Descoberta mais uma operação de ciberespionagem mundial
Lucian Constantin

Campanha SafeNet infectou computadores pertencentes a empresas, governos e outras organizações de mais de 100 países, diz a Trend Micro

Pesquisadores de segurança da Trend Micro identificaram uma operação de ciberespionagem ativa que, até agora, comprometeu computadores pertencentes a órgãos governamentais, empresas de tecnologia, meios de comunicação, instituições de pesquisas acadêmicas e ONGs de mais de 100 países.

A operação, que a Trend Micro apelidou de SafeNet, atinge potenciais vítimas usando e-mails phishing com anexos maliciosos. Os pesquisadores da empresa publicaram uma pesquisa.

A investigação mostrou dois conjuntos de servidores de comando e controle (C&C) usados para o que parecem ser duas campanhas de ataque distintas, que possuem diferentes alvos - mas usam o mesmo malware.

Uma das campanhas usa e-mails phishing com conteúdo relacionado ao Tibete e à Mongólia. As mensagens contêm anexos ".doc", que exploram uma vulnerabilidade do Word corrigida pela Microsoft em abril de 2012.

Logs de acesso coletados a partir desta campanha revelaram um total de 243 endereços IP únicos de vítimas de 11 países diferentes. No entanto, os pesquisadores descobriram que apenas três vítimas ainda estavam ativas no momento da investigação com endereços IP da Mongólia e do Sudão.

Os servidores C&C correspondentes à segunda campanha de ataques registraram 11 563 endereços IP únicos de 116 países diferentes, mas o número real de vítimas é provavelmente bem menor, disseram os pesquisadores. Em média, 71 vítimas estavam se comunicando ativamente com este conjunto de servidores, em determinado momento durante a investigação, disseram.

Os e-mails utilizados na segunda campanha de ataque não foram identificados, mas o golpe parece ser maior em alcance e as vítimas mais amplamente dispersas - geograficamente falando. Os cinco principais países por contagem de endereços de IP de vítimas são a Índia, EUA, China, Paquistão, Filipinas e Rússia.

O malware instalado nos computadores comprometidos foi projetado principalmente para roubar informações, mas sua funcionalidade pode ser melhorada com módulos adicionais.

Os pesquisadores descobriram componentes com propósitos especiais nos servidores de comando e controle, bem como programas que podem ser usados para extrair as senhas salvas do Internet Explorer e Firefox, e também credenciais do Remote Desktop Protocol armazenados no Windows.

"Enquanto determinar a intenção e a identidade dos crackers permanece difícil, determinamos que a campanha SafeNet é direcionada e utiliza o malware desenvolvido por um engenheiro de software profissional que pode estar conectado a cibercriminosos na China", disseram os pesquisadores. "Este indivíduo estudou em uma universidade técnica de destaque no mesmo país e parece ter acesso ao repositório de código-fonte de uma empresa de serviços de Internet."

Os operadores dos servidores C&C acessaram eles com endereços IP de vários países, mas, na maioria das vezes, a partir da China e Hong Kong. "Vimos também o uso de VPNs e ferramentas de proxy, incluindo o Tor, o que contribuiu para a diversidade geográfica de endereços IP dos operadores.", afirmam.

Fonte: CIO [Portal]. Disponível em: <http://cio.uol.com.br/noticias/2013/05/20/descoberta-mais-uma-operacao-de-ciberespionagem-mundial/>. Acesso em: 21 maio 2013.