CIBER BOLETIM
Royal Ransomware

Tem-se aumentado o número de ataques de Ransomware que empregam a variante intitulada "Royal Ransomware" em escala global.

As investidas são direcionadas, sobretudo, para sistemas Windows, servidores ESXi e plataformas Linux, sendo que os alvos mais frequentes são os datacenters corporativos.

O modus operandi do Ransomware envolve a utilização de um esquema de dupla extorsão, no qual são extraídas informações empresariais sensíveis e, caso a vítima não efetue o pagamento exigido para o resgate, há ameaças de divulgação pública desses dados.

Exploração

Verificou-se o emprego de phishing por meio de arquivos PDF nocivos e a exploração de protocolos, tais como o RDP. A origem do ataque consiste na utilização de credenciais de VPN expostas.

No processo do ataque, são utilizados diversos recursos de tunelamento para viabilizar a comunicação entre servidores, e são também empregadas ferramentas com o objetivo de possibilitar movimentação lateral e persistência.

Prevenção

Recomenda-se as seguintes medidas, para prevenção:

- A implementação de política de backup que contemple os procedimentos e testes de restauração, com a previsão de locais seguros e fisicamente segmentados para armazenamento de mídias, além de um plano de recuperação;
- A segmentação de redes pode ser uma medida preventiva contra a propagação de ransomware e o movimento lateral, e o uso de ferramentas EDR pode ajudar na detecção de atividades suspeitas ou maliciosas nos endpoints;
- Para aumentar a segurança dos hipervisores utilizados pela organização, é importante manter um programa de atualização e acompanhar os boletins de segurança disponíveis em https://www.vmware.com/security/advisories.html;
- A política de controle de senhas da organização deve ser executada de forma efetiva, observando as recomendações para processos de autenticação, ciclo de vida de autenticadores e controle de acesso lógico disponíveis em https://pages.nist.gov/800-63-3/sp800-63b.html;
- É recomendável adotar a autenticação de multifator (MFA) para todos os serviços críticos, como e-mail e redes virtuais privadas (VPN);
- Para dificultar a escalada de privilégios e o movimento lateral, é importante desativar o uso da linha de comando e permissões de execução de scripts em estações de trabalho.