BOLETIM DE SEGURANÇA

Ataque com backdoor a supply chain de Plugins do WordPress.org

heimdall
security research
A DIVISION OF ISH

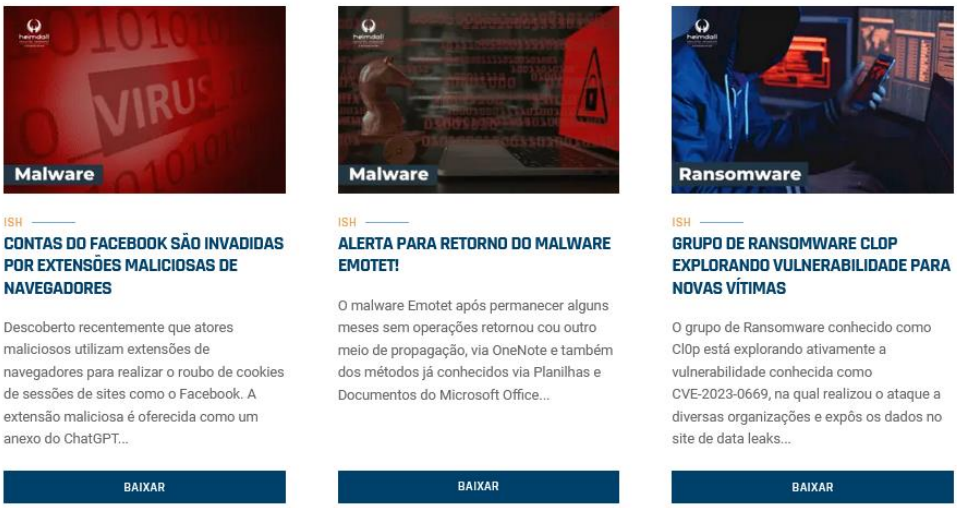
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

1 SUMÁRIO EXECUTIVO

Recentemente foi alertado que vários plug-ins para WordPress hospedados no WordPress.org foram comprometidos e injetados com scripts PHP maliciosos. Um agente de ameaça mal-intencionado comprometeu o código-fonte de vários plug-ins e injetou código que exfiltra credenciais de banco de dados e é usado para criar novos usuários administradores mal-intencionados e enviar esses dados de volta para um servidor.

2 PLUGINS AFETADOS

Conforme a nota da Wordfence os plugins afetados foram o seguintes, também segue as versões corrigidas.

Social Warfare

- Versões afetadas: 4.4.6.4 – 4.4.7.1 (corrigido na versão **4.4.7.3**)

Blaze Widget

- Versões afetadas: 2.2.5 – 2.5.2 (corrigido na versão **2.5.4**)

Wrapper Link Element

- Versões afetadas: 1.0.2 – 1.0.3 (corrigido na versão **1.0.5**)

Contact Form 7 Multi-Step Addon

- Versões afetadas: 1.0.4 – 1.0.5 (corrigido na versão **1.0.7**)

Simply Show Hooks

- Versão afetada: 1.2.1 (nenhuma correção disponível até o momento)

A Wordfence recomenda que devido a não atualização e correção do Simply Show Hooks, desinstalar os plug-ins por enquanto e executar uma verificação completa de malware.

3 CONCLUSÃO

Plugins de WordPress com backdoors representam um sério risco para as organizações, comprometendo a segurança dos dados e a integridade dos sistemas. Esses plugins maliciosos permitem que atacantes obtenham acesso não autorizado aos servidores, podendo roubar informações sensíveis, injetar código malicioso e manipular o conteúdo do site. Além disso, a presença de backdoors facilita a instalação de malware adicional, como ransomware ou keyloggers, agravando o impacto das invasões. A exploração contínua de vulnerabilidades nos plugins compromete a confiança dos usuários e pode resultar em perdas financeiras significativas, bem como danos à reputação da organização.

4 RECOMENDAÇÕES

Além do indicador de comprometimento elencado abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- Atualizar para as versões recomendadas e corrigidas pela Wordfence.

Verificações de segurança

- Realize auditorias de segurança regulares e utilize ferramentas de segurança para escanear plugins e detectar possíveis backdoors ou códigos maliciosos.

Permissões restritas

- Limite as permissões dos plugins, garantindo que tenham apenas os acessos necessários para seu funcionamento, minimizando assim os riscos de exploração.

Monitoração contínua

- Implemente sistemas de monitoramento para detectar atividades suspeitas e responder rapidamente a possíveis incidentes de segurança.

Backup regular

- Mantenha backups regulares e atualizados de todo o site e banco de dados, garantindo uma rápida recuperação em caso de comprometimento.

Treinamento de equipe

- Treine a equipe de TI e administradores do site para identificar e responder a ameaças, bem como para seguir as melhores práticas de segurança.

Redução de plugins

- Use o mínimo de plugins necessários, removendo aqueles que não são mais utilizados para reduzir a superfície de ataque.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de IPs

Indicadores de URL, IPs e Domínios	
IP	94[.]156.79[.]8

Tabela 1 – Indicadores de Compromissos de Rede.

Nomes de usuários conhecidos atuais das contas de usuários administrativos que estão sendo geradas maliciosamente.

- Options
- PluginAuth

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Wordfence**
- **Bleepingcomputer**

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH