

Adversary Resistant Computing

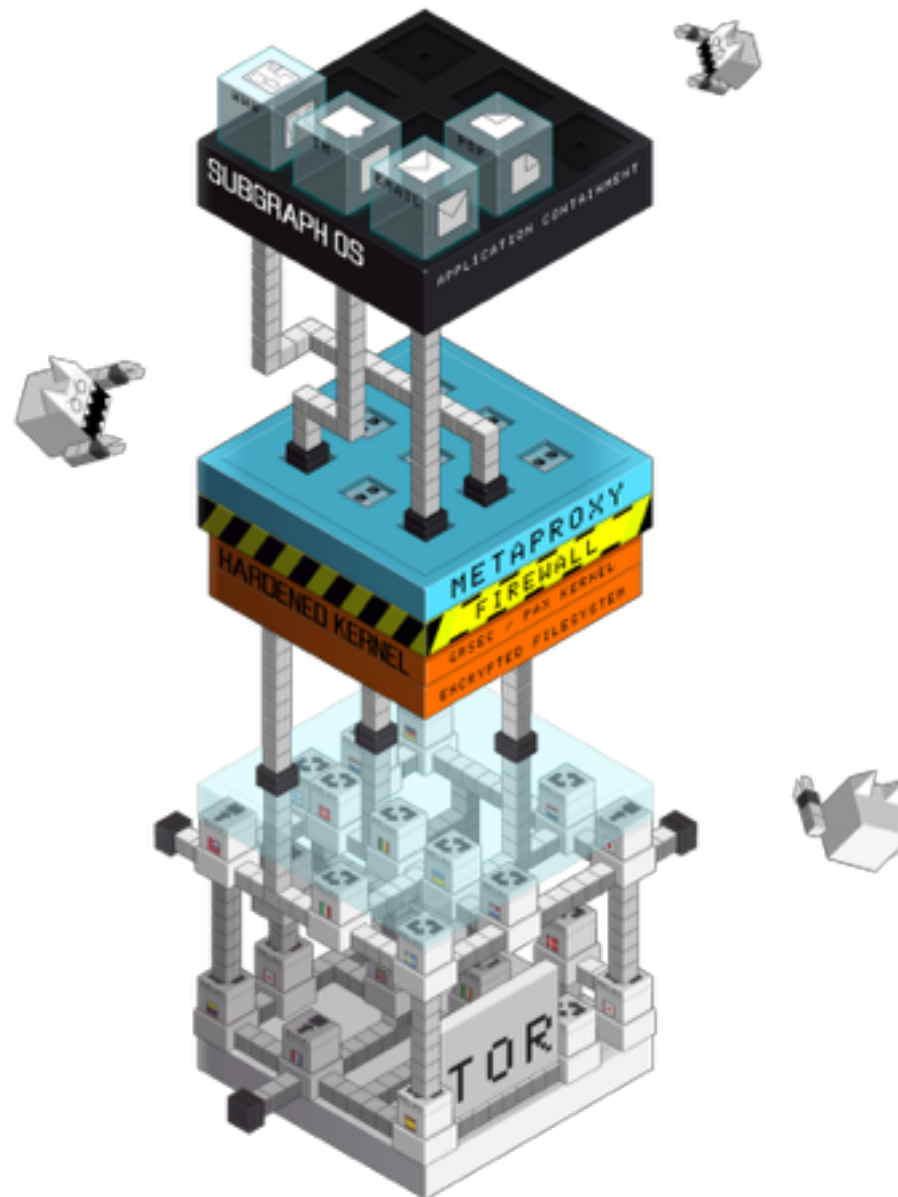
David Mirza Ahmad, Subgraph
Montreal



"THEN CAME A TREMENDOUS BLOW; THEN A FOOT WAS SEEN FORCING ITS WAY OVER THE DOORSILL."—p. 85.

Who We Are

- Montreal-based security technologists and privacy researchers
 - Offensive security
 - Development of privacy software
 - Anti-censorship work
- Currently working on:
 - Usable privacy and security tools
 - Subgraph OS
 - Subgraph Mail
 - Nyms.io



Adversary Resistant Computing

Resistance to network-borne,
targeted attacks.

What are Targeted Attacks?

