Estudo de caso

A solução da Cisco protege antes, durante e depois de um ataque

Cisco Cloud Web Security Premium ajuda companhia de óleo e gás global a descobrir e solucionar uma infecção persistente por ransomware.

Desafios

Manter o conteúdo em segurança nunca foi tarefa tão difícil. Estamos em uma era na qual o roubo ou o comprometimento dos dados é frequentemente o principal estímulo para um ataque. Segundo o Relatório Anual de Segurança da Cisco de 2014, nossos pesquisadores descobriram que 100% das redes empresariais analisadas direcionavam o tráfego para sites que hospedam malware.[1] Ao observarem essa atividade, eles também concluíram que quando essas redes foram invadidas, provavelmente já estavam comprometidas há algum tempo e a infiltração central não havia sido detectada.[2]

Os seguintes fatores dificultam a prevenção e a detecção de ameaças pela equipe de segurança:

- **A mobilidade e a nuvem**, sem medidas de segurança adequadas, reduzem a visibilidade e aumentam a complexidade da segurança. À medida que mais empresas adotarem a computação em nuvem, virtualização, trabalho móvel e remoto e a tendência de Consumerização de TI, cada vez mais dados estão migrando para fora do controle corporativo. A rede está se tornando mais porosa, criando assim mais vetores de ataque. E à medida que mais serviços importantes para a empresa forem transferidos para a nuvem e acessados fora do perímetro seguro, a superfície de ataque continuará a aumentando.
- **Os invasores**, segundo o *Relatório de Segurança Anual da Cisco de 2014,* "estão trabalhando de forma proativa para compreender que tipo de solução de segurança está sendo implantada para poderem optar por padrões de comportamento menos perceptíveis, com conteúdo menos detectável, de forma que as ameaças fiquem bem disfarçadas."[3] Essa estratégia significa que as ameaças não são mais tão facilmente detectadas pelas soluções e pelos profissionais de segurança, e as empresas terão de enfrentar um tráfego mais codificado e criptografado, e maior randomização por parte dos agentes mal-intencionados, que buscam tornar a conduta de comando e controle (C&C) indistinguível do tráfego real".[4]

PERFIL DO CLIENTE

Setor: óleo e gás

Funcionários: aproximadamente 15.000

Operações: globais

Equipe de segurança: 12 pessoas

Outras medidas de segurança: Antivírus, Firewall, Intrusion Detection System (IDS), Security Information and Event Management (SIEM)

DESAFIO

- Detectar ameaças avançadas que entram por meio do tráfego na Web, e podem ultrapassar as barreiras de soluções de segurança desatualizadas e se incorporarem à rede corporativa.
- Desenvolver uma inteligência reativa para ajudar a equipe de segurança a priorizar as ameaças.
- Identificar uma solução única que possa ser implantada em todo o ambiente distribuído e se integre à infraestrutura de segurança atual para oferecer proteção em todo o ciclo do ataque.

SOLUÇÃO

- O Cisco CWS Premium, que inclui todos os recursos do Cisco CWS Essentials
- Cognitive Threat Analytics (CTA) e Advanced Malware Protection (AMP) para automatizar a pesquisa de ameaças de alto risco no tráfego da Web e oferecer visibilidade dos ataques avançados em atividade na rede corporativa.

RESULTADOS

- Infecção por malware persistente, e não descoberta anteriormente, identificada e resolvida
- A proteção contra ameaças agora está em todo o ciclo do ataque
- A equipe de segurança do cliente agora pode se concentrar no combate às ameaças mais relevantes.

[1] *Relatório de Segurança Anual da Cisco de 2014*. http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibid.
[3] Ibid.
[4] Ibid.

No dinâmico e complexo cenário das ameaças, a abordagem mais moderna de segurança de conteúdo é a da descoberta, o que é ainda mais importante do que a própria defesa. As empresas devem se concentrar na inspeção de conteúdo, na detecção de anomalias e na análise avançada para saber quais ameaças já encontram-se presentes na rede — a chamada fase "posterior" de um ataque.

Figura 1. Novo modelo de segurança: segurança contínua após o ataque

O Cisco® Cloud Web Security (CWS) Premium ajuda as empresas a enfrentarem o desafio de manter a segurança contínua em toda a extensão da rede. A plataforma Cisco CWS é uma versão na nuvem do Cisco Web Security e estende a segurança na Web para dispositivos móveis e ambientes distribuídos. Ela protege todos os usuários com a inteligência contra ameaças global da Cisco, recursos avançados de defesa e proteção do usuário em roaming. Inclui todos os recursos do Cisco CWS Essentials, mas também combina dois sistemas inovadores de detecção de malware para automatizar a pesquisa de ameaças de alto risco no tráfego da Web:

- **O Cognitive Threat Analytics (CTA)** é um sistema de análise de comportamento da rede em tempo quase real, que usa a aprendizagem automática e estatísticas avançadas para identificar alguma atividade incomum na rede — indicadores de comprometimento (IOCs). O CTA identifica anomalias e direciona os analistas de segurança para os possíveis problemas, ajudando-os a reduzir a carga de trabalho e a priorizarem as ameaças.
- **O Advanced Malware Protection (AMP)** usa uma combinação de reputação, sandbox e análise retrospectiva dos arquivos para identificar e bloquear ameaças no ciclo do ataque.

A combinação dessas soluções ajuda o CWS Premium a identificar novos canais de comando e controle não detectados anteriormente pelo setor de segurança

Este estudo de caso examina como o CWS Premium ajudou uma companhia global de óleo e gás a:

- Obter maior visibilidade sobre um grande e crescente volume de tráfego na Web (mais de 35 milhões de solicitações HTTP/HTTPs por dia).
- Gerar informações práticas que facilitem que sua equipe priorize as respostas à ameaça.
- Implantar uma solução única que se integre à sua infraestrutura atual de segurança, além de oferecer proteção durante todo o ciclo do ataque — antes, durante e depois.

Solução

A Cisco recomenda que o cliente atualize sua solução para o CWS Premium, que inclui o CTA e o AMP, com o objetivo de obter maior visibilidade da rede e assim poder ajudar a equipe de segurança a priorizar as respostas às ameaças.

A análise retrospectiva do AMP pode revelar que um arquivo considerado “limpo” por ter passado pelas proteções de perímetro é, na realidade, um malware avançado bem disfarçado. O AMP imediatamente alerta o administrador de segurança e identifica qual usuário pode ter sido contaminado e quando isso ocorreu.

Enquanto isso, o CTA detecta ameaças ainda mais disfarçadas que derrubam as defesas e estão ativas na rede corporativa. É um sistema inovador de detecção de malware que usa a análise comportamental e a detecção de anomalias para localizar dispositivos comprometidos. O CTA conta com modelagem estatística avançada e aprendizagem automática para identificar novas ameaças de forma autônoma, aprendendo com o que observa e se adaptando no decorrer do tempo, sem necessidade de ajuste ou configuração.

O CTA identificou e relatou evidências de atividades de malware na rede do cliente. O malware consistia em um conjunto de módulos controlados por uma entidade de malware. Nesse caso, o payload foi o ransomware Cryptolocker, um tipo de malware que criptografa os arquivos nos computadores das vítimas e "trava" o dispositivo até que um resgate seja pago.[5]

Conforme ilustrado na Figura 2, o invasor operou uma infraestrutura de comando e controle para realizar o ataque. Quatro etapas fundamentais estavam envolvidas nessa campanha:

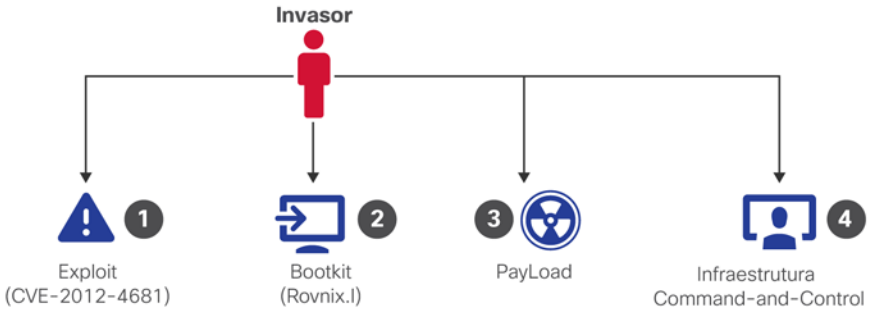
Passo 1. O invasor usou um exploit (CVE-2012-4681) para tirar proveito da vulnerabilidade no componente Java Runtime Environment (JRE) no Oracle Java SE 7, Atualização 6. Isso permitiu que ele executasse um código remotamente, ignorando o gerenciador de segurança.

Passo 2. Em seguida, o bootkit (Rovnix.l) foi instalado para garantir a persistência na máquina.

Passo 3. Em seguida, o payload foi fornecido, tornando o malware totalmente operacional. (Nesse caso, o payload foi o ransomware Cryptolocker.)

Passo 4. O ataque estabeleceu canais de comando e controle para manter a operação ativa.

Figura 2. Quatro etapas fundamentais no ataque

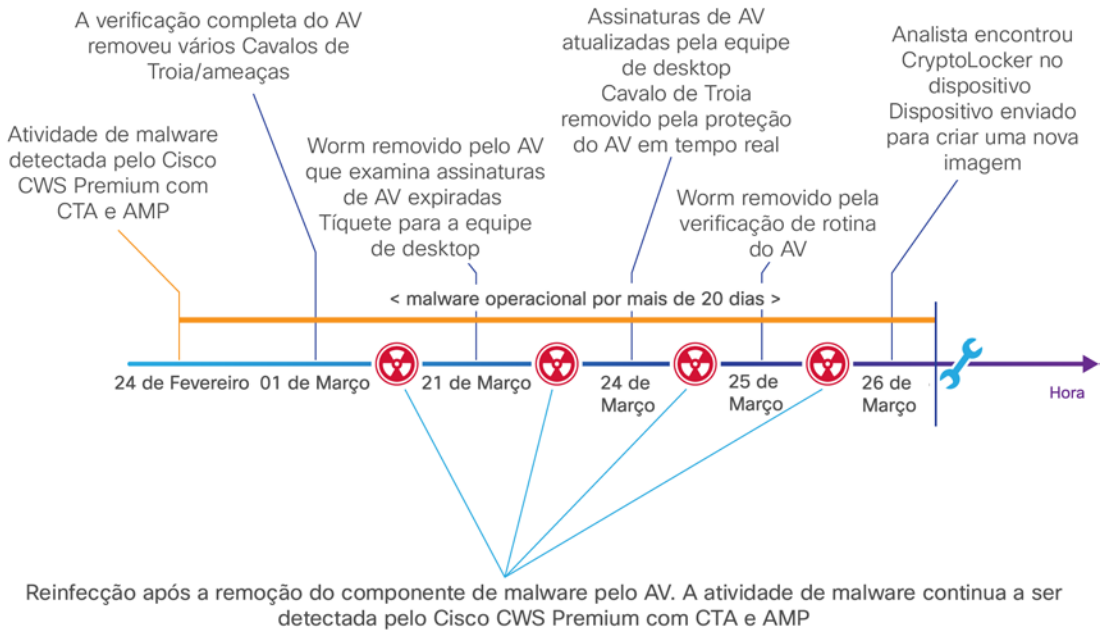


[5] A chamada Malvertising, a publicidade online que espalha malware, teve uma participação importante na disseminação do Cryptolocker, que foi neutralizado. O malvertising e o ransomware ainda são as principais ameaças e estão sendo usadas pelos invasores para lançar campanhas direcionadas por meio da Web. Para obter mais detalhes, consulte o Relatório Semestral de Segurança da Cisco de 2014 : http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf.

A equipe de segurança do cliente tentou solucionar as ameaças com ferramentas de AV. Entretanto, como a infecção foi no rootkit, o malware estava totalmente integrado ao sistema infectado. A solução de AV foi capaz de eliminar somente alguns componentes de malware. Até que a infecção tivesse sido completamente eliminada, o CTA continuou a alertar a equipe de segurança sobre a presença de atividade mal-intencionada persistente.

A Figura 3 mostra o cronograma completo desde a detecção de atividade de malware até a eliminação da ameaça.

