THE BITGLASS "WHERE'S YOUR DATA?" EXPERIMENT +

WHO'S KEEPING TABS ON YOUR DATA? +

BITGLASS REPORT

bitglass

THE STORY

Visibility into where sensitive data is travelling has never been so crucial. With breaches like Target, Home Depot, JP Morgan, Sony and Anthem - the ability to track data is a necessity.

Today, the majority of breaches stem from malware and hacks, which make up 53% of all breaches. Shockingly, it takes 205 days before the average breach is finally recognized and snuffed out. Given this ability for cyber criminals to stay one step ahead of IT heroes, it's only a matter of time until the next newsworthy breach hits the mainstream headlines (Premera, anyone?).

205

Avg. days to discover breach

Did you ever wonder what happens to all of that sensitive data once it is actually stolen? Does it simply sit on a hacker's device collecting digital dust, is it shared with friends, or is it sold off on the black market to the highest Bitcoin bidder? In January 2015, Bitglass set forth on a mission to answer the question, "where is your data?"

The challenge? Daunting. The findings? Fascinating.

Bitglass' data tracking and watermarking technologies allow enterprises to track their data anywhere it goes. Key foundational technology in-hand, we conducted the **world's first data tracking experiment in the Dark Web,** using common hacker techniques to target our unsuspecting criminal victims.

BEHIND THE SCENES

Bitglass' security research team wrote a tool to generate several thousand very real looking names, social security numbers, credit card numbers, addresses, phone numbers, and more. We saved this data to an Excel spreadsheet, creating versions with different names to find which was the best criminal click bait. This was world's first A/B test for stolen credit card numbers on the Dark Web.

The files were downloaded through the Bitglass proxy service, where a unique watermark was applied to each copy, ensuring that from that point forward, it would call back to Bitglass each time the data was viewed and/or downloaded.

The next step? Finding takers (and it turns out there were plenty). We used a common hacker tactic called "phishing" to entice criminals into taking the bait. To do that, we went where they hang out - the Dark Web.

WHAT IS THE "DARKWEB"?

The Dark Web is a part of the web not indexed by Google and other popular search engines and estimated to be about 500 times larger than the normal Internet. Getting to and using the Dark Web requires a new set of tools, but your primary weapon is ToR and a ToR browser, cyber criminals' system du jour for anonymity online.

THE TECHNOLOGY

Whether files are downloaded from your email provider or sent as an attachment, **Bitglass allows enterprises to watermark their files with a unique fingerprint that identifies who downloaded the file, from what device and when the transaction occurred**. Once watermarked, the Bitglass service is notified every time that file is accessed, allowing you to track corporate data anywhere it goes. The watermark persists even if sections of the document are copied over to another document. All tracking data can be viewed via the Bitglass customer portal.

ALLOWS ENTERPRISES TO MAINTAIN

CONTROL & VISIBILITY

THE FINDINGS

The speed at which the bait was taken was staggering. In the first few days, **the data had reached over 5 countries, 3 continents and was viewed over 200 times**... by 12 days it had received over **1,081 clicks**, and had spread across the globe to **22 different countries**, in **5 different continents**. By the end of the experiment the fake document of employee data had made its way to North America, South America, Asia, Europe, and Africa.

Countries frequently associated with cyber criminal activity, including Russia, China and Brazil, were the most common access points for the identity data. Additionally, time, location, and IP address analysis uncovered a high rate of activity amongst two groups of similar viewers, indicating the possibility of **two cyber crime syndicates**, one operating within Nigeria and the other in Russia.