- Target Identification & Location
 - Open source intelligence, social engineering
- Exploitation
 - Payload typically, but not always, delivered by web or email
 - Exploitation of a software vulnerability in browser, browser plugin, email client, document viewer.. can be zero-day (unpublished), or not.
- Implantation
 - Post exploitation installation of malware known as a RAT, “remote access tool”
 - Also known as backdoors, rootkits, Trojan Horses, etc

Timeline of a Targeted Attack

- Obtain target email address or locate a target 'watering hole' (a website target visits)
- Send social engineering email content with bad attachment or link to website with browser exploit
 - "Spearphishing"
 - Or just embed exploit and payload in target's 'watering hole'
 - Can rely on exploit to deliver payload, but often this is not even necessary
- RAT implantation and data exfiltration
 - Does not require escalating privileges. Especially on a single user desktop system
- Lateral movement from target to extend the breach

The Objective of RAT Implantation

- Long-term surveillance: tracking and monitoring the target's activities, communication, movement
- Data exfiltration
- Persistent remote access
- Against an organization:
 - Establish a beachhead, and then extend the breach laterally
 - Exploitation of trust relationships to “pivot” from the initial target
 - E.g. collect their private crypto keys, system passwords to extend compromise



Year of the RAT: China's malware war on activists goes mobile

Is the Chinese government spying on Hong Kong protesters' phones?

(ars technica)

Rat image:
yves_guillou

Targeted Attacks: Journalists

- Ethiopian journalists targeted for surveillance using malware
- Alleged tool used is available commercially

Journalists, media under attack from hackers: Google researchers

BY JEREMY WAGSTAFF

SINGAPORE | Fri Mar 28, 2014 5:48am EDT

Tweet



136



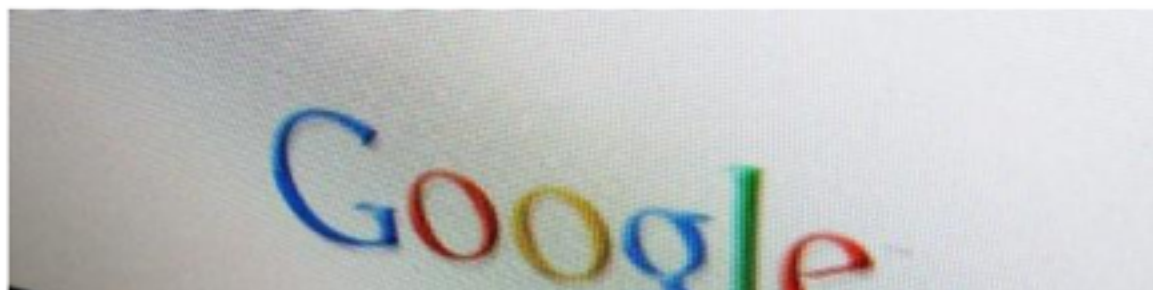
Share this



Email



Print



Targeted Attacks: Journalists

Governments spy on journalists with weaponized malware – WikiLeaks

Published time: September 16, 2014 10:36

[Get short URL](#)



Reuters/Phil McCarten

Targeted Attacks: Journalists

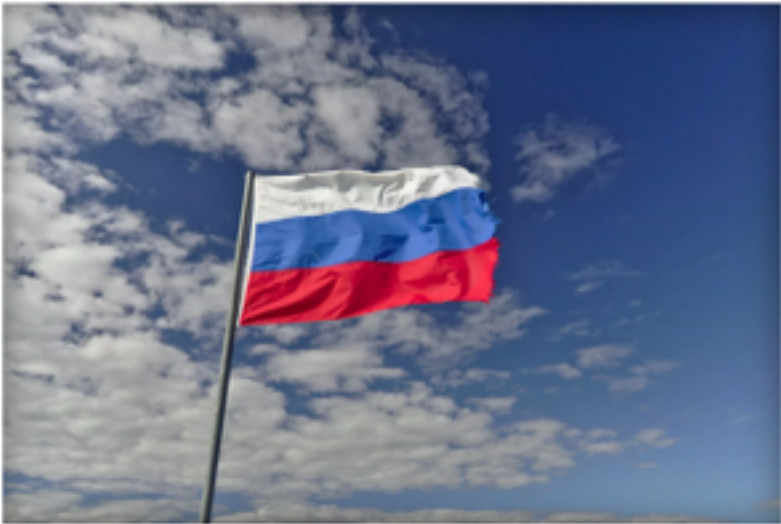


“Seven-year malware campaign”

US & WORLD

A new report ties the Russian government to a seven-year malware campaign

By **Russell Brandem** on September 17, 2015 6:00 am [Email](#) [@russellbrandem](#)





(Ondrej Dohus / Flickr)



Targeted Attacks: Activists

Topic: [Security](#)


Follow via:  

'Lame' Mac malware finds success in spearphishing

Summary: Barely concealed security threat found on activist's Mac.



