A Atuação do Equation Group no Âmbito da Ciberespionagem

Victor Conde, Marina Sales, Leandro Silva, João Marins
vddc@cin.ufpe.br, mrs5@cin.ufpe.br, lvrs@cin.ufpe.br, jpbm@cin.ufpe.br
LSEC – Liga de Cibersegurança

Resumo
Este documento discorre sobre o Equation Group, uma organização de APT (Ameaça Persistente Avançada) especializada em exploração de redes de computadores. Por meio de métodos variados, seus membros são considerados os 'deuses da ciberespionagem', devido ao uso de ferramentas extremamente sofisticadas. Neste documento, abordamos um pouco da multiplicidade dos seus ataques e locais de atuação, aprofundando de forma técnica em alguns tópicos.

Palavras-chave: Equation Group. Ciberespionagem. Cibersegurança.

Introdução

O Equation Group possui um dos níveis mais elevados de sofisticação já observados na ciberespionagem. Eles estão envolvidos em diversos ataques que, segundo o Kaspersky Lab, uma multinacional russa especializada em segurança cibernética, remontam ao ano de 2001, e possivelmente até mesmo 1996. Essa estimativa é dada a partir do primeiro implante utilizado pelo grupo, o EquationLaser, ativo entre 2001 e 2004 e compatível com versões como Windows 95 e 98. A atribuição pública mais recente do grupo a uma operação foi em 2022, quando foram acusados de cometer um ataque a uma universidade politécnica da China.

O nome conferido ao grupo vem de sua preferência por algoritmos de criptografia e estratégias de ofuscação. O grupo tem personalizações de algoritmos de criptografia em seus módulos como o RC5, que é um algoritmo de bloco simétrico. Seus módulos mais recentes utilizam algoritmos como RC6, RC4 e AES, além de hashes criptográficos e outras funções análogas.

Através de uma pesquisa aprofundada, a Kaspersky Lab conseguiu identificar a existência do grupo durante uma pesquisa sobre a operação "Regin", em 2014. Para isso, foi utilizado um computador situado no Oriente Médio, o qual foi apelidado de "imã de ameaças". Analisando a infecção pelo Regin nesse computador, eles analisaram um módulo que não fazia parte da infecção por esse malware e nem a qualquer outro APT conhecido. Investigando o módulo mais a fundo, descobriram a plataforma EquationDrug. Além dessa plataforma, outras também foram atribuídas ao grupo através do estudo de análises estatísticas, correlação e pivoteamento baseado em C&C.

O objetivo principal do grupo é a exploração de redes de computadores (CNE - Computer Network Exploitation) com finalidade de espionar e obter inteligência. Seus membros possuem ferramentas que operam com bastante persistência e habilidade de permanecer imperceptível. Um de seus implantes de malware mais moderno é o GrayFish, que tem a capacidade de armazenamento oculto e executar comandos maliciosos no Windows. Sua capacidade de permanecer indetectável por um período longo o torna crucial para operações de espionagem realizadas pela organização.

O grupo tem uma preferência por alvos de alto valor, como instituições governamentais, diplomáticas, instituições financeiras e militares, justamente por serem estas portadoras de diversos dados sensíveis que podem ter um grande impacto geopolítico.

Histórico e Impacto

A evolução das capacidades ofensivas em cibersegurança atingiu patamares alarmantes com grupos desenvolvendo arsenais digitais com complexidade notável. O Equation Group representa uma ameaça para a cibersegurança mundial. Agindo nas sombras, o enigmático grupo força organizações a estarem alerta e a investirem constantemente em suas tecnologias. As infecções do grupo foram observadas em pelo menos 42 países espalhados pelo globo e o número de vítimas estimadas está na casa das dezenas de milhares. Em 2015, o Kaspersky Lab divulgou a investigação que apontou mais de 60 alvos dos quais o grupo teria direta responsabilidade, e alguns datados do final do século passado.

No ano de 2010, a empresa bielorrussa VirusBlokAda descobriu algo que mudou a percepção de ciberataques que existia na época: um sistema operacional desenvolvido pela Siemens foi alvo de um malware que mais tarde ficou conhecido como Stuxnet. Esse malware era especificamente um worm que realiza um ataque do tipo "man-in-the-middle" em computadores responsáveis por sistemas de controles industriais. Seu objetivo era danificar máquinas e equipamentos, e seus alvos principais foram centrífugas de enriquecimento de urânio iranianas. Embora a autoria deste não seja creditada ao Equation Group, o que se descobriu foi que um dos exploits (CVE-2010-2568) usados pelo Stuxnet para invadir os computadores através de conexões USB's já havia sido utilizado antes em um malware conhecido como Fanny, este creditado explicitamente ao Equation Group, que era ainda mais pervasivo. Acredita-se que tenha havido colaboração direta entre os supostos grupos. Independentemente dos objetivos específicos por trás do ataque, ele demonstrou a capacidade destrutiva e de infiltração do grupo o que acionou um alerta mundial e direcionou os holofotes para o Equation.

Em 2012, outro ataque foi descoberto, e posteriormente vinculado ao Equation Group, dessa vez o malware Flame, supostamente em atividade desde 2007. Este, que se destaca por sua capacidade massiva de coleta, redirecionava documentos, áudios, vídeos, informações compartilhadas por bluetooth, modelos 3D CAD (Computer-Aided Design), e informações de arquitetura e senha de redes das máquinas infectadas para os atacantes, chegando até a gravar o áudio de microfones conectados e fazer capturas de tela com total anonimato. Segundo o Kaspersky Lab, que também foi um dos responsáveis por catalogar esse ataque, os traços que aproximam o Flame do Equation são as plataformas de desenvolvimento e as vulnerabilidades exploradas, o que torna provável que exista uma conexão forte entre os grupos.

Os incidentes de alto perfil supracitados tiveram alvos parecidos, países do oriente médio, principalmente o Irã. A autoria desses ataques é um ponto levantado extremamente importante, pois o nível de complexidade dos "projetos" não é comumente atribuído a grupos pequenos, principalmente pelo caráter da aplicação, espionagem e sabotagem. Geralmente esse é um feito atribuído às grandes nações devido ao grau tecnológico e ao investimento necessários. Em 19 de Junho de 2012, o jornal The Washington Post publicou uma matéria atribuindo a autoria de ambos, Stuxnet e Flame, à uma ação conjunta dos Estados Unidos e Israel na busca por atrapalhar o desenvolvimento nuclear do Irã, tese corroborada por um ex-oficial de inteligência dos EUA. Tais acontecimentos evidenciam a crescente militarização do ciberespaço, transformando todo o cenário da segurança mundial. Os incidentes ocorridos na última década serviram como um catalisador, impulsionando as nações a investirem alto em suas defesas e capacidades ofensivas cibernéticas.

No dia 13 de agosto de 2016, um ano após o grupo ter sido descoberto pela Kaspersky Lab, o grupo anônimo de hackers autoproclamado "Shadow Brokers" anunciou publicamente que havia invadido o sistema da Agência de Segurança Nacional (NSA) dos Estados Unidos, conseguindo acesso ao código fonte de diversos malwares

utilizados pelo Equation Group, e que estava disposto a comercializar as armas cibernéticas para inimigos do governo americano.

Para tal, os Shadow Brokers criptografaram os arquivos descobertos para que só fossem acessados mediante o pagamento de ₿1.000.000,00 (um milhão de bitcoins), valor equivalente a aproximadamente meio milhão de dólares à época.

Em abril de 2017, em resposta a um ataque contra um campo de aviação sírio por parte do governo americano, os Shadow Brokers divulgaram a senha para arquivos criptografados divulgados no ano anterior.

O conflito entre ambos os grupos continuou por meses, visto que os Shadow Brokers continuaram a divulgar material confidencial pertencente ao Equation Group. A disputa culminou com a divulgação do exploit Eternal Blue, que tem como alvo uma falha, denominada CVE-2017-0144 no protocolo SMBV1 utilizado nos sistemas Windows. O Eternal Blue se aproveita de bugs internos no SMBV1. Entre eles, há um erro matemático, que leva a um estouro de buffer, e diversas falhas na alocação de memória, as quais tornam possível para os invasores controlarem o sistema. Em maio de 2017, o famoso ataque do ransomware WannaCry se utilizou do exploit para ser disseminado, tornando-se um marco na história dos ciberataques a nível global.

