Security Newsletter

29 April 2019

Subscribe to this newsletter

Breach at IT Outsourcing Giant Wipro

Indian information technology (IT) outsourcing and consulting giant Wipro Ltd. is investigating reports that its own IT systems have been hacked and are being used to launch attacks against some of the company's customers, multiple sources tell KrebsOnSecurity. Wipro has refused to respond to questions about the alleged incident.

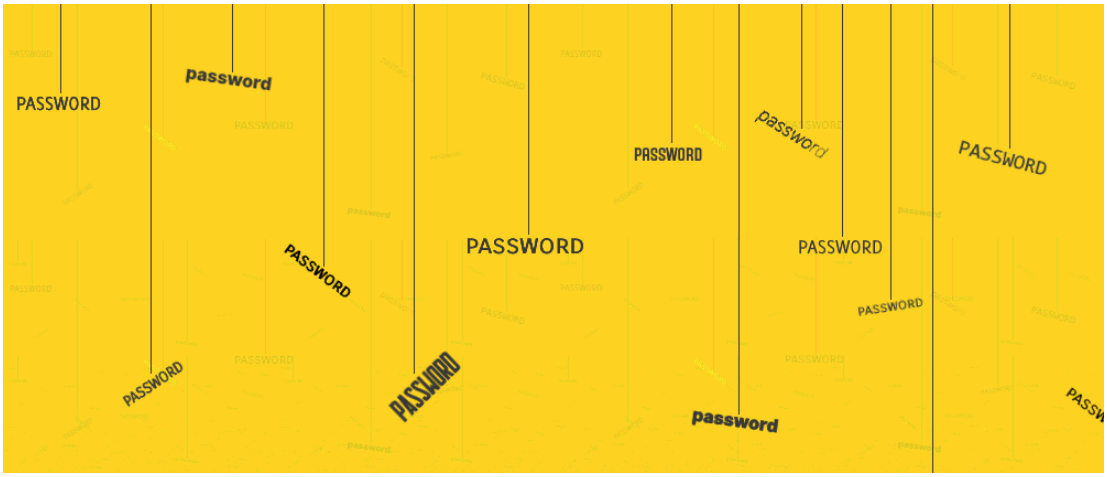
Both sources, who spoke on condition of anonymity, said Wipro's systems were seen being used as jumping-off points for digital fishing expeditions targeting at least a dozen Wipro customer systems. The security experts said Wipro's customers traced malicious and suspicious network reconnaissance activity back to partner systems that were communicating directly with Wipro's network.

One source familiar with the forensic investigation at a Wipro customer said it appears at least 11 other companies were attacked, as evidenced from file folders found on the intruders' back-end infrastructure that were named after various Wipro clients. That source declined to name the other clients. The other source said Wipro is now in the process of building out a new private email network because the intruders were thought to have compromised Wipro's corporate email system for some time. The source also said Wipro is now telling concerned clients about specific "indicators of compromise," telltale clues about tactics, tools and procedures used by the bad guys that might signify an attempted or successful intrusion. Wipro says it has more than 170,000 employees helping clients across six continents with Fortune 500 customers in healthcare, banking, communications and other industries. In March 2018, Wipro said it passed the $8 billion mark in annual IT services revenue.

Read More on KrebsOnSecurity

How Not to Acknowledge a Data Breach

The Anatomy of Highly Profitable Credential Stuffing Attacks



Credential stuffing attacks are one of today's most prevalent threats to online businesses everywhere. But despite this threat rising on everyone's radar in the infosec community, very little is known about how criminal groups are performing these attacks.

Credential stuffing is a term used by the cybersecurity industry to describe a particular type of automated attack against a website or application's login system. It relies on a hacker taking username-password combos that have been leaked via data breaches at other companies, and attempting to use these leaked credentials in the hope of gaining access to accounts on other sites -- exploiting users' habit of reusing usernames and passwords across multiple online services.

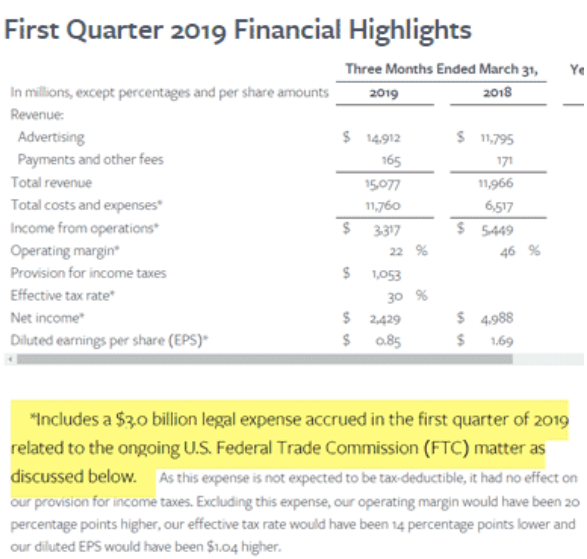
Credential stuffing is a relatively new attack vector and has been fueled by the huge leaks of user credentials that have taken place since 2016, after hacks at LinkedIn, VK.com, Tumblr, Twitter, and many other major platforms. Hundreds of millions of username and password credentials were dumped online in 2016, and other leaks have continued to pop up regularly since then, supplying fresh cannon fodder for criminal gangs to use for their attacks.

Organizations can protect their users by implementing multi-factor authentication (MFA) "which blocks the credential stuffing attack vector" but some of them already confirmed that they "may not be prepared to choose security over convenience." On the other hand, end users can do their part by never using the same password on more than one service, utilizing a password manager to safely store their credentials and generate more complex passwords, as well as turning on two-factor authentication (2FA) for all services that support it.

Read More on ZDNet

Even More on BleepingComputer

Facebook Could Be Fined Up To $5 Billion Over Privacy Violations



First Quarter 2019 Financial Highlights

In millions, except percentages and per share amounts	Three Months Ended March 31, 2019	2018	Ye
Revenue:			
Advertising	$ 14,912	$ 11,795	
Payments and other fees	165	171	
Total revenue	15,077	11,966	
Total costs and expenses*	11,760	6,517	
Income from operations*	$ 3,317	$ 5,449	
Operating margin*	22 %	46 %	
Provision for income taxes	$ 1,053		
Effective tax rate*	30 %		
Net income*	$ 2,429	$ 4,988	
Diluted earnings per share (EPS)*	$ 0.85	$ 1.69	

*Includes a $3.0 billion legal expense accrued in the first quarter of 2019 related to the ongoing U.S. Federal Trade Commission (FTC) matter as discussed below. As this expense is not expected to be tax-deductible, it had no effect on our provision for income taxes. Excluding this expense, our operating margin would have been 20 percentage points higher, our effective tax rate would have been 14 percentage points lower and our diluted EPS would have been $1.04 higher.

Facebook expects to face a massive fine of up to $5 billion from the Federal Trade Commission (FTC) as the result of an investigation into its privacy policies—that's about one month's revenue for the social media giant.

To be clear the amount of fine is not what the FTC has announced or hinted yet; instead, it's an estimated due that Facebook disclosed on Wednesday in its first quarter 2019 financial earnings report. In its earnings report, Facebook said the company had set $3 billion aside in anticipation of the settlement with the FTC, who launched a probe into Facebook following the Cambridge Analytica scandal.

The FTC launched an investigation into Facebook last year after it was revealed that the company allowed Cambridge Analytica access to the personal data of around 50 million Facebook users without their explicit consent.

Read More on TheHackerNews

How many days since last Facebook Scandal?

