itworldcanada.com

# Understanding Cybersecurity on Smartphones (UCS-Sph) Part 2 - IT World Canada

*MohammadMoein Shafi and Arash Habibi Lashkari*

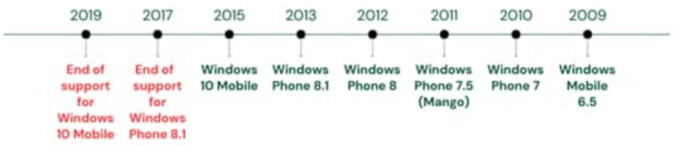
26–33 minutes

This second article of the Understanding Cybersecurity on Smartphones (UCS-Sph) series delves into Microsoft's Windows Phone, a mobile OS that has undergone significant changes over the years. The Windows Phone was first known as Windows Mobile in its early days, until Microsoft recognized the need to adapt and innovate in response to the competitive landscape of the smartphone market. After the changes introduced by Apple (iOS) and Google (Android) in 2007, Microsoft decided to take a new direction and created Windows Phone as a response. This article delves into the history, evolution, and unique features of Microsoft's Windows Phone, from its early beginnings as Windows Mobile to its updates and innovations as Windows Phone.

Contents

## 1. Learning Basics: Windows OS History

The development of Microsoft's mobile OS is a fascinating story of technological evolution and market competition. What factors led to the creation of Windows Phone, and how did it differ from its predecessor, Windows Mobile? How did Microsoft respond to the rise of Apple's iOS and Google's Android, and what impact did this have on the development of Windows Phone? These are just a few of the questions that arise when we consider the dynamic history of the mobile OS. Let's look at **Figure 1**'s timeline of significant Windows Mobile releases and events from 1999 to 2019 to get some answers to these queries.



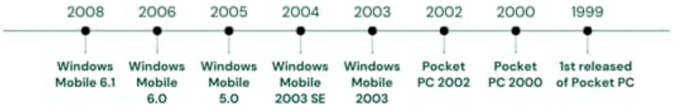


Figure 1: Windows OS timeline from 1999 until 2019

Windows Mobile launched in 1999 as the Pocket PC 2000, which operated on Pocket PC PDAs. However, Windows Mobile's origin story goes back to Windows CE, released in 1996 [1]. The evolution of Microsoft's mobile OS has gone through several name changes and updates over the years. In the early to mid-2000s, Windows Mobile 2003, Windows Mobile 2003 SE, and Windows Mobile 5.0 were its foundation. In the late 2000s, Windows Mobile 6.0, 6.1, and 6.5 were introduced, and Windows Phone 7 and 7.5 (Mango) followed in the early 2010s. The OS was renamed Windows 10 Mobile in 2015, after the release of Windows Phone 8 and 8.1 in 2012 and 2013, respectively. However, Microsoft's entry into the mobile phone industry ended in 2017 when it stated that mainstream support for Windows Phone 8.1 and Windows 10 Mobile would expire in 2019 [2].

The mobile OS underwent various improvements and changes to its user interface, features, and functionality to keep up with the rapidly evolving mobile landscape. The new interface, for example, was designed to be more modern, user-friendly, and optimized for touchscreens, as touchscreen technology was becoming more prevalent in smartphones. Windows 10 Mobile was also released to deliver a consistent experience across all Windows devices, such as PCs, tablets, and smartphones. However, despite these efforts, Windows Mobile failed to gain a significant market share and eventually faced stiff competition from other mobile operating systems, such as iOS and Android [3].

