Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.591

윈도우 이벤트 로그 기반 기업 보안 감사 및 악성코드 행위 탐지 연구*

강 세 림,[1†] 김 소 람,[1] 박 명 서,[1] 김 종 성[1,2‡]
[1]국민대학교 금융정보보안학과, [2]국민대학교 정보보안암호수학과

Study on Windows Event Log-Based Corporate Security Audit and Malware Detection*

Serim Kang,[1†] Soram Kim,[1] Myungseo Park,[1] Jongsung Kim[1,2‡]
[1]Dept. of Financial Information Security, Kookmin University,
[2]Dept. of Information Security, Cryptology and Mathematics, Kookmin University

요 약

윈도우 이벤트 로그는 윈도우 운영체제에서 시스템 로그를 기록하는 형식이며, 시스템 운영에 대한 정보를 체계적으로 관리한다. 이벤트는 시스템 자체 또는 사용자의 특정 행위로 인해 발생할 수 있고, 특정 이벤트 로그는 기업 보안 감사, 악성코드 탐지 등에 사용될 수 있다. 본 논문에서는 기업 보안 감사 및 악성코드 탐지와 관련된 이벤트 로그(외부장치 연결, 응용 프로그램 설치, 공유 폴더 사용, 프린터 사용, 원격 연결/해제, PC 시작/종료, 로그온/오프, 절전모드, 네트워크 연결/해제, 이벤트 로그 삭제, 시스템 시간 변경, 파일/레지스트리 조작, 프로세스 생성, DNS 질의, 윈도우 서비스 추가)들을 선정하고, 발생하는 이벤트 ID를 분류 및 분석하였다. 또한, 기존의 이벤트 로그 분석도구는 EVTX 파싱 기능만을 포함하고 있어 이를 포렌식 수사에 이용할 경우 사용자의 행적을 추적하기 어렵다. 이에 본 연구에서 새로운 분석도구를 구현하였으며, EVTX 파싱과 행위 분석이 가능하다.

ABSTRACT

Windows Event Log is a format that records system log in Windows operating system and methodically manages information about system operation. An event can be caused by system itself or by user's specific actions, and some event logs can be used for corporate security audits, malware detection and so on. In this paper, we choose actions related to corporate security audit and malware detection (External storage connection, Application install, Shared folder usage, Printer usage, Remote connection/disconnection, File/Registry manipulation, Process creation, DNS query, Windows service, PC startup/shutdown, Log on/off, Power saving mode, Network connection/disconnection, Event log deletion and System time change), which can be detected through event log analysis and classify event IDs that occur in each situation. Also, the existing event log tools only include functions related to the EVTX file parse and it is difficult to track user's behavior when used in a forensic investigation. So we implemented new analysis tool in this study which parses EVTX files and user behaviors.

Keywords: Windows Event Log, Digital Forensic, Anti-Forensic

Received(02. 20. 2018), Modified(03. 27. 2018), Accepted(03. 27. 2018)

* 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 작성되었습니다. (No.2017-0-00344, 최신 모바일 기기에 대한 암호해독 및 포렌식 분석)

† 주저자, ksl5442@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

I. 서 론

윈도우 이벤트 로그(Windows Event Log)는 윈도우 Vista부터 시스템과 애플리케이션의 작동 상태 및 사용자의 행위에 따라 발생하는 모든 동작에 대한 기록을 EVTX (Windows XML Event Log) 파일 형식으로 관리하는 기능이다. 애플리케이션, 운영체제 또는 다른 시스템 구성요소는 중요한 이벤트를 기록하고, 시스템 관리자는 에러 발생 시 로그를 확인하여 원인을 찾거나 주기적인 로그 확인을 통해 디스크 손상과 같은 심각한 문제를 미리 대비할 수 있다[1]. 하나의 이벤트는 메타데이터(원본, GUID, 로그된 날짜, 이벤트 ID, 작업 범주, 수준 등)와 메시지로 구성되어 있다. 이벤트를 생성한 서비스 공급자(원본)에 따라 파일(*.evtx) 단위로 저장되며, 식별자(이벤트 ID) 및 작업 범주에 따라 각 이벤트를 구분할 수 있다.

이와 같은 시스템 로그는 사용자의 의도와 관계없이 생성되는 정보이다. 디지털 포렌식 수사에서는 시스템에 유해한 악성코드에 의해 생성된 윈도우 이벤트 로그를 분석하여 악성코드의 실행 원인, 유입 경로 및 동작 과정을 파악한다. 그러나 사용자의 악의적인 행위, 예를 들어 기업 내 임직원이 퇴사하거나 타 회사로 이직하면서 주요 기밀을 유출한 후, 자신의 부정한 행적을 감추기 위한 안티 포렌식을 시도했을 경우에도 시스템은 해당 이벤트를 정상 행위로 기록할 수 있다. 따라서 수사관은 특정 행위 발생 시에 기록되는 이벤트 ID를 숙지하고, 사건 발생 시간대에 저장된 로그를 조사해야 한다. 윈도우 버전에 따라 생성되는 이벤트 ID나 메시지에 차이가 있으나, 현재까지 의미 있는 데이터가 어디에, 어떤 형식으로 남아있는가에 대한 연구가 미흡하다.

