

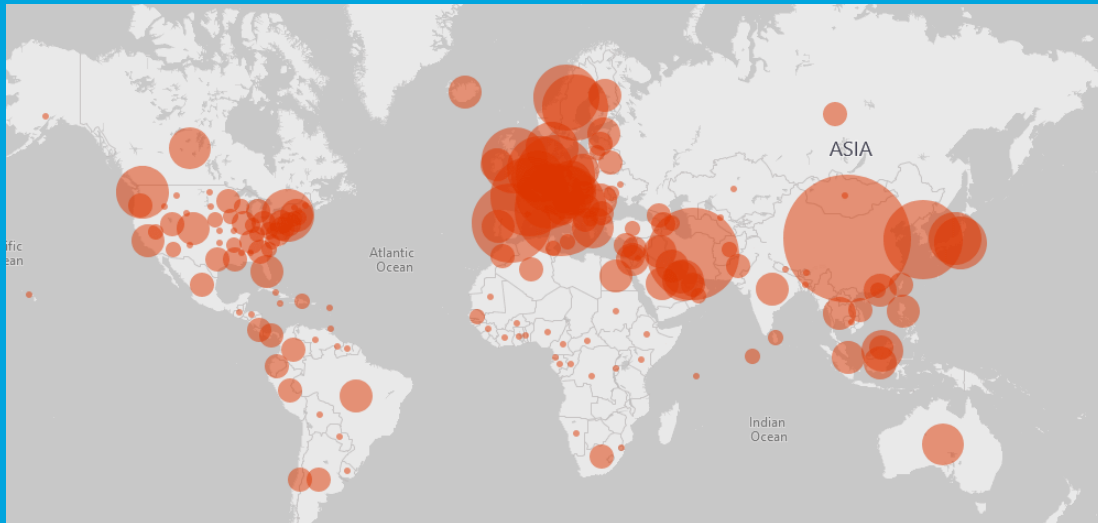


Security Newsletter

23 March 2020

[Subscribe to this newsletter](#)

Mukashi: Mirai botnets are back for DDoS



A new version of the infamous Mirai botnet is exploiting a recently uncovered critical vulnerability in network-attached storage (NAS) devices in an attempt to remotely infect and control vulnerable machines. Called "Mukashi," the new variant of the malware employs brute-force attacks using different combinations of default credentials to log into Zyxel NAS, UTM, ATP, and VPN firewall products to take control of the devices and add them to a network of infected bots that can be used to carry out Distributed Denial of Service (DDoS) attacks.

The Mirai botnet, since its discovery in 2016, has been linked to a string of large-scale DDoS attacks, including one against DNS service provider Dyn in October 2016, causing major internet platforms and services to remain inaccessible to users in Europe and North America. Just like other Mirai variants, Mukashi operates by scanning the Internet for vulnerable IoT devices like routers, NAS devices, security cameras, and digital video recorders (DVRs), looking for potential hosts that are protected only by factory-default credentials or commonly-used passwords to co-opt them into the botnet.

Meanwhile, at least three botnet operators have secretly exploited three zero-day vulnerabilities in LILIN digital video recorders (DVRs) for more than six months before the vendor finally patched the bugs last month, in February 2020. It will most likely take months – if not years – for the patch to make it to some devices. If there's an Achilles' heel to today's IoT landscape then it's the fact that there's no easy one-button-push to update firmware on most devices. Once shipped to customers, the vast majority of these systems remain unpatched until decommissioned.

[Read More on TheHackerNews](#)

[DDoS botnets abusing zero-days in LILIN video recorders](#)

US, Israel, South Korea, and China look at intrusive surveillance solutions for tracking COVID-19



As the global coronavirus (COVID-19) outbreak is leaving its mark across the world, at least four governments are deploying or at looking at implementing privacy-intrusive surveillance systems to track citizens and the disease's spread. Countries like China and South Korea have already deployed extensive citizen tracking systems, while Israel and the US are preparing similar surveillance measures.

For example, the Chinese government has introduced a new scheme called Health Code, which, according to the Guardian, is currently being deployed in over 100 cities. Chinese citizens can sign up for a Health Code account using their Alipay or WeChat profiles. Once they have a Health Code account, they will be assigned a color code -- red for infected, yellow for quarantined, and green for healthy. The system allegedly works by taking a user's Alipay or WeChat account history and mapping their travel history. It then weighs other factors like the time spent in outbreak hotspots and if the user had contact with other citizens deemed potential carriers of the virus, and then assigns a health color code.

The system leverages the vast quantities of mobile data and geo-location points Chinese tech companies have been collecting to map infection hotspots and then triage China's population based on their previous interactions. But if this system seems intrusive, Chinese authorities are taking it one step further in Hong Kong, where they have been using wristbands to track infected locals.

[Read More](#)



WordPress to add auto-update feature for themes and plugins



Plugins



The following plugins have new versions available. Check the ones you want to update and then click "Update Plugins".



