

NEWS

KASPERSKY SAYS NEW ZERO-DAY MALWARE HIT iPhones including its own

On the same day, Russia's FSB intelligence service launched wild claims of NSA and Apple hacking thousands of Russians.

THE MOSCOW-BASED CYBER-SECURITY firm Kaspersky has made headlines for years by exposing sophisticated hacking by Russian and Western state-sponsored cyberspies alike. Now it's exposing a stealthy new intrusion campaign where Kaspersky itself was a target.

In a report published today, Kaspersky said that at the beginning of the year, it detected targeted attacks against a group of iPhones after analyzing the company's own corporate network traffic. The campaign, which the researchers call Operation Triangulation and say is "ongoing," appears to date back to 2019 and utilized multiple vulnerabilities in Apple's iOS mobile operating system to let attackers take control of victim devices.

Kaspersky says the attack chain utilized "zero-click" exploitation to compromise targets' devices by simply sending a specially crafted message to victims over Apple's iMessage service. Victims received the message, which included a malicious attachment, and exploitation would begin whether victims opened the message and inspected the attachment or not. Then the attack would chain together multiple vulnerabilities to give the hackers deeper and deeper access to the target's device. And the final malware payload would automatically download to the victim's device before the original malicious message and attachment self-deleted.

Kaspersky's revelation of the new iOS hacking campaign comes on the same day that Russia's FSB intelligence service separately announced a claim that the US National Security Agency has hacked thousands of Russians' phones.

Even more remarkably, the FSB claimed that Apple had participated in that broad hacking of iOS devices, willingly providing vulnerabilities to the NSA to exploit in its spying operations. Apple said in a statement to WIRED, "We have never worked with any government to insert a backdoor into any Apple product and never will."

When asked about Kaspersky's report, an Apple spokesperson noted that the findings only appear to pertain to iPhones running iOS version 15.7 and below. The current version of iOS is 16.5. Kaspersky says that the malware it discovered cannot persist on a device once it is rebooted, but the researchers say they saw evidence of reinfection in some cases. The exact nature of the vulnerabilities used in the exploit chain remains unclear, though Kaspersky says that one of the flaws was likely the kernel extension vulnerability CVE-2022-46690 that Apple patched in December.

Zero-click vulnerabilities can exist on any platform, but in recent years, attackers and spyware vendors have focused on finding these flaws in Apple's iOS, often in iMessage, and exploiting them to launch targeted attacks on iPhones. This is partly because services like iMessage present unusually fertile ground within iOS for discovering vulnerabilities, but also because attacks on iOS devices with this approach are often very difficult for victims to detect.

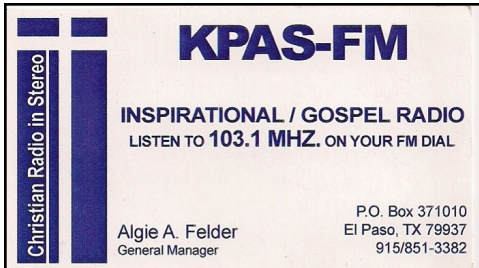
"Kaspersky, arguably one of the best exploit detection companies in the world, was potentially hacked via an iOS zero-day for five years, and it was only discovered now," says longtime macOS and iOS security researcher Patrick Wardle. "That shows how ridiculously hard it is to detect these exploits and attacks."

- KTSM-TV
- KVIA-TV
- KRWG-TV
- KBNA-AM/FM & KAMA-AM
- KHEY-AM/FM, KPRR-FM & KTSM-AM/FM
- KLAQ-FM, KISS-FM & KROD-AM
- KPAS-FM-ALGIE A. FELDER CSBE
- KINT98.COM
INTERNET RADIO NETWORK
- BURST COMMUNICATIONS INC.- KIRK BASEFSKY
- JOHN LACKNESS
- ENTRAVISION COMMUNICATIONS
- SCMS, INC.-
- ABS ADVANCED BROADCAST SERVICES, LLC
- KSCE-TV
- RF Specialties of Texas
- KCOS-TV
- KELP-AM
ARNOLD McClatchy.
- MARSAND, INC.
- Ho Tah Say. LLC



KINT
EL PASO'S MOST
MUSIC VARIETY
ON-LINE
RADIO STATION

98 LIKE US ON FACEBOOK
.COM

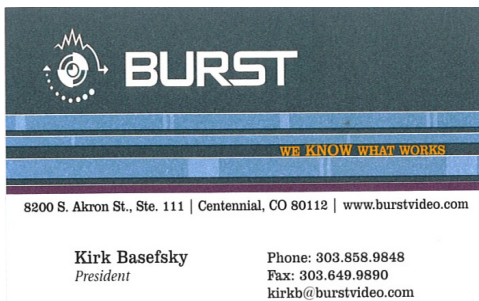


KPAS-FM
INSPIRATIONAL / GOSPEL RADIO
LISTEN TO **103.1 MHZ.** ON YOUR FM DIAL

Christian Radio in Stereo

Algie A. Felder
General Manager

P.O. Box 371010
El Paso, TX 79937
915/851-3382



BURST
WE KNOW WHAT WORKS

8200 S. Akron St., Ste. 111 | Centennial, CO 80112 | www.burstvideo.com

Kirk Basefsky
President

Phone: 303.858.9848
Fax: 303.649.9890
kirkb@burstvideo.com



KTSM.com
ph: 915.532.5421

3801-D Constitution
El Paso, TX | 79922

Nexstar KTSM.com estrellaTV

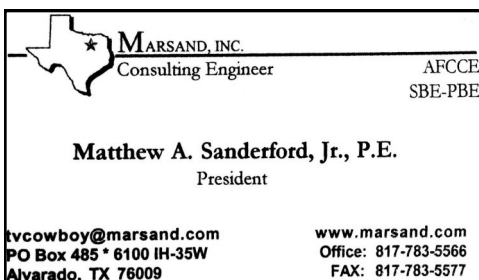


BRENDA DE ANDA-SWANN
GENERAL MANAGER

KVIA-TV
4140 Rio Bravo El Paso, TX 79902

Office (915) 496-1770
Cell (915) 204-5365
brenda@kvia.com

abc KVIA.com
EL PASO
LIVE COVERAGE
CW
AMERICA



MARSAND, INC.
Consulting Engineer

AFCCCE
SBE-PBE

Matthew A. Sanderford, Jr., P.E.
President

tvcowboy@marsand.com
PO Box 485 • 6100 IH-35W
Alvarado, TX 76009

www.marsand.com
Office: 817-783-5566
FAX: 817-783-5577

In their report, the Kaspersky researchers point out that one of the reasons for this difficulty is iOS's locked-down design, which makes it very tough to inspect the operating system's activity.

"The security of iOS, once breached, makes it really challenging to detect these attacks," says Wardle, who was formerly an NSA staffer. At the same time, he adds that attackers would need to assume any brazen campaign to target Kaspersky would eventually be discovered. "In my opinion, this would be sloppy for an NSA attack," he says. "But it shows that either hacking Kaspersky was incredibly valuable for the attacker or that whoever this was likely has other iOS zero days as well. If you only have one exploit, you're not going to risk your only iOS remote attack to hack Kaspersky."

The NSA declined WIRED's request for comment on either the FSB announcement or Kaspersky's findings.

With the release of iOS 16 in September 2022, Apple introduced a special security setting for the mobile operating system known as Lockdown Mode that intentionally restricts usability and access to features that can be porous within services like iMessage and Apple's WebKit. It is not known whether Lockdown Mode would have prevented the attacks Kaspersky observed.

The Russian government's purported discovery of Apple's collusion with US intelligence "testifies to the close cooperation of the American company Apple with the national intelligence community, in particular the US NSA, and confirms that the declared policy of ensuring the confidentiality of personal data of users of Apple devices is not true," claims an FSB statement, which adds that it would allow the NSA and "partners in anti-Russian activities" to target "any person of interest to the White House," as well as US citizens.

SBE CHAPTER 38 OFFICERS

CHAIRMAN

Antonio Castro
SBE member # 11456.
KFOX/COX retired Chief Eng.
800 Arredondo dr.
El Paso. TX 79912
915-584-1220 home
915-525-8507 cell
farahjac@sbcglobal.net

VICE CHAIRMAN

Bruno Cruz
SBE member # 25867
200 E. Alto Mesa
El Paso, TX. 79912
915-757-7898
915-526-1842 cell
Bruno.cruzJR@kfoxtv.com

TREASURER

Walter Hanthorn
SBE member # 18307
KSCE TV
4461 Gen. Maloney
El Paso, TX. 79924
915-269-7583 home
915-532-8588 office

CERTIFICATION COMMITTEE:

David Halperin.

