Inspired eLearning October Newsletter

2020 NATIONAL CYBERSECURITY AWARENESS MONTH

Our theme this year is: Know Your Role In Security Awareness. Help continue to educate employees on security awareness by downloading our CSAM resources!

LEARN MORE

EMAIL SECURITY CUBED: A LAYERED APPROACH TO REDUCING CYBER-RISK

Download this whitepaper created with our partners, GreatHorn and dmarcian, to learn how you can reduce the security pitfalls associated with email communication.

DOWNLOAD

Breach at Dickey’s Barbecue Pit compromises 3 million Cards

Dickey's Barbecue Pit is a family-owned American barbecue restaurant chain, the company suffered a POS breach and card details of more than three million customers have been posted on the carding portal Joker’s Stash.

The huge trove of payment card data was spotted by researchers from the cyber-security firm Gemini Advisory. The Joker’s Stash dark web marketplace is one of the most popular carding websites, it is known for advertising and card details from major breaches.

The card details of Dickey’s Barbecue Pit‘s customers were included in a dump titled “BLAZINGSUN.” JokerStash originally claimed that the breach would be available in August, then again in September, and finally it was posted online on October 12.

“Gemini Advisory determined that the compromised point of purchase (CPP) was Dickey’s Barbecue Pit, a US-based restaurant franchise.” reads the post published by Gemini Advisory.

“The advertisement claimed that BLAZINGSUN would contain 3 million compromised cards with both track 1 and track 2 data. They purportedly came from 35 US states and “some” countries across Europe and Asia.”

This BLAZINGSUN breach contains 3 million compromised payment records that are available for a median price of $17 per card. The experts worked with several partner financial institutions who independently confirmed the authenticity of the stolen data.

According to Gemini, the hackers obtained the card details after compromised the in-store Point-of-Sale (POS) system used at Dickey’s Barbecue Pit restaurants.

Crooks compromised 156 of Dickey’s 469 locations across 30 states, most of them in California and Arizona.

The compromise took place between July 2019 and August 2020. Gemini reported that the root cause of the security breach was the use of the outdated magstripe method for payment transactions, which exposed car holders to PoS malware attacks.

The company published an official statement that confirmed that it has immediately started the incident response procedure.

“We received a report indicating that a payment card security incident may have occurred. We are taking this incident very seriously and immediately initiated our response protocol and an investigation is underway. We are currently focused on determining the locations affected and time frames involved.” reads the statement provided by the company. “We are utilizing the experience of third parties who have helped other restaurants address similar issues and also working with the FBI and payment card networks. We understand that payment card network rules generally provide that individuals who timely report unauthorized charges to the bank that issued their card are not responsible for those charges.”

The payment card records are mostly for cards using outdated magstripe technologies and are being sold for a median price of $17 per card.

“Based on previous Joker’s Stash major breaches, the records from Dickey’s will likely continue to be added to this marketplace over several months.” concludes the post.

This article was originally posted by SecurityAffairs.co. Read the full article here.

Cybercrime Losses Up 50%, Exceeding $1.8B

The world is rightly obsessed with the COVID-19 pandemic right now, but there's also a growing cybercrime pandemic. The good news is that fewer firms are reporting breaches. The bad news is that for those who are victimized, the attacks are more severe — and more expensive.

According Hiscox, a Bermuda-based insurance provider, cyber losses rose nearly sixfold worldwide over the past 12 months. Its recently released "Cyber Readiness Report 2020" pins the total cyber losses among affected firms at $1.8 billion — up a sobering 50% from the previous year's total of $1.2 billion. Overall, more than 6% of the respondents in the report paid a ransom, and their collective losses totaled $381 million.

Interestingly enough, Hiscox says that companies are 15 times more likely to experience a cyberattack (30% in UK) thana fire or theft (2% in UK).

Who Was Most at Risk?
Not surprisingly, larger organizations were the most common targets — and shelled out the most money — for cybercriminals. The financial impact differed widely across countries, verticals, and firm sizes. According to Hiscox, the energy, manufacturing, and financial services sectors are especially at risk. This is the result of low maturity in cyber resilience and low tolerance to what is often a high-impact outage.

Irish and German companies reported the biggest median losses, but the pain was widely shared. Among the attacked organizations, the median losses for energy firms increased over 30-fold, while a number of other sectors faced losses many times greater than the previous year. The biggest recorded loss for a single organization was $87.9 million (for a UK financial services firm), and the greatest loss stemming from a single attack was $15.8 million (for a UK professional services firm).

Cybercriminals demanded ransoms from roughly 17% of the companies they attacked, and caused dire financial consequences for the targets. The highest loss from ransom was more than $50 million for one unfortunate organization.

According to the Hiscox report, malware, ransomware, business email compromise, and distributed denial-of-service (DDoS) are still the most commonly used attack vectors. Besides malicious encryption imposed through ransomware, other extortion campaigns include DDoS attacks that causes the victim's IT infrastructure to crash over and over due to a constant flood of bogus IP traffic. Recently, the stock exchange in New Zealand weathered a barrage of DDoS attacks that disrupted business operations and trading for four consecutive days. CNBC reported that the exchange's websites and markets announcement platform were also affected.