By [liam tung](#) | May 17, 2013 -- 12:36 GMT (13:36 BST)

 Follow @ZDNET

209K followers

[Get the ZDNet Security newsletter now](#)

Comments

0

 Share on Facebook

0

 Tweet

0

 Share

more +

Security researchers have found a new but technically lame piece of Mac malware that has been used to spy on activists.

Security researcher Jacob Appelbaum recently discovered the malware on the Mac of an Angolan activist. He used the case to discuss security with activists from across the globe at the [Oslo Freedom Forum](#) in Norway this week.

Targeted Attacks: Activists

Syrian Cyber-Attacks Expose Activists, Firms to Malware Infection

By [Robert Lemos](#) | Posted 2014-08-20  [Print](#)

 [Twitter](#)  [LinkedIn](#)  [Like](#) [33](#)  [Share](#) [3](#)  [Share](#)  [Email](#)



Hacking groups operating from Syria, Russia and Lebanon have targeted activists on both sides of the Syrian civil war with malware campaigns, says security firm Kaspersky.

Groups of attackers have targeted activists on both sides of the Syrian civil war with a new malware campaign that, while not particularly sophisticated, has grown to compromise more than 10,000 systems, according to researchers from Kaspersky Labs, which analyzed more than 100 files used by group.

Who has the capability?

- Nation states have vast resources and can passively monitor network traffic, stockpile exploits, develop or acquire custom malware
- Very easy for an adversary to obfuscate itself as the source for attacks, low risk even if detected
- Risk and opportunity cost are low for many would-be adversaries
 - Means this is a high risk for potential targets

