BITSIGHT *Insights*

Beware the Botnets:
Botnets Correlated to a Higher Likelihood of a Significant Breach

April 2015

BITSIGHT Insights

Beware the Botnets

Major data breaches affecting some of world's largest organizations have elevated cyber security to a top concern of executives and board directors. Beyond grabbing headlines, these data loss events can result in serious repercussions for businesses, including financial and reputational damage.

Perhaps the most prominent example is the highly publicized Target breach, estimated to cost the retailer $162 million (after $90 million in insurance compensation) and resulting in the termination of the CEO and public criticism of the board by a shareholder advocacy group. While companies' systems are frequently breached, it is the severe breaches -- where thousands (and, in many cases, millions) of records containing sensitive information were exposed -- that often result in public disclosure. These large scale breaches show little sign of abating; a recent survey from the Pew Research Center found that cyber attacks are likely to increase in coming years, according to top technology leaders. In response to this growing threat, organizations are actively looking to assess the likelihood of being directly affected by a major data breach event. By better understanding key indicators of vulnerability to breaches, executives and directors can begin to effectively mitigate the risk of a data breach.

Recognizing the growing importance of providing credible metrics to assess and mitigate the impact of threats, BitSight has performed an analysis of the risk vectors that comprise BitSight Security Ratings and publicly disclosed data breaches. One important risk vector is botnets, networks of computers that have been compromised or infected with malicious software and controlled as a group by an adversary without the owners' knowledge. A botnet infection means that an attacker has obtained partial or complete administrative control of a system. Although a botnet compromise may not always equate to data loss, it invariably means that one or many protective controls have failed and that at least some data or system confidentiality, integrity, or availability is at risk.

This study indicates that there is a solid correlation between BitSight botnet grades and publicly disclosed breaches. More specifically, **companies with a BitSight botnet grade of B or lower were more than twice as likely to experience a publicly disclosed data breach.** BitSight botnet grades (which are a component of the top-level security rating) can therefore serve as a key metric for executives, board members, insurers, and security and risk teams. This correlation provides important insight that can be leveraged for the following initiatives:

- Benchmarking your organization against peers
- Vendor risk assessment and engagement
- Cyber underwriting decision making
- M&A due diligence

BitSight Technologies provides organizations worldwide with data-driven ratings to quickly and objectively measure cyber risk. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. Armed with daily ratings, organizations can proactively identify, quantify and manage cyber security risk throughout their ecosystem. This automated service analyzes, rates, and monitors security performance, all from outside the company. Rated organizations do not need to provide any information to BitSight.

Study Overview

Recent analysis suggests a strong statistical relationship between publicly disclosed data breaches and the factors that go into an organization's security rating. Findings show that companies with poor grades are more likely to have experienced a publicly disclosed data breach in the past. Botnet grades, in particular, have shown a solid correlation with publicly disclosed breaches. Also called "zombie armies," botnets are used to steal confidential data such as passwords and credit card information, send spam messages, relay viruses, or even conduct distributed denial-of-service attacks. The data used to compute this grade is derived from a variety of distributed sources and methods from around the globe. The majority of the botnet measurement data for this analysis originates from proprietary streams from AnubisNetworks, a BitSight subsidiary. The AnubisNetworks data provides BitSight unparalleled access and visibility into high quality and diverse global botnet infection data critical to calculate security ratings for organizations.

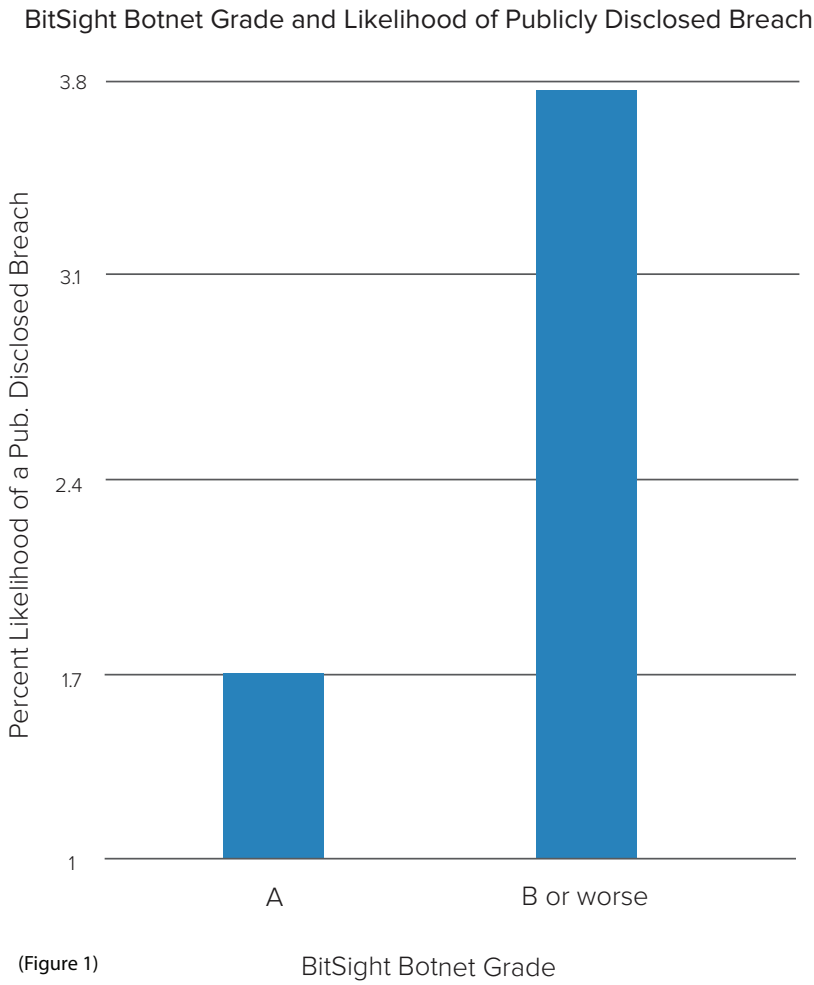
To perform this analysis, which covered the time period from March 2014 to March 2015, BitSight examined the ratings of 6,273 companies with 1,000 or more employees, of which 199 (3.3%) had experienced at least one recent publicly disclosed breach. These breaches are publicly disclosed incidents of data loss or theft resulting from successful attacks, employee negligence, or hardware theft. BitSight collects data breach information from various news sources and by filing Freedom of Information Act (FOIA) requests.

BitSight Security Ratings range between 250 and 900, with higher ratings indicating better performance. These ratings are calculated using terabytes of data, including nearly 4 years of historical information, on risk vectors using a proprietary algorithm. Risk vectors include security events, which are observed compromises on a company's network, and diligence risk vectors, which show steps a company has taken to prevent attacks. For each risk vector, an overall letter grade (A-F) is assigned, indicating the company's performance relative to others. The grade takes into account factors such as frequency, severity, and duration (for events) as well as record quality, evaluated based on industry-standard criteria (for diligence).

Using both automated and hand-curated tools and processes, BitSight creates comprehensive network maps of a company's Internet footprint. These maps allow BitSight to determine the organizational origin of compromised devices belonging to tens of thousands of companies across the globe.

Analysis

The companies analyzed were divided into two groups: those which had suffered recorded breaches, and those which had not. Of the grades, botnet grades differed the most between groups. Among companies with botnet grades of A, the percentage having breaches was 1.7%; for those with a B or lower, the incidence was 3.7% (Figure 1). Thus, within this data set, companies with a botnet grade of B or lower experienced a publicly disclosed breach 2.2 times more often than those with A's.[1] This does not mean the infections were the cause of the breaches; rather, it means that the infections and breach incidents are correlated.



