Tempest

ACADEMY

Conference

2023

Respondendo Cenários de Ameaça Usando Splunk

Uma abordagem prática de Hunting em resposta de incidentes

Classificação da Informação: PÚBLICA
Autor da apresentação: Samuel Lima - CSIRT

Tempest

ACADEMY

Conference

01 User Execution

02 Scheduled Tasks

Tempest

ACADEMY

Conference

Importância da Detecção de Ameaças

Importância da Detecção de Ameaças

Em um ambiente corporativo, a segurança das informações é essencial para proteger a reputação da empresa e evitar prejuízos financeiros. O Splunk é uma ferramenta que ajuda a detectar ameaças em tempo real, permitindo que você responda rapidamente a possíveis ataques e reduza o impacto de uma violação de segurança.

User Execution

Hipótese

Tempest
:ACADEMY:
Conference

O Agente Malicioso tentará estabelecer uma posição segura no Froth.ly (nossa Aplicação fictícia), induzindo um usuário a executar uma ação em um arquivo

ID: T1204

Tactic: Execution

Platform: Linux, Windows, macOS

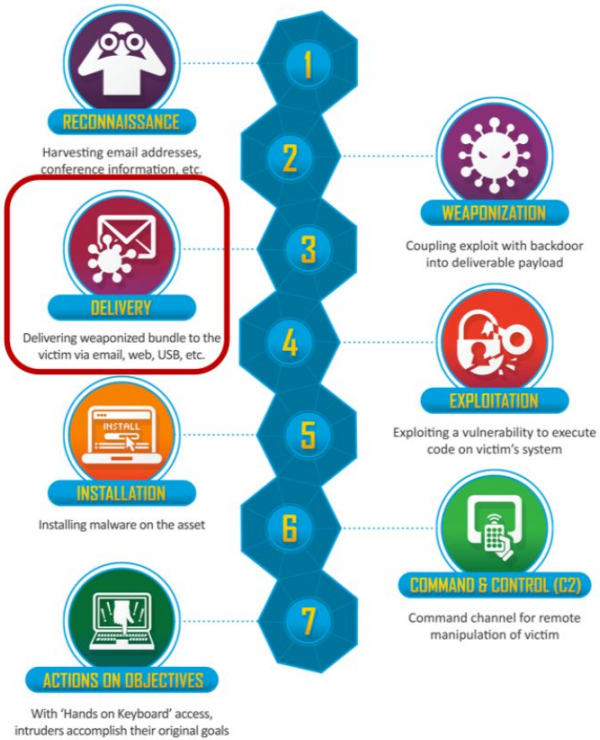
Permissions Required: User

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Version: 1.0

Descrição

Um atacante pode confiar em ações específicas de um usuário para obter execução. Isso pode ser uma execução direta de código, como quando um usuário abre um executável malicioso entregue via Spear phishing anexado a um arquivo de documento. Embora a execução do usuário ocorra frequentemente logo após o acesso inicial, ela pode ocorrer em outras fases de uma intrusão, como quando o atacante coloca um arquivo em um diretório compartilhado ou na área de trabalho de um usuário esperando que ele clique nele.



Tempest
ACADEMY
Conference

Como podemos confirmar ou descartar a nossa hipótese?

Fazendo as Seguintes Perguntas:

- Em quais data sources (sourcetype) a execução dos arquivos deve/pode ser executada?
- Deveríamos procurar execuções de arquivos antes ou depois do recebimento de anexos de spear phishing?
- Que tipo de informação de suporte é encontrada em eventos quando ocorre a execução de um arquivo?
- Que outros indicadores temos para começar a procurar a execução do usuário?

Tempest
[ACADEMY]
Conference

Como podemos confirmar ou descartar a nossa hipótese?

Fazendo as Seguintes Perguntas:

- Neste caso, sabemos que um anexo de spear phishing chamado invoice.zip foi recebido
- Em qual sistema a execução ocorreu?
- Qual foi o nome do usuário que executou o arquivo?
- O que aconteceu na execução de um arquivo?

