Cyber Espionage – A Threat to Humanity

Akshit Kurani[1], Prakruti Joshi[2], Hrisha Yagnik[3]

[1-3]Student, Department of Computer Engineering, Indus University, Ahmedabad, India

---***---

Abstract - ***Cyber Espionage*** *is a kind of cyber-attack. It steals data and even intellectual property to get some benefits over a particular company. It is now growing in a big number looking into the benefits of the nation by* ***attacking privacy*** *of the target ones. It generally happens using* ***Slingshot*** *but there are some other methods also available for it. It is generally done with evil motive but it can be detected or even* ***avoided*** *using some techniques discussed in the paper.*

Keywords: *Cyber Espionage, Slingshot, Privacy, Cyber Attack, Data Privacy.*

1. INTRODUCTION

Cybersecurity is a global challenge as Cyberspace is never risk free. [1] Now, Cyber espionage can be considered to be an act against cybersecurity that steals classified and sensitive data or even intellectual property to get benefits over a particular company. Generally, it's an act done against government or military infrastructure to steal their data. It's a notorious practice to damage or even misuse the data for political or even economic advantages apart from military ones. The threat actors who do this act can be either state actors or nation-states with a sole motive of gaining advantage in the world of cyber espionage. Cyber Espionage is emerging along with the expansion of the World Wide Web, which origins a gigantic impact either on heavy solid economic, politic, agency groups, or on individual people[2].

An Iranian cyber-espionage group called APT39 was recently caught by California-based cybersecurity firm FireEye. They had set their most of the targets to be telecommunication firms in the Middle East. The study also found that the group's activities were in the favour of Iran. They had targeted the telecommunication industry with a strong reason to get the personal and customer data and the telecommunication industry stores a huge amount of personal and customer data and hence it resulted in a wide range of potential and ill minded targets across multiple verticals. Also, challenges in cybersecurity are tough as the trends are in demand and also the new attacks are exploiting the vulnerabilities easily.[3]

1.1 Espionage in Nations

Espionage among nations is something that is not new for nations. It has always existed since the early medieval period. But, these days, spies have evolved to one of the greatest numbers and due to it, we are facing one of the greatest challenges under the name of cyber espionage which is since a long time now. This is something that makes use of cyber warfare techniques to gain military, economic or even political benefits. It is also well organized and deliberate which makes it even more difficult to detect.

1.2 Growth of Espionage

Organizations or even various nations are now hiring various skilled cyber criminals to damage or steal data or even shut down government or military infrastructures. They even try to gain unauthorized access to financial systems through these criminals. These events may not look to be big enough but the fact is they are highly capable of creating a situation of complete chaos and that too on a global level. They can change the outcome of major political elections or even create mayhem at international events which might turn out to be a major event on the globe. The most disturbing portion of this cyber espionage is that the perpetrator follows the modus operandi and hence ensures that their tracks remain untraceable even after job has been done for years on end.

2. HOW DOES IT HAPPEN?

The exact method used in the first instance by Slingshot to exploit the routers is not yet clear. This links to the router and downloads some DLLs (dynamic link libraries) from the router file system when the target user runs Winbox Loader program (a tool used for Mikrotik router configuration). The APT has put one of them, ipv4.dll, with what is in fact, a downloader for other malicious components. This ipv4.dll library is downloaded by Winbox Loader to the target device, loaded into memory and executed. This DLL then links to a hard-coded IP and port (we saw it was the IP address of the router in every case), downloads and runs the other malicious components.

Slingshot loads vulnerable drivers and runs its own code through their vulnerabilities to run its code in kernel mode in the most recent versions of operating systems, which have Driver Signature Compliance.

Slingshot will load a variety of modules onto the victim system following infection, including two large and powerful ones: Cahnadr, the module for kernel mode, and GollumApp, a module for user mode. In information collection, persistence and data exfiltration, the two modules are related and able to support each other.