Several factors contributed to the decline and eventual termination of Windows Phone. Some of the key reasons are as follows:

- **Poor Sales Performance**: The inability of Windows Phone to establish momentum in the market was one of the main causes of its eventual demise. IDC reported that Windows Phone only had 2.7 per cent of the worldwide smartphone market in 2015, while Android had 81.5 per cent and iOS had 15.9 per cent [4].
- **Lack of App Support**: The lack of app support on Windows Phone is primarily a result of the platform's difficulty in attracting and retaining developers. Popular apps like Snapchat and WhatsApp were unavailable or were supported poorly on Windows Phone, which was a major problem for users. As a result, users often turned to other platforms with more robust app ecosystems. Compared to Android and iOS, there were a limited number of tools for the assurance of the extensibility, performance, scalability, and robustness of apps under Windows OS [5]. The lack of such automatic assurance tools opens doors for adversaries for malicious purposes.
- **Stiff Competition**: Established smartphone platforms like Android

and iOS were competitive with Windows Phone. These platforms provided customers with a vast array of features and functionalities and had already cemented a solid position in the industry. This made it difficult for Windows Phone to differentiate itself and gain a competitive advantage.

Instead of focusing on building and maintaining its own mobile OS, Microsoft shifted its attention to creating applications and services for other mobile OSes, such as Android and iOS. Additionally, Microsoft is now focusing on offering enterprise mobility solutions through tools, such as Microsoft Endpoint Manager and Microsoft 365, which enable businesses to manage and secure their mobile devices, applications, and data. This move suggests that Microsoft is still invested in the mobile space, but is choosing to approach it from a different angle that better aligns with its current strengths and market realities [6].

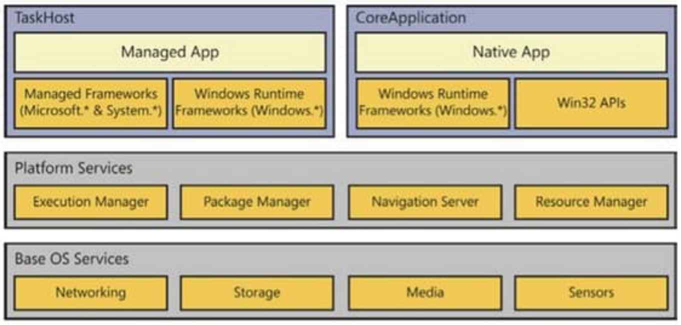


Figure 2: Windows Phone Architecture [c4-5]

Although the Windows Phone architecture is similar to that of the Windows OS for desktop computers, some differences arise as a result of the particular hardware and software requirements of the mobile platform. As shown in **Figure 2**, the architecture of Windows Phone is a sophisticated system of components that work together to provide a seamless user experience. At the heart of this architecture are several crucial elements that are instrumental in ensuring the stability and performance of the platform. These elements include the Task Host, which manages the processing of background tasks; the Core Application, which provides a range of services to developers; and the Platform Services, which allow the applications to interact with the underlying hardware. The Base OS Services also provide a range of low-level services critical to the platform's proper functioning. The following list provides an explanation of each component:

- **Task Host**: Although it is tailored for mobile devices, the Task Host in Windows Phone is similar to the one in desktop Windows. It controls the background operations and tasks, ensuring they function correctly without affecting the system's overall performance.
- **Core Application**: The Start screen, Phone, Messaging, and other essential applications that offer customers critical functionality are included in Windows Phone's basic Applications. These applications are made to function perfectly with other elements of the OS and are tailored for the mobile platform.

- **Platform Services**: Platform Services in Windows Phone provide system-level services that support the OS and applications. These services include security services, networking services, device management services, and others. Like desktop Windows, they are designed to be extensible so that developers can create custom application services. The platform services have four sub-components, namely Execution Manager, Package Manager, Navigation Server, and Resource Manager.
- **Base OS Services**: In Windows Phone, base OS services include kernel-level services for managing system resources, drivers for hardware devices, and other low-level services essential to the system's operation and ensure the OS functions effectively, and are tailored for mobile devices. The base OS services have four sub-components: Networking, Storage, Media, and Sensors.

The Windows Phone was primarily written using C++ and C#. Higher-level apps and user interfaces were created using C#, while lower-level system components were created using C++. The platform also used other programming languages for web-based applications, including JavaScript and HTML5.

