Canarytokens.org - Quick, Free, Detection for the Masses

Introduction

This is part 2 in a series of posts on our 2015 BlackHat talk, and covers our Canarytokens work.

You'll be familiar with web bugs, the transparent images which track when someone opens an email. They work by embedding a unique URL in a page's image tag, and monitoring incoming GET requests.

Imagine doing that, but for file reads, database queries, process executions, patterns in log files, Bitcoin transactions or even Linkedin Profile views. Canarytokens does all this and more, letting you implant traps in your production systems rather than setting up separate honeypots.

Canarytokens is available for free at http://canarytokens.org, or you can download and run your own installation (source and Docker images are available.)

Why should you care?

Network breaches happen. From mega-corps, to governments. From unsuspecting grandmas to well known security pros. This is (kinda) excusable. What isn't excusable, is only finding out about it, months or years later.

Canary tokens are a free, quick, painless way to help defenders discover they've been breached (by having attackers announce themselves.)

How tokens works (in 3 short steps):

1. Visit the site and get a free token (which could look like an URL or a hostname, depending on your selection.)
2. If an attacker ever uses the token somehow, we will give you an out of band (email or sms) notification that it's been visited.
3. As an added bonus, we give you a bunch of hints and tools that increase the likelihood of an attacker tripping on a canary token.

More Details:

Tokens consist of a unique identifier (which can be embedded in either HTTP URLs or in hostnames.) Whenever that URL is requested, or the hostname is resolved, we send a notification email to the address tied to the token. You can get one in seconds, using just your browser.

To obtain a token:

1. Visit http://canarytokens.org.
2. Enter your email address. (It's only used to notify you when the token is triggered, mails are not used for any other purpose.)
3. Enter a comment which describes where you're using the token. If the token is triggered in six months time, a comment will help you remember where you placed the token. Be specific (e.g. "file watch on 192.168.100.2:/repos/repo3/README.txt" or "Password lure email in user@domain.com inbox". We envisage having loads of tokens, so a good description is necessary.

it your token is:

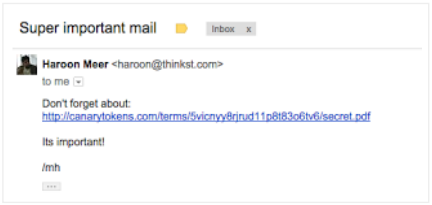
- `http://canarytokens.com/terms/5vicnyy8rjrud11p8t83o6tv6/contact.php`

then someone visiting an y of these:

- *`http://canarytokens.com/terms/5vicnyy8rjrud11p8t83o6tv6/admin.asp`*
- *`http://canarytokens.com/terms/5vicnyy8rjrud11p8t83o6tv6/admin.asp`*
- *`http://canarytokens.com/includes/5vicnyy8rjrud11p8t83o6tv6/login.docx`*
- *`http://canarytokens.com/foo/bar/5vicnyy8rjrud11p8t83o6tv6/anything-really`*

would still activate your token. This gives us a the simplest use-case for a token, **an old fashioned w eb-bug**.

For example, you could send yourself an email with a link to the token plus some lure text:



Simply keep it in your inbox unread since you know not to touch it. An attacker who has grabbed your mail-spool doesn't. So if your emails are stolen, then an attacker reading them should be attracted to the mail and visit the link – and while your week is about to get worse, at least you know.

If you like, you could even use the same token as an embedded image. This way it works like the classic 1x1 transparent GIF. Now an attacker reading your inbox could trip over it just because his mail client renders remote images. (In this way you can use free Canarytokens as a classic web/mail-bug, to receive a notification when an email you send has been r ead.)

Production Usage

Canarytokens can be used as simp le web-bugs, but they are incredibly flexible as we'll see.

You may have a fancy SIEM tha t lets you know when stuff happens, but you'll find that with a little creativity, there's a bunch of places that you could get wins from a token (that can be deployed in seconds) that you couldn't easily get to otherwise.

Do you trust the admins/support at DropBox to leave your files alone? (or Office365? or HipChat?)

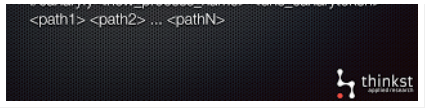
Simply generate a token and drop it in your folder, or mention it in your HipChat channel. If some admin is browsing contents in their spar e time (or is being coerced to do so by a 3rd party) they will trip over your URL and you'll be notified.

Tokens + helper tools

FileWatchers

Every time someone g ets owned, and their homedir gets published, theres a bit of speculation on "*how they got taken.*" While we may not always know the answer to that question, there is something we _do_ know. **Files in their home directory were read.** (This will include files tha t were never likely to be read by anyone, so this could be a really high quality mark er that bad stuff has happened!)

We include a no-dependency C pr ogram (Canaryfy) that will compile and run on Linux . Generate a token, then use it to watch a file. If the watched file is ever read.. you will get your notification..

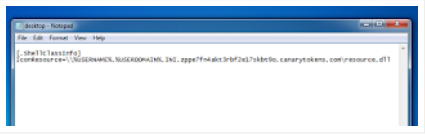


On OSX, without iNotify events, we make use of DTrace to get the same result.

You could use DTrace to monitor binaries executing too, so XXX will take a token as input, and will notify you if someone runs `uname`, `id`, `ifconfig` or `hostname` on your machine.

desktop.ini share + zip-files

Windows provides an even cooler way to get notified, in the guise of the venerable old desktop.ini configuration file. Dropping a desktop.ini file in a folder allows Explorer to set a custom icon for a file. Since this icon can reside on a remote server (via a UNC path), using DNS we can effectively make use of a token as our iconfile.



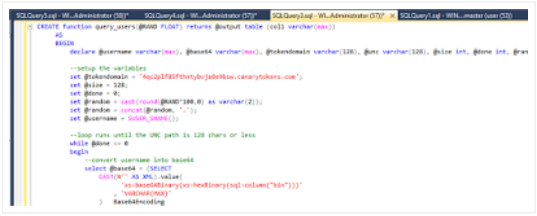
This means anytime someone browses the directory in Explorer, a notification is sent! It's an actual file tripwire without any agents or log file monitoring.

(WinZIP and WinRAR both maintain directory structures and honour desktop.ini – you can download a Zip file with the desktop.ini already packaged after you generate your token, and you'll get notified if someone opens (expands) the Zip file.

MSSQL & MYSQL

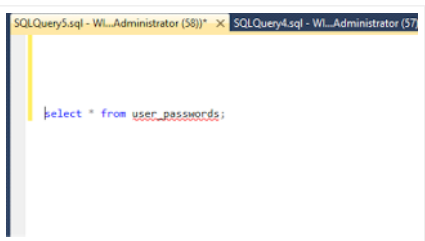
Inserting Canary rows into a database, and then watching if they are ever accessed is a pretty common piece of advice when reading about database security. Interestingly, we will wager that most people who have given this advice, have never actually tried making this happen. Its surprisingly painful, and likely not possible in the version of the database you're running!

It isn't natively possible to have MSSQL server trigger an action on a SELECT statement, but what one can do is create a custom VIEW which triggers a DNS query when a SELECT is run against the VIEW.



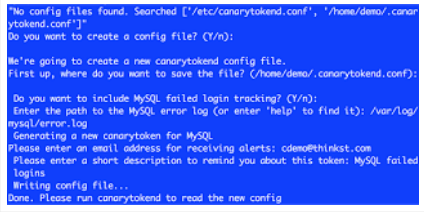
(it's also possible to set permissions on the VIEW so anyone can run a select on it without seeing its source).

Then, if anyone queries the, say, the `user_password` view:



The DNS lookup is triggered an a notification is sent:

Since the DNS query is built in T-SQL, we have fine-grained control of the query. It means we can embed additional information like the querying user in the notification.
On MySQL, we make use of another simple tool called canarytokend. This simple utility tails the MySQL log file, matches preset regexes and triggers alerts through the canarytokens console.



Canarytokend is useful since its highly extensible; it simply tails log files and triggers tokens (MySQL is just the example log file). You can use it to watch any kind of log, and fire emails on matches.

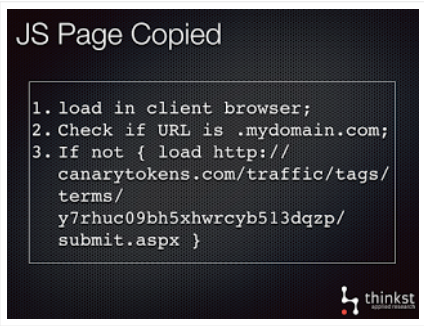
Document Open

Honeydoc files are relatively well known. Simply placing a token in the document meta-data, give us a reliable ping when the document is opened. Canarytokens generates both a Word document and a PDF document.

One trick: the PDF document will trigger a notification by Adobe Reader regardless of whether the user allows network communications!

JS Page copied

The Canarytoken server can also notify you if a web page you care about is copied (and hosted on another site). This is usually step0 in a well executed phishing campaign. To make this happen, we simply create our token from canarytokens.org, then:



Imgur, Bitcoin and LinkedIn

Imgur, LinkedIn and Bitcoin give us other channels for the Canarytokens server. We can use these sites as oracles to determine if they have been accessed, or touched.

