# Atividade

Um grupo criminoso tem tentado atacar uma empresa para roubar seus segredos de forma persistente. Eles visam ter acesso a um laboratório para roubar segredos industriais. Com alguma engenharia social, eles já conseguiram nomes e endereços de e-mails das poucas pessoas da organização que trabalham dentro desta área e fizeram campanhas de phishing específicas (spear phishing) para eles. Algumas pessoas clicaram, mas o malware não conseguiu na movimentação lateral chegar a máquinas do laboratório.

Aparentemente, esta rede do laboratório está completamente segregada da rede do restante da organização. Como alternativa, os atores maliciosos ainda tentaram o truque de esquecer um dispositivo USB em locais estratégicos. Da mesma forma, computadores infectados não levaram o APT para dentro do laboratório. Nada é mantido nas máquinas dos pesquisadores do laboratório. Pelo jeito, existe mesmo uma rede segregada da rede da empresa, conectando os 3 laboratórios da empresa ao redor do mundo.

# Atividade

Os pesquisadores acessam diretamente a console dos computadores nos laboratórios. O grupo planejou então partir para uma intrusão física para inserção de um implante nesta rede que pudesse ficar de forma persistente roubando dados confidenciais. Investiram meses em ações de engenharia social para descobrir a dinâmica da empresa. Em particular, sobre duas áreas seguras: o datacenter e próprio laboratório. Descobriram que o lixo corporativo era descartado em local de fácil acesso. Entrou em ação a prática contínua de trashing. No lixo, encontraram uma informação bem interessante. E-mails de pessoas que aprovam a entrada de terceiros na empresa, incluindo períodos especiais.

Além dos emails dos aprovadores, foi possível verificar o conteúdo das mensagens enviadas dando aprovação para a recepção da empresa permitir a entrada de terceiros. O grupo então partiu para a primeira intrusão física. Enviaram um email falsificado supostamente aprovando a entrada de um membro do grupo naquele dia pela noite. Funcionou!

# Atividade

Na recepção, o intruso se passava por um terceiro que faria um trabalho de manutenção nos cabos. Mas percebeu que, sem alguém da TI para acompanhar, não conseguiria chegar em qualquer daquelas áreas restritas. No entanto, o intruso foi capaz de verificar armários abertos, impressos nas mesas, informações nas lousas em salas de reunião e lixeiras. Não foi possível conectar na rede Wi-Fi da empresa por causa do NAC e do IEEE 802.1X implementados. No entanto, o intruso conseguiu conectar a máquina em alguns pontos de rede usando o cabo RJ-45 (não havia NAC para alguns destes pontos de acesso). Nada demais foi conseguido com a conexão.

Foi possível verificar que o datacenter controla a entrada dos usuários usando crachás baseados em RFID. Já o laboratório, faz uso da fingerprint para permitir o acesso. Câmeras existem apenas em alguns pontos, como entradas/saídas. Acredita-se que padrão similar seja usado nestas áreas mais restritas também. Portanto a cobertura das câmeras não é completa.

# Atividade

O grupo passou algum tempo estudando o material recuperado e fotos do ambiente para planejar o próximo passo. Investiram na tentativa de clonar um crachá de acesso ao datacenter. Algumas pessoas com tal acesso foram identificadas com as informações obtidas e com OSINT (LinkedIn, principalmente). Em uma semana, eles voltaram ao prédio com um cartão clonado.

O processo usado para a entrada não autorizada funcionou mais uma vez. Desta vez, os atores maliciosos conseguiram entrar no datacenter como funcionários da TI. Clonaram a credencial de um dos usuários que quase nunca participa de atividades noturnas. Isto pode ter ajudado a evitar que o pessoal da segurança daquele turno da noite percebesse alguma coisa estranha. No datacenter, acharam algumas câmeras. Aparentemente, não havia pontos cegos. Mas agiram como qualquer membro da TI, mexendo nos cabos e avaliando discretamente o ambiente. Acharam oportunidades para a implantação de um Raspberry PI. Um Rubber ducky foi deixado no lugar também. O melhor: o implante foi capaz de conectar a um C2 do grupo e fazer sniffing de tráfego.

# Atividade

Agora o grupo tem um implante na rede que dá uma certa persistência e diminui os riscos de muitas intrusões físicas.

Com algum tráfego coletado, o grupo começou a analisar e percebeu que câmeras de vigilância não usam criptografia e possibilitam ataques: https://www.bleepingcomputer.com/news/security/researchers-hack-surveillance-systems-to-show-fake-video-feed/.

Agora o grande desafio é a biometria do laboratório. Mas as informações coletadas nas lixeiras permitiram descobrir que o controle para o estacionamento, para algumas áreas e para o próprio laboratório era configurado usando um sistema centralizado de gestão controlado pelo pessoal da TI. A console era simples e não tinha autenticação e, por isto, ficava trancada numa sala e nenhuma forma de acesso remoto era conhecida. Duas alternativas então poderiam ser usadas: lock picking ou uma cópia da chave.

# Atividade

Toda uma pesquisa sobre as pessoas da TI no email foi feita e membros do grupo passaram a buscar formas de conseguir uma cópia da chave usando engenharia social. Ficar visitando muitas vezes o site de forma não autorizada poderia despertar a desconfiança do pessoal de segurança.

O lock picking poderia falhar. A boa notícia para os criminosos foi que algumas chaves puderam ser fotografadas em momentos de descuido de funcionários da TI, enquanto fora da empresa (durante almoço ou em outros locais públicos). Com a foto, eles foram capazes de criar cópias: https://hackaday.com/2015/05/23/pictures-that-defeat-key-locks/. https://www.popsci.com/science/article/2013-08/app-tells-locksmiths-how-make-keys-photos/

E o grupo fez mais um acesso físico ao site, levando ferramentas para lock picking e cópias de chaves que poderiam funcionar para abrir a sala. E funcionou com uma das chaves!

# Atividade

Conseguiram acesso ao sistema e puderam cadastrar as suas digitais e um PIN para a abertura da cancela. Foram embora e esperaram um melhor momento para entrar no laboratório.

Quando voltaram pela última vez ao prédio da empresa, entraram pelo estacionamento sem precisar passar pela recepção. Conseguiram também acesso ao laboratório e não deixaram qualquer evidência nas câmeras desta área. Ela era acessada por um número menor de pessoas e facilmente um intruso poderia ser detectado. Deixaram inúmeros implantes e criaram uma rede Wi-Fi (backdoor) que fazia a supressão do envio do SSID para evitar a detecção. O grupo conseguiu manter a persistência desejada e passou a espionar tudo o que era realizado nos laboratórios da empresa. A exfiltration das informações acontecia pelo Wi-Fi escondido no laboratório sem que qualquer funcionário percebesse. Além de computadores Orange PI, usaram LAN turtles (https://shop.hak5.org/products/lan-turtle), o implante Scree Crab em salas de reunIão (https://shop.hak5.org/products/screen-crab) e o packet Squirrel (https://shop.hak5.org/products/packet-squirrel).

# Atividade

1. Quais as estratégias do grupo criminoso para conseguir o acesso persistente?
2. Quais os problemas de segurança física encontrados no cenário?
3. Quais soluções (tecnológicas e não tecnológicas) poderiam ser empregadas para atenuar ou eliminar as chances de sucesso do grupo criminoso?
4. Depois de tentativas frustradas com ciberataques, como explica o sucesso do grupo?
5. Que conclusões você poderia tirar deste incidente?