Is that a government in your network or are you just happy to see me?

Eric M. Fiterman
www.spotkick.com
2000-2012 military spending increases

Data courtesy of SIPRI: http://www.sipri.org/
Which of the following is a more cost-effective intelligence collection platform?
OR
Superpower status is not a prerequisite to \{collect/disseminate\} intelligence anymore.
Wikileaks is rollin’ on 20s
This means you probably have someone in your network that can maneuver around as well as you can.
My background in incident response gave me visibility into tactics and techniques used by sophisticated adversaries.
I also write a lot of code.
I DON'T ALWAYS TEST MY CODE

BUT WHEN I DO I DO IT IN PRODUCTION
So here I’m going to present you with...
3 ROGUE TECHNIQUES TO SNIFF OUT THE NASTIES IN YOUR NETWORK
ROGUE TECHNIQUE #1

- TROJANIZE YOUR DOS/WIN32 SHELL
In our case, threat actors were heavy command-line users – using the *net* executable to mount shares and propagate malicious payloads.
We trojanized the shell

- Placed a net.com binary in the system32 folder (runs 1st)
- Our version beaconed out to a Google App Engine service that logged the activity and ran the original utility as intended
- Transparent to the attackers
- This gave us a subtle, **last-ditch warning** if a compromise was not caught by our other sensors

- Very simple wrapper makes outbound HTTP calls (interestingly, not flagged by enterprise A/V either)

**Code available at:**

https://github.com/RogueNetworks
In case you’re wondering, this is supposed to be Socrates, not God.

*Any similarity between this Socrates clip-art and Jesus is purely coincidental.

How can we extend this concept?

Where do we go from here?
Let’s build sandboxed versions of the COMMAND.COM shell that can present actors with the illusion of access to real system resources!

* Any similarity between this Socrates clip-art and Jesus is purely coincidental
The propagation of malicious payloads also depends on weaknesses in Active Directory authentication
The use of NTLM hash-injection tools allow seamless + native file/share access as any domain (or local) user
What is PTH?
Chef Monte’s World-Famous Recipe for Pass-the-Hash

Delicious and low-calorie, too!
Ingredients

✓ 1 Microsoft Active Directory Network

✓ 1-3 servings of domain admin hashes, unsalted

✓ 1 teaspoon of lemon zest

✓ 1 hash-injection tool
Step 1: Remove the hash

✓ First, ensure the local host is ripe enough and has the residue necessary to extract NTLM hashes

✓ Using the edge of a bowl, crack open the LSASS process to extract cached or in-memory hashes to produce your hashes
Step 2: Inject the hash

✓ After allowing the hashes to rest, prepare the NTLM hash using your injection tool of choice (console recommended)

✓ Then, carefully whisk the extracted hash into memory to replace the in-memory NTLM hash with the desired hash of your choice
Step 3: Enjoy!

✓ Congratulations, you are now able to access resources and generate Kerberos tickets as any domain user!

✓ Remember to wash your hands when done!
Chef Monte Says:

Remember to try my spam loaf recipe!!
While this problem has persisted for years, it is possible to detect and identify the characteristics associated with this technique.
ROGUE TECHNIQUE #2

• TURN PASS-THE-HASH INTO TRASH-THE-HASH
Lateral authentication looks odd:
The {code}

- **Breachbox core**: a suite of Linux daemons for monitoring Kerberos authentication traffic in the core
Features

• **Flexible deployment**: can be deployed via span port or in-line layer-2 for extra stealth

• **Zero-trust certified**: Rebuilds authentication transactions from the wire, *not from log data*

• **Plays well with log management**: Send alerts to enterprise log platforms via Syslog interface
Caveats

• Doesn’t completely support newest SMB protocols

• Protocol analyzer code is scary
The {code}

Code available at:

https://github.com/RogueNetworks
ROGUE TECHNIQUE #3

• PROFILE YOUR APPLICATIONS
Good
Blacklist malicious activity

Better
Whitelist acceptable activity

Best
Use math + lists!
Math is powerful

Holy moley – is that an A-bomb right outside Vegas?

It sure is, Pardner!
Math lets you soar to new heights
Many spam-detection systems work this way. They use Bayesian statistics to flag anomalies.
How email looks in a Bayesian world
Eric:

Thanks for the note. Did you see the article about how Walmart’s employees slammed the company on its own website?

Later,

-Skinner
Whatever your illness or disorder is it’s better to be sure of the medications you take! Cialis, Viagra, Prozac...
We can apply the same approach to web traffic.
http://www.spotkick.com/api/push?
c=breachbox&tid=1234567&ctype=3

http://www.spotkick.com/api/push?
c=spotkick&tid=7654321&ctype=2

Profile for push api service call:

c: alphanumerics, 9+-2 characters

tid: numeric, 7+-1 characters

cctype: numeric, 1+-1 characters
Profile for *push* api service call:

- c expects: alphanumeric, 9+2 character
  received: alphanumeric, 9 characters  *(PASS)*
- Ctype expects: numeric, 1+1 characters
  received: numeric, 1 character  *(PASS)*
- tid: numeric, 7+1 characters
  received: alphanumeric + control characters, 14 characters  *(FAIL)*
The {code}

• **Breachbox web**: a suite of Linux daemons for monitoring HTTP traffic
Features

• **Flexible deployment**: can be deployed via span port or in-line layer-2 for extra stealth

• **Hybrid scheme reduces false positives**: Statistical can be combined with list-based approaches
I DIDN'T HEAR YOUR QUESTION...

BUT THE ANSWER IS ALIENS