This isn't new!

Agreed, the basic concept is old. Lance Spitzner spoke about honeytokens in 2003 and Spafford & Kim mentioned the concept back in 1994.

In fact, map makers have been mixing fake data with real data for hundreds of years to catch map thieves.

What Canarytokens does however, is makes this concept trivially useable by everyone, and implements a bunch of techniques and approaches which haven't been publicly discussed.

What if attackers blacklist the honeytokens.org domain? Doesn't that work?

This would work! That's why we suggest that you download the canarytokens docker image and run your own server. (You can grab the source to build it yourself from here)

Future announcements

34 comments :

Unknown September 9, 2015 at 7:44 AM

But couldn't the bad guy work around this with blocking outgoing traffic to that URL first?

Reply

Replies

marco September 9, 2015 at 8:07 AM

Definitely, that's a risk to the canarytokens.org site. It's why we've published the source as well as Docker images; you can rely on our site but the better approach will be to run your own with multiple domains, used only in your own tokens. Any attacker would need to first discover your custom domains before blocking them.

(We mention this at the end of the page, and link to the Docker images and source there too.)

groadires September 9, 2015 at 1:46 PM

This comment has been removed by the author.

Reply

Anonymous September 12, 2015 at 4:53 PM

Will it still work if if CNAME somthingimportant.mydomain.com to point to canarytokens.org?

Reply

Replies

Zach Varnell September 14, 2015 at 6:58 AM

Yep! Worked for me.

Reply

marco September 14, 2015 at 6:16 AM

According to this Reddit comment it works, though we haven't tried it.

Reply

rantinc September 14, 2015 at 11:39 AM

Will this system send out repeated notifications for each trip or only the first event triggers a notification?

Reply

Anonymous September 23, 2015 at 6:32 PM

Thinkst:

Elegant, and seems effective.

Without code changes, would it be possible to configure SMTP servers, other than Mandrill, within switchboard.env for the Docker implementation?

Anonymous April 9, 2017 at 11:18 PM

The answer seems to be 'No.' I had to change the Code to support SMTP, which is easy with Python. I don't really get, why they dindt made it an option in the first place.

Reply

Anonymous October 3, 2015 at 10:59 AM

I appreciate the effort, I am even using the tokens under my own DNS to point at canarytokens.org. However, I wanted to use this on my own servers. I'm sorry, but docker is not an acceptable deployment path for most people. This project needs to have some rudimentary install directions for those of us NOT using docker. I'm somewhat annoyed that the install directions basically say to use Docker..... and that's it.

Love the service, love what you guys do. But please PLEASE don't announce that it's available for deployment on our systems if you have a jumble of files on Git and don't even have install instructions.

Once again, Docker should NOT be the go-to deployment schema supported for this. It should be an alternative to a "normal" install, included only after you have everything else complete.

Sorry if it sounded like a rant. I'm just very excited about this project and want to use it more in production.... but cant.

Reply

Replies

MH October 3, 2015 at 3:47 PM

Hiya Anonymous.

Thanks.. We appreciate your appreciation.. and we are sorry to have caused you annoyance.

Could you maybe explain why Docker is so horrible here? (We know a few people who are happily using the images).
It seemed to us like the quickest way to help get people up and running.

Henry March 21, 2016 at 6:21 PM

I see two other options. One is to release a bunch of instructions on how to get all the programs involved up and running (like you'd have to install and configure redis even) alongside your code. You chose to release a container instead of this because that sounds really annoying, of course.

And then the only other option I see is to release it as a VM image, a virtual appliance. But if Anonymous could run that, then they could just as easily make their own VM and install Docker on it and run your container.

So really the only thing they could be asking for to do is the first option, since if they can run VMs, they can run Docker. And that makes me think they maybe don't understand what's involved here. What production environment would disallow Docker but would allow installing all the various things inside the container?

Mashiara January 25, 2017 at 10:11 PM

I know I'm late to the party but... IMO the Dockerfile (and docker-compose.yml) are just about the most explicit installation instructions one can- get. Sure they may be quite specific to the base images they use but who wants to maintain separate installation instructions (with instructions on how to secure the various parts, like Redis, alongside) for N distros ?

eax October 11, 2015 at 1:01 PM

Excellent ideas, thanks a lot for this inspiring project!

Reply

Anonymous November 2, 2015 at 6:42 AM

The HTTP canary tokens work great, but correct me if I'm wrong, if a network is using DNS forwarding, then the DNS lookups reflect the IP address of the DNS forwarders, not the network where the token was triggered, correct?

