Wolf in Sheep's Clothing: Your Next APT is Already Whitelisted

Fabio Assolini (@kassolini)
Juan Andres Guerrero-Saade (@juanandres_gs)
Global Research and Analysis Team (GReAT), Kaspersky Lab

Public Release Version

KASPERSKY

Wolf in Sheep's Clothing: Your Next APT is Already Whitelisted

Fabio Assolini (@assolini)
Juan Andres Guerrero-Saade (@juanandres_gs)
Global Research and Analysis Team (GReAT), Kaspersky Lab

Public Release Version

Trust-Based Security Creates Problems

Whitelisting depends on the accurate characterization of code's intended use

Inherited --Is the developer trustworthy?

Behavior --Is the behavior seemingly benevolent?

Crowdsourced Trust --Do many people trust this application?

Can you accurately characterize the use of code?

KASPERSKY

Benevolent Design

!=

Benevolent Use

KASPERSKY

A History of Abuse

GREAT
Global Research
& Analysis Team

KASPERSKY

APTs and Targeted Attacks

Interpreters -for ease and power!

Machete – Bring all that you need!
Python interpreter for ease of coding

Flame – Prepare for every eventuality!
Lua interpreter for modular design

Admin Tools –Management for all!

SkeletonKey –PSEXEC is vital in SK's lateral movement towards the target domain controller to allow the attacker's authentic

MiniDuke/CosmicDuke –Windows Task Scheduler for persistence and malware operations scheduling

KASPERSKY lab

Interpreters -for ease and power!

Machete -- Bring all that you need!

Python interpreter for ease of coding

Flame -- Prepare for every eventuality!

Lua interpreter for modular design

KASPERSKY lab

Admin Tools --Management for all!

SkeletonKey --PSEXEC is vital in SK's lateral movement towards the target domain controller to allow the attacker's authentic

MiniDuke/CosmicDuke --Windows Task Scheduler for persistence and malware operations scheduling

KASPERSKY lab

Wipers

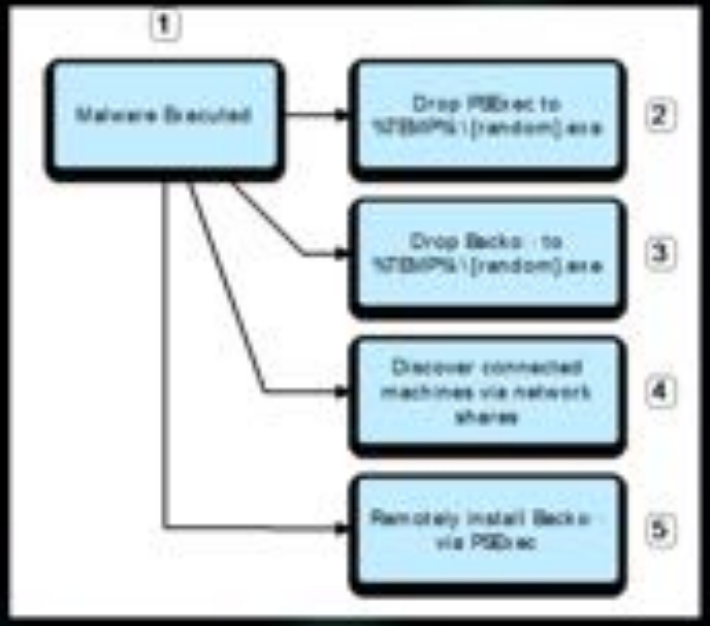
Sabotage -- Powered by Eldos RawDisk

Abusing RawDisk lib to evade NTFS permissions

KASPERSKY lab

Point-of-Sale Malware

Backoff -- Abusing psexec



Banking Trojans

Antirootkits – A story of friendly fire

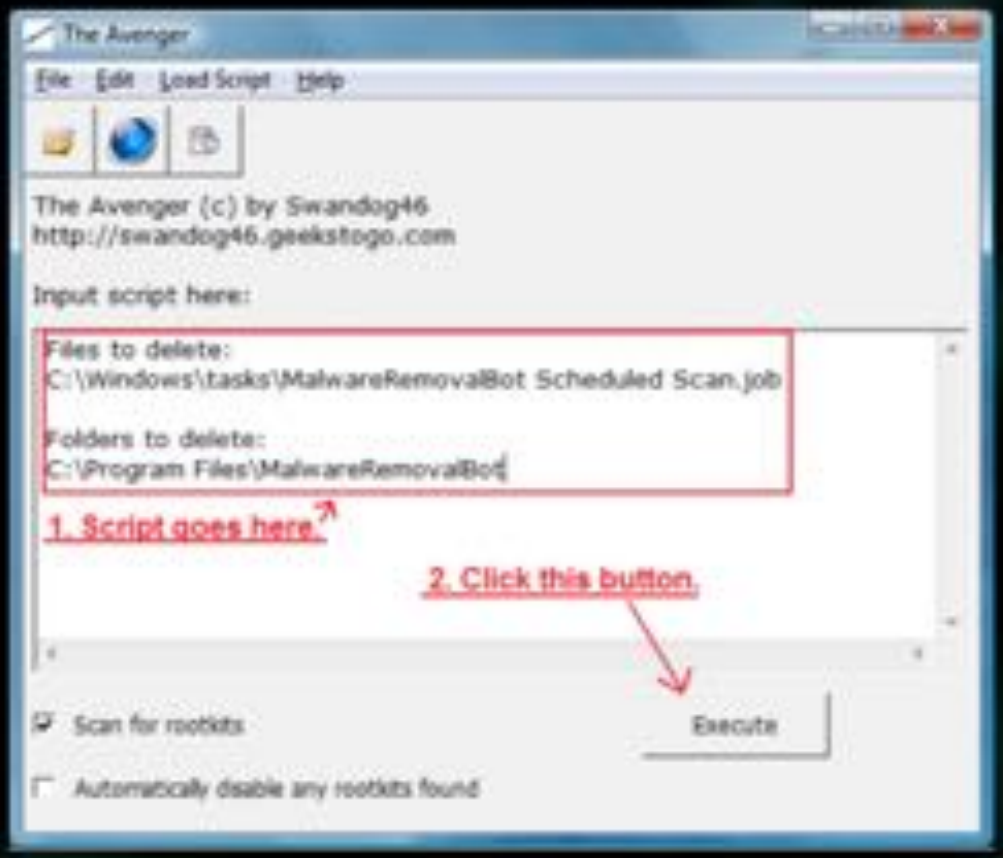
Repurposing antirootkit tools to remove security software