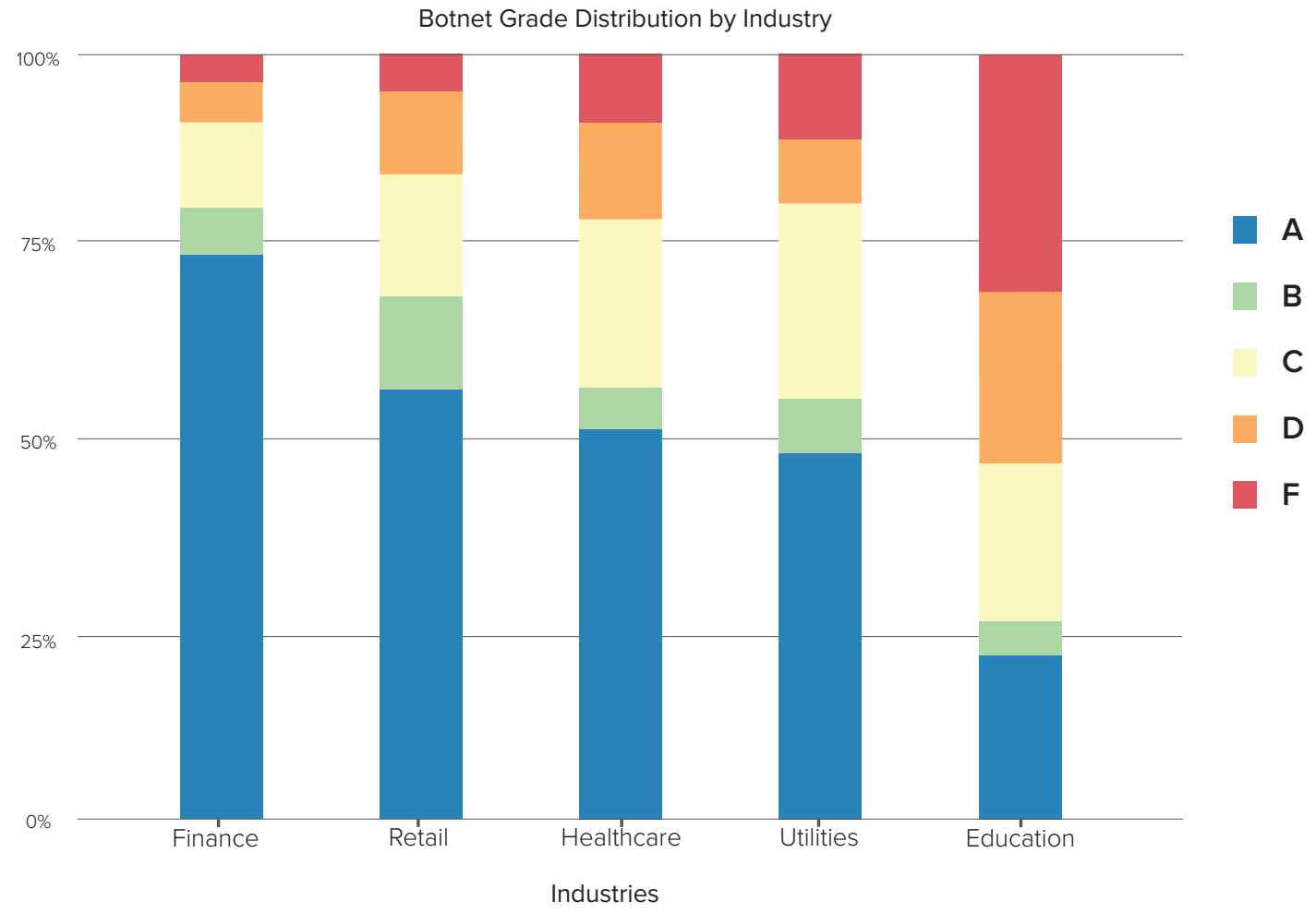
(Figure 1)

	No Breach	Breach	All	Percent Breached
Botnet: A	1,538	26	1,564	1.7
Botnet: B or lower	4,536	172	4,709	3.7
All	6,074	199	6,273	3.2

1 The results were statistically significant (p = 0.0097), even when taking into account the distribution of company sizes.