MEMBERSHIP COMMITTEE:

Antonio Castro
Warren Reeves

FREQUENCY COORDINATION

COMMITTEE:

Warren Reeves
Owen Smith

SCHOLARSHIP COMMITTEE:

Rick Vilardell

WEB SITE COMMITTEE:

Norbert Miles

SUSTAINING MEMBERSHIP:

Antonio Castro

PROGRAM CHAIRMAN:

Warren Reeves

NEWSLETTER:

Antonio Castro

EAS CHAIRMAN:

Michael Rivera

EXECUTIVE COMMITTEE:

Antonio Castro
Bruno Cruz
Walter Hanthorn



David Grice
President

915-308-1227
4774 Villa Hermosa Dr
El Paso TX 79912
www.AdvancedBroadcastServices.com
Dgrice@AdvancedBroadcastServices.com



KRWG
PUBLIC MEDIA

n p r

SCMS INC.
YOU KNOW WE KNOW
RADIO

for
Broadcast
Equipment
Solutions

800 438 6040 Sales
704 889 4508
www.scmsinc.com

Walter Alvarez
Market President | El Paso
iHeartMedia

4045 N Mesa Street
El Paso, TX 79902

915.351.5473
915.201.7627

walteralvarez@iheartmedia.com



EL PASO, TX SBE CHAPTER 38 MEETING MINUTE

DATE 5/9/2023 **LOCATION:** COMO'S ITALIAN REST.

MEETING CALLED TO ORDER: 12:13 PM , BY ANTONIO CASTRO. WE WERE 7 (SEVEN) ATTENDANTS

REPORT OF THE SECRETARY: MINUTES IN THE MAY NEWSLETTER. ACCEPTED BY MICHAEL RIVIERA, SECONDED BY BRUNO CRUZ.

REPORT OF THE TREASURER: \$ 5,041.05 IN THE BANK ACCEPTED BY NORBERT MILES, SECONDED BY WALTER HANTHORN.

REPORT OF THE CERTIFICATION COMMITTEE: NO REPORT

REPORT OF THE MEMBERSHIP COMMITTEE: GLENN LEFFLER WAITING FOR KELP OWNER IN ORDER TO RENEW THEIR MEMBERSHIP. WARREN REEVES WILL ASK TO "ZARCO ELECTRONICS" TO BE A MEMBER. .

REPORT OF THE FREQUENCY COORDINATOR COMMITTEE: NO NOISE IN THE CLEAR SPECTRUM.....NO REPORT.

REPORT OF THE SCHOLARSHIP COMMITTEE NO REPORT.

REPORT OF THE WEBSITE COMMITTEE: NOW 4375 VS. 4293 EQUAL 82 HITS. POSTED THE ENNES WORKSHOP FLYER. TO POST THE NEXT BEST THING FLYER.

REPORT OF THE EAS CHAIRMAN: TEXAS MONTHLY TEST WAS FINE. NEW MEXICO FAIL TO DO MONTHLY TEST BECAUSE NO OPERATOR AT Kkob IN ALBUQUERQUE, NM..

REPORT OF THE PROGRAM COMMITTEE: BRUNO CRUZ WILL LOCK FOR SOMEBODY.

NEW BUSINESS OR ANY ITEMS FOR THE CHAPTER INTEREST : UPDATE "ENNES WORKSHOP" TO BE HOLD ON JUNE 9, 2023. WINDHAM AIRPORT HOTEL.

OTHER. THE NEXT BEST THING TOUR WILL DISPLAY IN JUNE 15 AT THE KVIA-TV PARKING LOT.

NEXT MEETING DATE AND LOCATION: JUNE THE 15th .AT THE KVIA-TV PARKING LOT.

MEETING ADJOURNED: AT 12:36 PM

MEET OUR NEW CHAPTER MEMBER
IAN PETER LEWIS

See page 6 for bio and info..

JUNE PROGRAM

FOR THE MONTH OF MAY, WE HAD OUR MEETING FACE TO FACE, IN PERSON, NO PRESENTATION, NOTHING TO CELEBRATE !!!

WE MET AT THE ITALIAN RESTAURANT COMO'S

OUR JUNE MEETING WILL TAKE PLACE ALONG WITH THE NEXT BEST THING TOUR SHOW.

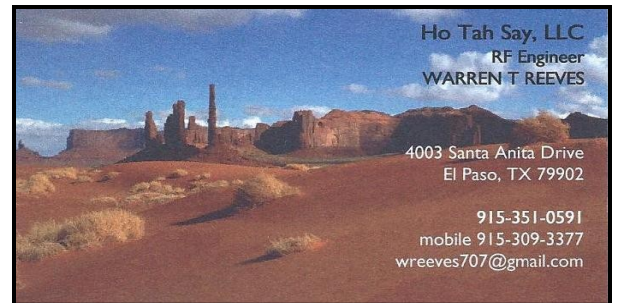
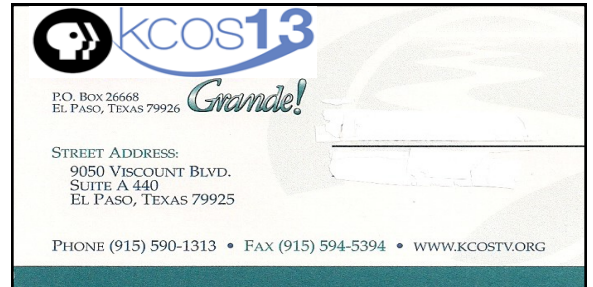
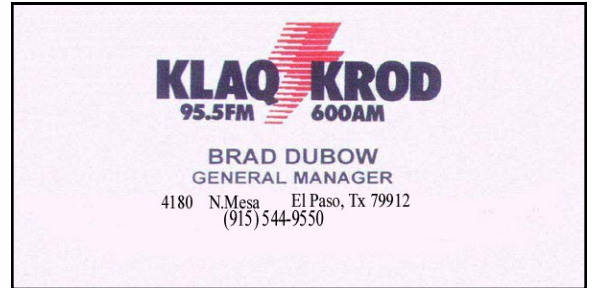
WHEN: JUNE 15 THURSDAY.

WHERE: KVIA TV PARKNG LOT.

TIME: 11 AM TO 2 PM.

PIZZA "ENGINEER", DRINKS AND TREATS WILL BE PROVIDED.

BUT BEFORE, REMEMBER THAT THE "**ENNES WORKSHOP**" WILL BE THIS WEEK. IF NOT REGISTERED, YOU CAN BE A WALK-IN. THIS IS AN EDUCATION EVENT SPONSORED PARTIALLY BY OUR CHAPTER. IT IS A MUST GO !!!



The FSB statement wasn't accompanied by any technical details of the described NSA spy campaign, or any evidence that Apple colluded in it.

Apple has historically resisted pressure to provide a “backdoor” or other vulnerability to US law enforcement or intelligence agencies. That stance was demonstrated most publicly in Apple's high-profile 2016 showdown with the FBI over the bureau's demand that Apple assist in the decryption of an iPhone used by San Bernadino mass shooter Syed Rizwan Farook. The standoff only ended when the FBI found its own method of accessing the iPhone's storage with the help of Australian cybersecurity firm Azimuth.

Despite its announcement coming on the same day as the FSB's claims, Kaspersky has so far made no claims that the Operation Triangulation hackers who targeted the company were working on behalf of the NSA. Nor has the cybersecurity firm attributed the hacking to the Equation Group, Kaspersky's name for the state-sponsored hackers it has previously tied to highly sophisticated malware, including Stuxnet and Duqu, tools widely believed to have been created and deployed by the NSA and US allies.

Kaspersky did say in a statement to WIRED that, “Given the sophistication of the cyberespionage campaign and the complexity of analysis of the iOS platform, further research will surely reveal more details on the matter.”

US intelligence agencies and US allies would, of course, have plenty of reason to want to look over Kaspersky's shoulder. Aside from years of warnings from the US government that Kaspersky has ties to the Russian government, the company's researchers have long demonstrated their willingness to track and expose hacking campaigns conducted by Western governments that Western cybersecurity firms don't. In 2015, in fact, Kaspersky revealed that its own network had been breached by hackers who used a variant of the Duqu malware, suggesting a link to the Equation Group—and thus potentially the NSA.

That history, combined with the sophistication of the malware that targeted Kaspersky, suggests that as wild as the FSB's claims may be, there's good reason to imagine that Kaspersky's intruders could have ties to a government. But if you hack one of the world's most prolific trackers of state-sponsored hackers—even with seamless, tough-to-detect iPhone malware—you can expect, sooner or later, to get caught.

BY LILY HAY NEWMAN AND ANDY GREENBERG

MEET THE NEW CHAPTER 38 MEMBER: IAN PETER LEWIS

Member number:# 35685

Chapter: El Paso (38)

Member Since: December 8, 2012

Contact Information

PO Box 404
Marfa, TX 79843 USA

Primary Phone: (781) 987-4206

E-mail: ianpeterlewis@gmail.com

Here is a short bio: Born in Massachusetts, I have been living in Marfa since 2014. I'm a filmmaker and radio producer, but got into the technical side of broadcast radio in 2016 and became the engineer at Marfa Public Radio. I now work with fellow Chapter #38 member Will Floyd, providing servicing and consultation for radio stations with our company Field Effect. I play pickup soccer wherever I can and support Liverpool FC.