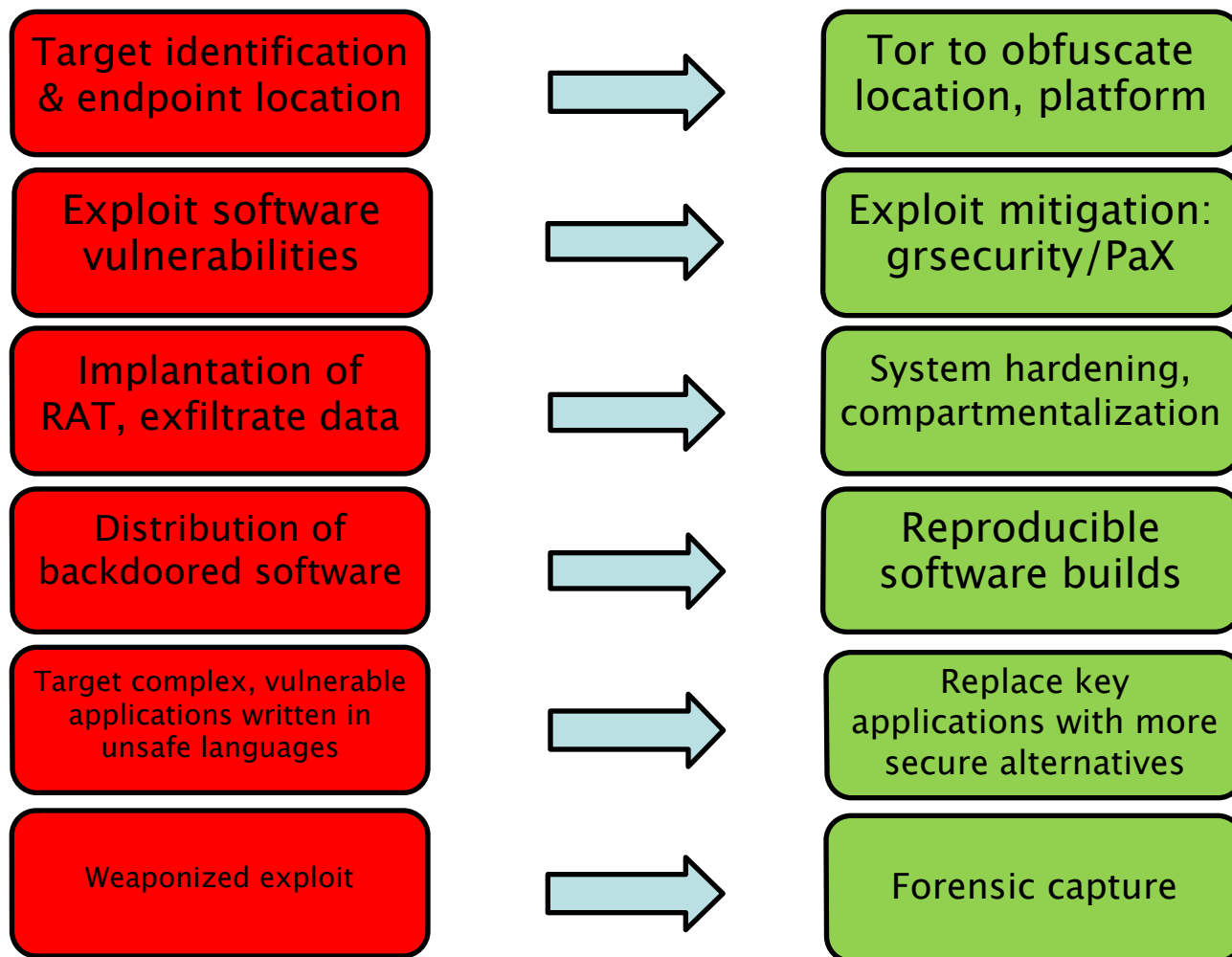
Grey Market

- Adversaries need not exclusively be nation states
- “Grey market” for surveillance malware and the exploits used to deliver them
- Several companies around the world selling:
 - Exploits for published or unpublished vulnerabilities ideal for RAT delivery
 - Custom RATs
- Customers alleged to be ‘good governments’, law enforcement agencies
 - But who knows who is buying this stuff?

Countermeasures

- Awareness, adherence to best practices?
 - Don't open files sent to you in email from strangers
 - It's not hard to spoof email, and a little open source intelligence goes a long way in making an unfriendly email look friendly
- Patching vulnerabilities?
 - Doesn't prevent exploitation of zero-day vulnerabilities
 - Total attack surface: many layers where vulnerabilities can exist
 - Could be the mail client, the browser, document viewer, image viewer..
 - Not all applications patch reliably, quickly, or at all
- Run anti-virus?
 - Typical signature-based detection ineffective against sophisticated, custom RATs
 - Anti-virus can itself have exploitable vulnerabilities..
- We need to do better.
 - It should be possible to safely open an email!

Raising the cost of targeted attacks.



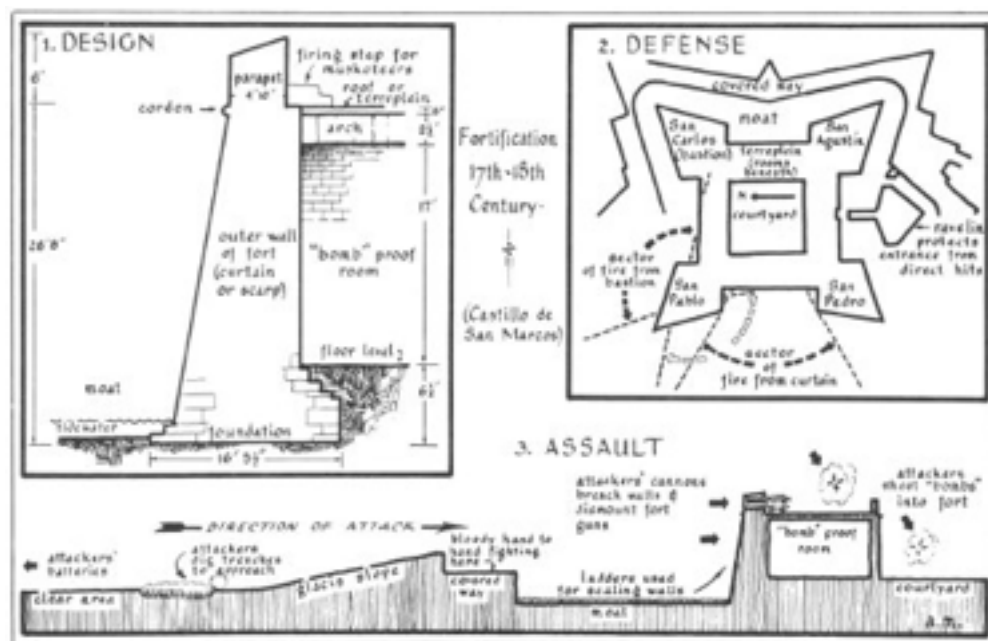
Effective technology countermeasures exist that accomplish this.

