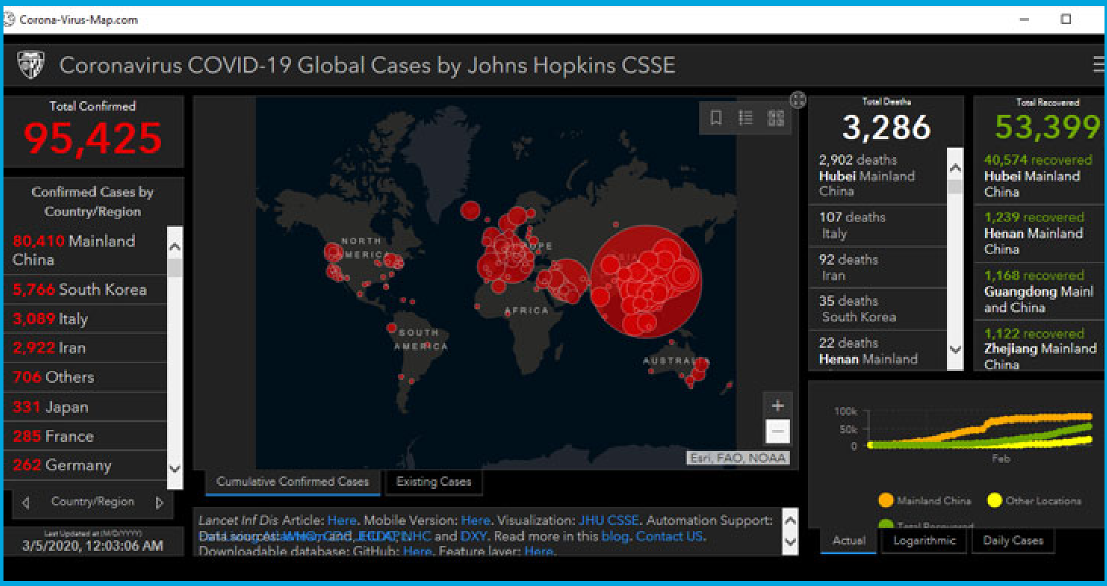
kindred

# Security Newsletter

16 March 2020

Subscribe to this newsletter

# How cybercriminals are taking advantage of COVID-19: Scams, fraud, and misinformation



Total Confirmed
95,425

Confirmed Cases by Country/Region

| | |
|---|---|
| 80,410 | Mainland China |
| 5,766 | South Korea |
| 3,089 | Italy |
| 2,922 | Iran |
| 706 | Others |
| 331 | Japan |
| 285 | France |
| 262 | Germany |

Last Updated at (M/D/YYYY)
3/5/2020, 12:03:06 AM

Total Deaths
3,286

2,902 deaths Hubei Mainland China

107 deaths Italy

92 deaths Iran

35 deaths South Korea

22 deaths Henan Mainland

Total Recovered
53,399

40,574 recovered Hubei Mainland China

1,239 recovered Henan Mainland China

1,168 recovered Guangdong Mainland China

1,122 recovered Zhejiang Mainland China

*Lancet Inf Dis* Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US. Downloadable database: GitHub: Here. Feature layer: Here.

Cybercriminals will stop at nothing to exploit every chance to prey on internet users. Even the disastrous spread of SARS-COV-II (the virus), which causes COVID-19 (the disease), is becoming an opportunity for them to likewise spread malware or launch cyber attacks.

These scams aim to exploit people's fear and uncertainty concerning the disease's spread. These can be broadly split into the following three categories: Phishing and social engineering scams; Sale of fraudulent or counterfeit goods; Misinformation.

To help prevent the spread of misinformation, individuals should ensure that they only follow guidance from official national health institutions like the CDC and NHS, as well as international organizations like the WHO. Use fact-checking tools to challenge potentially dubious claims on social media. Be wary of unsolicited correspondances that contain alarmist messaging and/or impersonate official health and safety institutions. Grammatical and formatting errors can help you identify malicious phishing emails. Be wary of emails soliciting charitable donations. Do not download files or visit unknown websites linked in unsolicited emails. Do not purchase medical equipment from unofficial third-party vendors (particularly on the dark web!). If a deal seems too good to be true, then it probably is.