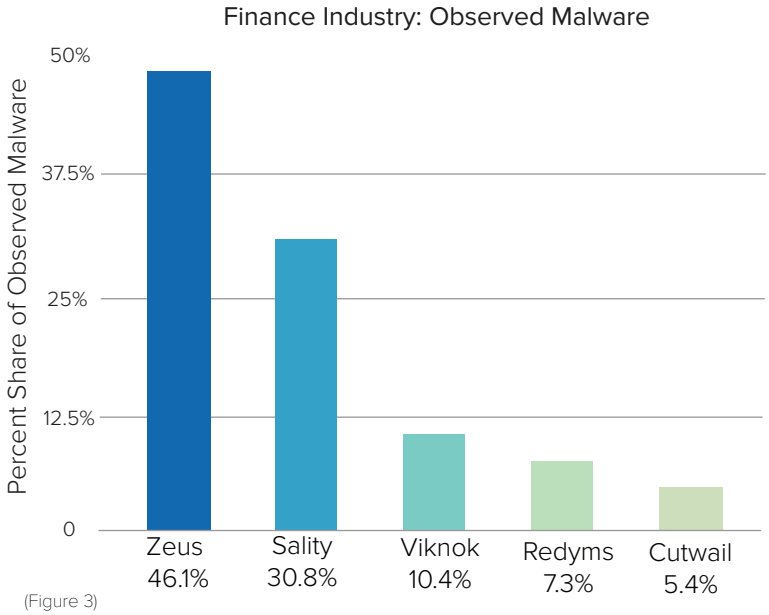
Industry Breakdown of Botnets

As we have noted in previous BitSight Insights, industries often have differing levels of performance across multiple risk vectors. Industries that have historically had better security performance, such as Finance, continue this trend when it comes to botnet infections. The graph below (Figure 2) shows the distribution of letter grades among five important sectors of the US economy.



(FIgure 2)

Finance

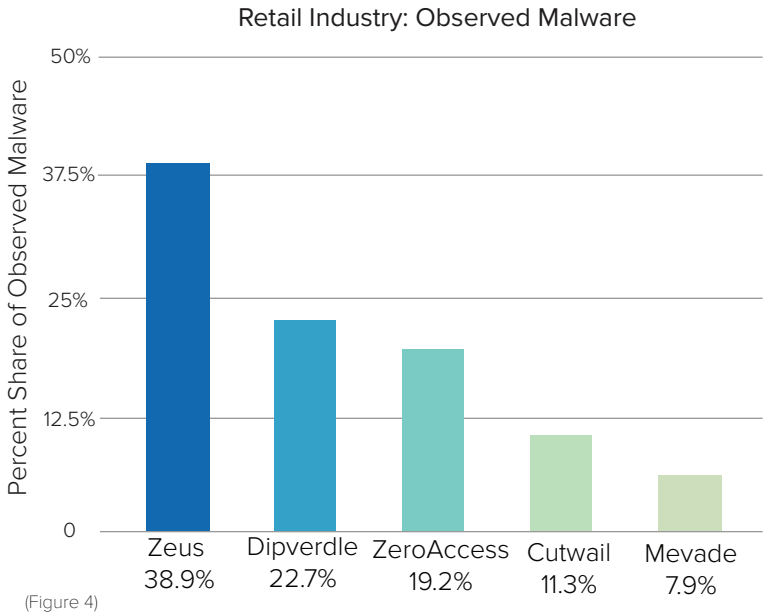


(Figure 3)

Seventy-four percent of finance firms in this sample had an A grade. This signifies that financial firms are quick to address existing infections on their network and are more effective at preventing new infections. That said, major infections[2] within the Finance industry included Zeus, Sality and Viknok. Zeus is used to carry out many malicious and criminal tasks, and Sality can be used to relay spam, proxy communications, exfiltrate sensitive data, and compromise web servers. Viknok is used to gain elevated operating system privileges, which can lead to theft of personal information.

Retail

The retail industry has had its fair share of high-profile breaches over the past two years, including Goodwill, Michaels, Neiman Marcus, and Home Depot. Nevertheless, these major breaches do not tell the whole story. A large portion of the breaches in this study's sample came from FOIA requests, many of which never make it into news headlines. Overall, the retail industry actually outperforms some industries. Yet it is important to note that this alone does not mean that retail is safe; 43% of companies are under the A threshold in an industry that is targeted for its valuable credit card information. Botnets affecting this industry include Zeus[3], Dipverdle, and ZeroAccess.[4] Dipverdle and ZeroAccess are Trojan horses that affect Microsoft Windows operating systems and are used to redirect traffic to Web pages that attempt to steal information. Takedowns of Zeus and ZeroAccess will likely diminish the effects of this malicious software on the industry. That said, even when a botnet has been taken down, infections still persist because not all machines are cleaned up.



(Figure 4)

