TLP: CLEAR

BOLETIM DE SEGURANÇA

Golpe utiliza aplicativos de videoconferência falsos para roubar dados de profissionais da Web3

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INFORMAÇÕES SOBRE A AMEAÇA

Foi descoberta uma nova fraude direcionada a profissionais da Web3. A operação envolve o malware Realst, um stealer de criptomoedas com versões para **macOS** e **Windows**, ativo há cerca de quatro meses. Os cibercriminosos por trás desse malware criaram empresas fictícias utilizando IA para parecerem mais legítimos. Atualmente, a empresa é conhecida como "Meetio", mas já passou por diversos nomes nos últimos meses. Para se apresentarem como uma empresa autêntica, os criminosos desenvolveram um site com conteúdo gerado por IA e criaram perfis em redes sociais. Eles entram em contato com as vítimas para agendar uma videoconferência, solicitando que o usuário baixe o aplicativo de reunião do site, que na verdade é o malware Realst.

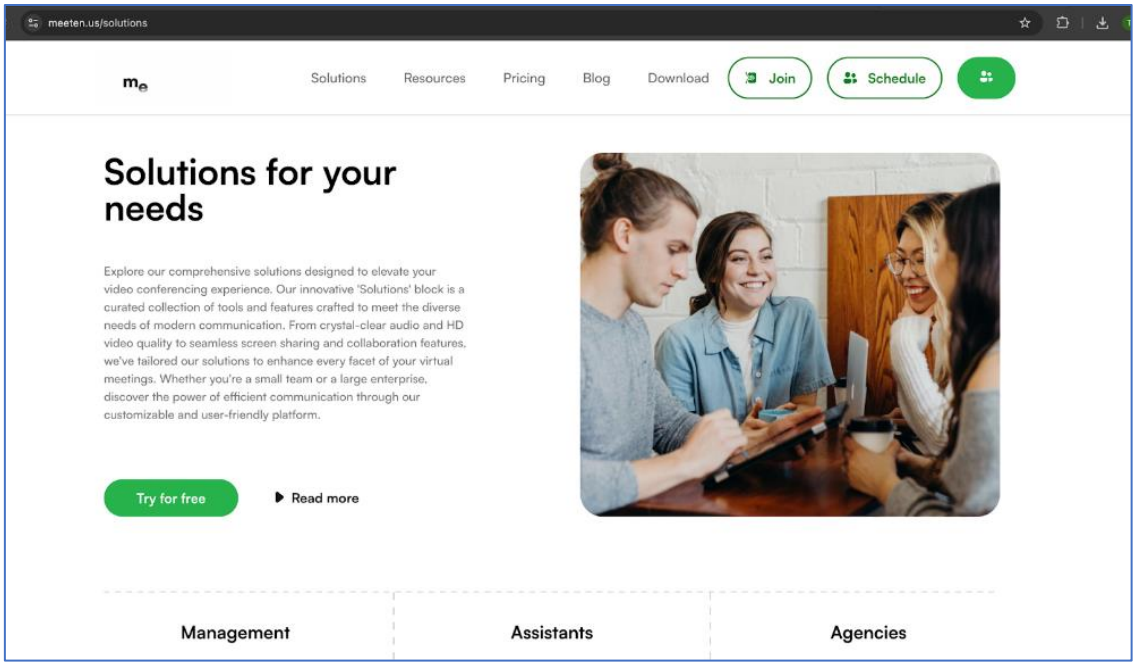

Figura 1 – Tela inicial do aplicativo Meeten.

O aplicativo "Meeten" está tentando burlar usuários para que baixem um software que rouba informações. A empresa frequentemente muda de nome, tendo usado Clusee[.]com, Cuesee, Meeten[.]gg, Meeten[.]us, Meetone[.]gg e atualmente operando como Meetio. Para parecer legítima, os criadores da ameaça desenvolveram sites completos com blogs, conteúdo gerado por IA e perfis em redes sociais como Twitter e Medium.

