FOR IMMEDIATE RELEASE

Contacts:

Chris Nicholson
Media Relations
+1 617 444 2987
cnichols@akamai.com

Tom Barth
Investor Relations
+1 617 274 7130
tbarth@akamai.com

Media Industry Full of Credential Stuffing Attacks: Akamai

Twenty percent of credential stuffing attacks directed toward media companies according to "Akamai 2020 State of the Internet / Credential Stuffing in the Media Industry" Report

CAMBRIDGE, Mass. (July 17, 2020) – The media industry suffered 17 billion credential stuffing attacks between January 2018 and December 2019 according to a new report from Akamai (NASDAQ: AKAM), the intelligent edge platform for securing and delivering digital experiences. Released today, the *Akamai 2020 State of the Internet / Credential Stuffing in the Media Industry* report found that 20% of the 88 billion total credential stuffing attacks observed during the reporting period targeted media companies.

Media companies present an attractive target for criminals according to the report, which reveals a 63% year-over-year increase in attacks against the video media sector. The report also shows 630% and 208% year-over-year increases in attacks against broadcast TV and video sites, respectively. At the same time, attacks targeting video services are up 98%, while those against video platforms dropped by 5%.

The marked uptick in attacks aimed at broadcast TV and video sites appear to coincide with an explosion of on-demand media content in 2019. In addition, two major video services launched last year with heavy support from consumer promotions. These types of sites and services are well aligned to the observed goals of the criminals who target them.

Much of the value in media industry accounts lies in the potential access to both compromised assets, like premium content, along with personal data according to Steve Ragan, Akamai security researcher and author of the *State of the Internet / Security* report. "We've observed a trend in which criminals are combining credentials from a media account with access to stolen rewards points from local restaurants and marketing the nefarious offering as 'date night' packages," Ragan explained in the report. "Once the criminals get a hold of the geographic location information in the compromised accounts, they can match them up to be sold as dinner and a movie."

Video sites are not the sole focus of credential stuffing attacks within the media industry, however. The report notes a staggering 7,000% increase in attacks targeting published content. Newspapers, books and magazines sit squarely within the sights of cybercriminals, indicating that media of all types appear to be fair game when it comes to these types of attacks.

The United States was by far the top source of credential stuffing attacks against media companies with 1.1 billion in 2019, an increase of 162% over 2018. France and Russia were a distant second and third with 393 million and 243 million attacks, respectively.

India, was the most targeted country in 2019, enduring with 2.4 billion credential stuffing attacks. It was followed by the United States at 1.4 billion and the United Kingdom at 124 million.

“As long as we have usernames and passwords, we’re going to have criminals trying to compromise them and exploit valuable information,” Ragan explained. “Password sharing and recycling are easily the two largest contributing factors in credential stuffing attacks. While educating consumers on good credential hygiene is critical to combating these attacks, it’s up to businesses to deploy stronger authentication methods and identify the right mix of technology, policies and expertise that can help protect customers without adversely impacting the user experience.”

Q1 2020 Update

Publication of the *Akamai 2020 State of the Internet / Credential Stuffing in the Media Industry* report was delayed from April to July due to the COVID-19 pandemic. The extra time allowed Q1 2020 data to be added to the original report.

Most notably, there was a large spike in malicious login attempts against European video service providers and broadcasters during the first quarter of 2020. One attack in late March, after many isolation protocols had been instituted, directed nearly 350,000,000 attempts against a single service provider over a 24-hour period. Separately, one broadcaster well known across the region, was hit with a barrage of attacks over the course of the quarter with peaks that ranged in the billions.

Another noteworthy trend during the first quarter was the number of criminals sharing free access to newspaper accounts. Often offered as self-promotional vehicles, credential stuffing campaigns must still be initiated in order to steal the working username and password combinations that are given away.

Akamai researchers also observed a decline in the cost of stolen account credentials over the course of the quarter, which traded for approximately $1 to $5 at the start and $10 to $45 for package offers of multiple services. Those prices fell as new accounts and lists of recycled credentials populated the market.

The Akamai 2020 State of the Internet / Security Report is available here. For additional information, the security community can access, engage with, and learn from Akamai’s

threat researchers and the insight that the Akamai Intelligent Edge Platform affords into the evolving threat landscape, visit Akamai's Threat Research Hub.

About Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations.

###