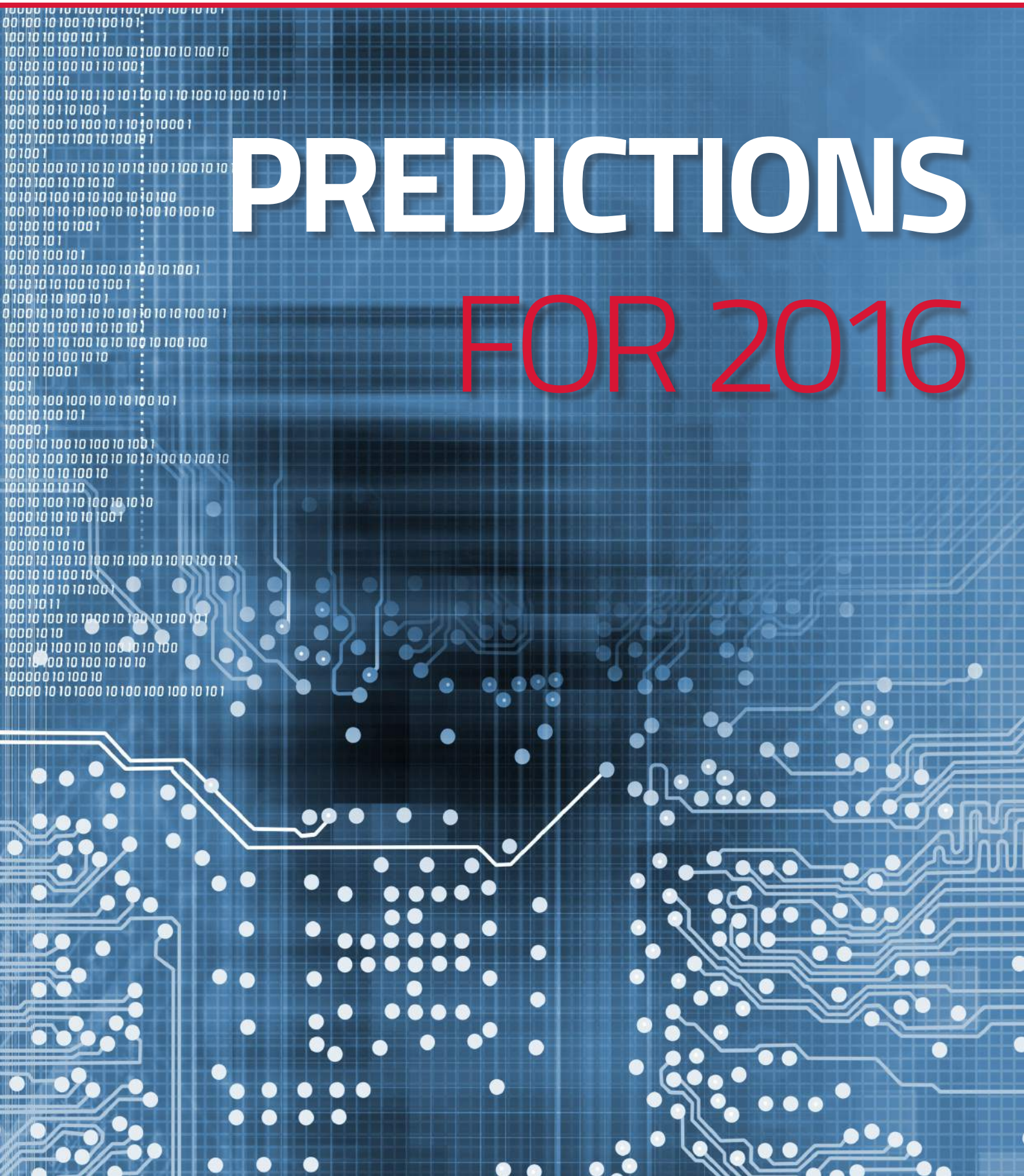
CCi

Cloud Computing Intelligence

www.cloudcomputingintelligence.com



PREDICTIONS FOR 2016

2016 Cyber Security Predictions

Sophos Labs experts offer their top predictions for the threats and exploits your business is liable to see in 2016

1. Android threats will become more than just headline-grabbers

Next year will see an increase in the number of Android exploits becoming weaponized (as opposed to bugs like Stagefright which was heavily reported earlier in 2015 but was never fully exploited). There are significant vulnerabilities on the Android platform which can take months to patch. Although Google claims that nobody has actually exploited these vulnerabilities to date, it will ultimately be an invitation too tempting for hackers to ignore.

