

Malicious and Unauthorized Software

About STEALTHbits

STEALTHbits Technologies, Inc. provides a rich set of solutions to help manage your Microsoft infrastructure and beyond. As an industry leader in Auditing, Reporting, and Compliance software, solutions from STEALTHbits increase efficiencies, reduce downtime, and optimize the performance of your systems and applications to provide instant value and the quickest return on investment.

StealthAUDIT

StealthAUDIT is a lightweight, high speed and agent less tool. Using Data Collectors, information is returned on nearly every attribute with respect to Windows servers, workstations, Active Directory, Exchange, and more.

To ensure maximum flexibility, results are stored in Microsoft SQL Server and a built in report writing engine enables the information to be delivered in a variety of formats; email, published, Excel, or XML.

Instant alerting is provided by tracking critical threshold via the change and conformance module, and analysis will provide email notification any time such changes have taken place.

Rich historical data collection endows our customers with powerful trending and statistical capabilities.

StealthAUDIT is a powerful tool which comes packaged with pre-built solutions in Active Directory, Backup Validation, Compliance, Entitlement, Exchange, Investigation, Public Folder, Software Inventory, and much more!



STEALTHbits Technologies, Inc.

SALES DIRECT: (201) 447-9300

www.stealthbits.com | sales@stealthbits.com

Overview

Managing the exponentially growing number of authorized and licensed software applications across your corporate infrastructure is a constant an ever increasing area of concern. Along with license management and software metering programs, is the growing need to control the instances of unauthorized and malicious software. Since it is far from a simple task to track thousands of different software titles that are allowed to be installed on your systems, it seems a simplified approach is to make a quick hit list of the software packages that you don't ever want to find on your systems.

STEALTHbits Technologies has assembled that quick hit list to spin you into motion immediately, allowing you to begin to make tangible reduction of risk to the loss of corporate information, financial responsibilities, and increase your general security posture.

Our unauthorized software list includes over 30 key applications that span from applications that take remote control over your systems, enable Peer-to-Peer sharing of files, and support non-standard corporate approved methods to communication with internal or external parties.

Our malicious software list includes over 20 key applications that span from account enumerators, multi-function hacking tools, to stenography tools used to hide sensitive or proprietary information.

Where we help:

- Establish an Application Baseline
- Review Unauthorized Software Compliance
- Review Malicious Software Compliance
- Collaborate with Users and/or Managers
- Reduce Exposure and Risk

The Application Inventory Solution Set is the 4th and newest section being built out within our Global Infrastructure Inventory Management Solution Set. These Solution Sets are an out-of-the-box collection of comprehensive audit jobs that collect everything you need to get started with your initiative. Charts and graphs provide various levels of detail that position you to launch into action and summarize project progress.

Malicious and Unauthorized Software

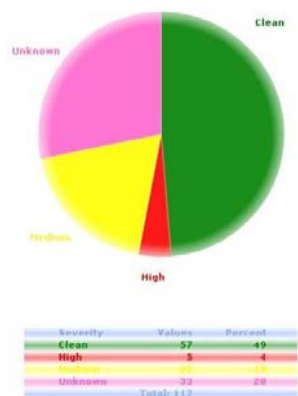
Establish an Application Baseline

First, you'll need to audit a full list of applications spread out across your servers and workstations. StealthAUDIT can quickly gather this information and can be set up to re-audit those systems that are currently offline until information has been collected from all your global systems.

The full list of installed applications is consolidated into a central database for automated review and assessment of what is found to be considered malicious or unauthorized in your environment. From this central location, StealthAUDIT summarizes the information you need to launch your programs for reduction of these unwanted applications in your environment or track your progress towards reducing and eliminating them from your infrastructure.

Review Unauthorized Software Compliance

Systems reviewed for Unauthorized Software



Each organization will have a different extended list for what is unauthorized in their corporate environment.

Our unauthorized software list includes over 30 key applications that span from applications that take **remote control** over your systems, enable **Peer-to-Peer sharing** of files, and non-standard corporate approved **communication applications** with internal or external parties.

