cyberTAN Information Security

CANARY - Know When it Matters

Not just another Honeypot

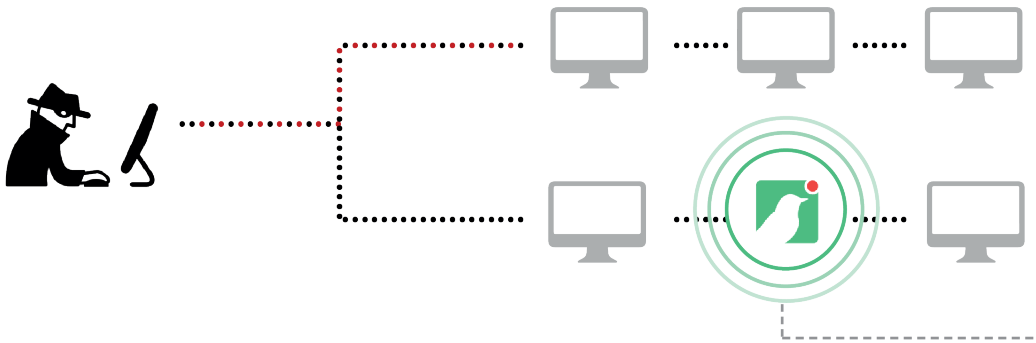
Every year, hundreds of companies only find out that they have been compromised when they are notified by a third party.
This is a stupid problem.

Even companies that spend millions of dollars on their security have no idea if malicious insiders are trawling around where they shouldn't be.
This is a solvable problem.

Skilful adversaries move laterally within compromised networks for days or months before locating and exfiltrating a companies crown jewels.
This is a hidden opportunity.

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 HAD NO CLUE!!



Thinkst Canary changes this. Canary devices can be set up in under **5 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 5 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. 0 False-Positives. 0 Excuses

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.

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, 2016-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_02\Planning \2016_forecasts.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.

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.

thinkst applied research

Who is Thinkst Applied Research?

Thinkst is an Applied Research company with a deep focus on information security. Thinkst was founded to respond to the simple (but often repeated) call in infosec today: "We are not winning against X". Thinkst exists to work on difficult problems and to solve them. With a decade of history in well published applied research and a strong network of partners, thinkst aims at turning the current tide, because we strongly agree with Voltaire when he said: "No problem can withstand the assault of sustained thinking!"

Who is CyberTAN?

CyberTAN is a data security specialist focused on providing sound, organised and well structured data security guidance and solutions. Protecting your critical data is crucial to remaining competitive and to do this we provide strategic clarity and direction using a combination of consulting and customised solutions to help you make informed decisions. Whether you're a small business or major enterprise CyberTAN can assist you to find a cost effective, fit-for-purpose data security solution to meet your company information security objectives.

CANARY TOKENS

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

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.

A the simple use-case for a token (and there are several), **an old fashioned web-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 read).

CANARY

"The median number of days that attackers stay dormant within a network before detection is over 200"

— "Microsoft Advanced Threat Analytics" | Microsoft

REQUEST A DEMO:

Contact us today to schedule a demonstration.

sales@cybertan.co.za

cyberTAN Information Security

How can I find out more?

Contact Andrew Kirkland @ CyberTAN Information Security on +27 83 636 0099 or akirkland@cybertan.co.za to discuss how we can help you and your clients.