For instance, Windows Phone 7 is written in .NET managed code, which handles error-prone tasks. It supports two popular programming platforms, Silverlight and XNA, and development is done in Visual Studio. Programs are packaged into XAP files, which are Silverlight application packages. In conclusion, C++ and C# were combined to create Windows Phone, with support for JavaScript and HTML, among other languages [7].

## 2. Getting into Cybersecurity: Windows Vulnerabilities and Risks

One of the key features of Windows Phone is its security measures. Like Apple's iOS, Windows Mobile OS takes a proactive approach to security by vetting and approving each piece of software uploaded to the Windows Store. This ensures that harmful programs cannot be downloaded onto the device, providing a safer and more secure user experience. In contrast to Android OS, Windows Mobile does not require special antivirus or anti-malware software, further simplifying the user experience.

The Microsoft Windows OS was the safest mobile OS for enterprises (from 2006 until 2009) before it was discontinued in 2010. In contrast, Android continues to be the mobile device paradise for cybercriminals. Look at **Table 1** for Windows OS vulnerabilities trends with the following categories of vulnerabilities:

- Denial of Service (DoS): DoS aims to bring down a computer system or network so its intended users cannot access it. DoS attacks achieve this by bombarding the victim with excessive traffic that causes a crash.
- Code Execution: An attacker could exploit this flaw remotely to execute malicious code. An attacker can remotely execute

commands. No matter where the device is physically located, remote code executions can happen.

- Overflow: This involves code execution due to a buffer overflow. A buffer, in this context, is a sequential area of memory set aside for storing anything from a character string to an array of numbers. Writing outside the boundaries of a block of memory that has been allocated can corrupt data, cause a program to crash, or even execute malicious code.
- Memory Corruption: This vulnerability in computer systems can happen when memory is changed without a clear assignment. Programming flaws cause the contents of a memory region to change, allowing attackers to execute malicious code.
- SQL Injection (SQLi): SQLi injection enables an attacker to alter the database queries that an application makes. SQL injection exploits holes in websites or computer programs, typically through data entry forms.
- Cross-Site Scripting (XSS): XSS attacks occur when an attacker sends malicious code, typically a browser-side script, to a separate end user using an online application.
- Directory Traversal: Directory traversal enables an attacker to access any files on the server hosting an application. This could comprise critical operating system files, back-end system login information, application code and data.
- Authentication Bypass: This attack uses weak authentication protocols to provide hackers access to systems and data, including stealing legitimate session IDs or cookies to bypass the device's authentication system.
- Information Gain: This permits a local attacker who has been authenticated to obtain authentication details and gain unauthorized access to the system or database.
- Privilege Escalation: A privilege escalation attack aims to break into a system with privileged access without authorization. Attackers exploit user error or design weaknesses in operating systems or web applications.

**Table 1**: Windows Mobile OS vulnerabilities trends from 2006 to 2009[1]

| **Year** | **Types of Vulnerabilities** | | | | | | | | | | **Total Number of Vulnerabilities** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **DOS** | **CE** | **OF** | **MC** | **SQLI** | **XSS** | **DT** | **AB** | **IG** | **PE** | |
| 2006 | ✓ | ✓ | ✓ | | | | | | | | 1 |
| 2007 | ✓ | | ✓ | | | | | | | | 4 |
| 2008 | ✓ | | | | | | | | | | 1 |
| 2009 | | ✓ | | | | | ✓ | | | | 1 |
| DOS: Denial of Service<br>CE: Code Execution | | | | | | | | XSS: Cross-site Scripting<br>DT: Directory Traversal | | | |

| | |
|---|---|
| OF: Overflow | AB: Authentication |
| MC: Memory Corruption | BypassIG: Information Gain |
| SQLI: SQL Injection | PE: Privilege Escalation |

