Adventures in Security Research

Runa Sandvik - Founder - Granitt
@runasand - glitch-cat.com - granitt.io

$ whoami

- From Oslo, now in New York
- Passionate about journalism/security
- Then: Tor, Freedom of the Press, New York Times
- Now: Granitt, advisor to Ford Foundation and CISA
- Run @journalistandspy on Instagram

$ whoami

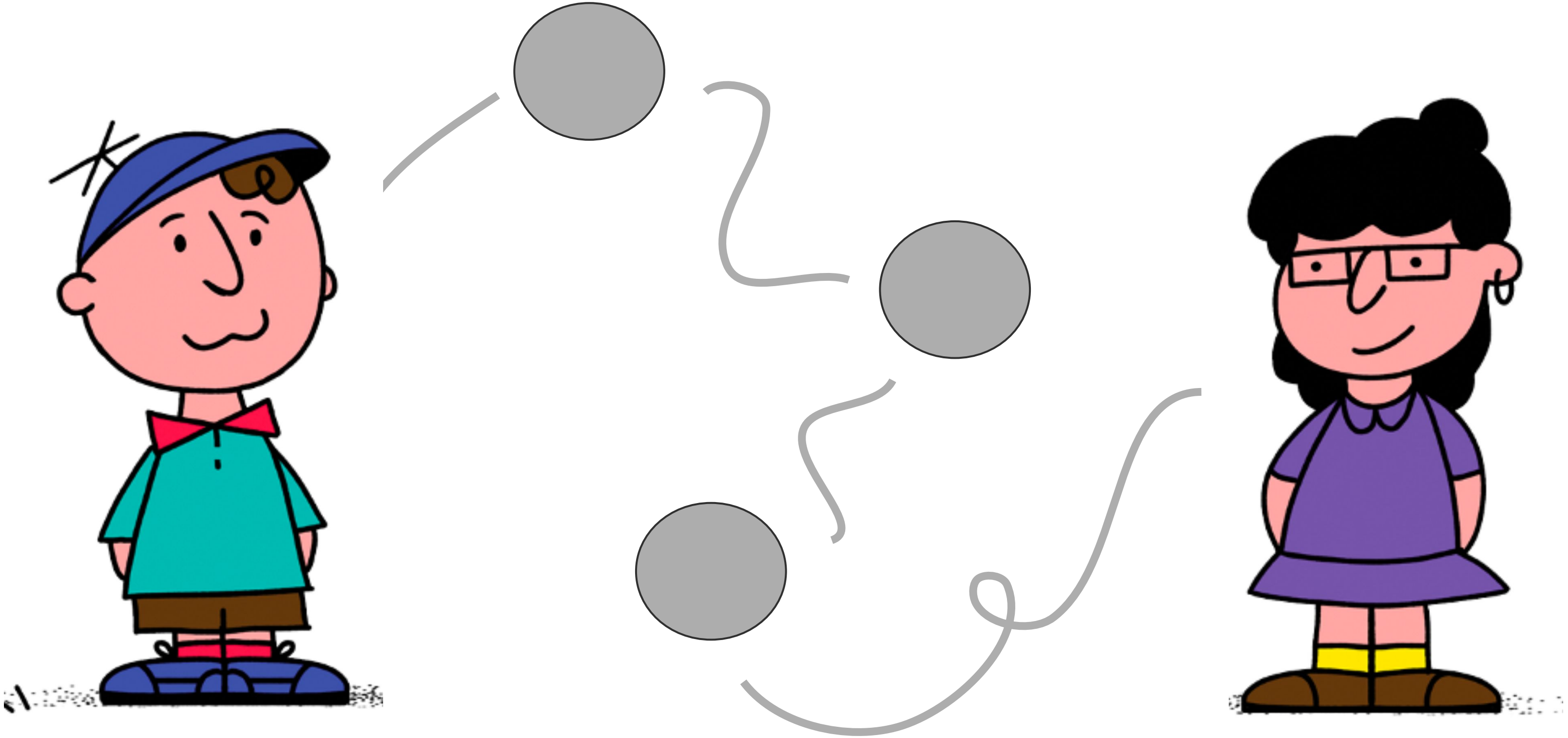
- From Oslo, now in New York
- Passionate about journalism/security
- Then: Tor, Freedom of the Press, New York Times
- Now: Granitt, advisor to Ford Foundation and CISA
- Run @journalistandspy on Instagram

