THINKST CANARY

Target, OPM, Belgacom, the NSA: All were compromised months (or even years) before realising it. They spent millions of dollars on security products and services, but when it mattered:

They just didn't know!

Every year, hundreds of companies like yours only discover that they've been compromised when informed by a third party.
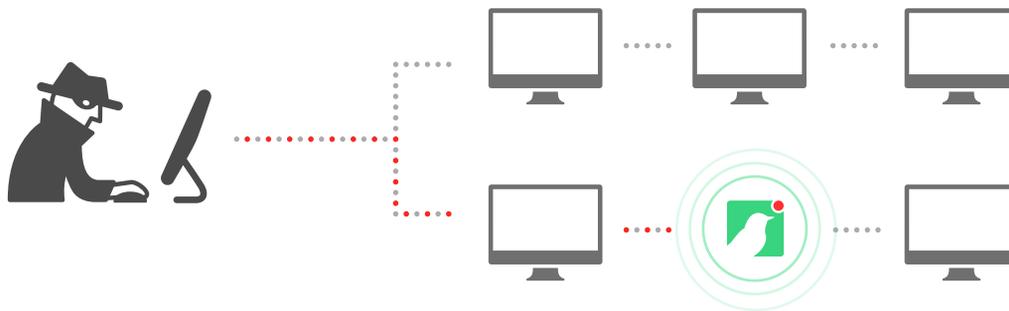
This is a stupid problem.

Millions of security dollars later, most companies still have no detection capabilities for roving malicious insiders.

This is a solvable problem.

Skilful adversaries move laterally within compromised networks for days or months before locating and exfiltrating a company's crown jewels.

This is a hidden opportunity.

Thinkst Canary changes this.

- Canary devices can be set up in under 4 minutes, even on complex networks, and emulate a variety of possible systems right down to their network signatures.

- Simply sprinkle Thinkst Canaries around your network, configure your alert settings, and wait.

- Attackers moving laterally, malicious insiders and APT all reveal their presence by interacting with your Canaries.

Many security products promise you the world, if you would just re-engineer your entire network or mold all your processes around them. These products demo well but are often found months later, half configured and barely used.
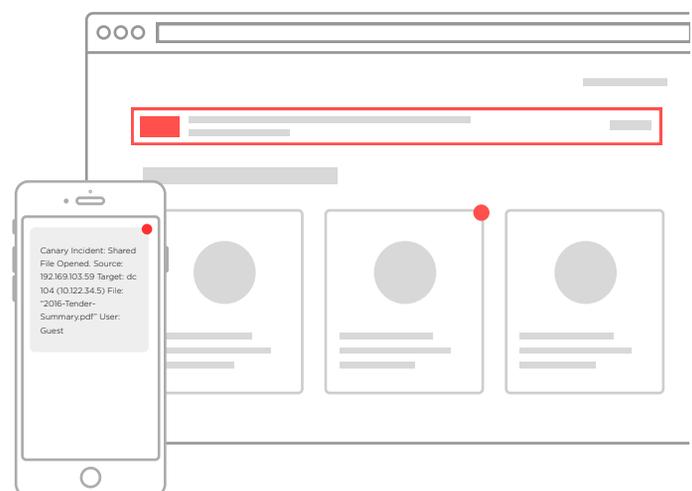
Canaries install in under 4 minutes, and are 100% useful on installation.

Nobody wants more alerts and nobody wants even more dashboards. Thinkst Canaries are silent, till you need them to speak up.

Not hundreds of alerts, not even tens of alerts.

Just one! When it matters.

0 Hype. Low False-Positives. 0 Excuses

Canary Incident: Shared File Opened. Source: 192.169.103.59 Target: dc 104 (10.122.34.5) File: "2016-Tender-Summary.pdf" User: Guest

■ Isn't this just a honeypot?

Yes and No.

Honeypots are a great idea. Everyone knows this, so why is almost nobody running them on internal networks? Simple: because with all the network problems we have, nobody needs one more machine to administer and worry about. We know the benefits that honeypots can bring but the cost and effort of deployment always drops honeypots to the bottom of the list of things to do.

Canary changes this. Canaries can be deployed in minutes (even on complex networks), giving you all of the benefits without the admin downsides.

■ How easily can they be deployed?

It usually takes less than 5 minutes from unboxing your Canary, to having it ready for action on your network. With just a few clicks, you'll have a high interaction honeypot, and be able to track who's browsing shares for PDF documents, trying to log into a NAS, or portscanning your network.

■ How do they communicate with the console?

Canaries are deployed inside your network and communicate with the hosted console through DNS. This means the only network access your Canary needs is to a DNS server that's capable of external queries, which is much less work than configuring border firewall rules for each device.

■ How much does this cost?

Less than you would imagine. Visit https://canary.tools/quote to check pricing options or drop us a note!

■ Ok. You have 2 minutes, how does this work?

Simply choose a profile for the Canary device (such as a Window box, brandname router, or Linux server). If you want, you can further tweak the services your Canary runs. Perhaps you need a specific IIS server version or OpenSSH, or a Windows file share with real files constructed according to your own naming scheme (say, 2019-tenders.xls). Lastly, register your Canary with our hosted console for monitoring and notifications.

Then you wait. Attackers who have breached your network, malicious insiders and other adversaries make themselves known by accessing your Canary. There's little room for doubt. If someone browses a fileshare and opened a sensitive-looking document on your Canary (\\fin_srv\planning\2019-tenders.xls) you'll immediately be alerted to the problem.

You possibly already do have a problem, you might just not know it. Canary changes that.

■ Are Canaries a hardware-only solution?

Canaries are available as hardware units, VMWare images, EC2 instances or GCP machines.

■ Does the console have pretty Web 2.0 coolness?

We have a console, and we think it's pretty, but we really don't want you to spend much time on it. After you setup your Canaries you forget about the whole thing completely. When one of your Canaries chirp, only then do you attend to the problem.

■ What if an attacker DoS'es the device or compromises it?

If your Canary can get off just one alert (and it really should) then your console far away is going to log and alert on this. Whatever happens to the Canary after that won't matter since it stores nothing of value.