




heimdall
security research

A DIVISION OF ISH



Entrevista do afiliado de Ransomwares, Wazawaka



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

[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](#)



ISH —
CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH —
ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH —
GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

Sumário

1	A entrevista de Wazawaka.....	6
2	Referências.....	9

Lista de Figuras

Figura 1 – Publicação do FBI sobre o afiliado procurado. 6

1 A ENTREVISTA DE WAZAWAKA

O governo dos EUA indiciou e sancionou no dia 16 de maio de 2023 um russo, conhecido como Mikhail Matveev por atuar em participações em ataques de Ransomwares.

Segundo o governo, o cibercriminoso é conhecido pelo vulgo de Wazawaka e atuou em operações de ransomware como LockBit, Babuk e Hive para exigir pagamento de resgates a empresas.



Figura 1 – Publicação do FBI sobre o afiliado procurado.

O russo teria chamado atenção no ano de 2022 após apresentar um comportamento com vários erros em suas operações, bem como foi descoberto detalhes que ligavam o russo com o grupo de ransomware **Babuk**, o qual teve seu código-fonte vazado em 2021.

Em sequência, foi publicada uma nova entrevista com o afiliado de ransomware Mikhail, na qual algumas perguntas acabam verificando e preenchendo lacunas de todas as suas operações. A entrevista foi realizada pela empresa RecordedFuture.

Reporter: Você está na lista dos mais procurados do FBI em ciber. Isso teria sido uma surpresa e mudou a maneira como está trabalhando?

Mikhail: Não fiquei surpreso. Entendi que isso iria acontecer. Há tantas novidades no mundo, então as notícias sobre mim serão esquecidas muito em breve... “o cachorro late, mas a caravana segue em frente”.

Reporter: O Departamento de Justiça alegou que você ajudou três grupos de ransomwares – LockBit, Babuk e Hive a lançar ataques contra várias entidades dos EUA?

Mikhail: Não, não fui eu, foram outras pessoas. Acabei de enviar os dados, porque achou que precisava carregá-los. Muitas empresas ocidentais de segurança cibernéticas pensam que muitos grupos de ransomware mentem... Enviei os dados para provar que realmente havia sido roubado e não era uma farsa.

Reporter: Então o departamento de justiça está errado em ligá-lo a esses ataques?

Mikhail: Acho que o Departamento de Estado costuma exagerar em tudo. Eles sempre trabalham assim e assim o farão. Em todos os projetos, sou um afiliado – como um contratado – **não estou executando essas operações.**

Reporter: Você trabalhou com várias equipes diferentes de ransomware. Na sua opinião, qual grupo de ransomware é executado com mais eficiência?

Mikhail: O **Conti particularmente era bem executado.** Se você olhar para o lockbit ou grupos como REvil, eles tendem a reivindicar o trabalho dos outros como seus, e é por isso que eles se perderam. Mas você não encontrará nada de ruim escrito sobre a Conti, como se eles não estivessem cumprindo suas promessas de negócios ou algo assim. Acho que o **Conti é o melhor produto nesse espaço e eles ainda estão por aí.** Nós simplesmente não os vemos. **Da forma como o mercado de ransomware está configurado agora, você não vê grupos... você apenas vê o hype.**

Reporter: Qual é a sua definição de ser uma pessoa afiliada a ransomware?

Mikhail: RaaS é um modelo de negócios no qual os desenvolvedores de malware fornecem ransomware e a infraestrutura para gerenciá-lo a outros invasores por assinatura. Os afiliados pagam para lançar ataques de ransomware desenvolvidos por esses operadores. Eu sou um afiliado.

Reporter: No que você está trabalhando agora?

Mikhail: Quero mostrar com meu exemplo que a TI na Rússia ainda está viva e bem. Você não precisa ir para os EUA para ganhar dinheiro. [...]

Quero levar a TI na Rússia para o próximo nível.

Reporter: Como o seu novo projeto é diferente do que você trabalhou anteriormente?

Mikhail: Meu novo projeto é socialmente orientado a ajudar nosso país, a **Federação Russa.**

Nos trechos apresentados acima, é possível verificar a insatisfação que o afiliado possui com os novos grupos de ransomwares que estão em operação no momento, como no caso do LockBit, bem como é possível verificar que Mikhail se encontra afiliado e trabalhando em causa a seu país de origem, a Rússia, empregando e influenciando que a Rússia precisa e pode ter cibercriminosos operando ransomwares e praticando ataques cibernéticos em seu quintal.

Caso queira ouvir a entrevista na íntegra, sugiro que acesse a gravação realizada da entrevista com o afiliado, na qual apenas exibimos alguns dos pontos interessantes.

2 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Entrevista](#) Recorded Future com Wazawaka, afiliado de Ransomware.



heimdall
security research

A DIVISION OF ISH