GOVERNMENT

New tool can help prevent government-mandated backdoors in software, Swiss researchers say

The framework, dubbed "Chainiac," makes it extremely difficult for governments to force vulnerabilities into the software supply chain.

BY J.M PORUP • JULY 25, 2017

By: qimono -- via CC0

A new framework from a lab in Switzerland could help prevent malware like Petya from spreading, but would also make it difficult — if not impossible — for governments to force software companies to deliver backdoored software updates in secret.

The Petya ransomware, and its wiperware variant NotPetya, spread on the wings of a software update unwittingly issued by Ukrainian accounting software company M.E. Doc. An attacker, who many believe to be agents of the Russian government, owned M.E. Doc's network and injected malicious code into a legitimate software update.

This new proof-of-concept technology, dubbed "Chainiac" by the Decentralized/Distributed Systems (DEDIS) lab at the Swiss Federal Institute of Technology in Lausanne (EPFL), offers a decentralized framework that eliminates such single points of failure and enforces transparency, making it possible for security analysts to continuously review updates for potential vulnerabilities.

"What Chainiac is trying to do," Bryan Ford, leader of the group that conducted the research, told CyberScoop, "is create an end-to-end architecture for software life cycle management, all the way from the developers to deployment and updates on end-user devices."

As criminals and nation-states attack the software supply chain, it becomes increasingly important to ensure the integrity of the software used by the public.

Documents released by NSA whistleblower Edward Snowden revealed that as early as 2011, the NSA was looking at how to compromise the Google Play Store (then called the "Android Store") in order to replace legitimate smartphone apps with backdoored versions to spy on users or even manipulate them with targeted propaganda.

In the U.K., the government may now legally compel software makers to backdoor their code using secret court orders, as part of the Investigatory Powers Act, which came into force in January of this year. Other nations around the world are engaged in similar practices.

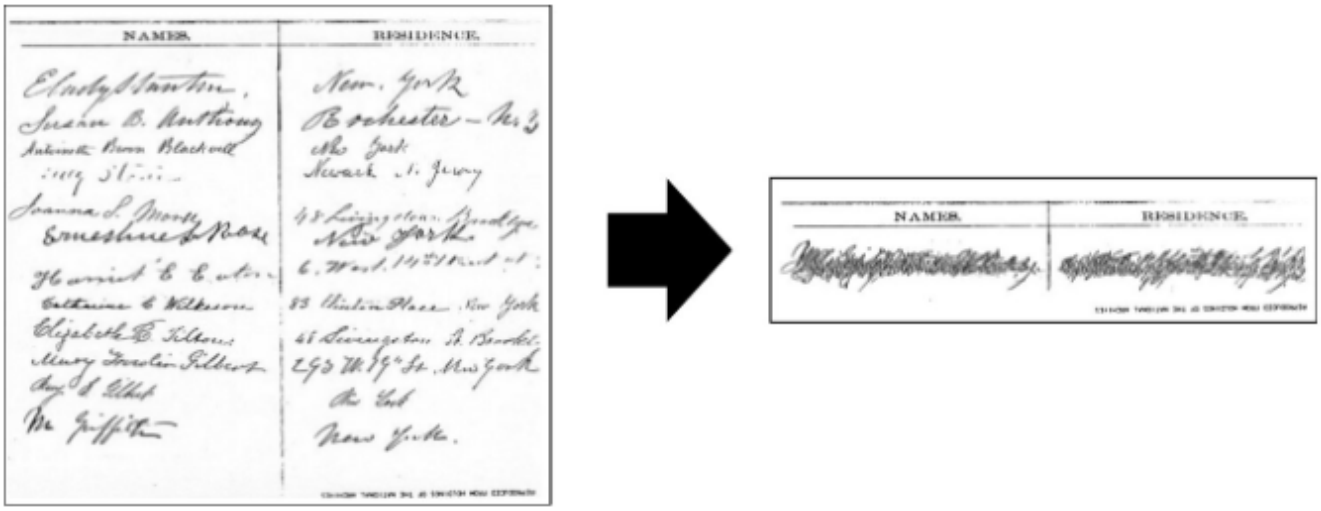
"How do we know what software we are really running?" Emin Gün Sirer, associate professor at Cornell University and co-director of the Initiative for Cryptocurrencies and Smart Contracts, told CyberScoop. "A lot of attacks go after that exact foundation. Someone switches the binaries you're using but everything appears to be the same."