SophosLabs has already seen samples that go to extreme lengths to avoid App Store detection and filtering—giving Apps a better chance of surviving on App stores. For example, some hackers will design an App that loads harmless games if it thinks it is being tested, but then loads the malicious payload when it detects it is 'safe' to do so. And more recently, we saw mobile users using third- party app markets, being tricked into granting malicious apps from the adware family Shedun with control over the Android Accessibility Service. Once they've handed over control the app has the ability to display popups that install highly intrusive adware, even if a user has rejected the invitation to install it. Because the apps root the device and embed themselves into the system partition they can't easily be uninstalled.

Android malware can be complicated and consumers cannot necessarily trust the App Store to detect these vulnerabilities in every instance.

2. Will 2016 be the year iOS malware goes mainstream?

We've already seen the Apple App Store get hit a few times this year, once with the InstaAgent app, which snuck through the vetting processes and which both Google and Apple pulled from their respective app stores, and before that, with XcodeGhost, which tricked Apple app developers into incorporating the code into their apps, thereby infecting them but cleverly hidden behind what looked like Apple code.

With more and more apps coming onto the market (both Apple and Google have more than a million apps each in their official marketplaces to date), it is not hard to imagine more criminals trying their hand at getting past the existing vetting processes. Nevertheless, the nature of Android, in particular support for the flexibility of third party markets will continue to contribute towards Android being an easier target than iOS.

3. IoT platforms – not yet the weapon of choice for commercial malware authors – but business beware

Every day, more and more technology is being incorporated into our lives. IoT (Internet of Things) devices are connecting everything around us and interesting new use cases are appearing constantly. IoT will continue to produce endless scary stories based on the fact that these devices are insecure (early 2015 saw many stories focusing on webcams, baby monitors and children's toys and latterly cars have become a hot topic – researchers hacked a jeep in July).

However, we won't see widespread examples of attackers getting IoT devices to run arbitrary code any time soon. Because they are not general purpose computing devices with the same broad suite of interfaces that we have on desktops/mobiles, IoT devices are relatively protected. What we will see is more research and Proof of Concepts demonstrating that non-vendor code can be installed on these devices because of insufficient validations (lack of code-signing, susceptibility to Man in the Middle-class exploitations) by the IoT vendors.

We can expect an increase in data-harvesting/leakage attacks against IoT devices, wherein they are coaxed to disclose information that they have access to, e.g. video/audio feeds, stored files, credential information for logging into cloud services, etc.

And as IoT devices evolve in their utility and ability to interact with their surroundings, i.e. as they become 'roboticized" – an app-controlled Roomba for example – the set of security concerns around IoT will start becoming very similar to the set of security concerns around SCADA/ICS, and the industry should look toward the best guidance that NIST, ICS-CERT and others have formulated.

4. SMBs will become a bigger target for cybercriminals

Throughout 2015, the focus has been on the big glamorous hacking stories like Talk Talk and Ashley Maddison, but it's not just big

businesses that are being targeted. A recent PwC report revealed that 74% of Small and Medium Businesses (SMBs) experienced a security issue in the last 12 months, and this number will only increase due to SMBs being perceived as 'easy targets'.

Ransomware is one area where criminals have been monetizing small businesses in a more visible way this year. Previously, payloads – such as sending spam, stealing data, infecting websites to host malware – were far less visible so that small businesses often didn't even realize they had been infected. Ransomware is highly visible and has the potential to make or break an SMB if they do not pay the ransom. This is why, of course, criminals are targeting SMBs. Expect to see this ramp in 2016.

Lacking the security budgets of large enterprises, SMBs often apply a best-effort approach to security investments, including equipment, services, and staffing. This makes them vulnerable as hackers can easily find security gaps and infiltrate the network. On average, a security breach can cost a small business anywhere up to £75,000 – a significant loss for any business. It's important therefore that SMBs take a consolidated approach to security. This requires a thoughtfully planned out IT strategy to prevent attacks before they happen. Installing software that connects the endpoint and the network will mean a comprehensive security system is in place where all components communicate, and ensure there are no gaps for hackers.

5. Data protection legislation changes will lead to increased fines for the unprepared

In 2016, the pressure on business to secure customers' data will increase as the EU data protection legislation looms closer. In future, business will face severe penalties if data isn't robustly secured. This will have a far reaching impact for how businesses deal with security, including the high risk area of employee personal devices.

Two major changes will be the EU General Data Protection Regulation (GDPR), and the Investigatory Powers Bill in the UK. The EU Data Protection regulation will come fully into force across Europe by the end of 2017, so companies need to start preparing in 2016. It has numerous components, but one key takeaway is that European businesses will now be held responsible for the protection of the data they process, including cloud providers and other third-parties.

In the UK, the Investigatory Powers Bill will modernise laws surrounding communications data. This will give the police and other intelligence bodies the ability to access all aspects of your communications on ICTs, whether you are suspected of a criminal offence or not. As this is due to go ahead in 2016, it will be interesting to see how this bill is shaped and shifted, and if people will start prioritising data security.

In the US, data protection is complicated by the fact there is no single overarching law. This has the effect that data protection tends to be less strict than in Europe, which has led to issues around the Safe Harbor agreement. Over time the US and Europe will hammer out their differences, but it seems unlikely that we will see a new agreement any time soon.

6. VIP Spoofware is here to stay

We'll see a growth in the use of VIP spoof wire transfers as we move into 2016. Hackers are becoming increasingly

talented at infiltrating business networks to gain visibility of personnel and their responsibilities, and then using this information to trick staff for financial gain. For example, sending an email to the finance team that appears to be from the CFO requesting the transfer of significant funds. This is just one of the ways we'll see criminals continue to target businesses.

7. Ransomware momentum

Ransomware will continue to dominate in 2016 and it is only a question of time before we see things beyond data being ransomed. It is perhaps some time off before we have a sufficient mass of internet-enabled cars or homes, but we should be asking the question: how long before the first car or house is held for ransom? Attackers will increasingly threaten to go public with data, rather than just taking it hostage and we have already seen websites being held ransom to DDoS. Many Ransomware families are using Darknets for either command or control, or for payment page gateways, as we saw with the likes of CryptoWall, TorrentLocker, TeslaCrypt, Chimera, and many more in 2015.

8. Social engineering is on the up

As cybersecurity comes to the fore and social engineering continues to evolve, businesses will invest more in protecting themselves from such psychological attacks. They will achieve this through investing in staff training, and ensuring there are strict consequences for repeat offenders. Employees need to be trained on how to be security savvy when on the company network.

Basic tips we would recommend incorporating into training include: Teaching staff about the implications of a phishing email and how to identify one; Ensuring staff don't click on malicious links that might be found in unsolicited emails; Encouraging staff to be wary that mis-spelt emails could be a sign of a scam; and to watch out for sites that ask for sensitive information, such as card PIN and national insurance number. Another golden rule is never to share a password. Each of us can help here by sending a signal to the market: let the providers who store your most valuable data (your bank, your health insurance company, your payroll management service, etc.) know that you demand strong security. If they don't give you the option to use multi-factor authentication, ask them why not? Or better still, just switch to a provider who does.

Finally, remind users of something they have probably all forgotten – don't open Office documents or pdfs unless you know who sent them and why. And never click 'yes" to warnings about macros or active content unless you know why the document needs it. We are already seeing a surge in downloaders of malicious code hiding in macros in legitimate looking office documents, and expect that to become huge in 2016.

9. Both bad and good guys will be more coordinated

The bad guys will continue to use coordinated attacks but the cyber security industry will make significant strides forward with information sharing. For some time the bad guys have been coordinating and collaborating, re-using tactics and tools, and generally keeping one step ahead of the cyber security industry. But the industry is now evolving and we expect to see the promising activity that has begun around information sharing and workflow automation continue and begin to deliver big differences in 2016 and onward.

10. Commercial malware authors will continue to invest heavily

Commercial malware authors will continue to reinvest at ever greater rates, bringing them towards the 'spending power' of nation-state activity. This includes purchasing zero days. These bad guys have lots of cash and they are spending it wisely.

11. Exploit kits will continue to dominate on the web

Exploit kits, like Angler (by far the most prevalent today) and Nuclear, are arguably the biggest problem we have on the web today as far as malware goes and this looks set to continue thanks to the thousands and thousands of poorly secured websites out there on the internet. Cyber criminals will exploit where they can most easily make money and therefore exploit kits have simply become stock tools of the trade, used by criminals to attempt to infect users with their chosen malware.