Mão na Massa

Tempest
ACADEMY
Conference

Conseguimos confirmar nossa hipótese?

Tempest
[ACADEMY]
Conference

- Conseguimos rastrear a execução de invoice.zip até um usuário específico
- Esse usuário codificou o PowerShell em execução em seu sistema imediatamente após o Windows abrir invoice.doc (extraído de invoice.zip)

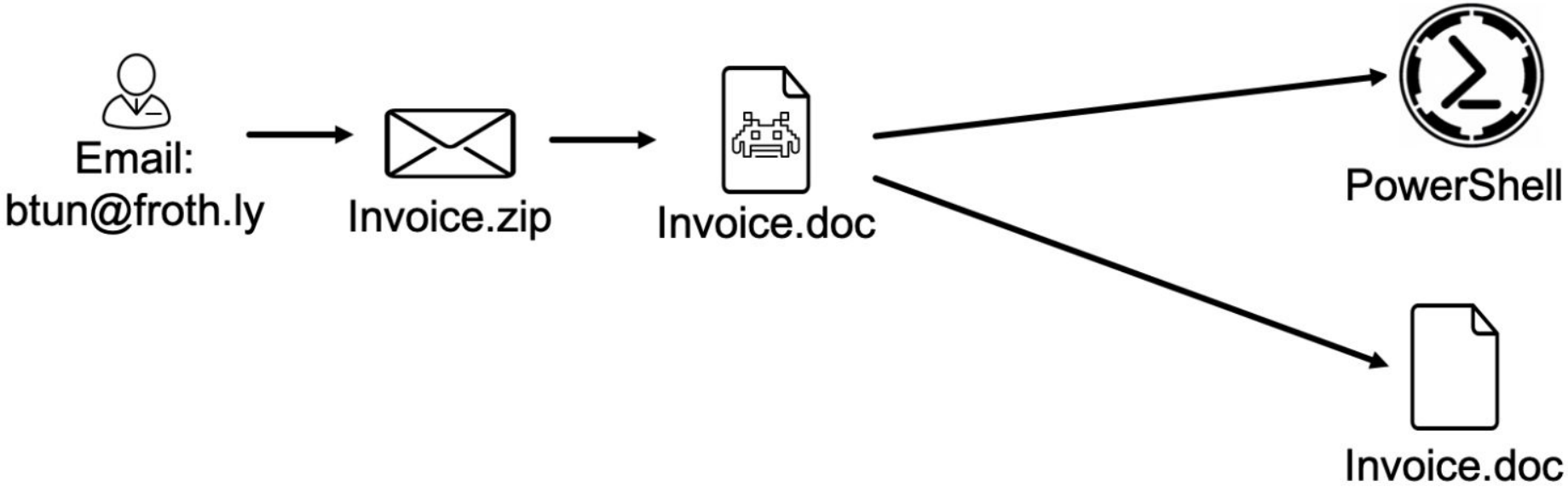
O que Aprendemos?

Tempest
[ACADEMY]
Conference

- Billy Tun parece ter executado o anexo invoice.doc
- Invoice.doc foi extraído de invoice.zip encontrado no e-mail de spear phishing
- O PowerShell foi executado após a abertura do documento, configurando que havia um payload junto.

Diagrama de User Execution

Tempest
[ACADEMY]
Conference



Tempest
[ACADEMY]
Conference

O que devemos pôr em operação?

- Proibir o uso de arquivos habilitados para macro (pode afetar o funcionamento da aplicação)
- Monitore sua execução
- Aplicar soluções EDR que analisam, registram e potencialmente bloqueiam sua execução.

