Did Anyone Get the Name of That Hacker Who PWNED Me?

Lance Cottrell

Ntrepid / Anonymizer

Session ID: BR-F43

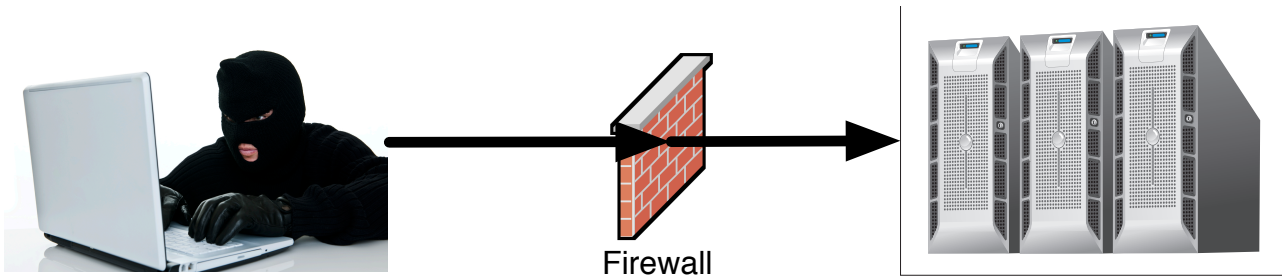
Session Classification: Intermediate

When You Are Under Attack

You may ask:

Did Anyone Get the Name of That Hacker Who PWNED Me?

As a Defender, You See....



IP: 37.123.118.67

Lat / Long: +54 / -2

Country: UK

Ping: 110ms

ISP: as13213.net (AKA UK2.net) server hosting

Open Ports: SSH, HTTP

Was That Really the Attacker?

Which is the "Real" Attacker?

It's Turtles All the Way Down

What If You Could Spot People Hiding?

- Block Web Access
- Redirect to Honeypot
- Add Firewall Rule
- Deny Credit Card
- Flag in Logs

How Do They Hide?

- Proxies
- VPNs
- Chained VPNs / TOR
- Botnets / Compromised Hosts
- Advanced Persistent Threats

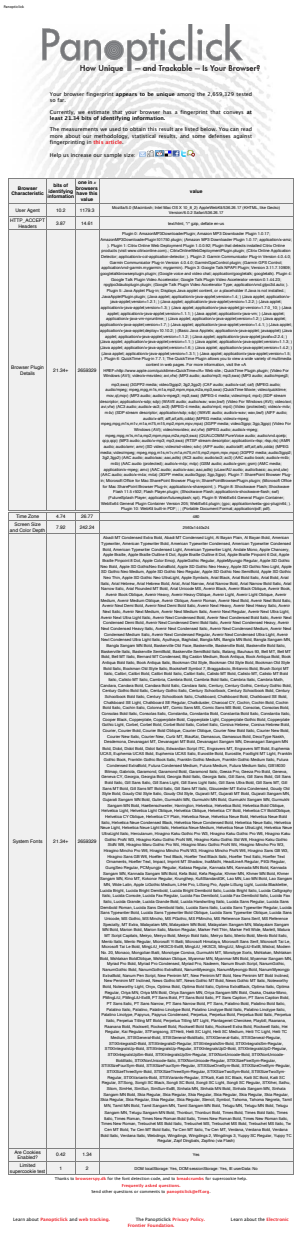
How You Can Spot Them

- Known Anonymity IP
- Open Proxy / VPN Ports
- Inappropriate / Non-consumer IP
- “Bulletproof” Host
- High Latency vs. Ping
- Protocol Leakage

Track the Computer Itself

Browser Fingerprints

- Fingerprint May Stand Out
- Unusual OS / Browser
- System TOO Clean
- System TOO Hardened
- Lying In UserAgent String



Virtualization Makes Your Job Harder

Advantages	Disadvantages
Easy to Clean	Cloned Each Time
No Cookies or Super-Cookies	Too Clean or Outdated Cruft
Detection as VM Requires Local Execution	Can Be Detected as VM

Fortunately (for you), Good OPSEC is Hard

- Tools can be slow and cumbersome
- May go direct for "innocent" activity / reconnaissance
- May forget to use it
- Accidentally cross the streams of personas
- Correlate attacker print with all previous activity

Why Should YOU be Stealthy

- Lurk in IRC and Forums
  - Discover Plans
  - Learn Techniques
  - Hide your interest & activity
- Bait Honeypots
  - Drop False Leads and Links
- Government
  - Has Other More Aggressive Options

10 Tips for Defender Stealth Part 1

1. Using a known anon IP is good
2. Use only VPN type privacy services
3. Use a VM for identity isolation and malware prevention
4. Use a different VM for each identity / activity
5. Vary your appearance and fingerprint for each VM

10 Tips for Defender Stealth Part 2

6. Files on the VM are definitionally contaminated
7. Check for DNS leakage
8. Ensure no local network or device is visible from the VM
9. Change clock, time zone, language, as appropriate
10. Stay on the right side of the law

Thanks

Contact me at:

Email: lance.cottrell@ntrepidcorp.com

Commercial / Gov: http://ntrepidcorp.com

Consumer: http://anonymizer.com

Blog: http://theprivacyblog.com

Twitter: @LanceCottrell

LinkedIn: http://linkedin.com/in/LanceCottrell

NTREPID