BOLETIM DE SEGURANÇA

Tendências de malwares do Q3 de 2023

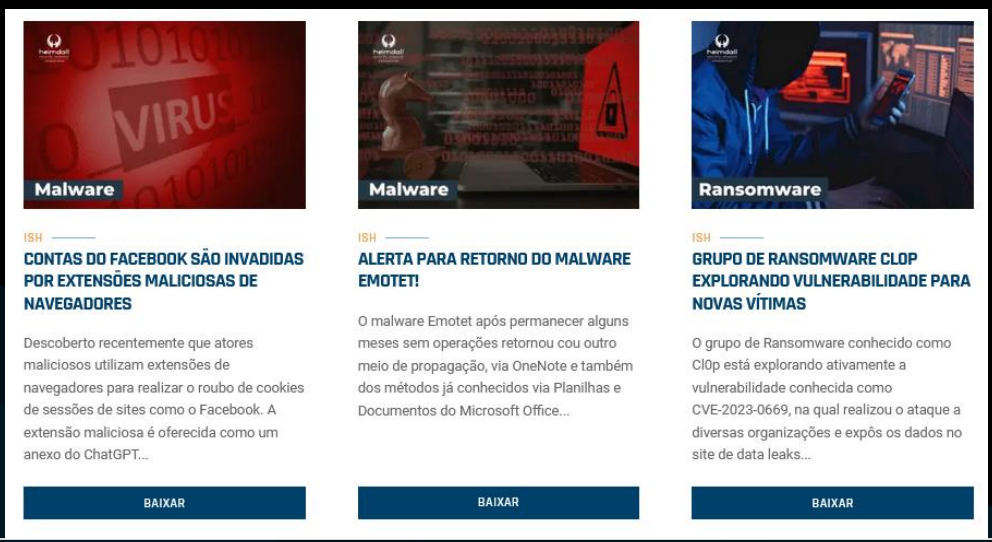
heimdall
security research
A DIVISION OF ISH

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



heimdall
security research

Sumário

Lista de Tabelas

Lista de Figura e Gráfico

1 SUMÁRIO EXECUTIVO

A equipe de inteligência da ISH Tecnologia, por meio de coleta de informações em fontes abertas foi possível identificar uma grande quantidade de envios de novos malwares do tipo Loader, Stealer e RAT os quais foram objetos de envios para sandbox que oferecem o serviço gratuitamente para análise e submissão por usuários.

Realizar a coleta destas informações com relação a submissões, e análises, dá um panorama de como está o cenário de ameaças ao longo do ano, sendo possível correlacionar incidentes ou fatos significativos quando ocorrem o envio de grande quantidade.

As informações deste boletim foram coletadas em conjunto com a Sandbox AnyRun, a qual oferece um serviço de análise de arquivos para diversos usuários na internet de forma gratuita, fornecendo posteriormente um relatório para estudos de casos.

2 ANÁLISE DOS DADOS Q2 E Q3

Antes que sejam apresentados os dados do Q3 de 2023, é importante que apresentemos os dados e informações do Q2 de 2023, para que possamos posteriormente realizar uma comparação das informações.

Como forma resumida, apresentamos abaixo os dados coletados do relatório:

