heimdall

security research

A DIVISION OF ISH

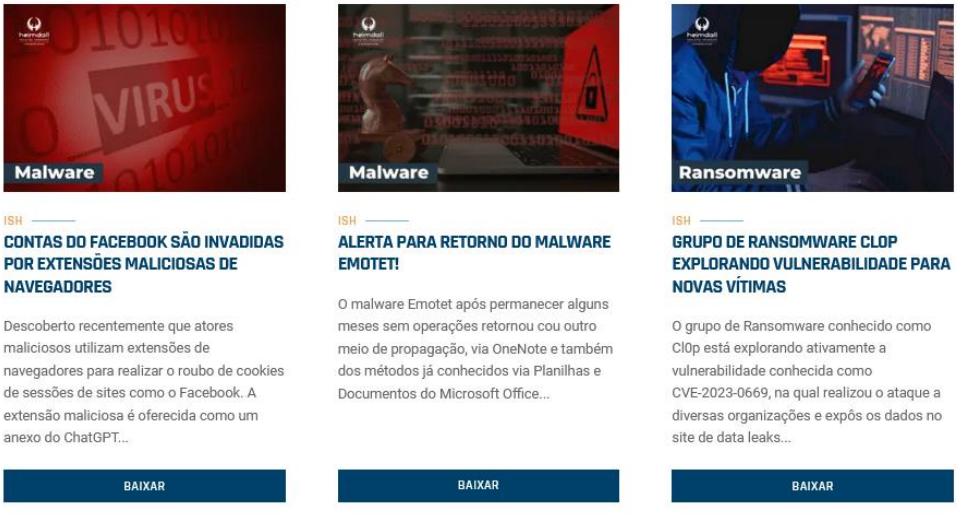
Utilização constante do PowerShell em ataques cibernéticos

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 INTRODUÇÃO

O PowerShell é uma poderosa ferramenta de linha de comando e automação desenvolvida pela Microsoft. Introduzido pela primeira vez em 2006, o PowerShell tornou-se rapidamente uma parte essencial do ecossistema do Windows e é amplamente utilizado em organizações para diversas finalidades. Ele oferece aos administradores de sistema, engenheiros de rede e profissionais de TI uma plataforma consistente e flexível para gerenciar e automatizar tarefas em ambientes Windows.

Através do PowerShell, os administradores podem interagir com o sistema operacional e com os produtos Microsoft de maneira mais eficiente do que usando interfaces gráficas tradicionais. O PowerShell permite que comandos complexos sejam executados com uma única linha de código, facilitando a automação de tarefas repetitivas e a execução rápida de operações em larga escala.

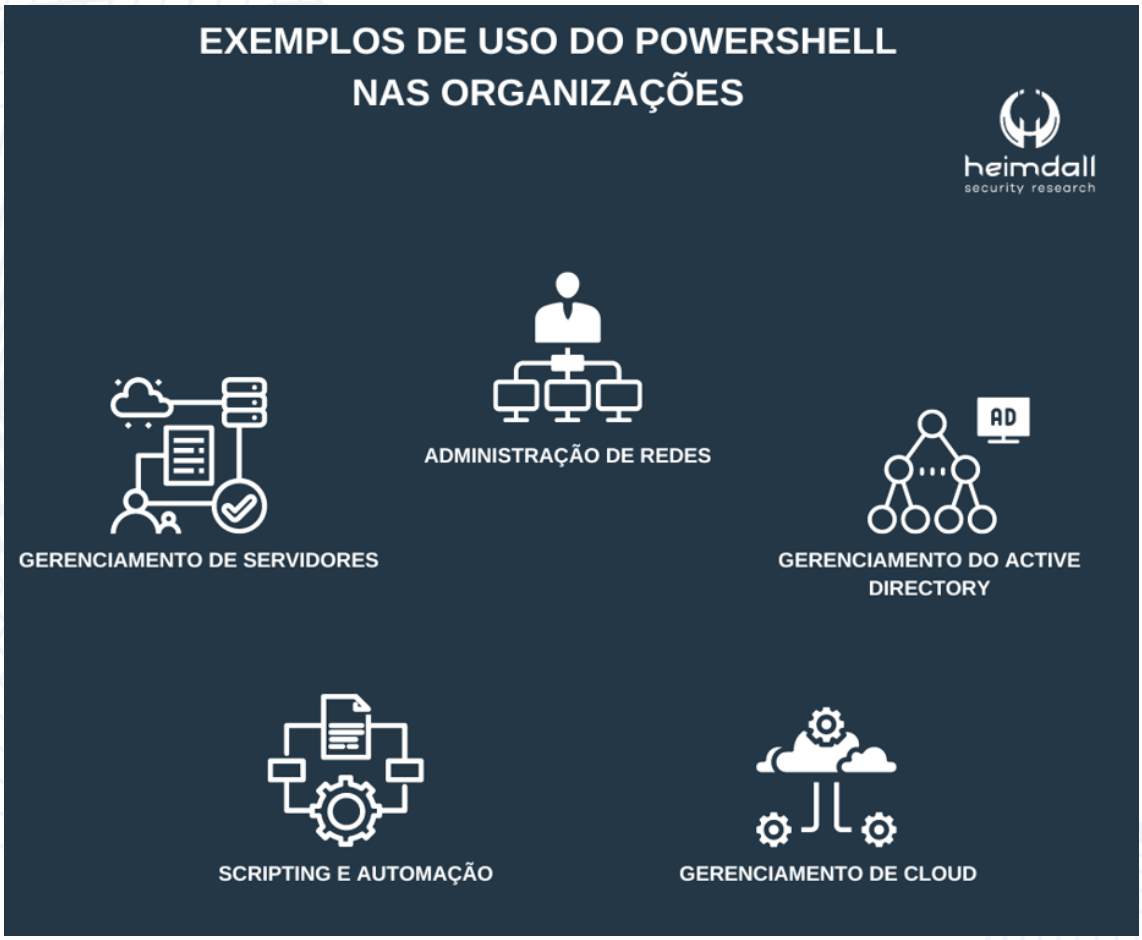


Figura 1 – Alguns dos principais uso do PowerShell nas organizações.

- **Gerenciamento de Servidores**, os administradores de sistemas usam o PowerShell para gerenciar servidores Windows, realizar tarefas de configuração, instalação de software, gerenciamento de usuários e grupos, criação e configuração de serviços e muito mais.
- **Administração de Redes**, o PowerShell permite que os engenheiros de rede configurem e monitorem dispositivos de rede, façam ações em switches, roteadores e outros equipamentos de rede.
- **Scripting e Automação**, PowerShell é uma linguagem de script completa que permite aos usuários escrever scripts para automatizar tarefas complexas e repetitivas, economizando tempo e reduzindo erros humanos.
- **Gerenciamento do Active Directory**, o PowerShell é uma ferramenta valiosa para administradores do Active Directory, permitindo a criação, modificação e exclusão de objetos do Active Directory, além de gerenciamento de políticas de grupo e outras configurações relacionadas ao AD.
- **Gerenciamento de Cloud**, com o surgimento do Azure, o PowerShell se tornou uma ferramenta essencial para gerenciar recursos e serviços na nuvem da Microsoft, como máquinas virtuais, redes, armazenamento e muito mais.

2 ABUSO DO POWERSHELL POR ATORES DE AMEAÇAS

Os atores de ameaças que violam um sistema provavelmente iniciam o utilitário de linha de comando PowerShell, usando essa técnica, os atores podem realizar o conhecimento e se mover lateralmente em uma rede, assim ganhando persistência na máquina comprometida.

A equipe de Inteligência Heimdall da ISH Tecnologia tem observado a utilização de comandos do PowerShell sendo usados em vários ataques por atores de ameaças com uma variedade de objetivos maliciosos na rede alvo, devido a flexibilidade e poder de automação do PowerShell.

Segue abaixo alguns dos principais métodos pelos quais eles fazem uso do PowerShell em suas atividades maliciosas, como por exemplo:

- **Execução de scripts maliciosos**, os atacantes criam scripts PowerShell maliciosos que podem ser executados em sistemas-alvo. Esses scripts podem ser distribuídos através de anexos de e-mail, downloads de sites comprometidos ou exploração de vulnerabilidades em serviços web. Uma vez que o usuário executa o script, o código malicioso começa a atuar no sistema infectado.
- **Download e execução de malware**, é usado o PowerShell para baixar e executar malware em sistemas comprometidos. O PowerShell oferece a capacidade de fazer solicitações de rede e baixar arquivos da Internet, permitindo que o malware seja instalado e ativado nos dispositivos da vítima.
- **Movimentação lateral**, após comprometer um sistema, os atacantes usam o PowerShell para se movimentar lateralmente na rede da organização. Eles podem explorar as credenciais obtidas, procurar outros sistemas vulneráveis e se espalhar pela infraestrutura para ampliar o impacto do ataque.
- **Comunicação de comando e controle** (**C2**), os invasores usam comandos do PowerShell para se comunicar com seus servidores C2, baixar/executar malware e exfiltrar dados confidenciais.
- **Roubo de credenciais**, o PowerShell pode ser usado para extrair credenciais de login (como senhas ou tokens) de um sistema comprometido.
- **Manipulação de dados**, é usado para modificar ou excluir arquivos, chaves de registro e outras configurações do sistema. Isso pode

interromper as operações normais do sistema e causar danos ao sistema.

- **Coleta de informações**, o PowerShell é usado para coletar informações valiosas sobre os sistemas-alvo, usuários e configurações de rede. Os atacantes podem usar comandos PowerShell para extrair credenciais armazenadas, informações de registro, detalhes de configuração do sistema e muito mais.
- **Ofuscação de atividades maliciosas**, para evitar a detecção de suas atividades, os atacantes frequentemente usam técnicas de ofuscação para tornar o código PowerShell menos visível para os mecanismos de segurança. Eles podem codificar o script em Base64 ou usar outras técnicas de camuflagem para evitar a detecção de assinaturas de antivírus.
- **Criptografia de dados**, os atores de ameaças também podem usar o PowerShell para criptografar arquivos e dados no sistema da vítima, tornando-os inacessíveis até que um resgate seja pago.

Devido a essa flexibilidade, o PowerShell é frequentemente usado em ataques de "***Living off the Land***" (**LOL**) pelos atores de ameaças. O LOL é uma abordagem em que os atacantes utilizam ferramentas, scripts e recursos legítimos do sistema operacional para conduzir suas atividades maliciosas, tornando mais difícil para as soluções de segurança detectarem e bloquearem seus comportamentos.

3 COMANDOS UTILIZADOS POR ATORES DE AMEAÇAS

Os atores de ameaças podem utilizar uma variedade de comandos do PowerShell em seus ataques cibernéticos, aproveitando a flexibilidade e o poder dessa ferramenta. Abaixo estão alguns exemplos de comandos do PowerShell comumente utilizados em atividades maliciosas:

- **Get-Process**, usado para listar os processos em execução no sistema. Atacantes podem usam esse comando para identificar processos em execução, incluindo aqueles associados a softwares de segurança, para evitá-los ou interrompê-los.
- **Get-Service**, utilizado para listar os serviços em execução no sistema. Os atacantes verificam quais serviços estão ativos e, se necessário, interrompê-los para facilitar suas atividades maliciosas.
- **Get-WmiObject**, permite que os atacantes recuperem informações do Windows Management Instrumentation (WMI), incluindo detalhes do sistema, configurações de segurança e informações sobre os usuários.
- **Get-NetAdapter**, usado para obter informações sobre as placas de rede do sistema. Isso pode ajudar os atacantes a entender a configuração da rede e identificar alvos potenciais para movimentação lateral.
- **Get-ChildItem**, equivalente ao comando "dir" no prompt de comando. Os atacantes usam esse comando para listar arquivos e diretórios em um sistema.
- **Invoke-WebRequest**, utilizado para fazer solicitações HTTP/HTTPS. Os atacantes usam esse comando para baixar arquivos maliciosos ou para interagir com servidores de comando e controle.
- **Invoke-Expression** (**iex**), permite que os atacantes executem comandos ou scripts a partir de uma string. Isso pode ser usado para executar comandos maliciosos sem a necessidade de gravá-los em disco.
- **New-Object**, permite a criação de objetos PowerShell, incluindo objetos COM (Component Object Model) e outros tipos de objetos que podem ser usados para fins maliciosos.
- **Start-Process**, utilizado para iniciar um processo. Os atacantes usam esse comando para iniciar aplicativos ou executar scripts maliciosos.

- **Set-MpPreference**, comando é usado para alterar as configurações do Windows Defender, permitindo que os atacantes desativem ou contornem as proteções de segurança.
- **Get-ADDomain**, atacantes utilizam para obter uma lista de domínios no diretório.
- **Get-ADUser**, utilizado para obter uma lista de usuários.
- **Get-ADComputer**, usado para obter informações detalhadas sobre cada host.

4 Importância de um time de Inteligência de ameaças cibernéticas (CTI)

O time de Inteligência de Ameaças Cibernéticas desempenha um papel crucial na detecção, análise e mitigação de ataques relacionados ao PowerShell e Living off the Land (LOL). Esses tipos de ataques são especialmente desafiadores, pois os atacantes exploram ferramentas legítimas do sistema operacional para conduzir suas atividades maliciosas, tornando-os mais difíceis de detectar pelas soluções de segurança tradicionais.

Ao contar com um time de Inteligência de Ameaças Cibernéticas eficaz, as organizações podem aumentar sua capacidade de detectar e responder a ataques que se aproveitam do PowerShell e LOL. A combinação de análises avançadas, desenvolvimento de regras personalizadas e monitoramento proativo é essencial para proteger os ambientes de TI contra essas ameaças cada vez mais sofisticadas.

5 Conclusão

Salientamos que o PowerShell é uma ferramenta legítima e poderosa para gerenciamento, automação de sistemas e integração em ambientes corporativos, amplamente utilizado por administradores de sistemas e profissionais de TI. No entanto, é importante lembrar que, como toda ferramenta poderosa, o seu uso indevido por atores de ameaças em ataques cibernéticos pode levar a sérios danos e comprometer a segurança das organizações.

Portanto, é essencial que as organizações implementem práticas de segurança adequadas, como o controle de acesso ao PowerShell e o monitoramento de atividades suspeitas, para evitar o uso malicioso dessa ferramenta.

6 RECOMENDAÇÕES

Listadas pela ISH, as medidas abaixo poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

- **Restrição do uso do PowerShell**, restringir o uso do PowerShell apenas a usuários autorizados e scripts assinados por editores confiáveis.
- **Adoção e medidas de proteção de borda,** como *Firewall*, IDS/IPS, *Honeypots*, MDR/XDR e outras soluções de segurança.
- **Não realizar o *download* de artefatos contidos em e-mails suspeitos** e não clicar em *links* de e-mails que apresentarem ter comportamento malicioso.
- **Adoção de medidas de antivírus,** visando verificar e varrer constantemente toda a infraestrutura e ativos utilizados.
- **Implemente o registro e monitoramento do PowerShell**, o PowerShell gera logs detalhados que podem ajudar a detectar atividades suspeitas. As organizações podem habilitar o log do PowerShell e monitorar os logs em busca de atividades incomuns, como a execução de comandos ou scripts suspeitos.
- **Monitoramento proativo**, implemente soluções de monitoramento e análise de logs para detectar atividades suspeitas relacionadas ao PowerShell. Fique atento a padrões de execução de comandos incomuns, ofuscação de scripts e tentativas de movimentação lateral.
- **Whitelisting**, mantenha uma lista de aplicativos e comandos autorizados que podem ser executados no ambiente. Isso ajuda a restringir o uso do PowerShell apenas a tarefas permitidas e evita a execução de comandos desconhecidos.
- **Atualizações e patches**, mantenha o PowerShell e outros componentes do sistema operacional atualizados com as últimas correções de segurança. Isso ajudará a corrigir vulnerabilidades conhecidas e evitar a exploração de falhas conhecidas.
- **Controle de acesso**, gerencie cuidadosamente as permissões de acesso ao PowerShell. Apenas usuários que realmente precisam usar o PowerShell devem ter permissões para fazê-lo. Evite fornecer privilégios de administrador desnecessariamente.
- **Políticas de senhas**, implemente políticas de senhas fortes e autenticação multifator para proteger as credenciais dos usuários.

Isso tornará mais difícil para os atacantes obterem acesso não autorizado ao sistema.

- **Conscientização dos usuários**, eduque os usuários sobre os riscos associados ao uso do PowerShell e a importância de evitar a execução de scripts desconhecidos ou provenientes de fontes não confiáveis.
- **Segmentação de redes**, considere a segmentação da rede para limitar o movimento lateral em caso de comprometimento. Isso impede que um ataque se espalhe facilmente para outros segmentos da rede.
- **Bloqueio de scripts maliciosos**, use soluções de segurança que possam identificar e bloquear scripts maliciosos ou comportamentos maliciosos do PowerShell em tempo real.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Forbes**
- **Mitre Att&ck**

heimdall
security research

A DIVISION OF ISH