TLP: CLEAR

BOLETIM DE SEGURANÇA

Ransomware Mogilevich se manifesta e encerra as operações afirmando ser fraude!

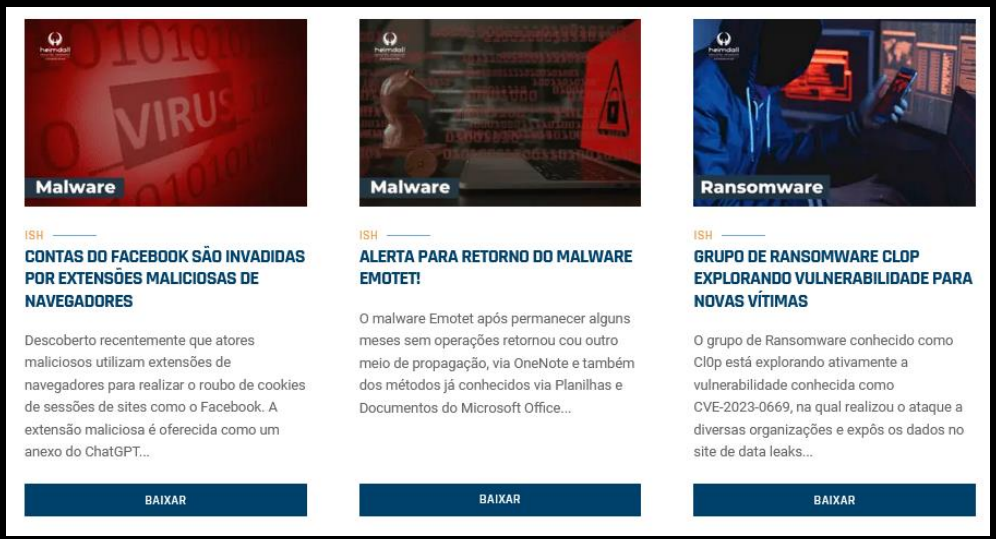
heimdall
security research
A DIVISION OF ISH

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



SUMÁRIO

LISTA DE FIGURAS

1 DETALHES DO RANSOMWARE MOGILEVICH

Um grupo relativamente novo de ransomware, conhecido como **Mogilevich**, teria anunciado a violação de inúmeras organizações, incluindo o Departamento de Relações Exteriores da Irlanda, Infinity USA, Epic Games, entre outras.

