Tunnel Cleaning:
One APT Evasion Technique

Agenda

1. Disclaimer
2. Purpose
3. Tunnel Cleaning: The Concept
4. In The Beginning
5. The Schedule
6. Full Tunnel Burn-In
7. The Transition
8. Shutting Down The Tunnel
9. Summary
10. Contact Us

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.

Purpose

The purpose of this slide deck is to provide insights into one way advanced persistent threat (APTs) are able to establish a data flow that blends into normal network traffic and some ways organizations can attempt to spot and close these tunnels.

Tunnel Cleaning: The Concept

Most people have heard the term “hidden in plain sight.” Tunnel cleaning is a technique for hackers to establish data flows that transparently integrate into normal corporate data flows. The idea is to create a normal data flow using standard corporate services and devices. Then, expand that data flow slowly to manipulate heuristic devices and administrative personnel into believing the increased traffic is a normal escalation of business resource use.

In The Beginning

With the rate of attack surface expansion that most organizations are experiencing with the integration of mobile devices, software, IOT devices, cloud services, missing patches, third-party service providers, custom code, etc., the ability to be penetrated becomes increasingly simplistic for a motivated entity/hacker. Once the entity is in your organization it will want to stay hidden, (unless it is a smash & grab). One way to stay hidden is to choose a way to hide all communications and data movements. (For this slide deck we will choose DNS.) For this example the hacker will create 2 cron jobs or windows tasks.

The Schedule

The two jobs/tasks that the hacker created (for this example) are:

1)Query DNS for this list of internet addresses

2)Every [hacker set time period] duplicate job 1 a set number of times

For the first job hacker selects a list of websites that organizational users might typically visit. Depending on the hacker's sophistication, this list may include only a couple social media sites, a list of vendors used by the organization, or any combination that can be conceived.

For the second job, the hacker will try to set a time that increases the amount of data flowing without setting off device alerts or arousing suspicion from network or security administrators.   This job must stop replicating after a set number of replications to keep the tunnel from becoming obscenely large.

Full Tunnel Burn-In

As time passes the tunnel will build itself and stop growing once it reaches a predetermined size. Once the tunnel has finished growing the hacker will permit “Burn-in” time to pass. This time gives confidence to the hacker that the tunnel has not been spotted by devices or personnel and is ready to be used. Depending on the experience, confidence, and urgency of the hacker, burn-in time can range from weeks to years. In the case of years, the hacker has most likely established your organization as an asset for future use.

The Transition

Once the tunnel has been burned-in the hacker will start to use it. As first, the entity/hacker may only tunnel a small amount of data through the established DNS flows. Possibly only using less than 10% of the total tunnel. As the hacker gains confidence that devices and personnel are not spotting the transition from normal DNS traffic to malicious DNS tunneling the 10% use will slowly increase until a full 100% take-over of the established tunnel.

Preventing The Tunnel

Prevention is the best way to stop a tunnel. Some common ways to stopping this type of APT tunneling include:

- **Knowing which cron jobs & schedule tasks are legitimate and authorized and the ability to detect illegitimate or unauthorized ADSs**

- **Inspecting the sources of sustained bandwidth consumption increases**

- **Using network flow diagnostics and intrusion prevention/detection systems to identify the initial breach**

- **Knowing which alternate data streams (ADS) are legitimate and authorized and the ability to detect illegitimate or unauthorized ADSs**

Summary

Tunnel Cleaning is one way hackers might choose to hide in plain site on an organization’s network. The ability to manipulate traffic patterns in undetectable ways using an organization’s own resources can result in a greatly increased time between initial infiltration and detection. The best way to stop this type of activity is to prevent it from ever starting.

Connect With Us

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

2. Our Website
   AnthkoCyberSecurity.com