As organizações devem atualizar as defesas para táticas de aranha disper

Data: 2025-09-23 13:33:08

Autor: Inteligência Against Invaders

As organizações devem atualizar urgentemente suas defesas para se protegerem contra táticas

implantadas pelo coletivo de hackers Scattered Spider este ano, de acordo com especialistas que

falaram durante o Gartner Security & Risk Management Summit 2025.

Deve ser dada especial atenção aos instrumentos e controlos de identidade, aos processos de segurança e à gestão de riscos de terceiros, a fim de combater as técnicas novas e altamente eficazes utilizadas pelo grupo.

Durante uma sessão na Cúpula, George Glass, diretor associado de gerenciamento da empresa de consultoria de risco Kroll, discutiu Aranha Dispersa abordagem altamente bem-sucedida no comprometimento de metas de alto perfil de abril a julho de 2025.

O grupo, afiliado à rede criminosa online The Com, foi vinculado a uma série de ataques a varejistas em abril e maio, incluindo Marks & Spencer (M&S)o Cooperativa e Harrods.

Em seguida, mudou o foco para o setor de seguros em junho e, no final do mês, para o transporte indústria. Os ataques seguiram o mesmo manual, com as técnicas altamente eficazes no acesso a dados confidenciais e na implantação de ransomware.

Glass observou que o grupo é conhecido por ter usado ameaças de violência física a executivos como tática de extorsão.

Desde então, a atividade da Aranha Dispersa tem significativamente reduzido, que Glass atribuiu a ações de aplicação da lei, incluindo o detenção de suspeitos de serem membros da equipe em julho e “lutas internas” internas.

Com outros atores, como Caçadores brilhantes, usando táticas semelhantes ao Scatter Spider com grande sucesso, é vital que as organizações atualizem suas medidas de segurança para lidar com as táticas empregadas.

Os especialistas acreditam que existem muitas sobreposições e cooperação entre os grupos afiliados ao The Com, como Scattered Spider e ShinyHunters.

Por exemplo, o Ataque cibernético recente na gigante da fabricação de automóveis Jaguar Land Rover (JLR) foi reivindicado por um grupo que se autodenomina “Scattered Lapsus$ Hunters”, sugerindo uma possível colaboração entre Scattered Spider, ShinyHunters e Lapsus$.

Como o Scatter Spider opera: um estudo de caso

Glass forneceu informações sobre um ataque do Scatter Spider a um cliente da Kroll, que a empresa conseguiu impedir.

O ataque começou com o agente da ameaça ligando para o helpdesk de TI do alvo, alegando ser um funcionário que foi bloqueado em sua conta.

Depois que a senha foi redefinida, o Scattered Spider procurou ignorar a autenticação multifator (MFA) do usuário usando "Fadiga de notificação por push" – bombardear os usuários com notificações push de celular até que o usuário aprove a solicitação por acidente ou interrompa as notificações.

Depois de obter acesso à conta, o invasor alterou rapidamente os dispositivos para os quais os códigos MFA são enviados.

A partir daí, a Scattered Spider agiu rapidamente para obter acesso a sistemas confidenciais na rede, aproveitando outras técnicas de engenharia social.

"Em alguns casos, em menos de uma hora eles passaram pelo SharePoint, eles capturaram informações muito importantes lá", observou Glass.

Nessa ocorrência específica, os atores obtiveram acesso a uma conta da Okta e usaram o Slack para spear phishing interno.

Isso levou o invasor a implantar uma ferramenta de acesso remoto e o trojan de acesso remoto AveMaria (RAT) para roubar mais credenciais. Glass observou que o Scattered Spider não implanta malware e outras ferramentas "até que seja absolutamente necessário".

Por meio desse processo, eles roubaram um token de login do LastPass, resultando no comprometimento de oito chaves de acesso secretas.

Nesse ponto, a Kroll conseguiu interromper o ataque antes que os agentes da ameaça obtivessem acesso ao sistema da vítima Isso provavelmente envolveria vasculhar o ambiente AWS da vítima em busca de buckets S3, exfiltrar informações confidenciais e implantar ransomware, de acordo com Glass.

Como se proteger contra ataques de aranhas espalhadas

Os especialistas estabelecem três áreas principais nas quais as organizações devem se concentrar para lidar com as técnicas usadas pelo Scatter Spider.

Proteção e resposta baseadas em identidade

Bill Sawyer, diretor administrativo da Kroll, observou que a identidade é a chave para a entrada da Scattered Spider nas organizações, com o objetivo de capturar senhas e MFA.

"Aplicando a proteção de identidade que eué mais maduro do que nome de usuário e senha é muito importante", disse Sawyer.

Isso inclui garantir que todos os aplicativos de software como serviço (SaaS) estejam conectados ao logon único (SSO).

Ele também recomendou que as organizações usem códigos MFA de correspondência de números, pois são mais difíceis de serem capturados pelos invasores.

A detecção e a resposta também estão fortemente ligadas à identidade. Por exemplo, as equipes de segurança devem garantir que sejam capazes de detectar rapidamente se um usuário está usando tokens de maneira incomum.

Atualize processos para lidar com a engenharia social

Sawyer também observou que a engenharia social é uma parte importante do manual da Scattered Spider – desde o uso de vishing para se passar por funcionários até o uso de canais internos do Slack para solicitar que os usuários façam coisas que normalmente não fariam.

Ele disse que era importante introduzir mais “atrito” nos processos para tentar lidar com essas técnicas. Isso pode incluir fazer com que os funcionários façam uma videochamada ou pessoalmente ao helpdesk de TI para solicitar uma redefinição de senha.

Gerenciamento de riscos de terceiros

Os ataques do Scattered Spider geralmente envolvem o direcionamento de fornecedores de tecnologia das vítimas, como SSO e outros provedores de identidade, para obter acesso aos sistemas.

Como resultado, as organizações devem garantir que estão trabalhando de forma eficaz com seus fornecedores no combate a quaisquer ataques de terceiros.

Falando com *Segurança da informação* durante o Gartner Summit, Debbie Janeczek, diretora global de segurança da informação do ING, enfatizou a necessidade de ter um relacionamento próximo com os fornecedores para ser rapidamente alertado sobre qualquer possível incidente.

“Tenho fornecedores que me enviam mensagens de texto e dizem ‘ei, verifique seu e-mail, fomos violados e é assim que isso afeta você’. Se você não tiver essa parceria, não receberá a bandeira imediata de que precisa olhar para algo”, explicou ela.

Janeczek também aconselhou as empresas a monitorar de perto os incidentes divulgados que afetam outras organizações, entendendo as táticas empregadas e atualizando as defesas de acordo.

“Você tem que observar as táticas, técnicas e procedimentos (TTPs) por si mesmo”, observou ela.