Read More on DigitalShadows

Even More on TheHackerNews

# Critical Patch Released for 'Wormable' SMBv3 Vulnerability

Microsoft released an emergency software update to patch the recently disclosed very dangerous vulnerability in SMBv3 protocol that could let attackers launch wormable malware, which can propagate itself from one vulnerable computer to another automatically.

The vulnerability, tracked as CVE-2020-0796, in question is a remote code execution flaw that impacts Windows 10 version 1903 and 1909, and Windows Server version 1903 and 1909. Server Message Block (SMB), which runs over TCP port 445, is a network protocol that has been designed to enable file sharing, network browsing, printing services, and interprocess communication over a network.

Earlier this week, due to what looks like a miscommunication between Microsoft and some antivirus vendors, details about this bug leaked online. At the time of writing, there is only one known PoC exploit that exists for this critical remotely exploitable flaw, but reverse engineering new patches could now also help hackers find possible attack vectors to develop fully weaponized self-propagating malware. While Microsoft was not initially planning to release fixes this month, the company was eventually forced to push today's patch after the cat was out of the bag. As of today, there are nearly 48,000 Windows systems vulnerable to the latest SMB compression vulnerability and accessible over the Internet.

Read More on TheHackerNews

Even More on ZDNet

# More #News

- New LVI Intel CPU Data Theft Vulnerability Requires Hardware Fix
- Flaw in popular VPN service may have exposed customer data
- Ex-Inspector General indicted for stealing data on 250k govt colleagues

- Google Play Protect Miserably Fails Android Protection Tests
- Real-life cybercrime stories from DART, the Microsoft Detection and Response Team
- Entercom Radio Giant Says Data Breach Exposed User Credentials
- This Unpatchable Flaw Affects All Intel CPUs Released in Last 5 Years
- Virgin Media Data Leak Exposes Details of 900,000 Customers
- Nearly 300 cybersecurity incidents impacted supply chain entities in 2019
- Empower Firstline Workers with Azure AD and YubiKey passwordless authentication
- Hackers Get $1.6 Million for Card Data from Breached Online Shops
- Protecting Accounts from Credential Stuffing
- DDR4 Memory Still At Rowhammer Risk, New Method Bypasses Fixes
- U.S. Senators Seek to Ban TikTok on Government Devices
- EARN IT Act threatens end-to-end encryption
- Confessions app Whisper spills almost a billion records
- New Android Cookie-Stealing Malware Found Hijacking Facebook Accounts

# #Patch Time!

- Microsoft Issues March 2020 Updates to Patch 115 Security Flaws
- 9 Years of AMD Processors Vulnerable to 2 New Side-Channel Attacks
- Intel Patches High Severity Flaws in Windows Graphics Drivers
- Multiple nation-state groups are hacking Microsoft Exchange servers

# #Tech and #Tools

- An Introduction to Starkiller, a GUI for Empire
- Jeopardize: threat intelligence&response tool against phishing domains
- Office 365 ATP To Block Email Domains That Fail Authentication
- Understanding AWS Traffic Mirroring and Malicious Use
- Cloud WAF Comparison Using Real-World Attacks
- Differential privacy: a comparison of libraries
- Pickl3: Windows active user credential phishing tool
- The unexpected Google wide domain check bypass
- Lessons learned on written social engineering attacks
- The Web Application Hacker's Handbook - Extra Content
- Malshare: Malware repo. providing access to samples, feeds, and Yara results.
- Red Team Tactics: Advanced process monitoring techniques in offensive operations
- saferwall: Multi-AV Malware sandbox
- Crescendo: real time event viewer for macOS using Apple's Endpoint Security Framework.
- Facebook's AppLocker cookbook

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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