Back in 1995…

Office of Naval Research

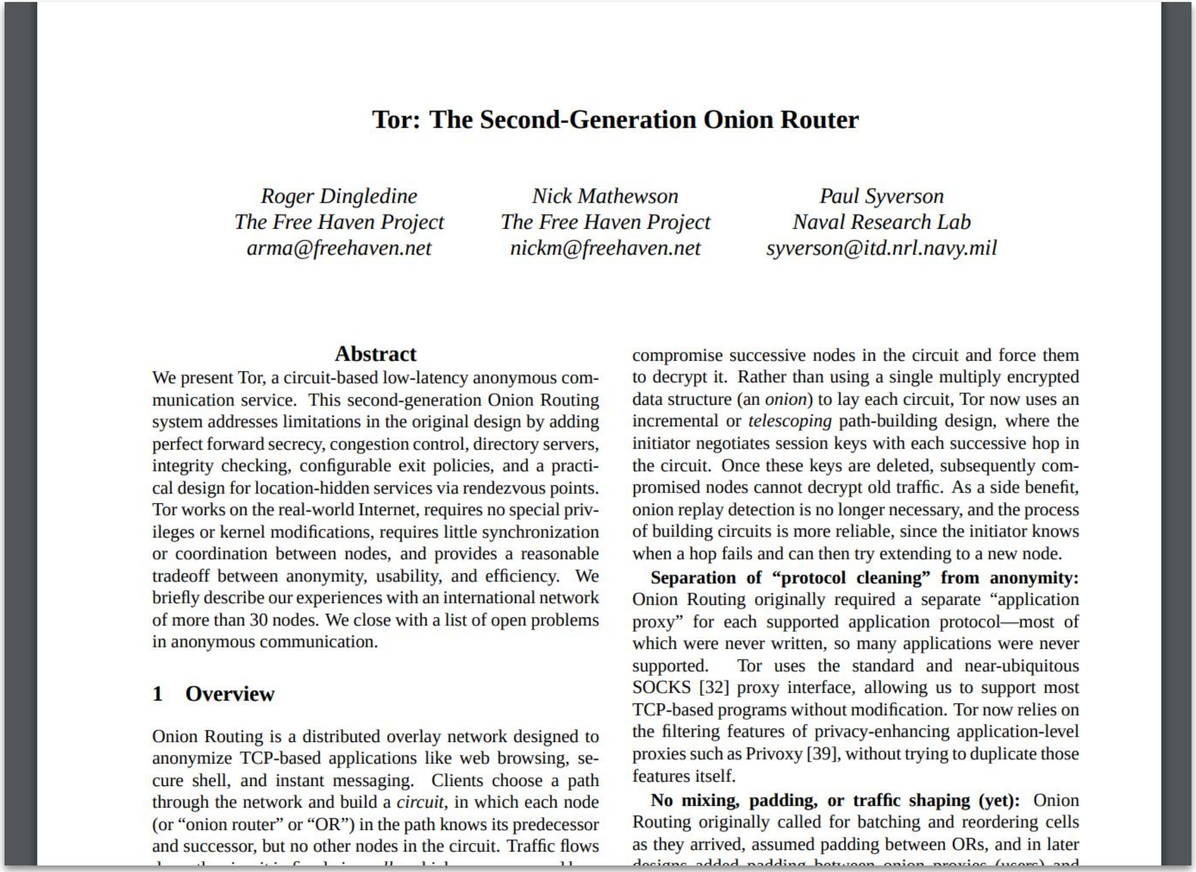
The Goal

- Build a system for Internet-based connections that can resist traffic analysis, eavesdropping, and other attacks



Illustrations from https://alicebobstory.com/

Then, in 2004…



Tor: The Second-Generation Onion Router

Roger Dingledine
The Free Haven Project
arma@freehaven.net

Nick Mathewson
The Free Haven Project
nickm@freehaven.net

Paul Syverson
Naval Research Lab
syverson@itd.nrl.navy.mil

Abstract

We present Tor, a circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency. We briefly describe our experiences with an international network of more than 30 nodes. We close with a list of open problems in anonymous communication.

1 Overview

Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging. Clients choose a path through the network and build a *circuit*, in which each node (or "onion router" or "OR") in the path knows its predecessor and successor, but no other nodes in the circuit. Traffic flows

compromise successive nodes in the circuit and force them to decrypt it. Rather than using a single multiply encrypted data structure (an *onion*) to lay each circuit, Tor now uses an incremental or *telescoping* path-building design, where the initiator negotiates session keys with each successive hop in the circuit. Once these keys are deleted, subsequently compromised nodes cannot decrypt old traffic. As a side benefit, onion replay detection is no longer necessary, and the process of building circuits is more reliable, since the initiator knows when a hop fails and can then try extending to a new node.

Separation of "protocol cleaning" from anonymity: Onion Routing originally required a separate "application proxy" for each supported application protocol—most of which were never written, so many applications were never supported. Tor uses the standard and near-ubiquitous SOCKS [32] proxy interface, allowing us to support most TCP-based programs without modification. Tor now relies on the filtering features of privacy-enhancing application-level proxies such as Privoxy [39], without trying to duplicate those features itself.

No mixing, padding, or traffic shaping (yet): Onion Routing originally called for batching and reordering cells as they arrived, assumed padding between ORs, and in later

Why am I telling this story?

Google
SUMMER
OF CODE
2009
code.google.com/soc

+

Tor®
TorProject.org

Ways to use Tor

- Browse anonymously using the Tor Browser
- Use the Tor Browser to access censored sites
- Share files securely using OnionShare
- Receive confidential news tips using SecureDrop
- Deploy websites with the Enterprise Onion Toolkit (EOTK)

Changing the narrative

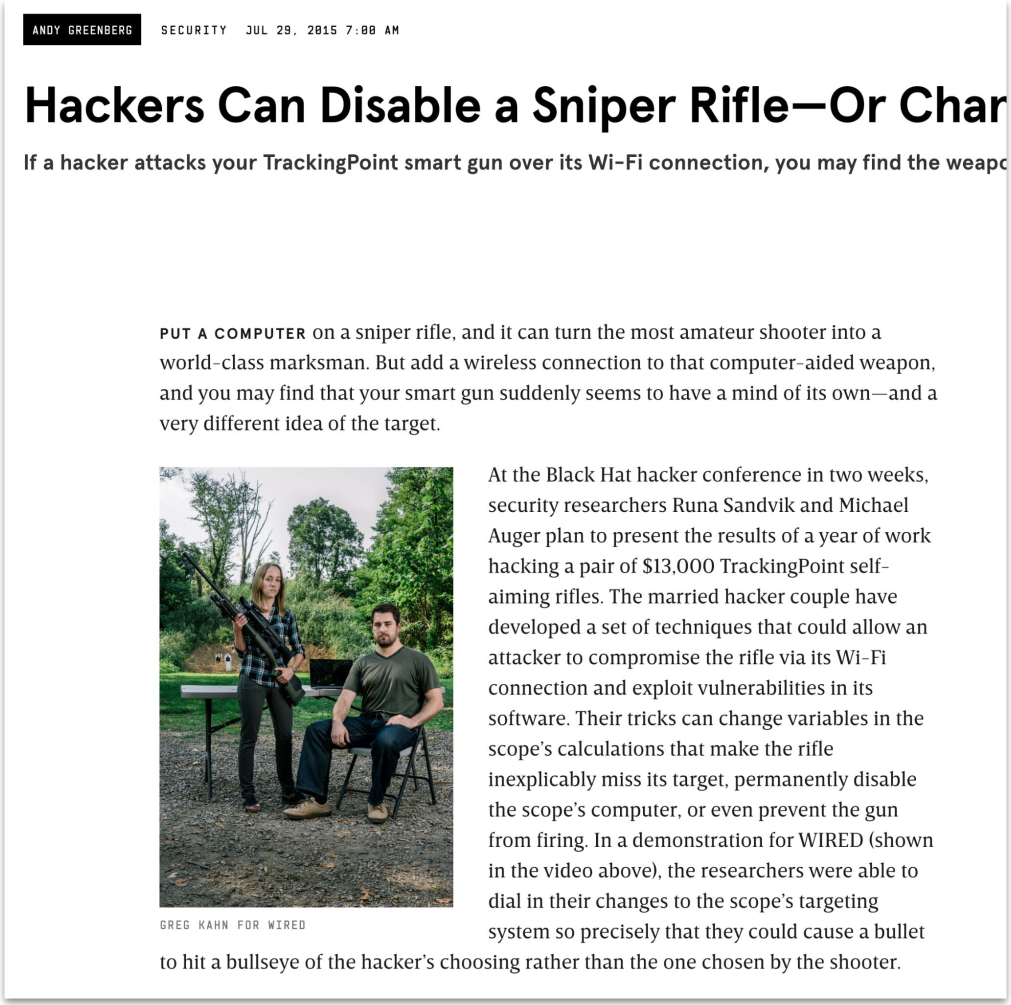
- From “nothing to hide” to “something to protect”
- Close your windows, lock your doors, encrypt everything
- End-to-end is becoming the new default (e.g. Signal, WhatsApp, FB)
- Bad people do bad things, but everybody deserves good security
- From hackers destroying the world, to changing it

Introducing Granitt

- Securing journalists and at-risk people around the world
- Being a journalist is more than a 9-5 (i.e. an *identity*)
- That work requires support from others (i.e. the *business*)
- How would you secure someone doing anti-corruption work?
- Great mission and big impact, plus curiosity and puzzles

What happens if…

2015 🙀



ANDY GREENBERG SECURITY JUL 29, 2015 7:00 AM

Hackers Can Disable a Sniper Rifle—Or Char

If a hacker attacks your TrackingPoint smart gun over its Wi-Fi connection, you may find the weapo

PUT A COMPUTER on a sniper rifle, and it can turn the most amateur shooter into a world-class marksman. But add a wireless connection to that computer-aided weapon, and you may find that your smart gun suddenly seems to have a mind of its own—and a very different idea of the target.

GREG KAHN FOR WIRED

At the Black Hat hacker conference in two weeks, security researchers Runa Sandvik and Michael Auger plan to present the results of a year of work hacking a pair of $13,000 TrackingPoint self-aiming rifles. The married hacker couple have developed a set of techniques that could allow an attacker to compromise the rifle via its Wi-Fi connection and exploit vulnerabilities in its software. Their tricks can change variables in the scope's calculations that make the rifle inexplicably miss its target, permanently disable the scope's computer, or even prevent the gun from firing. In a demonstration for WIRED (shown in the video above), the researchers were able to dial in their changes to the scope's targeting system so precisely that they could cause a bullet to hit a bullseye of the hacker's choosing rather than the one chosen by the shooter.

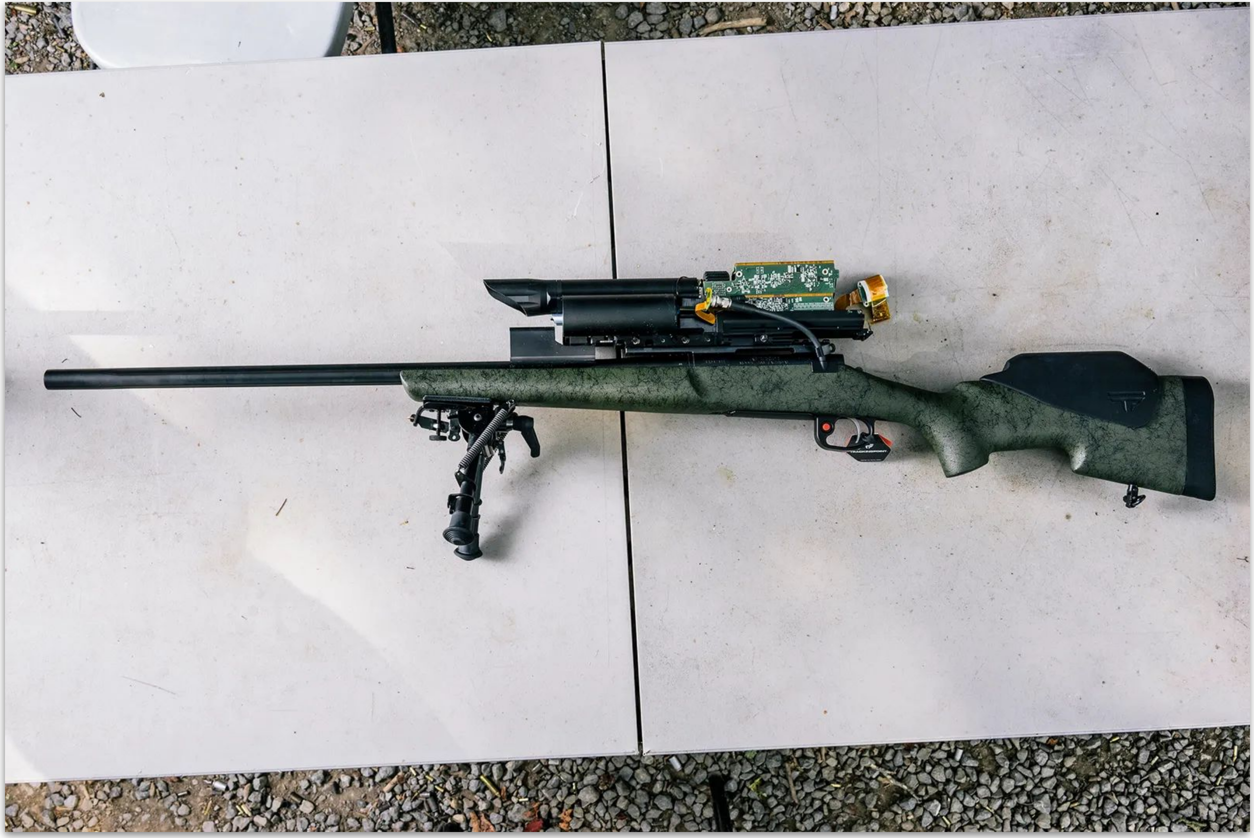
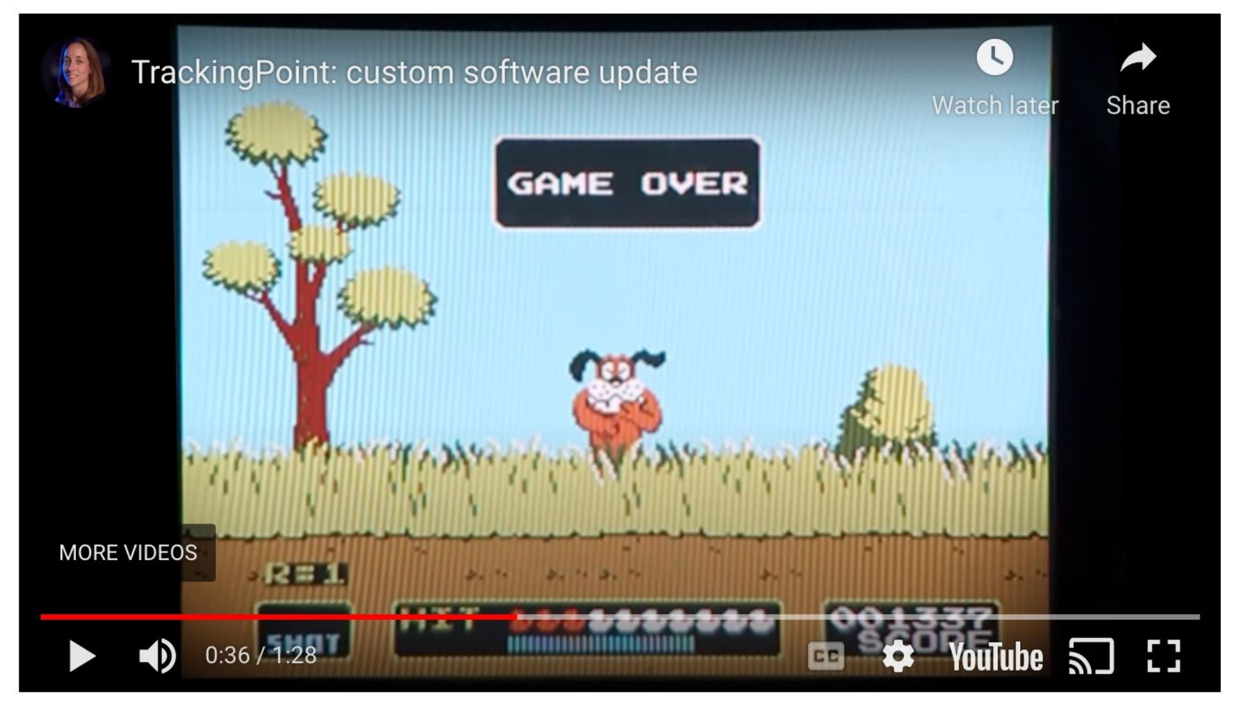
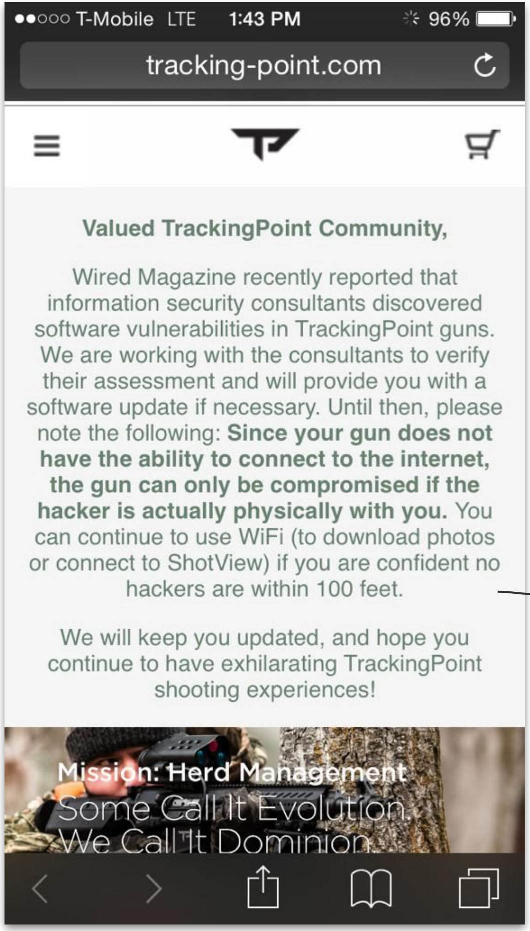


Photo by Greg Kahn for Wired

Not DOOM, but


TrackingPoint: custom software update
Watch later
Share
GAME OVER
MORE VIDEOS
R=1
HIT
SHOT
001337
SCORE
0:36 / 1:28
YouTube

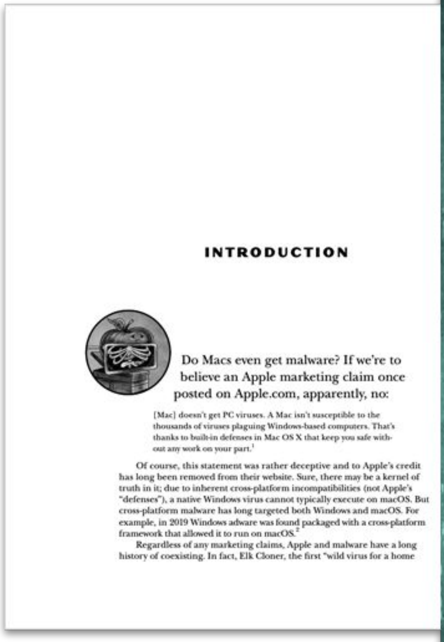


Valued TrackingPoint Community,

Wired Magazine recently reported that information security consultants discovered software vulnerabilities in TrackingPoint guns. We are working with the consultants to verify their assessment and will provide you with a software update if necessary. Until then, please note the following: **Since your gun does not have the ability to connect to the internet, the gun can only be compromised if the hacker is actually physically with you.** You can continue to use WiFi (to download photos or connect to ShotView) if you are confident no hackers are within 100 feet.