본 연구에서는 기업 보안 감사 및 악성행위 탐지 시 확인해야 할 행위를 선정하고, 이와 관련된 이벤트 ID와 메시지를 분석하였다. 또한, 현재까지 개발된 분석도구의 단점을 보완하여 행위기반의 이벤트 로그 분석도구를 개발하였으며, 이를 활용하여 외부장치 사용, 원격 연결, 파일/레지스트리 조작 및 이벤트 로그 삭제와 같은 행위의 발생 시각 및 상세 정보를 획득할 수 있다.

본 논문의 2장과 3장에서는 각각 이직, 퇴사, 근무태만 등의 기업 감사와 악성코드 행위 분석에 필요한 이벤트 로그를 분류한다. 4장에서 기존의 이벤트 로그 분석도구의 기능 및 장단점에 대해 설명한다. 또한 기업 감사와 악성코드 행위 탐지에 이용 가능한 새로운 분석도구를 소개하고 5장의 결론으로 마친다.

II. 기업 보안 감사

기업의 주요 영업 비밀은 외부 저장장치, 응용 프로그램, 출력물 형태 등 다양한 경로로 유출될 수 있다. 또한, PC 시작/종료 시간 및 절전모드 전환 관련 정보는 근무태만 여부를 판단할 수 있는 요소이며, 이벤트 로그 삭제 및 시스템 시간 변경과 같은 안티 포렌식 행위가 이루어졌는지 확인해야 한다. 본 장에서는 기업 보안 감사 시 조사해야 할 이벤트 로그를 분석한다.

2.1 외부장치 연결 정보

기업 내에서 외부장치는 허가된 장치만을 사용할 수 있다. 따라서 기업 감사 시 허가되지 않은 장치에 대한 정보가 필요하며, 해당 장치와 관련하여 어떠한 행위를 했는지 추적해야 한다.

Table 1. Event IDs for External Storage Connection

Event ID	Contents
System.evtx (Connecting New Devices)	
10000	Install driver package - Registry key for the device
20001	End the driver installation process - Device instance ID
20003	End the service addition process - Device instance ID
DriverFrameworks-UserMode/Operational.evtx (Connecting Devices)	
2003	UMDF host process is requested to load the driver for the device - GUID, Registry key for the device
2101	Complete Pnp or Power operation on the device - Registry key for the device
DriverFrameworks-UserMode/Operational.evtx (Disconnecting Devices)	
2102	Pass the completed Pnp or Power operation to the driver - Registry key for the device
2901	UDMF host shuts down the system

USB, 외장 하드 디스크와 휴대폰과 같은 외부장치 연결 관련 정보는 Microsoft-Windows-DriverFrameworks-UserMode/Operational.evtx 파일에 기록되고, 이벤트 ID 2003, 2101에서 장치에 대한 레지스트리 키 정보를 획득할 수 있다. 저장장치가 PC에 처음으로 연결된 경우, System.evtx에 드라이버 설치와 관련된 로그가 추가적으로 기록된다(Table 1.).

2.2 응용 프로그램 관련

팀뷰어(TeamViewer)와 같은 원격 프로그램이나 허용되지 않은 클라우드 프로그램은 외부로의 자료 유출 수단으로 이용될 수 있다. 또한, 파일 내부에 데이터를 숨기는 프로그램이나 파일 완전삭제 기능을 제공하는 등의 안티 포렌식 프로그램이 설치된 이후에 새로 생성된 파일이나 주요 파일이 삭제된 정황을 주의 깊게 살펴보아야 한다.

응용 프로그램 설치 관련 로그는 윈도우 7과 윈도우 10에서 각각 다른 로그 파일명으로 기록된다. 윈도우 7은 설치된 프로그램의 이름, 버전과 게시자, 윈도우 10은 설치 경로 및 확인자 이름이 기록된다. 프로그램에 따라 설치 시 로그가 기록되거나 설치 후 실행해야 로그가 남을 수 있다(Table 2.).

또한 마이크로소프트 오피스(Microsoft Office) 프로그램을 사용하는 경우, Microsoft Office Alerts.evtx 또는 OAlerts.evtx 파일에 알림 메시지에 대한 기록이 남게 되고, 사용한 오피스 프로그램의 종류와 알림 내용 등을 확인할 수 있다(Table 3.).

Table 2. Event IDs for Applications

Event ID	Contents
Application-Experience/Program-Inventory.evtx (Windows 7)	
903	The program is installed on the system - Name, Version, Publisher
904	
Application-Experience/Program-Compatibility-Assistant.evtx (Windows 10)	
17	Program installation path, Verifier name

Table 3. Event IDs for Microsoft Office Programs

Event ID	Contents
Microsoft Office Alerts.evtx	
300	Office program type, Notification contents

2.3 공유 폴더 사용

기업 내에서 허가되지 않은 공유 폴더에 대한 접근이 이루어졌다면 해당 경로상의 기밀 유출을 의심해 보아야한다. 공유 폴더 관련 이벤트 로그는 해당 폴더를 생성한 PC와 접근한 PC에 모두 기록된다. Security.evtx 파일에는 PC 외부에서 폴더에 접근한 흔적이 기록된다. 이벤트 ID 4656번, 4663번은 각각 외부에서 접근을 시도한 계정 이름 및 디렉터리/파일 정보가 기록되고, 5140번은 해당 계정의 네트워크 주소가 기록된다. Microsoft-Windows-SMBClient/Connectivity.evtx는 특정 PC가 접근한 공유 폴더 서버에 대한 이름과 주소를 기록한다(Table 4.).