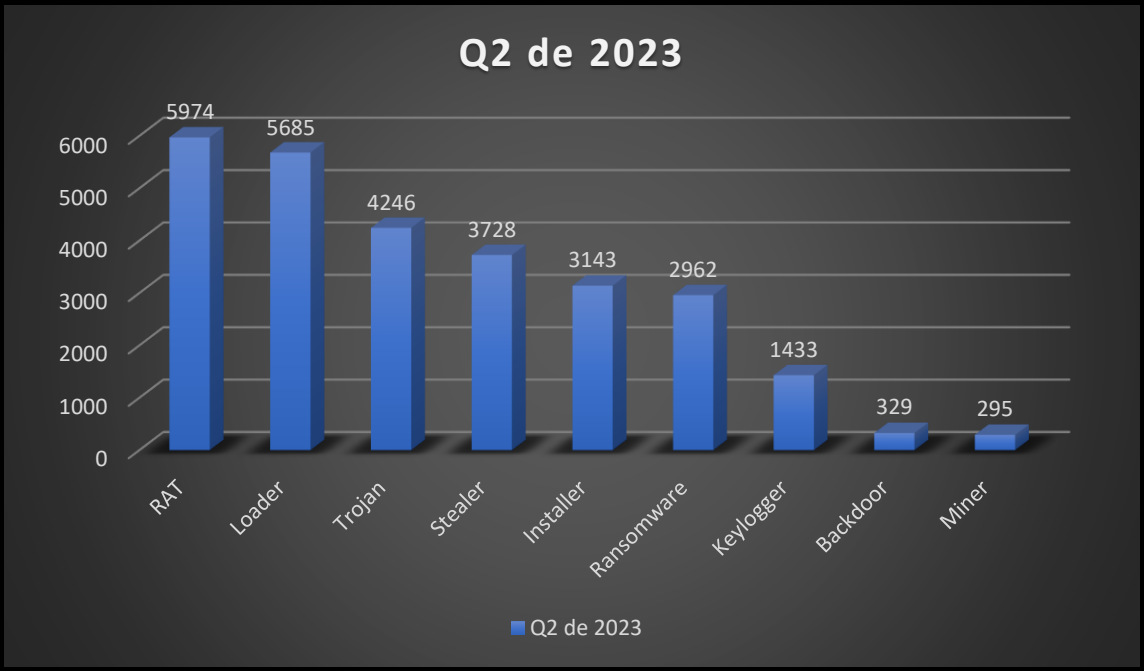


Gráfico 1 – Gráfico corresponde ao número de Malwares no Q2 de 2023.

É possível observar que dentre o TOP 3 dos malwares submetidos, podemos visualizar o RAT como primeiro, seguido do Loader e do Trojan.

Já analisando os dados relacionados ao Q3 de 2023, é possível observar que:

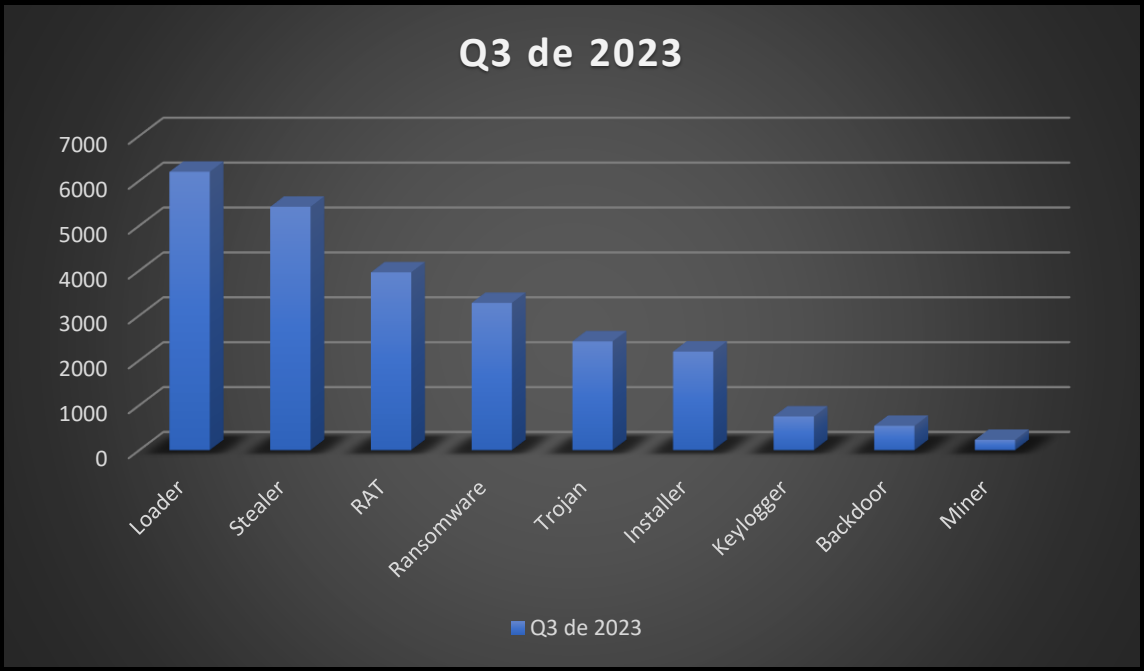


Gráfico 2 – Gráfico corresponde ao número de Malwares no Q3 de 2023.

Podemos observar que malwares do tipo Loader permaneceram altas e apresentou um pequeno aumento de 9,1% em comparação ao segundo trimestre do ano de 2023. Já o malware do tipo Stealer emergiu como um jogador importante, seguido pelos malwares do tipo RAT.

Outro fato relevante são os malwares do tipo Ransomware, o qual passou para a quarta posição, mas foi o Trojan que veio a ter uma queda entre os meses anteriores.