"How do we know what software we are really running?"

Chainiac builds on Cothority, a transparency tool Ford's team released after the 2015 San Bernardino shooting that enables collective signing of software updates by independent

witnesses.

Collective signing means that each time Apple, for example, released a new iOS update — for all users, for a targeted individual or for a group, perhaps as the result of a secret court order — the iOS device would not accept the update unless the code had been collectively signed by a threshold number of thousands of trusted witnesses attesting publicly that an update had been issued.



What an old-fashioned multi-signature would look like in Chainiac/Cothority

A collectively-signed software update might still contain backdoored code — developers could be bribed, blackmailed, or threatened to insert a backdoor — but Cothority, a component of Chainiac, would make it impossible to ship the update in secret.

Chainiac also integrates reproducible builds, a system which lets technical end users, or automated witness servers, to recompile the source code and get a byte-for-byte identical binary, ensuring the distributed binaries have not been tampered with.

“The essence of the idea is that [Chainiac] allows users, who just want the latest binary, to check this one collective signature,” Ford said, “and see that this signature shows that this group of Cothority servers has independently reproduced this binary, and tested that this is the one and only correct output corresponding to the source code that the developer has produced.”

The Debian Project has already deployed reproducible builds for 94 percent of the tens of thousands of software packages that make up that Linux distribution, which is widely used on cloud servers and embedded devices, plus its downstream variant Ubuntu. Ford’s team tested Chainiac on Debian packages with good results, and Debian seems likely to be an early adopter of the transparency tool.

Proprietary software, such as Apple's iOS or Microsoft's Windows, could also use Chainiac to achieve similar levels of transparency, Ford emphasized. "In that case the Cothority nodes responsible for checking the reproducible builds need to be run by … organizations that have NDAs with the software provider giving them access to the source code for this purpose."

"That makes it at least in principle feasible for proprietary software," he added.

The project also incorporates a novel form of blockchain technology, called a "skipchain." Software updates are announced on a distributed ledger.

"Blockchains are used to transfer things, but that's not their only use," Sirer said. "They're great for transferring things like Bitcoin, but they're also great for announcing facts. … [Chainiac] is a broadcast medium for vetting software updates."

Ford's research seems unlikely to please government leaders frustrated at the growing use of encryption, including the prime minister of Australia, Malcolm Turnbull, whose recent comments that the laws of Australia trump the laws of mathematics were widely mocked within the technical community.

Chainiac is the latest salvo in an increasingly bitter war between software makers and governments for control of the code on which our lives depend. Nation-states wanting to subvert the software development process for law enforcement or espionage purposes will look for ways to counter transparency mechanisms like Chainiac, sources speculated.

"We've seen sovereign states put enormous resources into hacking," Sirer said. "Will [Chainiac] be open to gaming? Will it be more secure or open to attack?… There is every reason for hope and every reason for experimentation."

Cryptographers have been vocal against government use of backdoored software updates, arguing that destroying trust in software updates makes everyone less safe. A few weeks ago cryptographer Matthew Green of Johns Hopkins University blasted the practice on Twitter.

Security expert Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University, said it is never acceptable for governments to use backdoored software updates.

"It is akin to a public health issue," he told CyberScoop in an email. "We need everyone to trust the update process implicitly — that it will always work in the best interests of the user."

"Hijacking that process for surveillance purposes," he added, "threatens to undermine trust in one of the critical security technologies we need."

Written by J.M Porup

J.M Porup J.M Porup j-m-porup 50627
jmporup@scoopnewsgroup.com

In This Story

FEDERAL IT SURVEILLANCE ENCRYPTION

NATIONAL SECURITY AGENCY (NSA) INTELLIGENCE COMMUNITY (IC)