Threat Actor Goals:
BLEED

Anthko
Cyber Security

Agenda

1. Disclaimer
2. Purpose
3. Bankrupt
4. Leverage
5. Educate
6. Exfiltrate
7. Destroy
8. Summary
9. Contact Us

Anthko
Cyber Security

Disclaimer

This slide deck is for informational and educational purposes only. Any content in this slide deck is intended to assist organizations understand one of many techniques that may be used to undermine the integrity of their information systems and network. The use of the information contained in this slide deck for any purpose other than stated above is prohibited. This slide deck may be redistributed without written consent in its original format without any alterations. This is an opinion document.

Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security

Purpose

Understanding the fundamental goal(s) of any threat actor is essential for effective proactive and reactive defense actions. There are five fundamental goals of threat actors. These goals have been presented in a variety of ways using a variety of mediums in the past several decades, but the acronym “BLEED” is the one we have developed to help draw attention to these goals. BLEED stands for bankrupt, leverage, educate, exfiltrate, and destroy. All threat actor actions from ransomware to hostile insider threats fall within these five categories. We attempt to effectively portray these five categories in this slide deck.

Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security Anthko Cyber Security

Anthko Cyber Security

Bankrupt

Reasons threat actors wish to bankrupt an organization include:

- **Ideological differences (hacktivists)**
- **Reprisal (scorned employee/former employee, contractor, 3rd-party)**
- **Eliminate industry competition**

Some ways threat actors may attempt to bankrupt a company:

- **Litigation (wrongful termination, intellectual property infringement, etc.)**
- **Compliance violations (reporting poor practices, stealing non-encrypted laptops)**
- **Causing loss of reputation**

Large organization litigating small organizations is the most public example.

Leverage

Reasons threat actors may want to leverage your resources include:

- **Hosting CPKP or other forbidden content**
- **Launching malware campaigns**
- **Creating espionage campaigns against competitors**
- **Perform computationally intensive task across a distributed environment**

Some ways threat actors may leverage your resources may include:

- **Creating covert channels for data movement**
- **Living off the land**
- **Using compromised user accounts**
- **Creating unauthorized virtual machines**
- **Adding unauthorized devices**

Anthko
Cyber Security

Educate

Some threat actors seek knowledge, reasons may include:

- **Personal knowledge and skill improvement**
- **Political maneuvering (attack/counter-attack orientation)**
- **Competitive advantage (offering release dates, ad campaigns/market strategy)**
- **Prepare for full incursion into your environment**

Some ways threat actors may gain knowledge include:

- **Public database queries (EDGAR, Google, your public facing pages)**
- **Former public disclosures**
- **Fake job listings (interrogating your employees during “interview”)**
- **Social Engineering (that new random friend that asks for advice about work)**
- **Parts of your organization that are leaking data due to misconfigurations**

Anthko
Cyber Security

Exfiltrate

Threat actors often need to exfiltrate data to:

- **Make money (sell trade secrets, blackmail, extortion, etc.)**
- **Expand operations (list of 3rd-parties, contractors, MOUs/ISAs, SLAs)**
- **Develop technology (create exploits, match competitor advancements)**
- **Prolonged attack (username/passwords, strategic goals, planned security)**
- **Seek new employment**

Exfiltration tactics may include:

- **Employee hardware use/theft (USB, laptop theft, IOT device use)**
- **Covert Channels (Loki ICMP, dns tunneling, NTP tunneling)**
- **Email (compromised accounts, abandoned accounts, auto-forwarding, meta data manipulation, etc.)**
- **Stenography (in pictures, in documents, in .bat and .conf files, etc.)**

Anthko
Cyber Security

Anthko Cyber Security

Destroy

Threat actors may destroy data to:

- **Alleviate frustration**
- **Conceal activities**
- **Disrupt organization activities**
- **Seek Revenge**
- **Reduce prosecutor capability**

Some ways a threat actor may attempt to destroy include:

- **Logic bomb malware**
- **Native remove/erase functionality (ex: rm -f)**
- **Physical destruction (degaus; a hammer; liquid damage; fire; etc.)**
- **Overwrite data**
- **Ransomware**

Anthko Cyber Security

Summary

Threat actors want to BLEED your organization. Understanding this will assist in developing questions about how you can be attacked. Knowing how you can be attacked will help you determine the most likely avenues of attack. Knowing how you are most likely to be attacked will help develop plans to reduce the damage from the attacks. Understanding how threat actors BLEED your organization is a critical step to ensuring a diligent and prudent security posture.

Connect With Us

1. LinkedIn
   https://www.linkedin.com/company/anthko-cyber-security
   (or search for “Anthko”)

2. Our Website
   AnthkoCyberSecurity.com