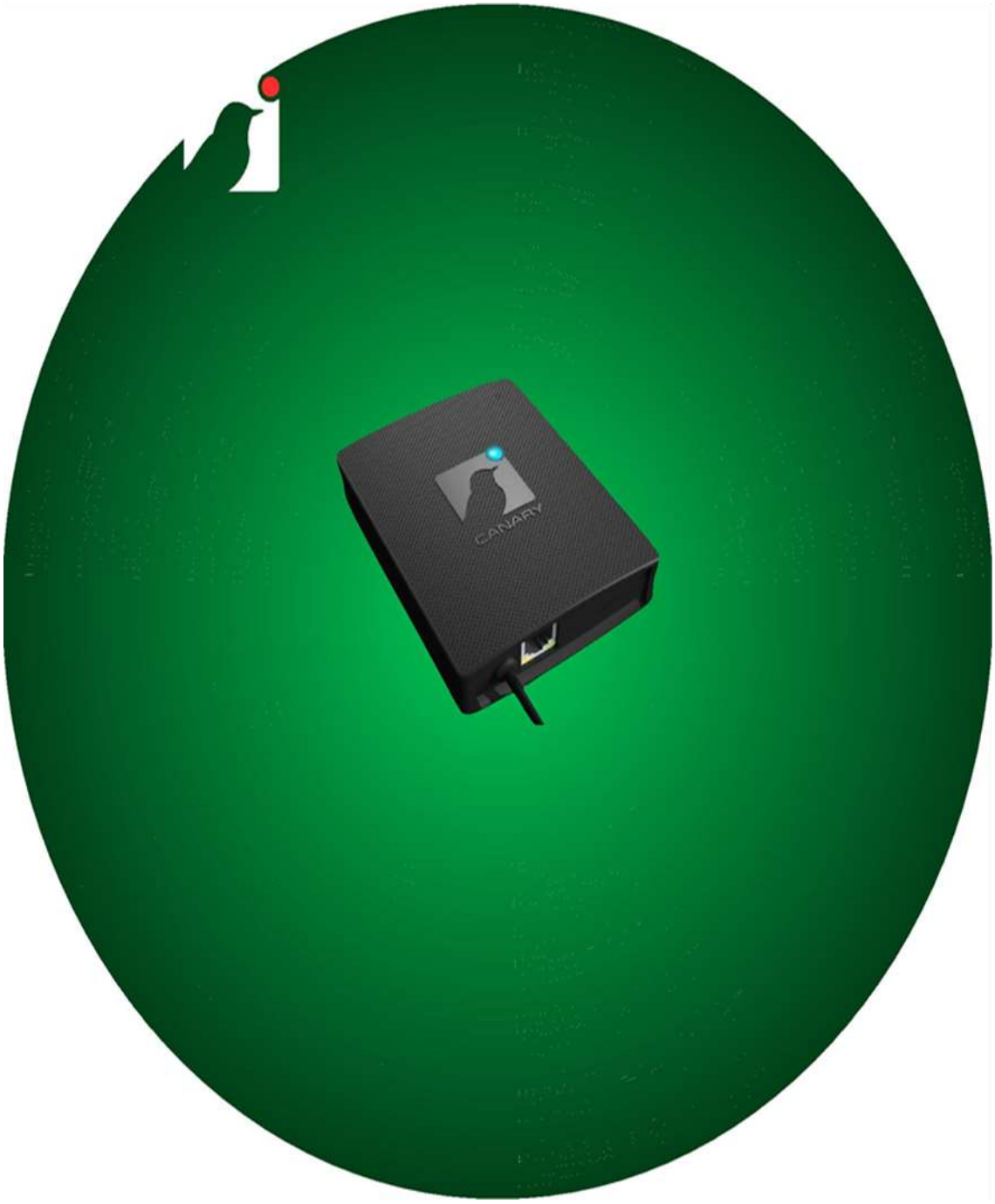
Canary V2 - Update



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 many different ways to deploy your birds. They can be deployed in under 3 minutes (this is a key design requirement and we will keep it this way) and, we've seen a number of these rapid deployed birds blow the whistle on crack red-teams and previously undiscovered "insiders".

Why not call us for an on-line demonstration? Possibly the best value 30-minutes of your cybersecurity time!

Cybercast Limited - an authorised distributer and reseller of innovative IT security services and solutions
Contact email: info@cybercast.co
Tel: +44(0)7702 286 834

Canary V2 - Update

The benefits *that honeypots can bring to the defender are well-recognised, however the typically associated high costs, specialized training plus the effort of deployment and management, usually drop honeypots to the bottom of the to-do list. The pocket-sized, plug 'n play* ***Canary*** *device can change all of this since it is an easy decision - crushes honeypot high costs, requires no specialized training and introduces great implementation and management simplicity. It is pleasingly inexpensive and typically can take a few minutes from the user unboxing Canary to having it ready on a network.*

Know when it matters - Canary, works by looking like an attractive target; a server or other piece of networking equipment that can easily be hacked: threat actors prowl target networks look for such openings. They browse Active Directory for file servers and explore file shares looking for documents, try default passwords against network devices and web services, and scan for open services across the network. When the attacker unknowingly encounters a Canary, the services on offer are designed to solicit further investigation, at which point it "chirps", notifying nominated users. Whilst systems' administrators could set up their own honeypots, most baulk at this prospect as with all the network problems faced, nobody needs yet more machines to manage.

Since launching of the Canary in mid-2015, the positive global market feedback & product success has led to a continually evolving and even greater, value-driven offering.

New capabilities, and improvements get rolled out frequently.

Here is a features' snapshot of this powerful and low-cost solution.

Canary engineering is based on the principle of detecting the first signs of lateral movement an attacker might make.

FEATURES

New Hardware
Canary v2 ships with awesome new hardware. It's faster, has more services, it's more reliable and so darn slick-looking you'll almost not want to send it to your data centres.

Canary API
Simple integration with your in-house security databases and SIEM solutions, now generally available with supporting documentation.

Customised Modules and Services
You want a photocopier or medical device, etc, personality? write your own modules / services, and upload them to your Canary. However, if there is a real major opportunity requiring a unique, tricky personality having a global appeal and demanding to be quickly created, let us know and our designers can look at it.

Remote Configuration
Whether applying a completely new personality or making subtle changes to the device, you can do it from the comfort of your console! Simply click on your Canary, and then select the "Remote management" option available on each Canary.

Canary Token Integration
Canary-tokens allow you to create mini tripwires in 3rd party sites or applications (in fact you can use them all over the place!). This version delivers your own, customisable token server as an integral part of the Canary consol. Get alerts whenever and wherever when your sites are cloned, documents are viewed or directories are browsed!

Canary V2 - Update

Canary Cloaking
Canary cloaking allows your Canary to be completely invisible to port-scanners and asset inventory systems.

New Services
Canary brings a bunch of new "fake" services with something for everyone: ICS fans get Modbus. Developers get GIT repositories and lovers of NoSQL get a safe implementation of our favourite key/value store (Redis!).

New OS Personalities
This release brings through a bunch of new personalities. Windows XP and Rockwell. It's all in there, and all deployable with just a few clicks! Deploy convincing and interactive Cisco routers, Dell switches, Windows or Linux servers (with a host of different services), in the standard 4-minute setup time you've come to expect.

Web Servers
Web Servers now have lots of options- JBoss, VMWare, Sharepoint and a host of friends. If you feel like it, now you can even upload your own document root (*or trivially wrap your service in SSL*)!

Windows File-share Enhancements
The Windows file share service is now much nicer to use, with an improved Explorer-like interface that supports nested files and directories.

MAC Camouflage
Choosing an OS Personality will now automatically prepare your Canary with an appropriate MAC address. This makes the fakery more complete and has a local segment NMAP looking more believable than ever!

Graph View
Canaries aren't supposed to generate lots of notifications, but what happens if there's a sudden flood of them? (Or if you only check your alerts after a horrible week?) Figuring out exactly what happened from a list of events can be sub-optimal. To help with this, your Canary console now has a handy graph-view. Clicking on the graph-view icon maps out the activity visually. Graph view is fully interactive, allowing an easy way to mass-delete events (but also just makes it trivial to spot what's going on).

Alert Pruning
Alert pruning allows mass deletion of alerts that have accumulated on your console over time. If alerts go above a certain threshold (and have been present for a while on your console) the "Alert Pruning" option will pop up to allow you to quickly delete older events.

IP Address and port whitelisting
Known systems like vulnerability scanners, asset management / inventory servers or an SCCM service scan easily be added to a white list to ensure that they don't set off alerts when interacting with Canary. In order to ignore alerts from specific IP addresses, ranges or ports, simply add them to the *"Ignore these IPs and ports"* list on your settings page.

SNMP and OID whitelisting
Similar to IP address whitelisting, specific SNMP Object Identifiers (OID) can also be ignored. This is done by adding the SNMP OID to the whitelist on your settings page. Once enabled, SNMP OID whitelisting follows the same format as the IP address and port whitelisting

Canary V2 - Update

Port Scan Consolidation
Apparent port scan activity is common on noisy networks. In order to avoid bothering you with several Port Scan notifications, we've added functionality to roll-up multiple port scan alerts and present them as a single consolidated alert.

Slack and HipChat Integrations
Canary alerts can be sent directly to either tool with quick configuration on your settings page. This makes it even easier to be notified of activity on your Canaries. To set this up, simply enable *"Webhook incident Reporting"* on your Console settings page then follow the simple prompts. Note that you can also enable a generic webhook.

Attack History
Sometimes you'd like to know more about an attacking IP. Have you ever seen it before? Has it attacked a Canary before today? Don't worry, we've got it covered. A "Click" on the link immediately shows what other incidents were attributed to the same source.

Canary for low-cost, trustworthy early alerts at:-

- **Global data centres**
- **Distributed branches**
- **Remote customers**
- **Small businesses**

It really does make <u>proven</u> sense

Great for Managed Security Service Providers!