JULY-AUGUST 2015 WWW.SCMAGAZINEUK.COM

SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

Attacks on critical national infrastructure are a growing concern set to present even more of a problem as SCADA systems become internet enabled

A CRITICAL THREAT

What's wrong with CBEST?

The industry grapples with how best to ensure critical infrastructure deploys first-rate practice P19

Women in security

Changes are afoot, while the reasons for the lack of women in IT security remains a topic of debate P21

IQ

2 MINUTES ON...

Duqu 2.0: a massive advance

As APT sophistication grows we're all at risk – even security vendors

The news last month (June) that Kaspersky Lab, one of the leading international cyber-security companies, was hit by a "next-generation" malware attack is an indication of both how far we have come in cyber-warfare and how much further we still have to go.

Eugene Kaspersky, founder of Kaspersky Lab, is certain that the software used in the attack represents version 2.0 of Duqu. According to Kaspersky Lab's analysis of Duqu 2.0, it is highly sophisticated malware which shows all the signs of having been crafted by someone with the resources of a nation-state behind them.

Duqu 1.0 is a malware discovered in 2011 by the Budapest University of Technology and Economics in Hungary. Thought to be related to the Stuxnet worm, it got its name from the prefix "~DQ" it gave to the names of files it created.

As Eugene Kaspersky has been at pains to explain, Duqu 2.0 is a massive advance on Duqu 1.0, exploiting three zero-day vulnerabilities, spreading through the system using MSI files, not creating or modifying any disk files or system settings and existing almost totally in memory.

Other cyber-security experts are in agreement about its sophistication. "After reviewing the technical analysis from Kaspersky, it's safe to say that Duqu 2.0 represents both the state of the art and the minimum bar for cyber-operations," Tod Beardsley, engineering manager at Rapid7, told *SC Magazine UK*.

Such was its stealthiness, Kaspersky believes the attackers were confident that they would not be discovered.

So this was a super-sophisticated zero-day attack but the method of entry into the network was distinctly old-school – an email attachment – which was sent to one of the company's sales representatives, purportedly from a customer or trusted supplier.

Eugene Kaspersky's company attacked by Duqu 2.0.

The industry will be alarmed that a company with Kaspersky Lab's expertise found itself invaded in this way. Eugene Kaspersky blames modern operating systems and their distinctly archaic security.

"Unfortunately modern operating systems were designed in a way, based on ideas and architecture of 40 to 50 years ago, and they are not immune to this kind of attack," Kaspersky told *SC* during a live video interview.

If there's one part of this attack that Eugene Kaspersky is downplaying, it's the value of the information that the hackers managed to get from his network.

Although the attackers were in the network for months, exfiltrating data about Kaspersky Lab research and processes, he insists that anti-malware software is evolving so quickly that the value of the information to the hackers is decaying rapidly.

Industry experts aren't so sure. By its nature, Duqu 2.0 operated in memory, possibly in a way that ensured nothing was written to the system, so that when the system was rebooted it would be almost impossible to detect.

This leads some to think that it's impossible for Kaspersky Lab to know what information was compromised.

So what are the likely long-term ramifications of this attack on the industry and Kaspersky Lab?

Gautam Aggarwal of Bay Dynamics is one expert who believes we haven't seen the end of this story. He says there are similarities to what happened to RSA in 2011 in which over 100,000 OTP authentication tokens were stolen. Weeks later Lockheed Martin was attacked by someone using legitimate usernames and OTP tokens, enabling them to steal secret blueprints.