Relatos de vítimas indicam que o golpe é aplicado de várias formas. Em um caso, um usuário foi contatado no Telegram por alguém que ele conhecia para discutir uma oportunidade de negócio e marcar uma reunião. No entanto, a conta do Telegram era falsa, criada para se passar por um contato da vítima. O golpista chegou a enviar uma apresentação de investimento da empresa da vítima, mostrando a sofisticação e o direcionamento do golpe. Outros relatos mencionam

que usuários em chamadas relacionadas ao trabalho Web3 baixaram o software e tiveram suas criptomoedas roubadas.

Após o contato, a vítima é direcionada ao site Meeten para baixar o produto. Além de hospedar softwares maliciosos, os sites Meeten contêm Javascript que rouba criptomoedas armazenadas nos navegadores, mesmo antes de qualquer malware ser instalado.

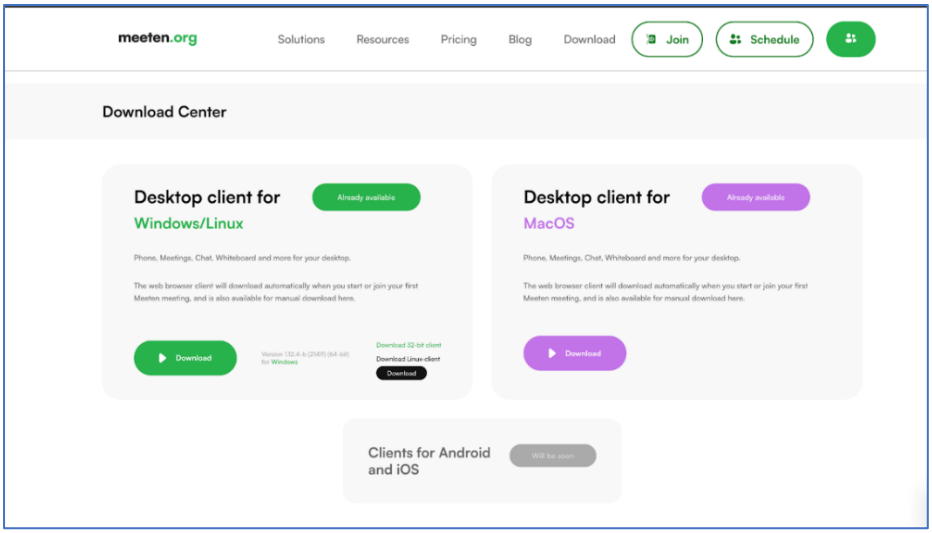

Figura 2 – Página de downloads no Meeten.

Ao acessar o site "Meeten", a vítima é direcionada para uma página de downloads que oferece opções para macOS ou Windows/Linux. No entanto, nesta versão do site, todos os links de download redirecionam para a versão macOS. O pacote baixado contém um binário de 64 bits chamado "fastquery", embora outras variantes do malware sejam distribuídas como um DMG com um binário multi-arquitetura. Este binário é desenvolvido em Rust e sua principal função é roubar informações.

Ao ser executado, duas mensagens de erro são exibidas. A primeira mensagem informa: "**Cannot connect to the server. Please reinstall or use a VPN**". e apresenta um botão de continuar. A ferramenta de linha de comando do macOS, osascript, é utilizada para solicitar a senha do usuário, um comportamento comum em malwares direcionados ao macOS.

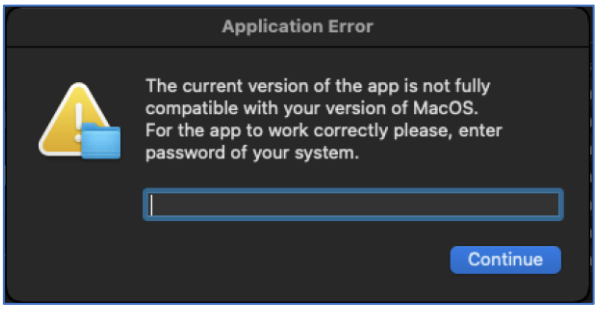

Figura 3 – Popup que solicita senha do usuário.

