# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>What this document is about</td>
<td></td>
</tr>
<tr>
<td>A Vanilla Deployment</td>
<td>3</td>
</tr>
<tr>
<td>The simplest of Canary deployments</td>
<td></td>
</tr>
<tr>
<td>Obvious Attacker Spawn Sites</td>
<td>4</td>
</tr>
<tr>
<td>Placing a Canary where attackers are likely to show up</td>
<td></td>
</tr>
<tr>
<td>Where are your Crown Jewels?</td>
<td>5</td>
</tr>
<tr>
<td>Canaries that resemble your Crown Jewels</td>
<td></td>
</tr>
<tr>
<td>All you Routers are belong to us</td>
<td>7</td>
</tr>
<tr>
<td>Canaries that look like routers are old favorites</td>
<td></td>
</tr>
<tr>
<td>Insiders in Gen Pop!</td>
<td>8</td>
</tr>
<tr>
<td>Canaries can be useful as user laptops too!</td>
<td></td>
</tr>
<tr>
<td>Server Farms</td>
<td>10</td>
</tr>
<tr>
<td>Attackers who compromise your server farm often look around.</td>
<td></td>
</tr>
<tr>
<td>The map is the Key?</td>
<td>11</td>
</tr>
<tr>
<td>Mapping a drive from some machines to a Canary are a good way to “deal them in”</td>
<td></td>
</tr>
<tr>
<td>Intranet Jackpot</td>
<td>12</td>
</tr>
<tr>
<td>Canaries make useful Intranet Servers (in a matter of minutes)</td>
<td></td>
</tr>
<tr>
<td>SCADA/PLC Birding</td>
<td>13</td>
</tr>
<tr>
<td>Canaries can pose as SCADA equipment too</td>
<td></td>
</tr>
<tr>
<td>Pimp my Canary</td>
<td>15</td>
</tr>
<tr>
<td>Adding custom services to your Canary</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Canaries are deployed all over the world. From the networks of billion dollar Silicon Valley darlings to the networks of Nuclear Research Agencies. From Universities in Australia to Aquariums in the US Midwest, they happily serve, always vigilant.

The heterogeneity of their deployments means that there are a number of different ways to deploy your birds. Sure they can be deployed in under 3 minutes (this is a key design requirement and we will keep it this way) and, sure, we’ve seen a number of these rapid deployed birds blow the whistles on crack red-teams and previously undiscovered “insiders” but wouldn’t it be great to have a doc that covered some typical deployment use cases? This is that document!

OS, service and port permutations possible on Canaries will number in the thousands (and will make this document both boring and unwieldy) so instead of being comprehensive, it aims to spark your thinking on common deployment configurations.

A Vanilla Deployment (because sometimes, Vanilla can be great too!)

Canary ships with a host of default “personalities”. At the time of writing, this included several flavors of Windows, several flavors of linux, some routers, switches and SCADA equipment.

What does this mean? Options!

What matters, of course, is where you place the birds. If you are a large financial, and place a “Dell Switch” in the CEO’s office, it may get tripped on by a really clumsy attacker, but you can really do much better than this. Let’s see how.

![Default personalities](https://canary.tools)

https://canary.tools Page 3 of 15 info@canary.tools
**Obvious Attacker Spawn Sites**

This Canary technique is simple and quick. There are several spots on your networks where attackers are likely to show up. On one of your DMZs, in your database segment, on your VOIP network, etc. A well chosen canary in those spots is bound to attract their attention.

I.e. An attacker who manages to compromise a host on your DMZ (through a web-server/web-framework/web-app exploit) often finds himself in foreign territory.

While step-0 is probably going to be raiding the server itself for data or access, the very next step is going to be situating himself and looking around. While the cautious attacker will first do this by examining other servers directly connected to the compromised host, the attacker is forced to look around. It may not be full blown Nmap scans, but its fairly common for an attacker in this position to reach out to hosts near-by.

If the web server you are running is a linux server, a Canary on the same subnet, running a typical LAMP stack is bound to get “touched”. (Note that this server need not be exposed to the Internet, in fact, we’d advise against it). You can deploy your Canary there, and forget it. It’s a pretty safe bet that the day one of the servers in your DMZ get popped, the attacker is going to let you know he is there by touching your Canary too.
What are your crown-jewels?

