OPSEC
IN THE AGE OF THE
EGOTISTICAL GIRAFFE

the grugq <the.grugq@gmail.com>
@thegrugq
EGOTISTICAL GIRAFFE

- 0day exploit against Firefox browser
- Targeted at Tor Browser Bundle users
- Similar to FBI Freedom Hosting malware
- Use a P.O.R.T.A.L.
QUESTIONS?
• Contextualizing 0day
• Lessons Learned
• Mobile Matters
• Tranquil Transmissions
CYBER CONTEXTUALIZING 0DAY
“Your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents.”

—Brian Snow, NSA Information Assurance Director
NOT EVERYTHING REQUIRES 0DAY
A FUNCTION OF SECURITY POSTURE AND ATTACK SURFACE
DON’T REALLY NEED 0DAY
PROBABLY DON’T NEED 0DAY
INDIVIDUALS
MIGHT NEED 0DAY, DEPENDS
NOT EVERYTHING WARRANTS 0DAY
^ DEFINITELY GETTING 0DAY
Phil Venables
@philvenables

Attackers have bosses and budgets too.
ATTACKERS HAVE FINITE RESOURCES
0DAY ARE EXPENSIVE
DOH!DAY ARE CHEAP
0LDAY ARE FREE
ATTACKERS NEED RESULTS
“If it's stupid but it works, it's not stupid”

–Murphy’s Laws of War
USE PUBLICLY AVAILABLE ATTACK TOOLS MADE BY OTHERS

GET LABELED A 'SOPHISTICATED' THREAT

WHAT IF THE SOPHISTICATED ATTACKERS WHO USE COMMONLY AVAILABLE TOOLS CAN'T ACTUALLY DO ANYTHING BETTER?
ENTERPRISE SECURITY

• Attack surface is too big
• Trust relationships too diverse and complex
• Security posture inconsistent
• Essentially unsolvable
• Compartment and secure something smaller
LESSONS LEARNED
DUDES!
I FINALLY FINISHED MY LIST OF ERRORS!
CHECK IT OUT!

MY LIST:
-nope

FEELS SO GOOD!
CONFIRMING THAT I'VE BEEN IN THE RIGHT ON EVERY SINGLE OCCASION?

SUPER LIBERATING!
WORSE THAN WE THOUGHT
IF YOU DEPEND ON YOUR DEFENSES BEING PERFECT

YOU'RE GONNA HAVE A BAD TIME
BECAUSE VUPEN
OPSEC STILL WORKS
IF YOU DO IT PROPERLY
TAKE THAT NSA!

PRIVATE BROWSING!
C'mon son

Rule number one; never trust anybody
Secrets I Keep From The Internet
OPSEC WORKS

• Counterintelligence hasn’t changed in thousands of years
  • It still hasn’t

• The same principles and fundamentals still apply
OPSEC: THREE C’S

• Cover
• Concealment
• Compartmentation
• To all appearances, normal

• Cover for Action
  • Normal to do what you are doing

• Cover for Status
  • Normal to be where you are
CONCEALMENT
• Hide the activity

• Prevent anyone from knowing about it

• Hide identities
• Limit the number of people involved
  • Reduce chance of leakage
• Limit scope of the damage if it goes wrong
  • Impact containment
• The last line of defence
THE SIZE OF SECRETS
<table>
<thead>
<tr>
<th>Terrorist Act</th>
<th># Operatives</th>
<th>Roles of Operatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosives bombing—dropped</td>
<td>1-2</td>
<td>1 bomber, 1 security/driver</td>
</tr>
<tr>
<td>Explosives bombing—thrown</td>
<td>1</td>
<td>1 bomber</td>
</tr>
<tr>
<td>Explosives bombing—suicide</td>
<td>2</td>
<td>1 bomber, 1 security/driver</td>
</tr>
<tr>
<td>Explosives vehicle bomb—suicide</td>
<td>1</td>
<td>1 bomber</td>
</tr>
<tr>
<td>Firearms assassination</td>
<td>1-2</td>
<td>1 shooter, 1 backup shooter</td>
</tr>
<tr>
<td>Firearms ambush</td>
<td>3+</td>
<td>3 shooters</td>
</tr>
<tr>
<td>Explosives ambush</td>
<td>2</td>
<td>1 shooter, 1 lookout/backup</td>
</tr>
<tr>
<td>Skyjacking</td>
<td>3-5</td>
<td>1 commander, 2-4 guards</td>
</tr>
<tr>
<td>In-flight bomb—dropped</td>
<td>1</td>
<td>1 bomber</td>
</tr>
<tr>
<td>In-flight bomb—suicide/martyrdom</td>
<td>1</td>
<td>1 bomber</td>
</tr>
<tr>
<td>Arson</td>
<td>1-2</td>
<td>1 arsonist, 1 lookout</td>
</tr>
<tr>
<td>Armed raid</td>
<td>5-10+</td>
<td>1 commander, 4-9 shooters</td>
</tr>
<tr>
<td>Light infantry weapons attack</td>
<td>3+</td>
<td>1 commander, 2-4 shooters</td>
</tr>
<tr>
<td>Surface-to-air missile attack</td>
<td>2</td>
<td>1 lookout, 1 missile launcher</td>
</tr>
<tr>
<td>Abduction</td>
<td>3+</td>
<td>1 driver, 2 gunmen/guards</td>
</tr>
</tbody>
</table>
3 things: If you email me please write down the date on all your messages. Second, keep in mind that it takes a few days for emails to get to me so if you are setting an appointment then give me advance notice. Third: you do not need to write “to the sheikh” when you email inspire. Anything from your email will be delivered to me.

