O novo Tinkywinkey Trojan tem como alvo os sistemas Windows com sofi

Data: 2025-09-02 08:17:12

Autor: Inteligência Against Invaders

Um sofisticado novo malware KeyLogger apelidado de “TinkywinKey” que está visando sistemas

Windows com recursos avançados de furtividade e recursos abrangentes de exfiltração de dados.

Primeiro observado No final de junho de 2025, esse malware representa uma evolução significativa na tecnologia KeyLogging, combinando vários vetores de ataque para manter a persistência e evitar a detecção.

O Tinkywinkey opera através de uma arquitetura de componentes duplos que maximiza a furtividade e a eficácia.

O malware consiste em um serviço tinky que gerencia a persistência e a integração do sistema, ao lado do WinKey Keylogger Componente responsável pela captura de dados e operações de monitoramento.

O componente de serviço estabelece a integração profunda do sistema, registrando -se como um serviço legítimo do Windows com a configuração automática de inicialização.

Essa abordagem garante que o malware seja ativado durante todos os ciclos de inicialização do sistema, mantendo a operação contínua sem a necessidade de interação do usuário.

O tópico do trabalhador do serviço inicia especificamente o executável da carga útil na sessão do usuário ativo, permitindo que o malware opere com privilégios apropriados enquanto permanece invisível para a observação casual.

Recursos sofisticados de coleta de dados

O que distingue o Tinkywinkey dos Keyloggers convencionais é sua funcionalidade abrangente de perfil do sistema.

O malware coleta sistematicamente informações detalhadas de hardware e software, incluindo especificações da CPU, capacidade de memória, detalhes da versão do sistema operacional e dados de configuração de rede.

Em seguida, ele preenche a estrutura rtl_osversionInfow com detalhes, como versão principal, versão menor e número de construção.

Essa fase de reconhecimento permite que os invasores entendam minuciosamente o ambiente de destino antes de prosseguir com a colheita de credenciais.

O próprio mecanismo de keylogging emprega ganchos de teclado de baixo nível que interceptam todos os eventos de pressionamento de tecla em todo o sistema.

Ao contrário do KeyLoggers básicos que capturam apenas a entrada alfanumérica padrão, o TinkywinKey processa com precisão chaves especiais, chaves de função, controles de mídia e caracteres unicode em vários layouts de idiomas.

O malware rastreia dinamicamente as alterações no layout do teclado, garantindo uma captura precisa quando os usuários alternam entre diferentes linguagens ou métodos de entrada.

Tinkywinkey demonstra sofisticação notável em suas técnicas de persistência e evasão.

O malware utiliza Injeção de DLL Para incorporar sua carga útil nos processos de sistema confiável, particularmente direcionando o explorer.exe para se misturar com a atividade legítima do sistema.

Essa técnica de injeção envolve alocação precisa de memória dentro do processo de destino, seguido pela criação de rosca remota que força o processo do host a carregar a DLL maliciosa.

O malware mantém a operação contínua por meio de um loop de mensagem dedicado que processa alterações de foco na janela e eventos do teclado.

A função get_ram_info () coleta detalhes sobre a memória física da máquina da vítima. Ele aproveita a API Windows GlobalMemoryStatusex () para consultar os recursos totais do sistema.

Ao monitorar as transições da janela em primeiro plano, o Tinkywinkey correlaciona as teclas capturadas com aplicativos específicos, permitindo que os invasores identifiquem quando as vítimas estão acessando portais bancários, clientes de email ou outras plataformas sensíveis.

Exfiltração de dados e armazenamento

Todas as informações capturadas são sistematicamente armazenadas nos arquivos de log codificados UTF-8 no diretório temporário do sistema.

O serviço está configurado com um tipo de inicialização automática, permitindo que o malware alcance a persistência, garantindo que o serviço seja chamado toda vez que o sistema inicializa. Isso garante que o KeyLogger permaneça ativo sem a necessidade de interação do usuário.

O mecanismo de registro emprega operações de arquivo no modo de anexo para garantir que nenhuma perda de dados ocorra durante os períodos de monitoramento estendido. Os registros de data e hora acompanham todos os eventos registrados, fornecendo aos atacantes que linhas de tempo detalhadas dos padrões de atividade do usuário.

A capacidade do malware de capturar metadados abrangentes do sistema, juntamente com os dados do pressionamento de tecla, aprimora significativamente o valor das informações roubadas.

Os invasores podem aproveitar as especificações de hardware, os detalhes da rede e as configurações de software para planejar fases de ataque subsequentes ou identificar metas de alto valor em redes comprometidas.

O Tinkywinkey representa uma evolução preocupante em ameaças de terminais, principalmente

para organizações que dependem das soluções antivírus tradicionais. O modelo de persistência baseado em serviços e os recursos de injeção de processo baseados em serviços permitem evitar muitos mecanismos de detecção convencionais.

Nos dias 24 e 25 de junho, o Tinkywinkey – ainda outro Windows 10 O KeyLogger foi identificado e acredita -se ser publicado por um usuário, que afirma estar baseado em Lyon, França.

As equipes de segurança devem priorizar abordagens de monitoramento comportamental que identificam registros incomuns de serviço, padrões inesperados de carregamento de DLL e operações persistentes de arquivos em diretórios temporários.

Monitoramento da rede para soluções suspeitas de comunicações de saída e detecção de terminais capazes de identificar instalações de gancho de baixo nível são medidas defensivas essenciais.

O surgimento de Tinkywinkey ressalta a sofisticação contínua de ameaças modernas de malware. As organizações devem adotar estratégias de segurança abrangentes que combinem a detecção tradicional baseada em assinatura com análise comportamental avançada e integração de inteligência de ameaças.

O treinamento regular de conscientização sobre segurança, o endinhamento de endpoint e o monitoramento proativo continuam sendo componentes críticos de defesa eficaz contra ameaças persistentes tão avançadas direcionadas aos ambientes do Windows.

IOCs

Indicador	Tipo	Observações
Fe6A696E7012696F2E94A4D31B2F076F32C71D44E4C3CEC69A6984EF0B81838A	SHA256	svc.exe
7834A64C39F85DB5F073D76DDB453C5E23AD18244722D6853986934B750259FD	SHA256	winkey.exe
EB6752E60170199E4CE4D5DE72FB539F807332771E1A668865AAC1EEE2C01D93	SHA256	keylogger.dll

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