Errata Security

Advanced persistent cybersecurity

Monday, June 05, 2017

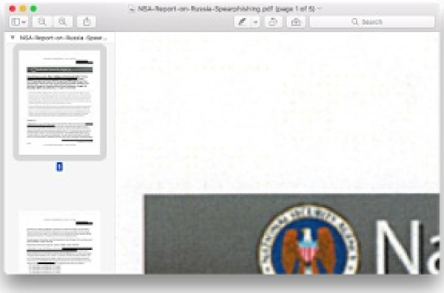
How The Intercept Outed Reality Winner

Today, The Intercept released documents on election tampering from an NSA leaker. Later, the arrest warrant request for an NSA contractor named "Reality Winner" was published, showing how they tracked her down because she had printed out the documents and sent them to The Intercept. The document posted by the Intercept isn't the original PDF file, but a PDF containing the pictures of the printed version that was then later scanned in.

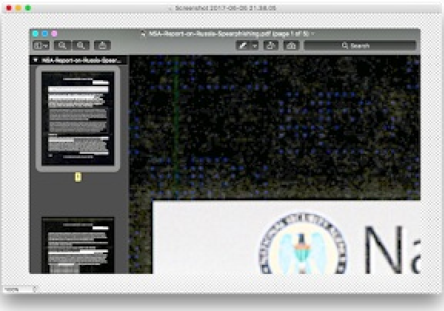
The problem is that most new printers print nearly invisibly yellow dots that track down exactly when and where documents, any document, is printed. Because the NSA logs all printing jobs on its printers, it can use this to match up precisely who printed the document.

In this post, I show how.

You can download the document from the original article here. You can then open it in a PDF viewer, such as the normal "Preview" app on macOS. Zoom into some whitespace on the document, and take a screenshot of this. On macOS, hit [Command-Shift-3] to take a screenshot of a window. There are yellow dots in this image, but you can barely see them, especially if your screen is dirty.



We need to highlight the yellow dots. Open the screenshot in an image editor, such as the "Paintbrush" program built into macOS. Now use the option to "Invert Colors" in the image, to get something like this. You should see a roughly rectangular pattern checkerboard in the whitespace.


Screenshot 2017-06-05 21.38.05
NSA-Report-on-Russia-Spearphishing.pdf (page 1 of 5)
Search
Na

It's upside down, so we need to rotate it 180 degrees, or flip-horizontal and flip-vertical:

Errata Security On Twitter

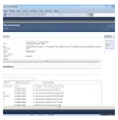
Robert Graham (@ErrataRob)

David Maynor (@Dave_Maynor)

Popular Posts

You are committing a crime right now

Are you reading this blog? If so, you are committing a crime under 18 USC 1030(a) (better known as the “ Computer Fraud & ...



Extracting the SuperFish certificate

I extracted the certificate from the SuperFish adware and cracked the password (" komodia ") that encrypted it. I discuss how dow...

How The Intercept Outed Reality Winner

Today, The Intercept released documents on election tampering from an NSA leaker. Later, the arrest warrant request for an NSA contractor ...

SideJacking with Hamster

NOTE: you can download the program at http://www.erratasec.com/sidejacking.zip ; make sure to read the instructions. Others have done a be...

That NBC story 100% fraudulent

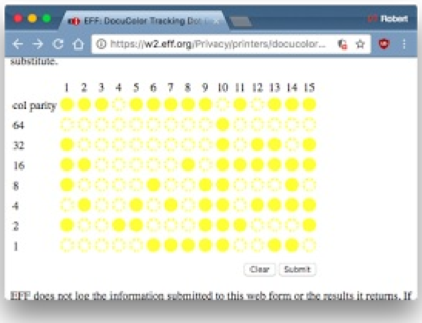
Yesterday (Feb 5 2014) On February 4th, NBC News ran a story claiming that if you bring your mobile phone or laptop to the Sochi Olympics...

Bash 'shellshock' bug is wormable

Early results from my scan: there's about 3000 systems vulnerable just on port 80, just on the root "/" URL, without Host fiel...

