악성코드 분석 보고서

파일명: dgrep.exe

분석일시: 2026년 4월

목차

1. 개요
   1.1 파일 기본 정보
   1.2 분석 요약
   1.3 주요 행위
2. 분석 환경
   2.1 분석 환경
   2.2 분석 사용 도구
3. 기초 분석
   3.1 자동화 분석
   3.2 파일 식별
4. 정적 분석
   4.1 PE 구조 확인
   4.2 Import 분석
   4.3 문자열 분석
5. 동적 분석
   5.1 프로세스
   5.2 레지스트리
   5.3 파일 변경
   5.4 네트워크
6. 공격 흐름 정리 (Kill Chain)
7. 결론
8. 대응 방안

부록. IOC 정리

1. 개요

1.1 파일 기본 정보

파일명	dgrep.exe
별칭	vbscript.dll / output.123910684.txt
크기	215.05 KB (220,214 bytes)
파일 타입	PE32 Windows GUI
MD5	68af0599e74d36bc2f39a2710754082c
SHA-1	c63f22e2d6feecbe9801c76a76f81589bce1b9a3
SHA-256	d3e4a46b95a3a54c762f0e1696e9167528bd1cf30b190e4893b44f0259e7893c
타임스탬프	2015-10-09 03:43:26 UTC
출처	멘토링 제공
진단명(V3)	Backdoor/Win.Venik.R573655

1.2 분석 요약

dgrep.exe(이하 악성코드) 실제 분석 결과 트로이목마, 웜, 백도어의 성격을 가진 악성코드로 확인되었다. 또한 VirusTotal(이하 VT) 참고 결과 65/71 탐지 점수와 pepatch / farfli 의 패밀리 유형을 확인할 수 있었다. 분석 시 dgrep.exe 복사본을 생성하고 셀프 삭제를 하는 행위로 탐지를 어렵게 악성코드가 레지스트리 등록을 통해 지속성을 확보하였다. C&C 서버와 실제 네트워크 연결이 수립되지는 않았지만 반복적인 연결 시도를 한다. C&C 서버가 살아난다면 언제든 네트워크 연결이 수립될 수 있고 추가적인 악성 명령을 받을 수 있어 위험하고 주의가 필요하다

1.3 주요 행위

- 실행 시 %TEMP% 경로에 랜덤 이름의 자기 복사본을 생성하고 실행한다.
- C 드라이브 외에도 다른 드라이브에 접근 및 파일 생성을 시도하여 전파 가능성이 있다.
- 정상 프로세스 rundll32.exe를 통해 페이로드 DLL을 로드하여 탐지를 회피한다.
- 재부팅 후 악성코드가 자동 실행되도록 HKCU₩Software₩Microsoft₩Windows ₩CurrentVersion₩Run₩EvtMgr 키를 등록한다.
- 107[.]163[.]241[.]198:6520, 107[.]163[.]241[.]197:12354와 지속적인 접속 시도를 한다.
- 원본 파일과 복사본 파일을 자기 삭제하여 숨긴다.

