Penetration Testing with Live Malware

Gunter Ollmann

CTO
NCC Group
@gollmann
The Pentest Conundrum
Pentesting Debate

- Penetration Testing
- Vulnerability Scanning
- Compliance Auditing
Pentesting Debate

- Morphing to vulnerability scanning and onto tick-box compliance

- “Penetration testing” being pulled to extremes:
  - Hardcore bug-hunting and reversing
  - Semiconductor reversing
  - Red Team testing

- “Testing as a pentester, rather than an attacker”
Where is the threat?

- “Hackers” continue to probe defenses, scan ports, and enumerate services.
- External attacks against unpatched OS-vulnerabilities (in)frequent.
- Attacks that exploit unpatched vulnerabilities and manage to breach corporate defenses through the front door are an increasingly rare breed.
The Real Threat
Ignoring the Real Threat

Most breaches start and end with malware…
Breached

- Malware accounts for vast majority of breaches
  - Vehicle for getting inside the target
  - Platform for horizontal movement
  - Tool for data extraction and remote access
- Successful attacks delivered through:
  - Barrage of social engineering & trickery
  - Browser & user-level application subversion
Enterprise Penetration

- Penetration of an enterprise network requires the defeat and subversion of multiple layers of defense
  - Including anti-virus and intrusion prevention technologies.
Enterprise Penetration

Cloud
- Email/attachment scanning, URL checking, etc.

Gateway
- Proxy filtering, URL filtering, etc.

DMZ
- Scanning appliances, Dynamic analysis, VM, etc.

Server
- Mail server/archive scanning, host scanning, etc.

Endpoint
- Desktop suites, etc.

Malware
Biggest Failure

- Unwarranted “faith” in (dynamic) malware analysis tools
  - Appeals like diet pills
  - Promise of weight loss without altering lifestyle
- No changes to business practices
  - Malware gets smarter
  - Vectors gets smarter
  - Network just as dirty as ever
Pentesting Requirements

- In order to test these defenses...
  - It is necessary to construct the same kind of advanced and stealthy malware as employed by the (best) cybercriminals
  - We need to deploy the malware in a similar fashion to the cybercriminals
The “Ethics” Question

- Beg, borrow, or steal tools from the bad-guys?
- Engage the underground ecosystem and pay their fees?
- Access or construct better tools than what the “average” bad-guys have?
- Pollution of commercial AV with non-criminal malware?
- Blah, blah, blah…
Pentesting Twenty-teenies

- Need new penetration testing methodologies designed to replicate current generation attack profiles and stress the layered defense model.

- Practical considerations
  - Which layer(s) detected it?
  - Did it compromise the target host?
  - Is the malware serviceable to an attacker?
Building Malware
Malware Construction

- Plenty of samples, but need something new…
  - Modification of existing source code
  - Tweaking of existing malware
  - “Lawful intercept” malware
  - Underground cybercrime kits
  - Commercial malware kits
  - Growing business need *(start a business!)*

- *Not* worth throwing yesterday’s malware at a target…
Malware Armoring

- “Off-the-shelf” malware trivial to detect
- Armoring tools & methodologies advancing at a rapid pace
  - Anti-debugging
  - Anti-virtualization
  - Anti-decompilation
  - Polymorphic manipulators, etc.
- Most tools are “commercial”, efficient, and not backdoored (surprisingly)
Malware Vetting

- Create one or many samples?
  - Many!!!
  - Create a “tree” of malware derivatives
    - Naked, armored, hardened, to “the works”
- Should I pre-test the malware?
  - Yes, but only if you can keep the samples to yourself
  - Turn off “cloud” submissions and analytics
- Can I reuse my old samples?
  - No.
Include a marker within your malware specific to the job

- Files identified through binary inspection
- Don’t make it obvious though

Choose carefully the method of C&C

- Protocols are important, so too is being proxy-aware
- Static and dynamic routes to C&C

Report/record which host affected

- Beaconing after XXX hours is good
Vectors Are Important

- But don’t get hung up on them
- Remember the scope of the pentest
- Red Team offers more opportunities

- Assessing the security of layered-defenses
  - Multiple samples, multiple vectors
  - Preparation is key
    - Expect to expend 4 days effort building, tuning, and watermarking samples
    - Takes 3+ days to research/build spear-phishing lists and messages
Attack Vectors

- Social engineering vectors tend to be more successful
  - Email with URL’s to download malware
  - Dropping Trojanized files on file servers
  - Career/recruitment portals accepting attachments
- Deploying malware through exploited vulnerabilities
  - Horizontal propagation done via malware
Client Considerations

1. Make sure T&C’s cover malware behaviors
2. Be specific on engagement scope and what vectors are allowable
3. Document and tag each sample that is to be deployed
4. Post-engagement C&C locations, beaconing, and tag information must be disclosed
5. Submit all samples to AV vendors afterwards
Conclusions

- Penetration testing methods need to include “malware”
- Difference between testing the layers of detection versus layers of prevention
- There are many good/safe tools
- Preparation effort and duration for testing are not insignificant
- CYA on T&C’s and post-op cleanup
Apply... actions...

- Immediate actions
  - Document your anti-malware defensive layers
  - Assume you will always be breached by malware – focus upon immediate detection & automated remediation

- Next 3 months
  - Plan on assessing malware defenses on a quarterly basis
  - Ensure that network anomaly detection tools are capable of detecting malware communication artifacts
  - Identify layers of implicit trust and double-down on defenses
Thank you

Gunter Ollmann
CTO, NCC Group
@gollmann