Talos

ANÁLISE DO ANO 2022

AMEAÇAS PERSISTENTES AVANÇADAS

BAIXE AQUI O RELATÓRIO COMPLETO EM INGLÊS

Ameaças persistentes avançadas (APTs) patrocinadas ou alinhadas pelo estado, adaptadas ao cenário geopolítico em constante mudança de 2022. O Cisco Talos observou várias campanhas cibernéticas ofensivas vinculadas a vários grupos para Rússia, Irã, China, Coreia do Norte e países do subcontinente indiano. Esses grupos se envolveram em diversas atividades mal-intencionadas, inclusive espionagem, roubo de propriedade intelectual e implantação de malware destrutivo. As principais tendências observadas incluem:

- Distribuir malware novo e personalizado e variantes atualizadas de malware já conhecido.
- Explorar vulnerabilidades conhecidas publicamente, como utilitários Log4j.
- Atualizar ferramentas e padrões de comportamento para evitar a descoberta.
- Aumentar a atividade de APT nos engajamentos do nosso Cisco Talos Incident Response (CTIR), inclusive o grupo MuddyWater patrocinado pelo estado do Irã e várias APTs afiliadas à China.

Rússia

Os grupos patrocinados pelo estado mais ativos observados pelo Talos em 2022, especialmente antes que a Rússia invadisse a Ucrânia em fevereiro.

Fancy Bear

Uma unidade suspeita da agência de inteligência militar da Rússia, a Directorate of the General Staff (GRU).

- Usou táticas, técnicas e procedimentos (TTPs) semelhantes aos observados em "WhisperGate", um ataque de limpador destrutivo várias semanas antes da invasão.

Gamaredon

Há suspeitas de que seja uma equipe de agentes apoiados pelo governo russo na Crimeia.

- Lançou uma grande campanha de spear phishing criada para infectar usuários do governo ucraniano com malware de roubo de informações, para extrair dados confidenciais.

Turla

Origem russa, atribuída por alguns ao Federal Security Service (FSB) da Rússia.

- Continua engajado em operações altamente direcionadas contra entidades do setor público e privado em países da OTAN e estados pós-soviéticos usando watering holes, campanhas de spear phishing, técnicas de engenharia social, exploração de vulnerabilidades conhecidas e backdoors personalizados, como Crutch e Gazer.

Irã

Esses grupos realizam ataques cibernéticos em todo o mundo com o objetivo principal de roubar propriedade intelectual e coletar inteligência. Provavelmente, mantêm os meios técnicos para implantar ransomware e outros malwares destrutivos.

MuddyWater

De acordo com uma análise abrangente, acreditamos que MuddyWater consiste em vários subgrupos encarregados de atingir um país ou uma região específica.

- Embora cada subgrupo do MuddyWater use TTPs exclusivos para comprometer os alvos designados, eles também compartilham malware, ferramentas e procedimentos considerados eficazes em outras campanhas regionais.
- Este ano, o MuddyWater tentou comprometer as entidades do governo turco e instalou um novo implante chamado SloughRAT no Oriente Médio.
- De acordo com os engajamentos do CTIR, observamos uma infinidade de ferramentas de backdoor e pós-exploração em uso. Mesmo após a correção, encontramos a presença de backdoors adicionais na infraestrutura do servidor e o uso de Impacket para execução remota de serviço e execução de ferramentas de ataque.

© 2022 Cisco e/ou suas afiliadas. Todos os direitos reservados.

AMEAÇAS PERSISTENTES AVANÇADAS

China

Os agentes de APT vinculados à China visaram entidades em uma ampla gama de setores, roubando propriedade intelectual e dados confidenciais dos principais mercados e setores de infraestrutura essenciais em alinhamento com os objetivos estratégicos da China.

Mustang Panda

Conhecido por explorar eventos atuais para comprometer as vítimas, especialmente localizadas nos EUA e na Ásia.

- Aproveitou a guerra entre Rússia e Ucrânia para atingir as empresas europeias, inclusive entidades russas, em uma campanha de espionagem generalizada.

Deep Panda

Um grupo de espionagem cibernética separado, patrocinado pelo estado, que visa governos, forças armadas, serviços de utilidade pública e entidades financeiras.

- Explorou a vulnerabilidade do Log4j para comprometer uma entidade de serviços de saúde, posteriormente implantando um backdoor personalizado para estabelecer persistência.

Coreia do Norte

O Talos observou a atividade prolífica dos agentes de ameaças vinculados ao governo da Coreia do Norte, especialmente o Lazarus Group, que apoia os objetivos políticos e de segurança nacional por meio de espionagem, roubo de dados e ataques disruptivos.

Lazarus Group

Conhecido por utilizar malware personalizado e se envolver em roubos monetários generalizados.

- Explorou as vulnerabilidades do Log4j em servidores VMware Horizon voltados para o público, visando as empresas de energia localizadas nos Estados Unidos, no Canadá e no Japão.
- O Talos descobriu um novo cavalo de Troia de acesso remoto, que chamamos de MagicRAT, bem como outros implantes personalizados usados para reconhecimento interno e roubo de dados.

Ásia Meridional

O Talos rastreou várias campanhas que visavam principalmente as entidades na Índia; a maioria parece vir de agentes vinculados ao estado no Paquistão, um adversário regional de longa data.

Transparent Tribe

- Visa predominantemente as entidades governamentais e militares, bem como as empresas afiliadas no Afeganistão e na Índia. O grupo começou a ter como alvo alunos e instituições educacionais na Índia, no que parece ser uma expansão da vitimologia padrão.

Bitter APT

- A espionagem parece ser o principal objetivo desse grupo. Em uma campanha de longa data, ele visou governos e entidades do Sul e do Leste Asiático nos setores de energia e engenharia.

Other APTs

- No início deste ano, o Talos publicou uma pesquisa sugerindo que vários agentes de APT que operam no sul da Ásia reutilizaram o código VBA gravado por diferentes grupos de ameaças, possivelmente de forma não intencional.

© 2022 Cisco e/ou suas afiliadas. Todos os direitos reservados.