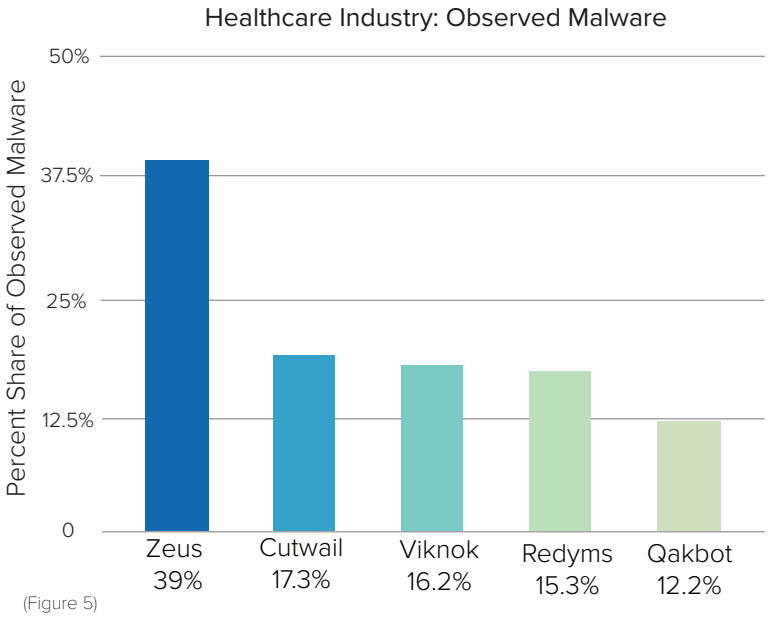
2 Conficker, one of the most widely distributed botnets in the world, infecting millions of devices since its discovery in 2009, was observed the most across all industries. Due to the high volume of Conficker infections, we have excluded this infection from the industry graphs (Figures 3 - 7).

3 The Zeus takedown happened in June 2014.

4 The ZeroAccess takedown happened in December 2013.

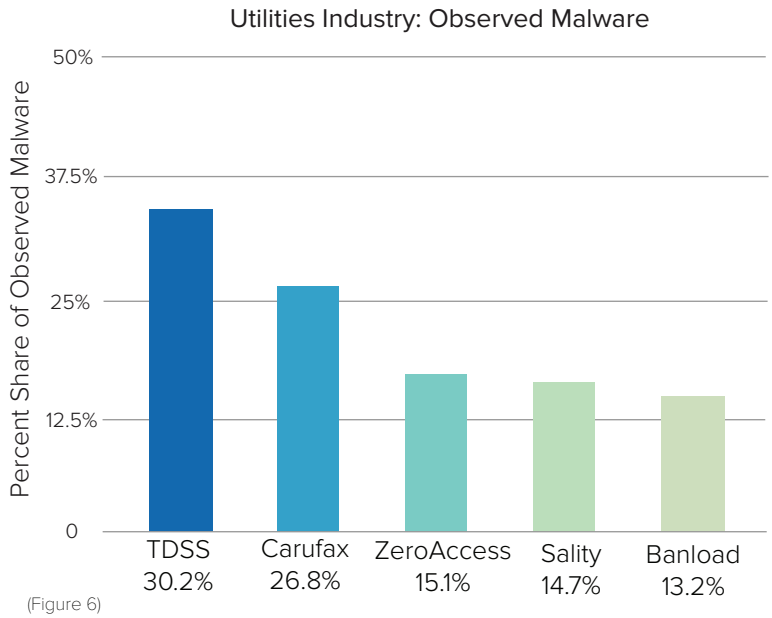
Healthcare

Healthcare, similar to Retail, has been struggling in recent months with breaches that hit major organizations like Anthem and Premera Health. Last year, Community Health Services also suffered a massive breach of patient data. When it comes to mitigating botnet infections, only 52% of these organizations are earning an A grade. In our previous report, Is Healthcare the Next Retail?, we found that many healthcare organizations were struggling with cleaning up infections on their networks. Our most recent analysis confirms this finding, with Zeus, Cutwail, and Viknok being the most common botnets affecting the industry. The fact that Viknok can be used to gain elevated operating system privileges, which can lead to theft of sensitive information, is concerning given the sensitivity of patient data.



(Figure 5)

Utilities



(Figure 6)

