BOLETIM DE SEGURANÇA

Disseminação de stealer através de anúncios tendo como alvos usuários de MacOS

heimdall
security research
A DIVISION OF ISH

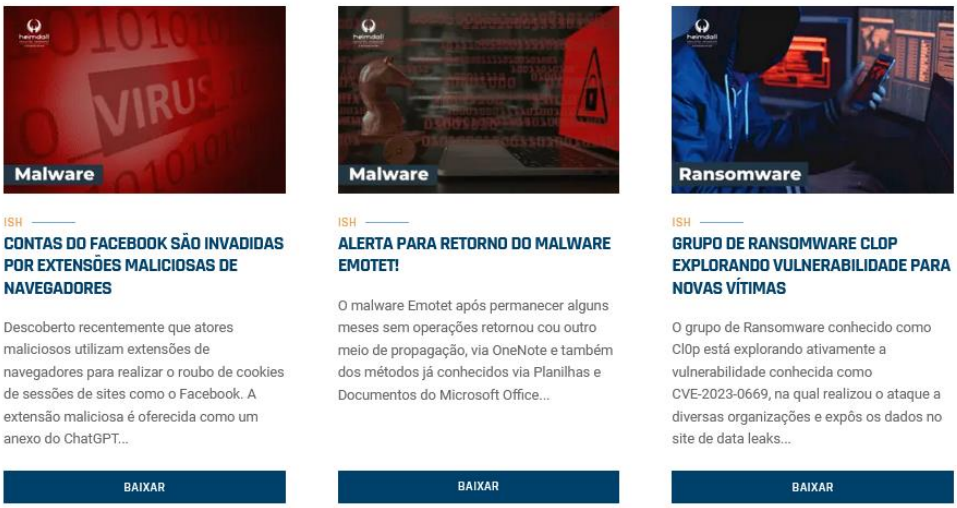
TLP: CLEAR

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

Foi informado por pesquisadores de ameaça sobre ataques de infostealer que visam usuários do macOS. Embora cada ataque utilize métodos distintos para comprometer os Macs, todos compartilham um objetivo comum: a apropriação indevida de informações sensíveis dos usuários. No último ano, o sistema macOS foi alvo constante de infostealers. Esses invasores focam principalmente em indivíduos ligados ao setor de criptomoedas, buscando coletar credenciais e informações de diversas carteiras de criptomoedas. Notou-se uma evolução inovadora nas estratégias e táticas empregadas por esses invasores para comprometer os usuários e extrair seus dados.

2 INFORMAÇÕES SOBRE ATAQUES CONTÍNUOS

Um dos ataques se refere ao do Atomic Stealer através de anúncios patrocinados. Ao realizar uma busca no Google pelo termo "Arc Browser", descobrimos que ao clicar no link patrocinado, que aparenta ser do navegador Arc legítimo, somos redirecionados para um site mal-intencionado, aricl[.]net, que se passa pelo site legítimo do Arc.

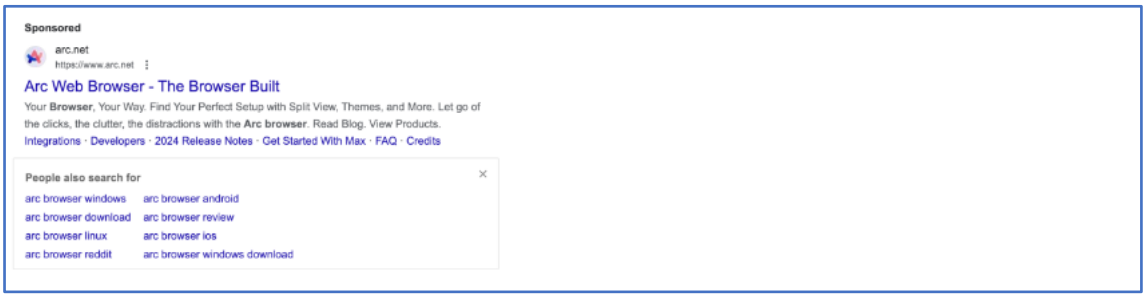


Figura 1 – Busca por Arc Browser.

```
Link dos serviços de anúncios do Google:

hXXps://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiC8Jm6-
ZSFAxUIwUwCHXbYB3MYABAAGgJ0bQ&ase=2&gclid=EAIaIQobChMIgvCZuvmUhQMVCMFMAh122AdzEAAYASAAEgKHuvD_BwE&e
i=0lQEZp-wCbWq ptQP-
Kq0mA8&ohost=www.google.com&cid=CAASJORoo4VHmMOQTyTY97tSpGD2A1DEcypIUn9R0xOdHJi1x9N3KQ&sig=AOD64_2I
OygLFSykCaouP6GmJOVlWRg3AA&q&sqi=2&nis=4&adurl&ved=2ahUKEwif4Y66- ZSFAxU1lYkEHXgVDfMQ0Qx6BAgJEAE
```

Figura 2 – redirecionamento para o site mal-intencionado.

A mesma conclusão foi alcançada pelos usuários do Reddit. De forma intrigante, o acesso direto ao site mal-intencionado é barrado por um erro. Aparentemente, para escapar da detecção, o acesso só é possível através de um link patrocinado gerado especificamente para esse fim.

Figura 3 – Mensagem de erro de retorno.

O site nocivo aricl[.]net é apresentada a seguir, local onde o usuário acaba por fazer o download de um aplicativo prejudicial. Em determinadas situações, um link patrocinado pode redirecionar o usuário para um site igualmente mal-intencionado, hospedado em airci[.]net.

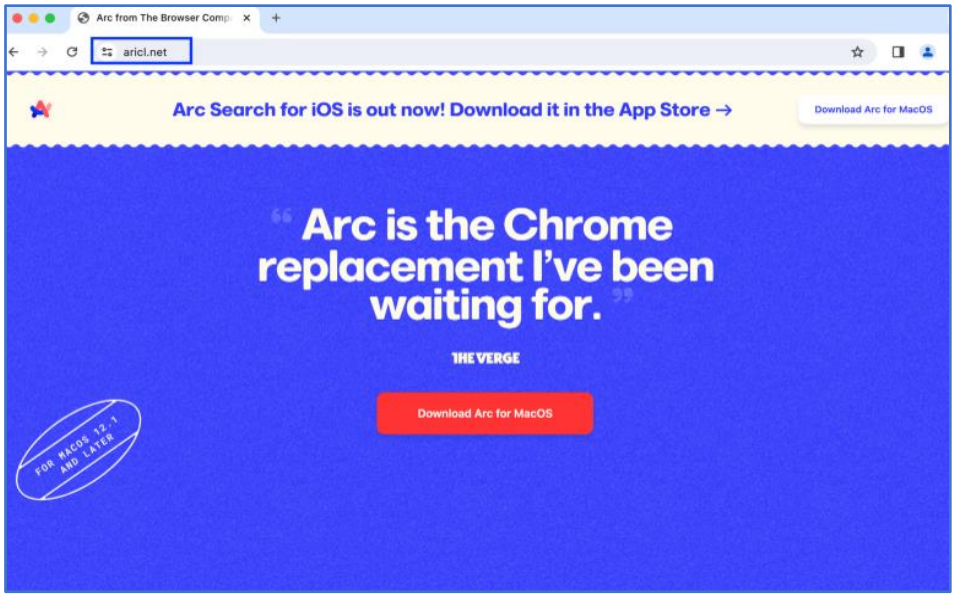


Figura 4 – Site malicioso idêntico ao original.

Notou-se uma tentativa de rodar um executável sem assinatura, que possuía um hash inválido conhecido, localizado em:

/Applications/Meethub.app/Contents/MacOS/sleve

A ausência de assinatura e o nome do pedido levantaram suspeitas, justificando uma investigação. A discrepância entre o nome do aplicativo e o nome do executável, embora não seja uma exigência do sistema operacional, é atípica e chamou a atenção. A exploração desse aplicativo se mostrou válida quando essa inconsistência foi descoberta. Uma análise mais detalhada nos direcionou ao site meethub[.]gg.

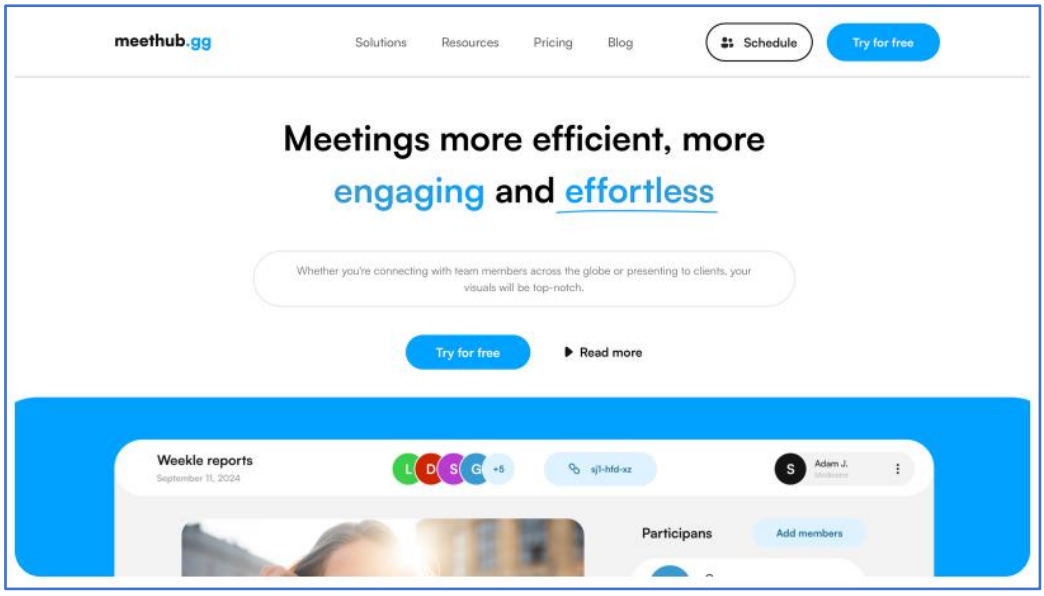


Figura 5 – Site meethub.org.

O Meethub, é uma organização com forte presença no Telegram e Medium, é conhecido por sua popularidade na plataforma X, onde reuniu mais de oito mil seguidores, muitos dos quais demonstraram interesse em criptomoedas. Relatos de vítimas indicam que golpistas, se passando por pessoas inofensivas, enviaram mensagens diretas com o objetivo de agendar reuniões. Em um caso, a reunião era para discutir a gravação de um podcast e, em outro, uma oportunidade de emprego. Ambos os perfis tinham forte envolvimento com Crypto e Blockchain.

Quando o contato foi feito, o golpista solicitou o uso do Meethub como plataforma para a reunião virtual. Ao acessar o site do Meethub e clicar em "Experimentar gratuitamente", são disponibilizados links para as versões Windows e macOS. Ao escolher a versão macOS, um pacote não assinado de 51 megabytes é baixado (7f22760d6d85f8173292d39ea087f35695ad65ab). Após o download, o site fornece instruções sobre como contornar qualquer aviso do Gatekeeper.