We will keep you updated, and hope you continue to have exhilarating TrackingPoint shooting experiences!

I wonder if…



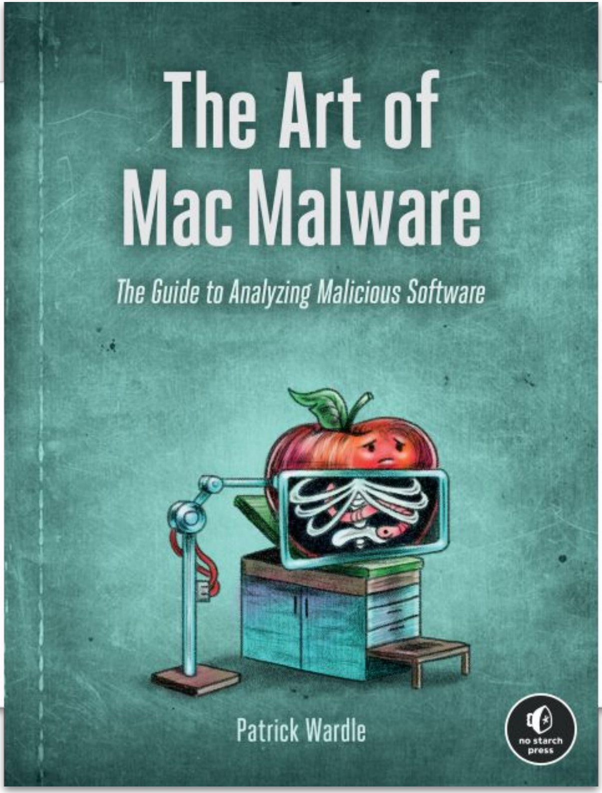
INTRODUCTION

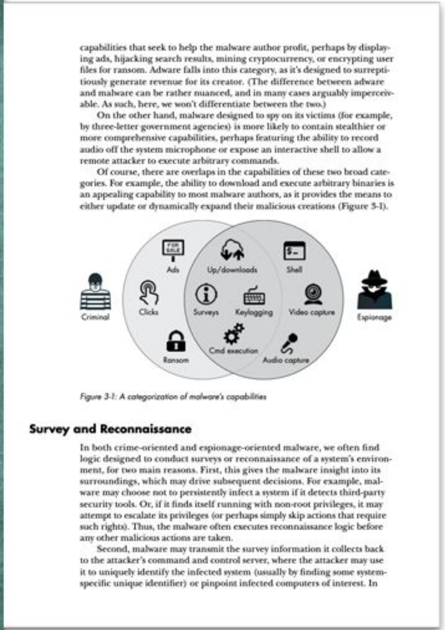
Do Macs even get malware? If we're to believe an Apple marketing claim once posted on Apple.com, apparently, no:

> [Mac] doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe without any work on your part.[1]

Of course, this statement was rather deceptive and to Apple's credit has long been removed from their website. Sure, there may be a kernel of truth in it; due to inherent cross-platform incompatibilities (not Apple's "defenses"), a native Windows virus cannot typically execute on macOS. But cross-platform malware has long targeted both Windows and macOS. For example, in 2019 Windows adware was found packaged with a cross-platform framework that allowed it to run on macOS.[2]

Regardless of any marketing claims, Apple and malware have a long history of coexisting. In fact, Elk Cloner, the first "wild virus for a home





capabilities that seek to help the malware author profit, perhaps by displaying ads, hijacking search results, mining cryptocurrency, or encrypting user files for ransom. Adware falls into this category, as it's designed to surreptitiously generate revenue for its creator. (The difference between adware and malware can be rather nuanced, and in many cases arguably imperceivable. As such, here, we won't differentiate between the two.)

On the other hand, malware designed to spy on its victims (for example, by three-letter government agencies) is more likely to contain stealthier or more comprehensive capabilities, perhaps featuring the ability to record audio off the system microphone or expose an interactive shell to allow a remote attacker to execute arbitrary commands.

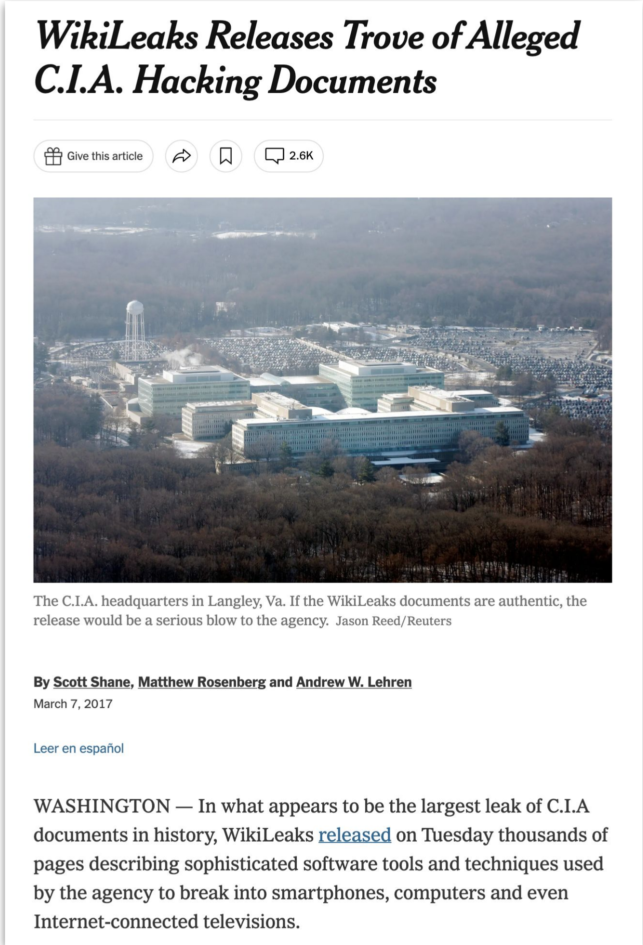
Of course, there are overlaps in the capabilities of these two broad categories. For example, the ability to download and execute arbitrary binaries is an appealing capability to most malware authors, as it provides the means to either update or dynamically expand their malicious creations (Figure 3-1).