Reply

Anonymous December 11, 2015 at 1:44 PM

So....I'm trying to run "docker-compose up" to get this running and receive the following nginx errors:

nginx_1 | 2015/12/11 21:41:21 [emerg] 1#1: host not found in upstream "frontend" in /etc/nginx/nginx.conf:33
nginx_1 | nginx: [emerg] host not found in upstream "frontend" in /etc/nginx/nginx.conf:33

If I perform a packet capture on port 53 while this command runs, I can see DNS requests to my external DNS server for a hostname of "frontend." This host obviously does not exist in my external DNS and I'm not sure why it would be querying the external DNS in the first place...

Suggestions on how to fix this?

Reply

Anonymous December 13, 2015 at 1:14 PM

So....I'm the same guy as above. It looks like the problem is that the switchboard and the frontend images are running an incorrect command and exiting immediately:

dude@bigcanary:~/canarytokens-docker⟫ sudo docker-compose ps
Name Command State Ports
---
canarytokensdocker_frontend_1 /bin/bash Exit 0
canarytokensdocker_nginx_1 nginx -g daemon off; Exit 128
canarytokensdocker_redis_1 /entrypoint.sh redis-server Exit 0
canarytokensdocker_switchboard_1 /bin/bash Exit 0

In the config.json for the switchboard and frontend, I can see that the Cmd entry contains only /bin/bash. On another working system, the Cmd entry contains more than /bin/bash. If I edit the config.json file, the changes are wiped out when I run "docker-compose up." So, any insight on what I can do to fix the broken system would be appreciated.

Reply

marco December 21, 2015 at 1:10 PM

@Anonymous x 2: Thanks for the report. We've pushed a new docker-compose.yml into the canarytokens-docker Github which makes the container commands explicit. Can you try that and let us know if it doesn't work out?

Reply

Anonymous January 9, 2016 at 12:25 PM

It would be nice if this thinkst.com and canarytokens.org were available via https.

Reply

Anonymous February 11, 2016 at 7:55 AM

HI,
Thanks for the intiative and for making it free & open source !

- Anyone has tested the Document Open in Word please ? How ???
Any clues/recommendations will help.

- Same for PDF, or file watching in windows which is what i'm going to test too.

Thanks !

Reply

Anonymous May 18, 2016 at 11:31 AM

Is this project still live? I've generated a token and tried to trip it 6 ways from Sunday and there's no alerts of any kind coming through to our mail server.

Is there any kind of support for this?

Reply

Replies

MH May 18, 2016 at 4:04 PM

Hi Anon.. (love your work by the way!)

It is indeed alive and is used daily.. You bumped into a quick DNS outage the site had. Its been fixed and your token alerts should have come through now. Sorry about that, and thanks for the heads up.

Reply

Anonymous May 20, 2016 at 4:22 AM

But honestly, why dont your docker images have descriptions and instructions?

Reply

Replies

marco May 20, 2016 at 7:30 AM

The old docker images are deprecated. Checkout the new image for description and instructions.

Reply

faceboogle September 2, 2016 at 12:51 AM

Hello.

I heard about your project on Risky.biz and it sounds great. I wanted to produce a proof of concept: a Word .DOC file (or a PDF) which sends an alert when opened. The options for creating tokens at http://canarytokens.org/generate don't seem to relate to what I want to do. They are: DNS/HTTP | Browser Scanner | Cloned site | Imgur | LinkedIn | Bitcoin

Any suggestions on how to embed one of these tokens in a .DOC?

faceboogle September 2, 2016 at 1:07 AM

Having tried it, the first option looks promising. Testing underway...

Harshu September 6, 2016 at 5:07 AM

Let me know[update all of us] if you get it to work.

Reply

Anonymous October 25, 2016 at 12:41 PM

So, how about some way to identify who has taken the bait? Like IP, computerusername, etc. coming back in the email notification as well?

Reply

Anonymous October 28, 2016 at 1:03 AM

What is the expected lifetime of a token ?

Reply

Anonymous January 24, 2017 at 4:29 PM

Use of a url-shortening service can further obscure the nature of the token.

Reply

Anonymous April 12, 2017 at 10:43 PM

Unique email address token doesn't work from docker installation, other tokens work great. Is there some additional configuration that should be set in order to make this token work?

Thanks

Reply

Anonymous April 12, 2017 at 11:13 PM

Is it possible to take an existing PDF and add the created caanrytoken ? If so, how do I do this. (I want to know if my documents is read :)

Reply

Anonymous May 27, 2017 at 7:08 AM

Hello,
Is that normal that the token is triggered only once ?
For example I did download and open the "token" folder with the token. -> Mail received, OK.
I reopen the same "token" folder and nothing happened...

Reply

Publish Preview

Home

Subscribe to: Posts (Atom)