APT ACTUATIONS AND CYBER ESPIONAGE: EQUATION GROUP

Ariel Sharon Vieira de Lima - asvl
Breno José Ramos da Silva - bjrs
Davi Matoso Torreão - dmt2
Janderson Santana de Freitas - jsf6
LPSEC - 2025

Abstração
Este estudo analisa o Equation Group, um dos grupos de ameaças persistentes avançadas (APTs) mais sofisticados já documentados, vinculado à unidade Tailored Access Operations (TAO) da Agência de Segurança Nacional dos EUA (NSA), cujas operações redefiniram os parâmetros da ciberespionagem global. Baseado em análises forenses da Kaspersky (2015) e vazamentos dos Shadow Brokers (20Pd16-2017), nota-se sua arquitetura única: mecanismos de persistência via firmware (implantes GrayFish e EquationDrug em HDDs/SSDs de fabricantes como Seagate e Western Digital) garantiam sobrevivência mesmo após formatações, enquanto exploits de zero-day (EXTRABACON para Cisco ASA, ETERNALBLUE para Microsoft SMB) permitiam infiltração em redes críticas. Já no âmbito geopolítico, o grupo focava em espionar países normalmente opositores ao governo americano, concorrentes, ou àqueles que tinham um desenvolvimento de armas ativo, como o Irã, China e Rússia. A atribuição à NSA é sustentada por evidências fortes, onde as principais são elas: codinomes coincidentes (STRAITACID, BACKSNARF) documentados no catálogo ANT da TAO vazado pelo Der Spiegel, e padrões operacionais alinhados ao fuso horário EST (UTC-5) com inatividade em feriados norte-americanos. Conclui-se que o Equation Group representa um marco na guerra cibernética estatal, pois combina inovação técnica com geopolítica a fim de espionar ou incapacitar governos e pessoas dissidentes.

Palavras-chave: Equation Group, NSA, firmware, zero-day, ciberespionagem.

1. Introdução

Diante do avanço da internet e da expansão da globalização através deste meio, as nações, que sempre estiveram uma de olho na outra a fim de melhorar suas políticas econômicas, militares e traçar um caminho mais claro para o desenvolvimento do seu país, entenderam que era necessário novas formas de manter-se a par das políticas exteriores. Essa necessidade catalisou o surgimento de operações de ciberespionagem estatal sofisticadas, onde a partir de grandes investimentos de capital e recursos quase que ilimitados eram capazes construir plataformas quase que indetectáveis em busca de obter informações ou sabotar políticas que poderiam de alguma forma afetar negativamente o seu país.

Baseado nisso, iniciou-se um grande investimento nas chamadas Ameaças Persistentes Avançadas (APTs), que visam acessos não autorizados a sistemas ou exploração de falhas críticas para permanecer ocultas em redes por longos períodos. Entre esses grupos, um se destacou pela sofisticação sem precedentes: o Equation Group, nome dado pela Kaspersky

Lab, empresa que descobriu e expôs o grupo em uma conferência no México em 2015. Esse termo, Equation Group, reflete sua predileção por criptografia baseada em equações matemáticas complexas para ocultar comunicações e dados roubados, além de sua precisão operacional cirúrgica, que é comparável à resolução de uma equação, daí vem o nome atribuído.

De acordo com informações de atuação, matchs de variáveis vazadas, ausência de ações em feriados dos EUA, o grupo foi vinculado à Agência de Segurança Nacional dos Estados Unidos (NSA). Essa atribuição também deve-se ao modelo de atuação do grupo, que costumeiramente atacou e espionou países "não-amigáveis, ou que possuíam dinâmicas políticas um pouco distantes da democracia americana, como China, Rússia, Irã e países latino-americanos.

O Equation Group foi responsável pelo desenvolvimento de diversas plataformas de espionagem cibernética. Suas primeiras atividades registradas datam de 1996, com testes experimentais do malware *EquationLaser* em sistemas Windows 95/98. Posteriormente, plataformas mais sofisticadas foram desenvolvidas, como:

- *EquationDrug*, capaz de capturar screenshots e exfiltrar documentos criptografados;
- *GrayFish*, que implementou persistência em firmware de HDDs, sobrevivendo a formatações;
- *Fanny*, worm que mapeava redes air-gapped via dispositivos USB e compartilhou vulnerabilidades zero-day com o *StuxNet*.

2. Análise do EquationDrug

O EquationDrug ou "Equestre" não é um simples malware desenvolvido para espionagem, é uma plataforma sofisticada que conta com vários recursos desde simples a mais avançados, onde é pré-construído a partir de um conjunto de plug-ins que suportam diversas funções, como screenshot de telas e roubo de arquivos; ele é descendente direto do EquationLaser, primeira plataforma usada pelo grupo para realizar espionagens no Windows 95/98. Porém seu diferencial é a capacidade de obter arquivos criptografados, manipular o firmware do disco e gerenciar plugins, normalmente como forma de ofuscar sua detecção, os processos costumam usar nomes iniciados em *ms* para se camuflar entre arquivos padrões do Windows; o EquationLaser também usava desse tipo de ofuscação.

2.1 Arquitetura do software

A arquitetura da plataforma se assemelha a sistemas como Unix, por se formatar como um mini-sistema operacional, onde possui componentes de modo kernel e modo usuário que interagem entre si de forma cuidadosa através de uma interface personalizada de envio de mensagens. A plataforma conta com conjunto de drivers, um núcleo e vários plug-ins, dessa forma cada plug-in contém um ID exclusivo e um número de versão que a partir disso define quais funções cada ferramenta pode oferecer e quais possuem uma relação de dependência com a outra para funcionar corretamente. Alguns desses módulos são incorporados ao sistema, ou seja, estão integrados a arquitetura e não dependem de outros plug-ins para funcionar, nem de recursos do Windows, também existem drivers que estão vinculados aos plug-ins que não são integrados, para dar suporte e obter melhores resultados no momento de coletar informações.

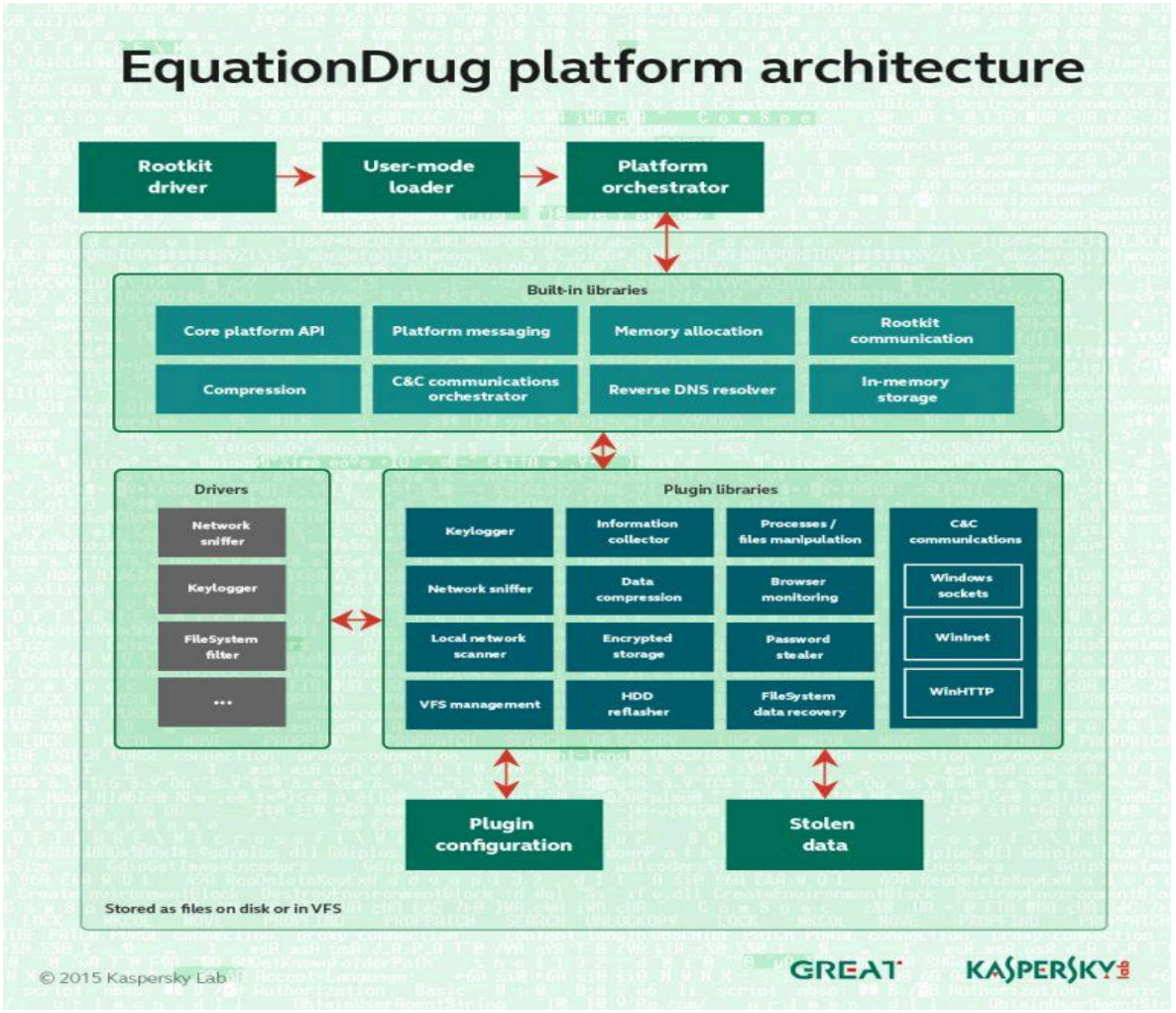

Figura 1 – Arquitetura EquationDrug
Fonte: Karpesky, 2015

Como representado na imagem, o EquationDrug é gerido por 3 componentes, sendo eles, o driver do modo kernel (Rootkit driver), nomeado de *msndsrv.sys* para Windows 2000 ou superior ou de *mssvc32.vxd*, no Windows 9x, já o modo usuário (User-mode loader) normalmente se chama *mscfg32.exe* e por fim o módulo principal (Platform orchestrator), que contém o núcleo e orquestra a execução dos plug-ins: *mscfg32.dll*. Existem outros componentes, que são bibliotecas e drivers adicionais, mas eles só são adicionados de acordo com a necessidade da execução de alguma ferramenta, por serem auxiliares, como é o caso do KeyLogger, que captura as teclas pressionadas pela vítima e em momentos específicos ou em sites que necessitam de autenticação.

Como foi falado, cada plug-in possui um ID exclusivo, esses valores são em formato WORD, como 0x8000, 0x8002, 0x8004 [...], todos iniciam com 0x80 bytes e são IDs em pares. Até o momento foram 30 valores encontrados, onde o ID mais alto foi o 0x80CA, assim podemos calcular que 70 ou mais módulos ainda não foram encontrados caso os desenvolvedores tenham usado incrementação para definir esses IDs, pois em decimal: 0x80CA é igual a 32970, enquanto 0x8000 é 32768, então temos que (32970 -32768 = 202), mas como são apenas os pares, temos que (202 / 2 = 101), se pelo menos 30 já foram encontrados, então ainda restam 101-30 = 71 módulos ou mais ainda não foram reportados.

2.2 Detalhamento técnico dos principais componentes

O módulo do modo kernel e rootkit *msndsrv.sys*, que atua em Windows 2000 ou superior, é um dos 3 principais componentes do mini-sistema da plataforma EquationDrug, ele possui tamanho de 105392 bytes, e sua localização normalmente é na pasta *%System32%\drivers\msndsrv.sys*, ele pode criar arquivos de log em alguns diretórios, que são: *%systemroot%\system32\mslog32.dat* e *%systemroot%\system32\msperf32.dat.* Este driver atua como o primeiro estágio da plataforma no Windows, onde seu objetivo principal é implementar funções de rootkit a fim de ocultar componentes usados pelo malware, quando isso ocorre, ele cria e injeta um código shell em "services.exe" ou "winlogon.exe", esse código shell é projetado para gerar o processo do carregador a partir do executável chamado *mscfg32.exe*. O código do rootkit implementado no drive do modo kernel conecta funções de API nativa, que protegem e ocultam chaves de registro e processos da plataforma em execução.

Já o carregador de modo usuário é um executável de 22016 bytes que inicia a infecção através de Process Hollowing: cria um processo legítimo em estado suspenso (ex: explorer.exe), substitui seu código pela DLL maliciosa (*mscfg32.dll*) e redireciona o ponto de entrada para o payload. Para evasão, emprega ofuscação de strings via XOR com chaves rotativas, falsifica assinaturas digitais usando certificados roubados e utiliza alocação de memória não contígua para evitar detecção heurística. Antes da execução, verifica ambientes de análise através de técnicas como IsDebuggerPresent e inspeção de registry keys específicas para identificar possível debug em máquina virtuais (ex: HKLM\HARDWARE\VBOX_), abortando silenciosamente se detectar risco de exposição.

Enquanto o orquestrador atua como núcleo modular do EquationDrug, gerenciando plugins através de uma tabela de funções LoadPlugin() que carrega DLLs específicas (IDs 0x8000-0x80CA) e fornece APIs para operações de sistema como FileWrite() e NetworkSend(). Implementa comunicação segura com servidores C2 usando criptografia RC6 com chaves de 128 bits e handshake assimétrico RSA-2048 para estabelecimento de sessões. Para persistência, registra-se como serviço com nomes legítimos e armazena configurações criptografadas em *%AppData%\Microsoft\Cryptnet* usando chaves voláteis. Monitora conexões via pacotes de heartbeat a cada 300 segundos e ativa um kill switch ao detectar ferramentas de análise como Wireshark ou Procmon.

```
lea     eax, [ebp+Status]
push    [ebp+NdisProtocolHandle] ; NdisProtocolHandle
mov     [ebp+ProtocolCharacteristics.OpenAdapterCompleteHandler], offset sub_B20779AA
mov     [ebp+ProtocolCharacteristics.CloseAdapterCompleteHandler], offset sub_B20779C2
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_1], offset sub_B207A170
push    eax             ; Status
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_2], offset sub_B2078970
mov     [ebp+ProtocolCharacteristics.ResetCompleteHandler], offset nullsub_2
mov     [ebp+ProtocolCharacteristics.RequestCompleteHandler], offset sub_B20776BA
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_3], offset sub_B20789E4
mov     [ebp+ProtocolCharacteristics.ReceiveCompleteHandler], offset nullsub_1
mov     [ebp+ProtocolCharacteristics.StatusHandler], offset sub_B2077728
mov     [ebp+ProtocolCharacteristics.StatusCompleteHandler], offset nullsub_1
mov     [ebp+var_38], offset sub_B2078B5A
mov     [ebp+var_34], offset sub_B20777B8
mov     [ebp+var_30], offset sub_B2077940
mov     [ebp+var_2C], offset sub_B2077AB8
call    ds:NdisRegisterProtocol
mov     eax, [ebp+Status]
pop     edi
```

Figura 2 – O driver msndsrv.sys captura todo o tráfego de rede usando hooks no kernel.
Fonte: Antiy, 2016

2.3 Principais plug-ins e suas cadeias de ataque

Na plataforma do EquationDrug são mais de 30 plugins descobertos, e outros que ainda não foram descobertos, cada um único e com nomes totalmente diferentes. Dos principais módulos, um dos mais importantes é o plugin 0x8000, o primeiro ID da plataforma, que é incorporado ao sistema, e de extrema necessidade, pois ele é uma API básica que permite a execução de outros módulos. Outro módulo muito importante para o funcionamento da plataforma é o 0x8024, normalmente vem com o nome de *cmib158w.dll,* sua principal função é coletar informações do sistema, como a versão do sistema operacional, o nome vinculado ao computador, nome de usuário, a localização da vítima, o layout do teclado (Capacita melhores respostas de DLLs como KeyLogger), fuso horários e listas de processo em execução.

Outro módulo importante é o 0x8048, que leva o nome de *mstkpr.dll* e é um driver incorporado„ ele realiza análises forenses ao disco e leitor NFTS direto, isso possibilita a busca por conteúdos dentro de HDDs/SSDs da vítima, assim módulos como o 0x8034, conhecido como *cmib456w.dll*, e outros plugins adicionais como o 0x8050 com nome de *khlp760w.dll* realizavam a relação de dependências entre módulos, ou seja, o 0x8048 varria o disco em busca de arquivos criptografados, enquanto os módulos como o 0x8034 coletavam esses arquivos, isso mostra a capacidade do Equation Group, já que obter arquivos criptografados é muito difícil, por ter várias proteções. Ainda existem outras DLLs importantes como o plugin 0x8058 (*khlp733w.dll*) e o plugin 0x807A (*mscoreep32.dll*), que são responsáveis por coletar informações locais do sistema, recuperar senhas armazenadas em cache e monitorar as atividades de navegadores web como Internet Explorer e Mozilla Firefox. Pode-se listar alguns outros, como:

- 0x800A (Embutido), atua como o núcleo de controle remoto do malware, gerenciando a comunicação entre os componentes locais (sniffer, keylogger, filtro de arquivos) e os servidores de comando e controle (C&C);
- 0x80AA (*nls933w.dll)*, responsável por manipular o firmware do HDD/SSD, assim ele pode manter-se no disco silenciosamente;
- 0x80AE (*wpl913h.dll*), módulo responsável pelo KeyLogger, também conhecido como “GROK”, ele monitora as keys e a área de transferência;
- 0x80C6 (*webmgr.dll*), responsável por extrair o histórico web, dados de formulários salvos nos navegadores e credenciais em caches;
- 0x803E (*nls_874w.dll*), um sniffer de rede, analisa e monitora as requisições da rede, como a plataforma wireshark;
- 0x800C (*perfcom.dll*), realiza comunicação HTTP a partir da máquina da vítima, enviando requisições em data;

As informações obtidas por esses módulos são enviadas de diversas formas para os cibercriminosos, desde e-mails, envios FTP e até mensagens em HTTP através de requisições de datas.

2.4 Drivers vinculados aos plug-ins

- ***atmdkdrv.sys***, driver vinculado ao plugin de monitoramento da rede, opera como sniffer de rede (modo padrão) ou patcher de memória (inoperante), selecionado via chave de registro Config2. Como sniffer, captura tráfego direccionado a interfaces

Ethernet/VPN (*ndiswanip*) usando NDIS-4/5, com regras de filtragem configuráveis via IOCTLs (ex: 44038004 para adicionar regras, 80000004 para ativar captura) e armazenamento limitado a 128 pacotes/regra. Como patcher, tenta substituir a ServiceTable de threads por cópia do ntoskrnl.exe (sem funcionalidade prática). Apresenta código desorganizado com três métodos de ofuscação de strings (RC5, cifra alfabética, XOR com RNG) e cria o arquivo *\SystemRoot\fonts\vgafixa1.fon* (modificando seu byte inicial 0x21 para 0x20 na inicialização), enquanto seu nome e dispositivo varia conforme a chave de registro.

- ***msrtvd.sys*** atua como driver do monitor de teclado e área de transferência, criando o dispositivo *\Device\Gk0* e o link simbólico *\DosDevices\Gk* na inicialização. Conecta-se ao processo csrss.exe para desmontar rotinas de user32.dll e ntdll.dll, obtendo índices da SDT de win32k.sys e ponteiros das APIs Nt/Zw, e utiliza um desmontador interno para interceptar funções críticas (*NtUserPeekMessage, NtUserGetMessage, NtUserGetClipboardData*). As rotinas de coleta (armazenadas na seção .msda) capturam teclas pressionadas e dados da área de transferência, anexando timestamp, nome do processo, texto da janela ativa e nome de usuário. Um thread dedicado ("dumper") consolida os dados, compacta-os com LZO e os armazena a cada 30 minutos em *%system-wide TEMP%\tm154o.da*. As strings internas são ofuscadas via XOR com RNG pré-semeados, e IOCTLs (ex: 0x22002C para iniciar o dumper, 0x220034 para verificar novos dados) controlam a operação.
- ***volrec.sys***, é um driver que opera como um filtro genérico de sistema de arquivos, criando o dispositivo de controle *\Device\volrec* e o link simbólico *\DosDevices\volrec0* na inicialização. Conecta-se a todos os dispositivos de sistema de arquivos, incluindo armazenamento removível (USB/FireWire), e monitora eventos como abertura/criação/fechamento de arquivos, operações de leitura/escrita, montagem/desmontagem de volumes e conexão de novos dispositivos. Os eventos são direcionados a plugins de modo usuário, controlados via IOCTLs (0x220004 para configuração da interface e 0x220008 para desativar chamadas). Todas as strings internas são ofuscadas por XOR com gerador de números aleatórios pré-semeados, visando evasão.

Existem muitos outros drivers auxiliando plug-ins que ainda não foram descobertos, como o driver de backdoor acionado por farejador de rede, conhecido como ***mstcp32.sys***, plugin de coletor para volrec, com nome de ***msrstd.sys*** e entre outros.

2.5 Informações vazadas e descriptografia dos arquivos

A atribuição dessas atividades hackers à Agência de Segurança Nacional dos Estados Unidos (NSA), especificamente a unidade Tailored Access Operations (TAO), deve-se à análise de códigos e informações vazadas nos principais processos relacionados ao EquationDrug. É comum em malwares, nas strings de despejo de arquivo vazar informações que possibilitam identificar se um arquivo é malicioso, mas no caso dos módulos dessa plataforma, como o *mstcp32.sys*, que é um módulo responsável por farejar o tráfego de entradas em interfaces Ethernet e VPN, esses vestígios não são deixados, o que mostra um alto desenvolvimento stealth do malware. A maioria dessas strings que deveriam ser exibidas,

são camufladas por criptografia e ofuscação de código, mas podem ser quebradas, e a partir daí é possível obter informações internas do código.

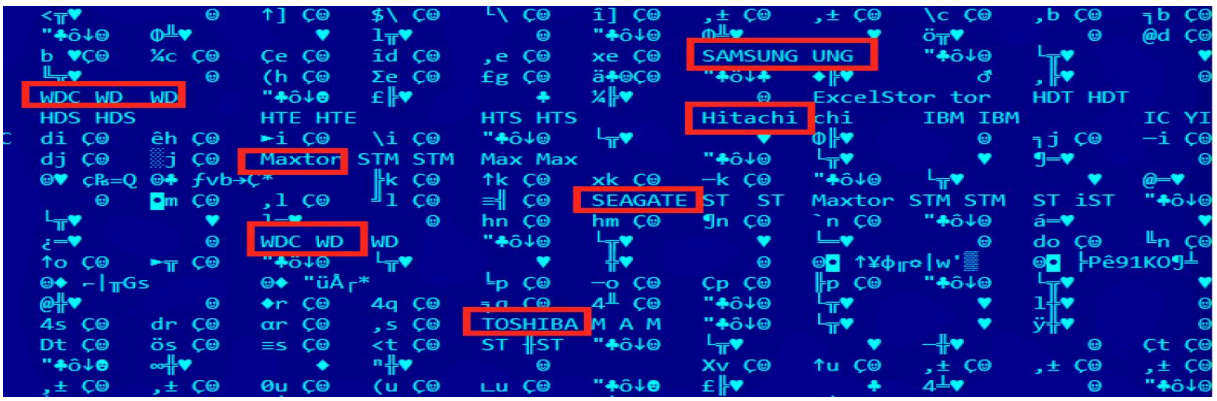

Figura 3 – Vazamento de fabricantes alvos nas strings
Fonte: Karpesky, 2015

Com a quebra dessa criptografia, foi possível associar através dessas strings que esses módulos se tratavam de malwares, pois algumas delas remetiam a ocultações de plugins e remoção de rastros, outras cadeias de texto tinham nomes que não fariam sentido ser do código de sistemas Windows, como: *DRINKPARSLEY, BACKSNARF e Skyhookchow*. Já algumas dessas variáveis foram mais delatoras, um exemplo é a *Dissecorp*, que é Process ID ao contrário; porém o que mais chamou a atenção de quem analisa essas cadeias de caracteres foram os codinomes: *STRAITACID e STRAITSHOOTER*, pois esse prefixo "STRAIT" foi visto em documentos vazados pelo Der Spiegel em 2013, no catálogo ANT (Advanced Network Technology) da NSA, como codinome: *STRAITBAZZARE,* que tinha como objetivo estabelecer acessos remotos e persistentes em redes de computadores comprometidos.

Sobre a análise desses arquivos obteve-se algumas informações como data e hora da compilação dos arquivos, com esses valores agrupados forma-se os horários e datas de trabalho dos desenvolvedores do malware, assim é possível saber aproximadamente de que país são os programadores da plataforma baseado no fuso-horário, no horário comercial coincidentes das compilações e nos feriados nacionais não trabalhados. Essas informações atribuíram o Equation Group ainda mais a NSA, por conflitar com o UTC-4 e UTC-5 presente nos Estados Unidos. Algumas outras informações vazadas também confirmaram o vínculo entre a NSA e o Equation Group, quando em 2017 um grupo de hackers chamados de Shadow Brokers conseguiram obter exploits do EQ no banco de dados da NSA, que estavam em servidores não seguros da agência.

3. Análise do GrayFish

GrayFish é um malware avançado desenvolvido pelo Equation Group entre 2008 e 2013 que serviu como sucessor do EquationDrug e é conhecido por ser quase invisível e extremamente difícil de ser removido. Ele possui a capacidade de se infiltrar no sistema do computador da forma mais indetectável possível para ganhar acesso ao boot do computador, ganhar privilégios administrativos e executar códigos maliciosos para roubo de informações. É compatível com com vários sistemas de firmware e inúmeras versões do windows, seu principal alvo, que eram utilizadas na época dos ataques como o Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, Windows 7 e 8.

3.1 Arquitetura do software

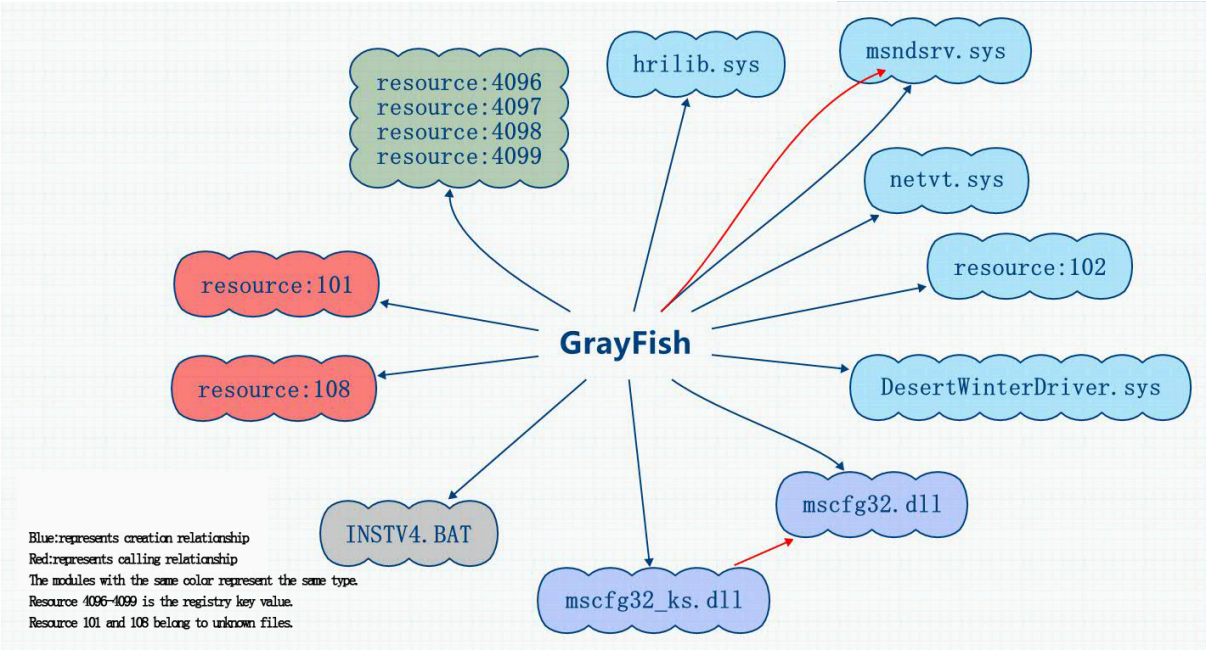

Figura 4 – Principais componentes e recursos do malware GrayFish.
Fonte: Antiy, 2016

O GrayFish, conforme ilustrado na figura acima, é formado por várias partes, incluindo componentes antigos como o driver *msnsrv.sys*, utilizado pelo EquationDrug e descrito em sua análise, também possui muitas melhorias e elementos novos como drivers e scripts além de recursos nativos como libs, arquivos de configuração, ferramentas de espionagem, que serão brevemente apresentados nesta seção.

Primeiramente, além do rootkit, esse malware possui outros drivers, como o *hrilib.sys* que é considerado um dos motivos do GrayFish ser considerado um avanço tão grande comparado com outros softwares maliciosos. A função deste módulo é criar blocos de memória virtual encriptados no banco de dados Registry do Windows, que serve para armazenar informações e configurações importantes para o funcionamento do sistema operacional, e salvar backups do GrayFish nessa memória muito difícil de ser removida aumentando a persistência do malware que, mesmo que seja apagado ainda possui essas cópias. Além disso, esse modo inteligente de guardar arquivos faz que o GrayFish não precise ser armazenado no disco rígido, utilizando apenas o Registry e a memória do computador, o que camufla ainda mais o malware de sistemas de segurança.

Outro driver importante da arquitetura desse sistema é o *DesertWinterDriver.sys*, que serve para expandir o acesso do GrayFish e aumentar as permissões e a área de influência do malware. Primeiramente o driver deve conseguir acesso administrativo, para isso normalmente utiliza de exploits, credenciais e senhas roubadas ou abusando de funções de administrador do Windows. Após conquistar isso, o driver foca em desabilitar mecanismos de segurança como o DSE do Windows, para que os drivers do sistema possam ser executados livremente, burlar o secure boot, capturar e modificar APIs do Kernel, e matar processos de segurança e, dessa forma, o driver permite que o GrayFish opere de forma discreta e quase sem restrições.

Por fim, o último dos drivers principais do GrayFish, o *netvt.sys*. Pouca coisa se sabe deste módulo, somente que ele serve para interceptar a comunicação entre o computador e fontes externas e modificá-las para sabotar comunicações do computador além de se comunicar com os agentes que implantaram o malware. Além dos drivers que servem para criar um ambiente perfeito para o software, o GrayFish possui outros módulos importantes, como o *mscfg32.dll*, o Platform orchestrator também presente no EquationDrug, o *mscfg32_ks.dll* que é o user-mode orchestrator e vários plugins como os resources 101, 102 e 108 que possuem backups e configurações para o malware funcionar propriamente e os resources 4096, 4097, 4098 e 4099 que possuem ferramentas, exploits comandos e informações úteis para o ataque como a versão do sistema operacional e a topologia da rede. O sistema ainda possui o módulo *INSTV4.BAT* que é um script de instalação do malware.

3.2 GrayFish em ação

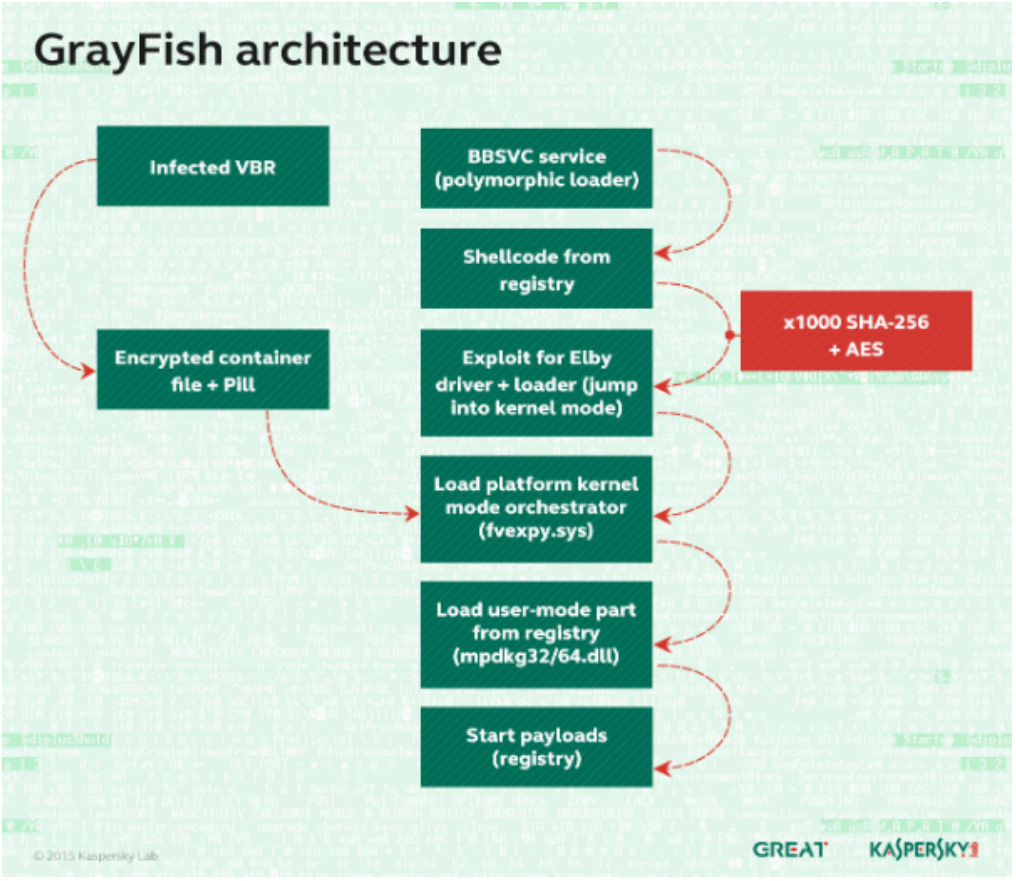

Figura 5 – Como o GrayFish se infiltra no sistema
Fonte: Kaspersky, 2015

Primeiramente, após o GrayFish entrar em um computador ele utiliza de exploits para conseguir acessar o modo kernel e posteriormente acessar o sistema Registry do Windows, onde o script *INSTV4.BAT* é executado e o processo de instalação é iniciado, após esse processo o script automaticamente se auto deleta. Nesse ponto o *mscfg32.dll* é carregado e com isso carrega todos os drivers maliciosos do malware na memória, e cada um deles começa a operar. A Partir desse ponto o hrilib.sys armazena o GrayFish no registry fazendo que o software só atuasse nesse banco de dados e na memória principal, o *msndsrv* é carregado escondendo processos e arquivos desabilitado medidas de segurança e garantindo

que o malware não será detectado, o *DesertWinterDriver* expande o acesso e as permissões do Software malicioso enquanto o *netvt* intercepta comunicações e manda mensagens para o grupo que iniciou o ataque.

Enquanto as instalações acontecem, o GrayFish também infecta o MBR do disco rígido alterando o Boot Manager da máquina. Desse ponto em diante, todas as vezes que o Windows for ligado o Boot Manager alterado irá injetar um ponteiro criptografado no primeiro driver não malicioso carregado, ele será descriptografado e o conteúdo de sua localização será carregado na memória. Esse ponteiro aponta para o bloco do Registry em que o *mscfg32.dll* está armazenado e quando esse módulo estiver na memória ele irá carregar todos drivers e plugins do GrayFish para o malware continuar escalando em permissões e coletando informações de forma imperceptível.

4. Fanny: A Ferramenta do Equation Group Que Conecta Mundos Isolados

O malware Fanny, uma das mais intrigantes ferramentas descobertas no arsenal do notório Equation Group, exemplifica a sofisticação e a furtividade empregadas em operações de ciberespionagem de alto nível. Sua relevância não se limita à sua capacidade operacional, mas se estende à sua função singular e à sua inesperada conexão com um dos mais infames malwares da história: o Stuxnet.

A principal função do Fanny ia muito além do roubo de dados convencional; ele foi meticulosamente projetado para mapear e coletar informações sobre a topologia de redes "air-gapped". Essas redes, fisicamente isoladas da internet, são a espinha dorsal da segurança em ambientes críticos como instalações militares, usinas nucleares e laboratórios de pesquisa. A barreira física que as protege representa um desafio significativo para invasores, e o Fanny foi a solução do Equation Group para superá-la.

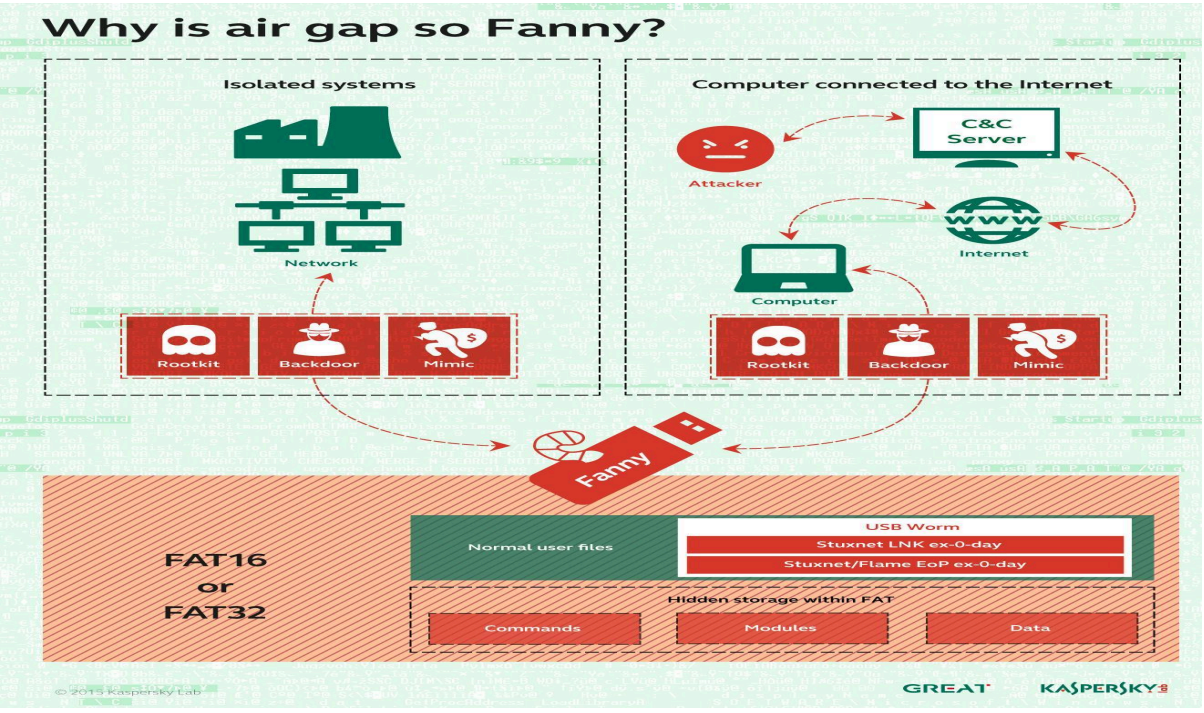

Figura 6 – Funcionamento do Fanny
Fonte: Kaspersky, 2015

Sua disseminação ocorria por meio de pendrives (USB). Quando um dispositivo USB infectado era conectado a um computador dentro de uma rede isolada, o malware operava em segundo plano, coletando discretamente informações vitais sobre a estrutura da rede, incluindo nomes de sistemas e topologia. O gênio por trás do Fanny estava em seu método de comunicação secreta: as informações coletadas eram armazenadas em uma área oculta do próprio pendrive. Dessa forma, se o mesmo pendrive fosse posteriormente conectado a um computador com acesso à internet, o Fanny atuava como uma ponte invisível, transmitindo os dados coletados para os servidores de comando e controle do Equation Group. Inversamente, essa mesma metodologia permitia que os operadores enviassem comandos para a rede isolada, transformando o humilde pendrive em um mensageiro bidirecional.

Normalmente, a vítima conecta um novo pendrive e o abre com o Windows Explorer, neste momento é possível observar visualmente os dois estágios da infecção a partir do pendrive, que levam segundos para serem executados mesmo que o Autorun (Funcionalidade do windows que executa automáticamente a instalação de arquivos através de unidades de armazenamento externas) tenha sido desativado. Conhecendo o famoso arquivo **fanny.bmp**.

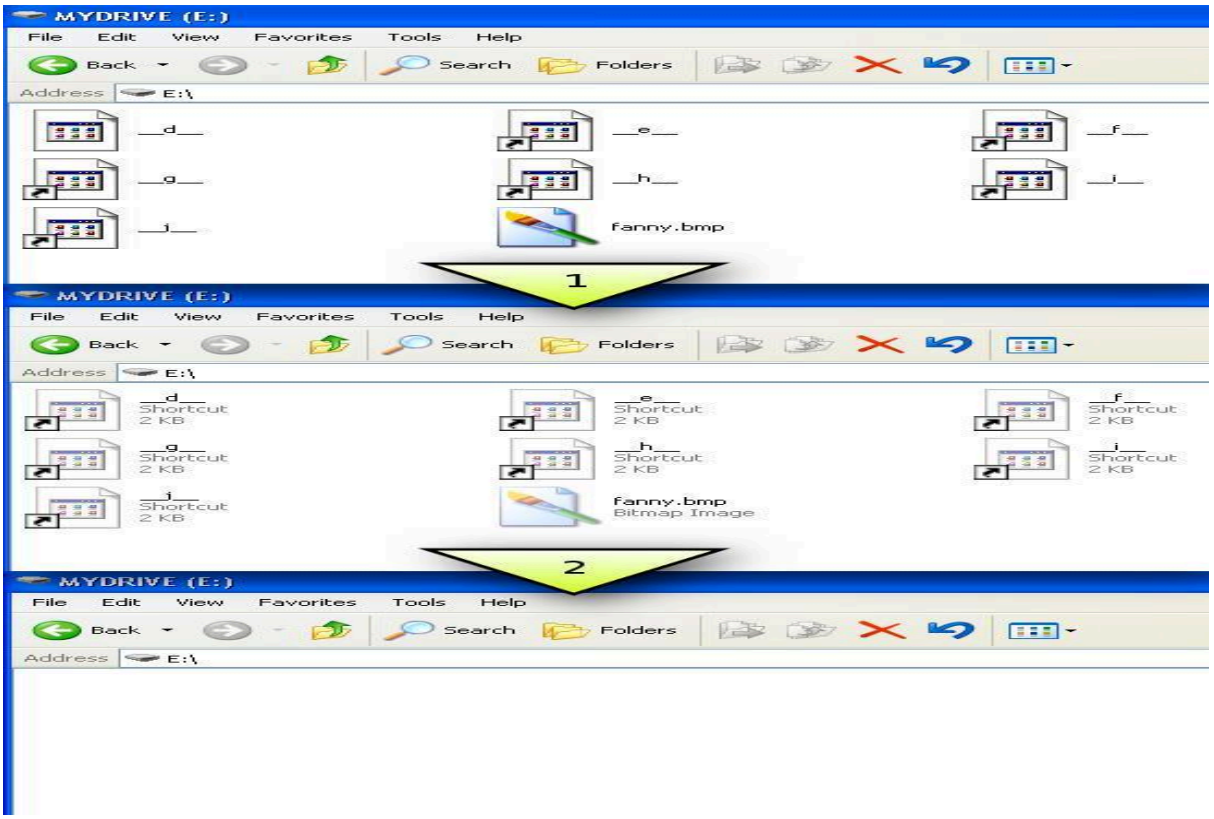

Figura 7 – Funcionamento fanny.bmp
Fonte: Kaspersky, 2015

Uma descoberta crucial da empresa russa Kaspersky Lab, revelou que, já em 2008, o Fanny utilizava duas das mesmas vulnerabilidades de dia zero que seriam, posteriormente, incorporadas ao Stuxnet em 2009 e 2010, a chamada "Stuxnet Vulnerability LNK". Essa sobreposição tecnológica foi um divisor de águas para a comunidade de segurança, estabelecendo uma ligação técnica sólida entre o Equation Group e o Stuxnet. O fato de o Equation Group ter tido acesso a essas vulnerabilidades antes do Stuxnet não apenas sugere

uma posição de superioridade em termos de capacidade ofensiva, mas também aponta para uma possível colaboração ou compartilhamento de recursos entre os grupos por trás dessas operações complexas.

Em essência, o Fanny é uma ferramenta de reconhecimento altamente especializada, uma verdadeira inovação projetada para transpor uma das maiores barreiras de segurança: o isolamento físico. Ele serviu como uma ponte vital de informações entre o mundo online e redes críticas offline, e sua descoberta foi uma peça-chave que ajudou a desvendar a teia de conexões entre o Equation Group e outras operações de ciberespionagem de alto nível, redefinindo nossa compreensão sobre a sofisticação e a interconexão das ameaças cibernéticas estatais.

4.1 Conclusão sobre o Fanny

O principal aprendizado é que nenhuma rede é verdadeiramente isolada. A concepção de "air gap", embora fundamental para a segurança de infraestruturas críticas, não é infalível. A exploração de vulnerabilidades em mecanismos aparentemente inofensivos, como arquivos de atalho, combinada com táticas astutas de engenharia social e o uso de dispositivos removíveis, demonstra que o ponto mais fraco em qualquer sistema pode ser o elo humano ou a confiança em funcionalidades básicas do sistema operacional.

Outro impacto significativo para o estudo da cibersegurança é a necessidade de uma abordagem mais proativa e preditiva. A dependência de "zero-days" por grupos como o Equation Group e em operações como o Stuxnet sublinha que as defesas ativas baseadas em assinaturas são insuficientes. É imperativo investir em pesquisa de vulnerabilidades, inteligência de ameaças e em soluções que possam detectar comportamentos anômalos, mesmo que a vulnerabilidade específica seja desconhecida.

Em suma, os casos do Stuxnet e do Fanny servem como um lembrete contundente de que a cibersegurança é um campo em constante evolução, onde a adaptabilidade e a inovação dos defensores devem espelhar a dos atacantes. A persistência na busca por vulnerabilidades, a criatividade na engenharia de ataques e a habilidade de operar furtivamente em ambientes altamente seguros são os desafios que definem o cenário atual e futuro da proteção cibernética.

5. Marcos e impactos globais

O Equation Group, trouxe marcos importantes para a evolução dos malware, o desenvolvimento de plataformas como Funny possibilitaram grande ciberataques como o *StuxNet* em 2010, esse mesmo grupo também descobriu e guardou informações sobre zero-days vinculados ao Windows como o *EternalBlue* (CVE-2017-0144), que possibilitou desenvolvimento de ransomware como *WannaCry* e *NotPetya*, que foram divulgados em 2017 no vazamento da Shadow Brokers. E esses marcos, com o tempo, se tornaram um tanto controversos já que por ser um grupo claramente vinculado à NSA, ela escolheu guardar falhas críticas para si mesmo como um “arsenal” ao invés de reportá-los para serem corrigidos. A própria Microsoft comparou os vazamentos de informações da agência americana a “mísseis tomahawk roubados”, pois a ameaça de vazamento dos dados ficou em pauta por dias, e mesmo assim a estatal americana não a notificou antes que as informações fossem vazadas. Grupos chineses (*APT3/Buckeye*) e russos (*APT28*) reutilizaram o

EternalBlue antes mesmo da divulgação pública, indicando vigilância prévia ou novos vazamentos; mesmo quase 10 anos depois, milhões de máquinas ainda são vulneráveis a essa falha, por patchs de atualização não conseguirem chegar a diversos computadores devido a sistemas antigos

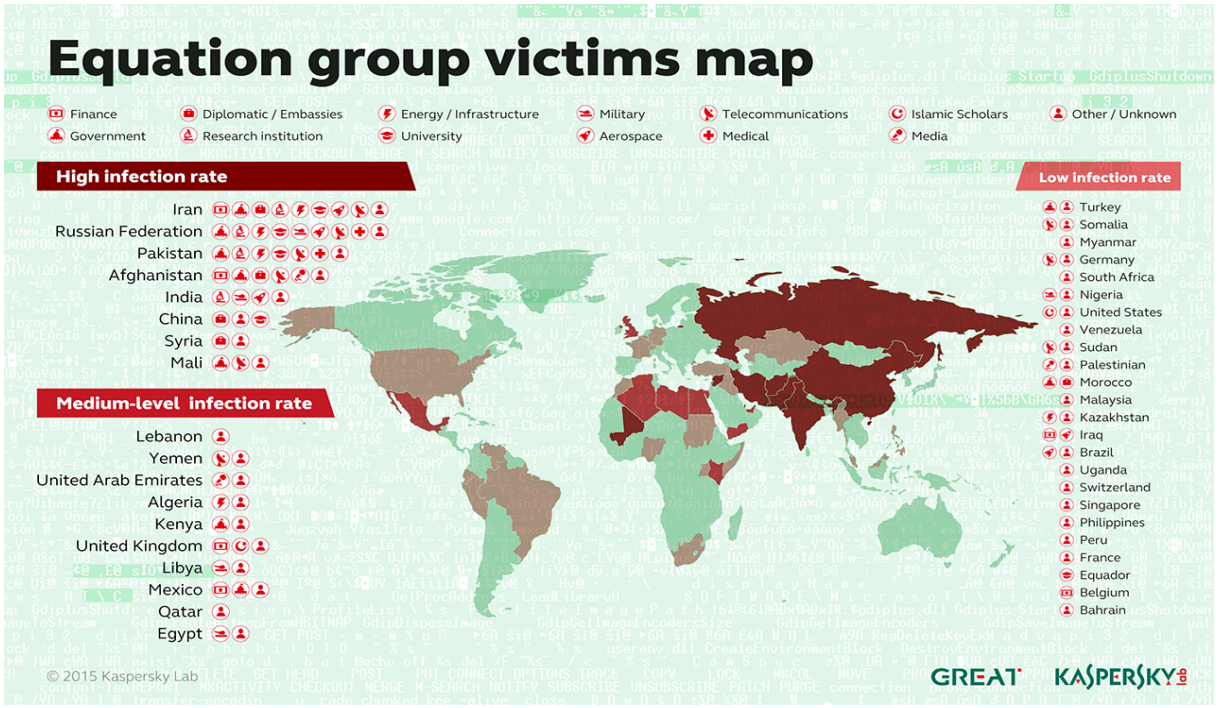

Figura 8 – Alvos do Equation Group
Fonte: Karpesky, 2015

Ainda dentro dos marcos impostos pelo Equation Group, um dos mais importantes, se não o mais importante é a manipulação de firmware, que garantiu total dominância no roubo das informações de outros países. Tornou-se muito difícil descobrir se um computador estava infectado com uma ferramenta de espionagem, com a manipulação do firmware o malware se tornou tecnicamente indestrutível, mesmo formatando o disco o vírus não saia dos HDDs/SSDs, já que a plataforma maliciosa substitui o firmware original por um modificado, onde ele utiliza comandos ATA não documentados para carregar código malicioso na memória flash do disco e criar setores ocultos e inacessíveis ao sistema operacional. Com isso o malware podia alocar um espaço de aproximadamente 30 MBs que armazenaria plataformas como *EquationDrug* ou *GrayFish*; esse particionamento seria invisível mesmo para ferramentas de diagnóstico como CHKDSK e formatações de baixo nível; alguns casos relatam de servidores de universidades chinesas afetados por essa técnica, além de um servidor no Irã que ficou mais de 5 anos infectado.

6. Conclusão

O Equation Group estabeleceu um paradigma irreversível na guerra cibernética estatal, fundindo inovação técnica extrema com estratégias geopolíticas de espionagem. Suas operações, documentadas ao longo de três décadas, redefiniram os limites da persistência e furtividade em APTs, evidenciados nas arquiteturas modulares de *EquationDrug* e *GrayFish*. Estas plataformas empregavam persistência via firmware em HDDs/SSDs (contornando formatações), rootkits de modo kernel (*msndsrv.sys*) e comunicação encoberta com criptografia RC6/RSA-2048, garantindo infiltração em alvos estratégicos como Irã, China e Rússia para espionar programas militares e infraestruturas críticas.

A atribuição à NSA, sustentada por codinomes vazados (*STRAITACID*) e padrões operacionais alinhados ao fuso EST, expõe o papel de agências estatais na militarização do ciberespaço. Ferramentas como *Fanny* — capaz de transpor redes air-gapped via USB e compartilhar zero-days com o *Stuxnet* — ilustram a sofisticação ofensiva do grupo. Contudo, seu legado é ambíguo: o acúmulo estratégico de vulnerabilidades (*EternalBlue*) pela NSA, não reportadas para correção, desencadeou crises globais (*WannaCry*) e deixou milhões de sistemas expostos.

Este caso demanda uma reestruturação urgente na cibersegurança: defesas preditivas que detectem anomalias além de assinaturas, governança transparente de falhas por agências governamentais e resiliência reforçada em infra estruturas isoladas. O Equation Group não é apenas um marco técnico, mas um alerta perene: em uma era onde estados armazenam vulnerabilidades como arsenal, a segurança coletiva depende da capacidade de antecipar — não apenas reagir — à próxima geração de ameaças.

Referências

DAVIES, A. Inside the EquationDrug Espionage Platform. **Securelist by Kaspersky**, 2015. Disponível em <https://securelist.com/>. Acesso em: 28 jun. 2025.

CONSTANTIN, L. Code name found in Equation group malware suggests link to NSA. **CIO**, 2015. Disponível em <https://www.cio.de/article/>. Acesso em: 29 jun. 2025.

GREAT. Equation: The Death Star of Malware Galaxy. **Securelist by Kaspersky**, 2015. Disponível em <https://securelist.com/>. Acesso em: 29 jun. 2025.

BARANOV, A. EquationDrug rootkit analysis (mstcp32.sys). **Artemon Security**, 2017. Disponível em <https://artemonsecurity.blogspot.com/>. Acesso em: 29 jun. 2025.

GREAT. Equation Group: Questions and Answers. **Kaspersky**, 2015. Disponível em <https://media.kasperskycontenthub.com/>. Acesso em: 29 jun. 2025.

AL-BASSAM, M. Equation Group firewall operations catalogue. **Mustafa Al-Bassam's blog**, 2016. Disponível em <https://musalbas.com/blog/>. Acesso em: 30 jun. 2025.

ANTIY LABS. A TROJAN THAT CAN MODIFY THE HARD DISK FIRMWARE — A Discovery to the Attack Components of the EQUATION Group. **Antiy Labs**, 2016. Disponível em <https://www.antiy.net/>. Acesso em 02 jul. 2025.

GOODIN, D. How “omnipotent” hackers tied to NSA hid for 14 years—and were found at last. **Ars Technica**, 2015. Disponível em <https://arstechnica.com/>. Acesso em: 03 jul. 2025.

GREAT. A Fanny Equation: “I am your father, Stuxnet”. **Securelist by Kaspersky**, 2015. Disponível em <https://securelist.com/>. Acesso em: 03 jul. 2025.

How does fanny computer worm work?. **Web Orion**, 2016. Disponível em <https://theweborion.com/blog/fanny-worm/>. Acesso em: 03 jul. 2025.

Worm "Fanny", Equation Group e Stuxnet. **Under-Linux.org**, 2015. Disponível em <https://under-linux.org/>. Acesso em: 03 jul. 2025.

APT Group: Equation Group (APT-Q-91). **Qianxin Threat Intelligence Center**, 2015. Disponível em <https://ti.qianxin.com/apt/>. Acesso em: 04 jul. 2025.