Figure 3-1: A categorization of malware's capabilities

Survey and Reconnaissance

In both crime-oriented and espionage-oriented malware, we often find logic designed to conduct surveys or reconnaissance of a system's environment, for two main reasons. First, this gives the malware insight into its surroundings, which may drive subsequent decisions. For example, malware may choose not to persistently infect a system if it detects third-party security tools. Or, if it finds itself running with non-root privileges, it may attempt to escalate its privileges (or perhaps simply skip actions that require such rights). Thus, the malware often executes reconnaissance logic before any other malicious actions are taken.

Second, malware may transmit the survey information it collects back to the attacker's command and control server, where the attacker may use it to uniquely identify the infected system (usually by finding some system-specific unique identifier) or pinpoint infected computers of interest. In



WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents

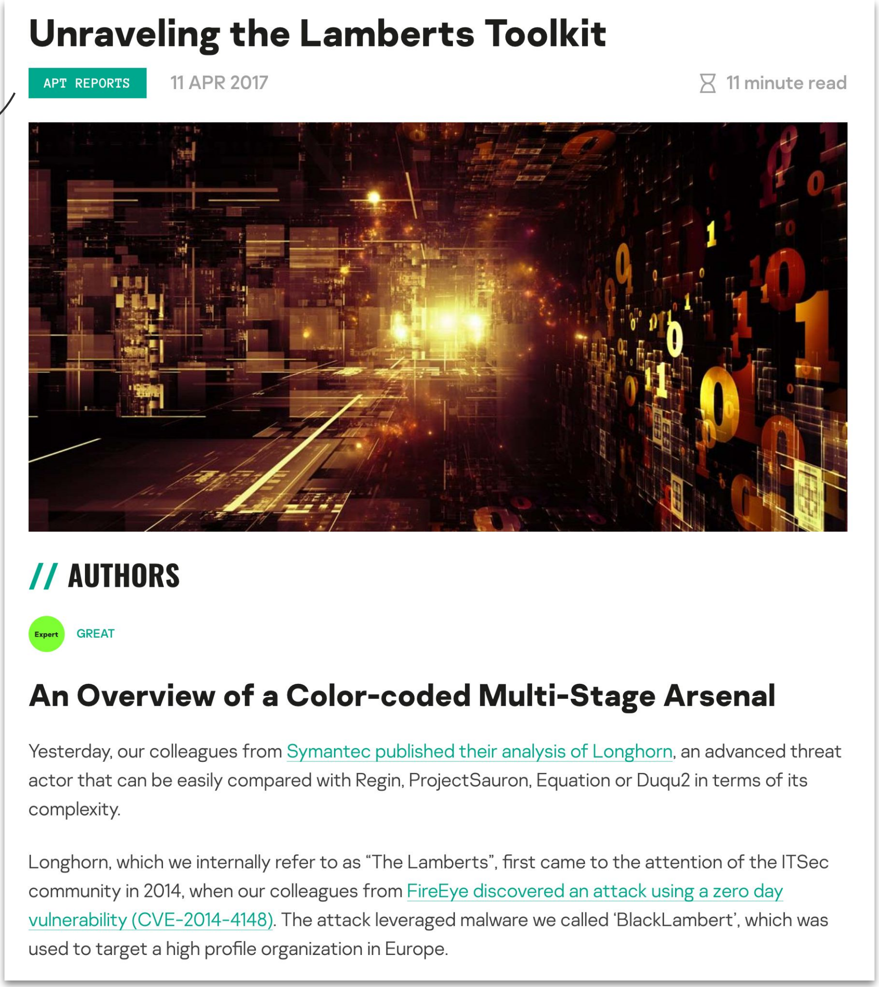
The C.I.A. headquarters in Langley, Va. If the WikiLeaks documents are authentic, the release would be a serious blow to the agency. Jason Reed/Reuters

By Scott Shane, Matthew Rosenberg and Andrew W. Lehren
March 7, 2017

Leer en español

WASHINGTON — In what appears to be the largest leak of C.I.A documents in history, WikiLeaks released on Tuesday thousands of pages describing sophisticated software tools and techniques used by the agency to break into smartphones, computers and even Internet-connected televisions.

