BOLETIM DE SEGURANÇA

Hackers russos utilizam HeadLace e sites de coleta de credenciais na Europa

heimdall
security research
A DIVISION OF ISH

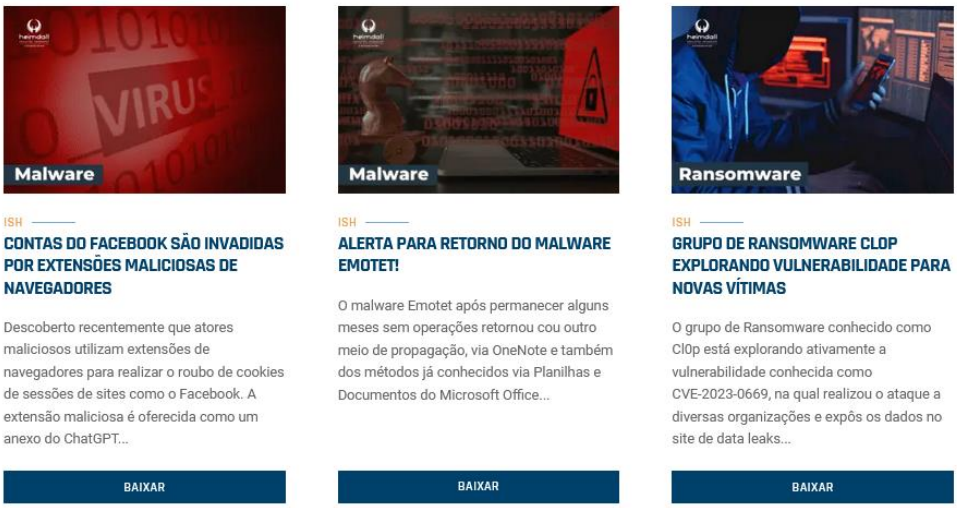
TLP: CLEAR

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

O grupo APT28, também conhecido por uma variedade de outros nomes, incluindo BlueDelta, Fancy Bear, Forest Blizzard, FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy e TA422, continua a representar uma ameaça significativa para a segurança cibernética na Europa. Apoiado pela unidade estratégica de inteligência militar da Rússia, o GRU, tem sido responsável por uma série de campanhas de ataques cibernéticos em toda a Europa. Esses ataques utilizam o malware HeadLace e sites de coleta de credenciais para comprometer as redes.

2 INFORMAÇÃO SOBRE O ATOR

Em setembro de 2023, o CERT-UA relatou uma campanha de phishing que utilizou o malware Headlace para atacar uma instalação crítica de infraestrutura energética na Ucrânia. Durante essa campanha, o BlueDelta enviou e-mails de phishing de um endereço de remetente falso contendo links para arquivos de arquivo. Em 6 de setembro de 2023, a Zscaler publicou um novo post no blog intitulado “Campanha Steal-It”, fornecendo informações adicionais sobre várias novas cadeias de ataque usadas pelo BlueDelta, que visavam entidades na Austrália, Bélgica e Polônia. Em outubro de 2023, o Insikt Group compartilhou um relatório interno sobre a atividade do BlueDelta envolvendo binários vivendo da terra e abuso do LIS para atacar vítimas europeias. Durante essa campanha, foram observadas três cadeias de infecção separadas, que usavam técnicas de geocerca para explorar vítimas localizadas apenas na Áustria, Lituânia e Espanha.

Em dezembro de 2023, a Proofpoint e a IBM publicaram pesquisas sobre uma nova onda de spearphishing do BlueDelta usando vários conteúdos de isca para entregar o malware Headlace. As campanhas visavam pelo menos treze nações separadas, conforme descrito neste relatório na fase três.

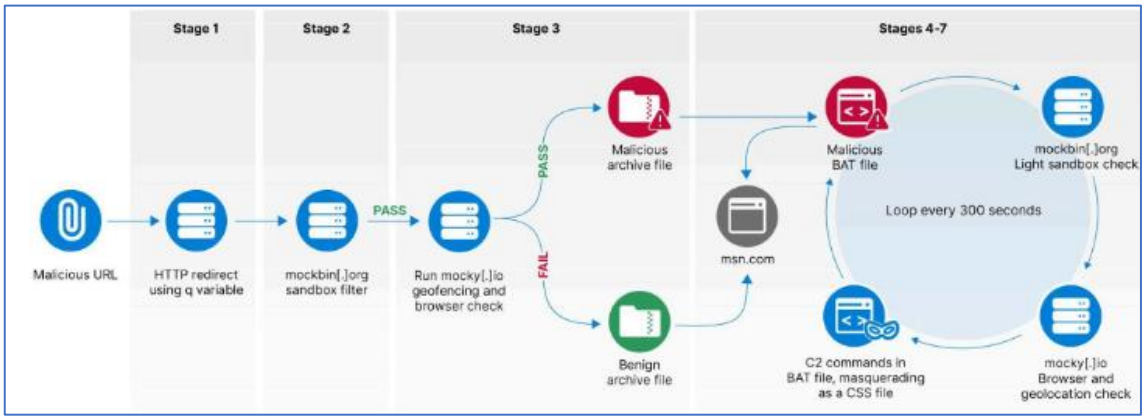


Figura 1 – Estágios da cadeia de infecção da primeira fase.

