# Yurei Ransomware usa o PowerShell para implantar criptografia de arquiv

Data: 2025-09-15 06:58:20

Autor: Inteligência Against Invaders

Um grupo de ransomware recém-descoberto chamado Yurei surgiu com recursos sofisticados de criptografia, direcionando as organizações por meio de táticas de dupla extensão e aproveitando o código de código aberto para dimensionar rapidamente as operações.

Observado pela primeira vez em 5 de setembro de 2025, esse ransomware baseado em GO emprega o algoritmo de criptografia chacha20 e comandos de powershell para comprometer os sistemas de vítimas, marcando outra evolução no ecossistema de ransomware como serviço.

Diagrama de fluxo ilustrando os estágios de um ataque de ransomware de extorsão dupla da preparação inicial do vetor à exfiltração de dados e criptografia de ransomware

A Pesquisa de Check Point (RCP) identificou Yurei como uma operação de ransomware de rápido crescimento que já se expandiu de uma vítima para três nos primeiros dias de operação.

A meta inicial do grupo era uma empresa de fabricação de alimentos do Sri Lanka, seguida pelas vítimas na Índia e na Nigéria, demonstrando sua estratégia de expansão agressiva em várias regiões geográficas.

O grupo de ransomware opera sob um modelo de dupla extorsão, combinando a criptografia de arquivo com a exfiltração de dados para maximizar a pressão sobre as vítimas.

Essa abordagem criptografa os arquivos da vítima enquanto rouba informações confidenciais, exige pagamentos de resgate tanto para chaves de descriptografia quanto para impedir a liberação pública de dados roubados.

Como Yurei afirma explicitamente em seu blog Darknet, “o medo e as implicações do vazamento de dados são seu principal ponto de pressão para fazer com que as vítimas paguem o resgate”.

Captura de tela mostrando o ambiente de programação e o terminal com uma sobreposição destacando o desenvolvimento de malware na linguagem de programação GO

## Yurei Ransomware

Investigação por CPR revelado O fato de o ransomware de Yurei ser derivado do Prince-Ransomware, uma família de ransomware de código aberto disponível no GitHub com apenas pequenas modificações.

Essa descoberta destaca uma tendência preocupante em que os cibercriminosos aproveitam o

código de malware prontamente disponível para iniciar operações sem exigir extensas habilidades de desenvolvimento.

O ransomware é escrito na linguagem de programação GO, que apresenta desafios de detecção para alguns fornecedores de antivírus, oferecendo recursos mais fáceis de desenvolvimento e compilação de plataformas cruzadas.

Notavelmente, os atores de ameaças cometeram um erro crítico ao não remover símbolos do binário, permitindo que os pesquisadores identifiquem nomes de função e módulos que indicam claramente a base de código Prince-Ransomware.

Técnicas de malware comuns explorando Powershell e vulnerabilidades do ambiente do Windows

O malware segue uma abordagem sistemática da criptografia:

- Enumera todas as unidades disponíveis no sistema infectado.
- Encrypts arquivos em paralelo em várias unidades.
- Anexa a extensão .yurei a arquivos criptografados.
- Tentativas de definir um papel de parede personalizado.
- Monitora continuamente para unidades de rede recém -anexadas.

A Yurei emprega o algoritmo chacha20 para criptografia de arquivo, gerando teclas e não -ces aleatórios exclusivos para cada arquivo. O ransomware criptografa a chave chacha20 e o nonce usando o ECIES (esquema de criptografia integrado da curva elíptica) com a chave pública do atacante.

Os arquivos criptografados armazenam a chave criptografada, nonce e o conteúdo de arquivos separado por “||” caracteres, criando um formato estruturado para descriptografia posterior.

Diagrama de blocos mostrando o processo de criptografia simétrica Chacha20-Poly1305 com núcleos de chacha20 paralelos e poli1305 para autenticação

## Vulnerabilidades do comando do PowerShell

O ransomware incorpora os comandos do PowerShell herdados diretamente do príncipeRansomware Base de código sem modificação.

Esses comandos foram projetados para baixar e definir um papel de parede personalizado, mas os desenvolvedores Yurei não forneceram um URL válido para o download do papel de parede.

Essa supervisão faz com que o comando do PowerShell seja um erro, resultando em Windows em um fundo de cor sólido em vez de exibir um papel de parede de mensagem de resgate.

