Protetor de malware asgard revertido: os pesquisadores expõem seus mé

Data: 2025-10-06 06:29:49

Autor: Inteligência Against Invaders

Os analistas da Spycloud Labs têm protetor de engenharia reversa com sucesso, uma sofisticada

ferramenta de crypter usada com destaque para ocultar cargas úteis maliciosas de sistemas de

detecção antivírus.

Este Crypter ganhou notoriedade particular por ser a escolha preferida entre os vendedores Oflummac2, atualmente o infotealer de mercadoria mais prevalente na paisagem cibernética. A análise revela técnicas intrincadas de evasão que demonstram a sofisticação em evolução dos métodos de distribuição de malware.

Os Crypters representam um componente crítico nas operações cibernéticas modernas, servindo como conchas de proteção que envolvem cargas úteis maliciosas em pacotes aparentemente benignos.

O Asgard Protectorhas se estabeleceu como um serviço premium em fóruns underground, com anúncios aparecendo no XSS que remonta a 2023.

O serviço opera através de um automatizado Telegram Bot Isso gera stubs criptografados com recursos personalizáveis, incluindo recursos de log IP, detecção de máquina anti-virtual e funcionalidade de autorun.

O.batfile que procura é o arquivo de texto ASCII, ou nesta amostra, bélgica.pst.

O modelo de negócios do Crypter reflete a profissionalização do crime cibernético, oferecendo várias camadas de assinatura e canais de suporte ao cliente.

Essa acessibilidade contribuiu para sua ampla adoção, principalmente entre os operadores Lummac2 que exigem métodos confiáveis ??para ignorar as soluções de segurança do Endpoint.

Arquitetura técnica e processo de instalação

Exploração do pacote Nullsoft

O mecanismo de entrega inicial do Asgard Protector alavanca os binários de instalação do NULLSOFT, que funcionam como arquivos auto-extraídos que contêm scripts de instalação.

Essa abordagem fornece legitimidade imediata, pois os instaladores da Nullsoft são comumente usados ??por fornecedores de software legítimos. Após a execução, o binário extrai todos os componentes no diretório temporário do sistema (%temp%) antes de localizar e executar um arquivo

em lote responsável pela rotina de instalação.

O Crypter emprega a incompatibilidade de extensão de arquivo deliberado como uma técnica de ofuscação. Arquivos críticos em lote são disfarçados com extensões como.pstaparecendo como arquivos de dados inocentes enquanto contém código de script executável.

Esse desvio de direção ajuda a evitar sistemas de varredura automatizados e analistas humanos que realizam triagem inicial.

Técnicas de ofuscação e montagem

O script em lote de instalação demonstra ofuscação significativa, tornando a análise estática desafiadora para os pesquisadores de segurança.

No entanto, a análise de Spycloud revelado Técnicas sofisticadas, incluindo a assembléia de peçasal de um binário executável de autoit.

O script reconstrói esse binário combinando arquivos de arquivos de táxi incorporados com cabeçalhos de número mágico codificado (MZ) e depois usa ofindstrComando para localizar compensações de arquivos específicas para o posicionamento adequado do cabeçalho do PE.

Esse método de reconstrução serve a propósitos duplos: evita armazenar arquivos executáveis ??completos que podem desencadear assinaturas de antivírus e demonstra uma compreensão avançada das estruturas de arquivos do Windows PE.

O binário automático remontado executa subsequentemente scripts de autoit compilados contendo a carga útil de malware real.

Injeção de carga útil baseada em memória

Depois que o ambiente de autoit é estabelecido, o Asgard Protectorimplements sofisticam técnicas de injeção de memória.

A carga útil de malware permanece criptografada no script automático e passa por descriptografia em tempo real usando o algoritmo RC4 diretamente na memória do sistema.

Essa abordagem garante que o código malicioso real nunca exista em forma não criptografada no sistema de arquivos, complicando significativamente a análise forense e a detecção baseada em assinatura.

A carga útil descriptografada é mais processada usandoRTLDecompressFragmentCom o algoritmo de compressão LZNT1, reduzindo a pegada de armazenamento do Crypter enquanto adicionava outra camada de ofuscação.

A carga útil final normalmente injeta emexplorer.exeO processo principal do Windows, fornecendo persistência e legitimidade, pois esse processo normalmente mantém conexões de rede e acesso ao sistema de arquivos.

Talvez o aspecto mais inovador do protetor de Asgard seja a metodologia de detecção de caixa de

eboen.

Em vez de depender da impressão digital do ambiente tradicional, o Crypter realiza testes de conectividade de rede, pingando nomes de domínio gerados aleatoriamente que não devem existir. Em ambientes legítimos, esses pings não recebem resposta, permitindo que o malware prossiga.

No entanto, em ambientes de sandbox, onde os produtos de segurança interceptam e simulam o tráfego de rede, esses pings podem receber respostas, alertando imediatamente o malware para o ambiente artificial.

Ao detectar essas respostas, o Asgard Protector encerra a execução, impedindo que os pesquisadores de segurança obtenham amostras de carga útil e dados de análise comportamental.

Estatísticas de distribuição de carga útil

Análise de Spycloud de mais de 1.200 amostras de protetor de asgard de VIRUSTOTAL revela padrões de uso significativos entre as famílias de malware.

O LUMMAC2 domina a paisagem, representando aproximadamente 69% das amostras criptografadas, demonstrando a forte relação entre esse Infotealer e o Serviço Crypter.

RhadamanthysResents A segunda carga útil mais comum em 11%, seguida por várias outras famílias de malware, incluindo ActStealer, Quasarrat, Vidar e Autorun, ladrão. A baixa porcentagem de amostras não identificadas (abaixo de 2%) sugere que o Asgard Protector serve principalmente famílias de malware estabelecidas, em vez de cargas úteis experimentais ou personalizadas.

Uma descoberta interessante da análise revela que vários fornecedores de antivírus identificam incorretamente as amostras de protetor de Asgard, outro crypter com funcionalidade semelhante.

Essa identificação incorreta sugere que as bases de código compartilhadas imitam deliberadamente técnicas projetadas para confundir sistemas de classificação automatizados. Tais erros de classificação podem levar a atualizações ineficazes de assinatura e esforços incompletos de caça de ameaças.

Apesar de suas sofisticadas técnicas de evasão, o Asgard Protector exibe padrões comportamentais detectáveis ??que as equipes de segurança podem alavancar. O processo de instalação do Crypter envolve seqüências de comando específicas que são suficientemente anômalas para detecção:

O malware usa constantementetasklistseguido pelafindstrComandos para identificar processos antivírus específicos, incluindo “BdServiceHost”, “SophosHealth”, “Avastui” e “avgui”. Além disso, ele procura processos de serviço de segurança usando padrões como “OPSSVC” e “WRSA”.

O processo de reconstrução binária envolve característicaextrac32comandos com parâmetros específicos, seguidos porfindstrOperações para localizar cabeçalhos de PE. Esses padrões de comando fornecem indicadores confiáveis ??para sistemas de detecção comportamental focados no monitoramento de execução de processos.

Implicações para a segurança corporativa

A sofisticação demonstrada pelo protetor de Asgard reflete a evolução mais ampla da paisagem cibernética, onde os operadores criminais empregam cada vez mais técnicas tradicionalmente associadas a grupos de ameaças persistentes avançados.

A integração do Crypter com Lummac2 Cria uma combinação formidável capaz de ignorar a maioria das soluções de segurança de terminais tradicionais.

As organizações devem adaptar suas estratégias de segurança para abordar essas ameaças em evolução por meio de abordagens de várias camadas que combinam detecção baseada em assinatura com análise comportamental, varredura de memória e inspeção de tráfego de rede.

As técnicas de evasão de sandbox empregadas pelo ASGARD Protector também destacam a importância de implementar diversos ambientes de análise que não podem ser facilmente impressos por malware.

As principais recomendações defensivas incluem o monitoramento para os padrões de comando específicos identificados nesta análise, implementando recursos de detecção de malware baseados em memória e mantendo a inteligência de ameaças atualizada que explica a rápida evolução dos serviços do Crypter.

As equipes de segurança também devem considerar as implicações da classificação incorreta do antivírus e garantir que seus recursos de detecção estendam além das assinaturas fornecidas por fornecedores para incluir regras comportamentais personalizadas adaptadas a seus ambientes específicos.