Table 4. Event IDs for Shared Folder

Event ID	Task	Contents
Security.evtx		
4656	File System	Request a handle to an object - Subject, Process information, Access request information
4663		Attempt to access an object - Subject, Process information, Access request information
5140	File Share	A network share object was accessed - Subject, Network/Share information, Access request information

Event ID	Task	Contents
SMBClient/Connectivity.evtx		
30804	-	A network connection was disconnected - Server name/address
30805	-	The client lost its session to the server - Server name
30806	-	The client re-established its session to the server - Server name/address
30807	-	The connection to the share was lost - Share name
30808	-	The connection to the share was re-established - Share name/address

2.4 프린터 사용

기업 내의 기밀 자료는 데이터가 아닌 출력물 형태로도 유출될 수 있다. 사용자가 특정 문서에 대한 인쇄 작업을 요청하면, Microsoft-Windows-PrintService/Operational.evtx 파일에 관련 로그를 기록한다. 그 중 이벤트 ID 307번에는 인쇄한 문서의 크기 및 페이지 수를 기록한다(Table 5.). 윈도우 7의 경우 이벤트 ID 307에서 문서 이름과 응용 프로그램 정보를 추가적으로 확인 가능하며, 로그에 기록되는 문서 이름을 확인해 기밀문서의 출력 여부를 판단할 수 있다. 또한, 짧은 시간 내에 비정상적으로 문서 출력 횟수가 많거나 출력 크기가 큰 시간대가 존재하는지 확인할 필요가 있다.

Table 5. Event IDs for Printer Usage

Event ID	Contents
PrintService/Operational.evtx	
307	Complete document printing - Owner, Location, Size in bytes, Pages printed
801	Printing job
802	Deleting job
842	The print job was sent through the print processor on printer

2.5 원격 연결/해제

원격 연결은 근무 시간 이외에 근무지 외부에서 PC를 이용해야 할 경우에 사용되며, 데이터 유출 경로가 될 수 있다. 또한, 해당 기능 자체를 허용하지 않는 기업도 존재하기 때문에 원격 연결이 이루어졌는지 확인해야 한다. 시스템은 분석 대상 PC(Host PC)에서 원격 PC(Guest PC)로 연결 또는 그 반대의 경우, Host PC의 각각 다른 파일에 로그를 남긴다.

2.5.1 Host PC → Guest PC

원격 연결 로그는 Microsoft-Windows-RDPClient/Operational.evtx에 기록되며, 이벤트 ID 1024번과 1102번에서 연결을 시도한 Guest PC의 주소를 확인할 수 있고, 1027번은 컴퓨터 이름을 확인할 수 있다. 원격 연결 해제 시에는 Security.evtx에 원격 데스크톱 프로그램(mstsc.exe)의 프로세스 종료 로그가 남고, 연결 해제된 Guest PC IP 주소의 정보는 알 수 없다(Table 6.).

Table 6. Event IDs for Remote Connection/Disconnection from Host to Guest PC

Event ID	Task	Contents
TerminalServics-RDPClient/Operaional.evtx (Connection)		
1024	Connection Sequence	RDP ClientActiveX is trying to connect to the server - Server address
1102	Connection Sequence	The client has initiated a multi-transport connection to the server - Server address
1027	Connection Sequence	Connected to domain - Domain Name
Security.evtx (Disconnection)		
4689	Process Termination	A process has exited - C:\Windows\System32\mstsc.exe

Event ID	Task	Contents
TerminalServics-RDPClient/Operaional.evtx (Disconnection)		
1105	Connection Sequence	The multi-transport connection has been disconnected
1026		RDP ClientActiveX has been disconnected

2.5.2 Guest PC → Host PC

Windows-TerminalServices-RemoteConnectionManager/Operational.evtx 파일에는 원격 연결을 시도한 PC의 IP 주소가 기록된다. 3.5.1의 연결 해제 경우와 달리, Microsoft-Windows-TerminalServices-LocalSessionManager/Operational.evtx의 이벤트 ID 24, 25번 로그에서 연결이 해제된 Host PC의 IP 주소를 확인할 수 있다 (Table 7.).

Table 7. Event IDs for Remote Connection /Disconnectionfrom Guest to Host PC

Event ID	Contents
TerminalServices-RemoteConnectionManager/ Operational.evtx (Connection)	
261	Listener RDP-Tcp received a connection
1149	Remote Desktop Services : User authentication succeeded - User, Souce Network Address
41	Start session arbitration
TerminalServices-LocalSeesionManager/Operational.evtx (Disconnection)	
24	Remote Desktop Services : Session has been disconnected - User, Source Network Address
25	Remote Desktop Services : Session reconnection succeeded - User, Source Network Address
42	End session arbitration

2.6 PC 시작/종료

PC 시작/종료 관련 로그는 System.evtx에서 확인할 수 있다. 이벤트 ID 12, 13번은 각각 운영체제 시작/종료 시간을 나타내고, 이는 UTC+0을 따른다. 6013번은 시스템 작동 시간에 대한 정보이며, 시스템 부팅 후 흐른 시간을 초 단위로 나타낸다 (Table 8.). 윈도우 7의 경우 Microsoft-Windows-Diagnostics-Performance/Operational.evtx에 윈도우 시작(이벤트 ID 100번)/종료(이벤트 ID 200번) 메시지가 추가적으로 기록된다. 근무 시간 외에 이와 같은 흔적이 남아있다면, 그 사이에 어떤 행위가 일어났는지 조사할 필요가 있다. 또한, PC 시작/종료 시간이 기업 내에서 정해져 있는 출/퇴근시간과 확연한 차이가 있는지 확인해야 한다.