## 3. Adversarial techniques

Compared to Android and Apple iOS, Windows Phone has become less popular among users. Few techniques used for adversarial purposes against the Windows Phone OSs have been detected. Since the exact security mechanisms used for Windows OSs (PC) are employed to protect against emerging security threats for Windows Phone OSs [8], similar adversarial techniques are commonly used to compromise the Windows Phone OSes. So many third-party apps are widely available for Windows PCs and Phones, making it possible for adversaries to employ Windows malware to compromise smartphones. Any interaction between a Windows PC and a Windows phone (e.g., software updating and file transferring) opens a door for an adversary. In **Table 2** some of the adversarial techniques that are used to compromise a Windows Phone are listed.

**Table 2**: Adversarial Techniques for Windows Phone [8]

| **Attack Phase** | **Adversarial Technique** | **Description** | **Sample Malware** |
|---|---|---|---|
| Propagation | Removable Media | Exploiting or copying malware to a Windows Phone connected to a Windows PC via USB. | DualToy [9], |
| | | Tracking a device's physical location through standard OS APIs via malicious/spyware applications on the compromised device. | |
| Activation | Privilege Escalation | Exploiting the software vulnerabilities, including a programming error in an application, service, OS's software, or kernel, to elevate privileges and execute an adversary-controlled code. | FinFisher [10] and Wingbird [11] |
| Carrier | Web Protocols | Avoiding detection/network filtering by blending the malicious traffic in with | Dark Caracal (Adds a registry key |

| | | | |
|---|---|---|---|
| | | existing traffic (e.g., HTTP/S) or mobile messaging services (e.g., Google Cloud Messaging (GCM) or Firebase Cloud Messaging (FCM)) | to the Windows folder or abuses Word documents macros) [12] |
| Persistence | Hijack Execution Flow | Abusing Windows' *KernelCallbackTable* is a process to hijack its execution flow to run the malicious payloads. | FinFisher [10] and Wingbird [11] |

## 4. Dissecting Malware: Types of Windows Phone OS Malware

The emergence of mobile technology has brought with it a new set of security challenges, and Windows Phone OS is no exception. Malware designed for Windows phones can cause significant harm to users and their data. To understand the different types of Windows Phone malware, a taxonomy can be established based on the method of attack, as shown in **Figure 3**.

This taxonomy categorizes Windows Phone malware into four categories: Trojanized Gaming Applications, Code Execution, Man-in-the-middle Attacks, and Cross-Platform Viruses. In this taxonomy, each category represents a distinct method that malware authors can use to compromise Windows Phone OS devices. By understanding the attack methods, users and security professionals can take steps to protect their devices against these types of malware.

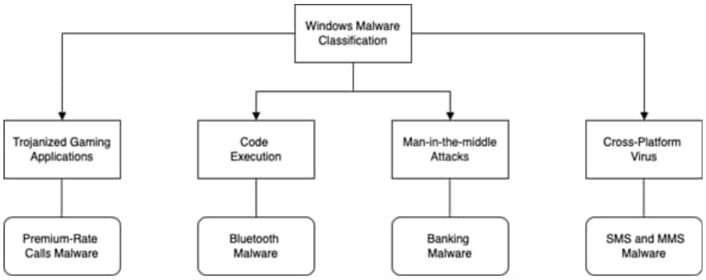

Windows Malware Classification
Trojanized Gaming Applications
Code Execution
Man-in-the-middle Attacks
Cross-Platform Virus
Premium-Rate Calls Malware
Bluetooth Malware
Banking Malware
SMS and MMS Malware

Figure 3: Taxonomy of Windows Phone OS malware

- **Trojanized Gaming Applications:** Trojanized gaming applications are a common type of malware that masquerades as a legal game or gaming application to lure victims, particularly gamers. According to a report by NortonLifeLock, in 2020, the number of malware detections for gaming-related threats increased by 340 per cent [13]. For instance, Windows-based smartphones have been infected by the malicious software "Dialer.BZ," built in 2015 and used to make illegal calls to premium-rate phone numbers, racking up expensive costs on the victim's phone bill. Microsoft stated that the attack affected users in countries such as Spain, Italy, Turkey, and India, and that they worked with local authorities to take down the infrastructure supporting the malware [14].

- **Code Execution:** Malware frequently uses code execution to compromise a target system and run malicious programs. This kind of attack can make use of vulnerabilities in the operating system or other software. The WannaCry ransomware outbreak, which hit thousands of computers worldwide in 2017, is a well-known illustration of code execution [15]. The attacker, who took advantage of a flaw in the Microsoft Windows operating system, encrypted data from the victim and demanded a ransom to decrypt it. One incident that involved code execution through Bluetooth malware on Windows Phone was reported in 2014. The malware, called "Kemoge," was distributed through third-party app stores disguised as popular apps like Facebook, WhatsApp, and Twitter. Once installed on the victim's device, it would silently connect to a remote server and download additional malware [16].
- **Man-in-the-middle Attacks:** Man-in-the-middle (MITM) attacks are a type of cyberattack in which an attacker eavesdrops on and alters the communication between two parties to steal sensitive data or engage in malicious activity. According to a report by Akamai, MITM attacks increased by 54 per cent in the first half of 2020 compared to the second half of 2019 [17]. MITM attacks with banking malware are a common threat to all mobile devices, including Android and iOS. These attacks typically involve intercepting the communication between the user and their bank's server, allowing the attacker to steal the user's login credentials and other sensitive information. One such incident occurred in 2015 when a banking Trojan called "Acecard" was discovered to target Windows Phone users and Android users. The malware was designed to steal banking credentials and other sensitive information by overlaying fake login screens over legitimate banking apps. The Acecard Trojan was distributed through various channels, including spam emails and third-party app stores [18].
- **Cross-Platform Virus:** Cross-platform viruses are malware that can infect several different operating systems or platforms, making them challenging to find and eliminate. One well-known example is the Mirai botnet, which targeted Internet of Things (IoT) gadgets, including routers, cameras, and DVRs. The botnet could infect devices running various operating systems, including Windows, Linux, and Android [19]. There have been reports of SMS/MMS malware affecting Windows Phone in the past. One such incident occurred when an SMS-based malware campaign called "SMSTrack" was discovered. The malware was spread through SMS messages that appeared to be legitimate tracking messages from popular delivery services but contained a malicious link that, when clicked, downloaded malware onto the device [20].

## 5. Mitigating Windows Attacks: The current solutions

Analyzing security threats (man-made or machine-made) is needed to identify and mitigate security attacks against mobile OSes. Modern information security solutions (e.g., machine-learning-based approaches) rely on identifying anomalies that can identify false positive results, creating a sense of mistrust toward the system and thus requiring human effort to investigate cases. Effective artificial intelligence solutions can be used to improve situational awareness and implement effective protection measures [21]. A variety of artificial intelligence-based cybersecurity solutions are already introduced and reused for end devices (e.g., mobile devices, including Windows Phones), as follows:

- IBM MaaS360 Mobile Device Management (SaaS) [22]

  IBM Maas360 provides a cloud-based Unified Endpoint Management (UEM) solution to manage and secure endpoints and end users, including applications, content, and data. MaaS360 can be utilized on all major mobile computing platforms, such as iOS, Android, and Windows Phones [21]. IBM MaaS360 Enterprise Mobility Management (EMM) tool is a mobile device management (MDM) tool introduced for Windows Phone devices. It has various features, including managing applications, devices, browsers, and email. It also provides some other unique solutions, such as mobile expense management, secure sharing of documents, and mobile threats management [23].