Além disso, foi possível identificar as principais famílias de malwares do terceiro trimestre de 2023, sendo as:

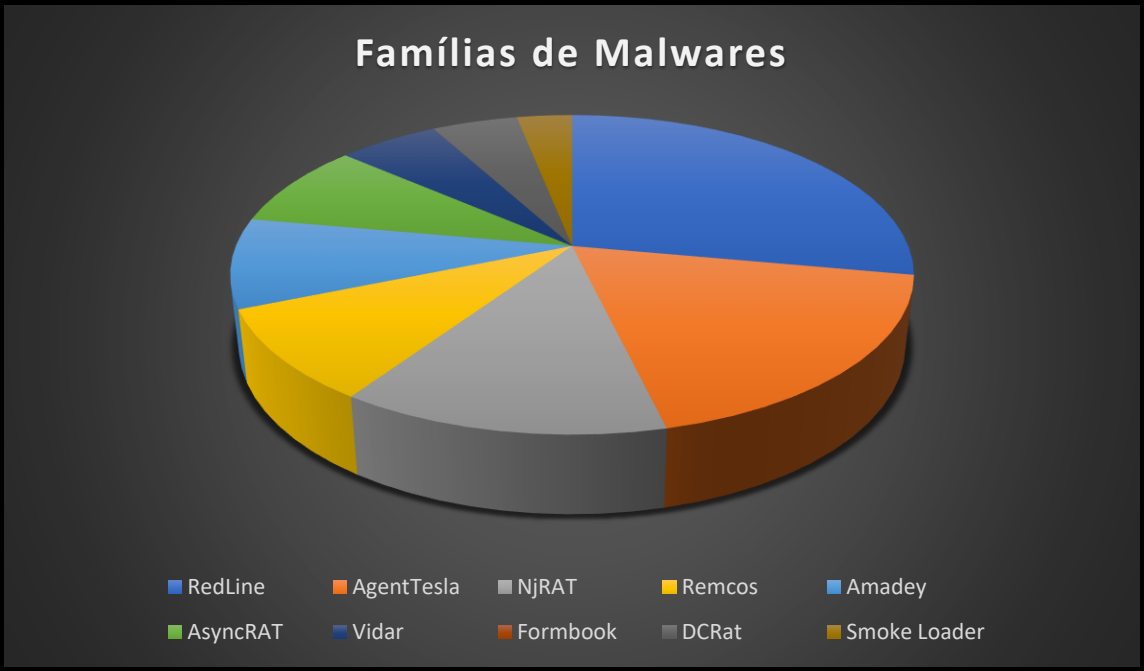


Gráfico 3 – Gráfico relacionado as principais famílias de malwares.

A família mais notória relacionada ao Q3 de 2023 é o Malware Redline, do qual a ISH Tecnologia já publicou boletim alertando sobre o malware do tipo Stealer que realiza o roubo de informações de um dispositivo infectado, informações que poderão conter credenciais, as quais podem ser vendidas posteriormente por atores para facilitar o acesso inicial a organizações.

Figura 4 – Análise publicada do RedLine da ISH Tecnologia

3 MITRE ATT&CK

Já com relação as principais técnicas coletadas e identificadas do MITRE ATT&CK, foi possível identificar a correlação dos comportamentos dos malwares:

Tática	Técnica
Evasão de Defesa TA0005	Mascaramento: Corresponder nome ou local legítimo. T1036.005
	Virtualização/Evasão de Sandbox: Evasão baseada em Tempo T1497.003
	Execução de proxy binário assinado: Rundll32. T1218.011
	Prejudicar defesas: desativar ou modificar ferramentas. T1562.001
Descoberta TA0007	Descoberta de software: Descoberta de software de segurança. T1518.001
Execução TA0002	Serviços do sistema: Execução de serviço T1569.002
	Tarefa/Trabalho Agendado: Tarefa Agendada. T1053.005
	Interpretador de Comandos e Scripts: Shell de comando do Windows. T1059.003
	Execução do usuário: Arquivo Malicioso T1204.002
Coleção TA0009	Coleta de e-mail: coleta de e-mail local. T1114.001

Tabela 1 – Principais Técnicas e Táticas identificadas em uso no Q3 pela AnyRun.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **AnyRun – Q2 de 2023**
- **AnyRun – Q3 de 2023**
- **Boletim ISH Tecnologia – Malware RedLine**

heimdall
security research
A DIVISION OF ISH