Figura 3. Cronograma de atividades de malware: da detecção até a eliminação



A situação vivida pelo cliente demonstra a importância da operação do CWS Premium na fase "posterior" a um ataque. O exemplo também ajudou a ressaltar por que é difícil mitigar ataques avançados com produtos de AV. O sistema CTA forneceu evidências dos canais de comando e controle ativos e contínuos. Além disso, identificou vários outros domínios usados na extração dos dados. Tais infecções representam violações de longo prazo encobertas na infraestrutura do cliente.

Resultados

No mundo atual, em que as equipes de segurança precisam gerenciar um alto volume de incidentes diariamente, não há tempo para ficar procurarando "uma agulha no palheiro". As equipes de segurança precisam de ajuda para se concentrar nos ataques mais avançados, que são detectados e categorizados pelo sistema de CTA.

No caso da infecção da rede do cliente por ransomware Cryptolocker, o CWS Premium detectou a atividade de malware e aplicou a inteligência de segurança atual para bloquear alguns canais de comando e controle alvos do dispositivo infectado. No entanto, o invasor usou um endereço IP adicional com reputação desconhecida, e esse novo canal estava ativo durante toda a infecção. Esse exemplo ressalta os pontos positivos (bloqueio automático) e negativos (novos canais não são bloqueados) de se confiar somente nas detecções baseadas em assinatura e na reputação, e o motivo pelo qual é necessária a proteção contínua após um ataque.

A seguir, veja uma análise dos canais de comando e controle identificados pelo sistema CTA no CSW Premium, bem como exemplos de solicitações e estatísticas de tráfego na web:

Tabela 1. Infraestrutura de ataque

Pedido	Servidor remoto	IP de destino	País de destino:	Número de solicitações	Status da atividade
1	Servidor nº1 de C&C	109.XXX.XXX.XXX	Holanda	17 (tentativas)	BLOQUEADO pelo Web Reputation
2	**Servidor nº2 de C&C**	**94.XXX.XXX.XXX**	**Luxemburgo**	**75**	**ACTIVE CHANNEL**
3	Servidor nº3 de C&C	fistristy.com	Luxemburgo	175 (tentativas)	BLOQUEADO pelo Web Reputation
4	Servidor nº4 de C&C	ffeed5.com	Rússia	7 (tentativas)	BLOQUEADO pelo Web Reputation

Tabela 2. Ameaças identificadas pelo CTA que foram posteriormente removidas do dispositivo

Nome da ameaça	Removido
Cridex Worm	19 de março
Worm Cridex.E	19 de março
Cavalo de Troia Tesch.B	19 de março
Java Exploit/CVE-2012-4681	19 de março
Trojan Downloader Win32/Upatre	19 de março
Worm Cridex	21 de março
Trojan Win32/Viknok.C	24 de março
Worm Cridex	24 de março
Defesa por criptografia	26 de março

Comunicação com o Servidor nº1 de C&C (109.XXX.XXX.XXX)

Características da comunicação:

- Total de 17 tentativas de solicitação no servidor, todas foram de comunicação de C&C e bloqueadas por reputação.
- As solicitações foram detectadas pelo CTA como tentativas de usar a string URL como o canal de comunicação (C&C). A URL (mostrada abaixo em "Exemplo de solicitação de HTTP ") representa uma mensagem codificada. A estrutura similar da URL (endereço IP /m/IbQ.*) foi compartilhada por várias URLs usadas nesse ataque. O fato de a comunicação ter sido bloqueada pelo sistema de reputação agrega ainda mais evidência contextual.
- O invasor também estabelece um segundo canal de C&C em um servidor que ainda não faz parte dos feeds de reputação, para garantir que o malware permaneça ativo. A URL propriamente dita é uma mensagem codificada.

Exemplo de solicitação de HTTP (anônima e truncada)

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…

Comunicação com o Servidor nº2 de C&C (94.XXX.XXX.XXX)

Características da comunicação:

- Total de 17 tentativas de solicitação no servidor, todas foram solicitações de C&C.
- Duas tentativas de C&C foram detectadas pelo CTA como **tráfego HTTP ao endereço IP (nenhum domínio especificado)**. Essa categoria de comportamento identifica as solicitações incomuns que representam uma comunicação fora de sequência para um endereço IP puro. Essa atividade pode ser executada pelo malware como verificação "permanente" para confirmar se ele ainda está ativo ou simplesmente extrair e receber instruções adicionais da infraestrutura mal-intencionada (C&C). Esse tipo de tráfego não é criado pela navegação normal na Internet.
- Todas as 75 solicitações de C&C não foram detectadas por tecnologias baseadas em assinatura e reputação.

Exemplo de solicitação de HTTP (anônima e truncada)

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

Comunicação com o Servidor nº3 de C&C (fistristy.com)

Características da comunicação:

- Total de 175 solicitações ao domínio fistristy.com, todas foram de comunicação de C&C.
- As tecnologias baseadas em assinatura e reputação bloquearam todas as solicitações.

Exemplo de solicitação de HTTP

hXXp://fistristy.com/aa/

Comunicação com o Servidor nº4 de C&C (ffeed5.com)

Características da comunicação:

- Total de 7 solicitações ao ffeed5.com, todas foram comunicação de C&C bloqueadas pelo CSW Premium.
- O CTA detectou 6 solicitações como **Tráfego HTTP anormal**. Essa categoria inclui o comportamento de malware que normalmente não se enquadra na linha de base comportamental estabelecida pela análise contínua de CTA. O termo “linha de base” indica o estado dos modelos estatísticos criados pelo sistema de CTA, que “aprendem” as tendências e as características do tráfego da Web analisado. O CTA ajusta automaticamente a linha de base durante a mudança de rede (por exemplo, dia e noite) para oferecer os melhores resultados de detecção.
- O CTA usa modelagem de longo prazo do comportamento da rede para correlacionar atividades aparentemente diferentes. Em seguida, ele compara esses dados com os comportamentos de cada usuário em toda a rede do cliente para melhorar os recursos de descoberta de ameaças disfarçadas e persistentes.

Exemplo de solicitação de HTTP

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

Conclusão

A equipe de segurança do cliente precisava de uma forma mais fácil de monitorar a atividade e priorizar os eventos de segurança em uma rede com mais de 15.000 usuários e gerando, em média, mais de 35 milhões de transações por dia na Web. O cliente também precisava de uma solução para bloquear ameaças, além de identificar com rapidez as que inevitavelmente não são detectadas por outras defesas. O cliente precisava de uma tecnologia desenvolvida para alertar a equipe de segurança em relação à presença de atividade suspeita persistente, até que a ameaça fosse totalmente eliminada.

Ao implantar o CTA, como parte do Cisco CWS Premium, o cliente agora tem um sistema de análise do comportamento da rede em tempo quase real, que usa a aprendizagem automática e estatísticas avançadas para detectar IOCs na rede. No exemplo da infecção do ransomware Cryptolocker, o CTA continuou a alertar sobre a presença de atividade mal-intencionada até que a equipe de segurança resolvesse completamente a infecção. Além disso, a percepção do comportamento do malware proporcionada pelo CTA permite à equipe de segurança concentrar-se somente nas ameaças mais importantes, antes, durante e depois de um ataque.

Saiba mais

O Cisco CWS Premium, que inclui o CTA e o AMP, integra-se à estratégia da Cisco de ajudar as empresas a solucionarem desafios de segurança conhecidos e novos, ajudando-as a detectar, compreender e deter ameaças por meio de análise contínua e informações de segurança em tempo real, fornecidas pela nuvem e compartilhadas por todas as soluções de segurança visando mais eficiência. A combinação dessas três soluções permite que o CWS Premium identifique novos canais de comando e controle não detectados anteriormente pelo setor de segurança, e ajude empresas a enfrentarem os desafios em todo o ciclo do ataque.

Para obter mais informações sobre o CWS Premium, acesse http://www.cisco.com/go/cws.

Para obter mais informações sobre o CTA, acesse http://www.cisco.com/go/cognitive.

Para obter mais detalhes sobre o AMP, acesse http://www.cisco.com/go/amp.

Sede - América
Cisco Systems. Inc.
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pte. Ltda.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam.
Holanda

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefone e de fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos EUA C36-733153-00 10/14