Please respond to this message with what you want to say and give it to the brother. We cannot have our brother travel with a laptop plus it is suspicious for you guys to type out a message in a public place.

This brother may be the messenger between us for now. One IMPORTANT note: The brother does not know that he is delivering messages for me and he doesn’t know where I am so do not mention that this message is for me. Just give it to him and he will deliver it where it needs to be delivered and will get to me insha Allah.

For future correspondence I believe it would be better if your wife delivers the flash to the brother. It’s up to you but I believe that you would definitely be watched and that might put you and the brother in jeopardy. Agree with the brother on the place of meeting. Also we need to keep the meetings to a minimum. The brother says it is not safe for him to enter sanaa frequently. So please mention all what you need to say in the message you send me.

Please let me know what your program is and the latest news from the west. Also please send the emails of ikrimah and this other brother with your message.

My wife needs some stuff from sanaa so can your wife buy it for her? We have sent other people before and nothing really suited her taste.

Awlaki’s first thumb drive message to me.
“Limit the number of people involved to the bare minimum.”

–OPSEC Maxim
“Distance in space and time increases adversarial costs”

–OPSEC Maxim
“When your adversary discovers there’s a secret, the first battle is lost.”

– OPSEC Maxim
“Never write if you can speak; never speak if you can nod; never nod if you can wink.”

–OPSEC Maxim (Martin Lomasney)
“Your adversary has a boss and a budget”

–OPSEC Maxim
“I must not trust. Trust is the OPSEC killer. Trust is the fatal error that brings total obliteration.”

–OPSEC Maxim
“People make mistakes.”

– OPSEC Maxim
SECURE PHONE

1058.0
updating...
TACTICOOL PHONES
STEALTH PHONE

- Secure stealth comms platform
DARKMATTER

- Secure stealth phone
- Plausible deniability
- Automated hardening
- Active response to attacks
EVENT BASED HARDENING
19 year old Brazilian girl swallows her phone to prevent her boyfriend from reading her texts.
TRANQUIL TRANSMISSION

Keep mum she's not so dumb!

CARELESS TALK COSTS LIVES
PGP is error prone
Errors are usually fatal
I JUST INSTALLED MUJAHIDEESEN SECRETS

SO I GUESS YOU COULD SAY THINGS ARE PRETTY SERIOUS
USING ENCRYPTION STANDS OUT
SECURE ANONYMOUS MESSAGING
POND
• Doesn’t rely on Tor

• Designed to resist timing correlations by a GPA

• Not p2p (but anyone can run a server)

• Server knows nothing about clients

• Can’t decrypt anything
• Strong PFS
  • Axolotl ratchet advances every send/reply
• Must be bootstrapped
  • Cumbersome manual KEX
• “Easy” via a shared passphrase + hookup server
POND IS PURE AWESOME
LETS MAKE IT BETTER
HOW DO WE GET THERE?
SECURE ANONYMOUS MOBILE MESSAGING APP
POND FOR MOBILE
1. Choose a name for this contact.

Bob

2. Enter the shared secret.

the_supreme_law

Generate
To: Bob  46/15810 bytes

How is the draft doing?
When in the Course of human events, it becomes necessary for one people to...
We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among...
Egotistical what?
OPSEC MAKES YOU HAPPY
"The ability to speak several languages is an asset, but the ability to keep your mouth shut in any language is priceless."
THANKS
NOT SURE IF KNOWS NOTHING

OR IS USING OPSEC

imgflip.com
DON'T TALK

THE WEB IS SPUN FOR YOU WITH INVISIBLE THREADS
KEEP OUT OF IT HELP TO DESTROY IT
STOP = THINK ASK YOURSELF IF WHAT YOU WERE ABOUT TO SAY MIGHT HELP THE ENEMY
SPIES ARE LISTENING

Intelligence Officer Northeastern Dept U.S. Army
BLASTED COMPUTER! HERE, EAT IT, YOU JOB-CONSUMING, TRANSISTORIZED, OVER-INFLATED ADDING MACHINE!
TECHNOLOGICALLY IMPAIRED HACKER

wears a mask because he can't figure out how to put tape over the webcam
I'VE KILLED BEFORE AN' I'LL KILL AGAIN! I WON'T SPLIT THAT DOUGH WITH NO ONE--NOT EVEN MYSELF!
ONLY TRUST YOUR FISTS
POLICE WILL NEVER HELP YOU
GOOD LUCK

I'M BEHIND SEVEN PROXIES
The Personal Internet Address & Password Logbook

Keep favorite website addresses, usernames, and passwords in one easy, convenient place!

Peter Pauper Press