kindred

Security Newsletter

11 June 2018

Subscribe to this newsletter

Prowli Malware Operation Infected Over 40,000 Servers, Modems, and IoT Devices

After the discovery of massive VPNFilter malware botnet, security researchers have now uncovered another giant botnet that has already compromised more than 40,000 servers, modems and internet-connected devices belonging to a wide number of organizations across the world. Named Prowli and discovered by the GuardiCore security team, this botnet is a diverse operation that relies on vulnerabilities and credentials brute-force attacks to infect and take over devices.

Since the attackers behind the Prowli attack are abusing the infected devices and websites to mine cryptocurrency or run a script that redirects them to malicious websites, researchers believe they are more focused on making money rather than ideology or espionage.

Besides cryptocurrency miner, attackers are also using a well known open source webshell called "WSO Web Shell" to modify the compromised servers, eventually allowing attackers to redirect visitors of websites to fake sites distributing malicious browser extensions.

Since the attackers are using a mix of known vulnerabilities and credential guessing to compromise devices, users should make sure their systems are patched and up to date and always use strong passwords for their devices. Moreover, users should also consider locking down systems and segmenting vulnerable or hard to secure systems, in order to separate them from the rest of their network.

Read More

Even More

ZipSlip: How poisoned archives can hack your computer

Booby-trapped archive files can exploit vulnerabilities in a swath of software to overwrite documents and data elsewhere on a computer's file system – and potentially execute malicious code. Specifically, the flaws, dubbed "Zip Slip" by its discoverers at security outfit Snyk, are path traversals that can potentially be exploited to perform arbitrary code execution attacks. It affects certain tools that handle .zip, .tar, .war, .cpio, and .7z formats.

Thousands of projects written in various programming languages including JavaScript, Ruby, Java, .NET and Go—from Google, Oracle, IBM, Apache, Amazon, Spring/Pivotal, Linkedin, Twitter, Alibaba, Eclipse, OWASP, ElasticSearch, JetBrains and more—contained vulnerable codes and libraries.

Using this Zip Slip attack an attacker can even overwrite legitimate executable files or configuration files for an application to trick the targeted system or the user into running it, "thus achieving remote command execution on the victim's machine," the company explains. Team Snyk said any developer who uses one of the vulnerable libraries should update their code to use the latest patched version, where available, and make sure users are updated, too – and also check their own code to make sure file names and paths are validated before extraction.

Read More

Even More

VPNFilter malware now targeting Asus, D-Link, Huawei, ZTE devices

The new strain of malware known as VPNFilter is targeting more makes and models of devices and boasting additional capabilities, including the ability to deliver exploits to endpoints and override reboots, Cisco Talos has reported. Originally, Talos found VPNFilter had infected at least 500,000 networking devices, mainly consumer-grade internet routers, across 54 countries.

According to new research technical details published today by the Cisco Talos security team, the malware —which was initially thought to be able to infect devices from Linksys, MikroTik, Netgear, TP-Link, and QNAP— can also infect routers made by ASUS, D-Link, Huawei, Ubiquiti, UPVEL, and ZTE. The list of devices vulnerable to VPNFilter has seen a sharp jump from Cisco's original report, going from 16 device models to 71 —and possibly more.

In addition to adding new devices to the list, Talos said it discovered a new stage 3 module -- named "ssler" -- that injects malicious content into web traffic as it passes through a network device, which allows the actor to deliver exploits to endpoints via a man-in-the-middle capability. Despite the FBI urging small businesses and households to immediately reboot routers following initial reports from Talos, it won't prevent the threat; even after a reboot, ssler renders the malware capable of maintaining a persistent presence on an infected device.

Read More

Even More

Cutting room floor

- Jira bug exposed private server keys at major companies, researcher finds
- Cisco fixes 9.8 CVSS critical bug in ACS that exposed networks to hackers
- Threats to the 2018 Football World Cup: Traditional Rules or a New Style of Play?
- WannaCry reverse-engineer Marcus Hutchins hit with fresh charges
- Ticketfly cyberattack exposed data belonging to 27 million accounts
- Update Google Chrome: High Severity CSP Bypass Vulnerability
- Facebook Bug Caused New Posts by 14 Million Users to be Shared Publicly
- Geneology Service MyHeritage Leaked 92 Million Credentials
- Adobe Patches Zero-Day Flash Flaw
- BabaYaga WordPress Malware Updates Your Site
- Misconfigured Google Groups Settings Leaking Sensitive Data
- 75% of the 'Left to Get Hacked' Redis Servers Found Infected
- All New Privacy and Security Features Coming in macOS 10.14 Mojave
- Mirai Variants Continue to Spawn in Vulnerable IoT Ecosystem
- Introducing DNS Resolver for Tor
- Drupalgeddon 2 wreaking havoc on 900+ sites because IT still hasn't applied updates
- Sofacy APT Has Subtly Changed Tactics

#Tech and #Tools

- Prowler: AWS Security Best Practices Assessment, Auditing, Hardening and Forensics Readiness Tool
- Adobe Flash Zero-day leveraged for targeted attack in the middle east
- Adding RetGuard to clang for OpenBSD
- A cartoon intro to DNS over HTTPS
- A Methodical Approach to Browser Exploitation
- Reading Your Emails With A Read&Write Chrome Extension Same Origin Policy Bypass (~8 Million Users Affected)
- WhaleTail: Reverse Docker images into Dockerfiles
- ZipSlip vulnerability: Technical details
- OTSECA: Open source security auditing tool to search and dump system configuration.

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our SOC analyst position
- You're into identity and access management? We are looking for an IAM Specialist
- Interested in Governance, Risk and Compliance? Apply for our InfoSec team

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. You can find all our open vacancies on our career page.

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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