The Crown-Jewel-Canary is one of my favourites. It requires five minutes of thought (which combined with our three minute setup time, is still a pretty good deal!) Here, what you do is first think about the data/objects in your organization that you would most want to protect. If you are a large mining house, this is your GIS and prospecting information. If you are a payment card processor its your stored Credit Cards and Track2 data. If you are a large defense contractor working on a Joint Strike Fighter.. well.. you get the picture.. Once you have identified what these crown-jewels would look like, you simply create a NAS storage device, or a Windows FileServer that appears to hold such jewels in an appropriate location.

You can place them in the appropriate network segment or workgroup:

Mapping to a shared folder on the Canary

Or you can happily enroll the servers into AD:
What's cool about this sort of Canary, is that you don't even need Domain Admin privileges to join Canaries to the domain, and even if your attacker were to portscan these birds (which they probably won't) they totally look the part.

```
bash-3.2# nmap -o 192.168.2.140
Starting Nmap 7.31 ( https://nmap.org ) at 2017-04-20 23:50 +03
Nmap scan report for LINFS2 (192.168.2.140)
Host is up (0.00869s latency).
Not shown: 996 closed ports
PORT                      STATE SERVICE
139/tcp open netbios-ssn
1433/tcp open ms-sql-s
1400/tcp open vnc
MAC Address: 00:04:EA:32:54:86 (Hewlett Packard)
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows Server 2008 R2 or Windows 8, Microsoft Windows Server 2008 R2 SP1 or Windows 8
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
bash-3.2#
```

The Canary is fingerprinted as a Windows 2008 R2 machine

A super fortuitous property of the crown-jewel Canary, is that you don't have to jump through elaborate hoops to make them discoverable. If your company builds the Joint Strike Fighter, and on the research network, you have a server called \RESEARCH with a folder called JSF2017 — the sorts of attackers you care about will reach out to you. It's why they are there.
All your routers are belong to us!

As a pen-tester, I loved network kit. They were often unhardened, hardly ever extensively monitored, and were analogous to Harry Potter’s FLOO Network (allowing you to pop up in different parts of the network). The Snowden leaks show that routers were a firm favorite of GCHQ too, who compromised core routers belonging to Belgacom for years before discovery. A fake router would be just the thing to detect network-focused attackers.

Fortunately, Canary makes this trivial. From unboxing, to a Cisco Router, in under 3 minutes:

Unbox, select “Cisco Router”, reboot to a Cisco router

For bonus points, you add routes to unused/non-existent private networks through your new Cisco Router. Valid traffic will never get there, but an attacker mapping out your network? Totally!

Adding routes on legitimate hosts to aid discovery
Insiders in Gen-Pop!

Many organizations throw their users into a common network. While we can certainly appreciate the Mad-Max, Thunder-dome'esque feeling this engenders, it also usually leaves users exposed to each other. Do you know when Alice maps to other users shares / browses their folders?

You can with a simple, well placed Canary!

Choose an OS that matches your environment, like Windows 10. Then let's give the laptop a suitable name \CEO-IBMX1 — let's see if Alice reaches out to his Private share. (If you are feeling curious, let's create Private\2018-Recruiting, Private\2017-Financials and Photos on that machine.

Canary will be very specific about what Alice did, so it's worth knowing what “she” was actually after.
What's cool is, even though this is a trivial deployment that unmasks your Alice's, it also sounds the alarm when you are about to face a Saudi Aramco style attack. (Where attackers touch hundreds of hosts for weeks or months before making their key-attack.)

Sure, local-admin problems plague lots of people and, sure, user segments are noisy. But some noises (like the chirping of a Canary) are clear as a bell.
Server Farms

Server farms are another simple place to drop in Canaries. Whether you’re aiming for a file-server in AD, a SQL-Server discoverable through MSDE/SQLPing or just a stray Sharepoint server with juicy looking contents. Builtin Canary Personalities make this a walk in the park.