BITSAdmin

Second-Step Payload –Powered by Microsoft!

Look no further than your own OS!

Antirootkits -- A story of friendly fire

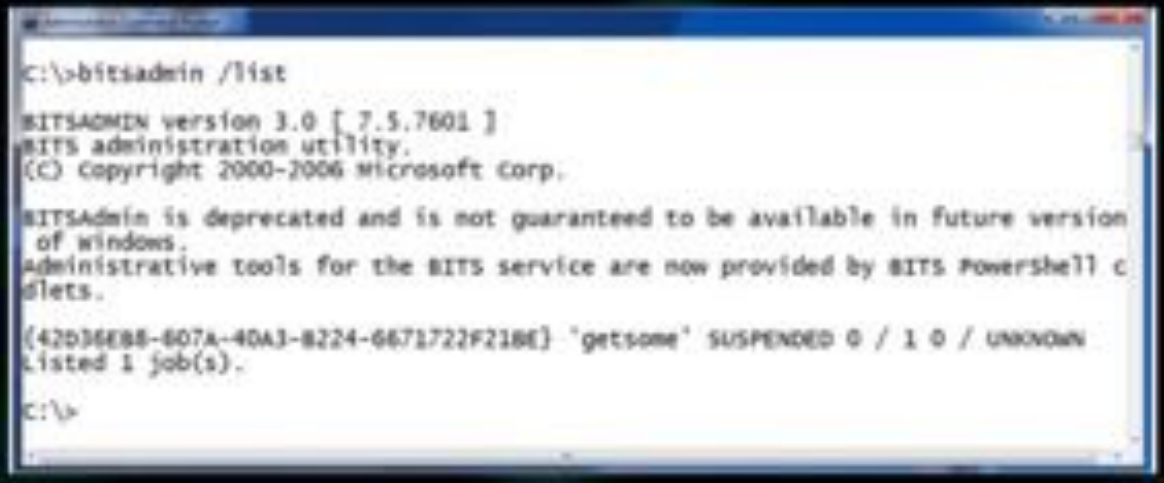


Repurposing antirootkit tools to remove security software

KASPERSKY lab

BITSAdmin

Second-Step Payload --Powered by Microsoft!



Look no further than your own OS!

KASPERSKY lab

Ransomware

ACCDFISA

Winrar –efficiently taking what you love!

Abusing access control tools

KASPERSKY

CTB-Locker

Trust, trust everywhere!

WinRAR, Zlib, and... sdelete

KASPERSKY

KASPERSKY lab

ACCDFISA

Winrar --efficiently taking what you love!

Abusing access control tools

KASPERSKY lab

CTB-Locker

Trust, trust everywhere!

WinRAR, Zlib, and... sdelete

KASPERSKY

A History of Abuse

GREAT
Global Research
& Analysis Team

KASPERSKY

What Good is Flagging 'Riskware'?

Legal necessity for dealing with litigious developers

Huge delay period for detection with no agreement across security vendors

... And I absolutely agree with you! Moreover, when you disable the riskware detection in KAV 6, it still counts all the riskware as a threat (however, automatically excluding it). So you have something like:

Threats found: 10
Unthreated: 0

... when all the "threats found" are just riskware, detection of which you wanted to disable ;-)

Dubious categories like 'Riskware', 'Suspicious', and 'HackTool' are often placeholders

Users put in effort into circumventing any blocking and detection of riskware

KASPERSKY

The Interim Solution -- DEFAULT DENY

Custom-Tailored Application Control

Hint: Password protect your configuration manager

KASPERSKY lab

A Necessary Paradigm Shift

Move away from 'All-Purpose Computing'

Hone Down Your Toolkit

or

Get Shanked with it!

KASPERSKY lab

Wolf in Sheep's Clothing: Your Next APT is Already Whitelisted

Fabio Assolini (@assolini)
Juan Andres Guerrero-Saade (@juanandres_gs)
Global Research and Analysis Team (GReAT), Kaspersky Lab

Public Release Version

Wolf in Sheep's Clothing: Your Next APT is Already Whitelisted

Fabio Assolini (@kassolini)
Juan Andres Guerrero-Saade (@juanandres_gs)
Global Research and Analysis Team (GReAT), Kaspersky Lab

Public Release Version

KASPERSKY