THE STATE OF SECURITY (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/)

News. Trends. Insights.

Ruckus Raucous: Finding Security Flaws in Enterprise-Class Hardware

CRAIG YOUNG (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/CRAIG-YOUNG/)

AUG 3, 2016 | VULNERABILITY MANAGEMENT (/STATE-OF-SECURITY/TOPICS/VULNERABILITY-MANAGEMENT/)

(HTTP://WWW.TRIPWIRE.COM/STATE-

87

Wireless routers designed for consumers often do not employ proper security practices.

This topic was extensively covered in VERT's 2014 report, "SOHO Wireless Router (In)security." Our research revealed that 74% of the 50 top-selling consumer routers on Amazon shipped with security vulnerabilities, including 20 different models where the latest firmware from the vendor was exploitable. Many people I have discussed this research with have expressed the opinion that, for one reason or another, this problem is more or less confined to the consumer sector.

My suspicion was that feature wars and low profit margins could be contributing to the epidemic of insecure routers. In an attempt to determine whether this issue was limited to the consumer market, I decided it would be necessary to obtain and evaluate a wireless router designed for enterprise networks.

Naturally, the first step of this research project was to pick a target.

Whereas there are many brands of affordable consumer routers, enterprise equipment is not cheap and my budget meant I would most likely be limited to testing a single product family. I started by conducting some "war walking (http://www.itworld.com/article/2776266/security/war-walking--detecting-wireless-networks.html)" with the Android Wi-Fi Analyzer app to get an idea of what brands are being installed in real-world environments. From this, I found that Ruckus and Cisco seem to have a strong hold on the market. A report from Dell'Oro Group (http://www.slideshare.net/CommsDay/cdsummit-2015-ruckus-wireless-david-wright/4) stated that Ruckus accounted for 42% of the units shipped in 4Q14 and so, with that, I decided to proceed with Ruckus.

METHODOLOGY

To keep my comparison meaningful, I decided it would be best to limit the scope of my testing to the HTTP interface and use the same methodology I used for finding vulnerabilities in the consumer routers.

This was easy because I had already established an effective testing process over the course of a few router security assessments. At a high-level, I use a combination of manual fuzz testing and partially automated querying based on information extracted from firmware and shell access where available.

Earlier this year, I taught about these techniques at length during an AusCERT tutorial session titled 'Brainwashing Embedded Systems.' I am also happy to report that I will again be sharing this knowledge in a DEF CON 24 workshop (http://www.tripwire.com/state-of-security/security-awareness/events/brainwashing-embedded-systems/) as well as a SecTor 2016 training session.

FIRST IMPRESSIONS

Before investing in an expensive high-end Ruckus model, I decided to start my tests with a second-hand Ruckus ZoneFlex running the latest available firmware as of 10/27/15.

Within a few minutes of setting up the device, I found a command injection, which is exploitable through a forged request due to a general lack of CSRF tokens. As with many of the consumer routers I had tested, the ZoneFlex offers administrators an option to perform diagnostics, including a simple ping test, with apparently no input sanitization. In every case where I've found this flaw on a consumer router, it has been pretty devastating.

Although the light-weight consumer embedded devices commonly have all processes running as uid 0 (root), I thought certainly an enterprise product would use privilege separation. The ping operation requires no special privilege, so it should be running as a user with limited access. I tested this theory by crafting a ping parameter to spawn a telnet daemon and to my surprise, it worked and I was granted a root shell.

This was more than enough confirmation to me that it would be worth the investment in a current model.

ANALYZING THE RUCKUS HTTP INTERFACE

After some Google searches, I found that I was not the only person aware of this blatant command injection.

My ZoneFlex model was EOL with rather old firmware so naturally, I expected that this low-hanging fruit would have been fixed in the new product. My research picked up again when I set up a Ruckus H500 access point with the latest firmware (100.1.0.0.432); I was shocked to find that the ping injection still worked! After obtaining a shell on this fully patched access point, I proceeded by creating a simple list of files contained in the web server's document root. This is a trivial process possible from either the shell access or through firmware extraction and can be supplemented by locating possible URIs embedded within the server's binaries.

In this particular case, I limited myself just to the files visible in the firmware update. I then fed this list into a script I have for crawling an HTTP server and recording which files are accessible without authentication.

