Vault 7: Ferramentas de hacking da CIA reveladas

Conteúdo

Comunicado de imprensa

Hoje, terça-feira, 7 de março de 2017, o WikiLeaks inicia sua nova série de vazamentos sobre a Agência Central de Inteligência dos EUA. Com o codinome "Vault 7" pelo WikiLeaks, trata-se da maior publicação de documentos confidenciais sobre a agência.

A primeira parte completa da série, "Ano Zero", abrange 8.761 documentos e arquivos de uma rede isolada e de alta segurança, localizada dentro do Centro de Inteligência Cibernética da CIA em Langley, Virgínia. A série segue uma divulgação introdutória, no mês passado, de que a CIA estava mirando partidos políticos e candidatos franceses na preparação para as eleições presidenciais de 2012 .

Recentemente, a CIA perdeu o controle da maior parte de seu arsenal de hackers, incluindo malware, vírus, trojans, exploits de "dia zero" como armas, sistemas de controle remoto de malware e documentação associada. Essa coleção extraordinária, que soma mais de várias centenas de milhões de linhas de código, confere ao seu detentor toda a capacidade de hacking da CIA. O arquivo parece ter circulado entre ex-hackers e contratados do governo dos EUA de forma não autorizada, um dos quais forneceu partes do arquivo ao WikiLeaks.

"Ano Zero" apresenta o escopo e a direção do programa global de hacking secreto da CIA, seu arsenal de malware e dezenas de explorações de armas de "dia zero" contra uma ampla gama de produtos de empresas dos EUA e da Europa, incluindo o iPhone da Apple, o Android do Google e o Windows da Microsoft e até mesmo TVs Samsung, que são transformadas em microfones secretos.

Desde 2001, a CIA conquistou preeminência política e orçamentária sobre a Agência de Segurança Nacional (NSA) dos EUA. A CIA se viu construindo não apenas sua agora infame frota de drones, mas também um tipo muito diferente de força secreta, com alcance global — sua própria frota substancial de hackers. A divisão de hackers da agência a liberou da necessidade de revelar suas operações, muitas vezes controversas, à NSA (sua principal rival burocrática) para poder recorrer às capacidades de hacking da NSA.

No final de 2016, a divisão de hackers da CIA, que formalmente está subordinada ao Centro de Inteligência Cibernética (CCI) da agência, contava com mais de 5.000 usuários registrados e havia produzido mais de mil sistemas de hackers, trojans, vírus e outros malwares "armamentados". A escala do empreendimento da CIA é tamanha que, até 2016, seus hackers haviam utilizado mais código do que o usado para administrar o Facebook. A CIA havia criado, na prática, sua "própria NSA", com ainda menos responsabilidade e sem responder publicamente à questão de se um gasto orçamentário tão vultoso na duplicação das capacidades de uma agência rival poderia ser justificado.

Em declaração ao WikiLeaks, a fonte detalha questões políticas que, segundo ela, precisam ser debatidas urgentemente em público, incluindo se as capacidades de hacking da CIA excedem seus poderes e o problema da supervisão pública da agência. A fonte deseja iniciar um debate público sobre a segurança, criação, uso, proliferação e controle democrático de armas cibernéticas.

Uma vez que uma única "arma" cibernética é "solta", ela pode se espalhar pelo mundo em segundos, para ser usada por estados rivais, máfia cibernética e hackers adolescentes.

Julian Assange, editor do WikiLeaks, afirmou que "Há um risco extremo de proliferação no desenvolvimento de 'armas' cibernéticas. É possível fazer comparações entre a proliferação descontrolada dessas 'armas', resultante da incapacidade de contê-las, aliada ao seu alto valor de mercado, e o comércio global de armas. Mas a importância do "Ano Zero" vai muito além da escolha entre a guerra cibernética e a paz cibernética. A divulgação também é excepcional de uma perspectiva política, jurídica e forense."

O Wikileaks revisou cuidadosamente a divulgação do "Ano Zero" e publicou documentação substancial da CIA, evitando a distribuição de armas cibernéticas "armadas" até que um consenso surja sobre a natureza técnica e política do programa da CIA e como tais "armas" devem ser analisadas, desarmadas e publicadas.