These are applications that most organizations would never want to see installed onto your corporate servers and/or workstations. This list is easily modified or extended based on each organization's unique needs.

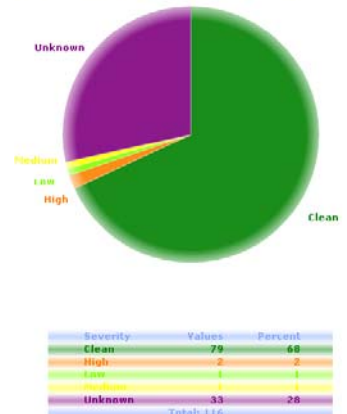
Review Malicious Software Compliance

Just like the unauthorized software list, every organization will have a different extended list of what applications are considered to be a threat to the safety of their environment.

Our malicious software list includes over 20 key applications that span from **account enumerators**, **multi-function hacking tools**, to **stenography tools** used to hide sensitive or proprietary information.

These are applications that most organizations would never want to see installed onto your corporate servers and/or workstations. This list is also easily modified or extended based on each organization's unique needs.

Systems reviewed for Malicious Software



STEALTHbits Technologies, Inc.

SALES DIRECT: (201) 447-9300

www.stealthbits.com | sales@stealthbits.com

STEALTHbits
TECHNOLOGIES

Malicious and Unauthorized Software

Collaborate with Users and/or Managers

Now that you've gathered and assessed the applications associated with a particular server or workstation, you will need to reach out to the owner of the system.

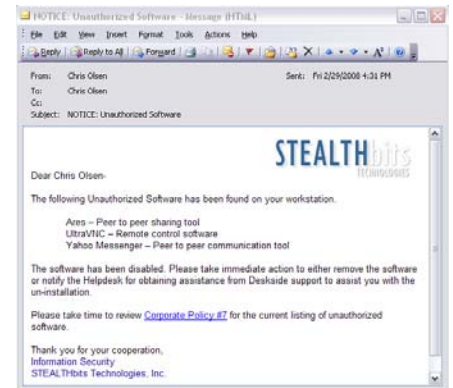
Servers can have hundreds of administrators associated with one server and often times administrators are forced to reference a stale list of server administrators stored in some other inventory or asset management system.

Workstations can even be shared in certain types of departments or passed to new owners as they are re-imaged or recycled.

This identification process used to be a slow and cloudy task, but now you can leverage StealthAUDIT's built-in business intelligence to quickly identify the most likely owner of a server or a workstation.

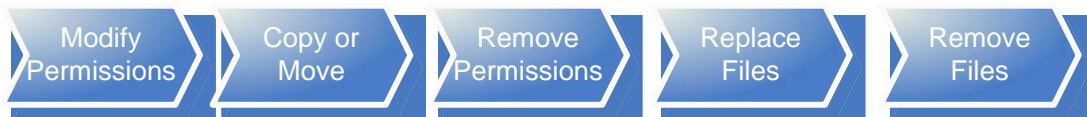
Next, leverage StealthAUDIT's unique workflow Action Modules to reach out and solicit information from your targeted users and tie those responses to the data stored in your central database.

Email requests and web-based survey forms can easily take on the look and feel of your internal corporate processes, including logos and color schemes, thus giving them a polished, professional, and official corporate look.



Reduce Exposure and Risk

Now that you have gathered the technical information and validated your program with your user base, it's time to take action! Leveraging our Action Modules to quickly and easily make changes based on your findings or even the survey results and responses that you have received back from Administrators, End Users, and Managers. You can cycle through options to modify permissions, copy or move files, reduce or remove permissions, replace files, or even remove them completely. Our action modules put you in control of your infrastructure right from our centralized console!



See our report website for additional sample reports and dashboards:
<http://www.stealthauditdashboard.com>

STEALTHbits Technologies, Inc.

SALES DIRECT: (201) 447-9300

www.stealthbits.com | sales@stealthbits.com

