The Washington Post
Democracy Dies in Darkness

TECH POLICY

Mysterious company with government ties plays key internet role

TrustCor Systems vouches for the legitimacy of websites. But its physical address is a UPS Store in Toronto.

By Joseph Menn

Updated November 8, 2022 at 5:37 p.m. EST | Published November 8, 2022 at 6:00 a.m. EST

An offshore company that is trusted by the major web browsers and other tech companies to vouch for the legitimacy of websites has connections to contractors for U.S. intelligence agencies and law enforcement, according to security researchers, documents and interviews.

Google's Chrome, Apple's Safari, nonprofit Firefox and others allow the company, TrustCor Systems, to act as what's known as a root certificate authority, a powerful spot in the internet's infrastructure that guarantees websites are not fake, guiding users to them seamlessly.

The company's Panamanian registration records show that it has the identical slate of officers, agents and partners as a spyware maker identified this year as an affiliate of Arizona-based Packet Forensics, which public contracting records and company documents show has sold communication interception services to U.S. government agencies for more than a decade.

One of those TrustCor partners has the same name as a holding company managed by Raymond Saulino, who was quoted in a 2010 Wired article as a spokesman for Packet Forensics.

Saulino also surfaced in 2021 as a contact for another company, Global Resource Systems, that caused speculation in the tech world when it briefly activated and ran more than 100 million previously dormant IP addresses assigned decades earlier to the Pentagon. The Pentagon reclaimed the digital territory months later, and it remains unclear what the brief transfer was about, but researchers said the activation of those IP addresses could have given the military access to a huge amount of internet traffic without revealing that the government was receiving it.

The Pentagon did not respond to a request for comment on TrustCor. After this story's publication, a TrustCor executive said the company had not cooperated with any government information requests or assisted with a third party's monitoring of its customers on behalf of others. Mozilla demanded more detailed answers and said it might remove TrustCor's authority.

TrustCor's products include an email service that claims to be end-to-end encrypted, though experts consulted by The Washington Post said they found evidence to undermine that claim. A test version of the email service also included spyware developed by a Panamanian company related to Packet Forensics, researchers said. Google later banned all software containing that spyware code from its app store.

A person familiar with Packet Forensics' work confirmed that it had used TrustCor's certificate process and its email service, MsgSafe, to intercept communications and help the U.S. government catch suspected terrorists.

"Yes, Packet Forensics does that," the person said, speaking on the condition of anonymity to discuss confidential practices.

Packet Forensics counsel Kathryn Tremel said the company has no business relationship with TrustCor. She declined to say whether it had had one previously.

The latest discovery shows how the technological and business complexities of the internet's inner workings can be leveraged to an extent that is rarely revealed.

Concerns about root certificate authorities, though, have come up before.

In 2019, a security company controlled by the government of the United Arab Emirates that had been known as DarkMatter applied to be upgraded to top-level root authority from intermediate authority with less independence. That followed revelations about DarkMatter hacking dissidents and even some Americans; Mozilla denied it root power.

In 2015, Google withdrew the root authority of the China Internet Network Information Center (CNNIC) after it allowed an intermediate authority to issue fake certificates for Google sites.

With Packet Forensics, a paper trail led to it being identified by researchers twice this year. Mostly known for selling interception devices and tracking services to authorities, the company is four months into a $4.6 million Pentagon contract for "data processing, hosting and related services."

In the earlier spyware matter, researchers Joel Reardon of the University of Calgary and Serge Egelman of the University of California at Berkeley found that a Panamanian company, Measurement Systems, had been paying developers to include code in a variety of innocuous apps to record and transmit users' phone numbers, email addresses and exact locations. They estimated that those apps were downloaded more than 60 million times, including 10 million downloads of Muslim prayer apps.

Measurement Systems' website was registered by Vostrom Holdings, according to historic domain name records. Vostrom filed papers in 2007 to do business as Packet Forensics, according to Virginia state records. Measurement Systems was registered in Virginia by Saulino, according to another state filing.

After the researchers shared their findings, Google booted all apps with the spy code out of its Play app store.

Tremel said that "a company previously associated with Packet Forensics was a customer of Measurement Systems at one time" but that there was no ownership stake.

When Reardon and Egelman looked deeper at Vostrom, they found it had registered the domain name TrustCor.co, which directed visitors to the main TrustCor site. TrustCor has the same president, agents and holding-company partners listed in Panamanian records as Measurement Systems.

A firm with the same name as one of the holding companies behind both TrustCor and Measurement Systems, Frigate Bay Holdings, filed papers to dissolve this March with the secretary of state in Wyoming, where it was formed. The papers were signed by Saulino, who listed his title as manager. He could not be reached for comment.

TrustCor has issued more than 10,000 certificates, many of them for sites hosted with a dynamic domain name service provider called No-IP, the researchers said. That service allows websites to be hosted with constantly changing Internet Protocol addresses.

Because root authority is so powerful, TrustCor can also give others the right to issue certificates.

Certificates for websites are publicly viewable so that bad ones should be exposed sooner or later. There have been no reports so far that the TrustCor certificates have been used inappropriately, for example by vouching for impostor websites. The researchers speculated that the system is only used against high-value targets within short windows of time. The person familiar with Packet Forensics' operations agreed said that was in fact how it has been used.

"They have this position of ultimate trust, where they can issue encryption keys for any arbitrary website and any email address," Egelman said. "It's scary this is being done by some shady private company."

The leadership page of the TrustCor's website lists just two men, identified as co-founders. Though that page does not say so, one of them died months ago, and the other's LinkedIn profile says he left as chief technology officer in 2019. That man declined to comment.

The website site lists a contact phone number in Panama, which has been disconnected, and one in Toronto, where a message had not been returned after more than a week. The email contact form on the site doesn't work. The physical address in Toronto given in its auditor's report, 371 Front St. West, houses a UPS Store mail drop.

TrustCor adds another layer of mystery with its outside auditing firm. Instead of using a major accounting firm that rates the safety of internet infrastructure companies, TrustCor selected one called Princeton Audit Group, which gives its address as a residential townhouse in Princeton, N.J.

In its comments Tuesday to an email list for Mozilla developers, TrustCor executive Rachel McPherson said that her company had been the victim of complex attacks that involved the registration of companies with names similar to those of its shareholders, perhaps to help set up some sort of phishing attack. She said she would research why some of the people were listed as officers.

In addition to TrustCor's certificate power, the firm offers what purports to be end-to-end encrypted email, MsgSafe.io. But researchers said the email is not encrypted and can be read by the company, which has pitched it to a variety of groups worried about surveillance.

MsgSafe has touted its security to a variety of potential customers, including Trump supporters upset that Parler had been dropped by app stores in January 2021, and to users of encrypted mail service Tutanota who were blocked from signing on to Microsoft services.

"Create your free end-to-end encrypted email today with over 40 domains to choose from and are guaranteed to work with Microsoft Teams," the company tweeted in August.

Reardon sent test messages over MsgSafe that appeared unencrypted in transmission, meaning MsgSafe could read them at will. Egelman ran the same test with the same result.

Jon Callas, a cryptography expert at the Electronic Frontier Foundation, also tested the system at The Post's request and said that MsgSafe generated and kept the private key for his account, so that it could decrypt anything he sent.

"The private key has to be under the person's control to be end-to-end," Callas explained.

Packet Forensics first drew attention from privacy advocates a dozen years ago.

In 2010, researcher Chris Soghoian attended an invite-only industry conference nicknamed the Wiretapper's Ball and obtained a Packet Forensics brochure aimed at law enforcement and intelligence agency customers.

The brochure was for a piece of hardware to help buyers read web traffic that parties thought was secure. But it wasn't.

"IP communication dictates the need to examine encrypted traffic at will," the brochure read, according to a report in Wired that quoted Saulino as a Packet Forensics spokesman. "Your investigative staff will collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VOIP encryption," the brochure added.

The brochure told customers they could use a decryption key provided by a court order or a "look-alike key."

Researchers thought at the time that the most likely way the box was being used was with a certificate issued by an authority for money or under a court order that would guarantee the authenticity of an impostor communications site.

They did not conclude that an entire certificate authority itself might be compromised.

Obtaining trusted root certificate authority takes time and money for the infrastructure and for the audit that browsers require, experts say.

Each browser has slightly different requirements. At Mozilla's Firefox, the process takes two years and includes crowdsourced and direct vetting as well as an audit.

But all of that typically focuses on formal statements of technological steps, rather than mysteries of ownership and intent. The person familiar with Packet Forensics said the big tech companies probably were unwitting participants in the TrustCor play: "Most people aren't paying attention."

"With enough money, you or I could become a trusted root certificate authority," said Daniel Schwalbe, vice president of technology at web data tracker DomainTools.

Mozilla currently recognizes 169 root certificate authorities, including three from TrustCor.

The case gives new focus to problems with that system, in which critical tech companies outsource their trust to third parties with their own agendas.

"You can't bootstrap trust, it has to come from somewhere," Reardon said. "Root certificate authorities are the kernel of trust from which it is all built on. And it will always be shaky, because it will always involve humans, committees and decision-making."

Reardon and Egelman alerted Google, Mozilla and Apple to their research on TrustCor in April. They said they had heard little back until Tuesday.

After publication of this story, Mozilla gave TrustCor two weeks to respond to a series of questions, including about its relationships with Measurement Systems and Packet Forensics, the shared officers, and how the banned spyware code from Measurement Systems got into an early MsgSafe app.