Abstract – This document provides a analysis of publicly known private companies involved in nation-state offensive cyber operations. The analysis delves into various aspects of the inventory, including the nature of the companies listed, the types of capabilities they offer, and the geopolitical implications of their services.

The extract provided is of high quality, aggregating publicly available information without disclosing sensitive or confidential data. It serves as a valuable resource for security professionals, offering insights into the landscape of private sector participation in offensive cyber operations.

I. What is the Equation Group?

The Equation Group is classified as an advanced persistent threat (APT) and is known for its sophisticated cyber-espionage activities. It has been active since at least 2001 and is renowned for its complex and highly advanced malware tools and techniques. The group has been involved in numerous cyber operations targeting a wide range of sectors and countries, including government, military, telecommunications, aerospace, energy, nuclear research, and financial institutions

II. Equation Technologies

A. Cyber capabilities

- **Remote Access Tools and Malware Platforms**: The Equation Group employs multiple remote access tools and has developed several malware platforms of high complexity and sophistication, such as EquationDrug, DoubleFantasy, Equestre (same as EquationDrug), TripleFantasy, GrayFish, Fanny, and EquationLaser. These tools are designed for espionage and have self-destruct mechanisms to reduce forensic evidence.
- **Firmware Reprogramming**: One of the most advanced techniques used by the Equation Group is the ability to reprogram hard drive firmware. This capability allows the group to persist on infected systems undetectably and effectively makes their operations invisible and indestructible.
- **Encryption and Obfuscation**: The Equation Group frequently uses sophisticated encryption schemes, including the RC5, RC6, RC4, AES cryptographic functions, and various hashes, to protect its malware and communications. This level of encryption and the strategies employed to camouflage its activity are indicative of the group's advanced capabilities.
- **Exploitation of Zero-Day Vulnerabilities**: The group has access to and has used zero-day exploits, which are vulnerabilities unknown to the software vendors and the public at the time of exploitation. For example, the Equation Group used two zero-day exploits in Fanny before they were integrated into Stuxnet, indicating access to these vulnerabilities before other known cyber-attack groups.
- **USB-Based Reconnaissance Tools**: To map air-gapped networks, which are not connected to the Internet, the Equation Group developed USB stick-based reconnaissance malware. This capability is significant for penetrating secure military facilities, intelligence organizations, and nuclear facilities.
- **Exploit Frameworks and Post-Exploitation** Tools: The Equation Group uses a variety of exploit frameworks and post-exploitation tools, such as DanderSpritz, which is a full-featured framework used after exploiting a machine. DanderSpritz contains a wide variety of modules for persistence, reconnaissance, lateral movement, and bypassing antivirus engines.
- **Firewall Exploit Chain**: The Equation Group has developed a near-complete exploit kit targeting major firewall manufacturers. This kit includes exploits like EXTRABACON (CVE-2016-6366) for gaining access to Cisco ASA and PIX firewalls, and EPICBANANA (CVE-2016-6367) for planting command and control shellcode.
- **Interdiction Techniques**: The group has used interdiction techniques, such as intercepting physical goods and replacing them with Trojanized versions, to deliver malware. This method demonstrates the group's capability to infect targets not only through the web but also in the physical world.

B. Equation Group's Malware

- **EquationDrug**: A complex malware platform that provides the group with a full-featured espionage platform.
- **DoubleFantasy**: A validator-style malware used to confirm the target is of interest and then deploy further malware.
- **Fanny**: A worm that uses two zero-day exploits to map air-gapped networks via USB sticks.

- **GrayFish**: A platform that resides entirely in the registry, encrypting its payload and storing it in a virtual file system.

One of the most powerful tools in their arsenal is a module known only by a cryptic name: “nls_933w.dll”, which allows them to reprogram the hard drive firmware of over a dozen different hard drive brands. This capability is an astonishing technical accomplishment and is testament to the group’s abilities.

C. *Remote Access Tools*

The Equation Group employs multiple remote access tools (RATs) and is known for using zero-day exploits. These tools are capable of overwriting disk drive firmware, further demonstrating the group's advanced capabilities:

- **UnitedRake (UR)**: A remote access tool that can target Windows machines. It is an extensible and modular framework provided with many plugins that perform different information collection functions.
- **DoubleFeature**: A post-exploitation tool that logs the use of other malware tools on the infected machine, providing a unique source of knowledge pertaining to Equation Group tools.
- **EquationLaser, EquationDrug, DoubleFantasy, Equestre (same as EquationDrug), TripleFantasy, GrayFish, Fanny, and EquationLaser**: Custom attack platforms, trojans, worms, and backdoors used by the Equation Group.

