CIA Hacking Tools in review: Cisco was a primary target

Published on March 7, 2017

Craig Dods | Following
Chief Architect - Security at Juniper Networks

299 14 106

As I'm sure news sites will be picking this up shortly, I'll try and be brief today and update this post later with more detailed information as I dig through the documentation.

confidential, CIA-devised hacking tools from an unknown source.

"Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

> Vault 7: CIA Hacking Tools Revealed
> http://wikileaks.org
> Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the...

While the tools themselves have not been released (as of today), the internal documentation for the projects has been (approximately 1200~ unique items).

As I was concerned for our own products, I began rummaging around the "Network Devices Branch (NBD)" tool-sets looking for Juniper-specific attacks and implants, of which there appear to be none (further review is of course required to confirm this). What I did find, however, was that the vast majority of them were targeting Cisco equipment.

A brief list of the affected devices that I've identified can be found below:

- Cisco ASR 1006

- Cisco SUP720 for Catalyst 6500's and 7600's
- Cisco 3560G
- Cisco c2900
- Cisco 2911

A more detailed list with links can be found below for their specific implants and modules with their associated code-names.

- JQJDRAGONSEED (Earl Grey) for Cisco ASR 1006
- JQJSECONDCUT for Cisco ISR 881
- JQJHAIRPIECE and JQJTHRESHER for Cisco 2960S
- JQJADVERSE Cisco 3560G
- CYTOLYSIS for Cisco SUP720 for Catalyst 6500/7600

These implants seem to take multiple modules, such as the ones for JQJADVERSE (Cisco 3560G)

- Powerman

- ROCEM

As an example, ROCEM is used by the CIA as part of their CONOP (concealed operations) for deploying an additional module (HG) on the Adverse platform (3560G)

For clarities sake, there are many other implant and modules available for SOHO/SMB-style routers like Linksys, Zyxel, and Microtik. Cisco appears to be, for the time being, the only "Enterprise Grade" vendor that was targeted by the CIA

As far as other interesting information that I've come across, there is an internal discussion on "What did Equation do wrong, and how can we avoid doing the same?" that occurred on an internal CIA discussion board. Scroll down for the comments on Kaspersky's research and how the CIA can avoid the same pitfalls as the NSA.

More to come as I dive deeper into the documentation.

Standard Disclaimer: *The views expressed in this article are my own and do not necessarily represent the views of my Employer.*

Report this

Craig Dods

14 comments

Newest

Leave your thoughts here…

John Evos ··· 3m
STFU MORONS

WOW.....guess everybody goes back to the "Cone of Silence" and the #2 pencil and yellow pad.....

Like Reply | 1

Shelley Overton ··· 47m
Entrepreneur

Clarity's sake.

Like Reply

Gonzalo Venditto ··· 1h
Empowering CALA organizations with innovative networks I Sales Leader@Juniper Networks

Thanks for the analysis Craig! good to know that...

Like Reply

Lee Mark Poitier ··· 8h
Member at InfraGard National Members Alliance (Cyber Patriot)

Thanks for the heads up!

Like Reply

Alex S. Gabor ··· 11h

#GMail all hacked by #CounterIntelligenceAgencies #Ihaveproof. #Askemeifyoulike

Like Reply | 1 1

James Cauchi ··· 7h

An individual seeking to make the World that which it should be.

I guess honey pots aren't exclusively reserved for malware and hackers any more.

Like Reply | 1

Dmitri Popov ··· 12h

Toxicologist, radiobiologist (PhD), medical doctor (Russia)

CIA vs Wiki leaks.

Like Reply | 1 1

Alex S. Gabor ··· 11h

Founder at Infinite Freedom Foundations of Washington

Dmitri Popov
#WorldCyberWar1.0

Like Reply

Bobby Meador ··· 15h

Network Security Consultant

I'm sure that black Suv is just the local florist. :)

Like Reply | 5

Kade Morton ··· 16h

Social Engineer | Crypto Nerd | Writer | Speaker | Infosec | Life Long Learner | Aspiring Pen Tester

We know Cisco was a target from TheShadowBroker dumps as well, interesting to see this continued.

Osasere Osifo ··· 17h
IBM Bluemix Data Center Technician

Great analysis, i am pretty sure the dynamics will change as more information get spilled out from Vault7.

Like Reply | 3

Vasquez Grant, CCNA, SEC plus ··· 17h
Security Ninjaneer at Academy Sports + Outdoors

So much for that Russian hacking fake news

Like Reply | 4

Efi Kaufman ··· 18h
Senior Cyber Security Analyst

Throwback to 2014:
https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Like Reply | 4 1

Craig Dods ··· 18h
Chief Architect - Security at Juniper Networks

The CIA would have had to be doing something eerily similar to this to deliver some of these. Wikileaks also touches on the interesting dynamics between NSA and the CIA's own, competing team.. . Definitely a good use of tax-payer $$$

Like Reply | 5

Allan Hansen ··· 18h
Threat Prevention Engineer at Check Point Software Technologies

Like Reply | 3 1

Craig Dods ··· 18h

Chief Architect - Security at Juniper Networks

Indeed - there are a massive amount of them, along with some interesting iOS toolkits (2 separate UEFI implants for Mac)

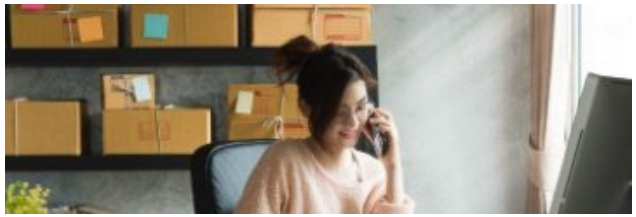
Like Reply | 1

There are 2 other comments. Show more.

Top stories from Editors Picks

Why do we assume men don't want female heroes?

Sarah Robb O'Hagan on LinkedIn



Around the globe and online, entrepreneurship is a male-typed activity — Let's change that!

Marianne Cooper on LinkedIn

The Business Case for Women's Empowerment

Christine Lagarde on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories

Help Center | About | Careers | Advertising | Talent Solutions | Sales Solutions | Small Business | Mobile | Language | **Upgrade Your Account**

LinkedIn Corporation © 2017 | User Agreement | Privacy Policy | Ad Choices | Community Guidelines | Cookie Policy | Copyright Policy | Send Feedback