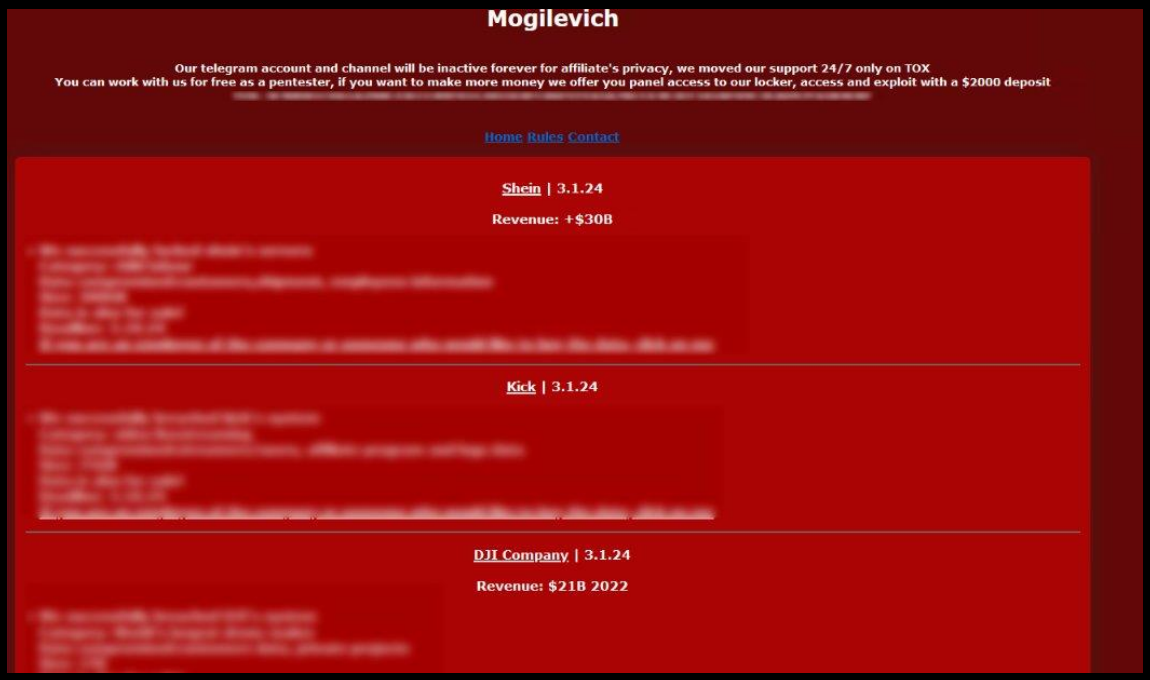
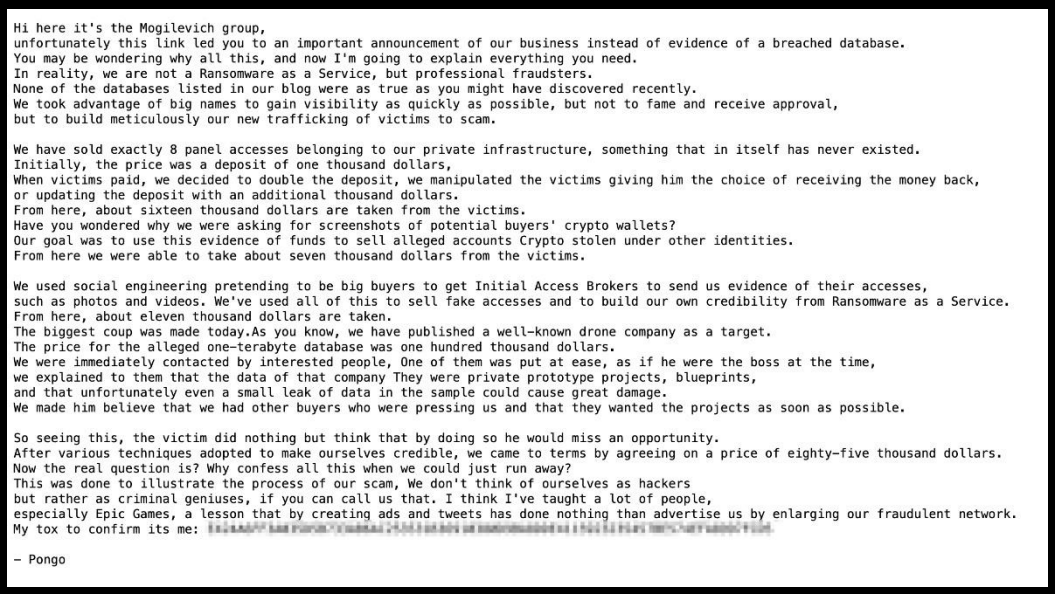


Figura 1 – Site anterior de publicação de vazamento de dados de organizações utilizado pelo grupo.

Ao contrário do que ocorre com outros grupos de ransomware, este grupo não compartilha amostras dos dados roubados e afirma que realiza a venda diretamente a compradores comprovados. A falta de compartilhamento dos dados levou à crença de que os atores de ameaças estavam tentando enganar os compradores com dados falsos.

Os atores de ameaças também afirmaram ser uma operação de Ransomware como Serviço (Ransomware-as-a-Service), recrutando afiliados para trabalhar com eles em troca de um criptografador de ransomware funcional e um painel de controle para negociações. Dias após esses anúncios, o suposto proprietário do Ransomware Mogilevich publicou uma nota sobre a alegada violação contra a Epic Games através de um site de vazamento de dados.



Hi here it's the Mogilevich group,
unfortunately this link led you to an important announcement of our business instead of evidence of a breached database.
You may be wondering why all this, and now I'm going to explain everything you need.
In reality, we are not a Ransomware as a Service, but professional fraudsters.
None of the databases listed in our blog were as true as you might have discovered recently.
We took advantage of big names to gain visibility as quickly as possible, but not to fame and receive approval,
but to build meticulously our new trafficking of victims to scam.

We have sold exactly 8 panel accesses belonging to our private infrastructure, something that in itself has never existed.
Initially, the price was a deposit of one thousand dollars,
When victims paid, we decided to double the deposit, we manipulated the victims giving him the choice of receiving the money back,
or updating the deposit with an additional thousand dollars.
From here, about sixteen thousand dollars are taken from the victims.
Have you wondered why we were asking for screenshots of potential buyers' crypto wallets?
Our goal was to use this evidence of funds to sell alleged accounts Crypto stolen under other identities.
From here we were able to take about seven thousand dollars from the victims.