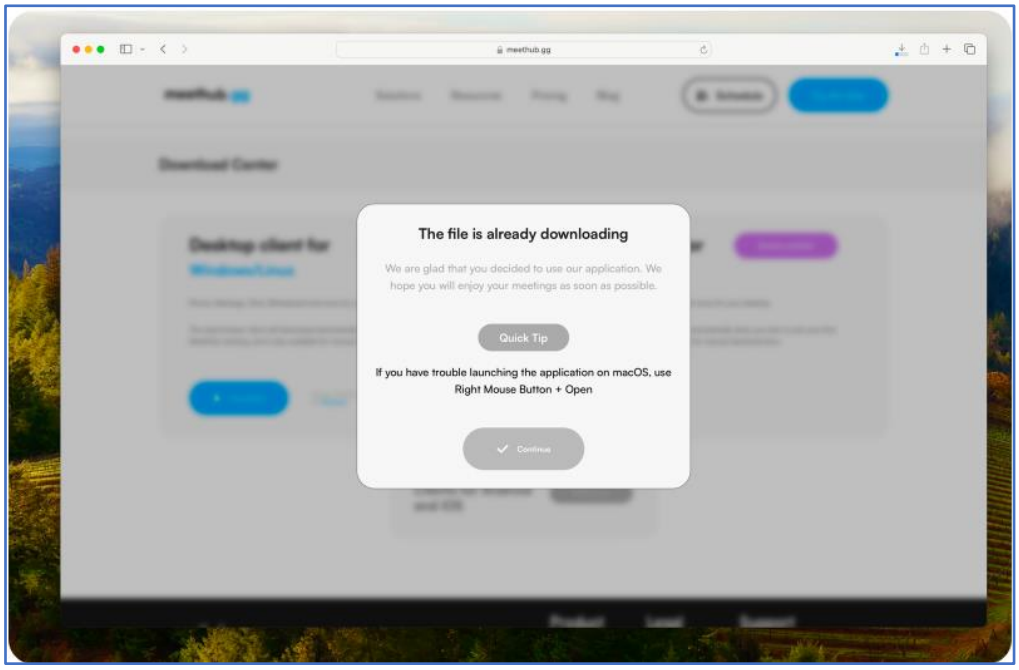


Figura 6 – Solicitação feita pelo golpista.

O aplicativo baixado, à primeira vista, parece ser compatível apenas com a arquitetura Intel, conforme indicado pelo comando:

file /Applications/MeetHub.app/Contents/MacOS/sleve

que retorna:

/Applications/MeetHub.app/Contents/MacOS/sleve: Mach-O 64-bit executable x86_64

Isso pode ser uma decisão deliberada ou um descuido do criador do malware. Para que o aplicativo funcione corretamente na mais recente arquitetura ARM, é necessário instalar o Rosetta. Se não estiver instalado, o aplicativo não será iniciado após a instalação, e o usuário terá que iniciá-lo manualmente e seguir as instruções para instalar o Rosetta.

O binário principal do aplicativo, localizado em Meethub.app/Contents/MacOS/sleve (3865636ed27ae81f146ed5b9ac9a25f53a6d10a7), inicia sua operação executando uma série de comandos de reconhecimento, como uname, sw_verse e ioreg. Este comportamento é semelhante ao do Atomic Stealer, que também solicita a senha de login do macOS ao usuário por meio de uma chamada AppleScript.

```
"osascript","-e","exibir caixa de diálogo \"O inicializador precisa de permissões para ativar
atualizações automáticas em segundo plano.\n\nPor favor, digite sua senha.\" com o título \"Sistema
de atualizações automáticas\" resposta padrão \"\ "com ícones de botões de cuidado {\"Continuar\"}
botão padrão \"Continuar\" com resposta oculta"
```

Figura 7 – Chamada AppleScript.

Embora a conexão direta não seja confirmada, existem várias semelhanças notáveis entre este stealer e o stealer conhecido como Realst. Ambos têm características comuns, como a preferência pela linguagem Rust para o executável principal e a utilização do chainbreaker.

3 CONCLUSÃO

No ano passado, foi observado vários ataques de infostealer contra usuários do macOS. Esses ataques tendem a focar na indústria de criptomoedas, pois podem resultar em grandes recompensas para os invasores. Tanto grupos APT quanto cibercriminosos estão usando engenharia social para obter ganhos em criptomoedas. A construção de relacionamentos antes da infiltração está se tornando cada vez mais comum na plataforma macOS. É essencial que os usuários permaneçam vigilantes e alertas para esses tipos de ataques.

