
Noisybear explora arquivos ZIP para carregadores e dados do PowerShell

Data: 2025-09-04 16:29:21

Autor: Inteligência Against Invaders

O ator de ameaças conhecido como NoisyBear lançou um sofisticado esforço cibernético chamado Operação Barreldfire, usando iscas de phishing especialmente projetadas que imitam a correspondência interna para o setor energético do Alvo do Cazaquistão, particularmente os trabalhadores do major estatal de petróleo e gás Kazmunaigas.

Pesquisadores de segurança do Seqrite Labs observaram a campanha pela primeira vez em abril de 2025 e observaram sua rápida escalada até maio.

A atração de phishing de lança imita os avisos de RH

O vetor de ataque inicial de Noisybear confiou em um e-mail comprometido do Departamento de Finanças na Kazmunaigas.

Em 15 de maio de 2025, os funcionários receberam mensagens com a linha de assunto urgente “Urgente! Revise o cronograma de salário atualizado”.

O órgão de e-mail instruiu os destinatários – em russo e cazaque – para baixar e extrair um arquivo zip chamado ???producking.zip (“schedule.zip”) e depois abrir um arquivo de atalho, ???ordar ??????.lnk (“Salary.lnk”), para a ser atualizada para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas para serem atualizadas.

A mensagem criou urgência impondo um prazo de conformidade e até referenciou a equipe de suporte de TI para melhorar a legitimidade.

Sob o capô, o Arquivo Zip continha três itens: um documento de engodo com o logotipo Kazmunaigas, um readme.txt com instruções do usuário e o malicioso .Lnk atalho.

Depois de executado, o atalho usou o próprio binário do PowerShell do Windows para baixar um script em lote de um servidor remoto em 77.239.125.41:8443, colocando -o na pasta “C: Users public” e iniciando -o automaticamente.

Cadeia de infecção de vários estágios revelada

Os pesquisadores dissecaram a cadeia de infecções em quatro estágios distintos:

1. Implantação de scripts em lote

O download inicial de lote (123.bat e it.bat) buscou dois scripts do carregador PowerShell – Support.ps1 e A.PS1 – da infraestrutura do atacante.

Cada script incluiu uma pausa deliberada (10 a 11 segundos) antes de executar para evitar ambientes de sandbox.

2. AMSI Bypass e execução do carregador

O script suport.ps1 alavancado .NET Reflection para desativar a interface de varredura anti-malware do Windows (AMSI) lançando o interno `amsilnitFailed` sinalizador, permitindo que as cargas úteis subsequentes carreguem sem controle.

O segundo script resolveu dinamicamente as funções da API do Windows para execução de código na memória e depois injetou o codificador de casca reversa do medidor no *explorer.exe* Processo usando o `CreateremOteThread`.

3. DLL Implant e seqüestro de threads

A carga útil final foi um implante de DLL de 64 bits que imponente um mecanismo de instância único por meio de semáforos e eventos nomeados.

Ele gerou um suspenso `rundll32.exe` Processo, sequestrou seu contexto de encadeamento, alocou a memória RWX e injetou uma carga útil de shell reversa antes de retomar a execução.

4. Comando e controle e persistência

Uma vez que a concha reversa foi estabelecida, os operadores da NoisyBear poderiam exfiltrar dados sensíveis-particularmente credenciais e documentos internos-e potencialmente manter o acesso a longo prazo às redes da empresa.

Os caçadores de ameaças da Seqrite descobriram que a infraestrutura de Noisybear foi hospedada em servidores sob o provedor de hospedagem russo sancionado AEZA Group LLC.

Um reconhecimento adicional revelou aplicativos da Web adicionais maliciosos que disfarçaram sites de bem-estar e fitness, provavelmente servindo como hubs de comando e controle alternativos.

Análise das ferramentas e técnicas-uso extensivo do PowerShell, injeção reflexiva de DLL, seqüestro de contexto de rosca, resolução dinâmica da API e comentários de língua russa em scripts-alinham-se com os grupos de ciberconexões de língua russa conhecidas.