The Equation Group's use of these tools and exploits does not change the path of a normal kill chain, making them a formidable opponent. Their operations are characterized by professionalism, organization, and a focus on retaining stealth

III. Relationship Between the Equation Group and the NSA

The Equation Group is suspected of being tied to the NSA's Tailored Access Operations (TAO) unit. This connection is suggested by several factors:

A. *Similarities Between the Equation Group and the NSA*

- **Sophistication and Resources**: The Equation Group is recognized for its highly sophisticated cyber capabilities, including the development and use of complex malware and zero-day exploits. The group's operations, which span decades and target a wide range of sectors globally, indicate a level of resources and expertise consistent with a state-sponsored entity like the NSA.
- **Similarities to NSA Tools and Techniques**: Analysis of the Equation Group's malware and exploits reveals significant similarities to those known to be used by the NSA. For instance, the use of specific encryption algorithms (RC5, RC6, RC4, AES) and obfuscation techniques mirrors those documented in NSA operations. Additionally, the malware's operational hours and the targeting of specific countries align with U.S. interests, further suggesting a connection to the NSA.
- **Shadow Brokers Leak**: In 2016, a group known as the Shadow Brokers leaked a trove of cyber tools and exploits they claimed to have stolen from the Equation Group. Analysis of these tools showed they exploited vulnerabilities in software and hardware in ways that were highly sophisticated and previously unknown, suggesting the involvement of an entity with extensive cyber warfare capabilities, like the NSA.
- **Snowden Documents**: Documents leaked by Edward Snowden have provided indirect evidence linking the Equation Group to the NSA. Certain codenames and operational details found in the Snowden documents match those associated with the Equation Group's activities, reinforcing the belief that the group operates under the NSA's auspices.
- **Shared Zero-Day Exploits**: Research has shown that the Equation Group had access to zero-day exploits before they were used in other known NSA-associated malware, such as Stuxnet and Flame. This temporal precedence suggests that the Equation Group either is part of the NSA or works closely with it, sharing tools and exploits for cyber operations.
- **Expert Analysis and Attribution**: Cybersecurity experts and researchers, including those from Kaspersky Lab, have pointed to the technical sophistication, targeting patterns, and operational security of the Equation Group as being indicative of a state-sponsored actor with objectives aligning with those of the NSA. While direct attribution is challenging in cyberspace, the accumulated evidence and expert consensus lean strongly towards the Equation Group being part of, or affiliated with, the NSA.

B. *Differences Between the Equation Group and the NSA*

While the Equation Group is primarily focused on cyber espionage and the creation and deployment of advanced malware, the NSA has a broader mission that includes both intelligence gathering and national security operations. The NSA's activities encompass a wide range of operations including signal intelligence, cyber-security, and global monitoring, with the aim of collecting and analyzing data that pertains to national security.

The NSA operates globally and is involved in various types of intelligence activities, which include but are not limited to cyber operations. It is structured to support broader U.S. intelligence and defense operations, whereas the Equation Group is specifically focused on sophisticated cyber espionage.

C. *Mission of the Equation Group vs. NSA's Mission*

The mission of the Equation Group revolves around conducting cyber espionage to gather intelligence, often by deploying malware that can infiltrate and persist in target systems undetected. Their operations are characterized using zero-day exploits, sophisticated malware, and techniques designed to breach high-value targets and remain hidden.

In contrast, the NSA's mission is more comprehensive and includes the collection and processing of global signals intelligence to inform U.S. national defense and foreign policy decisions. The NSA's activities are not limited to cyber operations; they also include a wide array of signal intelligence and information assurance products and services designed to protect U.S. information systems and produce foreign signals intelligence information

D. Central Intelligence Agency's Information Operations Center (IOC)

The Central Intelligence Agency's Information Operations Center (IOC) plays a crucial role in the agency's expanded mission, which now includes covert paramilitary operations alongside its traditional intelligence-gathering activities. The IOC, one of the CIA's largest divisions, has shifted its focus from counterterrorism to offensive cyber operations, reflecting the evolving nature of global threats and the increasing importance of cyber warfare in national security.

The IOC's foundation as the agency's digital and cyber operations hub was further solidified with the establishment of the Directorate for Digital Innovation (DDI) in 2015. This new directorate, the first new directorate in fifty years, was created to modernize the CIA's IT systems and further operationalize its cyber capabilities. It brought together the spy agency's CIO shop, cyber capabilities, and open-source intelligence efforts under one roof, aiming to provide CIA analysts with better IT tools for traditional espionage work and to locate and understand the "digital dust" left behind by actors in the cyber domain.

The creation of the DDI and the emphasis on the IOC's role in cyber operations underscore the CIA's recognition of the digital domain as a critical battlefield. The agency's efforts to integrate digital and cyber capabilities into its operations reflect a broader trend within the U.S. intelligence community to adapt to the challenges posed by the digital age, including cyber threats, electronic surveillance, and information warfare

E. CIA's Engineering Development Group (EDG)

The CIA Engineering Development Group (EDG) is tasked with the development, testing, and operational support of all backdoors, exploits, and malicious payloads used by the CIA in cyber operations. This group plays a critical role in creating the tools and techniques necessary for conducting cyber espionage and cyber warfare.

EDG's responsibilities include ensuring that the CIA maintains a cutting-edge capability in penetrating adversary systems and networks, leveraging vulnerabilities in software and hardware to gather intelligence or achieve other operational objectives.