Essa falha técnica, combinada com a preservação de símbolos de depuração no binário, demonstra o nível de habilidade relativamente baixo dos operadores por trás de Yurei.

Os atores de ameaças parecem ter usado o construtor Prince-Ransomware sem entender ou modificar sua funcionalidade principal.

Apesar de seus recursos de criptografia, o Yurei contém uma vulnerabilidade significativa que pode

permitir a recuperação parcial do arquivo.

O ransomware falha em excluir cópias de sombra de volume (VSS), instantâneos de backup embutidos do Windows que permitem a recuperação do sistema para os estados anteriores.

Essa supervisão significa que organizações com VSS ativadas podem potencialmente restaurar arquivos para instantâneos anteriores sem pagar o resgate.

No entanto, esse método de recuperação aborda apenas o aspecto de criptografia do ataque e não protege contra a exfiltração de dados.

Como Yurei opera sob um modelo de dupla extorsão, as vítimas permanecem vulneráveis ??a ter seus dados roubados publicados, mesmo que recuperem com sucesso arquivos criptografados por meio de cópias de sombra.

A análise dos padrões de envio e artefatos de código sugere que os atores de ameaças podem se basear no Marrocos.

Todas as amostras de ransomware foram submetidas ao Virustotal a partir de endereços IP marroquinos, com uma amostra sem um ID de ingresso, indicando potencialmente um acúmulo de teste enviado pelos próprios desenvolvedores.

Evidências adicionais incluem comentários árabes encontrados no código-fonte HTML da página de negociação de Yurei.

Como resultado, avaliamos com baixa confiança de que o ator de ameaças está sediado no Marrocos.

## Implicações para defesa de segurança cibernética

O surgimento de yurei demonstra como o malware de código aberto reduz significativamente as barreiras à entrada para cibercriminosospermitindo que os atores de ameaças menos qualificados lançem operações sofisticadas de ransomware.

Essa tendência apresenta desafios para os defensores, pois acelera a proliferação de variantes de ransomware, enquanto dificulta a atribuição.

As organizações devem implementar estratégias abrangentes de backup, incluindo a ativação do VSS, manter controles de segurança atualizados e preparar procedimentos de resposta a incidentes especificamente projetados para cenários de extensão dupla.

A mudança para a extorsão baseada em roubo de dados significa que as estratégias tradicionais de backup e recuperação sozinhas são proteção insuficiente contra as ameaças modernas de ransomware.

O rápido crescimento de uma a três vítimas em poucos dias indica que os operadores de Yurei estão buscando ativamente expandir suas operações, tornando essencial que as equipes de segurança monitorem indicadores de compromisso associados a essa ameaça emergente.

## Indicadores de compromisso

| Descrição | Valor |
|---|---|
| Página de cebola | poucoscret5rhoy66k6c4cyvb2pqrblxtx4mekj3s5l4jjt4t4kn4vheyd.onion |
| Yurei Ransomware | 49C720758B8A87E42829FFB38A0D7FE2A8C36DC3007ABFABBEA76155185D2902 |
| Yurei Ransomware | 4F88D3977A24FB160FC3BA69821287A197AE9B04493D705DC2FE939442BA6461 |
| Yurei Ransomware | 1EA37E077E6B2463B8440065D5110377E2B4B4283CE9849AC5EFAD6D664A8E9E |
| Yurei Ransomware | 10700EE5CAAD40E74809921E11B7E3F2330521266C822CA4D21E14B22EF08E1D |
| Yurei Ransomware | 89A54D3A38D2364784368A40AB228403F1F1C1926892FE8355AA29D00EB36819 |
| Yurei Ransomware | F5E122B60390BDCC1A17A24CCE0CBCA68475AD5ABEE6B211B5BE2DEA966C2634 |
| Yurei Ransomware | 0303F89829763E734B1F9D4F46671E59BFAA1BE5D8EC84D35A203EFBFCB9BB15 |
| Satanlockv2 Ransomware | AFA927CA549AABA66867F21FC4A5D653884C349F8736ECC5BE3620577CF9981F |
| Satanlockv2 Ransomware | D2539173BDC81503BF1B842A21D9599948E957CADC76A283A52F5849323D8E04 |

**Encontre esta história interessante! Siga -nos**LinkedIn**e**X**Para obter mais atualizações instantâneas**.