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:

Habilite a Autenticação Multifator (MFA)

- A MFA adiciona uma camada extra de segurança, exigindo mais de uma forma de verificação para acessar suas contas.

Alteração de senhas

- Troque suas senhas periodicamente e implemente uma gestão unificada de credenciais.

Limpeza de cookies

- Não salve senhas e limpe os cookies em navegadores regularmente.

Conscientize os funcionários

- Realize treinamentos sobre como identificar e evitar ameaças cibernéticas.

Mantenha suas soluções de segurança atualizadas

- Isso inclui antivírus, firewall e anti-malware.

Atualize seus sistemas e softwares regularmente

- As atualizações frequentemente corrigem vulnerabilidades que podem ser exploradas por malwares.

Faça backups regulares

- Isso garante a recuperação de dados em caso 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 compromisso do artefato	
md5:	3571b2d71386626a740c37c531635254
sha1:	ba59bb35e8dfbe77676c8130c8c2d61c22b14564
sha256:	271d55c5f38a1963188dbf459200971dd8fd57a9a5677ecbd5a097c3e5664990
File name:	ArcSetup

Indicadores de compromisso do artefato	
md5:	6794419fca2c1b2a0b52856f23ccfde5
sha1:	d294b86c5aa7e90ff1f7367eb9fdad8d47193f22
sha256:	6c3090b67aa303e814076c4165b7ebcd446fa3ae801d1b2775abd6086e7a70ae
File name:	localfile~.x64

Indicadores de compromisso do artefato	
md5:	e8d467bd59c91914d64ef224106d5498
sha1:	af33c2bc39371a5667b65c38a62919c59f5ad084
sha256:	a0fce15f14de251375fe6f88c60a635755213fabb4e616a0054ed418982c7fff
File name:	localfile~.arm64

Indicadores de compromisso do artefato	
md5:	631101eac05b977b2c741eb25197a9d6
sha1:	28e35f4d92f3a0bf85fdffeb5b695119de823548
sha256:	af4ff6e73a751c408e7f17b8843ccd49debffde155a1f39ab365a32a0f8f9cd8
File name:	ArcInstaller

Indicadores de compromisso do artefato	
md5:	1f70089d0049fac2e83ae2120e35cae0
sha1:	28cc0be3aad1479c4d4ba616be6462a2c5c7ac18
sha256:	32a5781b40d076d5e913e7a69eb65d80e4808ce1b3ed3e3b28bbd6f26c9d3de0
File name:	localfile~.x64

Indicadores de compromisso do artefato	
md5:	89f10403f84d7dc2d8fc3dcf7672429e
sha1:	0ac59146723d72b2faad6a637cdd9fb2a6221f7e
sha256:	387d6548a5a42280ba5b479043b2c6f65344513b730a802627b53b87a0034b48
File name:	localfile~.arm64

Indicadores de compromisso do artefato	
md5:	378bf27159443f404cc0b2d276ae3497
sha1:	7f22760d6d85f8173292d39ea087f35695ad65ab -
sha256:	2f28626c7189d15602fe244ebd42b21c1d0bf98737be8af325080af5da58e518
File name:	MeetHub.pkg

Indicadores de compromisso do artefato	
md5:	2bb85c592f35b3252155481cc47d8221
sha1:	3865636ed27ae81f146ed5b9ac9a25f53a6d10a7
sha256:	ebaab1a8d73c5131a034c6701c24b92648c6e511cd28524c06039873c86a2193
File name:	sleve

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	https://aricl[.]net https://airci[.]net https://meethub[.]gg
IP	46[.]101[.]104[.]172 193[.]233[.]132[.]188

Tabela 2 – 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**
- Jamf
- Thehackernews

heimdall
security research
A DIVISION OF ISH