2. 분석 환경

2.1 분석 환경 설명

가상머신 소프트웨어	VMware
가상머신 버전	-
가상머신 네트워크 설정	NAT
사용 OS	Windows 11 pro

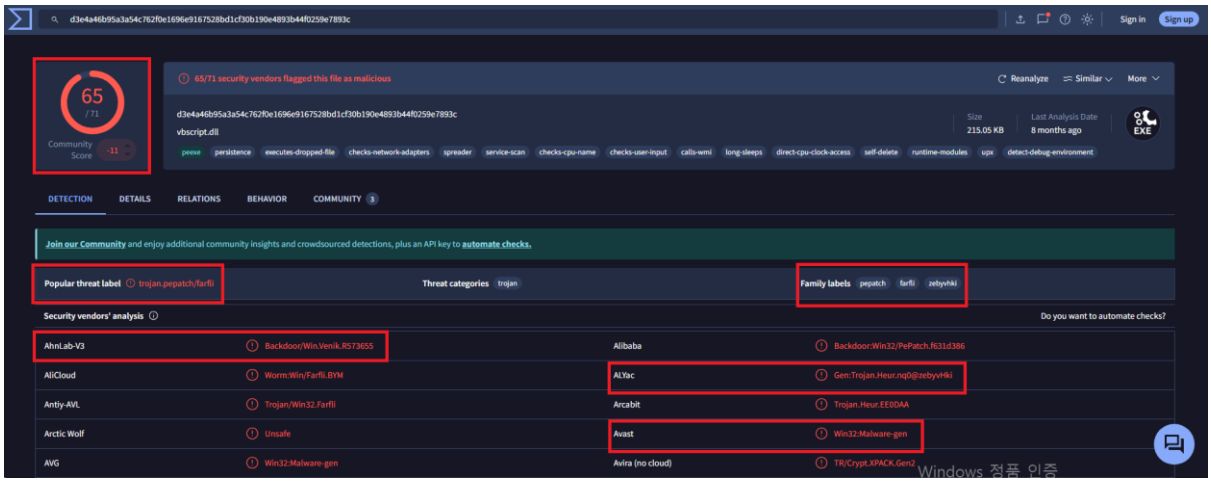
2.2 분석 도구

분류	도구명	주요 용도
자동화 분석	VirusTotal	자동화 분석 실제 분석 시 내용 참고
기초 분석	ExeinfoPE	파일 기본 정보 및 패킹 유무 확인
	DIE	파일 기본 정보 및 패킹 유무 확인
정적 분석	PEview	PE 구조 상세 확인, Import 확인
	BinText	악성코드에서 사용되는 문자열 확인
동적 분석	Process Explorer	프로세스 확인
	Autoruns	지속성 확보 확인
	System Explorer	스냅샷을 통한 파일 변경 이력 확인
	Process Monitor	악성코드 행위 자세한 로그 확인
	CurrPorts	악성코드와 연결된 IP, 포트 확인
	SmartSniff	실제 네트워크 패킷 요약 확인
	Wireshark	네트워크 패킷 상세 확인

3. 기초 분석

3.1 자동화 분석

VT에 해시 값으로 조회한 결과 전체 71개의 엔진 중 65개에서 악성으로 탐지되었다. 가장 많이 언급된 태그는 trojan, pepatch/farfil 태그이며 패밀리 유형은 pepatch, farfli, zebyvhki로 확인되었다. 행위 태그에 있는 persistence, executes-dropped-file, spreader, self-delete 등을 통해 지속성 확보, 드롭 파일 실행, 전파 시도, 자기 삭제의 행위를 참고할 수 있다.



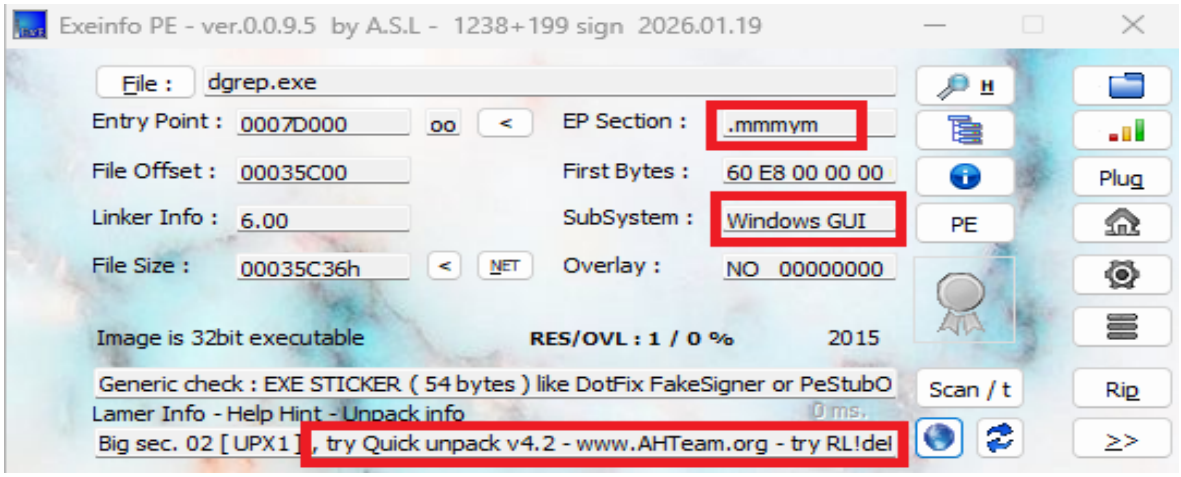
[그림 1] VirusTotal 탐지 결과

항목	내용
드롭 파일	wiseman.exe, jtztn.ttj, vbscript.dll, jckcpgh,exe
네트워크 연결	http://api.wisemansupport.com/wms/inf.php?pid admatching.co.kr 107[.]163[.]241[.]198 107[.]163[.]241[.]197

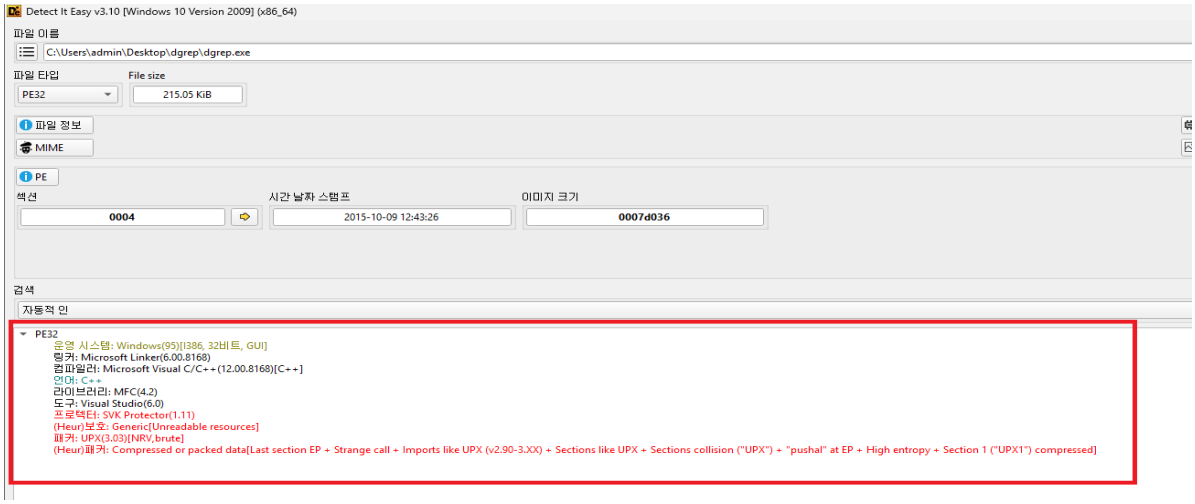
Relations 탭에서 .exe, .dll 등의 형식의 파일이 드롭되는 결과를 확인하였다. 또한 악성코드가 드롭한 파일과 연결되었던 네트워크 이력과 IP의 국가를 확인할 수 있다.

3.2 파일 식별

해당 악성코드는 PE32(32비트 실행 파일) 파일로 GUI(그래픽) 프로그램이다. 제작에 사용된 언어는 c++로 확인되었다. 패킹과 프로텍터가 모두 사용된 이중 패킹으로 확인되며 각각 UPX 3.03와 SVK-Protector v1.11로 확인되었다. EP 섹션명이 기본값인 UPX로 시작하는 것이 아니라 .mmmym으로 변조되어 자동 언패킹이 동작하지 않는다. 이는 자동 언패킹을 방해하고 정적 분석을 방해하는 행위로 볼 수 있다



[그림 2] ExeinfoPE 분석 결과



[그림 3] DIE 분석 결과

4. 정적 분석

4.1 PE 구조 확인

섹션명	Raw Size	Virtual Size	비고
UPX0	00000000	00046000	Raw Size와 Virtual Size의 차이가 큼으로 패킹이 되었다고 판단
UPX1	00034C00	00035000	Raw Size와 Virtual Size가 유사
rsrc	00000C00	00001000	리소스 섹션으로 판단됨
mmmym	00000036	00000036	일반적이지 않은 섹션명

일반적으로 PE 구조는 .text, .rdata, .data와 같은 구조를 가지고 있고 UPX로 패킹된 경우 UPX0, UPX1 같은 구조로 이루어져 있다. 본 파일에서는 mmmym와 같은 섹션명은 일반적이지 않은 섹션명이 확인되었다. 이는 패커 또는 프로텍터에 의해 변경되었을 수도 있고 제작자가 임의로 변경하여 언패킹을 방해한 것일 수 있다.

Virtual Size란 실행 중 메모리에서 차지하는 크기이다. Raw Size는 실제 파일에 저장된 크기를 의미한다. Virtual Size가 Raw Size 보다 지나치게 클 경우에는 패킹이 되었다고 의심할 수 있다.

4.2 Import 분석

Import Table에서 확인되는 DLL과 함수는 해당 악성코드가 어떤 행위를 할지 예측할 수 있는 참고자료가 될 수 있다. 다만 단정할 수는 없고 다른 분석과 함께 해석할 수 있다

DLL	추정 사용 용도
KERNEL32.DLL	파일 생성/복사/삭제, 프로세스 실행
GDI32.dll	그래픽 출력
SHLWAPI.dll	파일 경로, 문자열, 셸 관련 보조 기능 사용 가능
WS2_32.dll	네트워크 통신 (C&C 서버와 통신)

4.3 추출한 주요 문자열

발견된 문자열	추정 내용
api.wisemansupport.com	C&C 도메인 후보
RedTom21@HotMail.com	공격자 이메일로 추정
c:₩wiseman.exe c:₩windows₩system32₩rundll32.exe	파일 실행 후보
cmd.exe /c ping 127.0.0.1 –n 2&%s " %s"	자기 삭제 패턴 증거
CreateFile, WriteFile, RegSetValueEx	파일 드롭, 수정, 레지스트리 조작

5. 동적 분석

5.1 프로세스

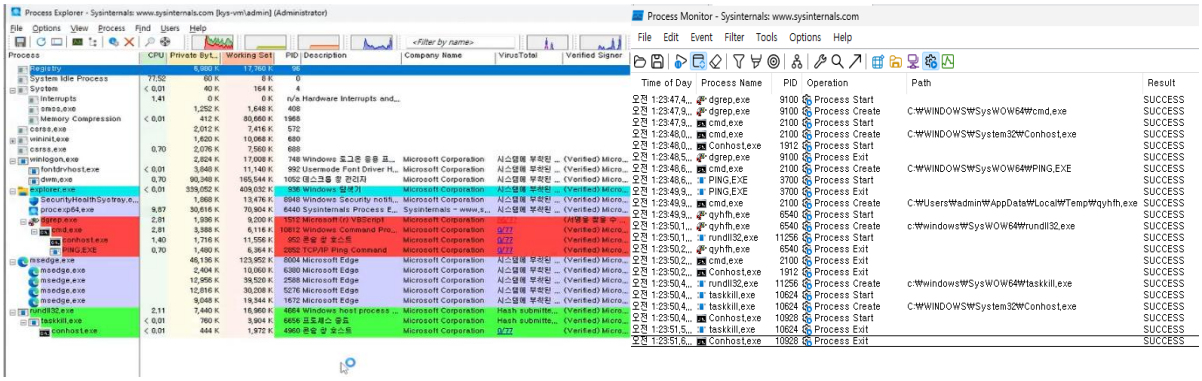
■ 프로세스 흐름

Process Explorer를 사용하여 실시간 프로세스 생성 트리 구조를 확인하고 행위 주체와 상세 내역을 Process Monitor를 사용하여 교차 검증하였다. 프로세스 생성 흐름을 트리 구조로 그리면 다음과 같다.

```
explorer.exe
 └── dgrep.exe
     └── cmd.exe
         ├── Conhost.exe          (정상 부속물)
         ├── PING.EXE             (Self-delete 딜레이)
         └── qayhfh.exe           (자기 복사본)
             └── rundll32.exe     (LotL-정상 프로그램 사용)
                 └── taskkill.exe (attrib.exe 종료, 의도 추정)
                     └── Conhost.exe (정상 부속물)
```

사용자가 원본 파일 dgrep.exe를 실행하면 dgrep.exe는 cmd.exe를 생성하여 자기 삭제 명령을 전달한 뒤 종료된다. 생성된 cmd.exe는 PING.EXE를 사용하여 2초간 대기하여 원본 프로세스가 완전히 종료될 시간을 확보하고 Temp 폴더에 생성된 복사본 파일을 실행하여 qayhfh.exe 프로세스를 생성한다. 생성된 qayhfh.exe 프로세스는 원본 파일을 삭제하고 정상 윈도우 프로세스인 rundll32.exe를 생성하고 종료된다.

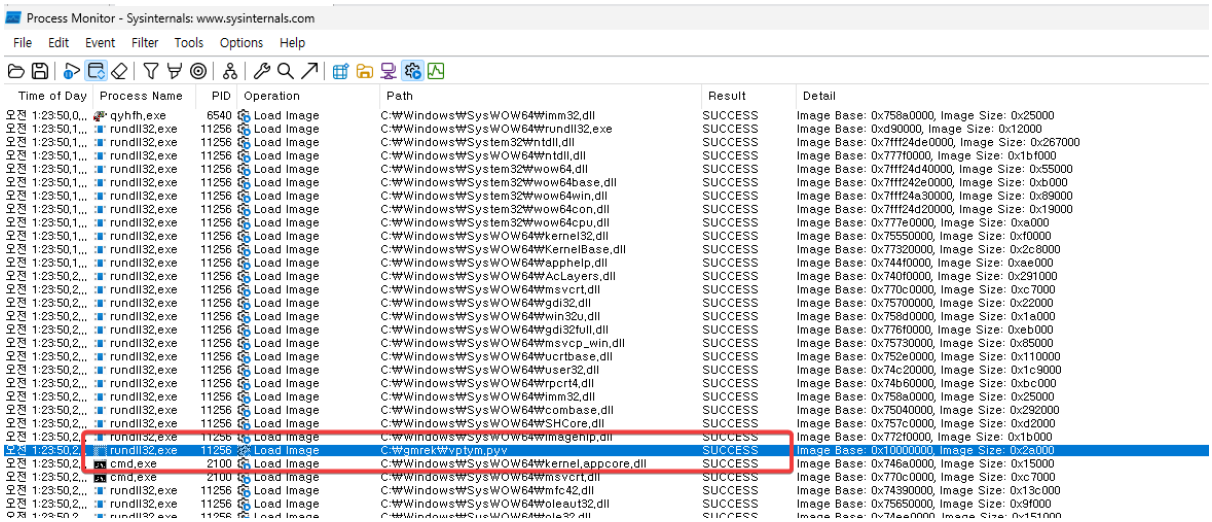
* Temp 폴더에 생성된 복사본 파일 qayhfh.exe는 매번 랜덤한 이름의 파일로 생성된다. 즉 프로세스 명도 매번 달라진다.



[그림 4] Process Explorer 프로세스 트리

■ 결과

최종적으로 dgrep.exe, cmd.exe, qayhfh.exe는 모두 종료되고, 메모리에는 rundll32.exe만 남게 된다. 남아있는 rundll32.exe는 악성 활동의 주체가 되어 악성 DLL 페이로드를 통해 악성 행위를 진행한다.



[그림 5] Process Monitor 프로세스 로그

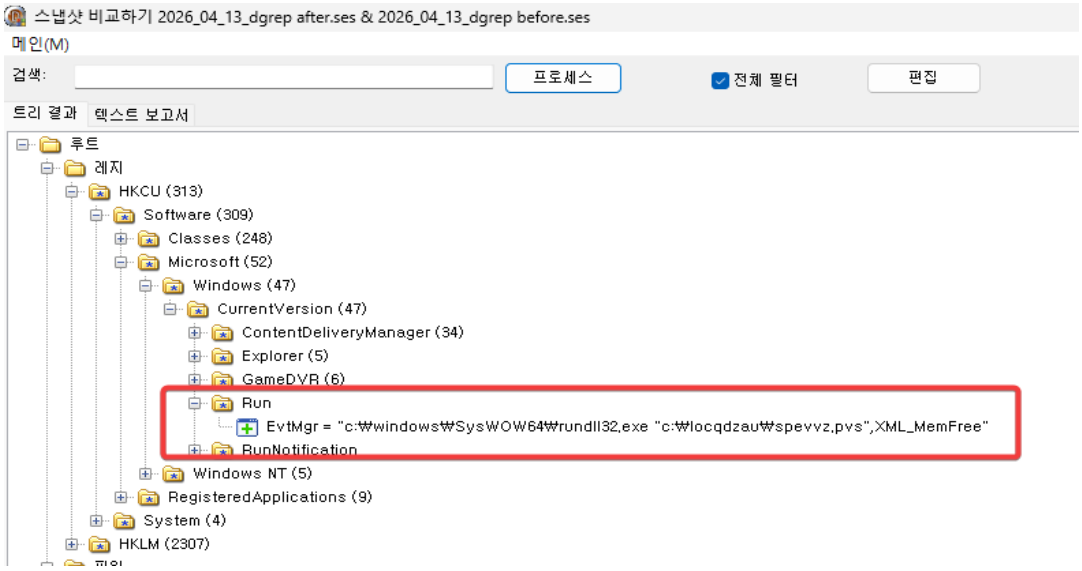
5.2 레지스트리

Autoruns를 사용하여 레지스트리 영역의 변경 사항을 빠르게 파악하고 System Explorer, Process Monitor를 사용하여 더욱 자세한 내용을 확인하고 교차 검증하였다.

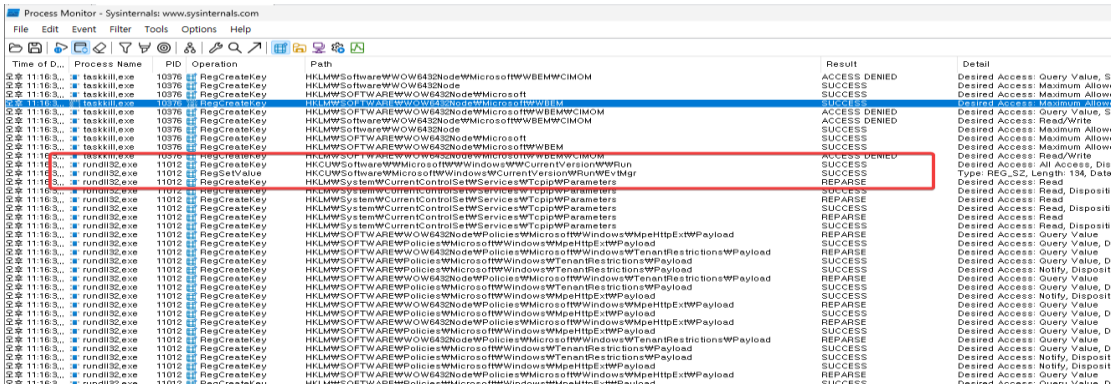
항목	값
등록 경로	HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run
등록명	EvtMgr
실행명령	rundll32.exe "[랜덤 경로]₩[랜덤 파일].[가짜 확장자]",XML_MemFree
등록주체	rundll32.exe

rundll32는 관리자 권한 없이도 레지스트리 등록이 가능한 현재 사용자 영역인 HKCU 영역에 EvtMgr라는 이름으로 키를 등록하였다. EvtMgr은 "Event Manager"라는 이름을 연상시켜 사용자가 정상 항목으로 오인할 가능성이 있다. 하지만 해당 분석에서 악성코드 실행 후에 생성된 것으로 확인되었다.

실행 경로는 랜덤한 이름의 폴더 생성과 가짜 DLL 페이로드 생성으로 일정하지 않지만 rundll32.exe 프로세스를 사용하여 XML_MemFree라는 함수(명령어)를 사용한다는 것을 확인할 수 있다.



