Three Hacker Flows:
Low & Slow, Blended, Smash & Grab

Agenda

1. Purpose
2. Low & Slow Flows
3. Identifying Low & Slow Flows
4. Blended Flows
5. Identifying Blended Flows
6. Smash & Grab Flows
7. Identifying Smash & Grab Flows
8. Summary

Purpose

With the plethora of events and transactions that happen continuously within organizations, identifying a specific event that is associated with a specific attack is becoming increasingly difficult and unreasonable. Identifying specific traffic flows associated with attacks and that are composed of many events increases the visibility of attacks. This slide deck has been created to discuss three traffic patterns used by intruders, the reasons they are used, and some common ways they are identified by organizations. The patterns being presented include:

- **Low & Slow Attack Flows**
- **Blended Attack Flows**
- **Smash & Grab Attack Flows**

Low & Slow Flows

Low and Slow attacks typically incorporate the use of advanced technical attacks, (such as laptop keyboard, battery, and touch-pad malware). The flow-based goal of the attacker is to be the "needle-in-the-haystack" by using only the lowest amount of bandwidth possible to achieve the objective in the amount of time permitted. These attacks have very focused objectives and typically have long-term goals that can range from several months to decades.

Identifying Low & Slow Flows

Because low & slow attack flows typically incorporate highly technical exploits that are independent of patch status, (they can't be patched,) these flows usually can't be identified without the use of external resources. Typical external sources include:

- **Net-flow sensors – connections are reconstructed from source to destination, connections that have been open for an extended duration are analyzed, and connections with data transfers below a certain bit rate are analyzed.**

- **Honey pots and honey nets – Organizations permit attacks against select resources that have all preset services, flows, software, firmware, settings, etc. cataloged and all changes are analyzed.**

Blended Flows

Blended attack flows incorporate techniques that blend into normal network traffic patters. The goal of the attacker here is to create attack flows that are indistinguishable from standard network traffic. These attack patterns can be conducted by very sophisticated attackers that seamlessly integrate into the network or by script-kiddies that find a new exploit kit that has finite pattern signatures.

Identifying Blended Flows

Blended attack flows are designed to be indistinguishable from standard traffic flows so organizations typically must identify these flows at the connection's onset. Some of the ways to identify these flows include :

- **At flow inception – Was there a login with a suspicious place, time, or concurrency with other use of the same credential; IPS signatures; setting or configuration changes, firewall rule updates, alternate data stream analysis, etc.**

- **Honey pots and honey nets – Organizations permit attacks against select resources that have all preset services, flows, software, firmware, settings, etc. cataloged and all changes are analyzed.**

Smash & Grab Flows

When an attacker has a very short time-frame they may leverage a smash-and-grab type attack. These attacks tend to be very noisy on the network, can be extremely unsophisticated, and can leverage publicly known vulnerabilities that could have been patched. Denial of service conditions may result from these flows.

Identifying Smash & Grab Flows

Smash and Grab flows are designed to be quick and noisy. Some ways to identifying smash and grab flows include:

- **Netflow – a sizable deviation in the network bandwidth consumption.**
- **IPS – heuristic and signature based detection methods can be leveraged**
- **Spam Filters – Phishing & Vishing can be effective ways to easily gain entry**
- **Service Monitoring – Substantial increases in DNS, ICMP, HTTP(s), SMB, or other service traffic may indicate a smash & grab**
- **Credential Use Monitoring – one password may be attempted against all organization user, service, and system accounts or many passwords against a single account.**

Summary

With the plethora of events and transactions that happen continuously within organizations, identifying a specific event that is associated with a specific attack is becoming increasingly difficult and unreasonable. Identifying specific traffic flows associated with attacks and that are composed of many events increases the visibility of attacks. This slide deck has discussed three attack flow types and some common ways to identify them. Attackers may use one, two, or all three of these attacks patters in conjunction. For example, smash and grab can be used to steal card holder data while low and slow can be used to create a golden ticket. Attack surfaces are only increasing and event based detection is becoming increasingly difficult to manage so increasing attacker visibility through attacker flow identification.

Connect With Us

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

2. **Our Website**
   AnthkoCyberSecurity.com