Proceedings of the 2024 Winter Simulation Conference
H. Lam, E. Azar, D. Batur, S. Gao, W. Xie, S. R. Hunter, and M. D. Rossetti, eds.

IMPACT OF OPERATING SYSTEM UPDATES ON CYBERCRIMINAL ACCESS DURATION: A SIMULATION-BASED STUDY

Jeongkeun Shin[1], Tanav Changal[3], L. Richard Carley[1], and Kathleen M. Carley[2]

[1]Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA
[2]Software and Societal Systems Department, Carnegie Mellon University, Pittsburgh, PA, USA
[3]Troy High School, Fullerton, CA, USA

ABSTRACT

For the best cybersecurity practices, it is essential to employ up-to-date operating systems. Organizations using outdated systems, particularly those no longer supported by manufacturers, are exposed to a broader spectrum of vulnerabilities. These vulnerabilities offer cybercriminals various opportunities to exploit during their attacks, increasing the likelihood of achieving their objectives. This paper leverages agent-based modeling to assess the risks associated with using outdated operating systems in organizations. We simulate a spearphishing campaign targeting virtual organizations that utilize either up-to-date or outdated operating systems. Our simulations incorporate a comprehensive cyber warfare scenario that includes MITRE ATT&CK-based cyber attack and defense strategies, alongside a detailed organizational model. We find that when defense strategies fail to address vulnerabilities unique to outdated systems, cybercriminals can maintain persistent access to compromised devices. This results in significantly longer access times for attackers compared to organizations with modern operating systems.

1 INTRODUCTION AND CYBER WARFARE SCENARIO MODEL

Using outdated operating systems increases vulnerabilities that cybercriminals can exploit during their campaigns. One example is the AppInit DLL, a weakness in Windows 7 operating system's design, which cybercriminals could potentially exploit to establish persistence on compromised devices (Shin et al. 2023). To assess how this vulnerability influences the duration of a cybercriminal's access to compromised computing devices, we used OSIRIS (Shin et al. 2024) to simulate cyber warfare scenarios. We constructed three virtual organizations comprising 235 end user agents with uniquely calculated phishing susceptibilities based on various human factor variables (Shin et al. 2024). All members of the first organization operate with the up-to-date Windows 11 operating system. In the second organization, half of the members use Windows 11 and the other half use Windows 7. All members of the last organization use the outdated Windows 7 system. Then, we modeled and simulated a basic cyber attack campaign, covering actions from the Initial Access to Persistence tactics, utilizing various cyber attack techniques from the MITRE ATT&CK framework (Strom et al. 2018), as outlined in Figure 1. In this simulation, a cybercriminal agent distributes spearphishing emails to all end user agents within the organization **(T1566.001)**, leading some to execute a malicious file attached to the email **(T1204.002)**. Upon gaining access to the computing devices of the deceived end user agents, the cybercriminal agent identifies the operating system version

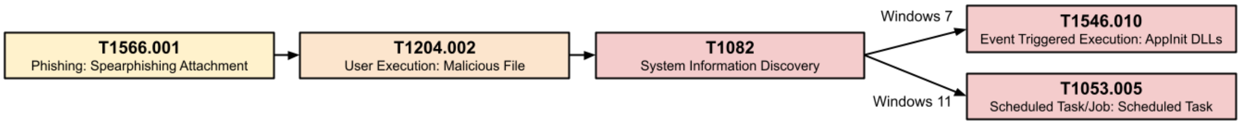
T1566.001
Phishing: Spearphishing Attachment
T1204.002
User Execution: Malicious File
T1082
System Information Discovery
Windows 7
T1546.010
Event Triggered Execution: AppInit DLLs
Windows 11
T1053.005
Scheduled Task/Job: Scheduled Task

Figure 1: Cyber attack scenario.

(T1082). For devices running Windows 11, it establishes persistence via Scheduled Tasks **(T1053.005)**. For those on Windows 7, persistence is achieved by manipulating the AppInit DLL **(T1546.010)**. To counteract potential intrusions, the organization has implemented a defense strategy that involves periodically inspecting unauthorized connections and analyzing scheduled job activities, corresponding to Scheduled Job Analysis **(D3-SJA)** in MITRE D3FEND (Kaloroumakis and Smith 2021). This strategy, optimized for up-to-date operating systems, fails to detect the exploitation of the AppInit DLL. This oversight allows cybercriminals to restore their connection to devices running the Windows 7 OS upon reboot, even after being detected and disconnected. We simulated this cyber warfare scenario with varying average inspection frequencies: 1, 2, 3, and 4 times per day.

2 SIMULATION RESULTS AND FUTURE WORKS

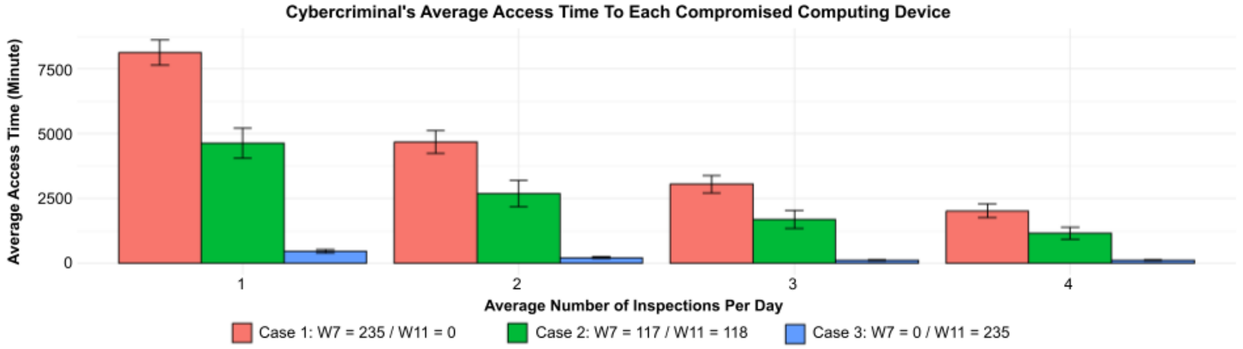

Figure 2: Simulation results.

Figure 2 summarizes our simulation results. Our simulation study underscores the importance of using recent operating systems. Employing outdated systems provides cybercriminals with opportunities to exploit additional vulnerabilities, thereby granting them extended access to compromised devices. This extended access increases their chances of achieving their malicious objectives. In future work, we plan to model additional vulnerabilities associated with the use of old operating systems or software that lack current updates. Then, we will expand our attack scenarios to include post-persistence activities. This will allow us to better assess the potential scale and impact of damage from various cyber attack scenarios.

ACKNOWLEDGMENTS

The author(s) disclosed receipt of the following financial support for the research and publication of this article: This research was supported in part by the Minerva Research Initiative under Grant #N00014-21-1-4012. The views and conclusions are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research or the US Government.

REFERENCES

Kaloroumakis, P. E. and M. J. Smith. 2021. “Toward a Knowledge Graph of Cybersecurity Countermeasures”. *The MITRE Corporation* 11.

Shin, J., L. R. Carley, and K. M. Carley. 2024. “Simulation-Based Study on False Alarms in Intrusion Detection Systems for Organizations Facing Dual Phishing and DoS Attacks”. In *2024 Annual Modeling and Simulation Conference (ANNSIM)*. May 20th-23th, Washington D.C., United States, Forthcoming.

Shin, J., G. B. Dobson, L. R. Carley, and K. M. Carley. 2023. “Revelation of System and Human Vulnerabilities Across MITRE ATT&CK Techniques with Insights from ChatGPT”. *CASOS Technical Report (2023)*.

Strom, B. E., A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas. 2018. “MITRE ATT&CK: Design and Philosophy”. Technical Report 10AOH08A-JC, The MITRE Corporation, McLean, VA.