Trustwave®

2013 GLOBAL SECURITY REPORT PREVIEW

WE TESTED,
WE ANALYZED,
WE DISCOVERED

EXECUTIVE SUMMARY

DURING 2012, NEARLY EVERY INDUSTRY, COUNTRY AND TYPE OF DATA WAS INVOLVED IN A BREACH OF SOME KIND.

Cybersecurity threats are increasing as quickly as businesses can implement measures against them. At the same time, businesses must embrace virtualization and cloud, user mobility and heterogeneous platforms and devices. They also have to find ways to handle and protect exploding volumes of sensitive data. The combination of business and IT transformation, compliance and governance demands and the onslaught of security threats continues to make the job of safeguarding data assets a serious challenge for organizations of all types—from multinational corporations to independent merchants to government entities.

Today, organizations need not only to understand current trends in security threats but also be able to identify inherent vulnerabilities within existing systems. In the 2013 Global Security Report, Trustwave tested, analyzed and discovered the top vulnerabilities and threats that have the most potential to negatively impact organizations. Read on for the key discoveries of 2012 and trends to watch in 2013 and beyond.

KEY DISCOVERIES

Retail businesses and their sensitive data are back in the crosshairs. For the first time in three years, the retail industry made up the highest percentage of investigations at 45%.

Web applications have now emerged as the most popular attack vector. E-commerce sites were the No. 1 targeted asset, accounting for 48% of all investigations.

Mobile malware explodes by 400%. As organizations embrace mobility, mobile malware continues to be a problem for Android, with the number of samples in Trustwave's collection growing 400% in 2012.

Businesses are embracing an outsourced IT operations model. In 63% of incident response investigations, a major component of IT support was outsourced to a third party. Outsourcing can help businesses gain effective, cost-friendly IT services; however, businesses need to understand the risk their vendors may introduce and proactively work to decrease that risk.

Businesses are slow to "self-detect" breach activity. The average time from initial breach to detection was 210 days, more than 35 days longer than in 2011. Most victim organizations (64%) took over 90 days to detect the intrusion, while 5% took three or more years to identify the criminal activity.

More responsibility falls onto security staff to stay on top of zero-day attacks. Software developers vary greatly in their ability to respond and patch zero-day vulnerabilities. In this study, the Linux platform had the worst response time, with almost three years on average from initial vulnerability to patch.

Spam volume declines, but impact on the business doesn't. Spam volume shrank in 2012 to a level lower than it was in 2007 but spam still represents 75.2% of a typical organization's inbound email. Most importantly, new malware research conducted by Trustwave found nearly 10% of spam messages to be malicious.

Basic security measures are still not in place. "Password1" is still the most common password used by global businesses. Of three million user passwords analyzed, 50% of users are using the bare minimum.

TACTICAL THREAT INTELLIGENCE

ENCRYPTION SOPHISTICATION **25%**

The **use of encryption by attackers** during data exfiltration is on the rise; over 25% of all data was encrypted by cybercriminals.

MEMORY SCRAPING DOMINANT **50%**

The **most popular malware family was memory scraping**; 20% of new case samples included memory scraping functionality, and such activity was detected in almost 50% of investigations where associated malware had identifiable data collection functionality.

PDF FILES AT RISK **61%**

Of all client-side attacks observed, 61% **targeted Adobe Reader users** via malicious PDFs.

BLACKHOLE ON THE RISE **70%**

Versions of the **Blackhole exploit kit made up over 70% of all client-side attacks** serving up zero-day exploits.

SQL & REMOTE STILL REIGN **73%**

Always the two most noteworthy methods of intrusion, **SQL injection and remote access** made up 73% of the infiltration methods used by criminals in 2012.

LOOKING AHEAD

Cybercriminals will never stop trying to compromise systems to obtain data. Organizations need to be aware of where they may be open to attacks, how attackers can enter their environment and what to do if (and when) an attack occurs. The 2013 Trustwave Global Security Report identifies the most serious and common vulnerabilities, how cybercriminals are breaking in and what they're mostly likely to steal. Based on research and analysis of hundreds of investigations and thousands of client engagements, the report further offers six key security pursuits for 2013, highlighting the tools organizations need to evaluate in order to build a comprehensive information security strategy that can reduce risk, protect data and safeguard their reputations.

TO DOWNLOAD THE FULL 2013 TRUSTWAVE GLOBAL SECURITY REPORT, VISIT WWW.TRUSTWAVE.COM/2013GSR

TO DOWNLOAD THE FULL 2013 TRUSTWAVE GLOBAL SECURITY REPORT, VISIT WWW.TRUSTWAVE.COM/2013GSR

CORPORATE HEADQUARTERS
70 West Madison St.
Suite 1050
Chicago, IL 60602
P: 312 873 7500
F: 312 443 8028

EMEA HEADQUARTERS
Westminster Tower
3 Albert Embankment
London SE1 7SP
P: +44 (0) 845 456 9611
F: +44 (0) 845 456 9612

APAC HEADQUARTERS
Suite 3, Level 7 100 Walker St.
North Sydney NSW 2060
Australia
P: +61 0 2 9466 5800
F: +61 0 2 9466 5899

LAC HEADQUARTERS
Rua Cincinato Braga, 340 nº 71
Edificio Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 - BRASIL
P: +55 (11) 4064-6101