[그림 6] System Explorer 레지스트리 스냅샷



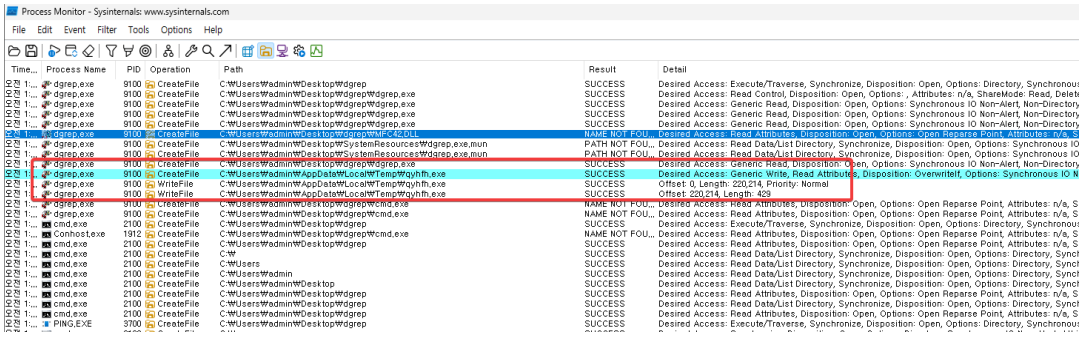
[그림 7] Process Monitor 레지스트리 로그

5.3 파일 변경

System Explorer의 스냅샷 기능을 통해 악성코드 실행 전후 파일 생성 변화를 비교하고 Process Monitor를 통해 더 자세한 내용을 확인하였다.

■ 자기 복사본 생성

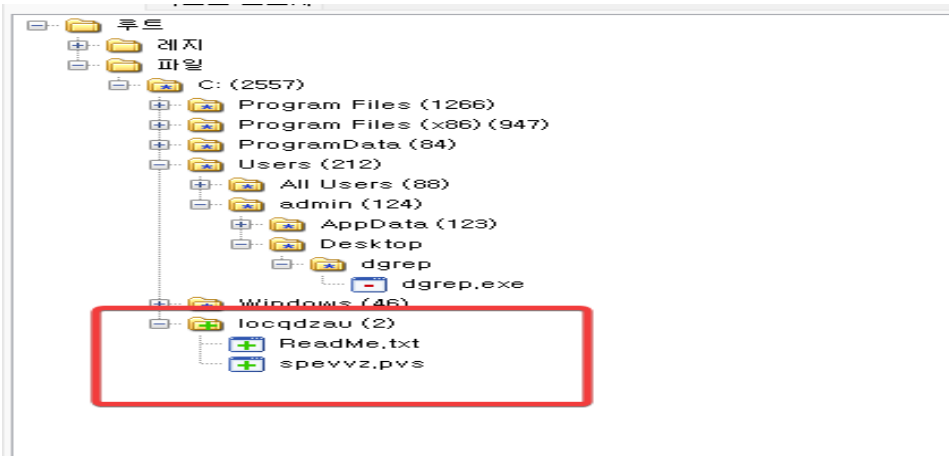
dgrep.exe(원본 파일)이 실행 후에 윈도우 임시 저장 폴더인 %TEMP% 경로에 자기 자신과 동일한 복사본을 생성하였다. 이때 생성된 복사본의 이름은 랜덤한 이름을 가져서 탐지를 어렵게 만든다.



[그림 8] Process Monitor 자가복제

■ 페이로드 DLL 드롭

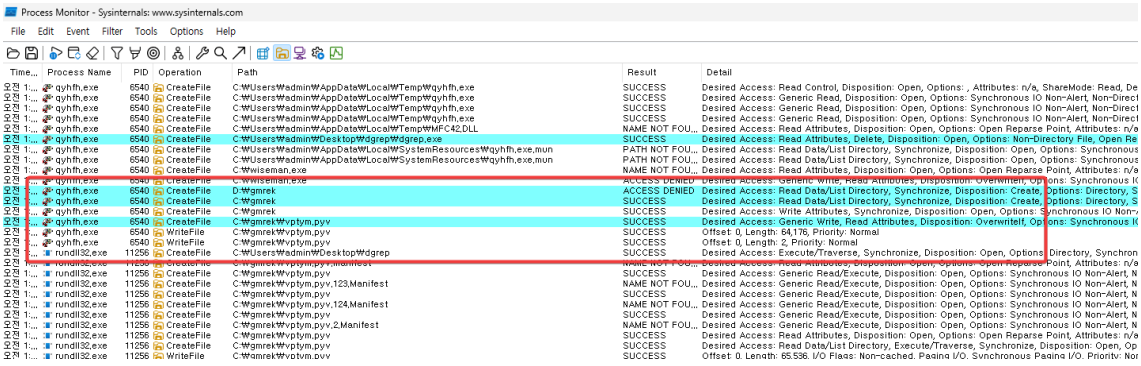
복사본이 C:₩경로 바로 아래에 폴더를 생성하고 그 안에 페이로드를 생성한다. 이때 생성된 폴더와 페이로드는 랜덤한 이름을 가지고 페이로드 DLL은 가짜 확장자로 위장한다. 랜덤한 이름과 가짜 확장자는 탐지를 어렵게 만든다.