F. Technical Aspects of CIA Cyber Operations (TAC)

The CIA's cyber operations involve sophisticated tools and techniques for intelligence gathering from adversary systems and networks. This includes the use of advanced tradecraft in cyber espionage, which is supported by the technical expertise within the agency.

Cyber Security Officers within the CIA are responsible for protecting agency data and systems against threats. They utilize sophisticated tools and knowledge of CIA Information Technology (IT) to monitor, evaluate, and manage IT risk. This includes identifying current threats, mitigating vulnerabilities, and anticipating future challenges.

The Operations Support Branch (OSB) of the CIA, part of its cyber-intelligence division, specializes in physical access operations, indicating a technical capability to develop tools for cyberintelligence missions on short notice. This highlights the technical agility and innovation within the CIA's cyber operations

G. The TAC Discussion on EQGRP

Vault 7 from Wikileaks provides a rare glimpse into the internal reactions and operational challenges faced by national intelligence agencies following the exposure of their cyber capabilities, emphasizing the ongoing need for security enhancements and strategic adjustments in cyber operations.

- **Collaborative Efforts and Shared Capabilities**: EQGRP was not a single entity but a collective term used to describe a range of cyber capabilities primarily managed by the NSA’s TAO and the CIA’s IOC. This highlights the collaborative nature of cyber operations between these two key U.S. intelligence entities.
- **Joint Development and Authorship**: The discussion indicates that some parts of the cyber implants associated with EQGRP were co-authored by both the CIA and the NSA. This joint authorship underlines the integrated approach to developing cyber tools and strategies.
- **Differences in Operational Processes**: There were notable differences in the processes or the lack thereof for re-using cyber capabilities between the CIA IOC and NSA TAO. These differences could potentially impact the efficiency and security of cyber operations.
- **Lessons Learned**: The leak and subsequent public exposure of these activities have led to significant introspection within these agencies. The discussion reflects a keen interest in learning from the incident to prevent future compromises and enhance the security of cyber operations.
- **Importance of High-Quality Threat Intelligence**: The discussion also underscores the value of high-quality threat intelligence, as demonstrated by Kaspersky’s report, which played a crucial role in uncovering these activities. The agencies recognize the need to understand and mitigate the implications of such intelligence findings on national security.

H. Thoughts

- **Collaborative Nature of U.S. Cyber Operations**: it emphasizes that U.S. cyber operations are not the domain of any single agency. Instead, they involve collaboration across various intelligence agencies, including the NSA and the CIA. This collaborative approach is typical of complex cyber operations which require a range of skills and resources that no single agency could effectively manage alone.

- **Role of CIA's IOC**: The CIA's Information Operations Center (IOC) is highlighted as a significant player in the activities attributed to the Equation Group. The IOC's involvement suggests that the operations of the Equation Group are more broadly based within the U.S. intelligence community than previously thought.
- **Misattribution and Misunderstandings**: the challenges and potential inaccuracies involved in attributing cyber activities to specific groups or agencies. Due to the clandestine nature of intelligence efforts and the intricate technicalities of cyber warfare, pinpointing responsibility accurately is exceedingly difficult. Consequently, there is a tendency to oversimplify matters by attributing all advanced cyber operations to the NSA
- **Public Perception and Media Simplification**: The criticism of media and public discourse often centers on their tendency to oversimplify the narrative surrounding cyber operations by exclusively attributing them to the NSA. This oversimplification fails to acknowledge the complex reality of inter-agency collaboration and the distributed nature of cyber intelligence and warfare capabilities.
- **Importance of a Broader View**: It necessitates a more sophisticated comprehension of how the U.S. government conducts cyber operations. Acknowledging the involvement of various agencies beyond the NSA is essential for a thorough grasp of U.S. capabilities and strategies in cyberspace..

IV. Conclusion

- **Identification of the Equation Group**: The Equation Group is identified as a highly sophisticated and advanced persistent threat, primarily linked to the NSA's Tailored Access Operations (TAO) unit. This group has been active in cyber espionage and cyber warfare, utilizing complex tools and techniques to infiltrate a wide range of targets globally.
- **Impact of Leaks**: The leaks by Shadow Brokers in 2016 revealed significant details about the Equation Group's operations, including the use of sophisticated tools like Bvp47. These leaks confirmed the group's connection to the NSA and exposed the extensive reach of their cyber operations, affecting over 287 targets in 45 countries.
- **Technical Sophistication**: The Equation Group's tools, such as Bvp47, demonstrated advanced capabilities in network attack, equipped with 0day vulnerabilities. Their operations were characterized by a high degree of covertness and technical sophistication, making them a dominant force in national-level cyberspace confrontations.
- **Global Impact and Victims**: The global impact of the Equation Group's activities was vast, with victims across various countries, indicating the strategic and widespread nature of their cyber operations. This included the use of victims' systems as jump servers for further attacks, highlighting the strategic depth of their operations.