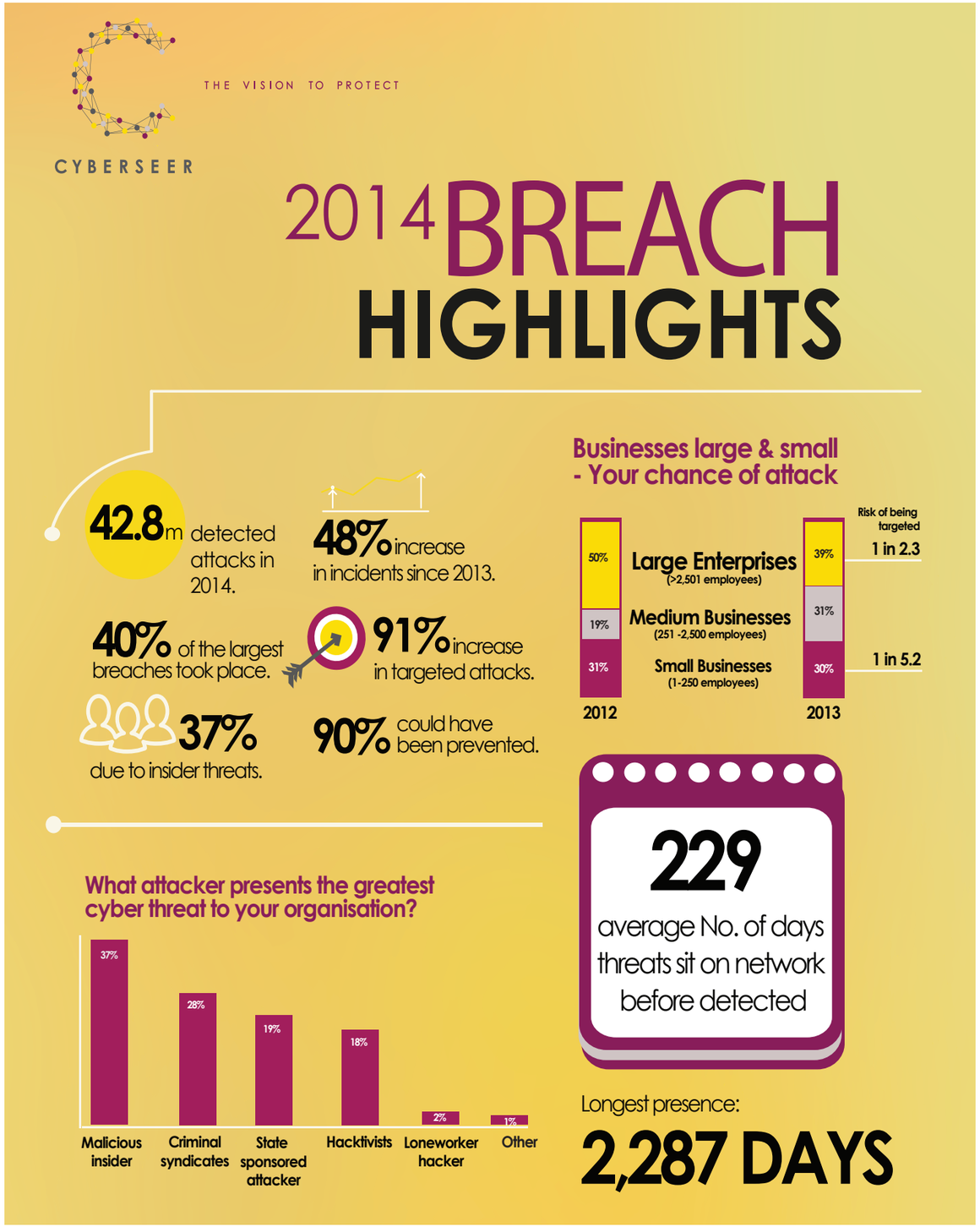
Aggarwal speculates that the Kaspersky attackers could be looking for vulnerabilities in the Kaspersky secure OS to be able to launch attacks on client sites.

As damaging as it might be to admit to being hacked in this way, Kaspersky Lab has clearly decided to own this story by releasing it on its own terms. Kaspersky said the company has shared the information with its technology partners, law enforcement agencies and customers.

It has won plaudits for being open, with a company official telling *SC* that this is proof of the company's commitment to transparency.

Discovering this vulnerability is also a success story of sorts. Although Duqu 2.0 remained undetected for months, it was discovered while the company was testing a new APT detection tool on its own servers, a fact that Eugene Kaspersky was more than happy to share.

As *SC* went to press, further concerns arose as it seems Duqu 2.0 successfully hid behind a legitimate digital certificate stolen from Foxconn, potentially undermining certificate credibility.



– Source: www.cyberseer.net