[Update Plugins](#)

Select All

 **Akismet Anti-Spam**
You have version 4.1.2 installed. Update to 4.1.3. [View version 4.1.3 details.](#)
Compatibility with WordPress 5.5: Unknown  Automatic update scheduled in 9 hours

 **Contextual Adminbar Color**
You have version 0.3.0 installed. Update to 0.3.1. [View version 0.3.1 details.](#)
Compatibility with WordPress 5.5: Unknown  Automatic update scheduled in 9 hours

 **Gutenberg PDF Viewer Block**
You have version 0.0.1 installed. Update to 0.1. [View version 0.1 details.](#)
Compatibility with WordPress 5.5: Unknown  Automatic update scheduled in 9 hours

 **Simple Site Map Page**
You have version 1.1 installed. Update to 1.2. [View version 1.2 details.](#)
Compatibility with WordPress 5.5: Unknown  Automatic update scheduled in 9 hours

Select All

[Update Plugins](#)

The WordPress developer team is working on adding an auto-update mechanism to themes and plugins, a common source of website hacks, primarily because site owners usually install themes and plugins, and then forget to update them.

Currently, the auto-update feature is already implemented for plugins, and work is underway on adding it to WordPress' themes feature. Once the auto-update option rolls out for the stable versions of the WordPress content management system (CMS), site owners will be able to configure themes and plugins to update themselves by checking an option in their site's admin panels.

Cyber-security firms like Sucuri, Wordfence, WebARX, and NinTechNet have often pointed out that a vast majority of today's hacked WordPress sites are being compromised after hackers exploit vulnerabilities in out-of-date plugins and themes. This feature is expected to reduce the number of hacked WordPress sites, once it rolls out with the upcoming WordPress 5.5 release.

[Read More on ZDNet](#)

More #News

- [WordPress and Apache Struts account for 55% of all weaponized vulnerabilities](#)
- [NIST Updates Flagship SP 800-53 Security and Privacy Controls](#)
- [Researcher: Microsoft Edge Least Private of 6 Browsers](#)
- [Firefox Password Manager To Be Secured With Windows 10 Credentials](#)
- [Rogers Data Breach Exposed Customer Info in Unsecured Database](#)

- [Hackers Hide Malware C2 Communication By Faking News Site Traffic](#)
- [Food Delivery Service in Germany Under DDoS Attack](#)
- [NIST shared dataset of tattoos that's been used to identify prisoners](#)
- [Fintech company Finastra hit by ransomware](#)
- [This PIN Can Be Easily Guessed](#)
- [Financial companies leak 425GB in company, client data through open database](#)
- [COVID-19 Testing Center Hit By Cyberattack](#)
- [Security flaws found in popular password managers](#)
- [Europol Dismantles SIM Swap Criminal Groups That Stole Millions](#)
- [Browser vendor leaks data via open server](#)
- [There is a Serious Lack of Corporate Responsibility During Breach Disclosures](#)
- [Most ransomware attacks take place during the night or over the weekend](#)

#Patch Time!

- [Adobe Fixes Nine Critical Vulnerabilities in Reader, Acrobat](#)
- [VMware patches privilege escalation vulnerability in Fusion, Horizon](#)
- [Two Trend Micro zero-days exploited in the wild by hackers](#)
- [Critical RCE Bug in Windows 7 and Server 2008 Gets Micropatch](#)
- [Cisco tackles root privilege vulnerability in SD-WAN software](#)
- [Drupal Updates CKEditor to Patch XSS Vulnerabilities](#)
- [Intel CPUs vulnerable to new 'Snoop' attack](#)
- [Slack fixes account-stealing bug](#)

#Tech and #Tools

- [LeakLooker GUI – Discover, browse and monitor database/source code leaks.](#)
- [Android – Coronavirus – related malware tracker](#)
- [Demonstrating that revocation checking is pointless!](#)
- [Hacking Docker Remotely](#)
- [Reversing Firmware With Radare](#)
- [HTTP Desync Attacks with Python and AWS](#)
- [Authorize: Automatic authorization enforcement detection extension for burp suite](#)
- [Using Content-Security-Policy with multiple policies](#)
- [Cloud WAF Comparison Using Real-World Attacks](#)
- [Red Team Tactics: Advanced process monitoring techniques in offensive operations](#)
- [Hiding Your .NET – ETW](#)
- [LDAPFragger: Bypassing network restrictions using LDAP attributes](#)
- [DNS for red team purposes](#)
- [Network IDS & Azure Sentinel](#)
- [Azure Security Benchmark—90 security and compliance best practices for your workloads in Azure](#)
- [Yaramod: Inspect, Analyze and Modify your YARA rules with ease](#)
- [Blue Team fundamentals Part Two: Windows Processes.](#)
- [Ukemi: A CLI tool for querying passive DNS services](#)

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>