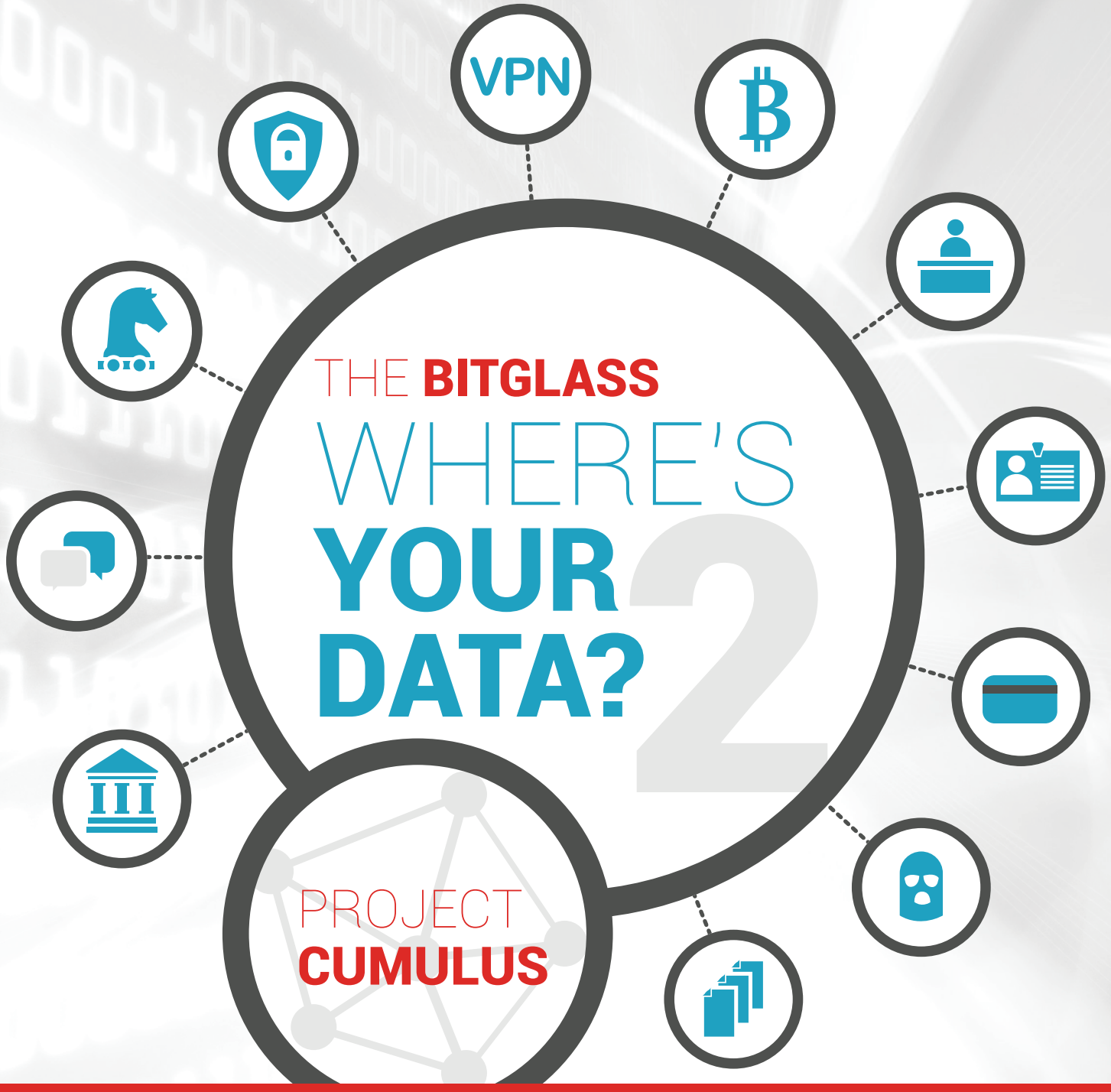


THE BITGLASS WHERE'S YOUR DATA? 2

PROJECT CUMULUS

WHAT HAPPENS WHEN YOUR **PASSWORD** IS **COMPROMISED?**

BITGLASS REPORT

bitglass

THE EXPERIMENT

Imagine one of your employees falls victim to a phishing attack, their login credentials to a cloud application compromised, unfortunately a common scenario for many enterprises today. What happens next? How fast does their password spread? What information are hackers most interested in accessing? How do hackers go about using the victim's personal information and how quickly do they attempt to access other cloud or on-premises applications?

To answer these questions, the Bitglass Research team created a complete digital identity for an employee of a fictitious retail bank, a functional web portal for the bank, and a Google Drive account, complete with seemingly real corporate and personal data. Among the files in the Google Drive were documents containing real credit card numbers, work-product, and more. The team then leaked the employee's "phished" Google Apps credentials to the Dark Web. What the hackers didn't know was that each file in the Google Drive was embedded with a watermark and all activities, from logins to downloads, were being tracked by Bitglass, deployed in monitor-only mode.