Erros operacionais, como reutilizar domínios de host remota e estagiários compartilhados, fortaleceram a atribuição.

Recomendações de defesa e indicadores técnicos

Para se proteger contra incursões semelhantes, as equipes de segurança devem:

- Aplique a filtragem e a caixa de areia de e-mail rigorosos e o acessório, principalmente para arquivos de arquivamento que contêm executáveis ??ou atalhos.
- Ative as técnicas de registro da AMSI e bloqueie as técnicas conhecidas de lolbin (vivendo o binário da terra).
- Monitor System.Management.Automation.AmsiUtils ou padrões refletivos de carregamento de código.
- Realize a caça regular de ameaças para semáforos e eventos nomeados vinculados à injeção de DLL não autorizada.

Seqrite Labs também [publicado](#) Indicadores extensos de compromisso (IOCs), incluindo hashes de arquivos para os estágios ZIP, LNK, LOTA, POWERSHELL e DLL, bem como domínios C2 e IPs do Noisybear:

Com o setor energético da Ásia Central cada vez mais sob o microscópio, as organizações devem permanecer vigilantes e adotar as defesas em camadas contra esforços de intrusão altamente personalizados e de vários estágios, como a Operação Barrelfire.

Indicadores de compromisso (COI):

Baseado em arquivo

Tipo de arquivo

Panorama	SHA-256 5168A1E22EE969DB7CEA0D3E9EB64DB4A0C6 48EEE43DA8BACF4C7126F58F0386
Zip	021B3D53FE113D014A9700488E31A6FB5E16C B02227DE5309F6F93AFFA4515A6
Zip	F5E7DC5149C453B98D05B73CAD7AC1C42B38 1F72B6F7203546C789F4E750EB26
Lnk	A40E7EB0CB176D2278C4AB02C4657F9034573 AC83CEE4CDE38096028F243119C
Lnk	26F009351F4C645AD4DF3C1708F74AE2E5F8D 22F3B0BBBB4568347A2A72651BEE
Script em lote	D48EB6AFCC5A3834B3E4CA9E0672B61F9D94 5DD41046C9AAF782382A6044F97
Script em lote	1EECF1C607BE3891E955846C7DA70B0109D B9F9FDF01DE45916D3727BFF96E0
Powershell	DA98B0CBCD784879BA38503946898D747ADE0 8ACE1D4F38D0FB966703E078BBF
Powershell	6D6006EB2BAA75712BFE867BF5E4F09288A7D 860A4623A4176338993B9DDFB4B
Powershell	FB0F7C35A58A02473F26AABEA4F682E2E483D B84B606DB2ECA36AA6C7E7D9CF8
Dll	1BFE65ACBB9E509F80EFCFE04B23DAF31381 E8B95A98112B81C9A080BDD65A2D

Baseado em rede

Domínios / ips

77[.]239[.]125[.]41
WellFitPlan[.]ru

Domínios / ips

178[.]159[.]94[.]8

MITRE ATT & CK Mapping

Tática	ID da técnica	Nome
Reconhecimento	T1589.002	Reunir informações de identidade da vítima: endereços de e -mail
Acesso inicial	T1204.002	Execução do usuário: arquivo malicioso
	T1078.002	Contas válidas: contas de domínio
Execução	T1059.001	Intérprete de comando e script: PowerShell
	T1059.00	Intérprete de comando e script
Evasão de defesa	T1562	Prejudicar as defesas
	T1027.007	Arquivo criptografado/codificado
	T1027.013	Resolução dinâmica da API
	T1055.003	Seqüestro de execução de threads
	T1620	Carregamento de código reflexivo
Comando e controle	T1218.011	Execução de proxy binária do sistema: runndll32
	T1105	Transferência de ferramentas de entrada
	T1567.002	Exfiltração ao armazenamento em nuvem

Encontre esta história interessante! Siga -nos [LinkedIn](#) [X](#) Para obter mais atualizações instantâneas.