Scheduled Tasks

Hipótese

Tempest
:ACADEMY:
Conference

Um Agente Malicioso tentará manter a persistência durante as reinicializações usando um agendador de tarefas

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: SYSTEM, Administrator, User

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

Supports Remote: Yes

CAPEC ID: CAPEC-557 Not a hyperlink

Contributors: Leo Loobeek, @leoloobeek, Travis Smith, Tripwire, Alain Homewood, Insomnia Security

Version: 1.0

Descrição

Um Agente Malicioso pode usar o agendamento de tarefas para executar programas na inicialização do sistema ou de forma programada para persistência, para conduzir a execução remota como parte de uma Movimentação Lateral para obter privilégios de SISTEMA ou para executar um processo no contexto de uma conta especificada.

Tempest
[ACADEMY]
Conference

Como podemos confirmar ou descartar a nossa hipótese?

Fazendo as Seguintes Perguntas:

- Quais DataSources (sourcetypes) são necessárias para identificar tarefas agendadas?
- Existem códigos ou valores de eventos específicos que indicariam a execução de tarefas agendadas?
- Existem valores-chave que as tarefas agendadas usam quando são criadas ou modificadas?
- Quem criou essas tarefas agendadas?

Tempest
ACADEMY
Conference

Como podemos confirmar ou descartar a nossa hipótese?

Fazendo as Seguintes Perguntas:

- Quais sistemas foram usados para criar as tarefas agendadas?
- Quais tarefas agendadas foram executadas?
- Qual era o nome da tarefa agendada?

O que é um Agendador de Tarefas?

Tempest
[ACADEMY]
Conference

- O Agendador de tarefas fornece um método para executar ações de acordo com uma programação. Estes podem ser criados na instalação pelo Windows, por um aplicativo ou por um usuário. O agendador de tarefas tem usos legítimos e uma instalação padrão do Windows pode ter muitas tarefas, de modo que um adversário pode encontrar um lugar para se aninhar, tornando-o difícil de encontrar.

O que é um Agendador de Tarefas?

Tempest
[ACADEMY]
Conference

Schtasks.exe

Enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. Running Schtasks.exe without arguments displays the status and next run time for each registered task.

Creating a Task

The following syntax is used to create a task on the local or remote computer.

```
schtasks /Create
[/S system [/U username [/P [password]]]]
[/RU username [/RP [password]] /SC schedule [/MO modifier] [/D day]
[/M months] [/I idletime] /TN taskname /TR taskrun [/ST starttime]
[/RI interval] [ {/ET endtime | /DU duration} [/K]
[/XML xmlfile] [/V1]] [/SD startdate] [/ED enddate] [/IT] [/Z] [/F]
```

Changing a Task

The following syntax is used to change how the program runs, or change the user account and password used by a scheduled task.

```
schtasks /Change
[/S system [/U username [/P [password]]]] /TN taskname
{ [/RU runasuser] [/RP runaspassword] [/TR taskrun] [/ST starttime]
[/RI interval] [ {/ET endtime | /DU duration} [/K] ]
[/SD startdate] [/ED enddate] [/ENABLE | /DISABLE] [/IT] [/Z] }
```

O que é um Agendador de Tarefas?

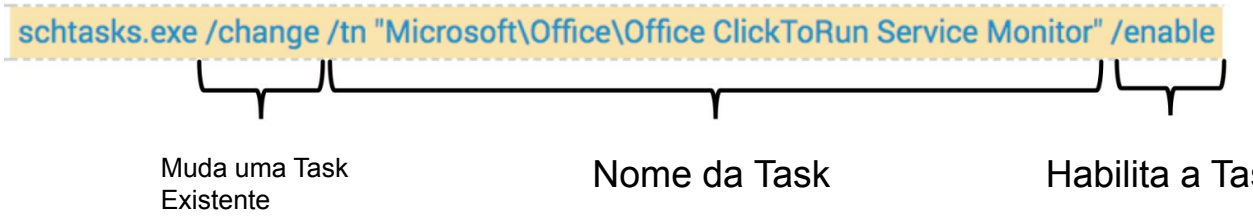
Tempest
ACADEMY
Conference

- Vamos dar uma olhada em como isso pode parecer no Windows. Uma pesquisa rápida nos levará à referência do comando schtasks.exe, onde podemos ver os argumentos da linha de comando necessários para criar uma tarefa. Isso será útil quando começarmos a procurar schtasks nos logs do Windows para determinar o que eles estão fazendo, se estiverem fazendo alguma coisa.