Addressing Targeted Attacks

- Obfuscate network, platform location
 - Prevent the adversary from knowing your location, and the location of your endpoint system
 - Prevent the adversary from determining the platform of your endpoint
 - Using Tor, privacy enhanced clients like Tor Browser, Torbirdy, etc, can help accomplish this
- Make certain classes of vulnerabilities difficult to exploit reliably
 - Assume zero-day vulnerabilities exist
 - Implement system-wide anti-exploitation technologies: on Linux, this includes grsecurity and PaX kernel patches
 - Reduce attack surface: run fewer applications, ensure those that are used are as trustworthy as possible
- Contain the impact of application breaches that do occur
 - Compartmentalize the system
 - Isolate applications from one another
 - Restrict their access to what is minimally required

Addressing Targeted Attacks

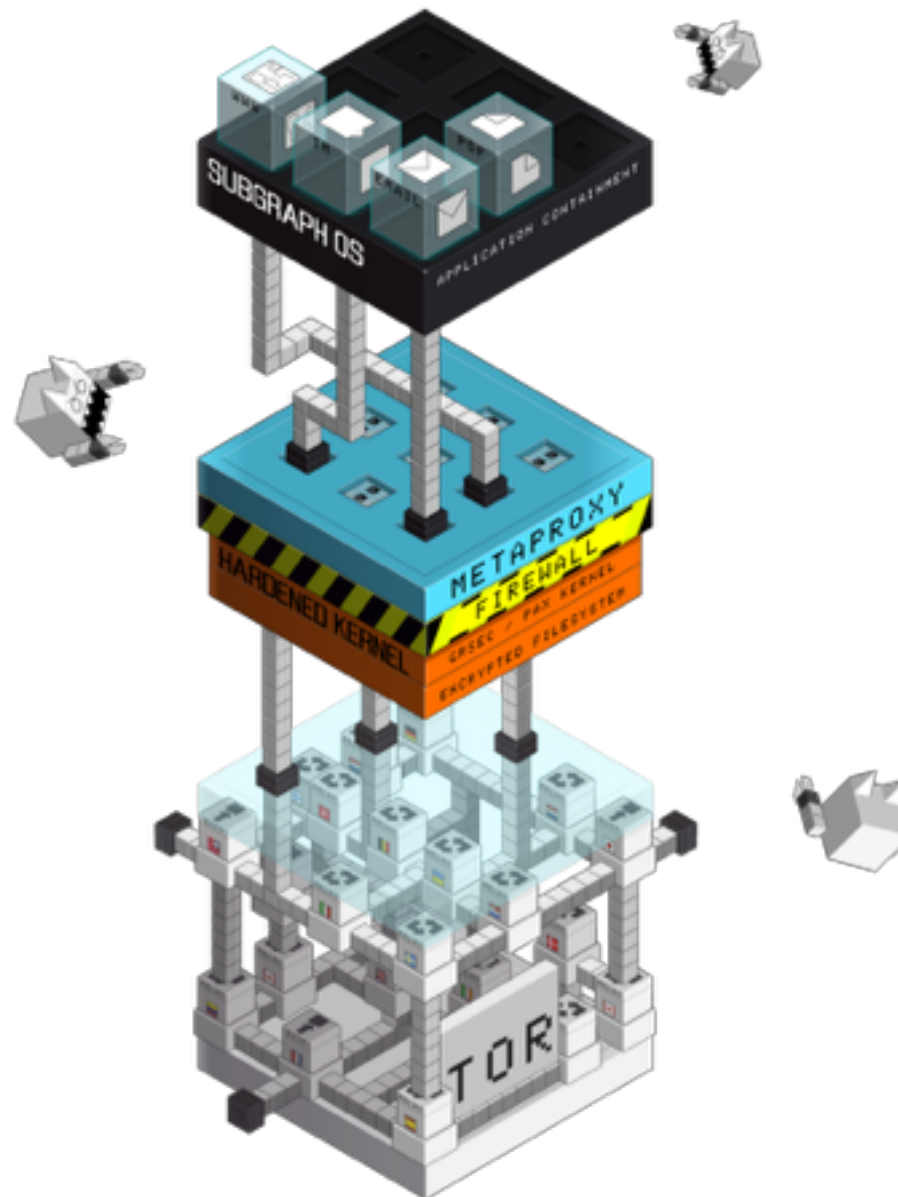
- Reduce set of installed software
- Strengthen distribution of packages
- Certain key applications probably need to be replaced
 - Making secure email easier to use
 - Email clients are highly complex, lots of attack surface in their many features
 - Written in dangerous programming languages (C, C++) where serious vulnerabilities are common
 - Secure desktop instant messaging has similar problems



Addressing Targeted Attacks

- Forensic capture
- Exploits cost money (time, money)
- RATs have a cost (time, money)
- Detection of RATs and exploits means they won't work anymore; early detection is a liability
- The risk of exploit/RAT loss is part of the adversary's deployment calculus
- Adversaries rely on relative low likelihood of detection:
 - Successful or failed exploit attempts
 - Deployed RATs
 - Material traces left behind
- Raising likelihood of detection will deter deployment
 - If the adversary does not know what the target platform is, and if there is a chance platform will compromise their tools
 - They may deploy more carefully, i.e., less frequently
 - **This benefits users on all platforms**





What is Subgraph OS?