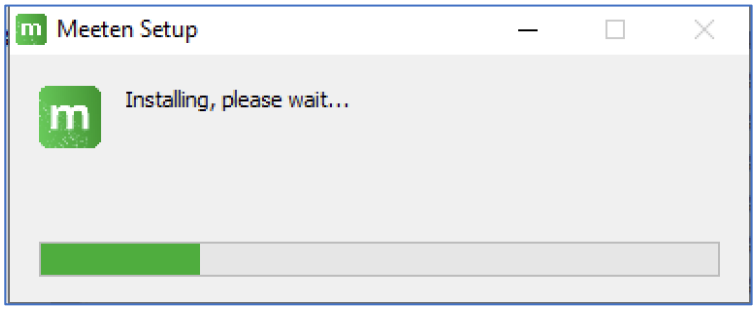

Figura 4 – Instalação do MeetenApp.exe em sistemas Windows.

Durante a análise da versão macOS do Meeten, a Cado Security descobriu uma variante do malware para Windows. O arquivo executável, denominado "**MeetenApp.exe**", é um instalador criado com o Nullsoft Scriptable Installer System (NSIS). Este instalador possui uma assinatura digital legítima da "Brys Software", que aparentemente foi roubada.

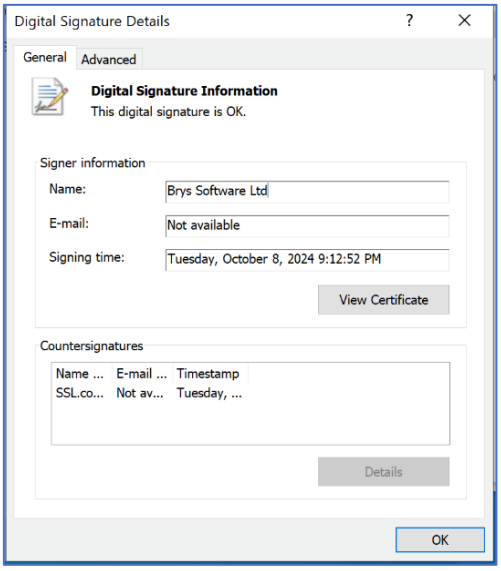

Figura 5 – Assinatura digital do Meeten.

Depois de extrair os arquivos do instalador, duas pastas serão oencontradas: $PLUGINDIR e $R0. Dentro da pasta $PLUGINDIR, há um arquivo 7zip chamado "app-64". Este arquivo contém recursos, ativos, binários e um arquivo app.asar, o que indica que se trata de um aplicativo Electron. Os aplicativos Electron são desenvolvidos usando a estrutura Electron, que permite criar aplicativos de desktop multiplataforma utilizando linguagens web como Javascript. Os arquivos app.asar são utilizados pelo runtime do Electron e funcionam como um sistema de arquivos virtual, contendo o código do aplicativo, ativos e dependências.

O UpdateMC.exe é um executável desenvolvido em Rust, com funcionalidades semelhantes à versão para macOS. Este software malicioso vasculha diversos repositórios de dados para coletar e exfiltrar informações sensíveis em formato zip. O Meeten é capaz de roubar dados de:

- Credenciais do Telegram
- Informações de cartões bancários
- Cookies, histórico e credenciais de preenchimento automático dos navegadores Google Chrome, Opera, Brave, Microsoft Edge, Arc, CocCoc e Vivaldi
- Carteiras Ledger
- Carteiras Trezor
- Carteiras Phantom
- Carteiras Binance

Os dados coletados são armazenados em uma pasta nomeada com o HWID do usuário, localizada no diretório *AppData/Local/Temp*, antes de serem enviados para o endereço IP 172[.]104.133.212.