THE FINDINGS

As was commonly the case with consumer devices, this rather simple process exposed a few flaws:

- **Authentication Bypass:** All requests containing a particular string received '200 OK' responses. By creatively adding this string to other requests, I was able to get response data intended only for authenticated queries. This is a behavior I have observed in routers from NETGEAR, TrendNET and Asus.
- **Denial of Service:** There is a particular page accessible over HTTP without authentication that, when requested over SSL, causes the management interface to become unavailable. This is a serious issue as the product relies on HTTP when used as a hot spot.
- **Information Disclosure:** The device's serial number is exposed by the HTTP server. It is unclear whether this has any direct security impact but it may be useful to an attacker as part of a social engineering ploy. I have also observed other products where the serial number is used as a means to prove ownership of a device.

Additionally, I also found that authenticated requests for a certain page would trigger excessive memory consumption causing the HTTP server to reload, as well as possible disruption to other services. This vector is exploitable via GET requests and therefore lends itself to CSRF attacks through malicious image tags in HTML documents or emails.

RUCKUS' RESPONSE

These were not the only vulnerabilities in the Ruckus access point but at this point, I reached out to the vendor.

Unlike with some vendors where it takes guess work to figure out an appropriate security contact, Ruckus has a page listing a PGP key and email address for reporting vulnerabilities. While this is normally a good sign of a responsive organization, repeated attempts to email them my report resulted in bounces.

In early January 2016, about a month after I first reached out to Ruckus, I emailed several other posted addresses stating my problem reaching the security contact. A webmaster contact responded letting me know that he would get the account setup but after resending the report and asking for receipt confirmation, I heard nothing. Later that month, I contacted CERT who assigned VU#974320 and confirmed that they could not get a response from Ruckus.

Ruckus did not acknowledge receipt of any vulnerability reports until Tripwire's Chief Research Officer, David Meltzer, reached out directly to Ruckus executives over LinkedIn.

After that I received a forwarded copy of my encrypted report from January with a request for receipt confirmation. During a follow-up call I was told that they had not been able to decrypt my message and had therefore ignored it. I was also told that they had no knowledge that CERT had attempted to contact them. I have been advised by Ruckus that these vulnerabilities present in the HTTPS interface are not exposed unless the product is running in standalone mode.

I have yet to validate these claims or to perform a full security audit on any Ruckus product.

LESSONS LEARNED

The lesson from this research project seems to be that “enterprise-class” hardware does not necessarily mean enterprise quality in terms of security.

My experience auditing Ruckus equipment is very similar to some of the experiences I’ve had auditing the wireless routers you might find in a local computer store. In fact, the authentication bypass and command injection are essentially the same problems I have found on SOHO devices in the $100-$200 range.

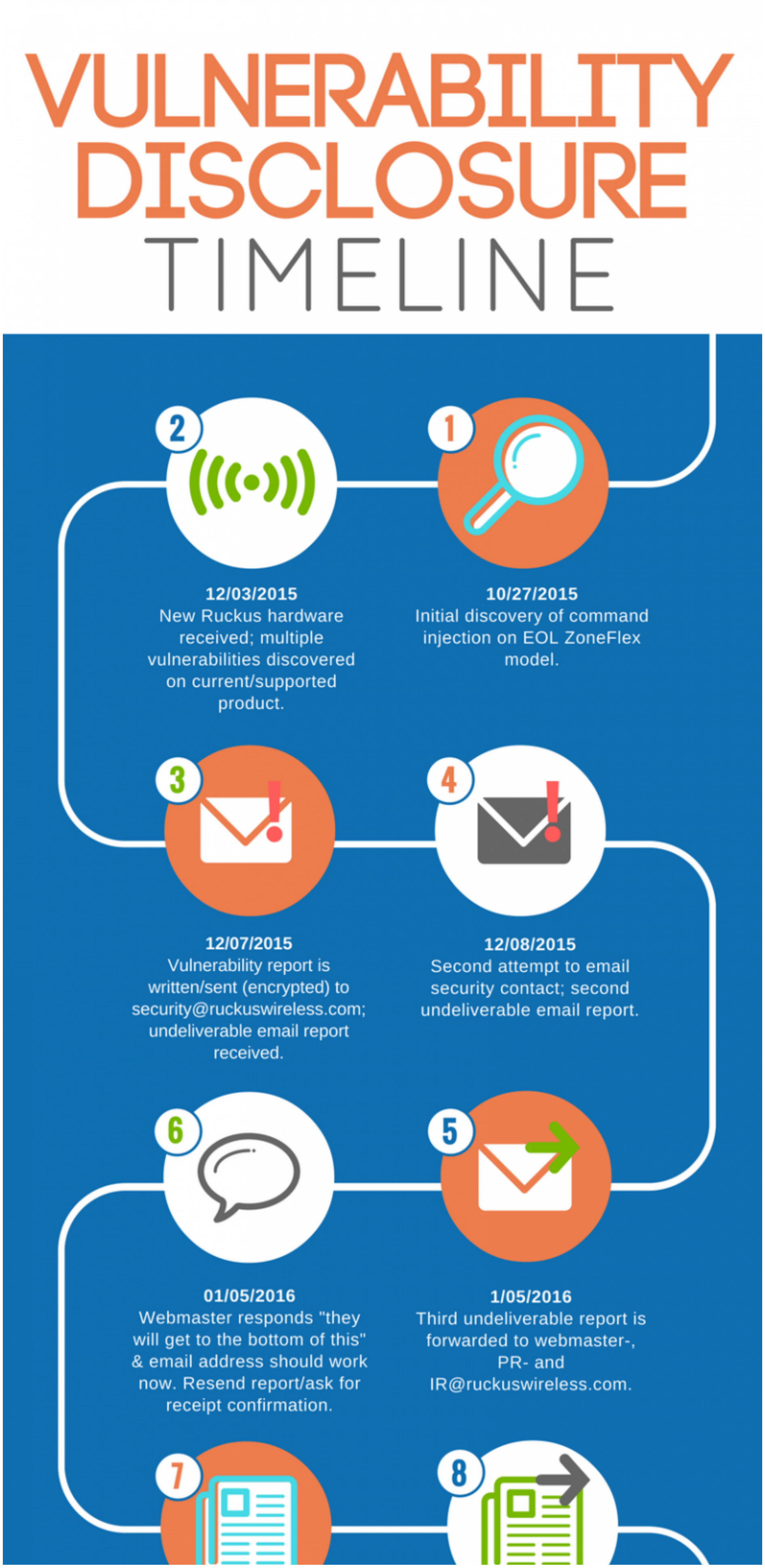
The biggest difference here is that my report to Ruckus appears was completely ignored for many months and required ‘Executive-to-Executive’ communication before the report was acknowledged. Organizations using Ruckus devices may be at risk for compromise, particularly when the access points are used to provide customers with Wi-Fi access.

An intruder to one of these systems could potentially become man-in-the-middle to all other users of the wireless network allowing a wide range of exploitation opportunities. Ruckus has advised that only standalone APs would be affected but I have not had a chance to evaluate this claim and do not know how prevalent the standalone mode is.

The bulk of the security research described in this article was performed in a single evening, so in my opinion it would be foolish to think that there are not more issues lurking or that the other operating modes are necessarily any more secure.

Discover how to help protect your embedded devices better by reading this article, “Five Security Tips to Protect Embedded Devices”. (http://www.tripwire.com/state-of-security/security-awareness/five-security-tips-to-protect-embedded-devices/)

A full timeline of this disclosure process is as follows:



VULNERABILITY DISCLOSURE TIMELINE

1

10/27/2015
Initial discovery of command injection on EOL ZoneFlex model.

2

12/03/2015
New Ruckus hardware received; multiple vulnerabilities discovered on current/supported product.

3

12/07/2015
Vulnerability report is written/sent (encrypted) to security@ruckuswireless.com; undeliverable email report received.

4

12/08/2015
Second attempt to email security contact; second undeliverable email report.

5

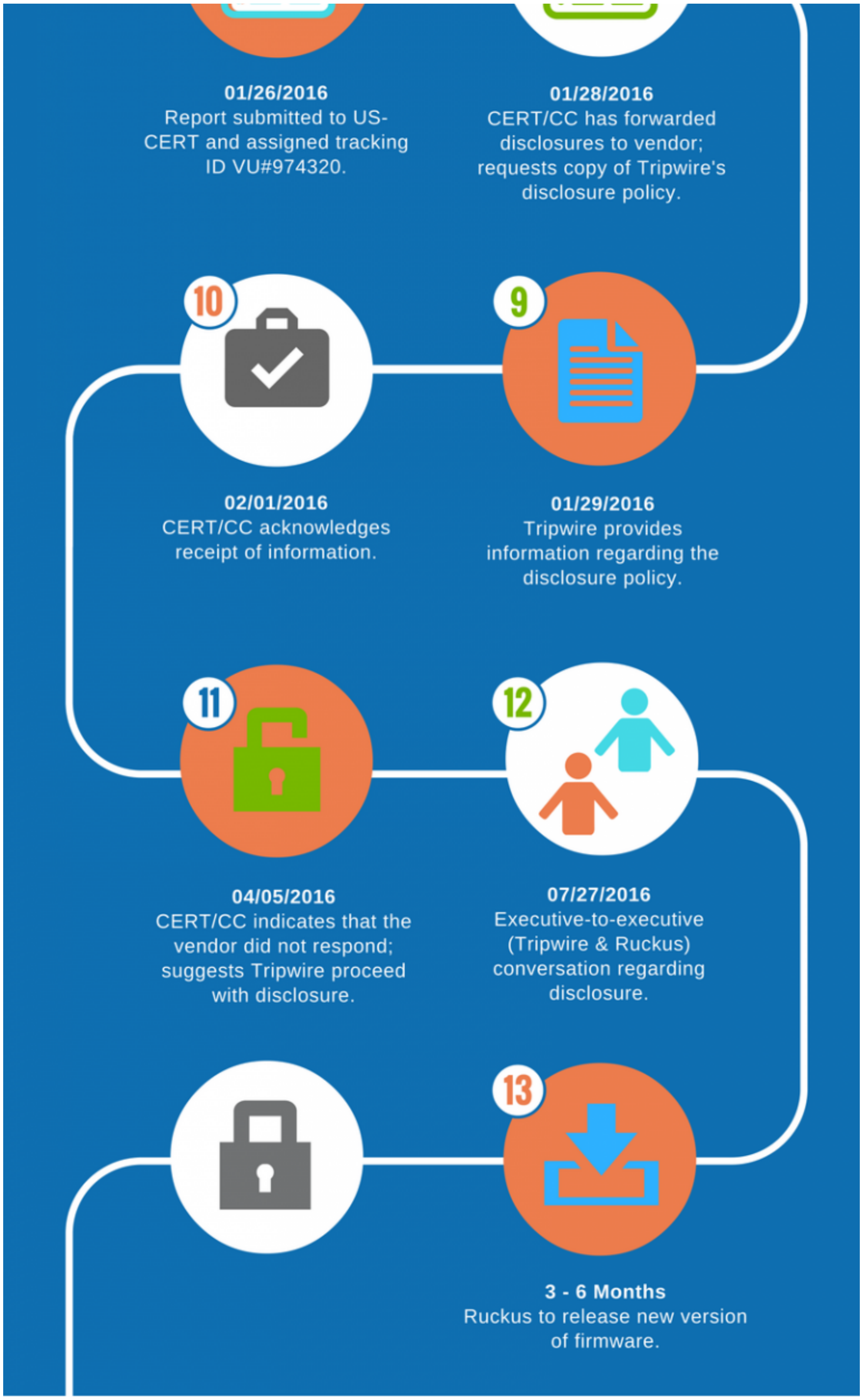
1/05/2016
Third undeliverable report is forwarded to webmaster-, PR- and IR@ruckuswireless.com.

6

01/05/2016
Webmaster responds "they will get to the bottom of this" & email address should work now. Resend report/ask for receipt confirmation.

7

8



01/26/2016
Report submitted to US-CERT and assigned tracking ID VU#974320.

01/28/2016
CERT/CC has forwarded disclosures to vendor; requests copy of Tripwire's disclosure policy.