Bash 'shellshock' scan of

Now we go to the EFF page and manually click on the pattern so that their tool can decode the meaning:



EFF: DocuColor Tracking Dot
Robert
https://w2.eff.org/Privacy/printers/docucolor...

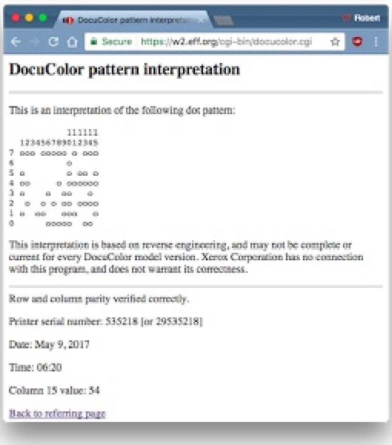
substitute.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
col parity	●	●	●	○	●	●	●	●	●	○	●	○	●	●	●
64	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
32	●	○	○	○	○	○	○	○	○	●	○	●	●	○	●
16	●	●	○	○	○	○	○	●	○	●	●	●	●	●	●
8	●	○	○	○	○	●	○	○	●	●	○	○	○	●	○
4	○	●	○	○	●	○	●	○	●	●	○	●	●	●	●
2	●	○	○	●	●	○	○	○	●	●	●	○	○	○	●
1	○	○	○	○	○	●	●	●	●	●	○	○	●	●	○

Clear Submit

EFF does not log the information submitted to this web form or the results it returns. If

This produces the following result:



DocuColor pattern interpreta
Robert
Secure https://w2.eff.org/cgi-bin/docucolor.cgi

DocuColor pattern interpretation

This is an interpretation of the following dot pattern:

```
           111111
  123456789012345
7 ooo ooooo o ooo
6          o
5 o        o oo o
4 oo     o oooooo
3 o    o  oo   o
2  o  o o oo oooo
1 o  oo   ooo   o
0      ooooo  oo
```

This interpretation is based on reverse engineering, and may not be complete or current for every DocuColor model version. Xerox Corporation has no connection with this program, and does not warrant its correctness.

Row and column parity verified correctly.

Printer serial number: 535218 [or 29535218]

Date: May 9, 2017

Time: 06:20

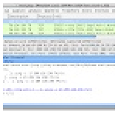
Column 15 value: 54

Back to referring page

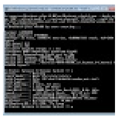
The document leaked by the Intercept was from a printer with model number 54, serial number 29535218. The document was printed on May 9, 2017 at 6:20. The NSA almost certainly has a record of who used the printer at that time.

The situation is similar to how Vice outed the location of John McAfee, by publishing JPEG photographs of him with the EXIF GPS coordinates still hidden in the file. Or it's how PDFs are often redacted by adding a black bar on top of image, leaving the underlying contents still in the file for people to read, such as in this NYTime accident with a Snowden document. Or how opening a Microsoft Office document, then accidentally saving it, leaves fingerprints identifying you behind, as repeatedly happened with the Wikileaks election leaks. These sorts of failures are common with leaks. To fix this yellow-dot problem, use a black-and-white printer, black-and-white scanner, or convert to black-and-white with an image editor.

Printers have two features put in there by the government to be evil to you. The first is that they recognize a barely visible pattern on currency, so that they can't be used to counterfeit money, as shown on this $20 below:



the Internet
NOTE: malware is now using this as their User-agent. I haven't run a scan now for over two days. I'm running a scan right now ...



Confirmed: LinkedIn 6mil password dump is real
Today's news is that 6 million LinkedIn password hashes were dumped to the Internet. I can confirm this hack is real: the password I use...

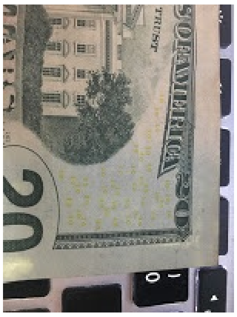
Notes on the Ashley-Madison dump
Ashley-Madison is a massive dating site that claims 40 million users. The site is specifically for those who want to cheat on their spouse. ...

x86 is a high-level language
Just so you know, x86 machine-code is now a "high-level" language. What instructions say, and what they do, are very different thi...

