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.

The analysis is particularly useful for cybersecurity experts, including those with interests in cyber security, devopsec, devops, IT, forensics, law enforcement, CVE, and CWE. It aids in understanding the threat landscape, preparing for potential nation-state level cyberattacks, and formulating strategic defense mechanisms against sophisticated cyber threats.

I. Introduction

Several companies have been involved in nation-state offensive cyber operations and have provided capabilities such as software implants, intrusion sets (including 0day exploits, exploitation frameworks, security bypassing techniques), and communications interception products. The list is not about leaking sensitive or confidential information, but rather aggregates what is already publicly available. The companies listed range from those that are active, ceased, or have been acquired, and are from various countries around the world. This inventory includes companies that provide capabilities such as software implants, intrusion sets (e.g., 0day exploits, exploitation frameworks, security bypassing techniques, communications interception products, etc.). The inventory serves as an aggregation of publicly available information and includes references to open-source intelligence (OSINT) that mention these entities' involvement in such activities.

II. Difference between private and public companies inventory

The difference between private and public companies lies primarily in their ownership structure and access to capital.

Private companies are owned by a select group of individuals, often closely held by family members, founders, or private investors. Their shares do not trade on public exchanges and are not issued through an initial public offering (IPO). As a result, private firms do not need to meet the Securities and Exchange Commission's (SEC) strict filing requirements. The shares of these businesses are less liquid, and their valuations are more difficult to determine.

On the other hand, public companies have their shares listed and traded on stock exchanges, making them accessible to a wider range of investors. This results in a more decentralized ownership structure. Public companies can often sell shares or raise money through bond offerings with more ease. They are also subject to more regulations and must make regular disclosures, publish their finances, and act in a transparent manner.

In the context of the Offensive Security Private Companies Inventory, the term "private" refers to companies that are privately owned. The inventory does not make a distinction between private and public companies; rather, it focuses on companies involved in nation-state offensive cyber operations. The term "public" in this context does not refer to publicly traded companies, but to the fact that the information about these companies is publicly available.

III. Private Companies Examples

Examples of private companies that have been involved in nation-state offensive cyber operations, as listed in the Offensive Security Private Companies Inventory, include:

- **CyberPoint (USA)**: Active since 2015, with references on Wikipedia.
- **CyberRoot Risk Advisory (India)**: Active since 2013, with references on IntelligenceOnline.
- **Cycura (Canada)**: Active since 2013, with references on IntelligenceOnline.
- **DarkMatter Group (UAE)**: Active since 2014, with references on Wikipedia.
- **Cytrox Holdings Zrt (Hungary)**: Active since 2017, with references on CitizenLab.
- **STEALIEN Inc. (South Korea)**: Active since 2015, with references on their official website.
- **Synacktiv (France)**: Active since 2012, with references on EX Files.
- **Syndis (Iceland)**: Active since 2013, with references on DarkReading.

These companies have been involved by providing capabilities such as software implants, intrusion sets (e.g., 0day exploits, exploitation frameworks, security bypassing techniques, communications interception products, etc.)

A. *Offered services*

Private cybersecurity companies, which are not publicly traded, offer a broad spectrum of services aimed at protecting organizations from cyber threats. These services are essential for safeguarding digital assets, ensuring data privacy, and maintaining the integrity of information systems.

CyberPoint (USA)

CyberPoint offers a range of cybersecurity services including:

- **Penetration Testing**: Simulated cyber attacks to identify vulnerabilities.
- **Vulnerability Management**: Continuous monitoring/testing and policies for managing vulnerabilities.
- **Incident Response**: Triage, live system capture, forensics, and analysis following a breach.
- **Cloud and Infrastructure Engineering**: Secure and fast infrastructure development processes.
- **Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity**: Utilizing AI and ML for malware detection, reverse engineering, network situational awareness, and attack mitigation.
- **Technology Consulting and IT/OT Strategies**: Tailored consulting for technology, policy, and operations in a global marketplace

CyberRoot Risk Advisory (India)

CyberRoot Risk Advisory's operations, as identified by Meta, involved:

- **Phishing and Spyware Networks**: Creating fake accounts for phishing and spying on users globally. They used spoofed domains of major email providers and other services for stealing login credentials

Cycura (Canada)

Cycura typically offer services such as:

- Cybersecurity Audits
- Forensics and Incident Response
- Malware Analysis
- Security Training

DarkMatter Group (UAE)

DarkMatter has been involved in:

- **Surveillance and Cyber Espionage**: Contracted for Project Raven to help the UAE surveil governments, militants, and activists. They employed former U.S. intelligence operatives for these operations.

Cytrox Holdings Zrt (Hungary)

Cytrox's activities include:

- **Spyware Development**: Known for developing the Predator spyware, used in operations spying on journalists, politicians, and others. They were blacklisted by the U.S. Commerce Department for trafficking in cyber exploits.