A month later



Unraveling the Lamberts Toolkit

APT REPORTS 11 APR 2017 11 minute read

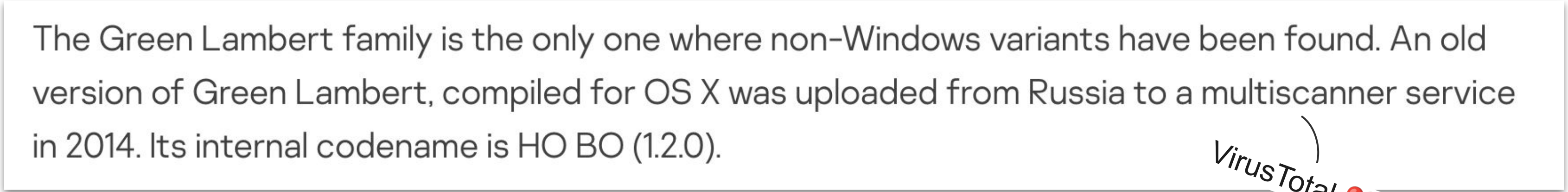
// AUTHORS

Expert GREAT

An Overview of a Color-coded Multi-Stage Arsenal

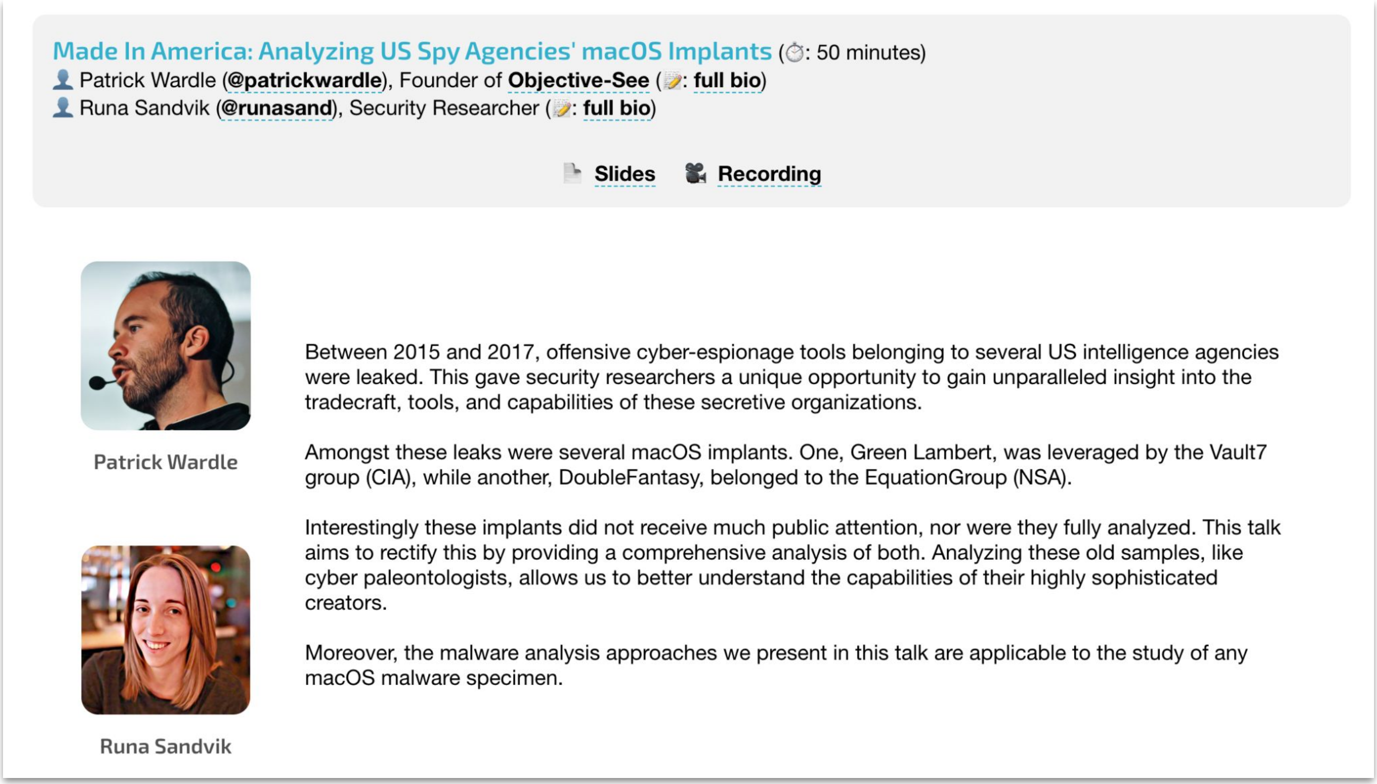
Yesterday, our colleagues from Symantec published their analysis of Longhorn, an advanced threat actor that can be easily compared with Regin, ProjectSauron, Equation or Duqu2 in terms of its complexity.

Longhorn, which we internally refer to as "The Lamberts", first came to the attention of the ITSec community in 2014, when our colleagues from FireEye discovered an attack using a zero day vulnerability (CVE-2014-4148). The attack leveraged malware we called 'BlackLambert', which was used to target a high profile organization in Europe.



The Green Lambert family is the only one where non-Windows variants have been found. An old version of Green Lambert, compiled for OS X was uploaded from Russia to a multiscanner service in 2014. Its internal codename is HO BO (1.2.0).

VirusTotal ❤️



Made In America: Analyzing US Spy Agencies' macOS Implants (⏱: 50 minutes)
👤 Patrick Wardle (**@patrickwardle**), Founder of **Objective-See** (📝: **full bio**)
👤 Runa Sandvik (**@runasand**), Security Researcher (📝: **full bio**)

📄 **Slides** 🎥 **Recording**

Patrick Wardle

Runa Sandvik

Between 2015 and 2017, offensive cyber-espionage tools belonging to several US intelligence agencies were leaked. This gave security researchers a unique opportunity to gain unparalleled insight into the tradecraft, tools, and capabilities of these secretive organizations.

Amongst these leaks were several macOS implants. One, Green Lambert, was leveraged by the Vault7 group (CIA), while another, DoubleFantasy, belonged to the EquationGroup (NSA).

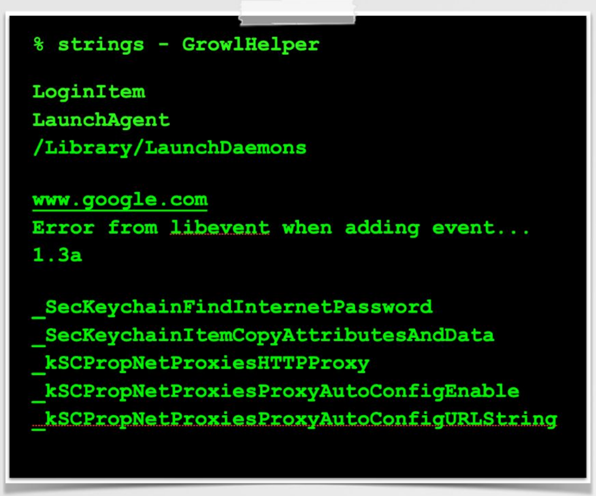
Interestingly these implants did not receive much public attention, nor were they fully analyzed. This talk aims to rectify this by providing a comprehensive analysis of both. Analyzing these old samples, like cyber paleontologists, allows us to better understand the capabilities of their highly sophisticated creators.