Blog Archive

June 2017 (3)

-



The second is that when they print things out, they includes these invisible dots, so documents can be tracked.

Yes, this code the government forces into our printers is a violation of our 3rd Amendment rights.

While I was writing up this post, these tweets appeared first:

[redacted] DIRNSA

Quinn's internet
@quinnnorton

Follow

oh wow, @knowtheory just pointed out the microdots on the first and late page of the intercept's docs. printer dots kill puppies, folks.

9:17 PM - 5 Jun 2017

447 493

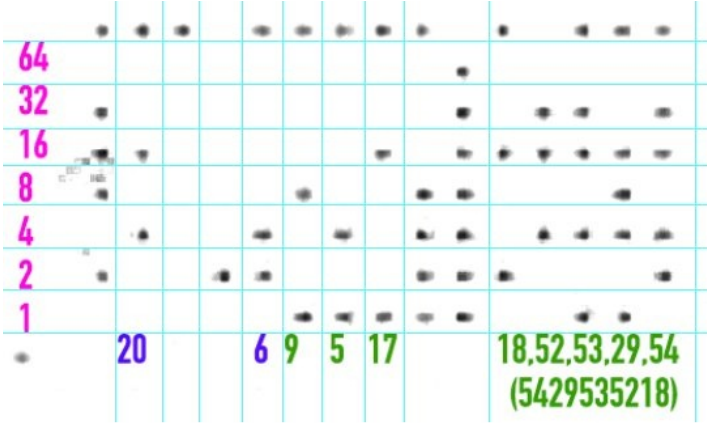
Quinn's internet @quinnnorton 19h
oh wow, @knowtheory just pointed out the microdots on the first and late page of the intercept's docs. printer dots kill puppies, folks. pic.twitter.com/w8qxJ9zvhf

Tim Bennett
@flashman

Follow

@quinnnorton @knowtheory The date in the microdots is 6:20 2017/05/09 from a printer with serial number #5429535218, according to w2.eff.org/Privacy/printe... pic.twitter.com/6BY7Y3MFhL

10:08 PM - 5 Jun 2017



387 493

Tweet Pin it Share 1.4K

By Robert Graham

Labels: leak, NSA, Reality Leigh Winner, The Intercept

49 comments:

popsiq said...

Poof goes a darn fine tracking tool.

12:16 AM

vliam said...

Not really.

This has been a pretty standard thing for the last decade or so and even NSA contractors forget, or are simply unaware, that it exists.

12:47 AM

Brian Bulkowski said...

3rd amendment? Really? You'll liken these yellow dots to quartering soldiers?

1:56 AM

KiTA said...

It's forcing you to run software on behalf of the US Government. That's against the 3rd Amendment.

2:04 AM

Christian Vogel said...

Simply converting to b/w is not sufficient!
http://imgur.com/a/kLovh

And even when you mask them out so that they are no longer visible in the "all white" (paper) background, e.g. by messing with the white/black point of the image there's still the possibility that they could be recovered with correlation methods in grey areas where they aren't visible to the naked eye or just by increasing the contrast.

2:33 AM

john gury said...

Technically I think she had already outed herself in multiple and more obvious ways like using her gmail to communicate with the Intercept, social media activities, etc. Still, a mistake on the part of the Intercept in providing evidence to finger and prosecute her.

3:27 AM

erroneus said...

Don't print in color or on a color printer unless the document warrants it. Black monochrome only people. It's also cheaper. Have two printers.

3:32 AM

sterniu said...

That's why, when Greenpeace leaked the TTIP documents, they first manually re-typed a copy of the original document that was then released.

Especially The Intercept should had have known better.

A terrible professional error that not only destroyed the life of one of the rare courageous citizens, but also shows that The Intercept cannot be considered as safe “whistle blower” platform anymore.

This is sad and very dangerous, as we need independent human rights defending journalism more than ever - and this can only work if these journalists are able to protect their sources.

