Hackers roubam segredos e credenciais das janelas não detectadas pela E

Data: 2025-08-25 06:54:53

Autor: Inteligência Against Invaders

Um pesquisador de segurança cibernética revelou um novo método sofisticado para extrair

credenciais e segredos do Windows que evita com êxito a detecção pela maioria das soluções de

detecção e resposta de terminais (EDR) atualmente implantadas em ambientes corporativos.

A técnica, apelidada de “Silent Harvest”, aproveita as APIs obscuras do Windows para acessar dados de registro sensíveis sem acionar alertas de segurança comuns.

A inovação representa um avanço significativo em Operações da equipe vermelha e destaca lacunas críticas na forma como as soluções de segurança monitoram as atividades do sistema.

Diferentemente dos métodos tradicionais de colheita de credenciais que são cada vez mais detectados e bloqueados pelas defesas modernas, essa abordagem opera inteiramente na memória sem criar artefatos reveladores que os produtos EDR normalmente monitoram.

Detecção de coleta de credenciais aumenta

As técnicas tradicionais de extração de credenciais do Windows tornaram -se cada vez mais confiáveis ??à medida que as soluções de segurança evoluíram.

A maioria dos métodos existentes depende de abordagens bem conhecidas, como a criação de cópias de backup de colméias de registro sensíveis, permitindo acesso ao registro remoto ou interagindo diretamente com o processo de Serviço de Subsistema de Segurança Local (LSASS) fortemente monitorado.

A Autoridade de Segurança Local do Windows gerencia as credenciais através de dois componentes críticos:

- **Banco de dados SAM**: Armazena usuários do Windows, grupos e credenciais locais em formato criptografado.
- **Banco de dados de política de segurança**: Contém credenciais de domínio em cache, Chaves da máquinae segredos da LSA.
- **Armazenamento de registro**: Ambos os bancos de dados correspondem ao SAM protegido e às colméias do registro de segurança no disco.
- **Requisitos de acesso**: O acesso padrão normalmente requer privilégios no nível do sistema para interação direta do registro.

No entanto, o acesso a essas colméias de registro protegidas normalmente requer privilégios no nível do sistema e gera evidências forenses significativas.

Os métodos atuais geralmente envolvem a criação de cópias de backup de colméias de registro no disco ou permitir serviços de registro remoto, os quais deixam indicadores claros de compromisso que as ferramentas de segurança modernas detectam prontamente.

As soluções modernas da EDR empregam mecanismos sofisticados de detecção centrados nas rotinas de retorno de chamada no modo de kernel que monitoram eventos críticos do sistema.

Esses produtos de segurança registram retornos de chamada no kernel do Windows usando funções como o CMRegisterCallBackBex para receber notificações sempre que ocorrerem operações de registro.

Quando as tentativas de acesso ao registro são feitas, o kernel fornece aos drivers de EDR informações detalhadas de contexto, incluindo o tipo de operação específico e o caminho completo da chave ou valor do registro direcionado.

Isso permite que as soluções de segurança identifiquem atividades suspeitas direcionadas a locais sensíveis, como HKLM SAM e HKLM Security.

Para manter o desempenho do sistema, Produtos EDR Monitore seletivamente apenas as operações de registro mais relevantes para a segurança, em vez de rastrear todos os eventos do sistema.

Essa abordagem focada lhes permite detectar tentativas de colheita de credenciais, minimizando o impacto do desempenho nas operações normais do sistema.

Colheita silenciosa via Windows APIs

O novo método de colheita silencioso contorna as restrições de controle de acesso e a detecção de EDR combinando duas APIs subutilizadas do Windows.

A técnica usa o NTopenKeyEx com o sinalizador reg_option_backup_restore, que ignora a lista de controle de acesso normal (ACL) quando o chamador ativou o sebackupprilege.

Mais criticamente, o método emprega RegQueryMultipleValuesw para ler os valores do registro em vez de APIs comumente monitoradas como RegQueryValueExw ou NtQueryValueKey.

Essa função raramente usada parece ter sido ignorada pelos fornecedores da EDR ao desenvolver suas regras de monitoramento, permitindo acessar dados confidenciais sem acionar alertas de segurança.

Testando em várias plataformas EDR confirmado Que o RegQueryMultipleValuesw chama contra valores de registro altamente sensíveis geraram alertas de segurança zero.

Toda a operação ocorre na memória sem criar backups do Registry Hive ou chamando APIs com frequência, dificultando a detecção com as soluções de segurança atuais.

Esta pesquisa ressalta o jogo em andamento de gato e rato entre pesquisadores de segurança e tecnologias defensivas, destacando como a funcionalidade do sistema esquecida pode fornecer novos caminhos para contornar os controles de segurança estabelecidos.

Encontre esta notícia interessante! Siga -nosGoogle NewsAssim,LinkedIneXPara obter atualizações instantâneas!