2.1 GollumApp

GollumApp is the most sophisticated module. This comprises close to 1,500 user-code functions and provides much of the persistence, file system access and C&C communications routines mentioned above. Canhadr, also known as NDriver, includes network, IO operations and so on low-level routines. The kernel-mode software will execute malicious code without crashing the entire file system or triggering a remarkable achievement for Blue Screen. Written in pure C language, despite device protection restrictions, Canhadr/Ndriver offers complete access to the hard drive and working memory and performs integrity monitoring of different machine components to prevent debugging and safe

2.2 Motive of attack

State-sponsored and private cyber espionage and criminal and foreign-intelligence surveillance have ramped up in part because the national security threat environment is ever more complicated and multifaceted, and the ability to meet it is increasingly dependent on good intelligence, in real time.[4] Cyber-espionage appears to be Slingshot's main aim. Analysis includes that screenshots, keyboard data, network data, passwords, USB connections, other desktop activities, clipboards, and more are obtained. But it can steal whatever it wants with complete access to the kernel portion of the system: credit card numbers, password hashes, social security account numbers, any form of data

3. REASONS BEHIND LONG LASTING ATTACK

The threat actor combined a range of existing methods to protect it from detection very effectively: including encrypting all strings in its modules, explicitly calling system services to circumvent security Product hooks, using a variety of methods for anti-bug use, and more.. In addition, it may shut down its modules, but ensure that before closing, they complete their tasks. When there are signs of an imminent in-system occurrence, such as a system shutdown, this mechanism is triggered and is possibly introduced to allow malware user-mode components to properly complete their tasks to avoid detection during any forensic testing.

This APT uses its own encrypted file system and can be found in an unused portion of a hard drive, among others. The defragment tool relocates data on the disk during defragmentation, and this tool will write anything to sectors where Slingshot holds its file systems (because the operating system thinks these sectors are free). The encrypted file system would be affected by this. In order to avoid this from occurring, we assume that Slingshot attempts to disable defragmentation of these particular areas of the hard drive.

4. VICTIMS

Cyberspace is essential in modern warfare at the operational level, where soldiers are increasingly dependent on cyberspace; and at the strategic

level, where a state's weaknesses and strengths in cyberspace can be used to deter and affect the strategic balance of power.[5] In Kenya, Yemen, Afghanistan, Libya, Congo, Jordan, Turkey, Iraq, Sudan, Somalia and Tanzania, researchers have seen about 100 victims of Slingshot and its associated modules so far. Instead of corporations, most of the victims tend to be targeted people, although there are several government organizations and institutions. Kenya and Yemen account for the bulk of the casualties confirmed to date.

5. STEPS TO PREVENT IT

Kaspersky Lab researchers suggest adopting the following steps in order to prevent falling victim to such an attack:

- To ensure security against known vulnerabilities, users of Mikrotik routers should update as soon as possible to the latest software edition. In addition, Mikrotik Winbox does not download anything from the router to the user's device anymore.

- Use a proven corporate-grade protection solution in conjunction with anti-targeted attack technologies and threat intelligence, such as Kaspersky Threat Management and Defense, which can spot and capture advanced targeted attacks by analyzing network anomalies and providing full visibility to cybersecurity teams across the network and automation of responses;

- Provide security personnel with access to the latest information on threat intelligence, which will arm them with valuable targeted attack analysis and mitigation resources, such as vulnerability indicators (IOC), YARA and personalized advanced threat reporting;

- If you recognize early signs of a targeted attack, consider controlled security services that help you to proactively identify advanced threats, minimize dwelling time and coordinate timely incident response.

6. CONCLUSION

With the advancement in technology, criminals don't have to go outside to commit a crime or they don't need any physical weapons.[6] Cyber Espionage is a cyber threat of sorts. To get any advantages over a specific business, it steals data and even intellectual property. It is now increasing in a large number by targeting the privacy of the targets, investigating the gains of the country. It typically happens using Slingshot, but some other techniques are also available for it. It is normally done for evil reasons, although certain strategies discussed can be used to identify or even prevent it. The threat of computer crime is not as big as the authority claim and hence its developing quickly.[7]

REFERENCES

[1] Giribabu D. et al, "Cyber Security in WebGIS Environment" International Journal of Computer and Internet Security, ISSN 0974-2247 Volume 10, Number 1, 2018

[2] Magalhães R., Barbosa H., "Cyber Espionage and Digital Privacy" International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 8, Issue 1, January-2017

[3] Madhusmita Rout, Amandeep Kaur "A review on Cybersecurity and its challenges" JETIR, ISSN-2349-5162 Volume 5, Issue 11, November 2018

[4] William C. Banks "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage" Emory Law Journal, Volume 66 Issue 3, 2017

[5] Hjortdal, Magnus "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence "Journal of Strategic Security, Volume 4, Number 2, 2011

[6] Mahima Rai, H.L.Mandoria "A STUDY ON CYBER CRIMES, CYBER CRIMINALS AND MAJOR SECURITY BREACHES" International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 06 Issue: 07 | July 2019

[7] Darshit Shah, Lokesh V.Soni, Dharmit Tailor,Pratyush Shukla "Cyber Crime and Security", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 03 Issue: 03 | Mar-2016