ANALYSES AND INVESTIGATION OF 0-DAY THREATS WITH FIREEYE

MARTIN RAKOV, VESELKA STOYANOVA*

National Military University Vasil Vevski, Veliko Tarnovo, Bulgaria
e-mails: veselka_tr@abv.bg, rakovm@mail.bg

Abstract. The current report is about the functions for analyzing and investigating 0-day threats using the Endpoint Detection and Response technology of FireEye - HX Endpoint Security. The console is deployed and installed in the Amazon AWS cloud, and the agents have been deployed to over 20 Windows workstations. A few tests were executed on a few machines to analyze the reaction of FireEye when unknown malicious code gets executed on the workstation.

Keywords: 0day, threats, FireEye, edr, endpoint

1. OVERVIEW

In the modern world, big organizations (enterprise or government sector) realize the need for more advanced threat protection engines. The need is driven by the impact of modern cybersecurity attacks and the damage that they cause to those organizations. So, the perimeter defenses of those organizations should be equipped with stronger analyses and incident response capabilities to be able to look deeper into the attacks and investigate and remediate the threats to the users. The most recent research in this area states that being successful in defending the parameter and the endpoint is not only in detection and protection but also in as early as possible investigation and response. In most cases, in huge organizations, around a month or even more to detect a threat successfully, and fully and if there is a breach – to respond and remediate it. Such cases can drastically disturb daily operations, expose sensitive data, or even impact revenue in a negative matter. Also, it can impact customer retention as the organization may go under different legal and regulatory actions. Most of the time, the risks are in [1], [2], [4], and [10]:

– Non-effective strategies for incident response – often, organizations' approach to incident response is connected to wiping the whole compromised system and start-

* Corresponding author
http://doi.org/10.7546/EngSci.LXII.25.01.01

ing from scratch. That strategy is no longer as effective as before because nowadays, modern threat actors are spreading as much as possible inside the organization as quickly as possible. With the establishment of deep footholds before the standard "cleaning" procedure. What is needed is a well-thought-out and thorough strategy for remediation, otherwise, the attacking party can easily maintain the presence and influence they have inside the organization.

- Attackers having access to sensitive data for longer periods of time – the key here is the validation of an alert. If it is successful and there is the exfiltration, without such an ability, the organizations can not really define a strategy of actions or to even realize if an action is needed in this case. All of that gives more time for the attackers to cause damage in any aspect of the organization.
- Reputation damage for the organization - bad incident response practices, ineffectiveness, etc, are the main reasons that raise questions about the management of the organization, about their trustworthiness, and especially about their expertise and competence. This can negatively impact their employees, their users, their customers, investors, and even their media sentiment.
- Exposure to legal liability and compliance – security incidents have to have effective incident management; otherwise, this can get the organization to legal action and getting out-of-compliance with industry regulations and standards. Additionally, the lack of monitoring and especially transparency and visibility into the root causes and consequences of a successful cyberattack can get the company to court. Also, claims of negligence and tricky practices are common in such situations.
- Revelation and risk management – due to the possibility of getting breached, organizations must prepare such a program because the misuse of it can get the organization to impacts such as fines, intangible damage to the reputation, etc. The way to get proper revelation is to quantify the impact properly and at the same time reveal the scope and analyze the breach.

For the need of the report, it was used FireEye HX Cloud appliance, hosted in FireEye EU cloud, and two virtual machines – 1 for the attacker and 1 for the victim. The attacker machine has the operating system – Kali Linux and the victim machine – Windows 7. The simulation was with the well-known 0-day attack "Clandestine Wolf," which FireEye identified that comes from the Chinese hacker group ATP3. The attack goes over multiple vectors of the system, starting from E-mail phishing and ending with the execution of malicious code on the endpoint itself. In the report, we are going to skip the steps of Reconnaissance, Weaponization, and Delivery and will hop straight to the execution of the malicious code on the endpoint machine.

We start with deploying the FireEye agent on the "victims" machines, and that is how they are going to get protected. The installation of the agent is easy – its .msi file, generated from the HX appliance, is coming preconfigured to communicate with the management. After that, we execute the script, which in our case is the bash script that executes malicious code and initiates communication between the endpoint and command and control server (the Kali Linux and based on Metasploit [6], [7] as

shown in Fig. 1. In the beginning, nothing happens, but after 2 minutes, the machines are automatically rebooted with a message warning for this action.