- Deep Instinct [24]

  In this solution, deep learning algorithms are employed to identify structures used in malicious software. Deep Instinct can detect and prevent the execution of malicious software at all levels of the organization. To comprehensively analyze an attack, find how it has taken, and what kind of endeavors adversaries had, Deep Instinct has an On-Time Review and Remediate layer functionality, which provides visibility into the threats [21].

- SparkCognition DeepArmor

  SparkCognition, an artificial intelligence system, has launched its DeepArmor solution to cybersecurity, which uses machine learning to identify unknown data and detect cyber threats. DeepArmor aims at fixing the vulnerability of the endpoint networks, such as laptops, mobile devices, and sensors [25].

- IBM QRadar [26]

  QRadar Security Platform, designed by IBM for information security analysis, reveals hidden threats and automates the authentication process of threats. This system provides automated threat investigations and uses Artificial Intelligence to detect high-level risks. QRadar implements local data mining of information security attacks by collecting relevant network data [21]. IBM QRadar Advisor with Watson provides automated research for threats and actors [27].

## 6. Utilizing Windows Mobile Services: The

### trend now

Unfortunately, Windows Phone has been discontinued by Microsoft since 2019, and there are no new trends in Windows Phone app development. Instead, Microsoft's current focus on mobile devices is on creating applications and services for other operating systems like Android and iOS, and offering enterprise mobility solutions through tools like Microsoft Endpoint Manager and Microsoft 365. The following are some of the trends in Microsoft Mobile Services:

- Developing cross-platform mobile apps using Xamarin, a tool for building native Android, iOS, and Windows apps with a shared codebase and user interface. For example, the mobile banking app of ANZ Bank uses Xamarin to provide a consistent user experience across different platforms.
- Leveraging Microsoft Endpoint Manager and Intune, cloud-based services for managing mobile devices and applications in the enterprise. For instance, Liberty Mutual Insurance Company uses Intune to deploy and manage apps on its employees' Windows phones and tablets.
- Built and deployed custom line-of-business apps on Windows phones and tablets, using tools like Power Apps, Power Automate, and Power BI. These apps can integrate with other Microsoft services, such as Dynamics 365 and SharePoint. For instance, the sales team of Vodafone Netherlands uses Power Apps to access and update customer information on the go.
- Developing Internet of Things (IoT) solutions with Windows 10 IoT Core and Azure IoT services. For example, the HoloLens, a mixed-reality headset developed by Microsoft, uses Windows 10 IoT Core and Azure IoT to connect and control smart devices in a manufacturing plant.

### 7. What is Next:

Windows Phone OS was a mobile OS developed by Microsoft Corporation to compete with other mobile platforms, such as iOS and Android. However, despite being praised for its unique and innovative design, it struggled to gain significant market share, eventually fading away. Throughout its development and existence, Windows Phone OS faced several security challenges, including malware attacks and vulnerabilities, prompting researchers to study various aspects of its security. Despite the decline of Windows Phone OS, the lessons learned from its development and security challenges remain relevant to the mobile industry. As mobile technology evolves, staying updated with the latest security trends and best practices to mitigate potential risks and threats is essential. In conclusion, Windows Phone OS may no longer be a player in the mobile market. Still, its history and security challenges provide valuable insights into the future of mobile security.

The next article in this series, "Understanding Cybersecurity on Smartphones (UCSSPh): Symbian, Tizen, Sailfish, Ubuntu, KaiOS, Sirin and Harmony," will focus on the other seven public mobile OSs.

References:

[1] "Windows Mobile OS: A Brief History" by Sagar Khillar, Interesting Engineering, July 9, 2020.

[2] "A Brief History of Windows Mobile OS" by Russell Holly, Android Central, January 30, 2016.

[3] "A Visual History of Windows Mobile" by Daniel Rubino, Windows Central, April 29, 2015.