Pre-packaged personalities let you get up and running quickly

The useful hook here, is that it’s not uncommon for attackers to scan server subnets looking for low hanging fruit, and once more, it’s super common for even advanced attackers to look around once they pop an existing server. Both ways, your bird quickly becomes a reasonable port of call.
A common question asked by first timers is: “how will attackers find the Canary?” People think they need complex “breadcrumbs” to make this happen, but they don’t. Our Canaries are made to look valuable, not vulnerable, and if you place something valuable on your network, the sort of attackers you really care about will make it their jobs to find them. “But as an attacker I only ever touch servers if i see them in active use,” says the pen-tester being kinda dishonest with himself.

No problem.

A simple, valuable way to bring Canary into play, when it’s running as a Windows server or NAS server is to map a network drive. If you created a permanent mapping from the CEO’s or CFO’s laptop to a Canary, it would simply sit there:

![Image of network drive mapping]

A permanent mapped share on a sensitive machine points the attacker toward the Canary

But.. when the CEO/CFO eventually gets popped, you can bet your bottom dollar that the attacker is going to explore the mapped connections on his machine, announcing his presence.

(The astute reader will notice that this mapped drive would also alert us if the CEO/CFO were hit by ransomware.)
While we totally forgive Diogo for calling them “honeytokens”, we also totally agree with the sentiment. As an attacker, I love stumbling onto Intranet sites. They are usually full of juicy data, pointers to valuable systems, possible credentials, and so on. Well, thanks to Canary, setting up fake systems like this are a breeze. You can use the “User Supplied Website” feature on your canary web server to allow you to upload your own webroot:

![User Supplied Website Feature](https://canary.tools)

Upload your own website to the Canary web server

This allows you to create a quality intranet site that looks genuine enough, but screams blue murder when touched.

![Canary with a custom website](https://canary.tools)

Canary with a custom website

Bring your other bird into play by populating the fake website with references to other Canaries in your environment.
**SCADA/PLC Birding**

Industrial control systems saw a raft of security research in recent years, and the general consensus is that they’re pokey at best. Combine that with a clear history of targeting and compromise (obligatory mention of Stuxnet), and administrators of control networks need ways to detect attackers.

Your Canary makes this trivial. With a few clicks, you can easily deploy a Modbus TCP endpoint to emulate either a Rockwell or Siemens PLC.

Quickly deploy a Canary for ICS environments

Should an attacker try to read or write data on the Canary PLC, it fires an alert and they’ll have revealed themselves sooner than you can say “Centrifuge error!”

The Canary’s Modbus TCP endpoint appears legitimate
When the query tool probes the Canary, an alert is received.
Pimp my Canary!

What if you have a service thats not currently available on your Canary? Wouldn’t it be great if you could easily get a fake version of the service running, and get the reporting and alerting for free?

Fortunately, you have two options:

1. Canary ships with an SDK. Once you are in Bluetooth config mode, you can upload your own user modules to the bird. This gives you complete control with simple primitives to generate alerts. (You can read all about it [here](#).)

2. You can use the “Custom TCP Service” to create super simple TCP Services on your birds.

When configuring your Canary, simple enable the “CUSTOM TCP SERVICE”.

```
CUSTOM TCP SERVICE

disable

What is this?

Custom TCP Service:

Port:

Banner on Client Connect:

Banner on Receiving Data:

Alert only if client sends

Accessible either in the Console or on the device’s config page
```

This simple module does exactly what it says on the tin: Allows you to create a custom TCP service on the bird. So simply give the module a port to bind to (8001 in our example) and then create a banner that will be served to the attacker on connecting. (Welcome to FooDemoDaemon - v2.1\n in our example). Thats it.. You've created a custom service and will be alerted accordingly.

```
$ nmap -p8001 192.168.2.140
Starting Nmap 7.31 (https://nmap.org) at 2017-04-20 23:30 +03
Nmap scan report for LINFS2 (192.168.2.140)
  Host is up (0.0038s latency).
  Not shown: 996 closed ports
  PORT   STATE SERVICE
  139/tcp open  netbios-ssn
  445/tcp open  microsoft-ds
  8001/tcp open vcom-tunnel
  8080/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds.
maruzu:~ haroon$ telnet 192.168.2.140 8001
  Trying 192.168.2.140...
  Connected to linfs2.
  Escape character is '^]'.
  Welcome to FooDemoDaemon - v2.1
  help
  411 - Command Unknown
```

Custom TCP service which echoes a banner on connect and generates an alert