Operational Security

NMSU Reverse Engineering
Joshua Reynolds
Sp24

Operational Security

“Systematic and proven process by which potential adversaries can be denied information … The process involves five steps: **identification of critical information**, **analysis of threats**, **analysis of vulnerabilities**, **assessment of risks**, and **application of appropriate countermeasures**.”

NIST Computer Security Resource Center

Identification of Critical Information

What sensitive information might a reverse engineer be guarding?

Identification of Critical Information

What sensitive information might a reverse engineer be guarding?

- The fact that the victims have discovered they are under attack
- Passwords, credentials, or keys embedded in the malware
- The fact that the victims have fallen victim to a cyberattack
- The particular security failings that allowed the attack
- What the attackers are likely doing/capable of
- Sometimes, who the attackers are

Analysis of Threats

Why is this information confidential?

For keys/credentials so no other adversaries copy the attack

Shouldn’t people know what happened?

- Legal Liability
- Insider trading & official reporting channels
- Organization reputation

In Case of Cyberattack, Call Lawyer

Sometimes it’s not the cyberattack, but the lawsuits and legal disclosures which are most damaging.

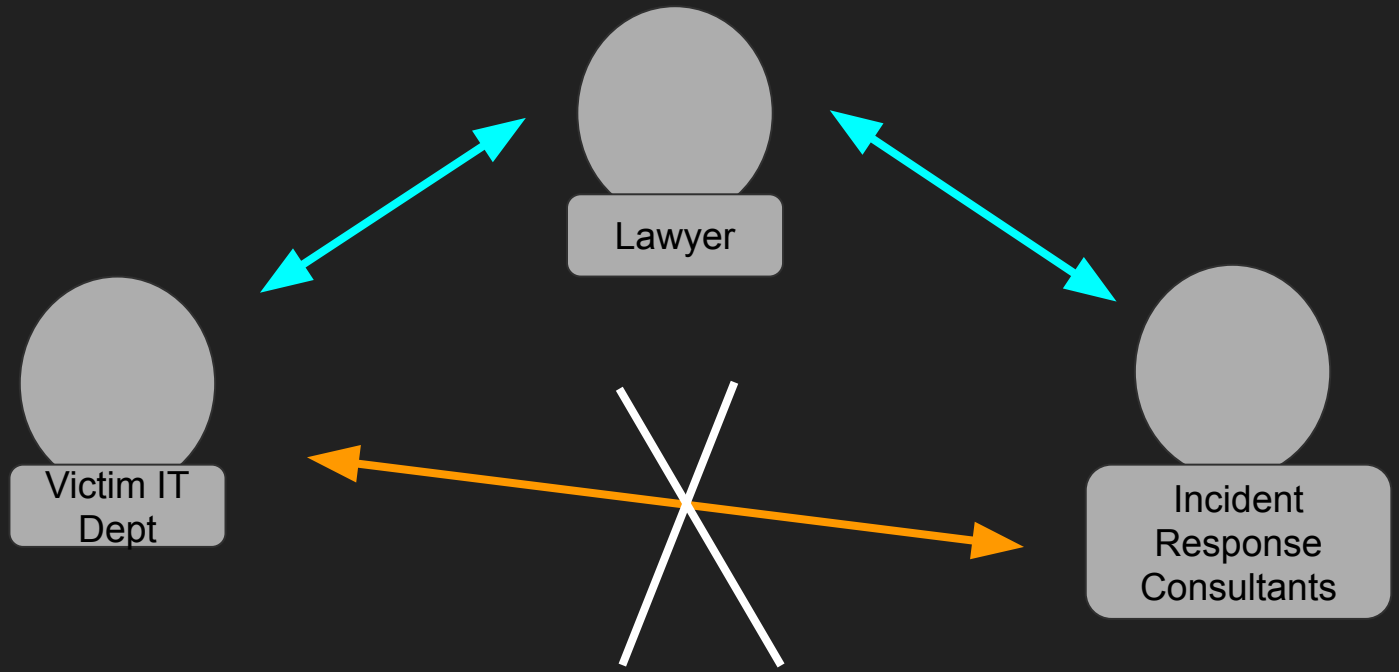
Legal Discovery:

The court orders company X to turn over all emails/DMs/SMS regarding the data breach on dd/mm/yyyy and internal investigations.

Exception: Attorney-Client Privilege:

“Attorney-client privilege protects confidential communications between a lawyer and their client that relate to the client's seeking of legal advice or services.” - Cornell Law School

The legal triangle: IANAL TINLA



A law firm specializing in data breach litigation

https://www.crowell.com/en/services/practices/privacy-and-cybersecurity/incident-response#experience

“Defended Starwood Hotels in a federal data security class action filed after Starwood announced that cyber criminals had installed malware on point of sale terminals at dozens of Starwood locations that permitted the cyberattackers to access customers’ credit card information. We obtained a voluntary dismissal of the action with prejudice with no payout to the plaintiff, after filing a motion to dismiss and convincing the court that, among other things, the plaintiff had failed to allege sufficient injury to establish federal jurisdiction.”

Analysis of Vulnerabilities & Risks

1. **Premature public disclosure**
    a. Ex. “I reversed a new variation of APT42’s “_____” malware that was found on _____’s servers. Details and malware sample on my blog! <LINK>”
2. **Anti-analysis systems or dynamic analysis mishaps**
    a. Some malware fights back, and tries to infect analysis machines, break out of VM guests into the hypervisor, or other devices on the RE engineer’s network.
3. **Sharing the malware sample with a friend or analysis service**

“The Principle of Least Surprise” From Michael Bailey, GATech

When you are wondering “Can I do _____?”

Ask yourself if it would surprise anyone.

If so, talk to them first and get permission.

Give people time to repair/recover their systems and make their official disclosures.

Asking forgiveness instead of permission is a bad idea when some parties can send you to prison.

Application of Countermeasures

1. Keep confidentiality, encourage appropriate reporting, don’t cover-up
    a. Remember you are more likely than most to have your emails/slack/texts subpoenaed. Let the record show you were trying to do the right thing.
2. Use **network isolation** when reversing to avoid being the cause of more infections
3. Use **system isolation** to keep malware from breaking out.
    a. Working on Windows malware? Use a VM on a *NIX host

Setup Lab Environment