O Wikileaks também decidiu redigir e tornar anônimas algumas informações de identificação no "Ano Zero" para uma análise aprofundada. Essas redações incluem dezenas de milhares de alvos e máquinas de ataque da CIA em toda a América Latina, Europa e Estados Unidos. Embora estejamos cientes dos resultados imperfeitos de qualquer abordagem escolhida, permanecemos comprometidos com nosso modelo de publicação e observamos que a quantidade de páginas publicadas na primeira parte do "Vault 7" ("Ano Zero") já supera o número total de páginas publicadas nos três primeiros anos dos vazamentos da NSA de Edward Snowden.

Análise

Malware da CIA tem como alvo iPhone, Android e TVs inteligentes

As ferramentas de malware e hacking da CIA são desenvolvidas pelo EDG (Grupo de Desenvolvimento de Engenharia), um grupo de desenvolvimento de software dentro do CCI (Centro de Inteligência Cibernética), um departamento pertencente à DDI (Diretoria de Inovação Digital) da CIA. A DDI é uma das cinco principais diretorias da CIA (veja este organograma da CIA para mais detalhes).

O EDG é responsável pelo desenvolvimento, teste e suporte operacional de todos os backdoors, exploits, payloads maliciosos, trojans, vírus e qualquer outro tipo de malware usado pela CIA em suas operações secretas em todo o mundo.

A crescente sofisticação das técnicas de vigilância atraiu comparações com 1984, de George Orwell, mas "Weeping Angel", desenvolvido pelo Embedded Devices Branch (EDB) da CIA , que infesta TVs inteligentes, transformando-as em microfones secretos, é certamente sua realização mais emblemática.

O ataque contra smart TVs da Samsung foi desenvolvido em cooperação com o MI5/BTSS do Reino Unido. Após a infestação, o Weeping Angel coloca a TV alvo em um modo "Falso Desligamento", para que o proprietário acredite falsamente que a TV está desligada quando ela está ligada. No modo "Falso Desligamento", a TV funciona como um grampo, gravando conversas na sala e enviando-as pela internet para um servidor secreto da CIA.

Em outubro de 2014, a CIA também estava considerando infectar os sistemas de controle de veículos usados por carros e caminhões modernos . O propósito desse controle não é especificado, mas permitiria à CIA realizar assassinatos quase indetectáveis.

A Divisão de Dispositivos Móveis (MDB) da CIA desenvolveu inúmeros ataques para hackear e controlar remotamente smartphones populares . Os celulares infectados podem ser instruídos a enviar à CIA a geolocalização, comunicações de áudio e texto do usuário, além de ativar secretamente a câmera e o microfone do aparelho.

Apesar da participação minoritária do iPhone (14,5%) no mercado global de smartphones em 2016, uma unidade especializada na Divisão de Desenvolvimento Móvel da CIA produz malware para infestar, controlar e extrair dados de iPhones e outros produtos Apple com iOS, como iPads . O arsenal da CIA inclui inúmeros "dias zero" locais e remotos , desenvolvidos pela CIA ou obtidos do GCHQ, NSA, FBI ou comprados de empresas de armas cibernéticas como a Baitshop. O foco desproporcional no iOS pode ser explicado pela popularidade do iPhone entre as elites sociais, políticas, diplomáticas e empresariais.

Uma unidade semelhante tem como alvo o Android, do Google, usado na maioria dos smartphones do mundo (~85%), incluindo Samsung, HTC e Sony . 1,15 bilhão de celulares Android foram vendidos no ano passado. "Ano Zero" mostra que, em 2016, a CIA tinha 24 Androids "dias zero" "armamentados" , desenvolvidos por ela mesma e obtidos do GCHQ, da NSA e de empresas de armas cibernéticas.

Essas técnicas permitem que a CIA ignore a criptografia do WhatsApp, Signal, Telegram, Wiebo, Confide e Cloackman, hackeando os telefones "inteligentes" em que eles operam e coletando tráfego de áudio e mensagens antes que a criptografia seja aplicada.

Malware da CIA tem como alvo Windows, OSx, Linux e roteadores

A CIA também realiza um esforço substancial para infectar e controlar usuários do Microsoft Windows com seu malware. Isso inclui múltiplas armas locais e remotas de "dia zero", vírus que saltam por lacunas de ar, como o "Hammer Drill" , que infecta softwares distribuídos em CDs/DVDs, infectadores para mídias removíveis, como USBs , sistemas para ocultar dados em imagens ou em áreas secretas de disco ("Brutal Kangaroo") e para manter suas infestações de malware em andamento .

Muitos desses esforços de infecção são reunidos pelo Automated Implant Branch (AIB) da CIA , que desenvolveu vários sistemas de ataque para infestação e controle automatizados de malware da CIA, como "Assassin" e "Medusa".

Ataques contra infraestrutura de Internet e servidores web são desenvolvidos pelo Network Devices Branch (NDB) da CIA .

A CIA desenvolveu sistemas automatizados de controle e ataque de malware multiplataforma que abrangem Windows, Mac OS X, Solaris, Linux e mais, como o "HIVE" da EDB e as ferramentas relacionadas "Cutthroat" e "Swindle", que são descritas na seção de exemplos abaixo .

A CIA "acumulou" vulnerabilidades ("dias zero")

Após os vazamentos de Edward Snowden sobre a NSA, a indústria de tecnologia dos EUA garantiu um compromisso do governo Obama de que o executivo divulgaria continuamente — em vez de acumular — vulnerabilidades graves, explorações, bugs ou "dias zero" para a Apple, Google, Microsoft e outros fabricantes sediados nos EUA.

Vulnerabilidades graves não divulgadas aos fabricantes colocam grandes parcelas da população e de infraestruturas críticas em risco para a inteligência estrangeira ou para criminosos cibernéticos que, independentemente, descobrem ou ouvem rumores sobre a vulnerabilidade. Se a CIA consegue descobrir tais vulnerabilidades, outros também conseguem.

O compromisso do governo dos EUA com o Processo de Equidades em Vulnerabilidades surgiu após um lobby significativo de empresas de tecnologia americanas, que correm o risco de perder sua fatia do mercado global devido a vulnerabilidades ocultas, reais e percebidas. O governo declarou que divulgaria continuamente todas as vulnerabilidades disseminadas descobertas após 2010.

Documentos do "Ano Zero" demonstram que a CIA violou os compromissos do governo Obama. Muitas das vulnerabilidades utilizadas no arsenal cibernético da CIA são generalizadas e algumas podem já ter sido descobertas por agências de inteligência rivais ou criminosos cibernéticos.

Por exemplo, um malware específico da CIA, revelado em "Ano Zero", é capaz de penetrar, infestar e controlar o software do telefone Android e do iPhone que administra ou administrou as contas presidenciais do Twitter. A CIA ataca esse software usando vulnerabilidades de segurança não divulgadas ("dias zero"), de propriedade da CIA, mas se a CIA consegue hackear esses telefones, todos os outros que obtiveram ou descobriram a vulnerabilidade também podem. Enquanto a CIA mantiver essas vulnerabilidades ocultas da Apple e do Google (que fabricam os telefones), elas não serão corrigidas e os telefones continuarão vulneráveis a hackers.

As mesmas vulnerabilidades existem para a população em geral, incluindo o Gabinete dos EUA, o Congresso, os principais CEOs, administradores de sistemas, agentes de segurança e engenheiros. Ao ocultar essas falhas de segurança de fabricantes como Apple e Google, a CIA garante que pode hackear qualquer pessoa — ao custo de deixar todos vulneráveis a hackers.

Programas de “guerra cibernética” representam um sério risco de proliferação

Não é possível manter 'armas' cibernéticas sob controle efetivo.

Embora a proliferação nuclear tenha sido restringida pelos enormes custos e pela infraestrutura visível envolvida na reunião de material físsil suficiente para produzir uma massa nuclear crítica, as "armas" cibernéticas, uma vez desenvolvidas, são muito difíceis de manter.