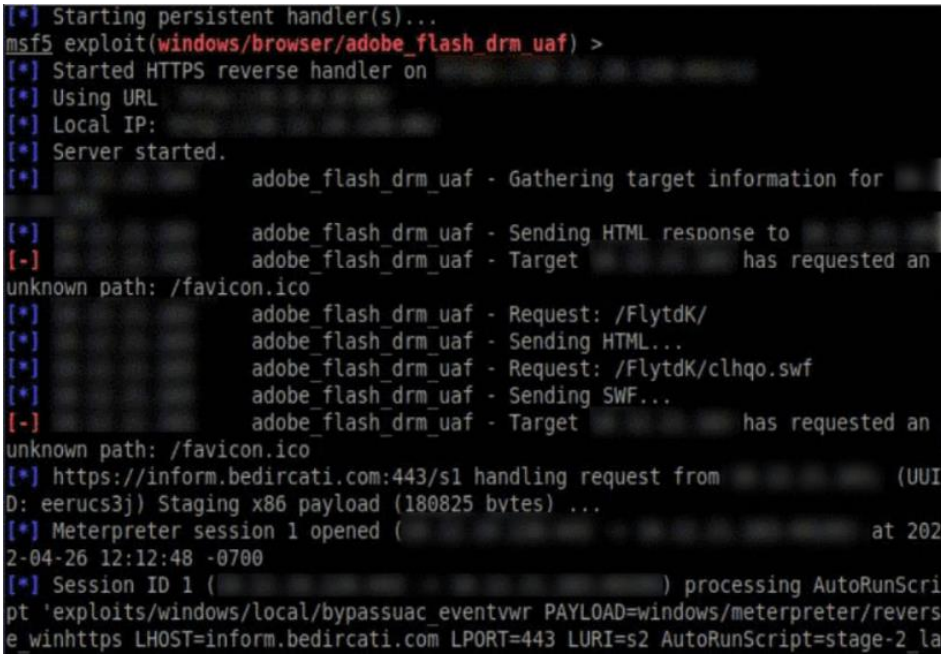

Fig. 1. Metasploit execution of malicious code and payload on endpoints

On the screen of the endpoints, the user sees only a black window (cmd) for a few seconds, and then the window closes with everything "back to normal." But what happened is much more, and that can be seen in the FireEye EDR (HX) web management console. Normally, the administrators got informed via email or some triggered alert that something happened. Also, there is a possibility of isolating the endpoint from the rest of the network. Inside the Alerts menu, we see 3 new types of alerts, as shown in Fig. 2:

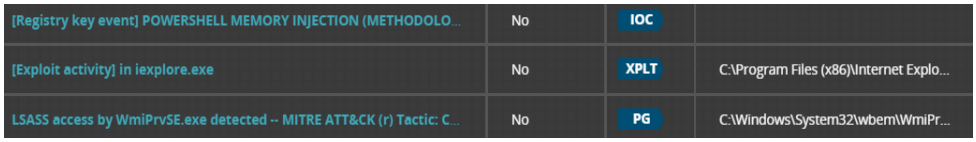

Fig. 2. Alerts triggered by Clandestine attack

As seen, the tags IOC XPLT and PG are marking those alerts, meaning all three of those engines have detected something abnormal happening on this machine. As seen – WmiPrvSE execution with exploitation for Internet Explorer (iexplorer.exe) and PowerShell execution for memory injection. In the console, it is possible to see also

the hashes of the processes and files, the timestamp, the recurring number, and much more.

For example, if we click on the exploit alert, we will see additional information about what exactly happened, as shown in Fig. 3:

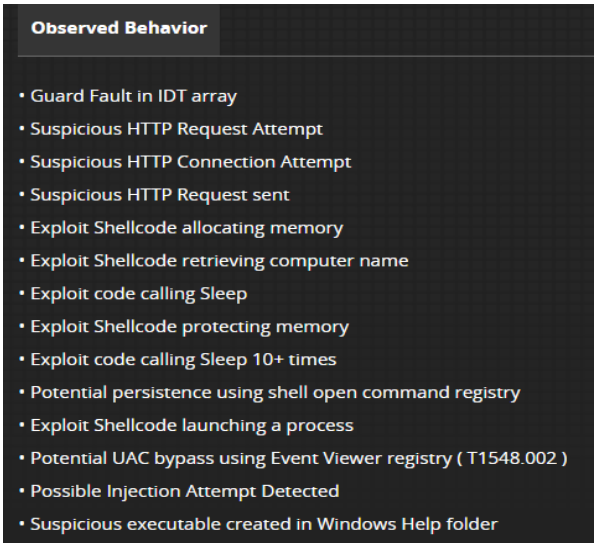

Fig. 3. ExploitGuard additional information after behavior analyses

If we click on the PowerShell execution alert that is detected by IoC, we will see what are the indicator objects that have been detected and what exactly has been executed (Fig. 4).

