Malware XWorm ressurge com módulo de ransomware, mais de 35 plugins

Data: 2025-10-06 11:45:05

Autor: Inteligência Against Invaders

Novas versões do backdoor XWorm estão sendo distribuídas em campanhas de phishing depois que

o desenvolvedor original, XCoder, abandonou o projeto no ano passado.

As variantes mais recentes, XWorm 6.0, 6.4 e 6.5, parecem ser adotadas por vários agentes de ameaças e têm suporte para plug-ins que permitem uma ampla gama de atividades maliciosas.

Os operadores de malware podem usar os módulos para roubar dados de navegadores e aplicativos, assumir o controle do host por meio de área de trabalho remota e acesso ao shell e criptografar ou descriptografar arquivos.

A última versão conhecida do malware desenvolvido pelo XCoder é a 5.6, que foi vulnerável a uma falha de execução remota de código, abordada nas variantes recentes.

Versátil e popular

O XWorm é um trojan de acesso remoto observado pela primeira vez em 2022. Ele ganhou reputação como um malware altamente eficaz devido à sua arquitetura modular e amplos recursos.

Normalmente é usado para coletar dados confidenciais (senhas, carteiras criptográficas, informações financeiras), rastrear pressionamentos de tecla, roubar informações na área de transferência,

No entanto, ele também pode ser usado para lançar ataques distribuídos de negação de serviço (DDoS) e carregar outros malwares.

Depois que o XCoder excluiu suas contas do Telegram, onde compartilhavam atualizações regulares, vários agentes de ameaças começaram a espalhar versões crackeadas do malware.

O XWorm era tão popular que um agente de ameaças o usou como isca para atingir cibercriminosos menos qualificados com um backdoor que roubava dados.

Essa campanha contou 18.459 infecções, a maioria deles na Rússia, Estados Unidos, Índia, Ucrânia e Turquia.

Variedade de métodos de entrega

Desde junho, pesquisadores da empresa de segurança cibernética Trellix notaram um aumento nas amostras do XWorm na plataforma de varredura VirusTotal, o que também indica uma alta taxa de adoção entre os cibercriminosos.

Em uma campanha de phishing, o malware foi implantado por meio de um JavaScript malicioso que iniciou um script do PowerShell, que poderia ignorar a proteção da interface de verificação antimalware e implantar o XWorm.

[IMAGEM REMOVIDA]Trellix disse.

Outros pesquisadores detectaram campanhas que entregou XWorm usando iscas com tema de IA e uma variante modificada da ferramenta de acesso remoto ScreenConnect.

Outra pesquisa fornece Detalhes técnicos em uma campanha de phishing que entrega o XWorm por meio de código shell incorporado em um arquivo MicrosoftExcelfile (. XLAM).

Ameaça de ransomware entre dezenas de módulos

De acordo com os pesquisadores da Trellix, o XWorm agora tem mais de 35 plug-ins que estendem seus recursos de roubo de informações confidenciais a ransomware.

A funcionalidade de criptografia de arquivos, Ransomware.dll, permite que os operadores de malware definam um papel de parede da área de trabalho depois de bloquear os dados, o valor do resgate, o endereço da carteira e o e-mail de contato.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]O ransomware NoCry foi observado pela primeira vez em 2021.

Ambos os códigos maliciosos usam o mesmo algoritmo para gerar o vetor de inicialização (IV) e a chave de criptografia/descriptografia, o processo de criptografia (AES com modo CBC em blocos de 4096 bytes).

Os pesquisadores também notaram que os dois malwares executavam o mesmo conjunto de verificações em ambientes de análise.

Além do componente de ransomware, a Trellix analisou 14 outros plugins para o XWorm:

- **RemoteDesktop.dll**: cria uma sessão remota para interagir com a máquina da vítima
- **WindowsUpdate.dll**, **Stealer.dll**, **Recovery.dll**, **merged.dll**, **Chromium.dll**e **SystemCheck.Merged.dll**: roubar dados das vítimas
- **FileManager.dll**: fornece ao operador recursos de acesso e manipulação do sistema de arquivos
- **Shell.dll**: executa comandos do sistema que o operador envia em um oculto *cmd.exe* processo
- **Informations.dll**: reúne informações do sistema sobre a máquina da vítima
- **Webcam.dll**: Usado para gravar a vítima. Também é usado pelo operador para verificar se uma máquina infectada é real
- **TCPConnections.dll**, **ActiveWindows.dll**e **StartupManager.dll**: lista de conexões TCP ativas, janelas ativas e programas de inicialização, respectivamente, para o servidor C2

Os pesquisadores dizem que os módulos de roubo de dados sozinhos permitir que um operador XWorm roube dados de login de vários aplicativos que incluem mais de 35 navegadores da web, clientes de e-mail, aplicativos de mensagens, clientes FTP e carteiras de criptomoedas.

Como os plug-ins têm uma função específica, a Trellix recomenda que as organizações usem uma abordagem de defesa em várias camadas que possa responder a atividades maliciosas após o comprometimento.

As soluções de detecção e resposta de endpoint (EDR) podem identificar o comportamento dos módulos do XWorm, enquanto as proteções proativas de e-mail e da web podem bloquear os droppers iniciais de malware.

Além disso, uma solução de monitoramento de rede pode detectar a comunicação com o servidor de comando e controle para baixar mais plug-ins ou exfiltração de dados.

Ionut Ilascu

Ionut Ilascu é um escritor de tecnologia com foco em todas as coisas de segurança cibernética. Os tópicos sobre os quais ele escreve incluem malware, vulnerabilidades, exploits e defesas de segurança, bem como pesquisa e inovação em segurança da informação. Seu trabalho foi publicado pela Bitdefender, Netgear, The Security Ledger e Softpedia.

Você também pode gostar: