A Spyware Vendor Seemingly Made a Fake WhatsApp to Hack Targets

vice.com/en/article/akdqwa/a-spyware-vendor-seemingly-made-a-fake-whatsapp-to-hack-targets

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

See More →

Hackers tried to trick iPhone users into installing a fake version of WhatsApp in a potential attempt to gather information about them. Technical analyses by both researchers from digital rights watchdog Citizen Lab and Motherboard suggest that this fake version of WhatsApp is linked to a specific Italian surveillance company.

The news highlights a sometimes overlooked attack on iPhones: tricking users into installing configuration files or so-called Mobile Device Management (MDM) profiles, which can then potentially push malware onto a target device. As the price of exploits for breaking into iPhones has steadily climbed, other government malware vendors have moved to leveraging MDM profiles to hack phones.

“I think it is targeted, I don’t think they were trying to spread this around,” Bill Marczak, a researcher from Citizen Lab, part of the Munk School of Global Affairs at the University of Toronto, told Motherboard.

Last Tuesday, the security company ZecOps said in a tweet that it had detected attacks against WhatsApp users. The company published a specific domain—config5-dati[.]com—and an IP address it said were related to the attacks. Then Marczak and fellow Citizen Lab researcher Bahr Abdul Razzak looked into the domain and found others linked to it, including one that hosted a site that purported to be a page to download WhatsApp. In reality, the site attempted to trick visitors into installing what was actually a special configuration file for iPhones designed to potentially gather information about the victims and send it back to the attacker, according to the Citizen Lab researchers.

Using data from cybersecurity vendors DomainTools and RiskIQ, Motherboard independently discovered multiple clusters of domains linked to the one publicly shared. The config5-dati[.]com domain shared an encryption certificate with other similarly named domains, revealing others such as config4-dati[.]com, config3-dati[.]com, and config6-dati[.]com. Citizen Lab searched for other numerical variations of that domain, including config1-dati[.]com; Google had preserved a cache of the WhatsApp phishing page on that domain.

A screenshot of the phishing page found by Citizen Lab. (Image: Citizen Lab)

"To keep in touch with your friends press the 'download' button and follow the instructions on the page," the phishing site reads in Italian. The page then instructs visitors how to install a configuration file via the iPhone's system settings menu. This is not how users install a legitimate version of WhatsApp: usually iPhone users download it from the Apple App Store.

Marczak said this file sends information to the config1-dati server, including the UDID, or Unique Device Identifier assigned to each iOS device by Apple; and the IMEI or International Mobile Equipment Identity, another unique code that identifies cellphones.

"[The MDM file is] the first bit of the installation process for what is ultimately likely to be a fake WhatsApp app containing spyware," Marczak said.

Citizen Lab researchers said they could not gather data on the next stage of the attack, meaning it is unclear exactly what other data the hackers would have been able to exfiltrate from a target device.

The phishing page is designed to look like an official WhatsApp site, with WhatsApp branding and professional graphics laying out the installation process step-by-step. The phishing page is not currently online. Citizen Lab shared a copy of the configuration file with Motherboard; when opened, the file says it is from "WhatsApp Inc." for "WhatsApp Messenger."

When presented with a summary of the findings, a WhatsApp spokesperson told Motherboard "We do not ask for these user privileges and people should be very suspicious of any app trying to do so."

"To help keep chats safe, we recommend that people download WhatsApp from the app store for their phone's platform. In addition, we may temporarily ban people using modified WhatsApp clients we detect to help encourage people to download WhatsApp from an authoritative source," the spokesperson added.

"We strongly oppose abuse from spyware companies, regardless of their clientele. Modifying WhatsApp to harm others violates our terms of service. We have and will continue to take action against such abuse, including in court," the WhatsApp spokesperson said. Facebook and WhatsApp are currently suing another spyware vendor, NSO Group, for allegedly abusing WhatsApp's infrastructure to deliver NSO's malware to targets.

Motherboard was unable to determine who the fake WhatsApp page was targeting.

Apple did not provide a statement.

> ***Do you have information about similar attacks? We'd love to hear from you. You can contact Lorenzo Franceschi-Bicchierai securely on Signal at* +1 917 257 1382*, Wire/Wickr @lorenzofb, or email* lorenzofb@vice.com*. You can contact Joseph Cox on Signal on* +44 20 8133 5190*, Wickr on josephcox, or email*** joseph.cox@vice.com

After researching the set of domains, Motherboard found a cluster of other domains that at one point shared an IP address with the config5-dati[.]com domain, and from there a third set that shared an IP address and followed similar naming conventions. One of these, check3[.]it, was registered to "cy4gate srl", a company with a Rome, Italy address, according to WHOIS records. Most of the domains analyzed were registered in Rome according to the WHOIS records.

Cy4Gate describes itself as a **"**Cyber Electronic Warfare & Intelligence" company on its Twitter account. The company develops several products, including Epeius, its solution for "lawful intercept," an industry term for hacking and surveillance as a service. In 2017, Cy4gate appeared before an Italian Senate committee to pitch its surveillance products, according to a document published online. Last year, it made headlines for developing a

product to track COVID-19 infections, which was part of a series of COVID-tracking solutions considered at the time by the Italian government, which eventually gave the bid to another company. Cy4gate is part of the Italian defense contractor Elettronica.

Cy4Gate has recently done business with high profile companies such as Fiat Chrysler as well as the United Arab Emirates, according to marketing material Motherboard found online. An Italian media report says Cy4Gate has also sold a product to the U.S. military, although it specifies it was not the company's Epeius product. Cy4Gate also offers cybersecurity products.

A screenshot of the login portal found by Citizen Lab. (Image: Citizen Lab)

Citizen Lab also found that an encryption certificate for an IP address associated with the config1-dati[.]com domain, which displayed the WhatsApp phishing page, mentioned "epeius," Cy4Gate's lawful intercept product. Motherboard found mentions of Epeius in certificates connected to IP addresses pointing to more of the config domains too.

The Citizen Lab researchers also found that the config1-dati[.]com domain at some point returned a login page with a Cy4gate logo and the name Epeius, and shared a screenshot of the portal with Motherboard. The branding matches that of a Epeius logo Motherboard found in Cy4Gate marketing material online.

A screenshot of the Epeius marketing material found by Motherboard. (Image: Motherboard)

"EPEIUS has been designed to address the LEAs (Law Enforcement Agencies) requirements to move from the 'cloud' of IP data flow to a targeted active interception approach directly on the target's endpoint like a Mobile phone, a Tablet or a personal computer," the brochure Motherboard found reads. The marketing material adds that "EPEIUS implements a number of innovative techniques to 'infect' a device," and that the product is designed to be configurable depending on the client's mission requirements.

"Example: if our task is the acquisition of target geolocalization and emails, EPEIUS will execute the pre-established modules," the brochure adds. The material adds that EPEIUS is designed to siphon data before it is encrypted and that data collection "is implemented through anonymous and untraceable connections." Cy4Gate took the Epeius product to market in 2019, according to the brochure.

When Motherboard shared the domain data with Cy4gate, a company spokesperson said in an email that the config domains identified by Citizen Lab researchers and Motherboard are not attributable to the company. The Cy4Gate spokesperson did confirm to Motherboard that the check3[.]it domain belonged to the company.

"I think it's pretty clearly their product," Marczak said.

Subscribe to our cybersecurity podcast CYBER, here.