STEALIEN Inc. (South Korea), Synacktiv (France), Syndis (Iceland)

STEALIEN Inc., Synacktiv, or Syndis. provide a range of cybersecurity services including:

- Penetration Testing
- Security Assessments
- Incident Response
- Security Consulting

B. *Offered services' list*

Private cybersecurity companies, which are not publicly traded, offer a variety of services to protect organizations from cyber threats. These services typically include:

- **Risk Assessment**: Identifying vulnerabilities in networks, data, and communications and recommending mitigations and security improvements.
- **Protection Services**: Implementing safeguards like firewalls, intrusion detection systems, and antivirus software.
- **Threat Detection and Response**: Monitoring for cyber threats, detecting them, and responding to prevent damage, which may include managed detection and response (MDR) services.
- **Security Operations Center (SOC) as a Service**: Providing 24/7 monitoring and threat management for businesses that cannot build an internal SOC
- **Threat Intelligence**: Offering information on the latest hacking tactics and emerging threats.
- **Compliance and Governance**: Helping organizations meet regulatory requirements and industry standards.
- **Incident Response**: Assisting organizations in responding to and recovering from security incidents, including forensic analysis and remediation plans.
- **Cybersecurity Training**: Educating employees on cybersecurity best practices to strengthen the human element of security.
- **Vulnerability Management**: Scanning and analyzing systems for vulnerabilities and providing solutions to address them.
- **Endpoint Protection**: Securing endpoints such as laptops, mobile phones, and tablets.
- **Network Security**: Protecting the integrity and usability of network and data.
- **Cloud Security**: Securing cloud-based infrastructure and applications.

- **Email Security**: Protecting email communication from threats like phishing, spam, and malware.
- **Managed Security Services**: Outsourcing the management of security devices and systems to third-party experts

IV. Public companies Examples

Examples of publicly traded companies that are involved in cybersecurity:

- **Palo Alto Networks (NYSE: PANW)**: A multinational cybersecurity company known for its advanced firewalls and cloud-based offerings.
- **CrowdStrike Holdings, Inc. (NASDAQ: CRWD)**: Provides cloud-delivered solutions for endpoint protection, threat intelligence, and cyber attack response services.
- **Check Point Software Technologies (NASDAQ: CHKP)**: An Israeli company specializing in IT security, including network security, endpoint security, cloud security, and mobile security.
- **CyberArk Software Ltd. (NASDAQ: CYBR)**: An Israeli-American cybersecurity company that specializes in privileged access security.
- **Cloudflare Inc. (NYSE: NET)**: An American company that provides web infrastructure and website security, including DDoS mitigation and secure content delivery network services.
- **Rapid7 (NASDAQ: RPD)**: A company that provides security data and analytics solutions, including vulnerability management services.
- **Cisco Systems (NASDAQ: CSCO)**: A multinational technology conglomerate that provides cybersecurity solutions as part of its diverse product portfolio.
- **Broadcom (NASDAQ: AVGO)**: A global technology company that provides a range of semiconductor and infrastructure software solutions, including cybersecurity software.
- **IBM (NYSE: IBM)**: A multinational technology company that offers a range of cybersecurity solutions as part of its broader product and service offerings.
- **VMware, Inc. (NYSE: VMW)**: A company that specializes in cloud computing and virtualization software and services, including security services

These companies offer a range of cybersecurity solutions, from network and endpoint security to cloud security and threat intelligence. They are publicly traded, meaning their shares are available for purchase on public stock exchanges.

A. Offered services per companies

Publicly traded cybersecurity companies offer a wide range of services designed to protect digital assets, data, and networks from cyber threats and attacks. These services cater to various aspects of cybersecurity, including network security, cloud security, endpoint security, threat intelligence, and more. Here's an overview of the services provided by some of the publicly traded cybersecurity companies

Palo Alto Networks (NYSE: PANW)

Palo Alto Networks offers a comprehensive suite of cybersecurity services, including:

- **Customer Success Services**: Guidance on securing businesses and technical outcomes, online self-service community support, and expert assistance for transitioning to new security technologies.
- **Global Support**: Fast, expert support to maximize uptime, mitigate risks, and streamline operations.
- **Training and Certification**: A wealth of training, certification, and digital learning options to expand knowledge and skills in cybersecurity.
- **Focused Services**: Enhanced support experience with account management and technical experts familiar with the client's environment, personalized case handling, root cause analysis for critical issues, and proactive alerts and upgrade planning.

CrowdStrike Holdings, Inc. (NASDAQ: CRWD)

CrowdStrike provides:

- CrowdStrike Falcon Platform: A unified platform for modern security, offering protection against cloud breaches with unified agent and agentless protection, real-time visibility, detection, and protection against identity-based attacks.
- Managed and On-Demand Cybersecurity Services: Incident response, technical assessments, training, and advisory services to prepare for and defend against sophisticated threat actors.
- Fully Managed Services: For detection and response (MDR), threat hunting, and digital risk protection.

