Offensive Tool Agnostics

Leveraging Pre-Installed Technologies for Penetration Testing

Overview

- What is it
- Benefits
- My objective
- Red & Blue challenges
- Toolkit
- Demo

whoami

- Lee Kagan
- @invokethreatguy
- Co-Founder of RedBlack Security
- Rogue Team
- $pentester
  - I like Microsoft stuff

What are “Tool Agnostics” ?

« Revolutionary Device Detects Mimikatz Use

Appropriate Covert Channels »

Flying a Cylon Raider

November 18, 2015

In Season 1, Episode 5 of Battlestar Galactica, Lieutenant Kara Thrace finds herself marooned on a barren planet with a crashed Cylon Raider. To get home, Lieutenant Thrace has to apply her knowledge of flight fundamentals to control the strange platform and pilot it back to safety.

And, so it goes with hacking. You don't always get to choose your tools. In mature environments, the combination of defenses and analysts you're working against will dictate which tools you can use.

When your favorite toolset is taken away from you, how do you operate?

Matt Graeber, Jared Atkinson – Living Off the Land 2: A Minimalist's Guide to Windows Defense

Living Off the Land 2: A Minimalist's Guide to Windows Defense Matt Graeber and Jared Atkinson - @mattifestation The ?living off the land? philosophy, as applied to InfoSec, is the idea that one can thrive using mostly the tools present in a target environment in an effort to remain hidden from an adversary. While historically this philosophy has been

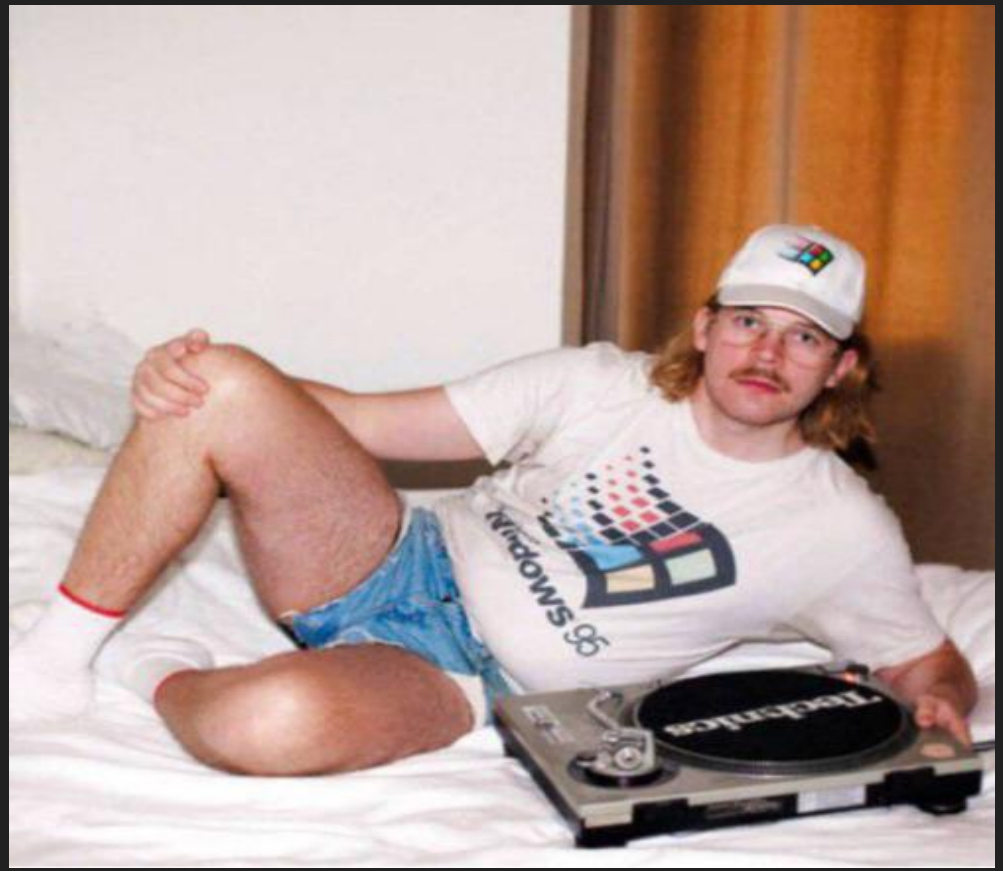
https://www.derbycon.com/events/living-off-the-land-2-a-minimalists-guide-to-windows-defense/

What is it?

- Not ***relying*** on $tool
- Integrating and ‘mix’ tools
- Replicating capabilities
- Emulating behaviour
- Intelligence driven

Benefits

- Custom tooling
- Flexibility
- Adapt
- Automation
- Education



My Objectives

- Reduce toolkit dependencies
- Reduce footprint and impact
- Automate and chain tasks

Challenges for Red

- Things break
- $tool not allowed
- $tool getting caught
- Defenders defending

Challenges for Blue

- Two-way street
- Creating wastelands
- Behaviour
- Focus on capabilities

Challenges

the grugq @thegrugq · Aug 13

Good point. Many modern attackers “live off the land” (to evade detection, etc) so give them only a barren waste.

> **Alex Stamos** @alexstamos
>
> PowerShell is great for AD/Exchange admins, I've never seen legit use on clients. Should not be installed by default twitter.com/botherder/stat…

35 43

Malicious macro using a sneaky new trick

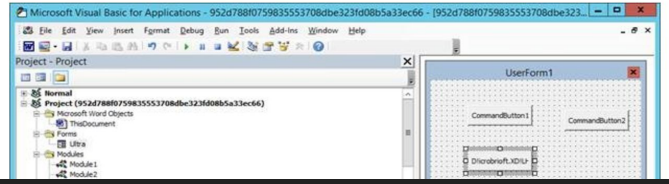
Rate this article

msft-mmpc May 17, 2016

Share 17 | 22 | 142 | 8

We recently came across a file (ORDER-549-6303896-2172940.docm, SHA1: 952d788f0759835553708dbe323fd08b5a33ec66) containing a VBA project that scripts a malicious macro (SHA1: 73c4c3869304a10ec598a50791b7de1e7da58f36). We added it under the detection TrojanDownloader:O97M/Donoff – a large family of Office-targeting macro-based malware that has been active for several years (see our blog category on macro-based malware for more blogs).

However, there wasn't an immediate, obvious identification that this file was actually malicious. It's a Word file that contains seven VBA modules and a VBA user form with a few buttons (using the **CommandButton** elements).



SECURELIST

THREATS ▾ CATEGORIES ▾ TAGS ▾ ENCYC

LOG IN

The rise of .NET and Powershell malware

By Santiago Pontiroli, Roberto Martinez on October 12, 2015. 10:08 am

RESEARCH

Home › Malware

Malware Increasingly Abusing WMI for Evasion

By Ionut Arghire on October 07, 2016

Share 41 | G+1 3 | Tweet | Recommend 33 | RSS

Malware is increasingly using Windows Management Instrumentation (WMI) queries to evade detection and to determine the environment it is running in, FireEye researchers warn.

Leveraging WMI to evade detection has been seen before, and Mandiant revealed last year that advanced persistent threat (APT) groups were **using WMI and PowerShell** to move laterally, harvest credentials, and search for useful information within Windows environments. Now, FireEye is offering more specific examples of how WMI queries can be leveraged for nefarious purposes.

Because WMI provides high-level interaction with Windows objects using C/C++, VBScript, JScript, and C#, the WMI services are being abused by malware authors to avoid virtualized environments and evade detection. In fact, FireEye explains that a WMI query can detect anti-virus programs because they are registered in **AntiVirusProduct** class under *root\SecurityCenter2* namespace.

Malware Employs PowerShell to Infect Systems

By Marc Rivero López on Mar 24, 2016

Like | Share 27 | Share 78 | G+1 2 | Tweet | Email

Email is one of the favorite methods used by attackers to infect systems. The malware used in email campaigns is often ransomware or banking malware.

We have recently seen some interesting tactical changes, including:

- Attachments with the malicious executable inside.
- Microsoft Office documents that contain a malicious macro. The macro will download ransomware or banking malware after execution.
- JavaScript files, executed by Wscript in Windows, dropping, for example, Locky ransomware.

https://securelist.com/blog/research/72417/the-rise-of-net-and-powershell-malware/ ,
https://blogs.technet.microsoft.com/mmpc/2016/05/17/malicious-macro-using-a-sneaky-new-trick/,
http://www.securityweek.com/malware-increasingly-abusing-wmi-evasion ,
https://blogs.mcafee.com/mcafee-labs/malware-employs-powershell-to-infect-systems/

Toolkit

Intelligence sources on the cheap

GitHub, Inc. (US) | https://github.com/rsmudge/Malleable-C2-Profiles/blob/master/APT/havex.profile

Search

Branch: master ▾ **Malleable-C2-Profiles** / APT / **havex.profile**

Find file | Copy path

rsmudge Crouching Yeti / Dragonfly / Energetic Bear / [Marketing Name Here] p... 26569cd on Aug 1, 2014

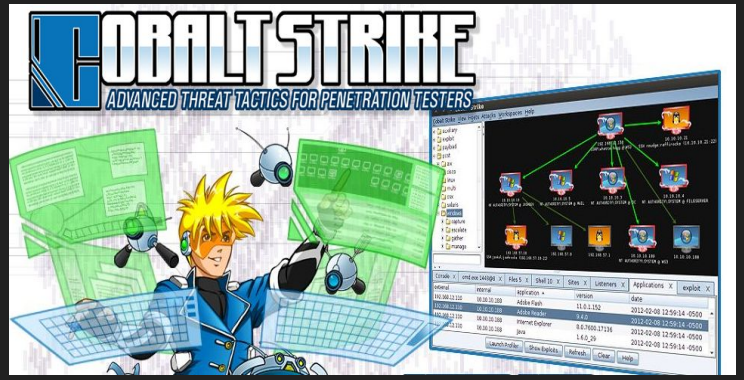
1 contributor

82 lines (68 sloc) | 2.27 KB | Raw | Blame | History

```
# havex trojan C&C profile
# Actor: Energetic Bear / Crouching Yeti / Dragonfly
#
# See:
# . http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group
# . https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf
# . http://pastebin.com/qCdMwtZ6
# . http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf
#
# Author: @armitagehacker

set sleeptime "30000";

set useragent "Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2) Java/1.5.0_08";

http-get {
        set uri "/include/template/isx.php /wp06/wp-includes/po.php /wp08/wp-includes/dtcla.php";

        client {
                header "Referer" "http://www.google.com";
                header "Accept" "text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
                header "Accept-Language" "en-us,en;q=0.5";
```

Threat Actor profile in Cobalt Strike's Malleable C2

https://github.com/rsmudge/Malleable-C2-Profiles/blob/master/APT/havex.profile



Still love these

A lot of options

Win32 API access, remoting, ul/dl, COM, network, lions and tigers and bears

- PowerShell
- WMI / CIM
- .Net
- C#
- VBA / VBScript
- WScript/CScript
- JScript
- HTA

DEMO

Thank you DC416 :)