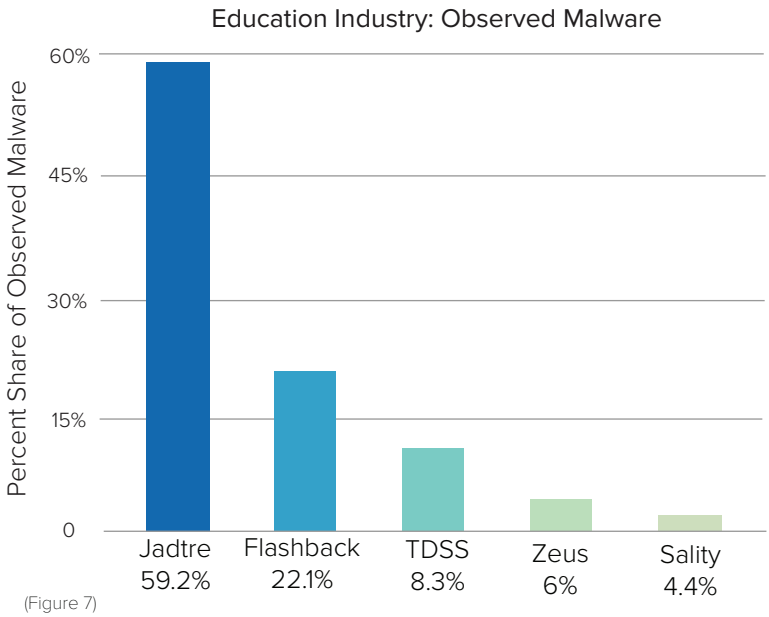
The Utilities industry is the second worst performer in this study, with more than 52% of the companies in this sector experiencing a botnet grade of B or lower. One particularly malicious botnet we observed in utility companies is TDSS, widely considered one of the largest and most complex botnets on the planet, according to Brian Krebs. The malware installs itself deep within infected PCs, ensuring that it loads before the Microsoft Windows operating system starts. Another botnet observed here, but less frequently among other industries, is Carufax, a Trojan program, which is designed to steal personal data and information. Utility systems have been traditionally focused on reliability and safety with a lack of focus on security, according to a senior Energy Department official.[5] Traditionally, the Operational Technology side of the organization was thought to be physically separated in terms of networking from Information Technology, but today more and more IT applications need data from Operations (e.g. smart meters). As more systems become accessible to the Internet, security concerns will grow.

5 http://www.energypost.eu/vulnerability-electric-utility-system-cyber-attacks/

.

Education

The worst performing industry in our analysis was Education. This industry, which includes educational companies, schools and colleges, is failing to effectively prevent these infections; fewer than 23% have an A grade while more than 33% have an F. In last year's BitSight Insights, Powerhouses and Benchwarmers, we found that many higher education institutions were struggling with a large volume of infections. This was in part due to unique challenges faced by colleges, such as a multitude of access points and devices running on college networks and a lack of security-focused leadership. Echoing our earlier research, the breakdown of observed botnets highlights the pervasiveness of Jadtre and Flashback.



(Figure 7)

Flashback is malware that targets Apple computers by taking advantage of a Java vulnerability. Mac computers are popular among younger generations and educational institutions, intensifying the proliferation of this malware in education. Although the Flashback botnet itself has largely been shut down, the large number of infections that still exist indicates that people are running machines that have not been updated; thus, they are still vulnerable to other forms of infection. These vulnerabilities have been documented in recent breach events, many of which were larger than the Sony hack, including the University of Maryland, North Dakota University, Butler University, Indiana University and Arkansas State.[6]

Conclusions

The results detailed in this report demonstrate that organizations with many compromised machines participating in botnets are more likely to experience a data breach large enough to require public disclosure. Differences between industries are also observable. Some industries, like Finance, have implemented stronger defenses, detection, and remediation capabilities that have yielded fewer system compromises and correspondingly lower rates of publicly disclosed breaches. Other industries like Healthcare, Utilities and Education have been less effective when it comes to preventing and recovering from malware infections.

The implications for organizations across industries are that botnet infections cannot be ignored. Companies with poor botnet grades have been breached far more often than those with the best grade. This insight that can be leveraged for the following initiatives, as organizations look to better prioritize areas of focus to address the most critical risks: benchmarking, vendor risk management, cyber insurance, and mergers and acquisitions.

The first step is to gain visibility into these risk metrics and communicate within the enterprise and/or with third parties about the importance of botnet grades within an organization's information security program. With this information, organizations can begin to remediate specific infections and take important steps to implement more effective controls to detect and more rapidly respond to future infections.

6 http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html

BITSIGHT®

The Standard in **SECURITY RATINGS**

About BitSight Technologies:
BitSight Technologies is transforming how companies manage information security risk with objective, evidence-based security ratings. The company's Security Rating Platform continuously analyzes vast amounts of external data on security behaviors in order to help organizations make timely risk management decisions.

125 Cambridge Park Drive, Cambridge, MA | www.bitsighttech.com | info@bitsighttech.com | 1.617.245.0469
Follow us on Twitter: @BitSight