More #News

- Former student destroys 59 university computers using USB Killer device
- Microsoft loses control over Windows Tiles
- Atlanta Hawks fall prey to Magecart credit card skimming group
- Apple Updates XProtect to Block 'Windows' Malware on Macs
- ExtraPulsar backdoor based on leaked NSA code – what you need to know
- Malware Hosted in Google Sites Sends Data to MySQL Server
- 'ShadowHammer' Spreads Across Online Gaming Supply Chain
- Microsoft drops password expiration from Windows 10 security

- New Twist in the Stuxnet Story
- 'Virus Infection' Prohibits Access to Patient Records
- DNS over HTTPS is coming whether ISPs and governments like it or not
- Devious Chase Bank Phishing Scam Asks For Selfies
- 'Karkoff' Is the New 'DNSpionage' With Selective Targeting Strategy
- Marcus "MalwareTech" Hutchins Pleads Guilty to Writing, Selling Banking Malware
- Academics hide humans from surveillance cameras with 2D prints
- 70 percent of attacks now target Office vulnerabilities
- Australian Child-Tracking Smartwatch Vulnerable to Hackers
- Microsoft Introduces Security Configuration Framework
- Adblock Plus filters abused to execute code in browsing sessions (Use uBlock Origin instead)
- New Microsoft Edge to Warn Users When in Administrator Mode
- Office 365 Custom Rules to Block Azure Blob Storage Phishing Attacks
- Scranos: New Rapidly Evolving Rootkit-Enabled Spyware Discovered
- Let's Encrypt to transition to ISRG root
- Vulnerabilities in the WPA3 Wi-Fi Security Protocol
- Trojanized TeamViewer used in government, embassy attacks across Europe
- Tracking Phones, Google Is a Dragnet for the Police

#Patch Time!

- 'Highly Critical' Unpatched Zero-Day Flaw Discovered In Oracle WebLogic
- Oracle, Gemalto Downplay Java Card Vulnerabilities
- Security flaw lets attackers recover private keys from Qualcomm chips
- Chrome 74 Patches 39 Vulnerabilities
- Windows 10 May 2019 Update to Be Blocked If Using USB Drives
- Hackers Actively Exploiting Widely-Used Social Share Plugin for WordPress
- Important Severity Remote Code Execution Vulnerability Patched in Tomcat
- Flood of exploits targetting ancient WinRAR flaw continues
- Patched Windows Zero-Day Provided Full Control Over Vulnerable Systems
- Multiple Enterprise VPN Apps Allow Attackers to Bypass Authentication
- Scranos: New Rapidly Evolving Rootkit-Enabled Spyware Discovered
- Let's Encrypt to transition to ISRG root
- Vulnerabilities in the WPA3 Wi-Fi Security Protocol
- Thousands of WordPress Sites Exposed by Yellow Pencil Plugin Flaw
- Popular jQuery JavaScript library impacted by prototype pollution flaw
- OpenSSH 8.0 release
- Drupal Releases Core CMS Updates to Patch Several Vulnerabilities

#Tech and #Tools

- Introducing Venator: A macOS tool for proactive detection
- Merlin is a cross-platform post-exploitation HTTP/2 C2 server and agent
- FLASHMINGO: The FireEye Open Source Automatic Analysis Tool for Flash
- Carbanak Source Code Discovered on VirusTotal

- "CI Knew There Would Be Bugs Here" — Exploring Continuous Integration Services as a Bug Bounty Hunter
- Case Study: Password Analysis with BloodHound
- Next Gen Phishing – Leveraging Azure Information Protection
- DNS based threat hunting and DoH (DNS over HTTPS)
- The most common OAuth 2.0 Hacks
- Termshark is a simple terminal user-interface for tshark.
- MalConfScan for Cukcoo Sandbox
- Ignoring Atlassian Confluence Security Advisories?
- How to obtain Office 365 credentials on Mac OS
- Simple Tool for Testing CVE Mitigation in Web Apps
- User privileges in Docker containers
- Password Spraying- Common mistakes and how to avoid them
- Praetorian's public release of our Metasploit automation of MITRE ATT&CK™ TTPs
- Privacy 2019: TOR, MEEK & the rise and fall of domain fronting
- CyLR - Live Response Collection Tool
- Drupal 1-click to RCE exploit chain detailed
- ThreatIngestor: Extract and aggregate threat intelligence.
- Two Privilege Escalation techniques abusing sudo token

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us