Table 8. Event IDs for PC Start

Event ID	Contents
System.evtx (PC Startup)	
12	The operating system started - System time
6013	The system uptime
System.evtx (PC Shutdown)	
13	The operating system is shutting down - System time
1074	The process has initiated the power off / restart of the computer - Computer name, Shutdown Type

2.7 로그온/오프

Microsoft-Windows-User Profile Service.evtx와 Security.evtx 파일에서 로그온(이벤트 ID 1, 2, 4648번)과 로그오프(이벤트 ID 3, 4, 7002번) 관련 메시지를 확인 가능하고, 해당 로그가 기록된 시간이 곧 사용자가 로그온/오프한 시각이다(Table 9.).

Table 9. Event IDs for Log On/Off

Event ID	Task	Contents
User Profile Service/Operational.evtx		
1	-	Received user logon notific-ation
2	-	Finished processing user logon notification
3	-	Received user logoff notifi-cation
4	-	Finished processing user logoff notification
Security.evtx		
4648	Log On	A logon was attempted using explicit credentials - Subject, Account whose credentials were used
7002	(1002)	User Logoff Notification for Customer Experience Improvement Program

2.8 절전 모드

근무 시간 동안 절전모드로 자동 전환된 횟수가 많다면 이는 근무태만으로 판단할 여지가 있다. 그러나 PC는 설정된 시간에 의한 자동 전환 뿐만 아니라 사용자의 선택에 의해서 절전 모드로 변경될 수 있다.

이 두 가지 경우는 System.evtx 파일 이벤트 ID 42번의 '절전 모드 전환 이유'를 통해 구별할 수 있다(Table 10.). 사용자의 의지에 따라 절전 모드로 전환한 경우에는 '응용프로그램 API'로 기록되고, 설정된 시간만큼 PC를 사용하지 않아 자동으로 전환되면 '시스템 유휴 시간'으로 기록된다. 절전 모드 해제 시 윈도우 7은 '절전 모드에서 다시 시작', 윈도우 10은 '저전원 상태에서 복귀'로 기록된다.

Table 10. Event IDs for Power Saving Mode

Event ID	Provider	Contents
System.evtx (Entered)		
42	Kernel-Power	The system is entering sleep - Sleep reason
System.evtx (Resumed)		
1	Power-Troblesh ooter	The system has resumed from sleep - Sleep/Wake time

2.9 네트워크 연결/해제

네트워크 연결/해제 관련 로그는 Microsoft-Windows-NetworkProfile.evtx 파일에 기록된다(Table 11.). 연결/해제 메시지와 함께 네트워크 이름이 남고, Wi-Fi를 사용하는 경우 SSID 정보가 남는다. 따라서 사용자가 노트북을 사용한 경우 어느 장소에서 얼마나 시간을 보냈는지 판단하는 정보로 사용될 수 있다.

Table 11. Event IDs for Network Connection

Event ID	Contents
NetworkProfile/Operational.evtx	
10000	Network connected - Name, Description, Type, State, Category
10001	Network disconnected - Name, Description, Type, State, Category

2.10 이벤트 로그 삭제

이벤트 로그는 이벤트 뷰어를 이용하여 간단하게 삭제할 수 있으나, 일반 사용자는 로그를 삭제할 가능성이 낮다. 따라서 사용자가 데이터를 임의로 삭제하는 안티 포렌식 행위로 의심할 수 있으며, 특정 행위와 관련된 로그 파일이 삭제되었는지 확인할 필요가 있다. 감사 로그가 삭제된 경우 해당 파일(Security.evtx)이 재 생성되며 삭제 로그가 남는다. 그 이외의 파일이 삭제되면 System.evtx의 이벤트 ID 1102번에 대상 파일의 이름이 기록된다(Table 12.).

Table 12. Event IDs for Event Log Deletion

Event ID	Contents
System.evtx	
104	The System log file was cleared - Deleted log file name
Security.evtx	
1102	The audit log was cleared - Security ID, Account name, Domain name, Logon ID

2.11 시스템 시간 변경

일반적으로 사용하던 기기의 장소를 해외로 이동했을 때 표준시간을 맞추기 위한 기능이지만, 이를 통해 다른 로그파일의 시간 정보나 메타데이터를 조작하기 위한 행위인지 확인해야 한다.

시스템 날짜 및 시간 변경은 Microsoft-Windows-DateTimeControlPanel.evtx에 기록되며, 임의로 시간을 변경한 정보(년/달/주/일/시/분/초/밀리초, 이벤트 ID 20000번)와 변경된 표준시간대 정보(이벤트 ID 20001번)가 남는다. System.evtx 파일에도 변경 전/후 시간이 기록되며, 추가적으로 자동으로 시스템에 의한 시간 조정이 이루어졌을 경우에도 로그가 기록된다(Table 13.).

Table 13. Event IDs for System Time Manipulation

Event ID	Provider	Contents
System.evtx		
1	Kernel-General	The system time has changed - New time zone, Change reason
DateTimeControlPanel.evtx		
20000	DateTimeControlPanel	Changed time informa-tion
20001		Changed time zone inf-ormation

III. 악성코드 행위 탐지

악성코드는 일반 실행 파일과 다르게 사용자의 정보를 탈취하고 파일을 조작하는 등의 악성 행위를 수행한다. 본 장에서는 악성코드에 의한 파일 및 레지스트리 조작, 프로세스 생성, DNS 질의 및 윈도우 서비스 추가 여부를 확인할 수 있는 이벤트 로그를 설명한다.

3.1 파일 조작 여부 확인

PC로 유입되는 대부분의 악성코드는 인터넷에서 또 다른 악성코드를 다운로드하거나, 자신의 몸체에 담고 있는 다른 악성 파일들을 드롭하는 등의 행위를 수행하기 때문에 해당 로그를 확인해야 한다.

파일 수정/삭제 관련 로그는 Security.evtx 파일의 이벤트 ID 4660번, 4663번으로 기록된다. 파일이 삭제되면 해당 개체의 핸들 ID가 4660번에 기록되며, 같은 핸들 ID가 기록된 4663번 로그를 확인함으로써 삭제된 파일의 이름을 확인할 수 있다[2]. 파일 수정 이벤트 발생 시에는 4663번만 기록되고, 메시지 상의 액세스 요청 정보는 'WriteData' 또는 'AddFile'이다(Table 14.).

Table 14. Event IDs for File Handling

Event ID	Task	Contents
Security.evtx		
4660	File-System	An object was deleted - Account name, Object handle ID, Process information
4663		An attempt was made to access an object - Object name, Process ID/Name, Access request information

3.2 레지스트리 조작 여부 확인

악성코드는 일반적으로 특정 레지스트리 키[1]에 자기 자신을 등록하여 재부팅 시 다시 실행되게 하는 등, 여러 레지스트리를 조작함으로써 악성행위를 극

1) HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run

대화한다. Security.evtx 파일에는 수정된 레지스트리의 키(이벤트 ID 4656), 해당 값을 수정한 프로세스 및 변경되기 전과 후의 값(이벤트 ID 4657)이 기록된다. 따라서 악성코드의 프로세스 정보를 알고 있다면 수정한 레지스트리에 대한 정보를 확인할 수 있다(Table 15.).

Table 15. Event IDs for Registry Handling

Event ID	Task	Contents
Security.evtx		
4656	Regis-try	Request a handle to an object - Subject, Process information, Access request information
4657		A registry value was modified - Object, Process/Change information

3.3 프로세스 생성 및 종료

악성코드가 실행됨으로써 악성 행위가 이루어지며, 그에 따른 프로세스가 생성되어야 한다. 또한, 다른 악성 파일을 드롭하여 추가적인 악성코드를 실행하는 경우도 있다. 프로세스 관련 로그는 Security.evtx 파일에 기록되며, 4688번과 4689번에서 각각 생성/종료된 프로세스의 ID와 이름을 확인할 수 있다(Table 16.). 악성코드의 메인 프로세스의 실행 시각을 알 수 있으며, 획득한 프로세스 정보를 활용하여 다른 로그로부터 해당 악성코드가 수행한 행위를 확인할 수 있다.

Table 16. Event IDs for Process Creation

Event ID	Task	Contents
Security.evtx		
4688	Process Creation	A new process has been created - New process ID/Name, Creator process ID/Name
4689	Process Termina-tion	A process has exited - Process ID/Name

3.4 DNS 질의 확인

악성코드가 사용자 PC에서 실행된 이후 유포지, C&C 서버가 차단되거나, 해당 웹서버가 사라지면 평소 접근하지 않던 도메인으로의 DNS 질의 건수가 급격하게 증가한다[3]. 관련 로그는 Microsoft-Windows-DNS Client Events/Operational.evtx에 기록되며 질의 이름, 유형, 결과 및 DNS 서버 주소 등을 알 수 있다(Table 17.).

Table 17. Event IDs for DNS Query

Event ID	Contents
DNS Client Events/Operational.evtx	
1001	Interface, Total DNS server count, Address
3006	DNS query is called - Query name
3008	DNS query is completed - Query name, Results
3010	DNS query sent to DNS Server - Query name/type, Server address
3019	Query wire called - Query name/type
3020	Query response - Query name/type

3.5 윈도우 서비스 추가

윈도우 서비스는 운영체제가 부팅한 후부터 백그라운드로 실행되는 프로그램이다. 악성코드는 이러한 윈도우 서비스에 자기 자신을 추가하여, 부팅 시에

Table 18. Event IDs for Windows Service

Event ID	Provider	Contents
System.evtx		
7040	Service-Control Manager	The start type of the Background Intelligent Transfer Service was changed
7045		A service was installed in the system - Service name/type/account, Service file name/type

자동으로 실행되게 한다. 서비스가 추가되면 System.evtx의 7045번에 설치된 서비스명, 유형 및 서비스 파일 이름 등이 기록된다(Table 18.).

IV. 윈도우 이벤트 로그 분석도구 개발

기존 이벤트 로그 분석도구는 로컬 PC상의 문제점을 확인하기 편리한 구조로 설계되어 있어, 현재 포렌식 수사에서 활용하기에 어려움이 있다. 이에 단순 분석 기능을 확장한 새로운 분석도구를 개발하였으며, 기업 보안 감사 및 악성코드 행위 탐지 시 사용될 수 있다.

