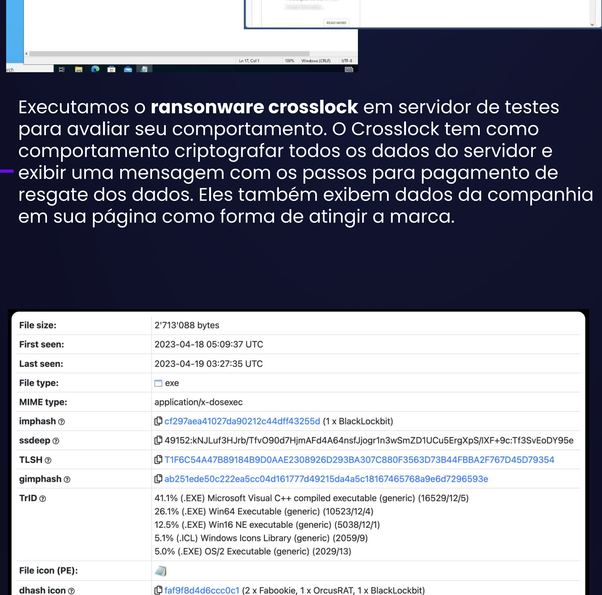
POPULOS

O **SentinelOne XDR** oferece proteção em tempo real contra os mais avançados tipos de ataque sejam eles **malwares** e/ou **ransonwares**.

SentinelOne Singularity XDR

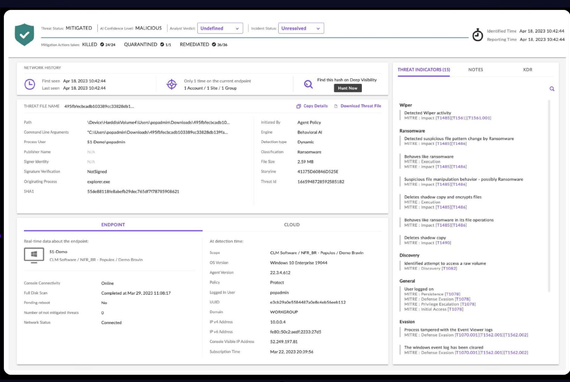
Através da console do **SentinelOne** é possível inventariar todos os softwares do ambiente e gerar um relatório minucioso de suas vulnerabilidades.



Executamos o **ransonware crosslock** em servidor de testes para avaliar seu comportamento. O Crosslock tem como comportamento criptografar todos os dados do servidor e exibir uma mensagem com os passos para pagamento de resgate dos dados. Eles também exibem dados da companhia em sua página como forma de atingir a marca.

File size:	2'713'088 bytes
First seen:	2023-04-18 05:09:37 UTC
Last seen:	2023-04-19 03:27:35 UTC
File type:	exe
MIME type:	application/x-dosexec
imphash	cf297aea41027da90212c44dff43255d (1 x BlackLockbit)
ssdeep	49152:kNJLuf3HJrb/TfvO90d7HjmAFd4A64nsfJjogr1n3wSmZD1UCu5ErgXpS/IXF+9c:Tf3SvEoDY95e
TLSH	T1F6C54A47B89184B9D0AAE2308926D293BA307C880F3563D73B44FBBA2F767D45D79354
gimphash	ab251ede50c222ea5cc04d161777d49215da4a5c18167465768a9e6d7296593e
TrID	41.1% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5) 26.1% (.EXE) Win64 Executable (generic) (10523/12/4) 12.5% (.EXE) Win16 NE executable (generic) (5038/12/1) 5.1% (.ICL) Windows Icons Library (generic) (2059/9) 5.0% (.EXE) OS/2 Executable (generic) (2029/13)
File icon (PE):	
dhash icon	faf9f8d4d6ccc0c1 (2 x Fabookie, 1 x OrcusRAT, 1 x BlackLockbit)
Reporter	@1ZRR4H
Tags:	CrossLock exe

Após, executamos o crosslock em um servidor com o **SentinelOne**.
Através de sua engine de análise comportamental o **SentinelOne** conseguiu impedir a execução do **ransonware** em tempo real, impossibilitando a criptografia dos dados e protegendo o ambiente.



No menu de incidente do **SentinelOne** podemos ter dados detalhados da tentativa de ataque como endpoint afetado, data, hash, indicadores comportamentais que foram usados para julgar se era uma **ameaça** real ou não, entre outros.

Ter uma ferramenta capaz de impedir **ameaças** recém-lançadas em tempo real é primordial para manter a saúde de ambientes críticos.

Nós, da **POPULOS**, temos as ferramentas necessárias para ajudá-los a evitar situações de crise como essa. Nossos profissionais estão à disposição.

POPULOS

comercial@populos.com.br

www.populos.com.br