Moreover, the malware analysis approaches we present in this talk are applicable to the study of any macOS malware specimen.

Objective By The Sea v4.0

Strings

A few clues



```
% strings - GrowlHelper

LoginItem
LaunchAgent
/Library/LaunchDaemons

www.google.com
Error from libevent when adding event...
1.3a

_SecKeychainFindInternetPassword
_SecKeychainItemCopyAttributesAndData
_kSCPropNetProxiesHTTPProxy
_kSCPropNetProxiesProxyAutoConfigEnable
_kSCPropNetProxiesProxyAutoConfigURLString
```

embedded strings

----> Options for gaining persistence

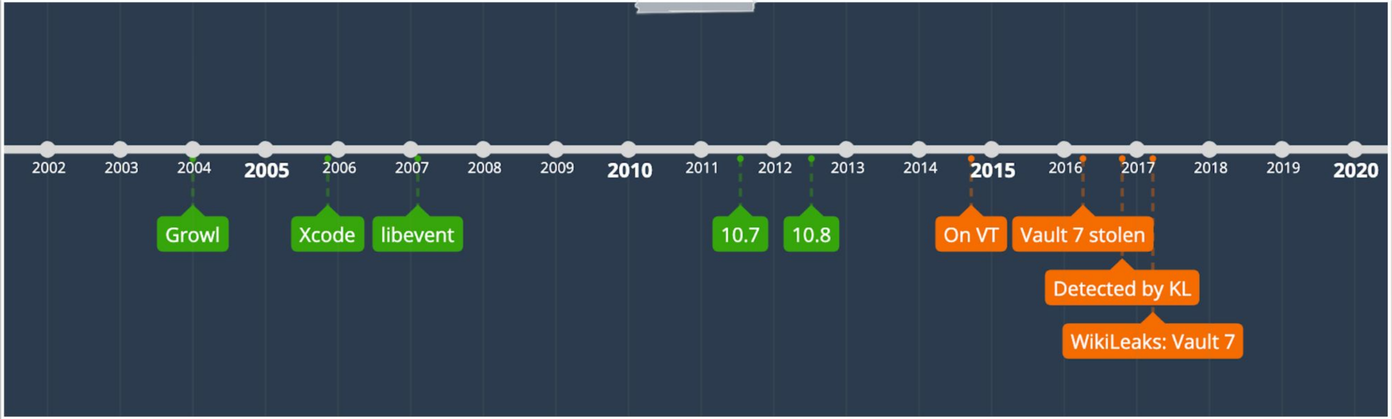
----> Event notification library, used in Tor, v. 1.3a released in Feb 2007

----> Auto-determines proxy settings

----> Xcode 2.2, released in Nov 2005

DEV/USE TIMELINE

2007 - 2013 (??)

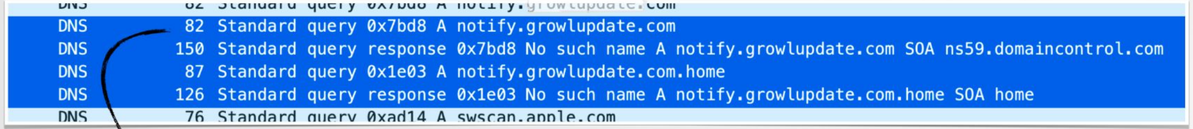


Matches timeline of activity from Kaspersky

Using an old laptop from eBay

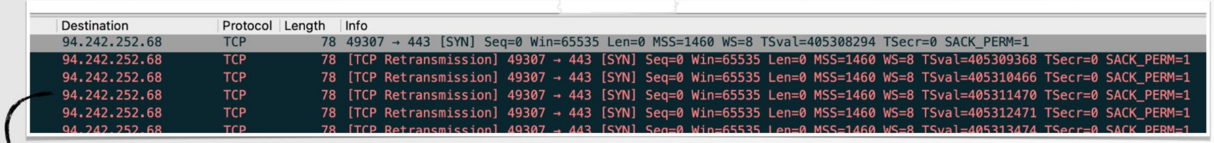
Network traffic

tcpdump + Wireshark



```
DNS      82 Standard query 0x7bd8 A notify.growlupdate.com
DNS      82 Standard query 0x7bd8 A notify.growlupdate.com
DNS     150 Standard query response 0x7bd8 No such name A notify.growlupdate.com SOA ns59.domaincontrol.com
DNS      87 Standard query 0x1e03 A notify.growlupdate.com.home
DNS     126 Standard query response 0x1e03 No such name A notify.growlupdate.com.home SOA home
DNS      76 Standard query 0xad14 A swscan.apple.com
```

Looks like a hostname! 🙀



```
Destination        Protocol  Length  Info
94.242.252.68      TCP           78  49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405308294 TSecr=0 SACK_PERM=1
94.242.252.68      TCP           78  [TCP Retransmission] 49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405309368 TSecr=0 SACK_PERM=1
94.242.252.68      TCP           78  [TCP Retransmission] 49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405310466 TSecr=0 SACK_PERM=1
94.242.252.68      TCP           78  [TCP Retransmission] 49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405311470 TSecr=0 SACK_PERM=1
94.242.252.68      TCP           78  [TCP Retransmission] 49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405312471 TSecr=0 SACK_PERM=1
94.242.252.68      TCP           78  [TCP Retransmission] 49307 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=405313474 TSecr=0 SACK_PERM=1
```

And the IP address 🎉

Not all APTs and 0days

tl;dr

- Do things you enjoy **and**
- Do things you don't know how to do
- Ask for help
- GSoC is still a thing!
- Check out The Tor Project && OONI

Thank You!

Runa Sandvik - Founder - Granitt
@runasand - glitch-cat.com - granitt.io

Resources

- https://www.onion-router.net/
- https://www.torproject.org/
- https://summerofcode.withgoogle.com/
- https://onionshare.org/
- https://securedrop.org/
- https://github.com/alecmuffett/eotk
- https://granitt.io
- https://taomm.org/
- https://objectivebythesea.org/
- https://objective-see.org/blog/blog_0x68.html