Leveraging OSIRIS to simulate real-world ransomware attacks on organization

Jeongkeun Shin
L. Richard Carley

Department of Electrical and Computer Engineering
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213, USA

Geoffrey B. Dobson
Kathleen M. Carley

School of Computer Science
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213, USA

ABSTRACT

The scale of ransomware damage increases every year. It is difficult to predict the magnitude of the ransomware damage to the organization since many human factors are involved as ransomware infection usually starts with end users downloading malware from the phishing email or message. In this paper, we leveraged OSIRIS (Organization Simulation In Response to Intrusion Strategies) framework to simulate the Avaddon ransomware attack to virtual organizations and analyze how three factors, organization size, proportion of communication, and end users' cybersecurity expertise level, affect to the overall impact and propagation of ransomware damage inside the organization.

1 SIMULATION DESIGN AND RESULT

We used the OSIRIS (Shin et al. 2022) framework to set up the virtual organization. End user agents in OSIRIS repeat daily routines. They arrive at work, build formal and informal relationships with other end user agents, do the work with human behavior patterns commonly observed in the organization, and leave the work. While they are working, phishing emails are delivered by cybercriminal agents through email or messenger. Each end user's cybersecurity expertise level property determines the probability to download the malware containing ransomware or spread it to other end user agents in the organization.

OSIRIS' cybercriminal agent originally conducts phishing attacks for general data breach. In this paper, we modified the attacking mechanism to conduct the Avaddon ransomware. Attacking mechanism is similar to that of Cyber-FIT's (Dobson and Carley 2017) offensive troops. However, while Cyber-FIT conducts cyberattacks based on cyber kill chain (Dobson et al. 2018), OSIRIS conducts Avaddon ransomware attack based on MITRE ATT&CK framework (Strom et al. 2018). According to the MITRE ATT&CK, after an end user downloads Avaddon ransomware malware to its computing device, the infection progresses by sequentially following 6 attack tactics composed of 19 attack techniques. Each technique takes 10 ticks to complete, thus 190 ticks are required to make the computing device completely disabled. OSIRIS' security agent randomly selects one end user agent and inspects its computing device every 10 ticks. It has an ability to eliminate the malware if the computing device is not completely disabled yet, but the success rate to remove the malware decreases as the cybercriminal agent's infection step is at the latter stage of the MITRE ATT&CK tactic.

We conducted simulation experiments with 4 different values of organization size, 4 different values of proportion of communication, and 5 different values of cybersecurity expertise levels. For each case, we ran 10 simulations, and calculated the average number of infections and disabled computers. Simulation results are summarized in Table 1. From this result, We could observe that the overall ransomware damage in the organization increases as organization size is larger, proportion of communication inside the organization is higher, and cybersecurity expertise level is lower.

Table 1: Projected overall ransomware damage in the organization.

Org Size	Proportion of Communication	Expertise Level	Total Infections	Standard Deviation	Disabled Computers	Standard Deviation	Proportion of Communication	Expertise Level	Total Infections	Standard Deviation	Disabled Computers	Standard Deviation
10	10%	1	4.2	1.549	1.8	1.033	20%	1	7.8	2.394	2.3	0.823
		2	2.3	1.337	0.7	0.483		2	6	4	2.2	1.686
		3	1.3	1.059	0.6	0.699		3	2.7	1.946	0.8	0.788
		4	0.9	0.737	0.5	0.527		4	0.9	0.875	0.5	0.527
		5	0.6	0.699	0.3	0.483		5	1	0.666	0.4	0.516
	40%	1	14.9	4.067	5.6	1.349	80%	1	20.8	2.347	7.6	1.074
		2	9.7	2.668	3.9	1.791		2	14.1	2.131	5	1.699
		3	5.4	1.712	1.4	0.843		3	7.7	2.057	2.8	1.475
		4	2	1.490	0.6	0.843		4	3	1.054	1.2	1.135
		5	1.4	1.074	0.3	0.483		5	2.4	1.173	0.7	0.948
20	10%	1	11.3	3.198	5.6	1.837	20%	1	14.9	2.233	9	1.632
		2	4.9	1.197	3.1	1.370		2	9.6	3.596	4.9	1.595
		3	2.7	1.159	1.9	1.197		3	5.9	2.514	3.2	1.932
		4	1.1	1.286	0.9	0.994		4	2.1	1.100	0.9	0.875
		5	0.4	0.699	0.2	0.421		5	1.3	1.337	0.8	0.918
	40%	1	24.4	4.115	13.1	1.663	80%	1	32.2	3.583	16.1	1.852
		2	13.4	3.657	8.1	1.852		2	20.6	4.718	11.1	2.469
		3	7.2	2.699	4.1	1.728		3	10.8	3.675	6.8	2.394
		4	5	2.708	2.4	1.776		4	7.4	2.951	3.8	2.043
		5	2.5	1.433	1.2	0.632		5	2.9	1.197	1.6	0.966
40	10%	1	14.9	2.424	11.5	1.715	20%	1	24.9	2.643	18.4	2.756
		2	9.1	2.643	7.4	2.412		2	15.1	2.923	11.3	2.110
		3	2.8	1.619	2.5	1.509		3	8.1	3.212	6.2	2.485
		4	2.6	0.966	2.3	1.059		4	4.7	2.406	3.8	1.751
		5	1.9	1.370	1.7	1.251		5	1.9	0.994	1.7	1.059
	40%	1	37	3.915	26.9	4.408	80%	1	49.3	6.429	32.5	2.013
		2	25.8	4.237	18.3	2.213		2	34.9	2.469	24.9	2.469
		3	14.1	2.469	11.3	3.164		3	20.1	3.541	15.5	2.368
		4	8.1	1.523	6.4	2.011		4	10.8	3.293	8.9	2.131
		5	3.6	1.264	2.9	1.197		5	6.7	2.263	5.1	1.663
80	10%	1	25.5	5.421	23.4	5.440	20%	1	45.3	5.735	38.8	4.825
		2	15	3.333	13	2.538		2	27.9	3.541	24	2.449
		3	7.9	2.330	7.1	2.330		3	14.2	4.104	12.6	4.376
		4	3.9	1.100	3.1	0.994		4	5.7	2.406	4.8	2.299
		5	1.7	1.766	1.6	1.505		5	3.1	2.330	2.7	2.002
	40%	1	67.6	4.427	54.9	4.581	80%	1	84.2	6.425	67.2	2.149
		2	42.8	5.788	34.7	5.926		2	59.4	5.168	48.7	2.869
		3	22.5	3.807	19.1	4.254		3	35.1	4.254	28.6	3.747
		4	13	2.748	11.4	2.756		4	20.6	4.299	18	4.294
		5	6.9	2.846	6.2	2.347		5	9.5	2.758	9	2.494

ACKNOWLEDGEMENT

This research was supported in part by the Minerva Research Initiative under Grant #N00014-21-1-4012, and by the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University. 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

Dobson, G., A. Rege, and K. Carley. 2018. “Informing Active Cyber Defence with Realistic Adversarial Behaviour”. *Journal of Information Warfare* 17(2):16–31.

Dobson, G. B., and K. M. Carley. 2017. “Cyber-FIT: An Agent-based Modelling Approach to Simulating Cyber Warfare”. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, edited by D. Lee, Y. Lin, N. Osgood, and R. Thomson, 139–148. Springer.

Shin, J., G. B. Dobson, K. M. Carley, and L. R. Carley. 2022. “OSIRIS: Organization Simulation in Response to Intrusion Strategies”. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, edited by R. Thomson, C. Dancy, and A. Pyke, 134–143. Springer.

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, The MITRE Corporation.