Na primeira fase, conforme relatado anteriormente pelo Insikt Group, o BlueDelta redirecionou as vítimas para os domínios principais *.lovestoblog[.]com e *.rf[.]gd na primeira etapa de sua sequência de ataque. O BlueDelta então se mudou para o GitHub para redirecionamento na fase dois e *.infinityfreeapp[.]com e *.rf[.]gd para a fase três. Ao longo das fases um a três, o BlueDelta usou o Mocky, um serviço gratuito de hospedagem de API, para hospedar código de filtragem e redirecionamento em JavaScript. Os atores de ameaças também usaram o Mockbin, outro serviço gratuito de hospedagem de API, nas duas primeiras fases, passando para scripts PHP: Hypertext Processor (PHP) hospedados no InfinityFree na fase três.

Na fase dois, a partir de setembro de 2023, o BlueDelta implantou uma nova infraestrutura de redirecionamento de primeira fase no GitHub. Os atores de ameaças criaram duas novas contas, “microsoft-update-com” e “windows-update-service”, cada uma hospedando um repositório de código chamado “kb5021042”, provavelmente em uma tentativa de se passar pelo Serviço de Atualização do Windows da Microsoft. O código da Base de Conhecimento da Microsoft “kb5021042” corresponde a um identificador de versão de atualização da Microsoft emitido para o Windows 10 e o Windows Server 2019 em novembro de 2022.

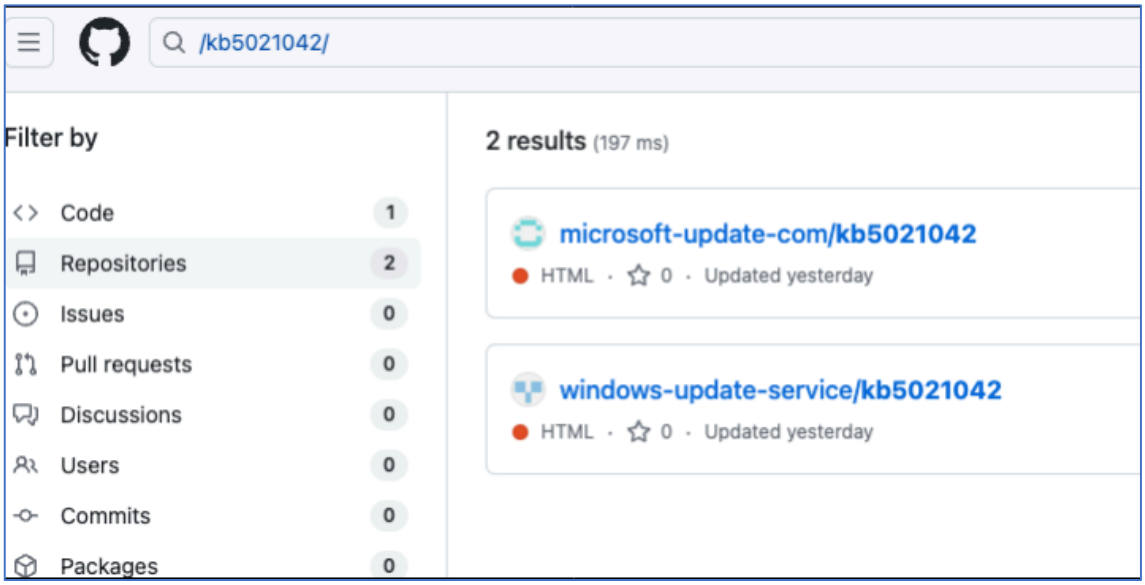


Figura 2 – Repositórios de código GitHub criados por BlueDelta.

Ao analisar os scripts de geofencing do Headlace e os países alvo das campanhas de coleta de credenciais a partir de 2022, o Grupo Insikt identificou que treze países distintos foram alvos do BlueDelta. Como esperado, a Ucrânia liderou a lista, representando 40% da atividade. A Turquia pode parecer um alvo inesperado com 10%, mas é importante notar que ela foi destacada apenas pelo geofencing do Headlace, ao contrário da Ucrânia, Polônia e Azerbaijão, que foram alvos tanto do geofencing do Headlace quanto da coleta de credenciais.