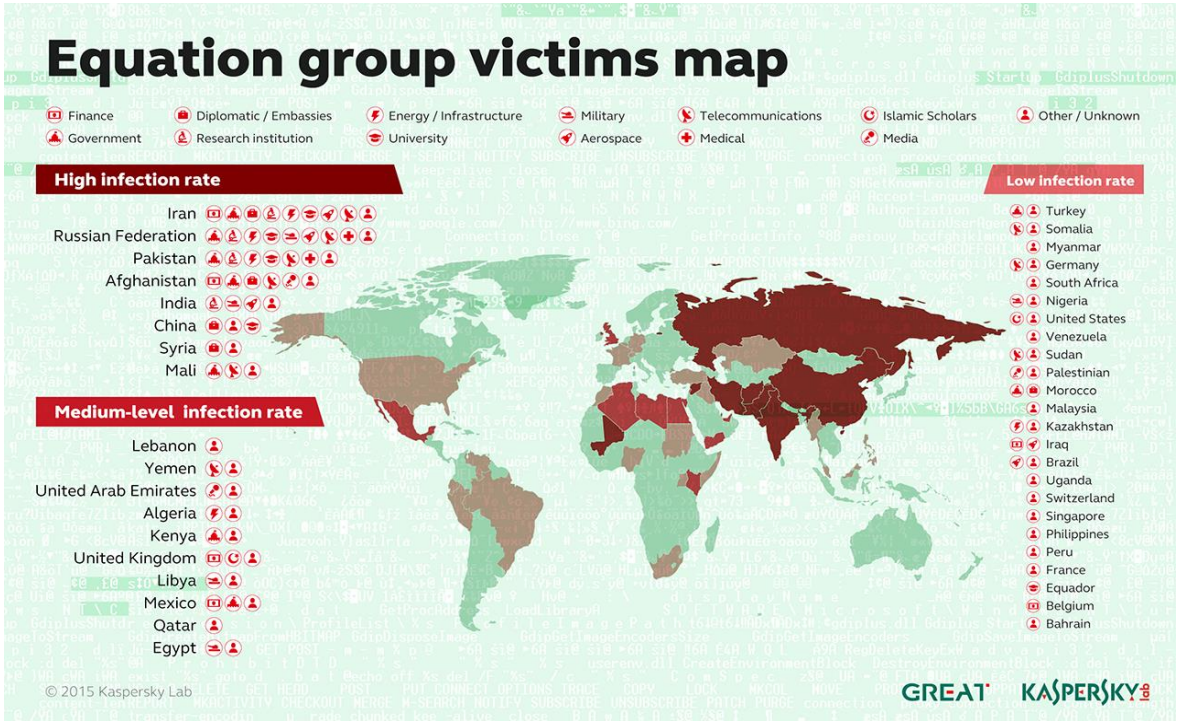

Figura 1: Mapa geral dos ataques do Equation Group

Ferramentas Utilizadas

Ao descobrir a existência do grupo em 2014, a Kaspersky Lab apresentou o Equation Group para o mundo. Dentre outras inovações, a capacidade dos membros do Equation de infectar o firmware do disco rígido rendeu-os a fama de 'deuses da ciberespionagem', visto que tal habilidade permite invadir diretamente o sistema operacional de uma determinada máquina e acessar os dados nela armazenados. Em 2016, um grupo autodenominado "Shadow Brokers" tornou públicos os exploits utilizados pelo grupo, revelando assim umas de suas armas mais poderosas.

Muitos ataques realizados pelo grupo se deram através do backdoor "Bvp47", nomenclatura conferida pelo grupo chinês Pangu Lab. De acordo com a organização,

esse artifício foi extraído de sistemas Linux e possui sistemas de autodestruição, ofuscação de código e um canal encoberto baseado em pacotes TCP SYN. Além disso, a possibilidade do invasor se utilizar desse backdoor de forma remota para invadir uma máquina torna o Bvp47 uma ferramenta ainda mais poderosa.

Malwares

- DoubleFantasy: plugin utilizado para validação das vítimas; é aplicado antes de outros malwares para assegurar que a vítima é de fato um alvo atrativo para o grupo.
- EquationDrug: após o DoubleFantasy validar a vítima, o EquationDrug é responsável por dar ao hacker total controle do sistema operacional da máquina da vítima. Caso as funcionalidades básicas da plataforma não sejam suficientes num ataque específico, plugins podem ser adicionados para garantir um ataque bem-sucedido.
- GrayFish: desenvolvido entre 2008 e 2013, o GrayFish é o mais invasivo e inovador malware desenvolvido pelo Equation. Após a infecção, o computador passa a ser controlado pelo próprio GrayFish, o qual, através de um mecanismo de etapas encadeadas, determina quando a máquina infectada irá iniciar. Além disso, sua habilidade de passar desapercebido pelos mecanismos de segurança também garante ao malware grande distinção em relação não só às ferramentas desenvolvidas pelo próprio Equation, mas também aos recursos até então concebidos no mundo da cibersegurança. O GrayFish é considerado um *bootkit* altamente sofisticado, sendo considerado mais complexo do que qualquer outro já visto, o que indica que seus desenvolvedores têm um altíssimo nível. Os principais mecanismos de infecção são via exploits baseados na web, dispositivos usb com exploits e outros métodos. Quando o computador inicia, o GrayFish se apropria dos mecanismos de carregamento do sistema operacional injetando o seu código no registro de inicialização, o que faz com que o computador não execute por si, mas sim o GrayFish que vai executar passo a passo e fazer as alterações necessárias durante esse processo, no Windows ele vai executar o sistema através de um mecanismo de múltiplas etapas aonde ele vai descriptografar e executar seu código no ambiente Windows, cada um desses estágios decodifica e executa o próximo, O loader da primeira etapa do GrayFish calcula o hash SHA-256 do ID da pasta do sistema de arquivos NTFS do diretório do Windows da vítima. Este hash, juntamente com o ID do objeto, é usado como uma chave de descriptografia AES para o próximo estágio, o que dificulta mover o malware para outra máquina já que ele está diretamente ligado a máquina infectada, sendo necessário o ID do NTFS correto para a descriptografia. Se houver qualquer erro nessa inicialização a plataforma GrayFish se autodestrói para evitar a sua detecção. Para conseguir armazenar as informações auxiliares do código e o seu sistema de arquivos virtual criptografado, o GrayFish vai manter isso dentro do registro do Windows o que não torna necessário ter módulos executáveis maliciosos e para contornar os mecanismos de segurança moderna ele pode explorar drivers legítimos com vulnerabilidades conhecidas.

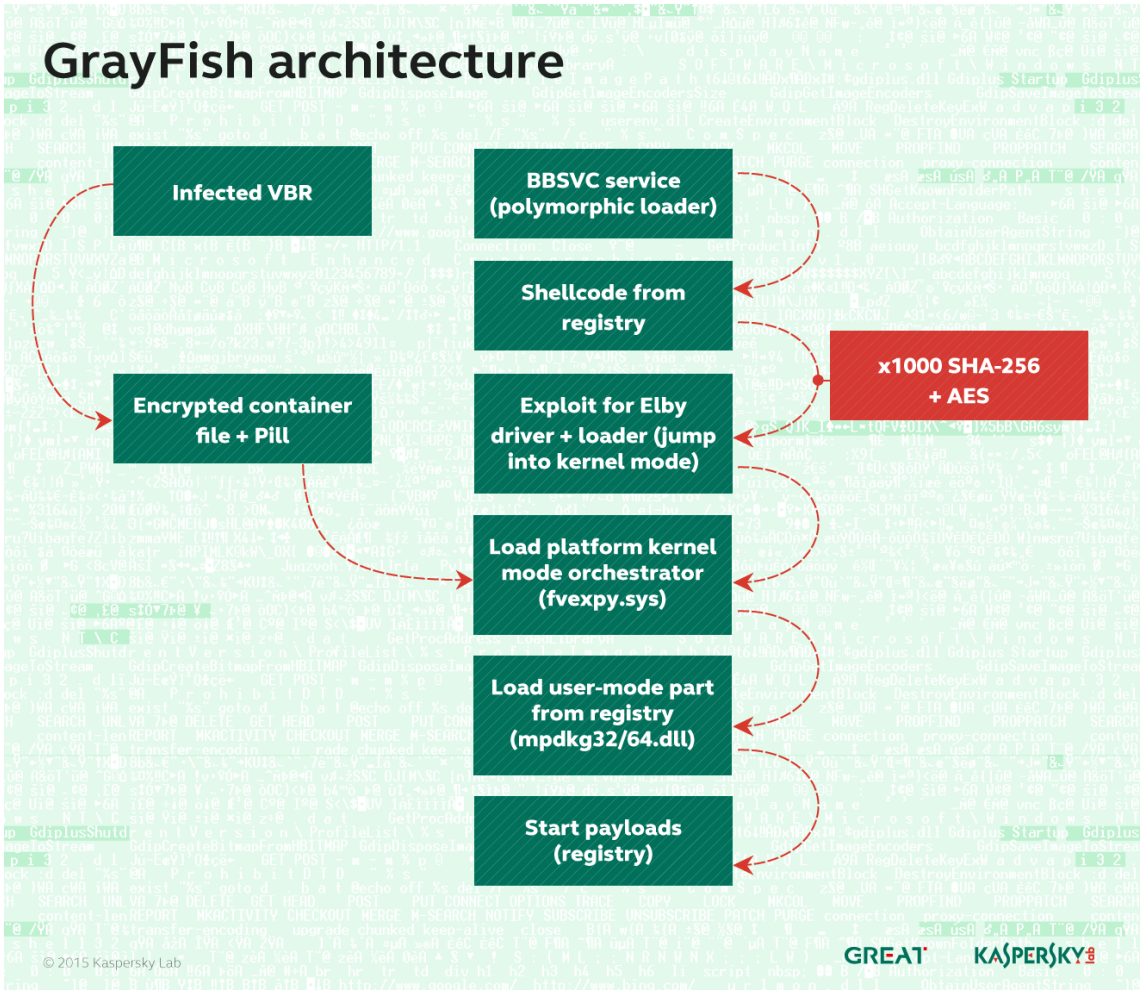

Figura 2: Ciclo de infecção do GrayFish

- Fanny: o diferencial do Fanny consiste na capacidade de invadir redes com lacuna de ar (air gapped networks). Comumente espalhado através de pen drives infectados, esse *worm* de computador acessa os dados de uma máquina que não possui acesso à internet e, ao ser conectado a um computador que tenha esse acesso, envia os dados descobertos aos invasores.

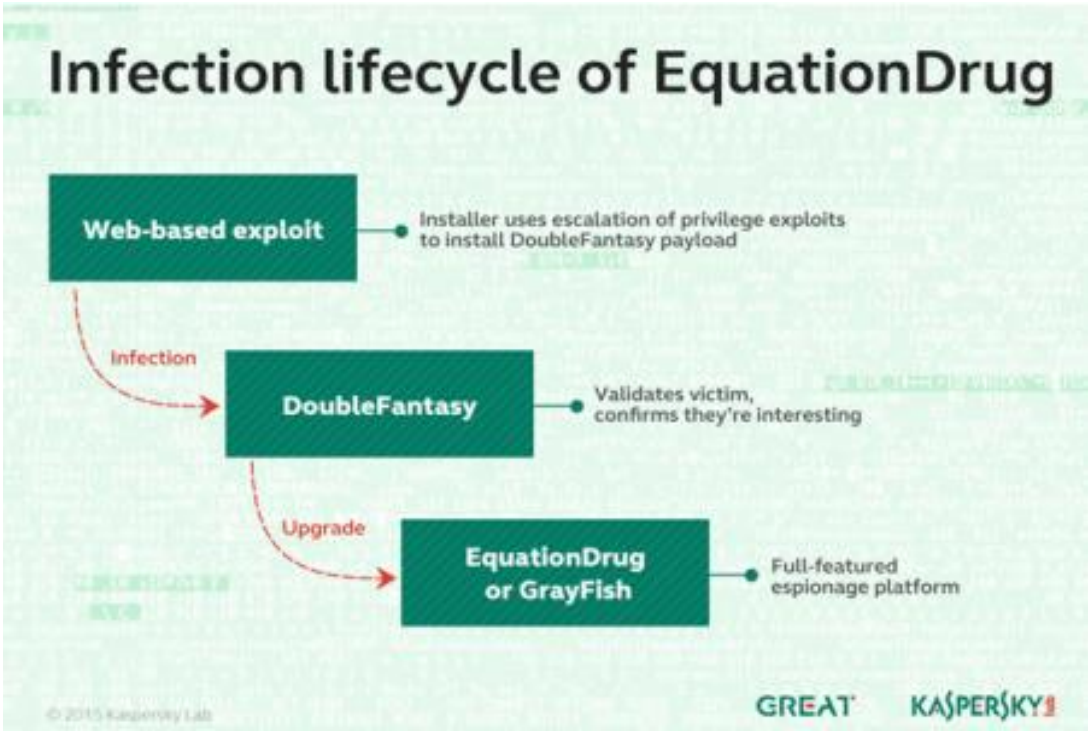

Figura 3: Ciclo de infecção do EquationDrug

Exploits

- Exploits de Elevação de Privilégio no Kernel do Windows: São quatro exploits diferentes de escalonamento de privilégio documentados no boletim de segurança da Microsoft MS09-025. Essas vulnerabilidades foram identificadas após serem usadas como *zero-day* em um dos primeiros ataques direcionados a máquinas industriais CLP. O malware do tipo Stuxnet utilizava esses exploits para assumir o controle do computador e se espalhar pela rede interna em busca de máquinas com o software Siemens STEP 7, responsável pela programação e controle de CLPs. Quando encontrado, o vírus instalava código malicioso tanto no CLP quanto no programa STEP 7. Caso o software não estivesse presente, o vírus permanecia inativo.

- Execução Remota de Código via TrueType Font (CVE-2012-0159 e CVE-2013-3894):
  Esses exploits exploravam uma vulnerabilidade na interpretação de arquivos de fonte TrueType (TTF). A falha poderia ser explorada quando o usuário carregasse uma fonte maliciosa, por exemplo, ao visitar um site que utilizasse fontes externas, caso o navegador estivesse configurado para baixá-las automaticamente. A exploração permitia execução remota de código, possibilitando inclusive a criação de um usuário com privilégios administrativos no sistema.

- Execução Remota de Código via Ícones de Atalhos (CVE-2010-2568): Este exploit explorava uma vulnerabilidade no Windows Explorer, permitindo a execução remota de código por meio de arquivos de atalho

(.LNK). O principal vetor de infecção era o uso de pen drives: se a função de "Reprodução Automática" estivesse ativada, o sistema carregava automaticamente o ícone do atalho, iniciando o exploit. Essa vulnerabilidade também foi explorada pelo Stuxnet.

- Execução Remota de Código via Internet Explorer (CVE-2013-3918): Essa vulnerabilidade envolvia o carregamento de objetos ActiveX maliciosos em páginas web abertas no Internet Explorer. Para que o exploit fosse acionado, bastava que o usuário acessasse um site especialmente criado com o código malicioso embutido. Inicialmente, essa falha foi utilizada pelo grupo APTgroup em um ataque em 2009, e mais tarde reaproveitada pelo Equation Group em operações contra membros do governo do Afeganistão.

- Execução Remota de Código Fora da Sandbox do Java Runtime Environment (CVE-2012-1723 e CVE-2012-4681): Essas vulnerabilidades afetavam aplicações Java executadas em navegadores. Ao acessar um site com código malicioso e com o plugin Java ativado, o exploit era executado, escapando da sandbox da Java Virtual Machine. Essas falhas eram frequentemente usadas para baixar e executar outros tipos de malware na máquina da vítima.

Técnicas de Ataque

Para acessar as máquinas de suas vítimas e roubar seus respectivos dados, os invasores do Equation Group se utilizam de diversos meios, como exploits online, pen drives, CD-ROMs e worms como o Fanny.
Um caso emblemático de infecção em massa através de pen drives aconteceu em 2009, em Houston, nos Estados Unidos. Numa conferência científica, os participantes receberam, através da organização do evento, CD-ROMs contendo materiais contemplados na conferência. Contudo, de forma ainda desconhecida, os dispositivos foram substituídos por materiais infectados por malwares atribuídos ao Equation. Após tentar executar um instalador através de exploits, o dispositivo inicializava o DoubleFantasy na máquina e, caso a vítima fosse de interesse dos invasores, seus dados eram então acessados e roubados.

Considerações Finais

A descoberta do Equation Group, bem como de seu arsenal de armas cibernéticas, revolucionou o mundo da cibersegurança de uma forma nunca antes vista. Seus inúmeros ataques, muitas vezes realizados em dias-zero, são dotados de estratégias de roubo de dados que, para a maioria, parecem inacreditavelmente invasivas e, para os profissionais da área da cibersegurança, configuram novo desafio a ser enfrentado no âmbito do hack ético.

O fato de o grupo ser afiliado ao governo dos Estados Unidos, a maior potência econômica da atualidade, potencializa a possibilidade de o Equation Group estar envolvido nos próximos conflitos intergovernamentais na esfera mundial. Isso é reflexo de como os ciberataques tem potencial de crescimento, tornando imperativo o investimento em medidas de cibersegurança.

Bibliografia Consultada

KASPERSKY LAB. Equation Group: Questions and Answers. Fevereiro de 2015. Disponível em: https://web.archive.org/web/20150217023145/https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

KASPERSKY BRASIL. Equation: o malware “indestrutível”. 19 fev. 2015. Disponível em: https://www.kaspersky.com.br/blog/equation-malware-indestrutivel/4837/.

GOLDBERG, Sharon. Equation Group. Boston University, 2015. Apresentação. Disponível em: https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/eqngroup.pdf.

GOODIN, Dan. 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/.

MICROSOFT. MS09-025: Vulnerabilidades no kernel do Windows podem permitir elevação de privilégio. *Microsoft Learn – Security Updates*. Publicado em 9 jun. 2009. Disponível em: https://learn.microsoft.com/pt-br/security-updates/securitybulletins/2009/ms09-025. Acesso em: 2 jul. 2025.

MICROSOFT. MS12-034: Vulnerabilidade de análise de fonte TrueType - CVE-2012-0159. *Microsoft Learn – Security Updates*. Disponível em: https://learn.microsoft.com/pt-br/security-updates/securitybulletins/2012/ms12-034#truetype-font-parsing-vulnerability---cve-2012-0159. Acesso em: 2 jul. 2025.

CVE DETAILS. CVE-2012-0159: Microsoft Windows and Silverlight TrueType Font Parsing Remote Code Execution Vulnerability. *CVE Details*. Disponível em: https://www.cvedetails.com/cve/CVE-2012-0159/. Acesso em: 2 jul. 2025.

MICROSOFT. MS13-081: TrueType Font CMAP Table Vulnerability - CVE-2013-3894. *Microsoft Learn – Security Updates*. Disponível em: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-081#truetype-font-cmap-table-vulnerability---cve-2013-3894. Acesso em: 2 jul. 2025.

NIST. CVE-2013-3894. *National Vulnerability Database*. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2013-3894. Acesso em: 2 jul. 2025.

MICROSOFT. MS10-046: Vulnerabilidade de carregamento de ícone de atalho - CVE-2010-2568. *Microsoft Learn – Security Updates*. Disponível em: https://learn.microsoft.com/pt-br/security-updates/securitybulletins/2010/ms10-046. Acesso em: 2 jul. 2025.

CVE. CVE-2010-2568. *CVE Record*. Disponível em: https://www.cve.org/CVERecord?id=CVE-2010-2568. Acesso em: 2 jul. 2025.

NIST. CVE-2013-3918. *National Vulnerability Database*. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2013-3918. Acesso em: 2 jul. 2025.

MICROSOFT. MS13-090. InformationCardSigninHelper Vulnerability - CVE-2013-3918. *Microsoft Learn – Security Updates*. Disponível em: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090. Acesso em: 2 jul. 2025.

RED HAT BUGZILLA. CVE-2012-1723 OpenJDK: insufficient field accessibility checks. *Red Hat Bugzilla*. Disponível em: https://bugzilla.redhat.com/show_bug.cgi?id=829373. Acesso em: 2 jul. 2025.