- Linux distribution, based on Debian stretch
- Subgraph package for kernel + grsecurity
- Oz, a desktop application isolation framework
- Metaproxy
- Paxrat
- Application firewall
- Macouflauge
- Installable and runnable as a live disk

Subgraph OS: Where are we today?

- Announced a little over a year ago (spring 2014)
- Slow start due to self-funding, but support from the Open Technology Fund has helped us move faster
- Progress in the first four months of OTF support:



◆Milestones:

- ◆Alpha SGOS with integrated:
 - ◆Hardened kernel
 - ◆Oz
 - ◆Metaproxy
 - ◆Subgraph Firewall
 - ◆Paxrat
- ◆Basic project infrastructure
- ◆Distribution to alpha-stage users
- ◆Alpha release: March 11, 2016

What's on the roadmap?

- Lots of testing, bugfixing, improving performance and user experience
- Harvester
 - Forensic capture if “strange events” occur, e.g. browser just vanishes while using Tor
 - Active tor circuits and exit nodes
 - Volatile data about the process
 - Software bug? Exploit attempt? Cosmic rays?
- Installer
- Localization
- UI enhancements and customizations
- Support for other architectures
- Very good documentation and community support

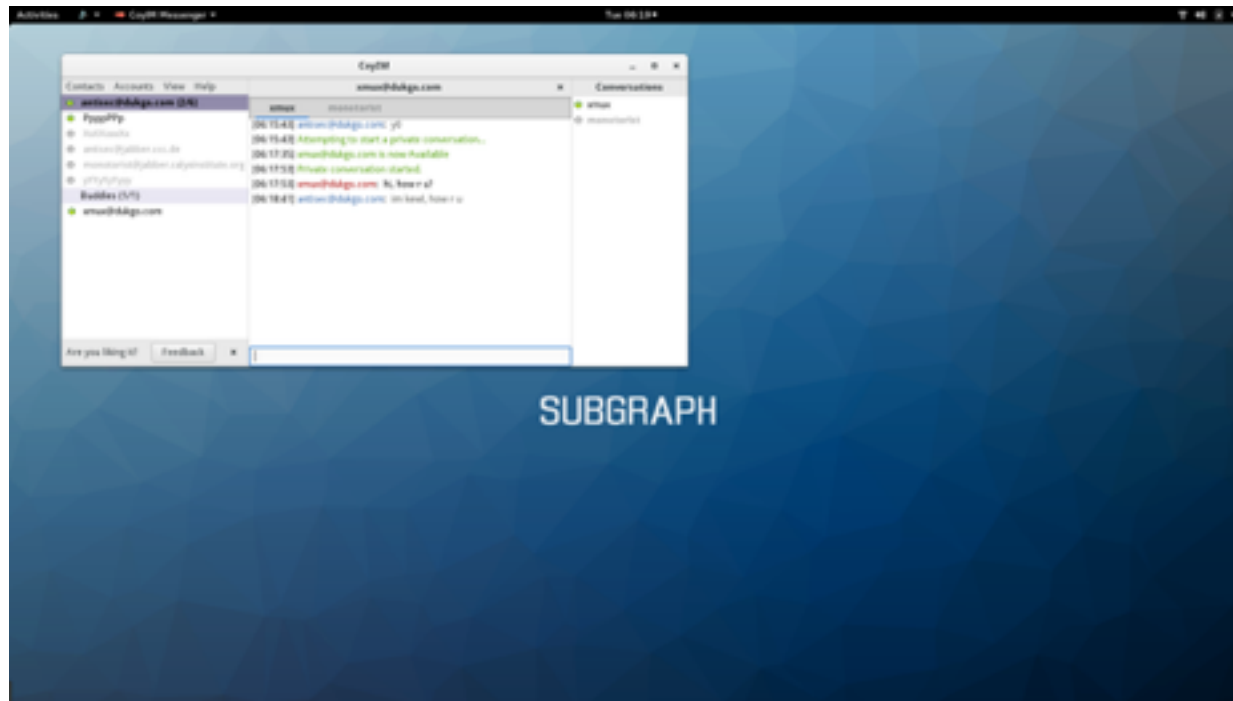
Vision: a platform for communication

- Mail
 - Subgraph OS will likely ship at first with Thunderbird + Torbirdy + Enigmail
 - This is not ideal for us for a number of reasons
 - Ancient, large, complex codebase
 - No longer well maintained
 - Not structured in a way that permits us to compartmentalize well
 - Interaction with GnuPG doesn't leave us feeling secure
 - Today email on the endpoint is at risk
 - We want to one day write a secure email client that can be compartmentalized and more resistant to client-side exploitation
- IM
 - CoyIM