3:43 AM

shevy said...

I consider it highly illegal that people are trackable that way in general.

That this is possible shows that the goverments do not work for the people but for other interest groups.

5:35 AM

Unknown said...

black and white is not greyscale, btw.

6:07 AM

Unknown said...

I don't think anti-counterfeiting measures mean the government is being evil to me.

6:28 AM

Matt said...

Wrong amendment! No Constitutional violation. What you expose to public even unknowingly is not protected. Government has to protect itself from saboteurs. Writer has head screwed on wrong if he thinks this is evil.

7:51 AM

codetaku - said...

"Forcing"? ... no it isn't. You are buying a printer that chooses to run that software. You can overwrite the software yourself if you have the motivation to do so.

8:09 AM

codetaku - said...

(that comment was directed to KiTA--the interface I was using had a reply-to-comment button and I wasn't sure how obvious it would be that I was replying to them)

8:10 AM

DJ said...

Christian Vogel, black and white means indexed (1-bit color palette). Every pixel is either pure black or pure white. There are no gray pixels. I believe this does defeat printer dots. The leaker should have done this themselves rather than trusting the journalist.

8:23 AM

georgeknightlang said...

Nice work. How could The Intercept be so naive by seeking contact with the NSA? I don’t get it, Glenn Greenwald, you know better. Do you?

8:37 AM

timb said...

This comment has been removed by the author.

8:56 AM

timb said...

Is there any chance people would realize the Amendment comment was a joke and stop failing to be pedantic with their "corrections."

8:58 AM

Bill Owen said...

#JWICs is a thing. Winner outed herself.

9:35 AM

Bob R. said...

Great article, but there is no such built in program called Paintbrush on macOS.

9:54 AM

Angelique said...

This was not a courageous citizen! She was a deranged anti American communist like 90% of the journalist today. This leak does nothing but alert foreign gov't of our capabilities. Claiming to be helping when your actually sabotaging our country is Straight out of the Alinsky playbook acuse others of what your actually doing

10:00 AM

Leslie Taylor said...

Spell check. Try it.

10:33 AM

haithabu said...

She may have assumed that secrecy laws are a dead letter with all the consequence-free leaking going on.

10:37 AM

Jonathan Zimmerman said...

Nothing wrong with microdots - especially when run on government hardware to protect government property from criminal intent.

10:40 AM

Michael Heller said...

Someone was definitely either careless or maliciously trying to out Winner, but I'm not sure we can jump to blaming The Intercept just yet. A WashPo article said the FBI questioned Winner -- who admitted everything -- on June 3rd, two days before the Intercept story went live.

10:51 AM

YourLocalGP said...

The specific constitutional rights violation is not of consumers, it is of private companies who manufacture printers being compelled to add this technology. Familiar to many following the case with Apple and encryption recently.

10:53 AM

Ellen P. said...

Or the know-how..... said the extremely tech-challenged 67 year old.... me.

10:56 AM

Sean Phillips said...

This comment has been removed by the author.

11:01 AM

Eric said...

Angelique is slightly right but mostly wrong. I agree that leaks can harm our ability to legitimately intercept nefarious foreign governments and foreign individuals seeking to harm our republic and citizens. On the other hand the fact that a foreign power has corrupted our election process in numerous ways and may very likely put in power an illegitimate president is a serious concern. When the only authority and oversight is the same president and his cronies then turning to the free press seems like a pretty good idea. This woman was very brave for bringing forth this information.

11:03 AM

Divemedic said...

Yes. The reason why the third Amendment is there is not because the founders were angry at being forced to run a hotel for British troops. It is because a common way of quelling dissent was to place soldiers in the homes of rabble rousers, and have them report on the dissenters' activities. Nowadays, the just do the same thing electronically with NSA email intercepts and the like.

11:17 AM

Sum_ID said...

Michael, fyi, the reason they questioned the girl is because The Intercept contacted them to see if they wanted anything redacted before printing, they gave them a copy of the document so as to not release sensitive information. It is common in media these days.

11:19 AM

Mitch **said...**

This comment has been removed by the author.