4.1 기존 이벤트 로그 분석도구

4.1.1 이벤트 뷰어

이벤트 뷰어는 윈도우 운영체제의 구성 요소이며[4], 로컬 또는 원격 컴퓨터의 이벤트 로그를 분석할 수 있다. 실행 시 기본적으로 로컬 컴퓨터의 EVTX 파일의 분석 결과를 출력한다. 외부 PC를 분석할 경우에는 이벤트 뷰어를 이용하여 해당 PC의 IP 주소로 연결하거나, 이벤트 로그를 기본 경로[2]에서 추출한 후 파일단위로 불러오는 '저장된 로그' 분석 기능을 이용할 수 있다. 또한, 원하는 조건(이벤트 ID, 수준, 작업 범주, 키워드 등)에 맞는 이벤트만 불러올 수 있는 '필터링' 기능이 있다. 필터링 된 이벤트는 새로운 EVTX 파일로 저장 가능하다.

운영체제의 기본 프로그램으로서 분석 속도가 빠르고 안정적인 반면, 포렌식 수사에서 사용하고자 할 때 몇 가지 어려움이 있다. 첫 번째로, 저장된 로그에 대한 폴더 단위 분석이 불가능하다. 이벤트 로그를 이용한 포렌식 수사 시, 여러 가지의 로그 파일을 복합적으로 확인해야한다. 그러나 해당 도구는 일일이 모든 파일을 추가해야하며, 통합적으로 결과를 확인할 수 없다. 두 번째로, 모든 로그파일에 대한 필터링을 적용할 수 없다. 현재 확인하고 있는 로그에 한정하여 필터링을 사용할 수 있어 원하는 파일을 선택한 후 각각 필터를 적용해야 한다.

4.1.2 Event Log Explorer

FSPro에서 개발한 Event Log Explorer는 Business(상용)와 Home(무료) 에디션으로 제공된다[5]. EVTX 형식을 사용하는 모든 윈도우 버전(Vista, 7, 8, 10)에서 이벤트 로그 분석이 가능하며, 본 연구에서는 4.6 버전, Home 에디션을 사용하였다. 파일 단위 분석, 저장된 로그 분석, 필터링 등 이벤트 뷰어의 기능과 더불어 추가적인 기능을 제공한다. 기본적으로 시간 관련 정보는 시스템 시간에 맞추어 분석하나, 사용자가 원하는 표준 시간대로 조정할 수 있다. 특정 이벤트에 북마크를 설정하여 필요시에 빠르게 이동할 수 있고, 로그 파일 별 출력(인쇄) 기능을 제공한다. 또한, 적용한 필터를 파일 형태(*.elc)로 저장하여 다시 사용가능하며, 설정한 기준(이벤트 ID별, 날짜별, PC별 등)에 따른 이벤트 발생 빈도를 분석하여 보고서를 제공한다. 그러나 이벤트 뷰어의 단점을 보완하지 못할 뿐만 아니라, 레코드별 메타데이터와 메시지에 사용자가 제어판에서 설정한 지역별 언어가 제대로 반영되지 않는다는 단점이 있다.

4.2 새로운 분석도구 개발

기존의 분석도구는 로컬 PC의 EVTX 파일 분석을 주목적으로 하고 있어, 시스템 상의 오류를 검출하고 해결하기에 용이하다. 또한, 각 로그 파일별로 발생한 이벤트를 확인하고 필터링을 적용할 수 있다. 그러나 포렌식 수사관은 용의자의 PC로부터 추출한 이벤트 로그를 분류하여 수사에 필요한 특정 이벤트들을 통합적으로 분석해야 한다. 이에 기존 분석도구를 사용하는 것은 빠른 시간에 정확한 분석 결과를 얻기 어렵다.

본 연구에서는 기존 분석기능과 함께 기업 감사와 악성코드 행위 분석에서 효율적으로 사용할 수 있는 분석도구를 개발하였다. 새롭게 구현한 윈도우 이벤트 로그 분석도구는 2, 3장의 체크리스트로 필터링을 적용, 사용자의 행위에 기반하여 결과를 출력한다. 해당 도구를 이용하여 확인할 수 있는 행위는 총 16가지이며, 행위별로 관련 로그의 정보를 확인할 수 있다. '세부 분석 결과' 항목은 각 이벤트의 메타데이터와 메시지를 출력, '분석 결과 요약' 항목은 행위별로 발생한 로그의 중요 정보를 통합하여 시간 순서대로 출력한다. Fig. 1.은 도구의 GUI 및 분석