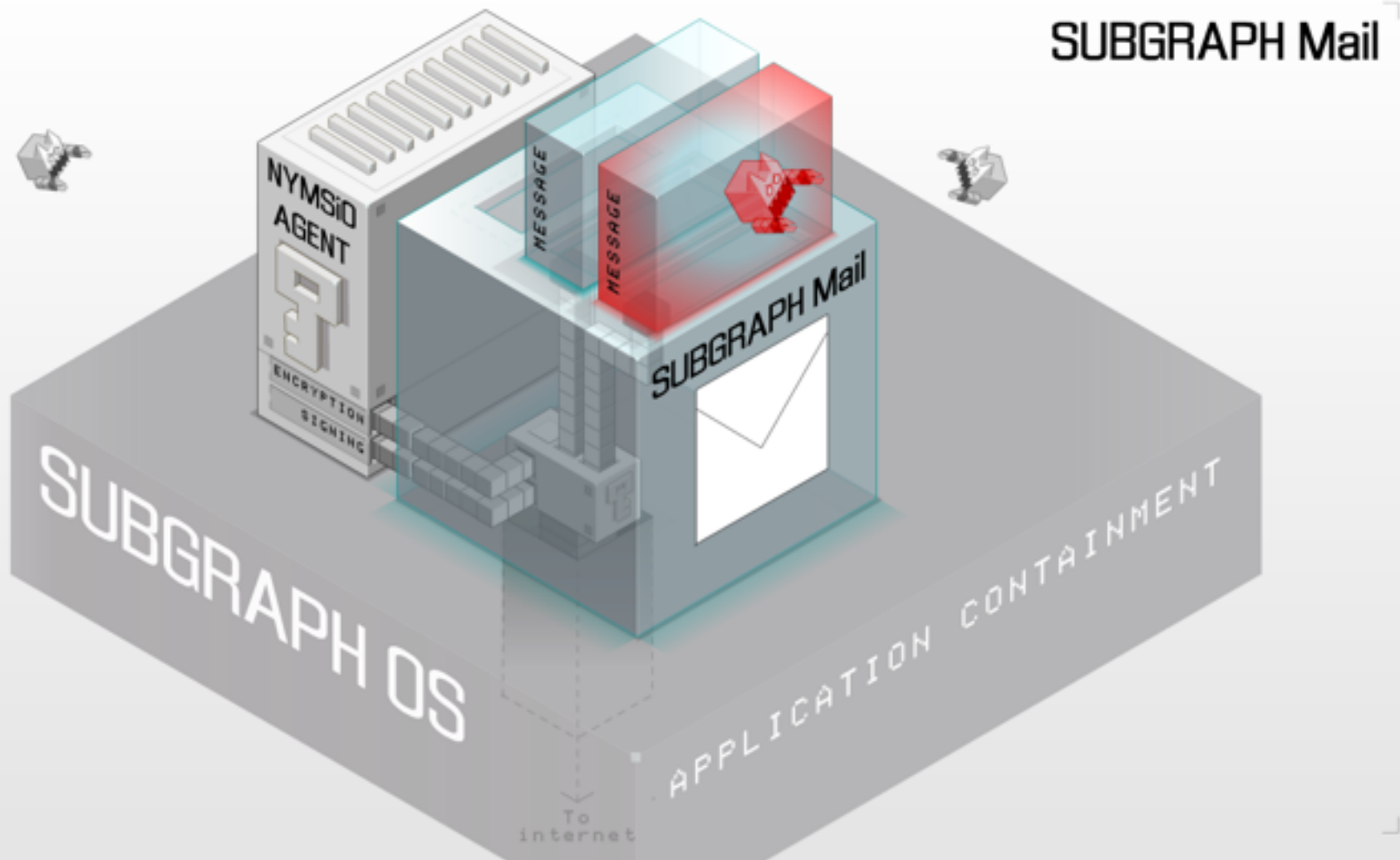
CoyIM

- Replace Pidgin / libpurple
 - Written in memory unsafe language
 - Security vulnerabilities not fixed quickly enough
 - Does too many things, too much attack surface
- Coy
 - ThoughtWorks Strike Team project
 - Written in Golang
 - Replaces Pidgin in Subgraph OS
 - Subgraph has contributed and will continue to do so
 - Single window, multi-conversation UI

