BIZCOMMUNITY

Focus on data protection will be paramount in 2016

By Thomas Fischer

25 Jan 2016

Wiper attacks, which erase files from victim's computer drives in order to cripple essential apps, have been growing steadily for years. A wiper attack will not only damage your IT systems, but can leave sensitive data exposed.

©Dmitriy Shironosov via 123RF

Sony have been the most prolific organisation to suffer this kind of attack to date; however, as these kinds of hacks become easier businesses of all sizes must be prepared to protect against them.

Investing in security is essential for any modern business, however it will only be effective if they invest in the right areas. Focussing on endpoint protection, disaster recovery and backup applications that can be easily scaled can significantly reduce the chances of wiper attacks causing lasting harm.

High profile data breaches such as the TalkTalk, Ashley Madison and Experian hacks have been extremely damaging for the companies involved and brought cyber security to the forefront of every business-owner's mind. Many of these attacks have been blamed on a rise in 'hacktivism'.

Reasons for hacktivism

Self-proclaimed 'hacktivists' will attack companies for a variety of reasons, the most common of these being:

- Ethics: To place the spotlight on a company engaging in morally questionable practices and expose them.
- Opposing values: As a result of fundamental differences in the values held by the attacking group and the organisation being hacked.

- Monetary gain: To extort victims for monetary gain in an effort to cripple the target organisation and fund their cause.

Part of the reason these attacks are becoming more widespread is the fact that they are far easier to carry out than they were just a couple of years ago. With hacking tools readily available to those who know where to look, the resources required to stage a high-profile attack are dangerously easy to find and implement.

Rise of nationalism

The rise of nationalism in countries like Russia, Iraq and Syria is also likely to have an effect. Nationalist and terrorist groups will use these publicly available tools to make public statements and intimidate corporations with conflicting values - attacking freedom of speech, the film industry and the literary community.

As information becomes more valuable with every passing year, there is a lot at stake not just for the information security industry, but for the world as a whole. This is why companies must do everything they can to research and implement a data protection solution that is designed to combat these new attacks.

Hundreds of thousands of customer details were leaked as a result of the 2015 data breaches. This data is most valuable to hackers before the leak is discovered and made public, when it becomes much harder to sell off or act without attracting attention. However, even after the breach is discovered this information is still out there, still accessible, and is often used in a second wave of attacks to target the victims themselves many months later.

Hackers will often bombard breached email addresses with phishing attacks in an attempt to gain access to more of their personal details. By impersonating banks, retail companies and government agencies the attacker will try to trick users into sending them money or personal information. These imitations are becoming more convincing, with hackers explaining to users that they are vulnerable to an attack and must change their details immediately by handing them over in some way.

Access to emails

If enough information is still available, hackers could also attempt to access the email accounts themselves using other details that have been leaked such as dates of birth. In some cases, malicious users could even try to access the victim's bank accounts directly using leaked account details. There is a new wave of organised crime happening online worth billions of pounds, and it's getting larger all the time.

The Internet of Things (IoT) is developing at an unprecedented pace. With an incredibly broad spectrum of uses across a plethora of sectors, a 'smart world' is not simply the stuff of science fiction. These IoT devices are populating every aspect our lives and it's important to understand that leaves people vulnerable in a way that hasn't been a problem before.

Smart homes, for example, offer convenient solutions for busy residents looking to save time and money, but smart tech companies must ensure it is not to the detriment of the user's security. Devices such as smart electricity meters or thermostats could moderate power consumption and room temperature based on when the residents are out. However, if criminals were to access the network these devices communicate through, this data could be used to plan a break-in.

There are three main entry points when it comes to IoT devices. Firstly, attackers can hack the service provider, gaining database information that gives access to data such as smart meter readings.

Wireless protocols

Secondly, it is possible to break in through the wireless protocols between the devices, which are inherently insecure due to the low quality routers often supplied with home Wi-Fi packages. The vulnerable ISP boxes are reverse engineered for security, and give easy access to the consumer's network. Finally, hackers could directly infiltrate the infrastructure, however this is much more difficult that the other two methods, as it so is unlikely to occur as frequently.

CIOs must take more responsibility when it comes to data theft. Leaving security vulnerabilities solely to the IT team is no longer excusable as data theft continues to be a prominent issue. Threat intelligent services are likely to be commissioned to provide reports and validation on malicious threats.

The increase in the power and safety of the cloud will also give SMEs a chance to move from relatively weak IT infrastructures to a platform where security is evolving constantly. Ultimately, the focus on data protection is going to be paramount for businesses heading into 2016, and it's up to them to ensure they are prepared.

ABOUT THE AUTHOR

Thomas Fischer is principal threat researcher for Digital Guardian at Credence Security