Implantação em um Ambiente Já Infectado

Contexto

As implantações de clientes da Cyber Crucible resultam rotineiramente na descoberta de infecções anteriormente desconhecidas. As redes normalmente não estão livres de infecções, mesmo que as ferramentas de defesa de segurança cibernética existentes tenham dado sinal verde.

Um ataque de ransomware fornece um ponto de demarcação, ou ponto crucial, altamente visível, para que uma empresa meça com que frequência os hackers conseguem realizar um novo ataque com sucesso, e qual é o grau de sucesso desses ataques.

- Relatórios de código aberto e inteligência de ameaças revelam uma taxa de reataque de clientes que não são da Cyber Crucible de cerca de 80%.
- A Cyber Crucible observou que cerca de 10% dos endpoints têm pelo menos uma tentativa de roubo de identidade, como senhas, chaves ou tokens, por período de 90 dias.
- A Cyber Crucible observa que os atacantes tentam retomar uma posição em um ambiente aproximadamente uma vez por mês.

Do ponto de vista de resposta a incidentes ou forense, a Cyber Crucible é uma excelente ferramenta para retomar o controle da rede. Especialmente para vítimas de ataques, suspeitamos que os atacantes mantêm visibilidade sobre o estado de recuperação e a saúde financeira das vítimas, para melhor cronometrar quando atacar novamente.

O Que Acontece Imediatamente Após a Instalação

A Cyber Crucible começa automaticamente a suspender programas em execução que sejam observados se comportando de forma maliciosa.

A implantação do produto Cyber Crucible pode resultar na suspensão de múltiplos programas em múltiplas máquinas, à medida que o ambiente é limpo.

Às vezes, uma implantação parcial da Cyber Crucible pode resultar em uma tentativa do hacker de retomar o controle através das máquinas que não possuem a proteção da Cyber Crucible.

Por exemplo, a Cyber Crucible foi certa vez instalada em apenas uma parte dos desktops de uma vítima recente de violação de dados. Os hackers tentaram desinstalar a Cyber Crucible conectando-se a partir das máquinas desprotegidas e, por fim, começaram a desligar as máquinas protegidas.

O Que Acontece com Malware Dormente, Aguardando Tarefas Futuras?

Um malware que não está agindo em nome dos atacantes é acionado quando o malware começa a acessar dados.

Vamos percorrer um cenário:

Duas máquinas têm malware nelas. Vamos chamá-las de Máquina A e Máquina B.

Ambas as amostras de malware são atualmente indetectáveis pelas suas ferramentas de segurança favoritas.

O malware da Máquina A não faz nada, apenas aguarda instruções. A Cyber Crucible não detecta o malware. O malware também ainda não é detectável por outras ferramentas de segurança.

O malware da Máquina B está tentando acessar dados ou dados de identidade. Imediatamente após um ataque bem-sucedido, os comportamentos mais comuns que observamos, quando os atacantes atribuem tarefas ao seu malware, são garantir que possuem dados de identidade atualizados, como senhas ou tokens, e enumerar novos dados. Ou seja, em parte, "obter as novas senhas após os administradores redefinirem as senhas", e, em parte, "ficar de olho em busca de novos dados".

Na Máquina B, a Cyber Crucible suspende imediatamente a aplicação.

Depois de um período que varia de um mês a um ano, o malware da Máquina A é finalmente identificado após um número suficiente de vítimas ter reportado o malware aos bancos de dados

dos fornecedores de segurança. Quanto mais disciplinados forem os atacantes na distribuição dessa amostra, mais tempo esse malware específico permanecerá indetectado.

O malware da Máquina B foi neutralizado, congelado no lugar.

O malware da Máquina A está preso. No segundo (bem, 100 milissegundos) em que tenta acessar quaisquer dados ou informações de identidade, o malware da Máquina A é suspenso. O cliente está protegido, mesmo que o malware exista por dias, ou até anos, sem ser detectado por outras ferramentas.

Detalhes Adicionais - Reinicializações Podem Ser Valiosas

Algumas de nossas análises são mais precisas quando o ciclo de vida do processo pode ser rastreado desde o início da aplicação até o estado presente.

Reinicializar uma máquina após a instalação pode ser vantajoso.

Programas já em execução antes da instalação não terão inspeção analítica completa por parte da Cyber Crucible. A reinicialização força esses programas a reiniciarem, proporcionando, assim, inspeção completa a todos os programas.

Revision #1
Created 2026-07-24 05:28:56 UTC by Dennis Underwood
Updated 2026-07-24 05:28:56 UTC by Dennis Underwood