9

01/29/2016
Tripwire provides information regarding the disclosure policy.

10

02/01/2016
CERT/CC acknowledges receipt of information.

11

04/05/2016
CERT/CC indicates that the vendor did not respond; suggests Tripwire proceed with disclosure.

12

07/27/2016
Executive-to-executive (Tripwire & Ruckus) conversation regarding disclosure.

13

3 - 6 Months
Ruckus to release new version of firmware.

Research conducted by: Craig Young, Sr. Security Research Engineer at Tripwire & the Vulnerability and Exposure Research Team (VERT)

tripwire TRIPWIRE VERT

87

ENTERPRISE NEEDS ON AN SMB BUDGET?
Get Compliance and Configuration Assessment in a box from the compliance solutions experts.
TRIPWIRE®
CCM EXPRESS
30-day free trial

CATEGORIES	FEATURED ARTICLES (/STATE-OF-SECURITY/TOPICS/FEATURED/), SECURITY AWARENESS (/STATE-OF-SECURITY/TOPICS/SECURITY-AWARENESS/), VULNERABILITY MANAGEMENT (/STATE-OF-SECURITY/TOPICS/VULNERABILITY-MANAGEMENT/)
TAGS	DISCLOSURE (/STATE-OF-SECURITY/TAG/DISCLOSURE/), RUCKUS (/STATE-OF-SECURITY/TAG/RUCKUS/), SECURITY (/STATE-OF-SECURITY/TAG/SECURITY/), VULNERABILITY (/STATE-OF-SECURITY/TAG/VULNERABILITY/)

0 Comments **The State of Security** 1 **Login**

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **THE STATE OF SECURITY**

The 'I'm Too Small to be a Target' Fallacy

1 comment • 14 days ago•

Keith Bishop — I completely agree with the concept of this article. We all need to protect the …

Mandatory Security Design Considerations for the IoT / IoE

1 comment • 2 months ago•

Mike Barrett — Thank you for your Points. I would submit that very few Industrial Control Systems …

DEF CON 24: Brainwashing Embedded Systems

2 comments • a month ago•

Tripwire, Inc. — Yes, August 6 is on the Saturday.

Security Pros Not Confident in Ability to Respond to …

1 comment • 2 months ago•

Khürt L. Williams — "Following the 3-2-1 backup rule is a good first step to prepare for a …

Subscribe Add Disqus to your site Add Disqus Add Privacy

About Craig Young

(http://www.tripwire.com/state-of-security/contributors/craig-young/)

Craig Young (http://www.tripwire.com/state-of-security/contributors/craig-young/) has contributed 45 posts to The State of Security.

View all posts by Craig Young ›

Follow @craigtweets (https://twitter.com/craigtweets)

Latest Security News (/state-of-security/topics/latest-security-news/)

French Dark Web Posts Ad for Content Cleaner to be Paid in Stolen Goods SEP 8, 2016

Seven Online Scammers Prison Bound for International Fraud Conspiracy SEP 8, 2016

Hutton Hotel Warns of Payment Card Breach That Lasted Over 3 Years SEP 7, 2016

Yelp Will Award Up to $15K for Exploits Found in Bug Bounty Program SEP 7, 2016

Mega Breach Strikes Rambler.ru with Leak of Nearly 100M User Records SEP 6, 2016

FEATURED RECENT

(http://www.tripwire.com/state-of-security/security-data-protection/why-technology-automation-is-a-sure-shot-way-of-strengthening-your-security-posture/)

Why Technology Automation Is a Sure-Shot Way Of Strengthening Your Security Posture (http://www.tripwire.com/state-of-security/security-data-protection/why-technology-automation-is-a-sure-shot-way-of-strengthening-your-security-posture/)

SEP 8, 2016

(http://www.tripwire.com/state-of-security/government/report-claims-national-security-was-put-at-risk-by-the-opm-data-breach/)

Report claims national security was put at risk by the OPM data breach (http://www.tripwire.com/state-of-security/government/report-claims-national-security-was-put-at-risk-by-the-opm-data-breach/)

SEP 8, 2016

(http://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/the-new-mindset-required-for-

The New Mindset Required for Making a Dent in the World of Cybercrime (http://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/the-new-mindset-required-for-making-a-dent-in-the-world-of-cybercrime/)

SEP 7, 2016

making-a-dent-in-the-world-of-cybercrime/)

(http://www.tripwire.com/state-of-security/security-awareness/evolution-of-the-camera-society/)

Evolution of a ‘Cameras Are Everywhere’ Society (http://www.tripwire.com/state-of-security/security-awareness/evolution-of-the-camera-society/)

SEP 7, 2016

(http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/august-2016-the-month-in-ransomware/)

August 2016: The Month in Ransomware (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/august-2016-the-month-in-ransomware/)

SEP 6, 2016

Tweets by @TripwireInc

Tripwire, Inc.
@TripwireInc

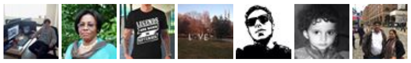
Monthly Windows rollup: simplification or loss of patching control? bit.ly/2cpbEQc via @searchsecurity @MT_Heller w/ @treguly

Embed View on Twitter

Tripwire
6,568 likes

Like Page Sign Up

Be the first of your friends to like this



Topics (/state-of-security/topics/)

- Government
- ICS Security
- Incident Detection
- IT Security and Data Protection
- Latest Security News
- Off Topic
- Regulatory Compliance
- Risk-Based Security for Executives
- Security Awareness
- Security Slice
- Tripwire News
- Vulnerability Management

FEATURED ARTICLES (/STATE-OF-SECURITY/TOPICS/FEATURED/)
TOPICS (/STATE-OF-SECURITY/TOPICS/)
ABOUT (/STATE-OF-SECURITY/ABOUT/)
CONTRIBUTORS (/STATE-OF-SECURITY/CONTRIBUTORS/)
PRIVACY POLICY (HTTP://WWW.TRIPWIRE.COM/LEGAL/PRIVACY/)
TRIPWIRE.COM (HTTP://WWW.TRIPWIRE.COM/)

FOLLOW US