2) %SYSTEMROOT%\System32\winevt\Logs

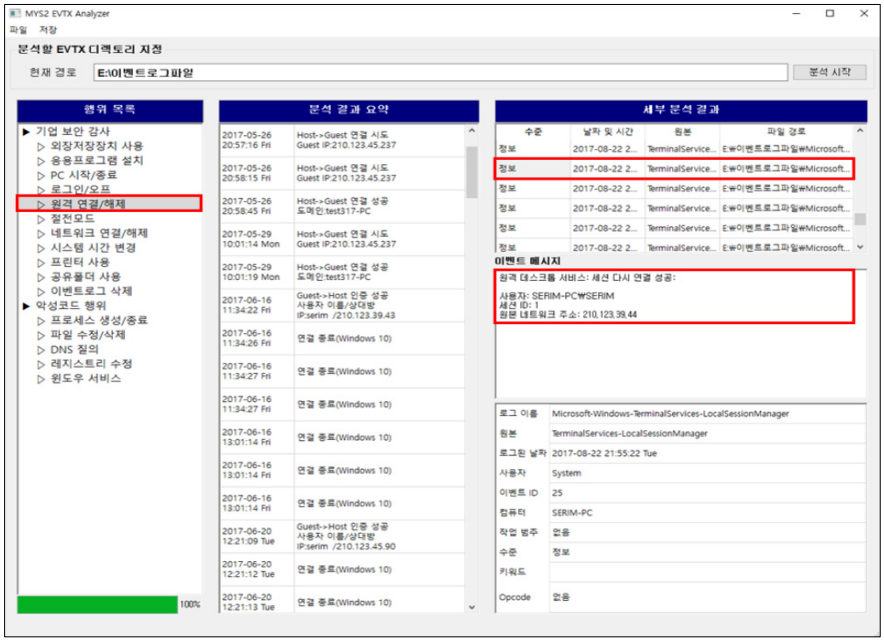

Fig. 1. The GUI of Newly Implemented Tool and Analysis Results of EVTX Files

결과를 나타낸 그림이며, 도구 사용 방법은 아래와 같다.

1. 분석 대상 PC로부터 이벤트 로그 폴더(winevt) 추출
2. 추출한 폴더를 도구에 입력, '분석 시작' 클릭
3. 분석 완료 후, '세부 분석 결과' 및 '분석 결과 요약' 항목에서 각 행위별 로그 확인

2번에서 입력받은 폴더 분석은 세 단계로 이루어진다. 첫 번째로, 폴더 내부에서 행위별로 분석해야 할 파일을 선별한다. 즉, 파일명에 따라 EVTX 파일들을 분류하며, 관련 없는 파일은 나머지 단계에서 고려하지 않는다. 두 번째로, 분류된 EVTX 파일을 분석하고, 관련 있는 로그 데이터를 추출한다. EVTX 파일은 여러 개의 레코드(record)로 구성되어 있으며, 하나의 레코드는 Binary XML 구조에 따라 특정 이벤트의 메타데이터를 저장한다[6]. 분석된 레코드의 이벤트 ID, 작업 범주와 3장의 체크리스트를 비교하여 필요한 레코드만 수집한다. 마지막으로, 시스템 내에서 수집된 레코드의 이벤트 ID에 해당하는 이벤트 메시지를 찾는다. 메시지 관련 정보는 dll 파일 형태[7]로 저장되며, 파일 경로는 GUID 또는 Channel과 Name을 포함한 레지스트리 키에서 확인할 수 있다[8]. 구체적인 메시지 탐색 과정은 아래와 같다.

1. 레코드에서 GUID(존재하지 않을 시 Channel/Name)와 이벤트 ID 추출
2. 추출한 GUID(또는 Channel/Name)를 반영한 레지스트리 경로에서 dll 파일 경로 획득

HKEY_LOCAL_MACHINE
- o SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{GUID}
- o SYSTEM\CurrentControlSet\Services\EventLog\{Channel}\{Name}

3. 해당 dll 파일의 'EVTN' 리소스 영역에서 이벤트 ID에 맞는 메시지 ID 추출
4. {dll 파일 경로}\ko-KR 내부 {dll 파일 이름}.mui 파일에서 3번의 메시지 ID에 해당하는 이벤트 메시지 획득 가능

획득한 메시지는 '세부 분석 결과' 란에 출력되어, 따로 이벤트 뷰어를 사용하지 않아도 이벤트에 대한 상세 정보를 확인할 수 있다. 또한, 해당 정보 중 IP 주소, 저장장치 정보, 네트워크 이름 등 주요 데이터를 담고 있는 이벤트를 필터링하여 '분석 결과 요약' 란에 출력한다. 해당 영역에서 행위 별로 보여주는

정보는 Table 19.와 같고, 모든 항목은 타임 스탬프를 포함하고 있다.

Table 19. The Analysis Results with Newly Developed Tool

Action	Results
Remote Connection	o Host→Guest / Guest→Host Connecting - Guest/Host IP : {IP address} o Host→Guest/Guest→Host Successfully Connected - Domain : {Guest/Host PC domain name} o Connection Terminated (Windows 10)
Application Install	o Name : {Application installation path}
External Storage Usage	o Device Disconnected o Device Connected - Storage Information : {Registry key}
Shared Folder Usage	o Access IP/Path : {IP address accessed to shared folder/Accessed file path}
Printer Usage	o Printing Document
File Manipulat-ion	o File Deleted or Modified o Name/Handle : {Targe file name/handle ID}
Registry Manipulat-ion	o Registry Manipulated o Object Name : {Manipulated registry key}
Process Creation	o Process Created/Exited o Name : {Process name}
DNS Query	o DNS Query o IP : {DNS server IP address}
Windows Service	o Service Installed o Service Name : {Installed Windows service name}
PC Startup/ Shutdown	o OS started at {Timestamp} o OS is shutting down at {Timestamp}
Log On/Off	o Log On o Log Off
Power Saving Mode	o Switch to Power Saving Mode o Resume from Power Saving Mode
Network Connection	o Network Connected - Name : {Network name}
Event Log Deletion	o Log File Deleted - Name : {Event log file name}
System Time Change	o System Time Setting o Standard Timezone is Changed - Information : {Timezone information}

V. 결 론

윈도우 이벤트 로그는 현재 가장 많이 사용되고 있는 운영체제인 윈도우 환경에서 시스템 로그를 관리하는 형식으로, 사용자의 행위 및 시스템 동작과 관련된 정보를 실시간으로 저장한다. 외장 저장장치, 응용 프로그램 설치, 원격 연결, 프린터 사용 등의 의미 있는 데이터가 기록되어 있으나, 다량의 로그 중 연관 있는 데이터를 선별하기 어려워 포렌식 수사에서의 활용도가 낮다. 이에 본 연구에서는 기업 감사 및 악성코드 탐지 시 확인해야 할 행위와 관련된 이벤트 로그 파일 및 ID를 분석하였다(Table 20.).