As "armas" cibernéticas são, na verdade, apenas programas de computador que podem ser pirateados como qualquer outro. Como são compostos inteiramente de informações, podem ser copiados rapidamente, sem custo marginal.

Proteger essas "armas" é particularmente difícil, visto que as mesmas pessoas que as desenvolvem e utilizam têm a habilidade de extrair cópias sem deixar rastros — às vezes, usando as mesmas "armas" contra as organizações que as contêm. Há incentivos de preço substanciais para que hackers e consultores governamentais obtenham cópias, visto que existe um "mercado de vulnerabilidades" global que pagará centenas de milhares a milhões de dólares por cópias dessas "armas". Da mesma forma, contratantes e empresas que obtêm essas "armas" às vezes as utilizam para seus próprios fins, obtendo vantagem sobre seus concorrentes na venda de serviços de "hacking".

Nos últimos três anos, o setor de inteligência dos Estados Unidos, que consiste em agências governamentais como a CIA e a NSA e seus contratados, como a Booz Allan Hamilton, tem sido sujeito a uma série sem precedentes de exfiltrações de dados por seus próprios funcionários.

Vários membros da comunidade de inteligência ainda não identificados publicamente foram presos ou sujeitos a investigações criminais federais em incidentes separados.

Mais visivelmente, em 8 de fevereiro de 2017, um grande júri federal dos EUA indiciou Harold T. Martin III com 20 acusações de manuseio indevido de informações confidenciais. O Departamento de Justiça alegou ter apreendido cerca de 50.000 gigabytes de informações de Harold T. Martin III, obtidas por ele de programas confidenciais da NSA e da CIA, incluindo o código-fonte de diversas ferramentas de hacking.

Uma vez que uma única "arma" cibernética é "solta", ela pode se espalhar pelo mundo em segundos, para ser usada por estados pares, máfia cibernética e hackers adolescentes.

Consulado dos EUA em Frankfurt é uma base secreta de hackers da CIA

Além de suas operações em Langley, Virgínia, a CIA também usa o consulado dos EUA em Frankfurt como base secreta para seus hackers que cobrem a Europa, o Oriente Médio e a África.

Hackers da CIA que operam a partir do consulado de Frankfurt ("Centro de Inteligência Cibernética da Europa" ou CCIE) recebem passaportes diplomáticos ("pretos") e cobertura do Departamento de Estado. As instruções para os hackers da CIA que chegam fazem com que os esforços de contrainteligência da Alemanha pareçam inconsequentes: "Passe pela alfândega alemã sem maiores problemas porque você já tem sua história de encobrimento impecável, e tudo o que eles fizeram foi carimbar seu passaporte."

> *Sua matéria de capa (para esta viagem)*
> **P:** Por que você está aqui?
> **R:** Apoiando consultas técnicas no Consulado.

Duas publicações anteriores do WikiLeaks fornecem mais detalhes sobre as abordagens da CIA aos procedimentos alfandegários e de triagem secundária .

Uma vez em Frankfurt, os hackers da CIA podem viajar sem mais verificações de fronteira para os 25 países europeus que fazem parte da área de fronteira aberta de Shengen — incluindo França, Itália e Suíça.

Vários métodos de ataque eletrônico da CIA são projetados para proximidade física. Esses métodos de ataque são capazes de penetrar redes de alta segurança desconectadas da internet, como bancos de dados de registros policiais. Nesses casos, um agente, agente ou agente de inteligência aliado da CIA, agindo sob instruções, infiltra-se fisicamente no local de trabalho visado. O invasor recebe um USB contendo malware desenvolvido pela CIA para essa finalidade, que é inserido no computador visado. O invasor então infecta e exfiltra os dados para mídias removíveis. Por exemplo, o sistema de ataque da CIA, Fine Dining , fornece 24 aplicativos de isca para os espiões da CIA usarem. Para as testemunhas, o espião parece estar executando um programa que exibe vídeos (por exemplo, VLC), apresenta slides (Prezi), joga um jogo de computador (Breakout2, 2048) ou até mesmo executa um antivírus falso (Kaspersky, McAfee, Sophos). Mas enquanto o aplicativo de isca está na tela, o sistema subjacente é automaticamente infectado e saqueado.

Como a CIA aumentou drasticamente os riscos de proliferação

No que é certamente um dos mais impressionantes objetivos de inteligência da memória recente, a CIA estruturou seu regime de classificação de tal forma que, para a parte mais valiosa do "Vault 7" no mercado — o malware armado da CIA (implantes + zero dias), Postos de Escuta (LP) e sistemas de Comando e Controle (C2) — a agência tem poucos recursos legais.

A CIA tornou esses sistemas não classificados.

O motivo pelo qual a CIA decidiu tornar seu arsenal cibernético não classificado revela como os conceitos desenvolvidos para uso militar não cruzam facilmente o "campo de batalha" da "guerra" cibernética.

Para atacar seus alvos, a CIA geralmente exige que seus implantes se comuniquem com seus programas de controle pela internet. Se os implantes da CIA, os softwares de Comando e Controle e Postos de Escuta fossem classificados, os agentes da CIA poderiam ser processados ou demitidos por violar as regras que proíbem a publicação de informações confidenciais na internet. Consequentemente, a CIA tornou secretamente a maior parte de seu código de espionagem cibernética/guerra não classificado. O governo dos EUA também não pode reivindicar direitos autorais, devido a restrições na Constituição dos EUA. Isso significa que fabricantes de "armas" cibernéticas e hackers podem "piratear" livremente essas "armas" se elas forem obtidas. A CIA tem se baseado principalmente na ofuscação para proteger seus segredos de malware.

Armas convencionais, como mísseis, podem ser disparadas contra o inimigo (ou seja, em uma área desprotegida). A proximidade ou o impacto com o alvo detonam a munição, incluindo suas partes classificadas. Portanto, militares não violam as regras de classificação disparando munição com partes classificadas. A munição provavelmente explodirá. Se isso não acontecer, não é a intenção do operador.

Na última década, as operações de hacking nos EUA têm sido cada vez mais disfarçadas de jargão militar para aproveitar as fontes de financiamento do Departamento de Defesa. Por exemplo, tentativas de "injeções de malware" (jargão comercial) ou "implantação" (jargão da NSA) estão sendo chamadas de "disparos", como se uma arma estivesse sendo disparada. No entanto, a analogia é questionável.

Ao contrário de balas, bombas ou mísseis, a maioria dos malwares da CIA é projetada para sobreviver por dias ou até anos após atingir seu "alvo". O malware da CIA não "explode com o impacto", mas sim infesta seu alvo permanentemente. Para infectar o dispositivo do alvo, cópias do malware devem ser colocadas nos dispositivos do alvo, dando-lhe a posse física do malware. Para exfiltrar dados de volta para a CIA ou aguardar novas instruções, o malware deve se comunicar com os sistemas de Comando e Controle (C2) da CIA localizados em servidores conectados à internet. Mas esses servidores normalmente não são aprovados para armazenar informações confidenciais, portanto, os sistemas de comando e controle da CIA também são considerados não confidenciais.

Um "ataque" bem-sucedido ao sistema computacional de um alvo assemelha-se mais a uma série de manobras complexas de ações em uma oferta hostil de aquisição ou à disseminação cuidadosa de rumores para obter controle sobre a liderança de uma organização do que ao disparo de um sistema de armas. Se for possível fazer uma analogia militar, a infestação de um alvo talvez seja semelhante à execução de uma série de manobras militares contra o território do alvo, incluindo observação, infiltração, ocupação e exploração.

Fugindo da perícia forense e do antivírus

Uma série de padrões define padrões de infestação de malware da CIA que provavelmente ajudarão investigadores forenses de cenas de crime, bem como Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens e empresas de antivírus a atribuir e se defender contra ataques.

"Tradecraft DO's and DON'Ts" contém as regras da CIA sobre como seu malware deve ser escrito para evitar impressões digitais que impliquem a "CIA, o governo dos EUA ou suas empresas parceiras conscientes" em "análises forenses". Padrões secretos semelhantes abrangem o uso de criptografia para ocultar a comunicação entre hackers e malware da CIA (pdf), descrever alvos e dados exfiltrados (pdf), bem como executar payloads (pdf) e persistir (pdf) nas máquinas do alvo ao longo do tempo.

Hackers da CIA desenvolveram ataques bem-sucedidos contra a maioria dos programas antivírus conhecidos. Esses ataques estão documentados em " Derrotas de antivírus" , "Produtos de Segurança Pessoal" , "Detectando e derrotando PSPs" e "Evitando PSP/Depurador/RE" . Por exemplo, o Comodo foi derrotado por malware da CIA, que se colocou na "Lixeira" do Windows . Já o Comodo 6.x apresenta um "Buraco de DESTRUIÇÃO" .

Os hackers da CIA discutiram o que os hackers do "Equation Group" da NSA fizeram de errado e como os criadores de malware da CIA poderiam evitar exposição semelhante .

Exemplos

O sistema de gerenciamento do Grupo de Desenvolvimento de Engenharia (EDG) da CIA contém cerca de 500 projetos diferentes (dos quais apenas alguns são documentados pelo "Ano Zero"), cada um com seus próprios subprojetos, malware e ferramentas de hackers.

A maioria desses projetos se refere a ferramentas usadas para penetração, infestação ("implantação"), controle e exfiltração.

Outro ramo de desenvolvimento se concentra no desenvolvimento e operação de Postos de Escuta (LP) e sistemas de Comando e Controle (C2) usados para se comunicar e controlar implantes da CIA; projetos especiais são usados para atingir hardware específico, de roteadores a TVs inteligentes.

Alguns exemplos de projetos são descritos abaixo, mas veja o índice para a lista completa de projetos descritos pelo "Ano Zero" do WikiLeaks.

RESFRIAMENTO

As técnicas de hacking artesanais da CIA representam um problema para a agência. Cada técnica criada cria uma "impressão digital" que pode ser usada por investigadores forenses para atribuir vários ataques diferentes à mesma entidade.

Isso é análogo a encontrar o mesmo ferimento de faca característico em várias vítimas de assassinato. O estilo único de ferimento cria a suspeita de que um único assassino seja o responsável. Assim que um assassinato no conjunto é resolvido, os outros assassinatos também encontram atribuição provável.

O grupo UMBRAGE da Divisão de Dispositivos Remotos da CIA coleta e mantém uma biblioteca substancial de técnicas de ataque "roubadas" de malware produzido em outros estados, incluindo a Federação Russa.

Com o UMBRAGE e projetos relacionados, a CIA não só aumenta o número total de tipos de ataque, mas também desvia a atribuição, deixando para trás as "impressões digitais" dos grupos dos quais as técnicas de ataque foram roubadas.

Os componentes do UMBRAGE abrangem keyloggers, coleta de senhas, captura de webcam, destruição de dados, persistência, escalonamento de privilégios, furtividade, prevenção de antivírus (PSP) e técnicas de pesquisa.

Jantar requintado

O Fine Dining inclui um questionário padronizado, ou seja, um cardápio preenchido pelos agentes da CIA. O questionário é utilizado pelo OSB (Setor de Suporte Operacional) da agência para transformar as solicitações dos agentes em requisitos técnicos para ataques de hackers (tipicamente "exfiltração" de informações de sistemas de computador) para operações específicas. O questionário permite que o OSB identifique como adaptar as ferramentas existentes para a operação e comunique isso à equipe de configuração de malware da CIA. O OSB funciona como interface entre a equipe operacional da CIA e a equipe de suporte técnico relevante.

Entre a lista de possíveis alvos da coleta estão "Ativo", "Ativo de Ligação", "Administrador de Sistema", "Operações de Informação Estrangeira", "Agências de Inteligência Estrangeira" e "Entidades Governamentais Estrangeiras". Notavelmente ausente é qualquer referência a extremistas ou criminosos transnacionais. O "Oficial de Caso" também é solicitado a especificar o ambiente do alvo, como o tipo de computador, o sistema operacional utilizado, a conectividade com a Internet e os utilitários antivírus (PSPs) instalados, bem como uma lista de tipos de arquivo a serem exfiltrados, como documentos do Office, áudio, vídeo, imagens ou tipos de arquivo personalizados. O "menu" também solicita informações sobre a possibilidade de acesso recorrente ao alvo e por quanto tempo o acesso não observado ao computador pode ser mantido. Essas informações são usadas pelo software "JQJIMPROVISE" da CIA (veja abaixo) para configurar um conjunto de malware da CIA adequado às necessidades específicas de uma operação.

Improvise (JQJIMPROVISE)

"Improvise" é um conjunto de ferramentas para configuração, pós-processamento, configuração de carga útil e seleção de vetores de execução para ferramentas de levantamento/exfiltração, compatível com todos os principais sistemas operacionais, como Windows (Bartender), macOS (JukeBox) e Linux (DanceFloor). Seus utilitários de configuração, como o Margarita, permitem que o NOC (Centro de Operações de Rede) personalize as ferramentas com base nos requisitos dos questionários "Fine Dining".

COLMEIA

HIVE é um conjunto multiplataforma de malware da CIA e seu software de controle associado. O projeto fornece implantes personalizáveis para plataformas Windows, Solaris, MikroTik (usado em roteadores de internet) e Linux, além de uma infraestrutura de Posto de Escuta (LP)/Comando e Controle (C2) para comunicação com esses implantes.

Os implantes são configurados para se comunicar via HTTPS com o servidor web de um domínio de cobertura; cada operação que utiliza esses implantes tem um domínio de cobertura separado e a infraestrutura pode lidar com qualquer número de domínios de cobertura.

Cada domínio de cobertura é resolvido para um endereço IP localizado em um provedor comercial de VPS (Servidor Virtual Privado). O servidor público encaminha todo o tráfego de entrada por meio de uma VPN para um servidor "Blot", que processa as solicitações de conexão dos clientes. Ele é configurado para autenticação opcional de cliente SSL: se um cliente enviar um certificado de cliente válido (somente implantes podem fazer isso), a conexão é encaminhada para o servidor de ferramentas "Honeycomb", que se comunica com o implante; se um certificado válido estiver ausente (o que ocorre quando alguém tenta abrir o site do domínio de cobertura acidentalmente), o tráfego é encaminhado para um servidor de cobertura, que exibe um site com aparência inusitada.

O servidor de ferramentas Honeycomb recebe informações exfiltradas do implante; um operador também pode encarregar o implante de executar tarefas no computador de destino, de modo que o servidor de ferramentas atua como um servidor C2 (comando e controle) para o implante.

Uma funcionalidade semelhante (embora limitada ao Windows) é fornecida pelo projeto RickBobby.

Veja os guias classificados do usuário e do desenvolvedor do HIVE.

Perguntas frequentes

Por que agora?

O WikiLeaks publicou assim que sua verificação e análise estavam prontas.

Em fevereiro, o governo Trump emitiu uma Ordem Executiva solicitando que uma revisão da "Guerra Cibernética" fosse preparada em 30 dias.

Embora a revisão aumente a atualidade e a relevância da publicação, ela não desempenhou nenhum papel na definição da data de publicação.

Redações

Nomes, endereços de e-mail e endereços IP externos foram redigidos nas páginas divulgadas (70.875 redações no total) até que uma análise mais aprofundada seja concluída.

1. **Excesso de redação:** alguns itens podem ter sido redigidos, pois não são funcionários, contratados, alvos ou estão relacionados à agência, mas são, por exemplo, autores de documentação para projetos públicos que são usados pela agência.
2. **Identidade vs. pessoa:** os nomes redigidos são substituídos por IDs de usuário (números) para permitir que os leitores atribuam várias páginas a um único autor. Dado o processo de redação utilizado, uma única pessoa pode ser representada por mais de um identificador atribuído, mas nenhum identificador se refere a mais de uma pessoa real.
3. **Anexos de arquivo (zip, tar.gz, ...)** são substituídos por um PDF listando todos os nomes de arquivo no arquivo. À medida que o conteúdo do arquivo é avaliado, ele pode ser disponibilizado; até então, o arquivo é redigido.
4. **Anexos com outro conteúdo binário** são substituídos por um dump hexadecimal do conteúdo para evitar a invocação acidental de binários que possam ter sido infectados com malware da CIA como arma. À medida que o conteúdo é avaliado, ele pode ser disponibilizado; até então, o conteúdo é redigido.
5. As **dezenas de milhares de referências de endereços IP roteáveis** (incluindo mais de 22 mil dentro dos Estados Unidos) que correspondem a possíveis alvos, servidores de postos de escuta secretos da CIA, sistemas intermediários e de teste, são redigidas para investigação exclusiva posterior.
6. **Arquivos binários de origem não pública** estão disponíveis apenas como dumps para evitar a invocação acidental de binários infectados por malware da CIA.

Organograma

O organograma corresponde ao material publicado pelo WikiLeaks até agora.

Como a estrutura organizacional da CIA abaixo do nível de Diretorias não é pública, a localização do EDG e suas filiais no organograma da agência foi reconstruída a partir de informações contidas nos documentos divulgados até o momento. Pretende-se que seja usado como um esboço da organização interna; esteja ciente de que o organograma reconstruído está incompleto e que reorganizações internas ocorrem com frequência.

Páginas Wiki

"Ano Zero" contém 7.818 páginas da web com 943 anexos do grupo de desenvolvimento interno. O software usado para esse fim é o Confluence, um software proprietário da Atlassian. As páginas da web neste sistema (como na Wikipédia) têm um histórico de versões que pode fornecer insights interessantes sobre como um documento evoluiu ao longo do tempo; os 7.818 documentos incluem esses históricos de páginas para as 1.136 versões mais recentes.

A ordem das páginas nomeadas dentro de cada nível é determinada pela data (das mais antigas para as mais antigas). O conteúdo da página não estará presente se ela tiver sido originalmente criada dinamicamente pelo software Confluence (conforme indicado na página reconstruída).

Qual é o período coberto?

Os anos de 2013 a 2016. A ordem de classificação das páginas dentro de cada nível é determinada pela data (das mais antigas primeiro).

O WikiLeaks obteve a data de criação/última modificação de cada página, informada pela CIA, mas estas ainda não aparecem por motivos técnicos. Normalmente, a data pode ser identificada ou aproximada a partir do conteúdo e da ordem das páginas. Se for essencial saber a hora/data exata, entre em contato com o WikiLeaks.

O que é o "Vault 7"

"Vault 7" é uma coleção substancial de material sobre atividades da CIA obtido pelo WikiLeaks.

Quando cada parte do "Vault 7" foi obtida?

A primeira parte foi obtida recentemente e abrange até 2016. Detalhes sobre as outras partes estarão disponíveis no momento da publicação.

Cada parte do "Vault 7" é de uma fonte diferente?

Detalhes sobre as outras partes estarão disponíveis no momento da publicação.

Qual é o tamanho total do "Vault 7"?

A série é a maior publicação de inteligência da história.

Como o WikiLeaks obteve cada parte do "Vault 7"?

Fontes confiam que o WikiLeaks não revelará informações que possam ajudar a identificá-los.

O WikiLeaks não está preocupado que a CIA aja contra sua equipe para interromper a série?

Não. Isso seria certamente contraproducente.

O WikiLeaks já "explorou" todas as melhores histórias?

Não. O WikiLeaks intencionalmente não publicou centenas de histórias impactantes para incentivar outras pessoas a encontrá-las e, assim, gerar conhecimento especializado na área para as partes subsequentes da série. Elas estão lá. Veja. Aqueles que demonstrarem excelência jornalística podem ser considerados para acesso antecipado às partes futuras.

Os outros jornalistas não encontrarão as melhores histórias antes de mim?

Improvável. Há consideravelmente mais histórias do que jornalistas ou acadêmicos em condições de escrevê-las.