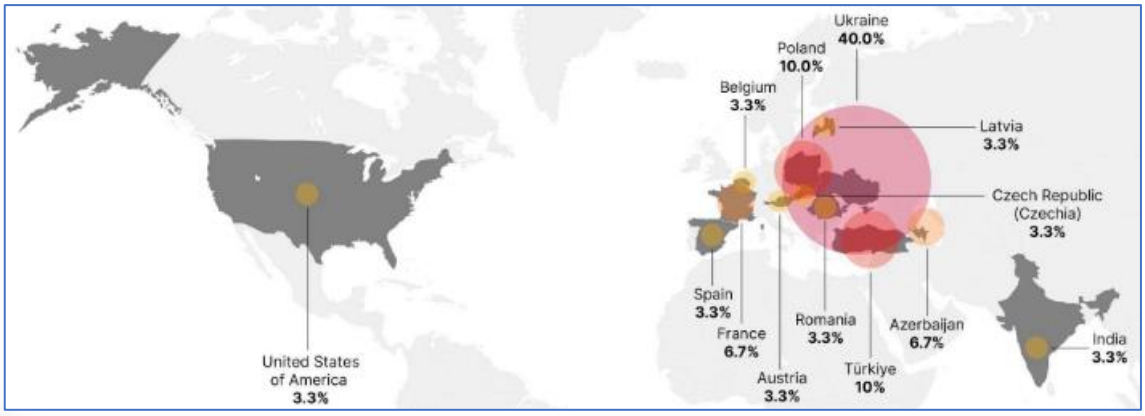


Figura 3 – Países visados pelo Headlace ou pela coleta de credenciais desde 2022.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Resource Development	T1583.001 T1583.006 T1608.001 T1608.005	É uma técnica que envolvem adversários criando, comprando ou comprometendo/roubando recursos que podem ser usados para apoiar a segmentação.
Initial Access	T1566.001 T1566.002	É uma técnica que utiliza vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Execution	T1059.001 T1059.003 T1059.005 T1059.007	É uma técnica que resulta na execução de código controlado pelo adversário em um sistema local ou remoto.
Defense Evasion	T1497.001 T1564.003	É uma técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Credential Access	T1056.003 T1111	É uma técnica para roubar credenciais, como nomes de contas e senhas.
Discovery	T1033	É uma técnica que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Command and Control	T1102.001 T1102.003 T1132.001	É uma técnica que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

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

Atualizações e patches de segurança

- Implemente melhorias de segurança, como atualizações regulares de software e patches de segurança.

Treinamento de conscientização em segurança

- Forneça treinamento de conscientização em segurança para os funcionários, para que eles possam reconhecer e evitar possíveis ameaças.

Compartilhamento de inteligência

- Compartilhe informações sobre ameaças e Indicadores de Compromisso (IoCs) com outras organizações e agências de segurança.

Proteção contra roubo de credenciais

- Implemente medidas adicionais de segurança contra o roubo de credenciais, uma tática comum usada pelo APT28.

Monitoramento de Rede

- Implemente um sistema robusto de monitoramento de rede para detectar atividades suspeitas e responder rapidamente a qualquer violação.

Plano de resposta a incidentes

- Desenvolva um plano de resposta a incidentes cibernéticos para garantir que sua organização possa responder efetivamente a qualquer 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 compromisso do artefato	
md5:	75d5bb70923f6873c395176df7f168bf
sha1:	03d8dadf3647a57b335b96ea4e8a60c70d114243
sha256:	2f1c2afdf17831e744841029bb5d5a3ea9fda569958303be03e50fb3a764913f
File name:	Zeyilname.zip

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	document-c[.]infinityfreeapp[.]com document-d[.]infinityfreeapp[.]com documents-cloud[.]infinityfreeapp[.]com downloadable[.]infinityfreeapp[.]com downloadc[.]infinityfreeapp[.]com downloaddoc[.]infinityfreeapp[.]com downloadfile[.]infinityfreeapp[.]com downloadingdoc[.]infinityfreeapp[.]com downloadinge[.]infinityfreeapp[.]com downloadingf[.]infinityfreeapp[.]com downloadingq[.]infinityfreeapp[.]com downloadingw[.]infinityfreeapp[.]com downloadx[.]infinityfreeapp[.]com downloadz[.]infinityfreeapp[.]com fdsagdfg[.]rf[.]gd file-download[.]infinityfreeapp[.]com filedwn[.]infinityfreeapp[.]com filehosting[.]infinityfreeapp[.]com filihosting[.]infinityfreeapp[.]com
IP	37.191.122[.]186:3578 73.80.9[.]137:35780 37.191.122[.]186:3578 68.76.150[.]97:8080 174.53.242[.]108:8080

Tabela 3 – Indicadores de Compromissos de Rede.

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**
- **Recordedfuture**
- **TheHackerNews**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH