KIM ZETTER SECURITY 01.28.16 9:23 AM

NSA HACKER CHIEF EXPLAINS HOW TO KEEP HIM OUT OF YOUR SYSTEM

IT WAS THE talk most anticipated at this year's inaugural Usenix Enigma security conference in San Francisco and one that even the other speakers were eager to hear.

Rob Joyce, the nation's hacker-in-chief, took up the ironic task of telling a roomful of computer security professionals and academics how to keep people like him and his elite corps out of their systems.

Rob Joyce, chief of the NSA's Tailored Access Operations (TAO). KIM ZETTER

Joyce is head of the NSA's Tailored Access Operations—the government's top hacking team who are responsible for breaking into the systems of its foreign adversaries, and occasionally its allies. He's been with the NSA for more than 25 years but only became head of the TAO division in April 2013, just weeks before the first leaks from Edward Snowden were published by the *Guardian* and *Washington Post*.

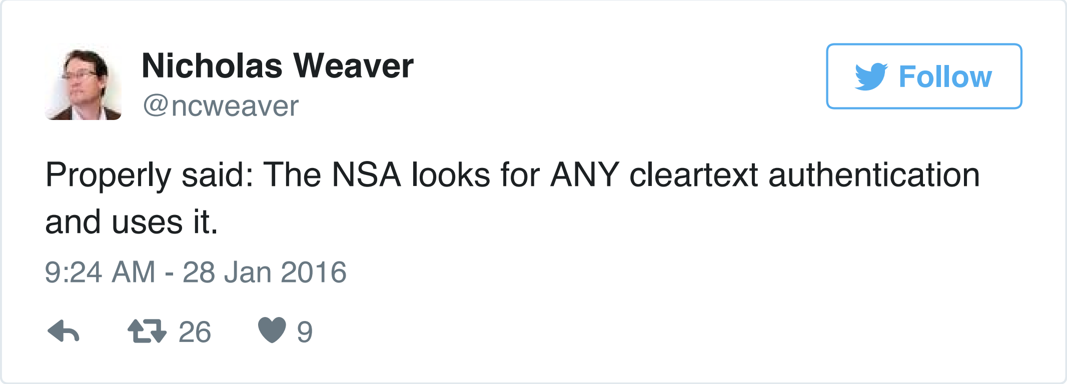
Joyce acknowledged that it was "very strange" for someone in his position to stand onstage before an audience. The TAO has largely existed in the shadowy recesses of the NSA—known and unknown at the same time—until only recently when documents leaked by Snowden and others exposed the workings of this cabal as well as many of its sophisticated hacking tools.

Joyce himself did little to shine a light on the TAO's classified operations. His talk was mostly a compendium of best security practices. But he did drop a few of the not-so-secret secrets of the NSA's success, with many people responding to his comments on Twitter.

How the NSA Gets You

In the world of advanced persistent threat actors (APT) like the NSA, credentials are king for gaining access to systems. Not the login credentials of your organization's VIPs, but the credentials of network administrators and others with high levels of network access and privileges that can open the kingdom to intruders. Per the words of a recently leaked NSA document, the NSA hunts sysadmins.

The NSA is also keen to find any hardcoded passwords in software or passwords that are transmitted in the clear—especially by old, legacy protocols—that can help them move laterally through a network once inside.



Nicholas Weaver
@ncweaver

Properly said: The NSA looks for ANY cleartext authentication and uses it.

9:24 AM - 28 Jan 2016

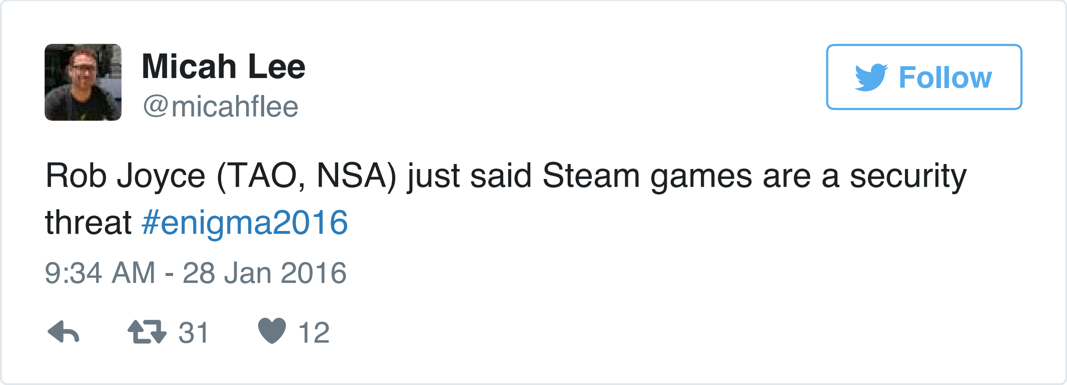
And no vulnerability is too insignificant for the NSA to exploit.

"Don't assume a crack is too small to be noticed, or too small to be exploited," he said. If you do a penetration test of your network and 97 things pass the test but three esoteric things fail, don't think they don't matter. Those are the ones the NSA, and other nation-state attackers will seize on, he explained. “We need that first crack, that first seam. And we’re going to look and look and look for that esoteric kind of edge case to break open and crack in.”

Even temporary cracks—vulnerabilities that exist on a system for mere hours or days—are sweet spots for the NSA.

If you’ve got trouble with an appliance on your network, for example, and the vendor tells you to briefly open the network for them over the weekend so they can pop in remotely and fix it, don’t do it. Nation-state attackers are just looking for an opportunity like this, however brief, and will poke and poke your network patiently waiting for one to appear, he said.

Other vulnerabilities that are favorite attack vectors? The personal devices employees bring into the office on which they’ve allowed their kids to load Steam games, and which the workers then connect to the network.



Micah Lee
@micahflee

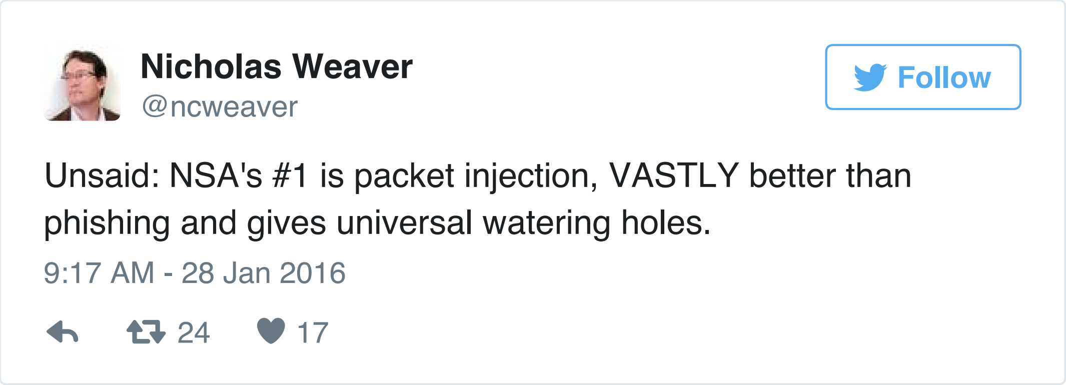
Rob Joyce (TAO, NSA) just said Steam games are a security threat #enigma2016

9:34 AM - 28 Jan 2016

31 12

The heating and cooling systems and other elements of building infrastructure also provide unexpected pathways into your network. Retail giant Target, of course, is very familiar with how a company’s HVAC system can be a gateway for attackers.

Left unsaid were a lot of the other nifty ways the NSA gets into systems, such as its Quantum insert code injection technique, which allowed it and the British spy agency GCHQ to hack the Belgium telecom Belgacom.



Nicholas Weaver
@ncweaver

Unsaid: NSA's #1 is packet injection, VASTLY better than phishing and gives universal watering holes.

9:17 AM - 28 Jan 2016

In general, Joyce noted, spies have little trouble getting into your network because they know better than you what's on it.

"We put the time in ...to know [that network] better than the people who designed it and the people who are securing it," he said. "You know the technologies you intended to use in that network. We know the technologies that are actually in use in that network. Subtle difference. You'd be surprised about the things that are running on a network vs. the things that you think are supposed to be there."

How to Keep the NSA Out

If you really want to make the NSA's life hard, he ticked off a list of things to do: limit access privileges for important systems to those who really need them; segment networks and important data to make it harder for hackers to reach your jewels; patch systems and implement application whitelisting; remove hardcoded passwords and legacy protocols that transmit passwords in the clear.

Another nightmare for the NSA? An "out-of-band network tap"—a device that monitors network activity and produces logs that can record anomalous activity—plus a smart system administrator who actually reads the logs and pays attention to what they say.

Jonathan Zdziarski
@JZdziarski

“One of the NSA’s worst nightmares is a sysadmin who pays attention.” Rob Joyce, NSA TAO #enigma2016

9:42 AM - 28 Jan 2016

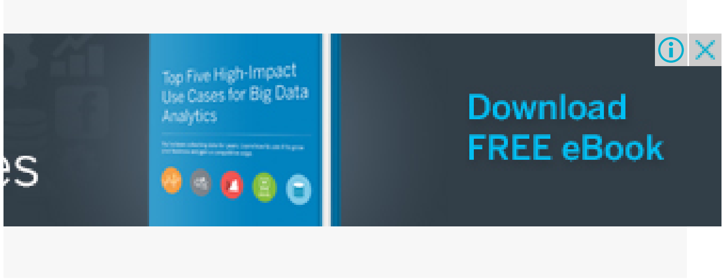
Contrary to popular opinion, he says the NSA and other APT attackers don’t rely on zero-day exploits extensively—unique attacks that take advantage of previously unknown software holes to get into systems. That’s because they don’t have to.

“[With] any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days,” he says. “There’s so many more vectors that are easier, less risky and quite often more productive than going down that route.” This includes, of course, known vulnerabilities for which a patch is available but the owner hasn’t installed it.

Trust the NSA

Following his talk, Juan Guerrero, an analyst with Kaspersky Lab's Global Research and Analysis Team, asked about the issue of attribution and efforts by some attack groups to manipulate and alter indicators of compromise to thwart attribution or point the finger at someone else.

"It's amazing the amount of lawyers that DHS, FBI and NSA have," Joyce said. "So if the government is saying that we have positive attribution too, you ought to book it. Attribution is really really hard, so when the government's saying it, we're using the totality of the sources and methods we have to help inform that. [But] because those advanced persistent threats aren't going away, … we can't bring all that information to the fore and be fully transparent about everything we know and how we know it."



Nicholas Weaver, a senior researcher at the International Computer Science Institute at UC Berkeley, asked a question in reference to recent news about the NSA engaging in actions that undermine the security of US systems—actions that are directly at odds with the spy agency's other mission to help defend and protect US government systems.

"After this kind of activity, how do you guys hope to regain trust?" Weaver asked.

"Over time there will be that interaction and that ability," Joyce replied. "NSA does a lot with industry, does a lot with standards, works with industry. I think we'll build that trust back up. But I can absolutely tell you, in the NSA world defense wins. I continually interact with both the Information Assurance Directorate and our director and the defensive community of the US, and absolutely hands-down, defense wins in this space."

He ended his talk with a slide showing a huge QR code, which got a laugh.

"Anybody holding up a camera?" Joyce asked. "Who's gonna [photograph] the QR code from the NSA guy?"

QR codes are one way hackers attack systems by sending their browser to a malicious web site where malware is downloaded to it. Joyce, however, said his QR code was on the up-and-up and would take visitors to a legitimate NSA web site for more information. "[T]hat is a real link," he said. "Trust me."

mark risher
@mrisher

Follow

"Trust me, this QR code is not a a Rick Roll" -Rob Joyce, NSA #Enigma2016

9:38 AM - 28 Jan 2016

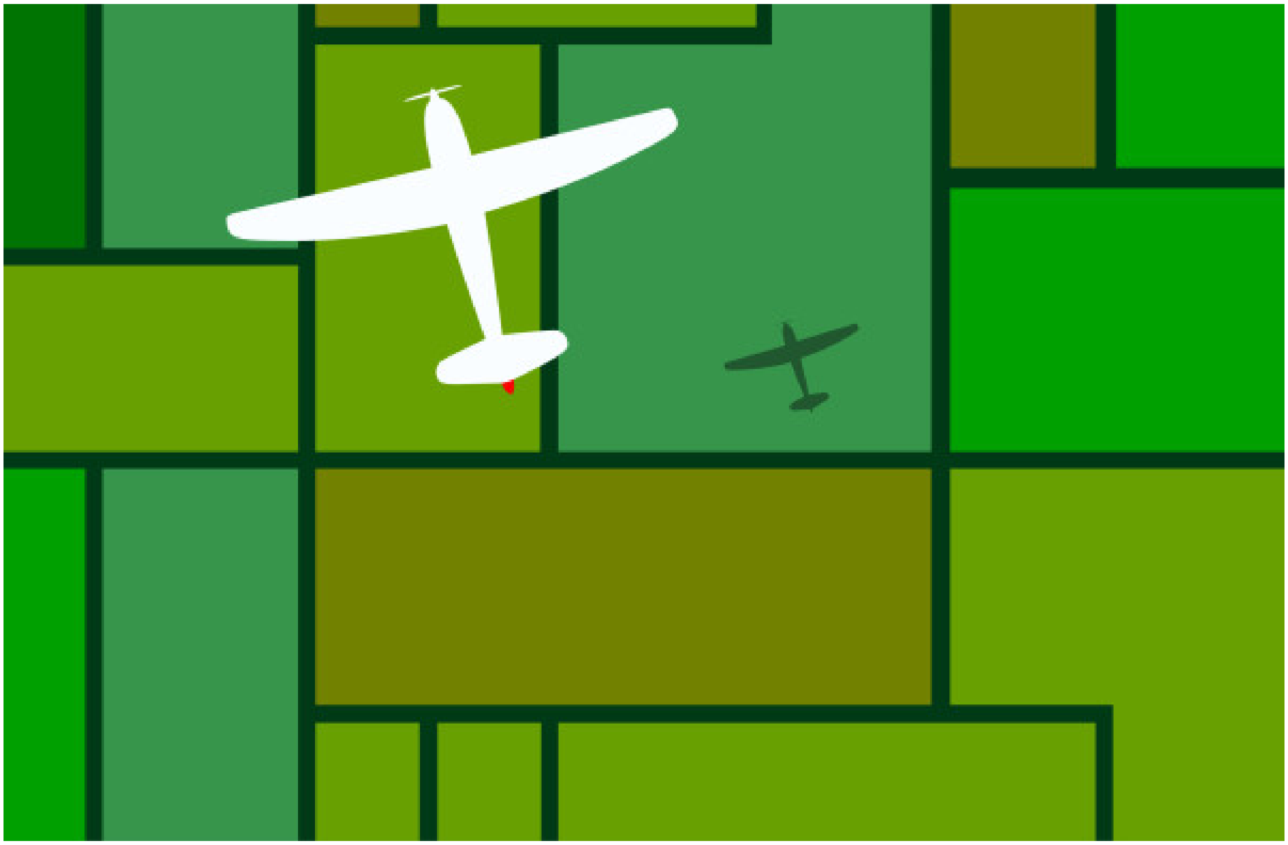
18 ♥ 21

#ENIGMA CONFERENCE #HACKING #NSA #ROB JOYCE #SECURITY #TAO

VIEW COMMENTS

SPONSORED STORIES

MORE SECURITY



SECURITY

California Police Used Stingrays in Planes to Spy on Phones

1 DAY

SECURITY

NYC Launches Investigation Into Hackable Baby Monitors

1 DAY

EXPLAINED

Answers to Your Burning Questions on the Ashley Madison Hack

08.21.15

SECURITY

Proposed State Bans on Phone Encryption Make Zero Sense

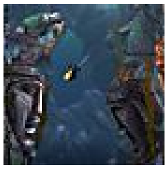
2 DAYS

SECURITY

Hack Brief: Don't Be Trolled by This iPhone-Crashing Link Meme

01.25.16

WE RECOMMEND

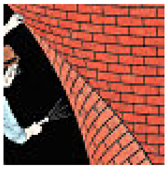


CHRIS KOHLER

GameStop Will Publish Insomniac's Next Game, "Song of the Deep"

JORDAN CRUCCHIOLA

Here's How London Is Making Its Shiny New Tunnels Ready for Trains



MIKE GAULT

The CIA Secret to Cybersecurity That No One Seems to Get

ISSIE LAPOWSKY

Anonymous Launches #OpTrump to Teach the Donald a Lesson

UNUSUAL BUSINESS IDEAS THAT WORK

5 Bootstrapping Strategies Every Startup Should Be Using

POWERED BY OUTBRAIN

FOLLOW US ON YOUTUBE

Don’t miss out on WIRED’s latest videos.

FOLLOW

WIRED

SUBSCRIBE

ADVERTISE

SITE MAP

PRESS CENTER

FAQ

CUSTOMER CARE

CONTACT US

NEWSLETTER

WIRED STAFF

JOBS

RSS