Table 20. List of EVTX Files for Actions

Action	File Name
Remote Connection	o Security o TerminalServics-RDPClient/Operaional o TerminalServices-RemoteConnectionManager/Operational o TerminalServices-LocalSeesionManager/Operational
Application Install	o Application-Experience/Program-Inventory(Windows 7) o Application-Experience/Program-Compatibility-Assistant (Windows 10) o Microsoft Office Alerts
External Storage Usage	o System o DriverFrameworks-UserMode/Operational

Action	File Name
Shared Folder Usage	o Security o SMBClient/Connectivity
Printer Usage	o PrintService/Operational
File Manipulat-ion	o Security
Registry Manipulat-ion	o Security
Process Creation	o Security
DNS Query	o DNS Client Events/Operational
Windows Service	o System
PC Startup/ Shutdown	o System
Log On/Off	o User Profile Service/Operational o Security
Power Saving Mode	o System
Network Connection	o NetworkProfile/Operational
Event Log Deletion	o System o Security
System Time Change	o System o DateTimeControlPanel

또한 포렌식 수사에 특화된 이벤트 로그 분석도구를 개발하였다. 현재 사용되고 있는 도구는 각 이벤트 로그 파일에 대한 단순 파싱 기능을 지원하고, 수사관이 원하는 이벤트 ID에 대해 직접 필터링을 적용해야 한다. 새롭게 개발한 분석도구는 기존의 파싱 기능을 포함하며, 기업 감사 및 악성코드 행위 탐지 시 확인해야 할 이벤트 로그를 분류함으로써 위의 16가지 행위와 관련된 정보를 빠르게 획득할 수 있다. 또한 행위 별로 요약 및 상세 분석 결과를 제공하며, 이를 csv 파일 형태로 출력 가능하다.

윈도우 이벤트 로그는 운영체제의 버전(Vista, 7, 8, 10)과 에디션(Home. Pro, Enterprise, Education 등)에 따라 저장되는 로그 파일과 이벤트 ID가 다르다. 따라서 모든 윈도우 버전 및 에디션에서 각 행위에 대해 발생하는 이벤트를 확인함으로써, 더 많은 상황에서 윈도우 이벤트 로그가 활용될 수 있는 환경을 구축해야 한다.

References

[1] Microsoft Developer Network, https://msdn.microsoft.com/ko-kr/library/windows/desktop/aa363632(v=vs.85).aspx

[2] Ultimate Windows Security, https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4663

[3] Igloo Security, http://www.igloosec.co.kr/BLOG_%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C%20%EA%B0%90%EC%97%BC%20%EC%82%AC%EC%9A%A9%EC%9E%90%EC%9D%98%20%EB%A1%9C%EA%B7%B8%20%ED%96%89%EC%9C%84%20%EB%B6%84%EC%84%9D?searchItem=&searchWord=&bbsCateId=47&gotoPage=1

[4] Wikipedia, https://en.wikipedia.org/wiki/Event_Viewer

[5] FSPro Labs, https://eventlogxp.com/

[6] Andreas Schuster, "Introducing the Microsoft Vista event log file format", Digital Investigation, vol. 4, pp.67-69, Sep. 2007.

[7] Github, https://github.com/libyal/libexe/blob/master/documentation/Executable%20(EXE)%20file%20format.asciidoc

[8] Github, https://github.com/libyal/libevtx/blob/master/documentation/Windows%20XML%20Event%20Log%20(EVTX).asciidoc

〈저자소개〉

강 세 림 (Serim Kang) 학생회원
2017년 2월: 국민대학교 수학과 졸업
2017년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 디지털 포렌식

김 소 람 (Soram Kim) 학생회원
2016년 2월: 국민대학교 수학과 졸업
2016년 3월~2018년 2월: 국민대학교 금융정보보안학과 석사
2018년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 정보보호, 디지털 포렌식

박 명 서 (Myungseo Park) 학생회원
2013년 2월: 국민대학교 수학과 졸업
2013년 3월~2015년 2월: 국민대학교 금융정보보안학과 석사
2014년 12월~2017년 2월: 국가보안기술연구소 연구원
2017년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 정보보호, 디지털 포렌식, 암호 알고리즘

김 종 성 (Jongsung Kim) 종신회원
2000년 8월/2002년 8월: 고려대학교 수학 전공 학사/이학석사
2006년 11월: K.U.Leuven ESAT/SCD-COSIC 정보보호 전공 공학박사
2007년 2월: 고려대학교 정보보호대학원 공학박사
2007년 3월~2009년 8월: 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월: 경남대학교 e-비즈니스학과 조교수
2013년 3월~현재: 국민대학교 정보보안암호수학과 부교수
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 부교수
〈관심분야〉 정보보호, 디지털 포렌식, 암호 알고리즘