Quer ver no Splunk como fica um Exemplo?

Tempest [ACADEMY] Conference

Type	Field	Value	Actions
Selected	CommandLine	schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable	
	EventDescription	Process Create	
	Image	C:\Windows\System32\schtasks.exe	
	ParentCommandLine	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service	
	host	wrk-ghoppy	
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational	
	sourcetype	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	
	user	NT AUTHORITY\SYSTEM	
Event	Computer	wrk-ghoppy.frothly.local	
	CurrentDirectory	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\	



Mão na Massa

Tempest
ACADEMY
Conference

Quer ver no Splunk como fica um Exemplo?

Tempest
[ACADEMY]
Conference

```
"C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:51
/TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
NonI -W hidden -c \"IEX
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp
HKLM:\Software\Microsoft\Network debug).debug)))\""
```

/Create – cria uma nova tarefa

/F – cria a tarefa à força e suprime avisos se a tarefa existir

/RU – Especifica o contexto do usuário sob o qual a tarefa é executada - sistema

/SC – Frequência de agendamento – Diariamente

/ST – Frequência de agendamento – DiariamenteHora de início da tarefa – 10:51

/TN– Nome da tarefa – Atualizador

/TR – Caminho e nome do arquivo do executável a ser executado

Descobertas

A hipótese foi Confirmada?

Tempest
[ACADEMY]
Conference

Sim, Schedule Tasks estão sendo executadas para manter a persistência do invasor, agendando regularmente a execução de um comando do PowerShell que se conecta ao seu C2

O que Descobrimos?

Tempest
[ACADEMY]
Conference

- O agendador de tarefas está sendo usado para manter a persistência em três sistemas
- Um Powershell codificado está sendo usado para criar essas tarefas
- As tarefas têm nomes idênticos
- As tarefas são idênticas, EXCETO a hora de início
- As tarefas são projetadas para chamar a base do PowerShell que está gravada no registro
- Quatro sistemas possuem este valor no registro indicando que quatro foram inicialmente comprometidos por um não possuir este nível de persistência
- A codificação no registro e no CommandLine foi projetada para ofuscar a intenção

Diagrama de Scheduled Task

Tempest
[ACADEMY]
Conference

Hostname: wrk-btun

CommandLine:
"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST **10:26** /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""

ParentCommandLine:
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden –enc...

Hostname: wrk-klagerf

CommandLine:
"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST **10:39** /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""

ParentCommandLine:
C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 –enc...

Hostname: Venus

CommandLine:
"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST **10:51** /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""

ParentCommandLine:
C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 –enc...

Tempest
ACADEMY
Conference

O que devemos pôr em operação?

- Esta é uma pergunta difícil devido à variabilidade no uso de agendadores de tarefas
- Monitorar para:
  - Schtasks.exe que se desviam de uma linha de base de TI
  - Nomes de tarefas agendadas que não correspondem ao padrão de TI
  - Tarefas agendadas em execução sob usuários inesperados
  - Tarefas agendadas que possuem sequências de comandos fora do normal

Tempest
ACADEMY
Conference

Resources

- Splunk Enterprise (Standalone)
- Dataset BOTS V2 (Boss of the SOC)
- Burp Suite Community Edition
- MITRE
- Lockheed Martin Cyber Kill Chain

Contato

- linkedin.com/in/samuelmaranhao/

FIM

Tempest
ACADEMY
Conference

Tempest

ACADEMY

Conference 2023