THE NUMBERS

OVER **1400**

HACKERS

VIEWED THE CREDENTIALS

1 in 10

HACKERS

WHO VIEWED THE CREDENTIALS ATTEMPTED TO LOG INTO THE BANK WEB **PORTAL**

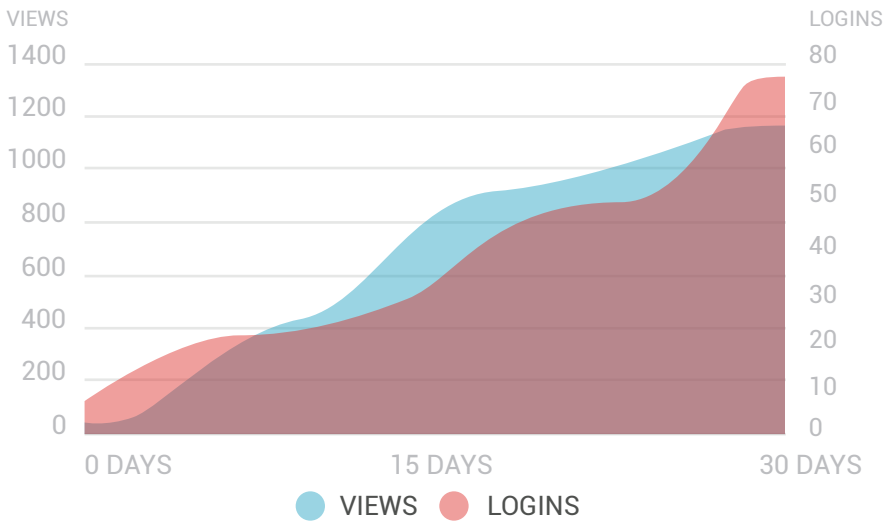
68%

GOOGLE DRIVE AND BANK LOGINS FROM **TOR-ANONYMIZED** IP ADDRESSES

12%

OF GOOGLE DRIVE HACKERS ATTEMPTED TO **DOWNLOAD FILES** WITH **SENSITIVE CONTENT**

A torrent of activity resulted within hours of leaking the credentials, with over 1400 visits from over 30 countries recorded between the Dark Web postings and the bank web portal.



HACKED ONCE, HACKED EVERYWHERE

Like many internet users, our fictitious bank employee used the same password across several web services including social media sites and personal banking accounts. Once hackers successfully accessed the employee's Google Drive using the leaked credentials, we discovered that most attempted to use those same credentials elsewhere.

Hackers were unrelenting when it came to accessing the victim's other accounts, in fact 36 percent successfully accessed the victim's personal banking account using the leaked password. Bitglass researchers also observed several recurring logins, some within hours of one another, others weeks after the initial login.

THE NUMBERS

94%

UNCOVERED AND ATTEMPTED TO LOG INTO OTHER **ACCOUNTS**

5

ATTEMPTED BANK LOGINS IN THE FIRST **24 HOURS**

3

ATTEMPTED GOOGLE DRIVE LOGINS IN THE FIRST **24 HOURS**

WITHIN

48

HOURS THE FIRST FILE WAS **DOWNLOADED**

VISITORS TO THE **BANK SITE** CAME FROM OVER **30 DIFFERENT COUNTRIES** ACROSS **6 CONTINENTS**

TOR:
AN OBSTACLE TO TRACKING

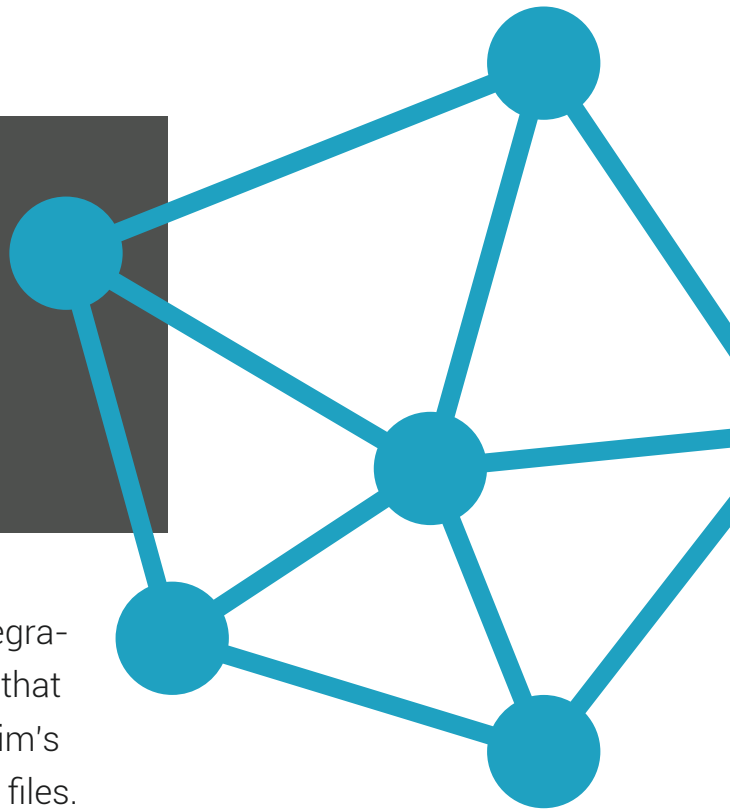
The bank experiment revealed that 68 percent of hackers, an incredibly high proportion, accessed both the Google Drive and the bank portal from Tor-anonymized IP addresses. One dark web community member encouraged novice hackers to use Tor in conjunction with a VPN service purchased using cryptocurrency, warning that any missteps could lead to prosecution under the Computer Fraud and Misuse Act.

The high rate of Tor usage in Project Cumulus and new document downloads from the original data experiment indicates hackers are becoming more security conscious and know to mask their IPs when possible to avoid getting caught.

HACKERS THAT DIDN'T USE TOR ATTEMPTED LOGINS FROM **CALIFORNIA** AND **WISCONSIN** IN **THE US**, **AUSTRIA, NETHERLANDS, PHILIPPINES,** AND **TURKEY.**

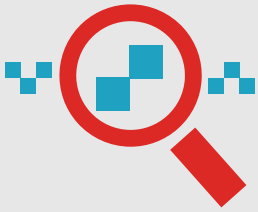
In the prior "**Where's Your Data?**" experiment, the Bitglass team leaked **watermarked documents** onto the **Dark Web**. Downloads quickly fell after the initial leak, but on the Dark Web, **leaked data** can always resurface. After an eight month quiet period, Bitglass researchers were alerted to a **sudden spike in downloads** of these documents, all **via Tor**.

LEAKED **CORPORATE DATA**



Bitglass activity logs, drawn from integration with the Google Apps API, reveal that many hackers who accessed the victim's Google Drive were quick to download files. Some mass downloaded all files hoping to find something of value, while others downloaded just those with the most sensitive content, most notably documents with real credit card data and bank customer information. One visitor went so far as to crack and view an encrypted file stored in Google Drive. Files that appeared to contain sensitive financial information were quickly opened (as verified by Bitglass watermarking "callbacks").

While no transactions were conducted on the real credit cards in the days immediately following the leak, we continue to monitor activity with the expectation that hackers will use or sell the credit card data in the near future.



OTHER OCCURENCES

- Hackers changed the victim's password
- Several attempts were made to crawl the Google Drive using third-party apps
- Some downloaded files that did not appear sensitive, including lunch menus

PREVENTING SIMILAR BREACHES

AVOID **REUSING PASSWORDS,** IMPLEMENT CONTEXTUAL **MULTIFACTOR AUTHENTICATION.**

By limiting password reuse and supporting more secure means of authentication, many successful bank portal logins could have been prevented. A solution like Bitglass, that boasts integrated identity management with support for single sign-on, multi-factor authentication, single-use passwords, and more, is essential. Suspicious logins and activities should always prompt for MFA.

SET UP **ALERTS** FOR **UNUSUAL ACTIVITY**

Whether your organization suffers a breach due to a targeted attack or use of an unsanctioned cloud app, IT needs a means of discovering potential breaches across all cloud applications. With cloud access security broker (CASB) technology, IT administrators are quickly alerted to unusual activity like that seen in the bank employee's Google Drive, particularly where multiple logins are coming in from distant geos, and can act to limit the damage. Watermarking technology can also provide a glimpse into suspicious use of data that has been downloaded from cloud apps. When combined with machine learning techniques to baseline user behavior and identify deviations, a CASB can find the suspicious needles in the haystack of sensitive data access.

APPLY **DATA LEAKAGE PREVENTION** POLICIES TO **CONTROL ACCESS.**

For public cloud apps like Google Drive, the ability to limit and prevent access in suspicious contexts is key to protecting sensitive data. In the case of the bank, IT could have used a CASB solution, like the one offered by Bitglass, to identify the suspicious login attempts and prevent downloads of customer information from the cloud, or to block upload of sensitive data to the cloud outright (e.g. credit card numbers). Just as Bitglass researchers applied watermarking technology to files stored in the bank employee's Google Drive, IT can leverage Bitglass' native DLP tools to track and secure corporate data.

bitglass

ABOUT BITGLASS

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

For more information, visit www.bitglass.com

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