2 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Execution	T1204	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Persistence	T1547.001	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Defense Evasion	T1070.004 T1553.001 T1553.002 T1497.001	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Credential Access	T1555.001 T1555.003 T1539	Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping.
Discovery	T1217 T1082 T1016 T1033 T1007	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Collection	T1005 T1074	Consiste em técnicas que os adversários podem usar para reunir informações e as fontes de onde as informações são coletadas que são relevantes para seguir os objetivos do adversário.
Command and Control	T1071.001	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Exfiltration	T1041	Consiste em técnicas que adversários podem usar para roubar dados da sua rede. Depois de coletar dados, os adversários geralmente os empacotam para evitar a detecção ao removê-los.
Impact	T1657	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

3 RECOMENDAÇÕES

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

Use senhas fortes e únicas

- Evite senhas óbvias e reutilizadas. Combine letras maiúsculas, minúsculas, números e símbolos.

Habilite a autenticação de dois fatores (2FA)

- Isso adiciona uma camada extra de segurança, exigindo uma segunda forma de verificação além da senha.

Baixe aplicativos apenas de fontes oficiais

- Sempre baixe aplicativos de videoconferência diretamente dos sites oficiais ou lojas de aplicativos confiáveis.

Mantenha os aplicativos atualizados

- Atualizações frequentemente incluem correções de segurança importantes.

Verifique os links antes de clicar

- Desconfie de links recebidos por e-mail ou mensagens que direcionam para downloads de aplicativos.

Limite o número de participantes nas reuniões

- Menos participantes reduzem as chances de invasões e facilitam o controle de segurança.

Encerre as chamadas corretamente

- Certifique-se de que a reunião está realmente encerrada para evitar que alguém permaneça na chamada sem ser notado.

4 INDICADORES DE COMPROMETIMENTO (IOC)

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores do artefato	
md5:	6a925b71afa41d72e4a7d01034e8501b
sha1:	80b91f12ac229bd0979e3980aeb79691996ebf79
sha256:	5e6cc2ed3876197561ba60a8d8aa7042d025e997cc1046ea351b5b2bc48f9dd7
File name:	5e6cc2ed3876197561ba60a8d8aa7042d025e997cc1046ea351b5b2bc48f9dd7.exe

Indicadores do artefato	
md5:	209af36bb119a5e070bad479d73498f7
sha1:	131bdc5089172486da69c6b7008ea836aa75737c
sha256:	8d731b0bd8c0cda9f923ed0980ea76d57ba036c3a73acb9f4ac8ffe4e4734b83
File name:	UpdateMC.exe

Indicadores do artefato	
md5:	d74a885545ec5c0143a172047094ed59
sha1:	10b6c73ecc4865c438464ee28b3b2533f1e5b801
sha256:	aea0bfbba8dd4f3cb99b33792e044af653c2ea07af960f9587d389160497d647
File name:	MicrosoftRuntimeComponentsX86.exe

Indicadores do artefato	
md5:	09b7650d8b4a6d8c8fbb855d6626e25d
sha1:	6757e75085a4fb93d29456a2916754932c1468a3
sha256:	be012ac8a3f046e56e1c6a293ae567462c01216d024032c4225f656d8002691e
File name:	CluseeApp.pkg

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	http[:]//172.104.133[.]212:8880/new_analytics http[:]//172.104.133[.]212:8880/opened http[:]//172.104.133[.]212:8880/metrics http[:]//172.104.133[.]212:8880/sede www[.]meeten[.]us www[.]meetio[.]one www[.]meetone[.]gg www[.]clusee[.]com
IP	139[.]162.179[.]170 199[.]247.4[.]86 172[.]104.133[.]212

Tabela 3 – Indicadores de Comprometimento 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CadoSecurity**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH