Espionagem Invisível: A Arquitetura Secreta dos Ataques do Equation Group

Eduarda Albuquerque
evas@cin.ufpe.br

Gabriel Monteiro
gms2@cin.ufpe.br

Isabella Mendes
imsr@cin.ufpe.br

João Henrique
jhss2@cin.ufpe.br

José Lucas
jlhm@cin.ufpe.br

Resumo. O estudo detalha minuciosamente a anatomia dos ataques executados pelo Equation Group, revelando um arsenal cuidadosamente elaborado de ferramentas e técnicas furtivas. Implantes-chave como EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny e GrayFish são analisados, destacando sua modularidade e natureza adaptativa ao longo do ciclo de vida do ciberataque, desde o reconhecimento inicial até a exfiltração de dados e rotinas de autodestruição. Além disso, o artigo explora as táticas de evasão e furtividade do Equation Group, as quais iluminam a notável capacidade do grupo de infectar e persistir no firmware de discos rígidos, tornando as infecções resilientes à formatação e reinstalação do sistema operacional. O uso estratégico de vetores físicos, incluindo pendrives USB comprometidos e CD-ROMs por meio de táticas de interdição, assim como técnicas avançadas de anti-análise, algoritmos de criptografia personalizados e medidas sofisticadas de anti-virtualização/anti-depuração também são discutidas. Por fim, conclui-se examinando o direcionamento estratégico de alvos do Equation Group em diversos setores, incluindo governo, telecomunicações, aeroespacial e infraestrutura crítica, e destaca-se o impacto global de vulnerabilidades desenvolvidas por eles, notavelmente o EternalBlue, que contribuiu significativamente para ciberataques de grande escala como WannaCry e NotPetya.

Palavras-chave: Equation group, hackers, APT group, GrayFish, fantasy.

1. Introdução

O Equation Group é uma organização de ameaças persistentes avançadas (*advanced persistent threat* - APT, em inglês) altamente sofisticada, amplamente reconhecida por suas capacidades cibernéticas sofisticadas e por suas ligações com a agência de segurança nacional dos Estados Unidos (*national security agency* - NSA, em inglês). Descoberto em 2015 pela Kaspersky Lab, suas operações iniciaram em meados de 2001 e talvez até antes, se tornando um dos grupos de ciberespionagem mais antigos e enigmáticos em atividade. A complexidade e o nível de sofisticação de suas ferramentas e técnicas de ataque são notáveis, incluindo o uso de implantes de firmware, a exploração de vulnerabilidades zero-days e a capacidade de reescrever o firmware de discos rígidos, tornando suas infecções extremamente persistentes e difíceis de detectar e remover.

Este documento tem como objetivo analisar as técnicas e procedimentos do Equation Group, destacando as principais características que o distingue de outros atores de ameaça cibernética. Abordaremos as ferramentas notáveis atribuídas ao grupo, como EquationDrug e DoubleFantasy, e discutiremos o impacto de suas operações em alvos globais, incluindo instituições financeiras, agências governamentais, telecomunicações e infraestruturas críticas. Além disso, exploraremos a possível conexão do Equation Group com Stuxnet e o vazamento de ferramentas da Shadow Brokers, eventos que revelaram a amplitude e profundidade de suas capacidades. Ao final, esperamos fornecer uma compreensão abrangente sobre um dos mais perigosos atores de ameaça no cenário da cibersegurança e as lições que podemos aprender com suas operações.

2. Anatomia de Ataque

O Equation Group dispunha de um arsenal sofisticado e estratégico de técnicas e ferramentas furtivas, cuidadosamente desenvolvidas para atuar em cada etapa do ciclo de ataque cibernético. Para comprometer seus alvos, o grupo criou uma série de implantes personalizados (trojans), identificados e estudados pelos laboratórios da Kaspersky, incluindo EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny e GrayFish. Essas ferramentas não operam isoladamente, pelo contrário, são modulares e coordenadas entre si, adaptando-se dinamicamente ao ambiente da vítima e aos objetivos específicos da operação.

Nesta seção, será apresentada a anatomia dos ataques realizados pelo Equation Group, desde o reconhecimento inicial até a exfiltração de dados e as possíveis rotinas de autodestruição, destacando os implantes e métodos utilizados em cada estágio da infecção, incluindo a análise mais detalhada do funcionamento de ferramentas avançadas como o EquationDrug e o GrayFish.

2.1 Seleção e validação do alvo

O Equation Group é conhecido por selecionar suas vítimas com alta precisão. O grupo demonstrou capacidade técnica avançada ao comprometer até mesmo redes fisicamente isoladas da internet e de outras redes externas, coordenando ataques por meio de mídias físicas, como CD-ROMs e dispositivos USB com exploit embutido. Esse cenário indica o uso

de uma tática altamente furtiva conhecida como *interdiction*, na qual os atacantes interceptam mercadorias enviadas e as substituem por versões comprometidas com trojans.

Quando esse método não é possível, os alvos são inicialmente comprometidos com o implante validador DoubleFantasy e, caso não sejam considerados “interessantes” pelos atacantes, são posteriormente desinfectados. Em redes conectadas, a infiltração inicial frequentemente se dava por meio de exploits baseados na web. Uma das técnicas utilizadas pelo grupo envolve a exploração de vulnerabilidades no Simple Network Management Protocol (SNMP) e na Interface de Linha de Comando (*command line interface* - CLI, em inglês) dos firewalls.

Esses ataques foram entregues por diferentes vetores. Um dos métodos recorrentes consistia na utilização de scripts PHP implantados em fóruns comprometidos, os quais permitiam atingir alvos estratégicos ao redirecionar ou executar cargas maliciosas durante a navegação em ambientes específicos, como fóruns de discussão jihadistas islâmicos ou páginas de anúncios em sites populares no Oriente Médio. Isso significa que os atacantes tiveram um cuidado especial na infecção dos alvos, visto que a estrutura de certos scripts continham especificidades que exploravam questões de autenticação de usuários e acessos a partir de determinados provedores de internet (ISPs), assegurando maior seletividade no processo de disseminação do malware.

2.1.1 Estrutura do DoubleFantasy

O trojan DoubleFantasy, utilizado como estágio inicial de exploração pelo Equation Group, destaca a inteligência estratégica da implementação e disciplina operacional do grupo, pois, em seu modus-operandi, utilizava-se softwares "validadores" que funcionavam como uma sentinela espiã. O bloco de configuração do trojan inclui um número de versão, que pode ser utilizado para reconhecimento e controle das builds do malware. Além disso, o malware armazena dados de hosts legítimos (como *microsoft.com* e *yahoo.com*), utilizados para verificar a conectividade com a internet antes do início das comunicações maliciosas. O objetivo principal era confirmar o interesse genuíno no alvo, isto é, avaliar se a máquina ou a rede correspondiam aos critérios específicos da missão do grupo, por exemplo se o ambiente era propício para a infiltração e se o alvo possuía dados ou acessos de alto valor. Somente após essa validação eram implantadas ferramentas mais sofisticadas, consolidando assim, o ataque.

Se tudo ocorresse como planejado, o sistema infectado recebia plataformas mais sofisticadas, como o EquationDrug ou o GrayFish. Essa prática cautelosa do grupo otimiza o uso de seus recursos e reduz sua exposição desnecessária em alvos não essenciais.

2.1.2 Estrutura do TripleFantasy

TripleFantasy é um backdoor completo (método de acesso secreto que burla os protocolos de segurança comuns, como login e senha, entre outros), geralmente usado em conjunto com GrayFish (que será explanado mais a frente). Aparenta ser uma evolução do DoubleFantasy, possivelmente atuando como um plugin de validação mais moderno.

2.2 Implantação do Malware Principal e Persistência

Nas fases avançadas do ataque, o Equation Group empregava mecanismos sofisticados para garantir persistência e ocultação, utilizando ferramentas como GrayFish, EquationDrug, *rootkits*, *bootkits* e cargas ocultas no registro do sistema, além de dispositivos USB com exploits que permitiam a troca de dados mesmo sem conexão de rede.

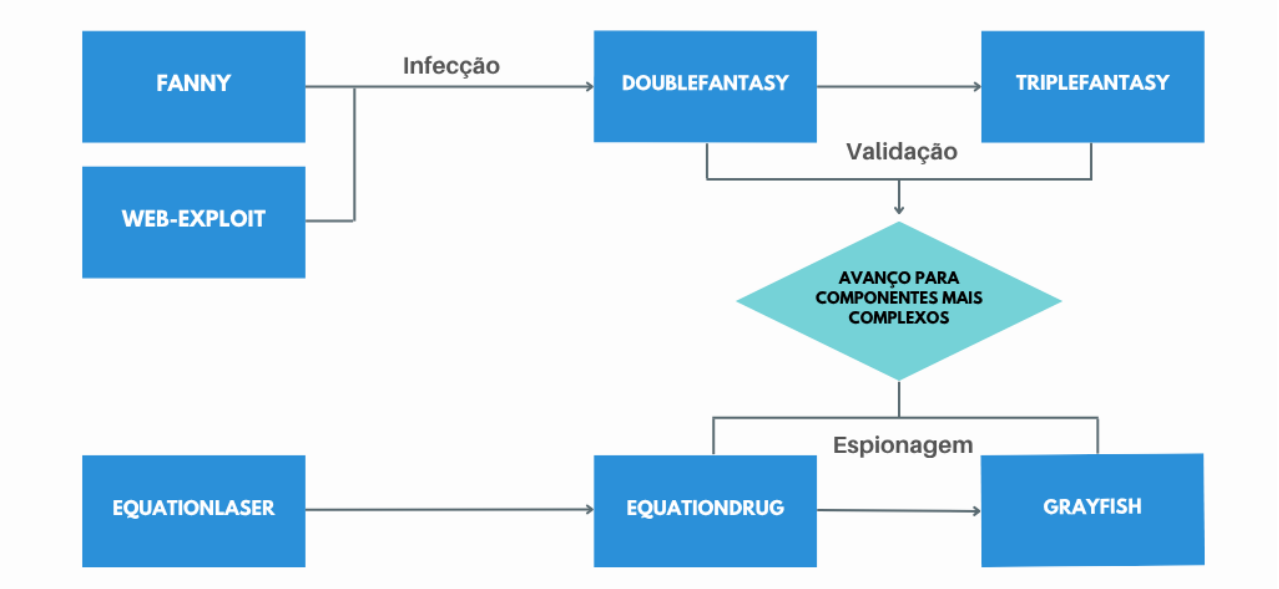


Figura 1 – Diagrama de Interação dos Malwares e Estratégias Utilizadas
Fonte: Elaboração própria

2.2.1 EquationDrug: Plataforma Espiã

O EquationDrug é uma das principais plataformas de espionagem avançada utilizada pelo Equation Group. Foi desenvolvida entre 2003 e 2013, sucedendo a EquationLaser e, posteriormente, substituída pela GrayFish.

Sua arquitetura geral é semelhante a um mini sistema operacional, com componentes em modo kernel e modo de usuário, incluindo drivers, um núcleo orquestrador e diversos plugins com IDs únicos que definem suas funções.

Alguns módulos são fixados ao núcleo da plataforma, realizando atividades básicas de ciberespionagem. Além disso, é possível ampliar a funcionalidade da plataforma por meio da implantação de módulos específicos nas máquinas das vítimas selecionadas.

A execução inicia com um driver em modo kernel (como msndsrv.sys ou mssvc32.vxd) que, após a inicialização do sistema, aciona o carregador de modo usuário (mscfg32.exe) e então o orquestrador principal (mscfg32.dll). Plugins adicionais podem ser carregados por bibliotecas auxiliares. Suas funcionalidades incluem interceptação de tráfego, espionagem do navegador, manipulação de firmware, controle remoto de processos e coleta de senhas e atividades do usuário em tempo real.

A infecção não é imediata. Após a validação do DoubleFantasy, o EquationDrug é instalado, permitindo que os atacantes tenham controle total sobre o sistema operacional. A plataforma possui um mecanismo de autodestruição se não receber comandos do servidor C&C por meses.

Plugins antigos eram compatíveis com Windows 95/98/ME, mas alvos com sistema mais modernos, como o Windows 7, recebiam TripleFantasy ou GrayFish.

Dados roubados são armazenados em um sistema de arquivos virtual criptografado, disfarçado como arquivos .FON na pasta Windows\Fonts, antes de serem enviados aos servidores de C&C.

Domínios associados incluem newjunk4u[.]com, phoneysoap[.]com, dowelsobject[.]com, easyadvertonline[.]com e gar-tech[.]com (este último neutralizado pela Kaspersky Lab).

2.2.2 GrayFish: Ataque invisível

O GrayFish é um implante de malware mais sofisticado do Equation Group. Ele foi projetado entre 2008 e 2013 para executar comandos maliciosos dentro do sistema operacional Windows, SO da Microsoft, incluindo Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, Windows 7 e 8, com mecanismo de persistência eficaz (quase “invisível”) e armazenamento oculto.

O GrayFish inclui um bootkit que é um tipo de malware altamente sofisticado que, ao iniciar o computador, injeta seu código no registro de inicialização (boot record) e assume o controle do carregamento do sistema operacional, permitindo controle total do Windows.

Já dentro do Windows, o GrayFish executa um processo de 4 a 5 etapas, cada etapa descriptografa e executa a próxima, até liberar o módulos maliciosos. Esses módulos estão escondidos e criptografados no registro do Windows. Se qualquer nível de execução falhar, o GrayFish se autodestrói.

Para ativar a segunda parte do código malicioso, o GrayFish gera uma chave criptográfica com base no Object_ID de uma pasta crítica, como por exemplo %Windows%, aplicando o hash SHA-256 mil vezes.

O mecanismo de carregamento (bootloader) implementa um sistema de arquivos virtuais criptografados (VFS) dentro do registro do Windows, para armazenar informações roubadas. Caso o SO tenha um mecanismo moderno de segurança, que bloqueia a execução de códigos não confiáveis em modo kernel, o GrayFish explora diversos drivers diferentes. Uma das opções é o <ElbyCDIO.sys>, que contém uma vulnerabilidade que será explorada para conseguir a execução de código em nível de kernel.

Projetado para máxima furtividade, o GrayFish não grava executáveis no disco: seus módulos são descriptografados e executados diretamente da memória, o que dificulta a detecção por antivírus. Todo o malware fica oculto na área de serviço do HD, e o bootkit persiste mesmo após a reinstalação do sistema, porém em muitos casos, só a substituição do disco ou atualização segura do firmware pode removê-lo.

3. Evasão e furtividade

A longevidade e o sucesso do grupo em permanecer indetectável por tanto tempo são um testemunho de sua engenharia de malware de ponta, táticas operacionais meticulosas e um profundo domínio de técnicas multifacetadas de evasão, persistência, furtividade e anti-análise.

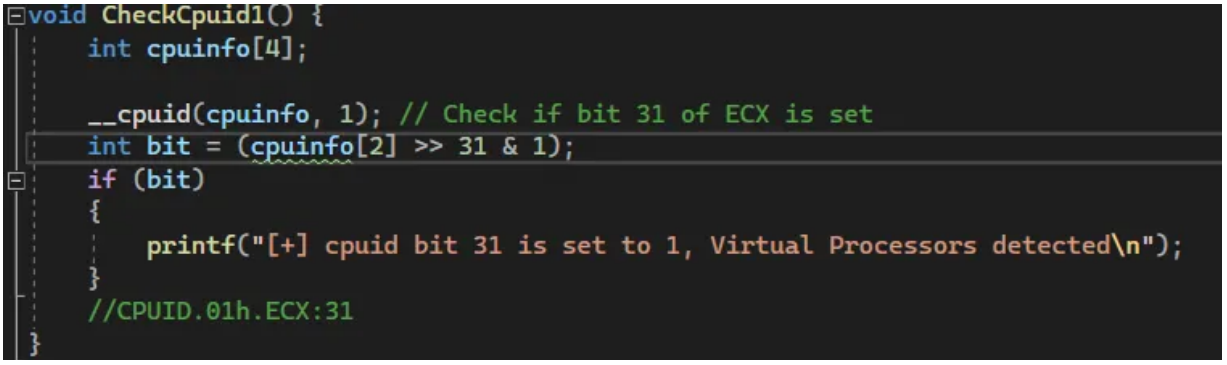
O GrayFish, considerado a plataforma de ataque (ou malware) mais sofisticada do grupo — cuja arquitetura era baseada em registro, era mais flexível, furtiva e complexa do que as outras, pois não se utilizava de arquivos armazenados em disco — demonstrava um nível notável de furtividade ao residir completamente no registro do Windows, dependendo de um bootkit para ser executado na inicialização do sistema operacional. Quando o computador era ligado, o GrayFish sequestrava os mecanismos de carregamento do sistema operacional e injetava seu código no registro de inicialização para controlar a inicialização do Windows em cada estágio. Por fim, executava módulos que também estavam armazenados no registro do sistema operacional, com cada estágio decodificando e executando o próximo numa espécie de execução em cadeia.

Crucial para a furtividade e evasão, muitos dos malwares do Equation Group incluíam um protocolo de autodestruição. Isso garantia que os artefatos de infecção fossem removidos após a conclusão da operação ou em caso de erro, dificultando a análise forense subsequente. O EquationDrug, por exemplo, possuía um temporizador de contagem regressiva para autodestruição caso os comandos do servidor de C&C não fossem recebidos a tempo.

O grupo tinha a prática de empregar implementações criadas por eles próprios de algoritmos como RC5, RC6, RC4 e AES, hashes e, no caso do método aplicado no GrayFish, mil vezes o cálculo do hash SHA-256 sobre o ID do objeto NTFS exclusivo da pasta Windows da vítima para descriptografar o próximo estágio do registro. Essa técnica vincula criptograficamente a infecção à máquina específica, tornando impossível a descriptografia dos dados sem o ID do objeto NTFS exato daquela máquina, o que impede a análise em massa em laboratórios e eleva significativamente a curva de progressão para a engenharia reversa que era dificultada por lidar com códigos confusos e de entendimento precário da lógica original do malware, pois o código fonte continha muitos "Junk" ou "Spaghetti" e técnicas de anti-análise como por exemplo o achatamento do Grafo de Fluxo de Controle (CFG flattening), que reestrutura o fluxo de controle das funções.

A cautela do Equation Group quanto ao sistema que estava sendo infectado e se o programa malicioso estava sendo observado ou extraído fica evidente nas suas diversas práticas de anti-virtualização e anti-depuração meticulosas que utilizavam métodos como a verificação do bit 31 do registrador ECX para detectar a presença de um hypervisor, ou a consulta do registrador EAX para identificar o fornecedor do hypervisor . Também realizavam a verificação de chaves de registro específicas de VMs (por exemplo, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters para HyperV, HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__ para VirtualBox), a enumeração de processos em execução ou arquivos no sistema para identificar padrões de sandbox, a verificação de endereços MAC conhecidos associados a fornecedores de VM (por exemplo, VMWare: 00:05:69 e VirtualBox: 08:00:27) e detecção de sandboxes automatizadas que frequentemente operam com resoluções de tela incomuns ou ausência de

dispositivos de entrada/saída como mouse e teclado. O grupo empregou diversas funções da API do Windows, como IsDebuggerPresent (que verifica a flag BeingDebugged no PEB — Process Environment Block), CheckRemoteDebuggerPresent, FindWindow, além de verificar o valor de NtGlobalFlag no PEB para 0x70, que indica se o programa está sendo depurado. A chamada de DebugBreak() seguida da verificação de como a exceção era tratada é outra tática, assim como técnicas de defesa baseadas em tempo, como GetTickCount(), que mediam o tempo de execução entre pontos específicos no código e portanto, se fossem detectados atrasos incomuns causados pela depuração, podiam indicar a presença de um depurador.



```
void CheckCpuid1() {
    int cpuinfo[4];

    __cpuid(cpuinfo, 1); // Check if bit 31 of ECX is set
    int bit = (cpuinfo[2] >> 31 & 1);
    if (bit)
    {
        printf("[+] cpuid bit 31 is set to 1, Virtual Processors detected\n");
    }
    //CPUID.01h.ECX:31
}
```

Figura 2 – Trecho de código que verifica se o bit 31 do registrador EXC é 1, ou seja, há um hypervisor ativo
Fonte: Medium, 2024

A longevidade do Equation Group, isto é, a capacidade de operar furtivamente durante tantos anos sem serem pegos, também foi sustentada pelo uso estratégico de vulnerabilidades zero-days que eram frequentemente exploradas antes de serem publicamente conhecidas ou utilizadas por outros grupos. Exemplos incluem dois exploits zero-days utilizados pelo worm Fanny em 2008, que mais tarde foram identificados no Stuxnet: o exploit LNK e uma vulnerabilidade corrigida pelo boletim MS09-025. Essa precedência no uso de vulnerabilidades não documentadas demonstrava que o Equation Group possuía acesso a um canal de inteligência de vulnerabilidades de alto nível, proporcionando uma janela de oportunidade incomparável para obter acesso inicial e estabelecer persistência sem detecção diante das agências de segurança da época.

4. Vulnerabilidade EternalBlue: Falha no SMBv1

MS17-010, mais conhecido como EternalBlue, é uma falha crítica de segurança no protocolo SMBv1 (Server Message Block versão 1) em sistemas Windows. Criada pelo Equation Group, ela afeta diversas versões do Windows, como XP, 7, 8, 10 e Windows Server 2003 até 2016.

Essa vulnerabilidade explora a forma como o Microsoft Windows manipulava incorretamente pacotes enviados por atacantes remotos, permitindo a execução de código maliciosos no computador de destino. Tudo o que o invasor precisava fazer era enviar um pacote criado com códigos maliciosos ao servidor visado. Isso permitia tomar controle do sistema ou instalar malwares remotamente.

Em março de 2017, a falha foi corrigida pela Microsoft e documentada por meio do boletim de segurança MS17-010. Porém muitos sistemas não foram atualizados a tempo, por conta disto, a falha permaneceu explorável por um longo período, o que levou a ataques globais. No mesmo ano, o famoso ransomware WannaCry explorou o EternalBlue para se espalhar por redes vulneráveis, atingindo instituições em mais de 150 países. Meses depois, o NotPetya usou a mesma vulnerabilidade para causar danos graves à infraestrutura de redes de maneira indiscriminada, sobretudo na Ucrânia, sendo um dos ataques cibernéticos mais destrutivos já registrados.

Ferramentas como Nmap identificam sistemas vulneráveis, enquanto Metasploit e FuzzBunch (da NSA) exploram a falha, permitindo ações como abertura de shell remota e instalação de malware. Scripts derivados do exploit original ajudaram a popularizar sua exploração entre hackers, cibercriminosos e pesquisadores, sendo amplamente usados em testes de penetração e ataques reais.

Para se proteger, é essencial aplicar o patch MS17-010, desativar o protocolo SMBv1, utilizar firewalls que bloqueiam portas SMB, como a 445, e manter sistemas operacionais e antivírus sempre atualizados.

5. Alvos e Setores

O Equation Group, sendo um *Advanced Persistent Threat* (APT) de nível estatal e altamente sofisticada (amplamente atribuído sua origem à NSA), tinha alvos mais específicos e estratégicos, visando principalmente a ciberespionagem e, em alguns casos, a sabotagem. Suas campanhas eram de longo prazo e focadas em coleta de inteligência. A pesquisa do Kaspersky Lab, que expôs o grupo em 2015, e análises subsequentes, identificou diversos setores como alvos prioritários:

Governos e Instituições diplomáticas: Este é o alvo mais óbvio para um grupo de ciberespionagem estatal. O Equation Group deixou claro que visava a obtenção de informações políticas, militares, econômicas e diplomáticas confidenciais pelo padrão de alvo das suas atividades. Telecomunicações: Comprometer empresas de telecomunicações é crucial para a vigilância de comunicação e para acesso de redes de alto valor. Isso permite a interceptação de dados de tráfego, metadados e, potencialmente, o direcionamento de ataques a outros alvos através de infraestrutura de telecomunicações. Indústria Aeroespacial: Este setor é de alto valor estratégico devido à pesquisas e desenvolvimento de tecnologias sensíveis, como sistemas de defesa, aviação militar e tecnologia de mísseis. Energia: Alvos no setor da energia, incluindo pesquisa nuclear, petróleo e gás, e serviços elétricos, são de extrema importância para a segurança nacional e econômica. A obtenção de inteligência nesses setores pode variar desde planos de desenvolvimento da infraestrutura até informações sobre capacidade e vulnerabilidades de um ponto estratégico. Militares: Organizações militares são alvos diretos por razão da coleta de inteligência sobre operações, capacidades, tecnologias de armamento e planejamento estratégicos. Pesquisas e Desenvolvimento (Nanotecnologia): Grupos de APTs frequentemente visam instituições de pesquisas e empresas de alta tecnologia para roubar propriedade intelectual, segredos comerciais e avanços científicos que podem ter aplicações militares ou econômicas. Instituições

financeiras: Embora menos comum que em outros grupos como motivação puramente financeira, o Equation Group visou instituições financeiras para ter acesso a informações de inteligência econômica ou para facilitar outras operações monetárias. Mídia: Organizações de mídia podem ser alvo para monitoramento de narrativas, identificação de fontes para ter acesso a informações privilegiadas e sensíveis antes do público. Transporte: O setor de transporte, incluindo logística e infraestrutura, pode ser visado para monitoramento de movimentações de bens, pessoas ou para obtenção de inteligência sobre cadeias de suprimentos. Empresas de Tecnologia (Criptografia): Empresas que desenvolvem tecnologia de criptografia são alvos de alto valor para APTs, pois comprometer seus produtos pode dar acesso a comunicações seguras de diversos outros alvos. Ativistas e Estudiosos Islâmicos: A inclusão desses alvos sugere um interesse em inteligência relacionada a movimentos sociais, ideológicos ou indivíduos específicos em regiões de interesse geopolítico.

O Kaspersky Lab em outras análises identificou uma concentração significativa de vítimas em regiões de interesse estratégico e geopolítico para os Estados Unidos e seus aliados, que reforça a atribuição à NSA. Os países mais monitorados pelo grupo foram: Irã, Rússia, Paquistão, Afeganistão, Índia, Síria e Mali. Além desses países, foram observados infecções em mais de 40 países, incluindo nações na Europa como: França, Suíça e Reino Unido. No continente da Ásia: China, Hong Kong, Japão e Coreia. Na América: Brasil, México e Estados Unidos embora em menor número aparente para evitar detecções.

6. As Armas Físicas

A atuação do Equation Group transcende os ataques de software convencionais, revelando um grau notável de planejamento e execução, com estratégias de infecção e exfiltração de dados que se destacam tanto pela persistência quanto pela furtividade.

Uma de suas capacidades mais impressionantes é a habilidade de infectar o firmware de discos rígidos (HDDs), resultando em um comprometimento de difícil detecção e recuperação. (KASPERSKY, 2015).

Adicionalmente, o grupo exibe um domínio técnico notável ao utilizar dispositivos físicos como ferramentas de disseminação. CD-ROMs adulterados e pendrives USBs com código malicioso foram empregados como canais de infecção, evidenciando operações de interdição, onde produtos são interceptados e manipulados com intuito malicioso antes de chegarem ao destino final. Um caso emblemático foi o worm Fanny, desenvolvido para mapear redes isoladas (*air-gapped*) com um engenhoso sistema de comando e controle via USB; essa tática revela um método inovador para contornar barreiras físicas e lógicas de segurança (KASPERSKY, 2015).

6.1 Infecção de firmware de discos rígidos

Entre as técnicas avançadas do Equation Group, destaca-se a habilidade de reprogramar o firmware de discos rígidos, uma das táticas mais distintivas do grupo. Mesmo que o disco seja formatado ou o sistema operacional completamente reinstalado, o malware permanecia funcional em computadores. Essa técnica representa o ápice da persistência em ataques

cibernéticos, superando em complexidade até mesmo outras ameaças avançadas como o Regin, portanto, não apenas assegurava persistência extrema, mas também permitia a criação de áreas ocultas e quase que permanentes dentro do disco rígido invisíveis para o sistema operacional.

6.2 Plataformas e módulos de reprogramação

A habilidade de reprogramar o firmware foi identificada nas plataformas de malware EquationDrug e GrayFish. Foram recuperados dois módulos distintos para essa finalidade: um do EquationDrug (versão 3.0.1), compilado em 2010, e outro mais complexo do GrayFish (versão 4.2.0), compilado em 2013. O plugin de reprogramação possuía um ID interno único (80AA) e estava disponível em versões de 32 e 64 bits.

6.3 Objetivos e capacidades

A reprogramação do firmware de um disco rígido permitia ao grupo alcançar dois objetivos cruciais. O primeiro era persistência extrema: a infecção sobrevivia à formatação do disco e à reinstalação completa do sistema operacional. Isso garante que o malware permaneça no sistema alvo indefinidamente, a menos que o próprio hardware seja substituído. O segundo era o armazenamento invisível e persistente: por meio de um plugin, era criada uma área de armazenamento oculta dentro do disco rígido, tornando-a invisível para o sistema operacional. Esse espaço permitia armazenar dados roubados ou outros módulos da plataforma de ataque, sem deixar vestígios no sistema de arquivos visíveis.

6.4 Fabricantes alvo e metodologia

Os módulos de reprogramação eram compatíveis com uma vasta gama de modelos de discos rígidos, utilizando comandos ATA não documentados e específicos de cada fornecedor. A análise dos plugins revelou suporte para múltiplas categorias de drives, incluindo os dos seguintes fabricantes:

1) Maxtor e Maxtor STM;
2) Seagate Technology;
3) Western Digital (WDC);
4) Samsung;
5) Hitachi, IBM e ExcelStor;
6) Toshiba;
7) Micron; e
8) SSDs de marcas como OCZ, OWC, Corsair e Mushkin.

O processo de *reflashing* (que é o processo de reescrever o firmware ou software de baixo nível de um dispositivo eletrônico) era extremamente direcionado, visando discos com números de série específicos. Devido à sua complexidade, o módulo era usado de forma muito seletiva, sendo reservado para as vítimas mais valiosas ou para circunstâncias muito especiais.

6.5. Pendrives USBs e o worm Fanny: mapeando redes isoladas

O Equation Group superou o desafio do *air gap* (isolamento físico de uma rede) utilizando o worm Fanny, que empregava pendrives USB como um trojan. Criado em 2008, o Fanny tinha como alvo principal a coleta de informações no Oriente Médio e na Ásia, explorando a vulnerabilidade LNK (CVE-2010-2568), a mesma que mais tarde foi descoberta no Stuxnet.

O principal objetivo do Fanny era mapear a infraestrutura de redes isoladas por meio de um mecanismo exclusivo. Primeiro, o malware realizava a criação de armazenamento oculto: ao infectar um pendrive, o Fanny criava uma área de armazenamento secreta no dispositivo. Em seguida, ocorria a coleta de informações offline: se o pendrive fosse conectado a um computador em uma rede *air-gapped*, o worm coletava dados básicos do sistema e os salvava nessa área oculta. Por fim, na etapa de exfiltração de dados, ao ser inserido em um computador previamente infectado e com acesso à internet, o pendrive transmitia as informações coletadas para os servidores de comando e controle (C&C). Esse mecanismo também permitia uma comunicação bidirecional, pois os atacantes poderiam salvar comandos na área oculta do USB para serem executados em máquinas na rede isolada.

6.6 Uso de CD-ROMs e técnicas de interdição

Além de pendrives, o Equation Group utilizava mídias físicas como CD-ROMs para infectar seus alvos, demonstrando capacidade para realizar operações de interdição. Dois exemplos foram identificados. No primeiro caso, durante uma conferência científica em Houston, alguns participantes receberam pelo correio um CD-ROM com os materiais da conferência após o evento. O disco estava comprometido e, por meio de um arquivo (*autorun.inf*), executava um instalador que tentava escalar privilégios e instalar o DoubleFantasy. No segundo caso, foi identificado um CD de instalação do software Oracle que continha, além do instalador legítimo, um *dropper* do trojan EquationLaser.

Esses ataques indicam um alcance operacional que vai além do mundo digital, envolvendo logística e manipulação física de objetos para alcançar alvos de alto valor.

7. Conclusão

O Equation Group representa uma marca na história da cibersegurança, demonstrando tamanho nível de sofisticação, criatividade e persistência raramente vistos. A capacidade de comprometer firmware de discos rígidos e a utilização de mídias físicas alteradas para infectar até mesmo redes isoladas mostram uma estratégia de acesso e controle sem precedentes. Essas táticas garantiam uma furtividade profunda, permitindo que suas operações de espionagem se estendessem por anos sem detecção.

As plataformas de espionagem EquationDrug e GrayFish ilustram a engenhosidade do grupo em manter controle total do sistema por meio de módulos ocultos e criptografados. Suas operações discretas, aliada a técnicas avançadas como *bootkits* e o uso de sistemas virtuais, não só assegurava a coleta eficiente de dados, mas também dificultava imensamente a identificação e a sua erradicação. A exploração de vulnerabilidades críticas, como EternalBlue no SMBv1, posteriormente utilizado em ataques massivos como WannaCry,

evidenciou, diante do mundo todo, a capacidade do Equation Group de capitalizar falhas zero-days mesmo antes que as informações se tornem de conhecimento público.

A longevidade notável do Equation Group não foi por acaso. Ela se baseou em uma combinação de táticas avançadas de evasão e furtividade, que incluem a capacidade de infectar o firmware para persistência extrema e a operação indetectável de malwares como GrayFish. Além disso, o grupo empregava mecanismos rigorosos de autodestruição, criptografia própria e técnicas anti-análise, explorando vulnerabilidades zero-days para garantir acesso e conduzir operações de espionagem de alto nível por uma década. O legado do Equation Group serve como um alerta contínuo sobre a necessidade de vigilância e inovação na defesa cibernética.

Referências

AVAST. **O que é EternalBlue e como funciona essa ameaça cibernética?** [S.l.], [2024?]. (eternalblue_avast.html, 480KB). Disponível em:<https://www.avast.com/c-eternalblue >. Acesso em: 2 jul. 2025.

BARANOV, Sergey. **Uncovering the Equation Group ring-0 tricks with GrayFish rootkit. LinkedIn Pulse**. 27 mar. 2017. Disponível em:<https://www.linkedin.com/pulse/uncovering-equation-group-ring-0-tricks-GrayFish-rootkit-baranov/>. Acesso em: 2 jul. 2025.

BUGCROWD. **Equation Group**. [s.d.]. Disponível em:<https://www.bugcrowd.com/glossary/equation-group/>. Acesso em: 01 jul 2025.

CHINA CYBERSECURITY INDUSTRY ALLIANCE (CCIA). **Review of cyberattacks from US intelligence agencies: based on global cybersecurity communities' analyses**. CCIA, abr. 2023. Disponível em:<https://www.china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file/20230411/20230411080719_9921.pdf>. Acesso em: 2 jul. 2025.

GALLAGHER, Sean. **How "omnipotent" hackers tied to the NSA hid for 14 years—and were found at last**. Ars Technica. 16 fev. 2015. Disponível em:<https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/#page-3>. Acesso em: 2 jul. 2025.

KASPERSKY. **EQUATION GROUP: QUESTIONS AND ANSWERS**. 2015. Disponível em:<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf>. Acesso em: 01 jul 2025.

KASPERSKY. **Mystery of Duqu, a sophisticated cyberespionage actor returns**. 2015. Disponível em:<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf>. Acesso em: 01 jul 2025.

KASPERSKY LAB. **Inside the EquationDrug espionage platform**. [S.l.], 2015. (securelist_equationdrug.pdf, 2MB). Disponível em:<https://securelist.com/inside-the-equationdrug-espionage-platform/69203/>. Acesso em: 2 jul. 2025.

MICROSOFT. **Boletim de segurança da Microsoft MS17-010 - Atualização de segurança para o SMB Server (4013389)**. [S.l.], 2017. (ms17-010.html, 512KB). Disponível em:<https://learn.microsoft.com/pt-br/security-updates/securitybulletins/2017/ms17-010>. Acesso em: 2 jul. 2025.

PAGANINI, Pierluigi. **Equation Group APT and TAO NSA: Two Hacking Arsenals Too Similar**. INFOSEC INSTITUTE. 09 mar 2015. Disponível em:<https://www.infosecinstitute.com/resources/threat-intelligence/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/>. Acesso em: 01 jul 2025.

PARAST, Fatemeh Khoda. **Unraveling Shadows: Exploring the Realm of Elite Cyber Spies**. [S.l.], 2024. Disponível em:<https://arxiv.org/pdf/2406.19489>. Acesso em: 2 jul. 2025.

RAPID7. **Metasploit: penetration testing software**. [S.l.], [2025?]. (metasploit_site.html, 1MB). Disponível em:<https://www.metasploit.com>. Acesso em: 2 jul. 2025.

SAAITAAMAA. **Malware 101: Anti-Virtualization & Anti-Debugging Methods**. MEDIUM, 06 ago 2024. Disponível em:<https://medium.com/@exploitdevvv/malware-101-anti-virtualization-anti-debugging-methods-04353f0a9407>. Acesso em: 01 jul 2025.

UNKNOWN AUTHOR. **Equation Group: the most advanced cyber-attack group in the world**. Boston University, Department of Computer Science. Disponível em:<https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/eqngroup.pdf>. Acesso em: 2 jul. 2025.