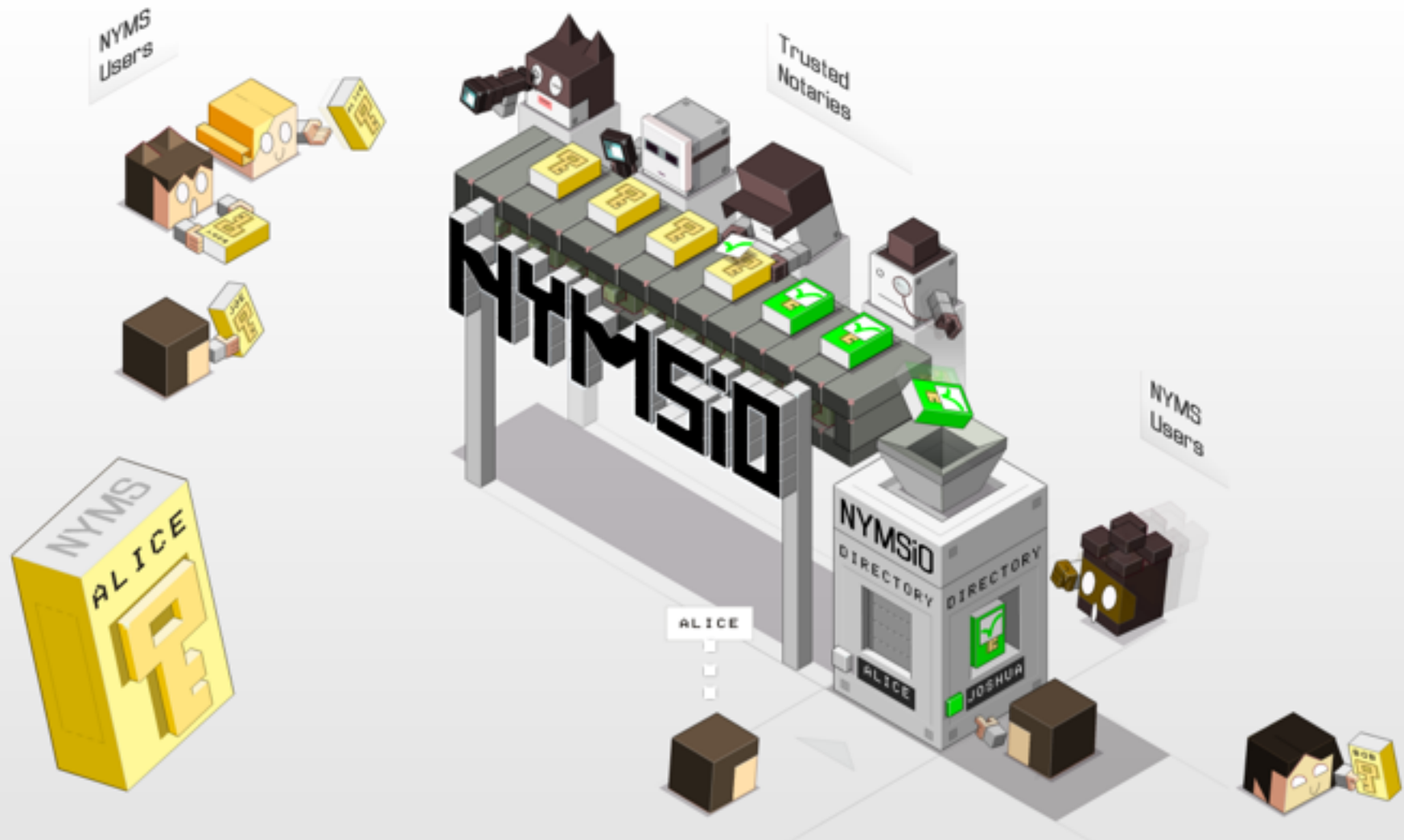
Coy



Mail



Nyms.io



Thanks

<https://subgraph.com>

@subgraph

info@subgraph.com



"THEN CAME A TREMENDOUS BLOW; THEN A FOOT WAS SEEN FORCING ITS WAY OVER THE DOORSILL."—p. 85.

Appendix: Oz

With Oz



Appendix: Attribution

Where not stated: Various B&W images from content hosted by Project Gutenberg. They do great work, thanks.

What's on the roadmap?

- Lots of testing, bugfixing, improving performance and user experience
- Harvester
 - Forensic capture if “strange events” occur, e.g. browser just vanishes while using Tor
 - Active tor circuits and exit nodes
 - Volatile data about the process
 - Software bug? Exploit attempt? Cosmic rays?
- Installer
- Localization
- UI enhancements and customizations
- Support for other architectures
- Very good documentation and community support