Adventures with Cybercrime Toolkits: Insights for Pragmatic Defense

Birhanu Eshete
Assistant Professor, Computer Science
University of Michigan, Dearborn
Exploit Kits: fishing trawlers of cybercriminals
Exploit Kits: typical structure

- Admin Dashboard
- Configuration Script
- Exploit Dropper
- Exploit Pool
- Cloaking Logic
- Obfuscation Routine
- Database Script
- Geo-Location API
- Installer Script
- Infection Statistics
- Style and Media
Typical exploit kit infection chain

ENTICE → REDIRECT → FINGERPRINT → INFECT → CALL HOME
With access to their source code, what can we learn about exploit kits?
The real reason why we ask such questions

Cybercriminals also ask similar questions when they explore blind spots in the systems we build, configure and deploy
In the cybercrime arms race, how do we improve the state of defense?
Advice 1.0: "be proactive"
Advice 2.0: "be pragmatic"
Advice 1.0: be proactive

Advice 2.0: be pragmatic
Is this really a thing?

How do we do this?
Probing exploit kits to milk behavioral fingerprints
Controlled probing of exploit kits to milk behavioral fingerprint

- Goal #1: common behavior, unique fingerprint
- Goal #2: actively probe & identify
Attack-Centric

- Victim Fingerprinting
- Redirection Chain
- Exploit Obfuscation
- Bring Your Own Exploit
Self-Defense

- IP Blocking
- Blacklist Lookup
- Signature Evasion
- Cloaking
Defense capability gained

- probe exploit kit URL
- milk signatures through interaction
- identify family

Full paper: https://tinyurl.com/tu7r7b7
Intriguing findings

- live probing enriched behavioral signatures
- identifying attributes remained stable

1.1K live exploit kits probed over 5 months
Lesson for pragmatic defense

**PROACTIVE**  
PREEMPTIVE DAMAGE AVOIDANCE

**REACTIVE**  
DETECTION & DAMAGE CONTROL
Leveraging blind spots in exploit kits to turn the table on cybercriminals
Take advantage of flaws in exploit kit code to fight back

- **Goal:** counter-offensive strategy backed by legal authorization

Full paper: [https://tinyurl.com/tp5ylu7](https://tinyurl.com/tp5ylu7)
Who will be using such a strategy and for what?
Defense capability gained

10 concrete exploits on 6 exploit kit families
How complex is a concrete exploit?

~ 15 lines of code!

Hijack exploit kit database

Wipe-out exploit kit installation
Lesson for pragmatic defense

with legal authorization and automation, defenders can deter damages done by exploit kits & potentially stop them
In the cybercrime arms race, how do we improve the state of defense?

**Advice 1.0:** be proactive

**Advice 2.0:** be pragmatic

In practice: neither mutually exclusive nor opposing forces
Takeaways

1: Just like defenders, cybercriminals have blind spots in coding, configuration, and deployment of their exploit toolkits.

2: Defenders can leverage these blind spots to build pragmatic defense and turn the table on cybercriminals.
Thank You!

birhanu@umich.edu

@birhanu_eshete