NIST. CVE-2012-1723. *National Vulnerability Database*. Disponível em: https://nvd.nist.gov/vuln/detail/cve-2012-1723. Acesso em: 2 jul. 2025.

MICROSOFT. Exploit:Java/CVE-2012-1723!generic. *Microsoft Malware Encyclopedia*. Disponível em: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:Java/CVE-2012-1723!generic. Acesso em: 2 jul. 2025.

NIST. CVE-2012-4681. *National Vulnerability Database*. Disponível em: https://nvd.nist.gov/vuln/detail/cve-2012-4681. Acesso em: 2 jul. 2025.

ORACLE. Oracle Security Alert for CVE-2012-4681. *Oracle Security Alerts*. Disponível em: https://www.oracle.com/security-alerts/alert-cve-2012-4681.html. Acesso em: 2 jul. 2025.

ORACLE. Oracle Java SE Critical Patch Update Advisory - June 2012. *Oracle Security Alerts*. Junho 2012. Disponível em: https://www.oracle.com/security-alerts/javacpujun2012.html. Acesso em: 2 jul. 2025.

RED HAT BUGZILLA. CVE-2012-4681 OpenJDK: beans insufficient permission checks. *Red Hat Bugzilla*. Disponível em: https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-4681. Acesso em: 2 jul. 2025.

VIRUS BULLETIN. An in-depth look at Stuxnet. *Virus Bulletin Conference 2010*. 2010. Disponível em: https://www.virusbulletin.com/conference/vb2010/abstracts/indepth-look-stuxnet. Acesso em: 2 jul. 2025.

ZDNET (via Internet Archive). Stuxnet attackers used 4 Windows zero-day exploits. 2010. Disponível em: https://web.archive.org/web/20141125225130/http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347. Acesso em: 2 jul. 2025.

ELECTRONIC TRANSACTIONS DEVELOPMENT AGENCY. Threat Group Cards: A Threat Actor Encyclopedia, APT group: Equation Group. Última alteração em 2 mar. 2025. Disponível em: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Equation%20Group. Acesso em: 1 jul. 2025.

KASPERSKY LAB. Equation: The Death Star of Malware Galaxy. 16 fev. 2015 Disponível em: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/. Acesso em: 1 jul. 2025.

ECLYPSIUM. Infographic: A History of Network Device Threats and What Lies Ahead. 2 dec. 2024. Disponível em: https://eclypsium.com/blog/infographic-a-history-of-network-device-threats-and-what-lies-ahead/. Acesso em: 1 jul. 2025.

KASPERSKY LAB. Equation Group: The Crown Creator of Cyber-Espionage. 17 feb. 2015. Disponível em: https://www.kaspersky.com/about/press-releases/equation-group-the-crown-creator-of-cyber-espionage. Acesso em: 1 jul. 2025.

KASPERSKY LAB . A Fanny Equation: "I am your father, Stuxnet" . 17 feb. 2015. Disponível em: https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/. Acesso em: 2 jul. 2025.

INTRODUCTION TO CYBER-WARFARE (book). Paulo Shakarian, Jana Shakarian and Andrew Ruef. Chapter 13 - Attacking Iranian Nuclear Facilities: Stuxnet . 2013 Disponível em: https://www.sciencedirect.com/science/article/pii/B9780124078147000130. Acesso em: 2 jul. 2025.

RADWARE. Flame. Disponível em: https://www.radware.com/security/ddos-knowledge-center/ddospedia/flame/. Acesso em: 3 jul. 2025.

KASPERSKY LAB. Lessons learned from Flame, three years later. 29 mai. 2015. Disponível em: https://securelist.com/lessons-learned-from-flame-three-years-later/70149/. Acesso em: 3 jul. 2025.

RT. 'Flame' Virus explained: How it works and who's behind it. 29 mai. 2012. Disponível em: https://www.rt.com/news/flame-virus-cyber-war-536/. Acesso em: 3 jul. 2025.

THE WASHINGTON POST. U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. 19 jun. 2012. Disponível em: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. Acesso em: 3 jul. 2025.