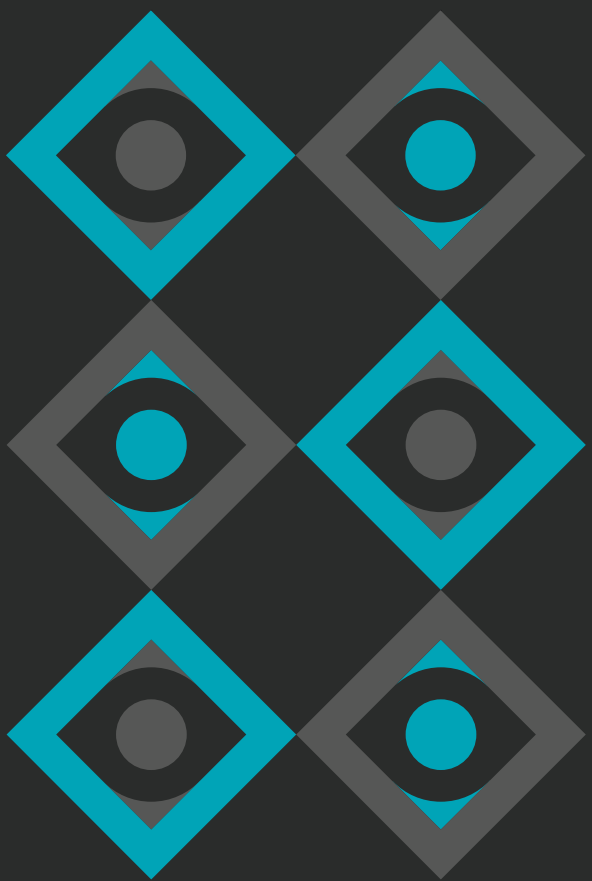
Executive summary

Section

01



Symantec

Cyber attackers revealed new levels of ambition in 2016, a year marked by extraordinary attacks, including multi-million dollar virtual bank heists, overt attempts to disrupt the US electoral process by state-sponsored groups, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices.

While cyber attacks managed to cause unprecedented levels of disruption, attackers frequently used very simple tools and tactics to make a big impact. Zero-day vulnerabilities and sophisticated malware now tend to be used sparingly and attackers are increasingly attempting to hide in plain sight. They rely on straightforward approaches, such as spear-phishing emails and "living off the land" by using whatever tools are on hand, such as legitimate network administration software and operating system features.

Mirai, the botnet behind a wave of major DDoS attacks, was primarily composed of infected routers and security cameras, low-powered and poorly secured devices. In the wrong hands, even relatively benign devices and software can be used to devastating effect.

Targeted attacks: Subversion and sabotage come to the fore

The world of cyber espionage experienced a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries. Cyber attacks against the US Democratic Party and the subsequent leak of stolen information were one of the major talking points of the US presidential election. With the US Intelligence Community attributing the attacks to Russia and concluding the campaign would have been judged a success, it is likely these tactics will be reused in efforts to influence politics and sow discord in other countries.

Cyber attacks involving sabotage have traditionally been quite rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in Ukraine in January and again in December, attacks which also resulted in power outages. Meanwhile the disk-wiping Trojan Shamoon reappeared after a four-year absence and was used against multiple organizations in Saudi Arabia.

The upsurge in disruptive attacks coincided with a decline in some covert activity, specifically economic espionage, the theft of intellectual property, and trade secrets. Following a 2015 agreement between the US and China, which saw both countries promise not to conduct economic espionage in cyber space, detections of malware linked to suspected Chinese espionage groups dropped considerably. However, this does not mean economic espionage has disappeared entirely and comes at a time when other forms of targeted attack, such as subversion or high-level financial attacks, have increased.

Financial heists: Cyber attackers chase the big scores

Until recently, cyber criminals mainly focused on bank customers, raiding accounts or stealing credit cards. However, a new breed of attacker has bigger ambitions and is targeting the banks themselves, sometimes attempting to steal millions of dollars in a single attack. Gangs such as Carbanak have led the way, demonstrating the potential of this approach by pulling off a string of attacks against US banks.

During 2016, two other outfits upped the ante by launching even more ambitious attacks. The Banswift group managed to steal US$81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its SWIFT credentials, allowing them to make the fraudulent transactions.

Another group, known as Odinaff, was also found to be mounting sophisticated attacks against banks and other financial institutions. It too appeared to be using malware to hide customers' own records of SWIFT messages relating to fraudulent transactions carried out by the group.

While Banswift and Odinaff demonstrated some technical expertise and employed tactics associated with advanced groups, much less sophisticated groups also stole massive sums of money. Business email compromise (BEC) scams, which rely on little more than carefully composed spear-phishing emails, continue to cause major losses; more than $3 billion has been stolen in the past three years.

Living off the land

Attackers ranging from cyber criminals to state-sponsored groups have begun to change their tactics, making more use of operating system features, off-the-shelf tools, and cloud services to compromise their victims. The most high-profile case of a living off the land attack took place during the US elections. A simple spear-phishing email provided access to Hillary Clinton's campaign chairman John Podesta's Gmail account without the use of any malware or vulnerabilities.

"Living off the land"—making use of the resources at hand rather than malware and exploits—provides many advantages to attackers. Identifying and exploiting zero days has become harder as improvements in secure development and bounty programs take hold. Web attack toolkits have fallen out of favor, likely due to the effort required in maintaining fresh exploits and a backend infrastructure.

Powerful scripting tools, such as PowerShell and macros, are default features of Windows and Microsoft Office that can facilitate remote access and malware downloads without the use of vulnerabilities or malicious tools. Despite existing for almost 20 years, Office macros have reemerged on the threat landscape as attackers use social engineering techniques to easily defeat security measures that were put in place to tackle the erstwhile problem of macro viruses.

When executed well, living off the land approaches can result in almost symptomless infections, allowing attackers to hide in plain sight.

Resurgence of email as favored attack channel

Malicious emails were the weapon of choice for a wide range of cyber attacks during 2016, used by everyone from state-sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years.

Email's renewed popularity has been driven by several factors. It is a proven attack channel. It doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials. Spear-phishing emails, such as spoofed emails instructing targets to reset their Gmail password, were used in the US election attacks.

Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were meanwhile the favored means of spreading ransomware. The availability of spam botnets-for-hire, such as Necurs, allowed ransomware groups to mount massive email campaigns during 2016, pumping out hundreds of thousands of malicious emails daily.

Ransomware squeezing victims with escalating demands

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to $1,077, up from $294 a year earlier.

Attackers have honed a business model that usually involves malware hidden in innocuous emails, unbreakable encryption, and anonymous ransom payment involving cryptocurrencies. The success of this business model has seen a growing number of attackers jump on the bandwagon. The number of new ransomware families uncovered during 2016 more than tripled to 101 and Symantec logged a 36 percent increase in ransomware infections.

New frontiers: IoT and cloud move into the spotlight

While ransomware and financial fraud groups continue to pose the biggest threat to end users, other threats are beginning to emerge. It was only a matter of time before attacks on IoT devices began to gain momentum, and 2016 saw the first major incident with the emergence of Mirai, a botnet composed of IoT devices such as routers and security cameras. Weak security made these devices easy pickings for attackers, who constructed a botnet big enough to carry out the largest DDoS attack ever seen. Symantec witnessed a twofold increase in attempted attacks against IoT devices over the course of 2016 and, at times of peak activity, the average IoT device was attacked once every two minutes.

Several of Mirai's targets were cloud-related services, such as DNS provider Dyn. This, coupled with the hacking of millions of MongoDB databases hosted in the cloud, shows how cloud attacks have become a reality and are likely to increase in 2017. A growing reliance on cloud services should be an area of concern for enterprises as they present a security blind spot. Symantec found that the average organization was using 928 cloud apps, up from 841 earlier in the year. However, most CIOs think their organizations only use around 30 or 40 cloud apps, meaning the level of risk could be underestimated, leaving them open to attack from newly emergent threats.

Breaches

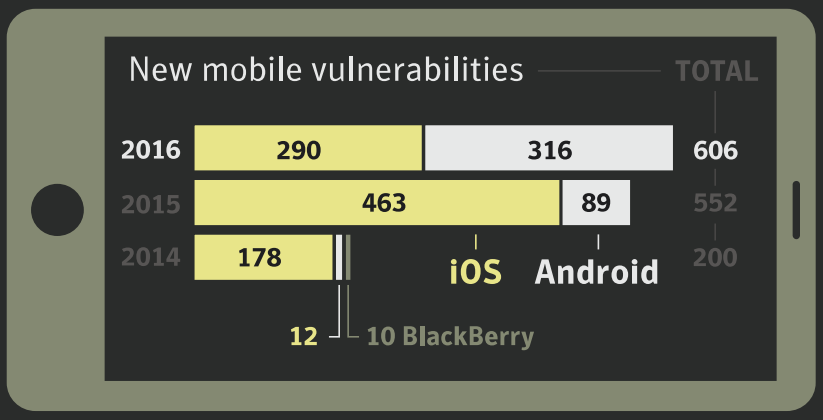
	2014	2015	2016
Total breaches	1,523	1,211	1,209
Breaches with more than 10 million identities exposed	11	13	15
Total identities exposed	1.2B	564M	1.1B
Average identities exposed per breach	805K	466K	927K

In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

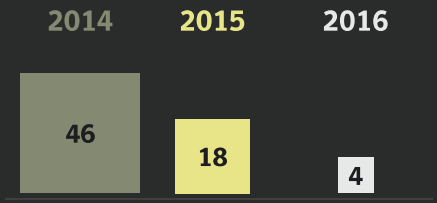
Email threats, malware, and bots

	2014	2015	2016
Spam rate %	60%	53%	53%
Phishing rate	1 in 965	1 in 1,846	1 in 2,596
Email malware rate	1in 244	1in 220	1in 131
New malware variants	275M	355M	357M
Number of bots		91.9M	98.6M

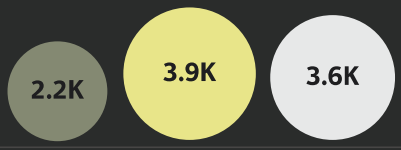
Mobile



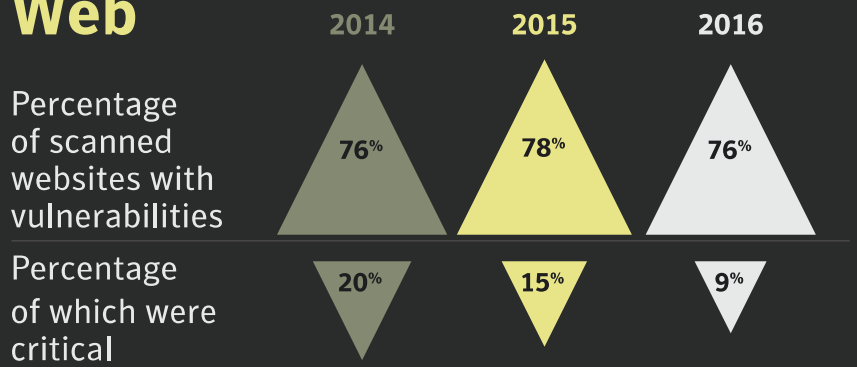
New Android mobile malware families



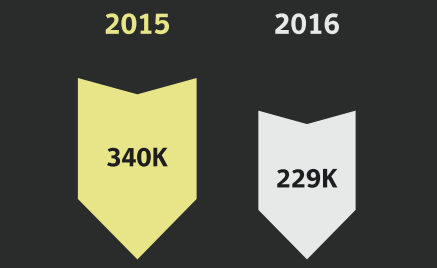
New Android mobile malware variants



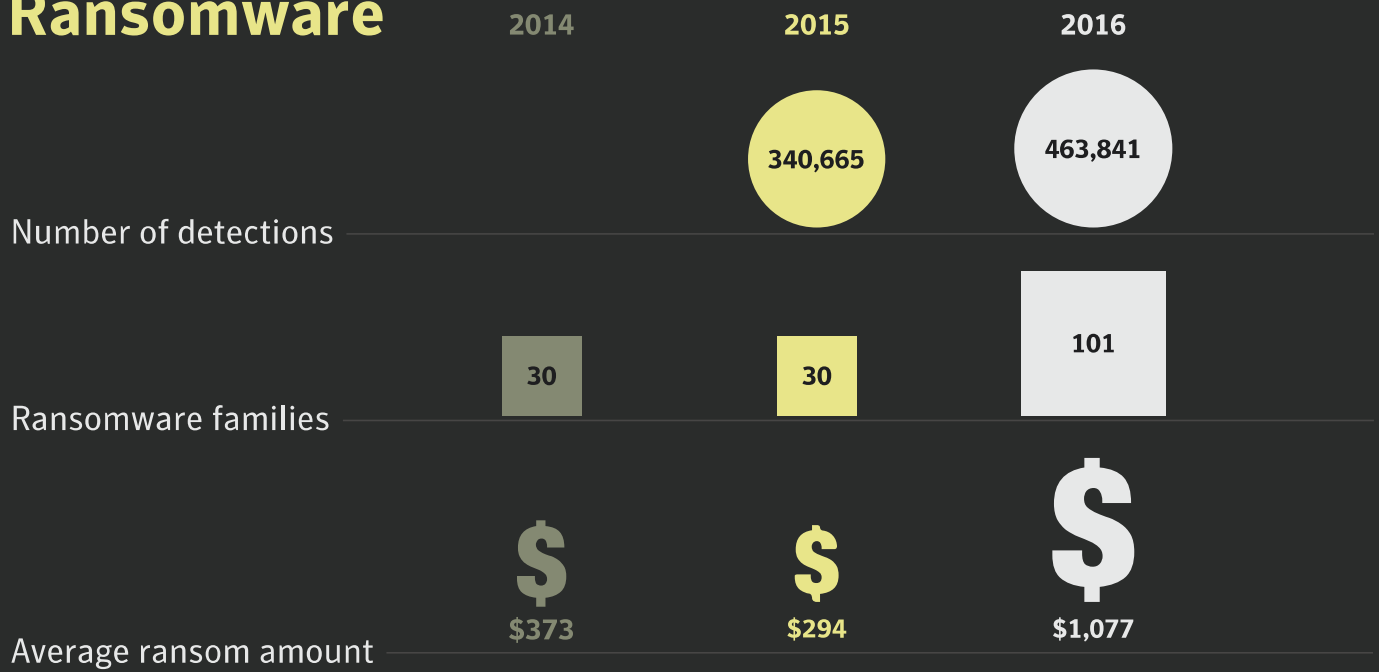
Web



Average number of web attacks blocked per day



Ransomware



Cloud

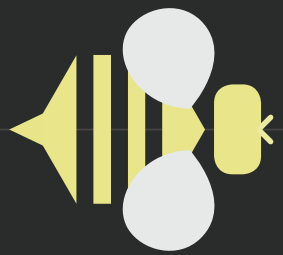
	JUL-DEC 2015	JAN-JUN 2016	JUL-DEC 2016
Average number of cloud apps used per organization	774	841	928
Percentage of data broadly shared	25%	23%	25%

Internet of Things

2 minutes: time it takes for an IoT device to be attacked

Speed of attack

Number of attacks against Symantec honeypot **per hour**



JAN|**2016** DEC|**2016**