11:36 AM

My Conservative Rants **said...**

She is a criminal and belongs in jail...

11:53 AM

beebah **said...**

I don't know that this would be any more a violation of 3rd Amendment rights than, for example, the ability to trace typewriting to a specific old-school typewriter would be. Let's put aside this specific case for a moment, given that she printed the doc on an NSA/work printer. If, say, the FBI wanted to track a specific printed document to a specific printer, there would need to be one of the following: 1) a catalog of all dotmark patterns, presumably registered by the manufacturers, or b) a record maintained by each individual manufacturer which the FBI could access, possibly with a warrant, that would narrow the printer to the retail location but possibly no further, or c) the FBI would have to match the document to the exact printer-- in which case, they perhaps have narrowed the search down to a possible printer and this is used for confirmation. This is quite different from planting either a government agent or a form of bug (computer, audio, whatever) in a private residence.

12:02 PM

Don Clifton **said...**

This comment has been removed by the author.

12:06 PM

RobPaulGru **said...**

DESTROY THIS BEAST

12:23 PM

articulett **said...**

A point of consideration is that the the Intercept knows this because of Snowden and they purposefully outed Winner as a message to leakers.

12:24 PM

articulett **said...**

http://observer.com/2017/06/reality-winner-intercept-nsa-leak-explained/

12:42 PM

Socialist Avenger **said...**

they v much want you to think this. her gmail was used for a completely unrelated communication with TI

1:30 PM

Acessa São Carlos **said...**

This document is a PDF.. there is no scanner that can acctually capture those dotes even in 1600P.. so HOW was that scanned?

1:31 PM

Socialist Avenger **said...**

this is because TI shared documents on 5/30 with the NSA who notified the FBI. winner was already in custody when the article was finally run

1:31 PM

Christopher Smith said...

Is it because it was *OUR* election and *Trump* won that has all you people so upset, or is the general principle of thing — in which case, were all of you *equally* upset about Obama's 2015 attempts to influence Israeli elections (using US taxpayer dollars), and all the other US attempts to influence foreign elections between 1947 and 2000?

https://townhall.com/tipsheet/mattvespa/2016/12/16/flashback-that-time-the-obama-administration-spent-hundreds-of-thousands-of-dollars-to-defeat-benjamin-netanyahu-n2260711

http://www.latimes.com/nation/la-na-us-intervention-foreign-elections-20161213-story.html

Just curious...........

1:59 PM

Charlie McHenry said...

Please read Alinsky's work. His "playbook" is all about how to give powerless people organizing tools to stand up to authority to protect their rights. If that is evil, or communist in some way, then I'm also guilty - as are many others.

2:09 PM

haithabu said...

But when these people attain power and continue to use Alinskyite tactics - that's a problem as we found out during the Obama administration.

2:16 PM

jon191 said...

This could all be elaborate theater - cleverly designed to help the oligarchy/establishment achieve certain objectives. It's good to be open minded, but not too gullible. Just because 300 million people believe a pack of lies, does not change the matter.

2:28 PM

@primesuspect said...

To people who think this is a newer innovation: This has been going on since at least the late 1990s when consumer color laser printers became viable. I had a leadership role at a retail copy chain and one of my stores was involved in a counterfeit money situation; the US Secret Service came in to verify serial numbers of our color laser printers and sat down with me to explain the yellow dots. This was in 1998.

3:06 PM

@primesuspect said...

https://en.wikipedia.org/wiki/Printer_steganography

3:07 PM

Brad Hartliep said...

As long as you accept the fact that Hillary Clinton and the DNC are just as Corrupt and Evil as Donald Trump and the RNC you have an argument for returning our Nation to Civil, Honorable, Citizenship-based Rule. If you're still brainwashed by either Party - or ANY Party - than you need to have your brain deprogrammed ..

Brad Hartliep. America's Independent Candidate 2020

3:25 PM

Amanda Black said...

Things are different if you're working for the government with security clearance.

3:47 PM

Post a Comment

Links to this post

Create a Link

Home

Older Post

Subscribe to: Post Comments (Atom)