A Cyber Crucible testa exaustivamente todos os ransomwares possíveis?

A Cyber Crucible opera com base em modelagem comportamental em nível de kernel, para descobrir rapidamente comportamentos de roubo de dados, roubo de credenciais e criptografia por ransomware. As decisões comportamentais são tomadas utilizando informações do comportamento de processos, comportamentos derivados de memória e certos tipos de comportamentos originados de arquivos, para tomar uma decisão exatamente no momento em que a extorsão está prestes a ocorrer.

Apesar do número muito grande de amostras de ransomware e de software com temática de extorsão, elas podem ser categorizadas comportamentalmente em um número relativamente pequeno de conjuntos.

Na superfície, porém, as defesas “superficiais” utilizadas por diversas ferramentas de segurança têm um número muito grande de ferramentas de extorsão a tentar combater. É importante entender que nossas análises comportamentais vão muito mais a fundo nas ferramentas e nas táticas dos atacantes, reduzindo drasticamente a necessidade de algum tipo de teste (impossível) exaustivo de todos os malwares possíveis o tempo todo.

Os desenvolvedores da Cyber Crucible categorizam os comportamentos de memória, processos e arquivos em nível de kernel de uma ferramenta de extorsão e, em seguida, garantem que ela se enquadre em uma das capacidades defensivas conhecidas. Ocasionalmente, de forma semelhante a uma vacina, a fórmula pode ser ajustada ligeiramente para produzir uma resposta mais precisa.

Muito raramente surge algo completamente novo.

A equipe da Cyber Crucible trabalha exaustivamente para descobrir preventivamente técnicas inéditas ainda não observadas em nossa base de clientes ou em inteligência de ameaças.

O efeito?

1. A defesa da Cyber Crucible contra ferramentas de extorsão é completa contra todas as variantes conhecidas de ransomware.

2. Novas variantes de ransomware são bloqueadas antes mesmo de atingirem os primeiros clientes. Nem sequer sabemos como chamar a maior parte do software contra o qual nos defendemos por cerca de 120 dias, até que os pesquisadores “se atualizem”.

3. Desenvolvedores de ransomware e de ferramentas de extorsão às vezes nos ligam para ver o que estamos fazendo, na tentativa de encontrar uma brecha. Infelizmente, a frustração causada pela nossa presença parece, às vezes, estimular a evolução por parte deles, o que torna outras ferramentas ainda menos eficazes.

4. Recebemos com satisfação os testes de nosso software. Quando testadores de intrusão, analistas de malware ou profissionais de emulação de adversários entram no processo de venda — ficamos entusiasmados!

Revision #1
Created 2026-07-24 05:52:13 UTC by Dennis Underwood
Updated 2026-07-24 05:52:13 UTC by Dennis Underwood