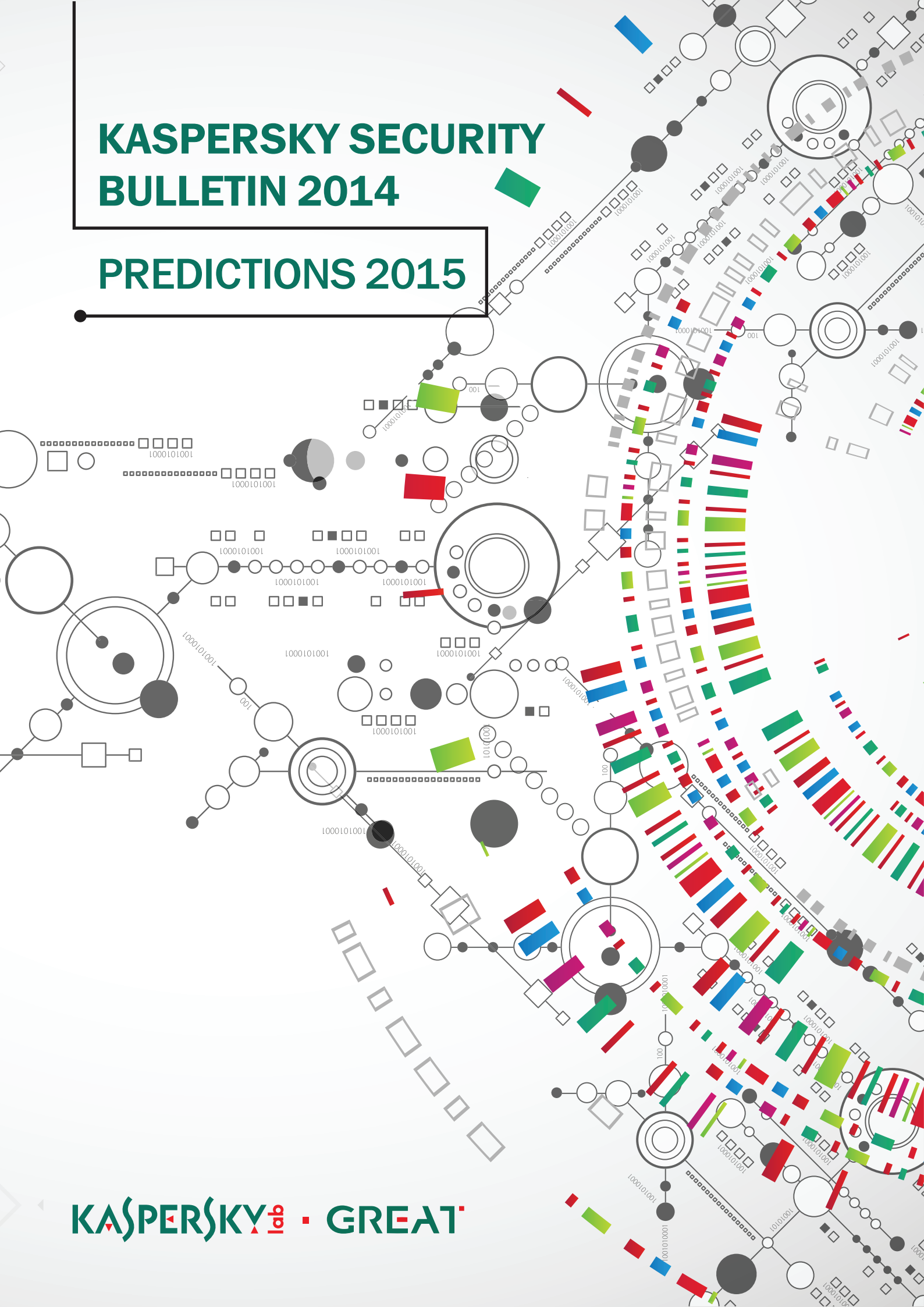
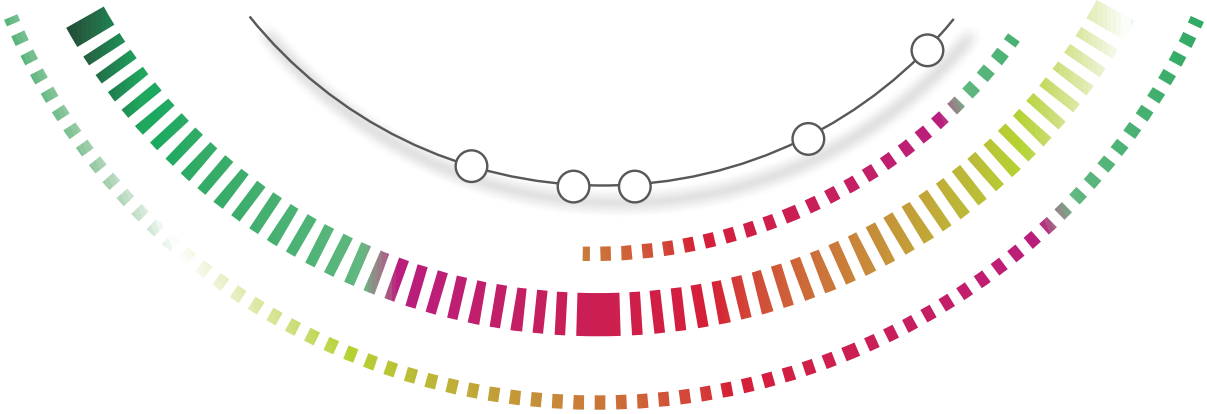
KASPERSKY SECURITY BULLETIN 2014

PREDICTIONS 2015



KASPERSKY lab · GREAT



CYBER-CRIMINALS MERGE WITH APT

In 2015, we expect to see another stage in the evolution of cyber-criminal activity with the adoption of APT tactics and techniques in financially motivated online criminal activity.

During a recent investigation, we discovered an attack in which an accountant's computer was compromised and used to initiate a large transfer with a financial institution. It represented the emergence of an interesting trend: targeted attacks directly against banks.

We are seeing an upsurge in malware incidents where banks are being breached using methods coming directly from the APT playbook. Once the attackers got into the banks' networks, they siphon enough information to allow them to steal money directly from the bank in several ways:

— Remotely commanding ATMs to dispose cash.

— Performing SWIFT transfers from various customers accounts,

— Manipulating online banking systems to perform transfers in the background.

Such attacks are an indication of a new trend that is embracing APT style attacks in the cybercriminal world.

APT GROUPS FRAGMENT, DIVERSIFY ATTACKS

The naming-and-shaming of APT groups in 2014 led to the public exposure and indictment of a hacking group that allegedly carried out cyber-espionage against U.S. businesses.

As security research teams continue to push for exposure of nation-state APT crews, we expect to see a shift in 2015 where the bigger, noisy APT groups splinter into smaller units, operating independently of each other. This in turn will result in a more widespread attack base, meaning more

companies will be hit, as the smaller groups diversify their attacks. At the same time it means that bigger companies that were previously compromised by two or three major APT groups (eg. Comment Crew and Webky) will see more diverse attacks, coming from more sources.

OLD CODE, NEW (DANGEROUS) VULNERABILITIES

Recent allegations of deliberate tampering and accidental failures in crypto implementations (“goto fail”), and critical vulnerabilities in essential software (Shellshock, Heartbleed, OpenSSL) have left the community suspicious of unaudited software. The reaction has been to either launch independent audits of key software or have security researchers poke them in search of critical vulnerabilities (tantamount to an unofficial audit). This means that 2015 will be another year of new, dangerous vulnerabilities appearing in old code, exposing the Internet infrastructure to menacing attacks.

ESCALATION OF ATM AND POS ATTACKS

Attacks against cash machines (ATM) seemed to explode this year with several public incidents and a rush by law enforcement authorities globally to respond to this crisis. A corollary of this publicity is an awareness that ATMs are ripe for the taking and cybercriminals are sure to notice. As most of these systems are running Windows XP and also suffer from frail physical security, they are incredibly vulnerable by default and, as the impersonal gatekeepers of the financial institutions’ cash, cybercriminals are bound to come knocking here first.

In 2015, we expect to see further evolution of these ATM attacks with the use of APT techniques to gain access to the “brain” of cash machines. The next stage will see attackers compromising the networks of banks and using that level of access to manipulate ATM machines in real time.

MAC ATTACKS: OS X BOTNETS

Despite efforts by Apple to lock down the Mac operating system, we continue to see malicious software being pushed via torrents and pirated software packages. The increasing popularity of Mac OS X devices is turning heads in the criminal world, making it more appealing to develop malware for this platform. The closed-by-default ecosystem makes it harder for this malware to successfully take hold of the platform, but there remains a subsection of users who'll gladly disable Mac OS X security measures – especially people who use pirated software. This means that those looking to hijack OS X systems for a variety of reasons know that they simply need to bundle their malware with desirable software (probably in the form of a key generator) to enjoy widespread success. Due to widespread beliefs about the security of the OS X platform, these systems are also unlikely to have an antimalware solution installed that will flag the infection so once the malware is installed, so it's likely to go unnoticed for a very long time.

ATTACKS AGAINST TICKETING MACHINES

Incidents such as the NFC hack on Chilean public transport show an interest in abusing public resources such as transportation systems. Some hackers won't be looking to turn a profit from these types of attacks and will be satisfied to get some free rides and 'stick it to the man' by sharing this ability with others. However, ticketing systems are being shown to be vulnerable (many of them running Windows XP) and in many cities handle credit card transaction data directly. We expect to see bolder attacks on these systems to either game the system or steal credit card data for themselves.

ATTACKS AGAINST VIRTUAL PAYMENT SYSTEMS

Conventional wisdom tells us that cybercriminals are looking to monetize their daring exploits as simply and efficiently as possible. What better target than virtual payment systems in their infancy? As some countries like Ecuador rush to adopt virtual payment systems, we expect criminals to leap at every opportunity to exploit these. Whether social engineering the users, attacking the endpoints (cellphones in many cases), or hacking the banks directly, cybercriminals will jump all over directly monetized attacks and virtual payment systems will end up bearing the brunt.

These fears can also be extended to the new Apple Pay, which uses NFC (Near Field Communications) to handle wireless consumer transactions. This is a ripe market for security research and we expect to the appearance of vulnerability warnings about weaknesses in Apple Pay, virtual wallets and other virtual payment systems.

APPLE PAY

Previous attacks have focused on NFC payment systems but, thanks to limited adoption, these have reaped limited rewards. Apple Pay is bound to change that. The enthusiasm over this new payment platform is going to drive adoption through the roof and that will inevitably attract many cybercriminals looking to reap the rewards of these transactions. Apple's design possesses and increased focus on security (like virtualized transaction data) but we'll be very curious to see how hackers will exploit the features of this implementation.

COMPROMISING THE INTERNET OF THINGS

Attacks against the Internet of Things (IoT) have been limited to proof-of-concepts and (sometimes overhyped) warnings that smart televisions and refrigerators will be targeted by hackers to create botnets or launch mischievous attacks.

As more and more of these connected devices become available, we expect to see a wider discussion about security and privacy, especially among businesses in this space. In 2015, there will surely be in-the-wild attacks against networked printers and other connected devices that can help an advanced attacker to maintain persistence and lateral movement within a corporate network. We expect to see IoT devices form part of an APT group's arsenal, especially at high-value targets where connectivity is being introduced to the manufacturing and industrial processes.

On the consumer side, IoT attacks will be limited to demonstrations of weaknesses in protocol implementations and the possibility of embedding advertising (adware/spyware?) into smart TV programming.