TORONTO STAR

ENTERTAINMENT

Cicada 3301, cryptography and the quest for anonymity

By Kim Nursall Staff Reporter
Fri., Jan. 3, 2014 | 6 min. read

Everyone except you is Cicada.

The motto (or warning) is one of many listed at the top of an Internet chat room. Here, dozens of cryptographers and code-breakers gather, waiting — scanning — wondering: will Cicada 3301 post again?

Cicada 3301 — also known as "the Internet mystery that has the world baffled" following a widely shared Telegraph article — has ensnared cryptic puzzle enthusiasts ever since its first public challenge in early January 2012.

"Hello, we are looking for highly intelligent individuals," began the original Cicada message, written in white text on a black background and posted on the anarchic bulletin board 4chan.

"To find them, we have devised a test. There is a message hidden in this image. Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through. Good luck."

It was signed 3301.

Since then, two Cicada recruitment sessions (a second began a year later, on Jan. 5, 2013) have included hidden messages, a seemingly random Twitter feed, audio files, the notorious "darknet" and GPS co-ordinates that led players to actual physical clues, from Seoul, South Korea, to Annapolis, Maryland, in the U.S. Both sessions ended unceremoniously, with no public acknowledgement of "winners." Beyond a leaked Cicada email from 2012, there remains no consensus as to just how far down the rabbit hole goes.

Although at first Cicada was an obscure Internet-based challenge, thanks to a flurry of media coverage it has since captured the public imagination. Dan Brown comparisons abound and people who can't figure out their Facebook privacy settings are suddenly pondering a cryptographic entity's origin. The name Cicada 3301 is thought to refer to the importance of prime numbers in cryptography. 3301 is a prime and the cicada insect (whose image became a common motif) has a life cycle based on primes.

Cicada highlights how little most people know about the Internet and the concept of anonymity, and touches on growing fears that no personal information is safe from prying governments and corporations. Calls for widespread email encryption and increased electronic security are making cryptography a household topic, as theories about Cicada's raison d'être flourish.

Is it the NSA recruiting elite data-gatherers? Is it a left-hand path religion seeking followers? Is it a global, decentralized think tank finding members who will help end censorship and establish privacy as an inalienable right? Or is it just a group of "neckbeards" (slang for overly dedicated computer nerds)?

Does anyone outside Cicada know the truth?

"Those who know don't tell," warns a common 3301 refrain. "Those who tell don't know."

Everyone except you is Cicada.

The art behind the game

Cicada's initial post in 2012 was a relatively easy cryptographic puzzle. By opening the image in a text editor, clue hunters were able to locate a distinct phrase: TIBERIVS CLAVDIVS CAESAR says "lxxt>33m2mqkyv2gsq3q=w]O2ntk."

To most people, gibberish. But for the average cryptographer, it was an obvious reference to one of the field's original tools: the Caesar cipher.

Named after Julius Caesar, who used it to conceal communication with his generals, it requires substituting each letter in a message with another letter in the alphabet. For example, a Caesar cipher with a rightward shift by three letters would turn the word "bee" into "ehh."

For the Cicada puzzle, players discerned they should shift the encrypted text by four letters, since Tiberius was the fourth Roman emperor. Doing so revealed an URL: http://i.imgur.com/m9sYK.jpg.

That URL became the start of an epic journey, which tested players on subjects as varied as Mayan numerology and cypherpunk literature, but always came back to its cryptographic roots: delivering a message only to those intended to receive it (in this case, those smart enough to crack the code).

Cryptography is "making information visible but unreadable to an adversary," said Torontonian Jairus Pryor, a 34-year-old web communications expert who has participated in both Cicada rounds.

Pryor's first run-in with a cryptographic adversary was as a 16-year-old, when he managed an online bulletin board system.

"I was just in my room reading (when I saw) someone logged in and tried to crack the administrative password," he said.

"I spent five minutes just totally panicked at my keyboard trying to change the passwords faster than he could crack them, before I realized I could just unplug the computer," he continued, laughing. "After that, I became the guy that other people who ran bulletin board systems, they would come to me when they got hacked. I became the de facto security guy."

Although it's easy to think of cryptography as a *Da Vinci Code* plot device, Charles Rackoff, a University of Toronto computer science professor, said modern encryption is largely algorithmic.

"I know when I was young and we bought cereal it would come with decoder rings," he told the Star. "Secret codes, languages, hand signals: there's always been that kind of thing (with cryptography).

"Starting in the late '70s, it became very different from what happened before then, because you don't need special, handcrafted devices for cryptography. What cryptographers do is they have general algorithms which are formed on an arbitrary computer. And we assume adversaries also have very powerful computer systems."

"To me, it doesn't really have that mystique. It's just deep questions about algorithms."

Crisis in cryptography

At the core of the Cicada community, you find people who try their best to live anonymously online. Many only spoke to the Star on chat rooms, while others required email communication to be encrypted and wouldn't use the phone.

But at the end of a year that included snowballing revelations about the extent of government and corporate surveillance, the cryptographic community is facing a crisis of confidence.

"When the NSA stuff all came out, the big response in the community was: oh s---, here it is. This is what we've been waiting for and it's so much worse than we expected," said a 25-year-old computer science student from Alberta who agreed to speak under the username Noxpopuli.

(Nox participated in Cicada last year and said he made it all the way to the end; he wouldn't say exactly what that meant though. "Those who know don't tell.")

"You see a lot of the big names in (the field) talking about how cryptography is dead," Nox said, adding Julian Assange recently argued this may be the last free generation, information wise, unless a drastic solution emerges.

Rackoff said that, outside of a few exceptions with limited cryptographic capability, "We don't know of anything that's actually, provably secure."

"It's very possible that tomorrow, someone will come along and break all existing cryptography," he said.

Contrast this with the fact that more and more people are now interested in encryption, in light of NSA and other government leaks.

"When I first started messing around with (email encryption), even a year or two ago, the average person would be like 'What the heck are you talking about?'" said Nox.

"Now name a major news organization and they've probably put out an article about how to encrypt your email. . . . Suddenly it's common household talk, which absolutely would have never happened a year or two ago," he said.

Cicada 3301, 2014

Perhaps it's because Cicada's purpose and origin have managed to remain secret, in a world where nothing seems secure and everything is accessible, that the cryptographic community is kept enthralled.

Now, 364 days after the launch of the 2013 challenge, thousands of clue hunters have gathered on various Internet forums, waiting for a sign, seeking the unknown. Many believe mainstream awareness about Cicada, whose very nature is anti-publicity, means it won't be back.

But that doesn't stop them from looking.

Everyone except you is Cicada.

Read more about: Edward Snowden

More from The Star & Partners