GitHub @deezombiedude612

SE6016 : FORENSICS

[I. OVERVIEW]

[Context] is impt in Forensics.
Wout [knowing what could happen] ⇒ ✕ context ⇒ ✕ forensics

Escalation of Ransomware

- Targeted at indus.; revenue: "retail victims" — INIT iter.
- Targeted at corps; revenue: data decryption — NEXT iter.
- Targeted at corps (often via supply chain); revenue: reputation & business preservation — CURRENT iter.

Importance of Cyber Risk Governance

businesses & orgs rely on tech (ex., PoS systems)

cyber risks continue to expand & influence other types of risks

(possible) some are essentially "tech companies" (to keep up w/ demands in evolving competitive landscape)
ex., tech involved in processes (supply chain, manufacturing, etc.) of (not necessarily tech) products such as handbags

↘ cyber risks permeate into enterprises

SG Cyber Trends

- more frequent data breaches
- biometric data more valuable to threat actors
- global supply chain threat
- more disruptive atks against cloud
- AI: double-edged sword!
- ↘ risk towards smart buildings & connected sys. ↑

Cyber Atk Techniques

1. **Obfuscation**
   * use of protection & obfuscation that is notoriously difficult to break
   * protection software hides intellectual props. contained in legit. commercial software
2. **Stealth**
   * malware files encrypted & camouflaged to blend w/ other legit sys. files
   ⇒ ✕ distinguish fm parts of OS
3. **Wipeout Techniques**
   * anti-forensic techniques to reliably erase traces of own activity
   ⇒ make retracing & understanding actions more difficult
4. **Hijacking**
   * hijack legit software to manipulate its logic
5. **Surveillance**
   * deploy malicious modules to record frames (ie., screenshots) & keystrokes → reassemble into viewable recordings
   * used to fully understand workings of sys. before attempting to subvert it
6. **Watering Holes**
   * masquerade as "legit website" to bait victim of interest before engaging
7. **Exploits**
   * find & exploit "holes" in system
   * ASYMMETRIC DEFENDER ATTACKER PARADOX: attacker only needs 1 hole to get in, but defender needs to fix all holes to be secure
8. **False Flags**
   * malware authors place false flags w/in their tools to stall/confuse investigators
   ex., diversionary language codes & various incorrectly transliterated words to mislead research into true identity of attkers
9. **Anonymity**
   * set up proxies btwn themselves & end target → long chain for investigators to trace

Change in Attkr's Approach

1. atks shifting fm tech → ppl
2. atk patterns hiding in plain sight
3. attkrs building widening capability gap
4. supply chain & business partner sabotage ↑
5. advanced threats defying traditional detection mechanisms

An atk scheme can involve multiple atk types.

Cyber Threats in Focus

* Advanced Persistent Threats (APTs)
* Scams
* Phishing
* Malware

Malware

programs that perform unwanted actions on computers (ex., steal personal info); possible artifacts:
→ virus, trojan, rootkit, worm, bot, [ransomware]
↓
used to extort $ fm victims; may restrict access to data by encrypting files or locking computer screens

Man-in-the-Middle (MITM)

act of eavesdropping on comms. btwn 2 parties online; info then used to intercept & go-btwn both parties in conversation
(ex., unknown Wi-Fi networks, man-in-the-browser, man-in-the-email)

Common Cyber Atk Types

Dumpster Diving

obtaining sensitive info that is discarded carelessly; can be used to fake legitimacy

Phishing

attempt to acquire impt info (ex., credentials, credit card info) by posing as a trusted source in an electronic communication
ex., deceptive emails, malware, compromised networks, malicious websites

Social Engineering

act of gaining access to buildings, sys, or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques

Cyberatk Impact Factors

(better-known cyber incident costs)

Above the surface

- Technical investigation
- Post-breach customer protection
- Public relations
- Customer breach notification
- Cybersecurity improvements
- Regulatory compliance
- Attorney fees & litigation

(hidden/less visible costs)

Beneath the surface

- devaluation of trade name
- loss of intellectual property
- value of lost contract revenue
- lost value of customer rships
- insurance premium ↑
- cost ↑ to raise debt
- impact of operational disruption/destruction