We used social engineering pretending to be big buyers to get Initial Access Brokers to send us evidence of their accesses,
such as photos and videos. We've used all of this to sell fake accesses and to build our own credibility from Ransomware as a Service.
From here, about eleven thousand dollars are taken.
The biggest coup was made today.As you know, we have published a well-known drone company as a target.
The price for the alleged one-terabyte database was one hundred thousand dollars.
We were immediately contacted by interested people, One of them was put at ease, as if he were the boss at the time,
we explained to them that the data of that company They were private prototype projects, blueprints,
and that unfortunately even a small leak of data in the sample could cause great damage.
We made him believe that we had other buyers who were pressing us and that they wanted the projects as soon as possible.

So seeing this, the victim did nothing but think that by doing so he would miss an opportunity.
After various techniques adopted to make ourselves credible, we came to terms by agreeing on a price of eighty-five thousand dollars.
Now the real question is? Why confess all this when we could just run away?
This was done to illustrate the process of our scam, We don't think of ourselves as hackers
but rather as criminal geniuses, if you can call us that. I think I've taught a lot of people,
especially Epic Games, a lesson that by creating ads and tweets has done nothing than advertise us by enlarging our fraudulent network.
My tox to confirm its me: [redacted]

– Pongo

Figura 2 – Publicação e declaração compartilhada do administrador do suposto ransomware Mogilevich.

De acordo com a nota, o grupo se identifica como Fraudadores Profissionais, e não como uma operação de Ransomware como Serviço (Ransomware-as-a-Service). Eles visavam ganhar visibilidade o mais rapidamente possível, utilizando nomes de grandes organizações não para fama ou aprovação da comunidade, mas para atrair mais vítimas.

O administrador afirmou que conseguiu vender acessos ao painel por uma quantia de 1.000 dólares cada. Após receberem o pagamento, eles decidiam dobrar o depósito, manipulando as vítimas com a opção de receber o dinheiro de volta ou adicionar mais mil dólares ao depósito.

Eles empregaram técnicas de engenharia social, fingindo ser grandes compradores para que os Corretores de Acesso Inicial (Initial Access Brokers) enviassem evidências de seus acessos, como fotos e vídeos. De acordo com ele, isso foi utilizado para vender acessos falsos e construir sua própria credibilidade a partir do conceito de RaaS, arrecadando assim 11.000 dólares.

O segundo golpe, conforme relatado pelo proprietário, ocorreu em 2 de março de 2024, quando divulgaram informações sobre uma grande empresa de drones conhecida, alegando que o acesso ao banco de dados de 1 TB valeria 100.000 dólares. Uma pessoa interessada acreditou que os dados continham informações sobre protótipos privados e plantas, cujo um pequeno vazamento na amostra poderia causar grandes danos.

Após várias negociações, chegaram a um acordo de 80.000 dólares, quantia que foi paga pela parte interessada. No final, o proprietário declarou que todo esse esquema foi uma demonstração do processo de golpe do grupo, que não se considera como hackers, mas sim como "gênios criminosos".

Uma prática adotada pelo agente de ameaça é conhecida como **“Extorsão de Incidente Fantasma”**, que consiste basicamente na utilização de certos aspectos das extorsões para executar fraudes visando o roubo de quantias específicas. Há componentes específicos empregados nesse tipo de golpe, incluindo:

1. **Legitimidade Projetada:** Esse aspecto crucial do golpe de incidente fantasma envolve o uso de informações únicas e reconhecíveis pela vítima, como um endereço de e-mail ou uma lista de contas de usuário. O propósito é fornecer credibilidade à ameaça, convencendo a vítima de sua autenticidade e não que seja algo fabricado.

2. **Pressão Social:** A extorsão de incidente fantasma emprega variadas formas de pressão social para forçar a vítima a atender às demandas de extorsão rapidamente. Essa pressão geralmente se baseia em prazos e na ameaça de prejuízo à reputação da marca ou outras consequências custosas, caso o pagamento não seja realizado.

3. **Oferta Financeira Assimétrica:** A demanda financeira representa apenas uma fração do custo percebido da ameaça, exacerbando a pressão social e persuadindo a vítima de que pagar é a opção mais econômica e segura para resolver a situação.

Dada a alta probabilidade de enfrentar tais riscos, é vital que as organizações fortaleçam suas defesas e estejam preparadas e capacitadas para reconhecer tais artimanhas. Analisar as ameaças com base nos elementos citados pode ajudar a identificar tentativas de extorsão como fraudulentas.

Reconhecer a necessidade de uma avaliação meticulosa de todas as ameaças, tratando-as com a devida seriedade e analisando as evidências que conferem uma aparência de legitimidade, é fundamental no processo de proteção contra esses golpes.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Ministério das Relações Exteriores da Irlanda afirma que "não há evidências" de violação – The Record**

heimdall
security research
A DIVISION OF ISH