Check Point Software Technologies (NASDAQ: CHKP)

Check Point offers:

- Check Point Infinity Platform: Predicts and prevents attacks across networks, clouds, endpoints, and devices with AI-powered, cloud-delivered security.
- ThreatCloud AI: Identifies and blocks emerging zero-day threats, delivering accurate prevention in under two seconds to hundreds of millions of enforcement points.
- Unified Security Solution: Protects everywhere work gets done, including email, endpoint, and mobile, with powerful AI tools for Security Operations Center teams.

CyberArk Software Ltd. (NASDAQ: CYBR)

CyberArk focuses on identity security, offering:

- Identity Security Platform: Secures every identity with the right level of privilege controls across any infrastructure.

- Seamless & Secure Access: Combines secure SSO, Adaptive MFA, Lifecycle Management, Directory Services, and User Behavior Analytics.
- Intelligent Privilege Controls: Applies world-class controls across the IT estate, securing workforce users, third-party vendors, endpoints, and machine identities

Additional Services

Other companies like Cloudflare Inc. (NYSE: NET), Rapid7 (NASDAQ: RPD), Cisco Systems (NASDAQ: CSCO), Broadcom (NASDAQ: AVGO), IBM (NYSE: IBM), and VMware, Inc. (NYSE: VMW) also offer a range of cybersecurity solutions. These include DDoS mitigation, secure content delivery network services, security data and analytics solutions, cybersecurity solutions as part of a diverse product portfolio, semiconductor and infrastructure software solutions, and cloud computing and virtualization software and services, respectively.

- **Cloudflare (NET)**: Offers cybersecurity services through its cloud security platform, acting as an intermediary between servers and visitors to client sites. Cloudflare's services are designed for multiple industries, including education, e-commerce, finance, the public sector, and gaming. Its global network spans over 300 cities in more than 100 countries.
- **Secureworks (SCWX)**: With over 20 years of experience in compiling threat intelligence and studying cyber attacks, Secureworks offers a cloud-based, SaaS security platform. Its Taegis platform can process over 470 billion events each day, providing a comprehensive overview of a company's network.
- **Cyren (CYRN)**: Builds internet security services for the cloud, helping protect against email-related attacks such as phishing scams. Cyren's technology identifies unusual patterns to prevent cyber attacks without compromising customer data privacy.
- **Splunk**: Specializes in cybersecurity software that identifies digital vulnerabilities and prevents malware attacks. Splunk's platform uses AI and machine learning for automated and accurate threat detection, allowing businesses to focus on true cyber threats.
- **A10 Networks (ATEN)**: Secures cloud presence and 5G wireless by deploying machine learning and automation to recognize and stop cyber threats. A10 also offers built-in data analytics for insights into attempted breaches.
- **Fortinet (FTNT)**: Provides security software used across various industries, offering tools like firewall protection, VPNs, endpoint protection, and cloud security. Fortinet embraces a zero-trust policy to ensure only approved personnel access applications and sensitive information.

B. Offered services' list

Cybersecurity companies, whether publicly traded or private, offer a wide range of services to protect organizations from cyber threats. These services typically include:

- **Risk Assessment**: Identifying potential network, data, and communications vulnerabilities and recommending mitigations and security improvements.
- **Protection Services**: Implementing safeguards such as firewalls, intrusion detection systems (IDS), and antivirus software to protect against unauthorized access and cyber attacks.
- **Threat Detection and Response**: Monitoring for cyber threats, detecting them, and responding quickly to stop them and prevent damage. This may include managed detection and response (MDR) services.
- **Security Operations Center (SOC) as a Service: Providing** 24/7 monitoring and addressing threats through a SOC, which is valuable for businesses that cannot build an internal SOC due to budget or talent constraints.
- **Threat Intelligence**: Keeping up with the latest hacking tactics and providing information on emerging threats to protect against them.
- **Compliance and Governance**: Ensuring that organizations meet regulatory requirements and industry standards, such as HIPAA for healthcare or GDPR for data protection.
- **Incident Response**: Offering services to help organizations respond to and recover from security incidents, including forensic analysis and remediation plans.
- **Cybersecurity Training**: Educating employees about cybersecurity best practices and potential implications of their actions to strengthen the human element of security.
- **Vulnerability Management**: Scanning and analyzing systems for vulnerabilities and providing solutions to address them.
- **Endpoint Protection**: Securing endpoints like laptops, mobile phones, and tablets from being exploited by cybercriminals.
- **Network Security**: Protecting the integrity and usability of network and data through various measures, including network segmentation and access control.
- **Cloud Security**: Offering solutions to secure cloud-based infrastructure and applications.
- **Email Security**: Protecting email communication from threats like phishing, spam, and malware.
- **Managed Security Services**: Outsourcing the management of security devices and systems to third-party experts