THE FAKE DATA TRAVELLED TO 22 DIFFERENT COUNTRIES AND 5 OF THE WORLD'S 7 CONTINENTS

COUNTRIES

1. US
2. BELGIUM
3. BRAZIL
4. NIGERIA
5. HONG KONG
6. SPAIN
7. GERMANY
8. UNITED KINGDOM
9. FRANCE
10. SWEDEN
11. FINLAND
12. MALDIVES
13. NEW ZEALAND
14. NORWAY
15. RUSSIAN FEDERATION
16. NETHERLANDS
17. CZECH REPUBLIC
18. DENMARK
19. ITALY
20. CANADA
21. TURKEY
22. LUXEMBOURG

CONTINENTS

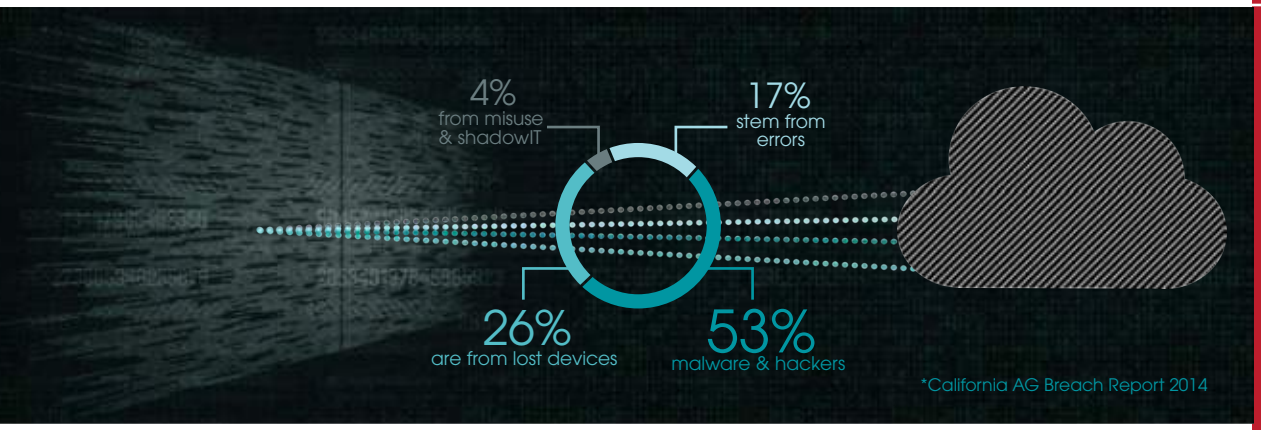
1. NORTH AMERICA
2. ASIA
3. EUROPE
4. AFRICA
5. SOUTH AMERICA

IMPLICATIONS FOR THE PUBLIC

Once sensitive data has been stolen, there is no limit to how far that data will travel, and how many different people will get their virtual hands on it. Although the level of access after just 12 days was extraordinary; **imagine how much further the data would spread in 205 days,** the average time it takes for enterprises to detect a corporate data breach.

But there is a light at the end ot the tunnel. Even though breaches are inevitable, there are still ways of limiting the damage that comes as a result of them. The key is being able to track and identify data as it leaves your network. Because without this, there is no telling who has access to your data, or what they plan to do with it...

+ DATA BREACH DISCOVERY +



LIMIT THE DAMAGE

Using proprietary threat intelligence and big data technologies, Bitglass Data Breach Discovery analyzes your firewall logs to identify suspect traffic in outbound data flows. Traffic leaving your network for suspect destinations is automatically subject to deep inspection and assigned risk scores.

Bitglass Data Breach Discovery is available as a monthly subscription service. No software to install - simply sign up for Bitglass and upload your firewall log files to get analytics and reports on data breach risk in your organization.

bitglass

ABOUT BITGLASS

In a world of applications and mobile devices, IT must secure data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they are developed to secure the corporate network perimeter. Bitglass is a Cloud Access Security Broker that delivers innovative technologies that transcend the network perimeter to deliver total data protection for the enterprise - in the cloud, on mobile devices and anywhere on the internet.

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Bitglass is based in Silicon Valley and backed by venture capital from NEA, Norwest and Singtel Innov8.

For more information, visit
www.bitglass.com

Phone: (408) 337-0190
Email: info@bitglass.com

/bitglass
/bitglassinc
/+Bitglass
/bitglass-inc