Large Number of "Don't Knows"
According to Hiscox, this year the share of firms that revealed they'd suffered a cybersecurity incident in the last year shrank from 61% to 39%. At least that's positive. The flip side is that the financial blowback has been far greater than before. Larger companies were more likely to be targeted than smaller ones. Just over half (51%) of all enterprise-level firms — those with 1,000-plus employees — reported at least one cyber incident, and the most cyber incidents by far (median: 100) and breaches (80). The most heavily targeted sectors were financial services; manufacturing; and technology, media, and telecoms (TMT) — with 44% of firms in each sector reporting at least one incident or breach.

Of particular concern is that 11% of the respondents said they weren't sure how many times they were targeted. (That's 4% more than the previous year.) Even more worrisome is that the greatest share of "I don't knows" (15%) came from enterprise firms.

Surge in Spending
The report revealed that a large and broad increase in cybersecurity spending has occurred over the past year. The average spending among the respondents was $2.1 million, up from $1.5 million the previous year. (Roughly 75% of the respondents provided figures for their cybersecurity spending.)

Assuming the numbers are an accurate reflection of what's going on more broadly, the total cybersecurity spending in the past year was a staggering $11.4 billion. That compares with $7.9 billion a year ago for a sample of companies that was 3% smaller. Nearly three-quarters of firms (72%) intend to boost cybersecurity spending by 5% or more in the next year — that's up from two-thirds (67%) from the 2019 number.

As one might expect, the companies that dedicated double-digit percentages of their IT budget were less likely to have suffered a breach than those that spent less than 5%. But those big spenders, typically larger firms, had higher average costs stemming from breaches. Greater size means more customers, higher notification expenses, and bigger ransoms.

Preparation Pays Off

A notably higher percentage of this year's respondents reported that they had a harder time attracting new customers (15% of firms were targeted, up from 5% last year) after a cyber incident. They also lost more customers (11%, compared with 5% in 2019) and/or business partners (12% compared with 4%).

When asked about the adverse effects of a breach, 14% of the respondents mentioned bad publicity that tarnishes the brand or the company's reputation. Only 5% said the same thing in 2019. Thirteen percent said business performance indicators — such as their share price — were affected, up from 5% last year.

This article was originally posted by Dark Reading. Read the full article here.

Massive Cyberattack Propagating via Redirector Domains and Subsidiary Domains

The GreatHorn Threat Intelligence Team has discovered a massive cyberattack propagating via open redirector domains and subsidiary domains belonging to multiple global brands, spreading through tens of thousands of mailboxes and targeting business users across industries, geographies, and companies.

The Threat Intelligence Team described this campaign as a “comprehensive and multi-pronged attack,” with multiple hosting services and web servers being used to host fraudulent Office 365 login pages. Malicious links, delivered via phishing emails to regular users worldwide, are bypassing their email providers’ native security controls and slipping past nearly every legacy email security platform on the market.

“This is a pervasive and significant event. While our customers are protected, this is an attack that appears to have easily bypassed both platform controls and multiple legacy secure email gateway solutions. Widespread and utilizing multiple techniques to deceive users, this represents the kind of advanced phishing attack that necessitates a modern email security program capable of finding and interdicting threats before, during, and after an incident,” said Kevin O’Brien, CEO, and Co-Founder of GreatHorn.

These attacks attempt to steal corporate email credentials, coupled with malicious JavaScript that deploys various trojans and malware on any user who visits these pages, regardless of whether they submit their credentials or not.

The similarity across the campaigns leads the GreatHorn Threat Intelligence Team to believe it is a singular entity behind the attacks. Moreover, the attackers appear to be attempting to evade detection by spoofing well-known applications, including Microsoft Office, Zoom, Microsoft Teams, and more.

The URLs in the phishing emails sent to users vary. Some employ redirects; others point directly at the phishing kit pages. The phishing kit itself uses the same naming structure in nearly all cases: t.****/r/, where *** represents the domain. However, the URL path varies across individual messages, as part of a common tactic used to bypass simple blocking rules that prevent these messages from reaching users.

When a redirect is in use, initial research has indicated that the open redirect occurs on apache servers. Known issues with mod_rewrite in apache versions prior to 2.4.41 may be responsible for the redirectors' creation, although confirmation is still outstanding as of this writing.

The phishing webpages impersonate a Microsoft Office 365 login, using the Microsoft logo and requesting that users enter their password, verify their account, or sign-in. Given this campaign's breadth and highly targeted nature, the sophistication and complexity suggest that the attackers' significant coordinated effort is underway. Additionally, GreatHorn's Threat Research Intelligence Team identified attempts to deploy the Cryxos trojan on multiple browsers, including Chrome and Safari.

Currently identified domains redirecting to the phishing kit and fraudulent login pages include:

- sony-europe.com (Sony)
- lafourchette.com (TripAdvisor)
- rac.co.uk (RAC)

Static webpage services hosting the phishing kit include:

- digitaloceanspaces.com (DigitalOcean)
- firebasestorage.googleapis.com (Google)

GreatHorn recommends that security teams immediately search their organizational email for messages containing URLs that match the threat pattern (t.****/r/) and remove any matches immediately.

With continued analysis, the GreatHorn Threat Intelligence Team has identified senior executives and finance personnel being targeted within the phishing campaigns. For organizations who are using role-based email security, users within these roles can be placed on more restrictive policies to minimize the risk associated with these attacks.

For the full article and more tips, check out the original posting here.

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:

info@inspiredelearning.com I 800.631.2078
4630 N Loop 1604 W, Suite 401
San Antonio, TX 78249 USA

Privacy Notice