who suffer damage from their use, according to studies otherwise funded

# \$3.5 MILLION

Stock reportedly offered by Google to a staffer not to join Facebook  
*For sources, see page 138*