Fig. 4. IOC conditions detected on the infected machine

We can get even more detailed here, thanks to FireEye Threat Intelligence, which gives additional information about this IoC, as shown in Fig. 5:

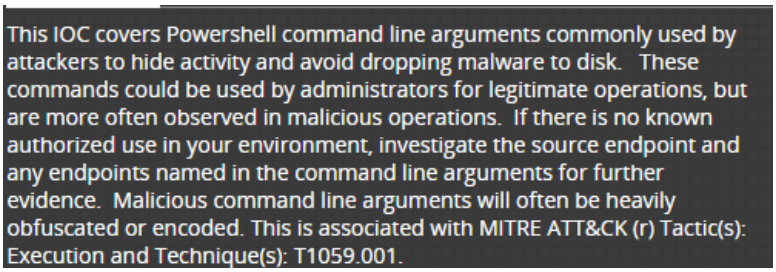

Fig. 5. FireEye Threat Intel-powered by Mandiant [8]

The forensics techniques integrated in FireEye EDR give the possibility of gaining a Triage with all the needed information for the attack for deeper investigation. The Triage can be automatically generated or manually requested by the admin. When high-priority alerts are generated for Exploits, Behaviour anomalies, or Malware executions – automatic triages have been generated. After that, via the Triage Summary, we can go deeper into the attack. The solution provides a time chart with deeper information about what happened, how it happened, via which processes, which files got included in the attack, which registry keys, what network activity, etc. All this is shown in Fig. 6:

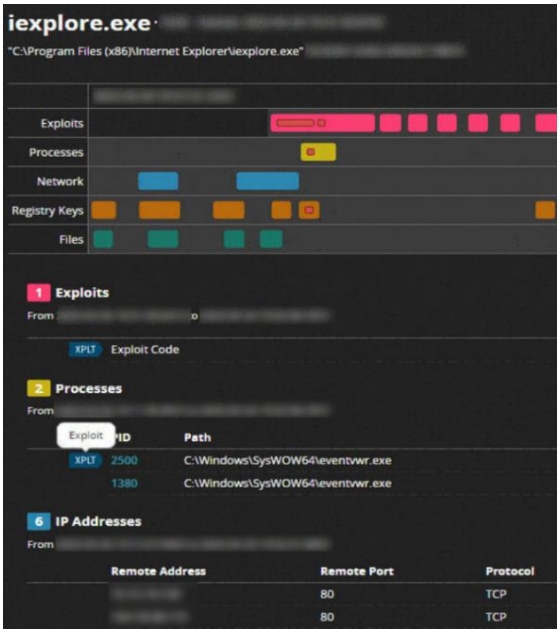

Fig. 6. Time stamp in Triage Summary

It's possible to click on each file that has been connected to the attack and see what is connected. For example, in our case – a .dll file is a hidden execution file that executes encryption over a file. FireEye can identify the fake execution file and see even the exact string command that has been used in the web console – the users see this in plain text – the full malicious command.

After the attack has been identified, it is possible to search all machines that have the FireEye agent installed. This feature is called – Enterprise search [9] and is like "Google search" for the endpoints. It is possible to search for hashes, strings, IoC, etc, but also to put a watchdog to monitor a specific search string that will return some results.

2. CONCLUSIONS

The purpose of this paper was to provide the reader with an understanding of 0-day threats with FireEye such that he/she may use it themselves. 0-Day threats with FireEye is a powerful tool that, like we said time and time again, in the wrong hands, can be used for great harm. It provides an abundance of resources for legitimate network security professionals, security administrators, product vendors, and developers to use in a variety of ways.

ACKNOWLEDGMENTS

The author would like to thank the NSP DS program for its support of this paper. This program has received funding from the Ministry of Education and Science of the Republic of Bulgaria under grant agreement No. Д01-74/19.05.2022.

REFERENCES

[1] P. CICHONSKI, T. MILLAR, TIM GRANCE AND K. SCARFONE, *Computer Security Incident Handling Guide*, Recommendations of the National Institute of Standards and Technology (2012) Special Publication 800-61, Revision 2, online: http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[2] OL. OLANIYAN, Applying the Diamond Model of Intrusion Analysis: FireEye Breach, online:https://www.researchgate.net/publication/354254596_Applying_the_Diamond_Model_of_Intrusion_Analysis_FireEye_Breach.

[3] 7 Steps of Cyber Kill Chain - Comprehensive Guide *Logsign,* online: https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/.

[4] R. GUNDUR, V. LEVI, M. TOPALLI AND AL., Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context, *CrimRxiv* (2021) online: https://doi.org/10.21428/cb6ab371.5f335e6f.

[5] FireEye Inc., MalwareGuard: FireEye's Machine Learning Model to Detect and Prevent Malware.

[6] J. YEO, Using Penetration Testing to Enhance your Company's Security, *Computer Fraud & Security* (2013) **2013** (4) 17–20, online: https://doi.org/10.1016/S1361-3723(13)70039-3.
[7] D. KENNEDY, J. O'GORMAN, D. KEARNS AND M. AHARONI, Metasploit: The Penetration Tester's (2011) No Starch Press, San Francisco, ISBN-10:1-59327-288-X, ISBN-13-978-1593272883.
[8] Penetration Testing Is What We Do, Cyber Threat Defense Solutions – Threat Intelligence Services, online: https://mandiant.com
[9] T. LEE, M. EL-BANNA AND D. DUMOND, HX 3. X Enterprise Search – Finding the Achilles Heel, FireEye Inc (2016).
[10] FireEye, Unauthorized Access of FireEye Red Team Tools. Retrieved from (2020) online: https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

Received January 10, 2025