Anthelio Healthcare Solutions
Global Information Security Group
Security Awareness Bulletin - Vol. 07

anthelio®
A higher aim. A newer standard.

Hacked – How to identify and what do next

Users play an important role in effectively thwarting potential security threats and attacks, by maintaining a clean system, timely identification of threat symptoms, and readily alerting abnormal activities to appropriate teams. However, if a compromise is discovered, victims are often at a loss and unaware of what to do next. This confusion can result in delays, which can stall efforts to identify and control the damage, and eventually extends the time it takes to recover. In reality, with awareness, prompt identification, and decisive action, one can act quickly to minimize damage, and safeguard against future attacks.

In general, a system compromise materializes through some well-known exploit channels, such as malware attacks, known weaknesses in systems, social engineering techniques, and insider threats. 'System Compromise' refers to any computing resource whose confidentiality, integrity, or availability is adversely impacted by an untrusted source, which can result in financial and/or material loss to the organization.

Becoming familiar with typical symptoms and indicators of a system compromise helps to safeguard the system from severe damage later. Today, the threats and exploit methods are becoming increasingly sophisticated and complicated. They look authentic, and can go undetected for days, months or even longer. Delays in the identification of the threat and related events allows the infection to spread wide and deep, gain strength to cause catastrophic damage to the organization.

Symptoms that may indicate a system compromise:

1. A unknown program requests authorization to make changes to your system that you did not initiate.
2. Your web browser auto-redirects to websites you did not intend to visit.
3. Antivirus software is disabled and ignores attempts to re-enable it.
4. Antivirus software alerts that it was unable to remove or quarantine the infected files.
5. Files disappear, new programs are running, or something changed, with which you are unaware.
6. System or applications are crashing, unknown icons appear on your desktop, or strange messages pop-up.
7. Bulk emails are sent from your account without your knowledge.
8. A pop-up window with a countdown timer keeps appearing.
9. Extreme system slowness and difficulty launching applications or the internet.
10. Systems fails to login with your valid login credentials.

Your system is likely to be compromised, Now What?

Step #1 – Do NOT panic. Do NOT take it personally.	
Step #2 – Do NOT try to fix the problem by yourself.	*Valuable Forensic information and investigative evidences can be lost if defined incident response procedures are not followed.*
Step #3 – Report to your IT Helpdesk immediately. Collaborate with incident response team to help analyze the problem.	*Even if you are not sure if you have been hacked or compromised, it is far better to report it just in case.*
Step #4 – Disconnect from network, and shutdown the computer	*Tracking down how the bad actors got in and addressing the weakness as quickly as possible is CRITICAL.*

Industry experts continue to highlight the importance of IT-security awareness and exert it as the most compelling technique to combat the threats related to system compromise and subsequent damages. Being mindful and following the **S**top. **T**hink. **C**onnect strategy is a powerful tool to prevent and minimize threats to an organization.