[4] IDC. (2016). Smartphone OS Market Share, 2015 Q4. Retrieved from https://www.idc.com/promo/smartphone-market-share/os

[5] Mohammad, Duaa R., Sajedah Al-Momani, Yahya M. Tashtoush, and Mohammad Alsmirat. "A comparative analysis of quality assurance automated testing tools for Windows mobile applications." In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0414-0419, 2019.

[6] Jansen, W. (2021). Microsoft 365 for Business and Enterprise. Springer International Publishing.

[7] Grønli, T. M., Hansen, J., Ghinea, G., & Younas, M. (2014, May). Mobile application platform heterogeneity: Android vs. Windows Phone v.s iOS vs. Firefox OS. In *2014 IEEE 28th International Conference on Advanced Information Networking and Applications* (pp. 635-641). IEEE.

[8] Ahvanooey MT, Li Q, Rabbani M, Rajput AR. A survey on smartphone security: software vulnerabilities, malware, and attacks. arXiv preprint arXiv:2001.09406. 2020

[9] Claud Xiao, DualToy: New Windows Trojan Sideloads Risky Apps to Android and iOS Devices, 2016.

[10] Allievi, A.,Flori, E. FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines. 2018. https://www.microsoft.com/en-us/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

[11] Microsoft. Twin zero-day attacks: PROMETHIUM and NEODYMIUM target individuals in Europe. 2017. https://www.microsoft.com/en-us/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/?source=mmpc

[12] Lookout, Dark Caracal: Cyber-espionage at a Global Scale, 2018, https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

[13] NortonLifeLock. (2021). NortonLifeLock Cyber Safety Insights Report.

[14] Microsoft. (2015, July 23). Dialer.BZ: Premium phone scam trojan on Windows phones. Microsoft Security.

[15] BBC News. (2017). WannaCry ransomware cyber-attacks slow but fears remain. Retrieved from https://www.bbc.com/news/technology-39901382

[16] Luo, Y., Zhu, H., Wang, Z., & Liu, P. (2016). Kemoge: Understanding Mobile Ad Fraud in Action. Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC).

[17] Akamai. (2020). State of the Internet / Security: Phishing for Finance.

[18] "Acecard banking trojan now targeting Windows Phone users," SC Magazine, 2015.

[19] KrebsOnSecurity. (2016). KrebsOnSecurity Hit With Record DDoS. Retrieved from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[20] "Windows Phone SMS malware threat discovered in Russia" by Anthony Cuthbertson (2016)

[21] Vähäkainu, Petri, and Martti Lehto. "Use of Artificial Intelligence in a Cybersecurity Environment." In Artificial Intelligence and Cybersecurity: Theory and Applications, pp. 3-27. 2022.

[22] IBM, IBM MaaS360 Mobile Device Management (SaaS), visited in 2023 https://www.ibm.com/docs/en/maas360

[23] IBM, Windows Phone 8 device MDM, visited in 2023 https://www.ibm.com/docs/en/maas360?topic=windows-enrolling-your-phone-8-device-mdm

[24] Deep instinct, https://www.deepinstinct.com/

[25] Zhang, YuLong, ZiJie Dai, LongFei Zhang, ZhengYi Wang, Li Chen, and YuZhen Zhou. "Application of Artificial Intelligence in Military: From Projects View." In 2020 6th International Conference on Big Data and Information Analytics (BigDIA), pp. 113-116. 2020.

[26] IBM Security QRadar Suite, IBM, https://www.ibm.com/qradar?utm_content=SRCWW&p1=Search&p4=43700074872917601&p5=e&gclid=CjwKCAjw1MajBhAcEiwAagW9MRLPpIdZxX5v4Cref8OJHY9QwQ35RD6wxdScMcFG4D4tMsWk gclsrc=aw.ds

[27] Sadowski G, Kavanagh K, Bussa T. Critical Capabilities for Security Information and Event Management. Gartner Group Research Note. 2020.

[1] Data collected from https://www.cvedetails.com/product/9709/Microsoft-Windows-Mobile.html?vendor_id=26