[그림 9] System Explorer 페이로드 드롭 스냅샷

■ 다른 드라이브로 전파 시도

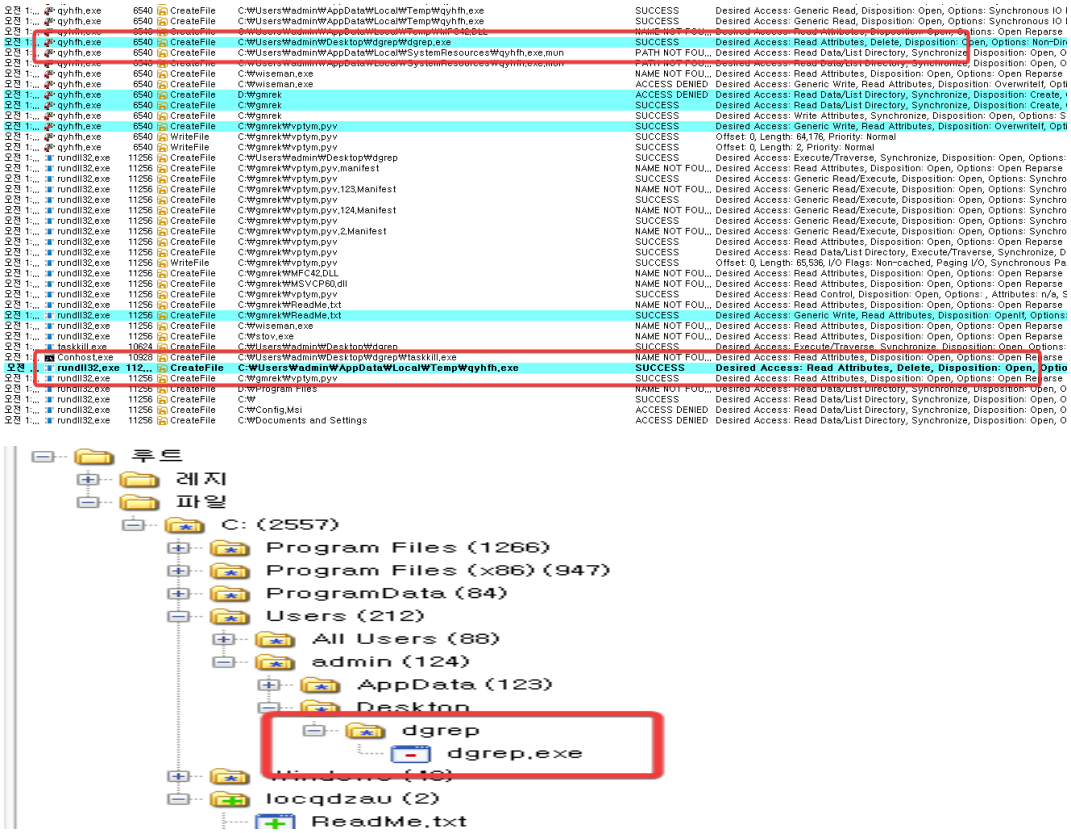
복사본은 C:₩경로 외에도 D:₩ 루트 경로에도 접근하여 파일을 생성하려 시도하였지만 접근 권한 없음(ACCESS DENIED)으로 실패한 이력을 확인할 수 있다.



[그림 10] Process Monitor 전파시도

■ 원본과 복사본 삭제

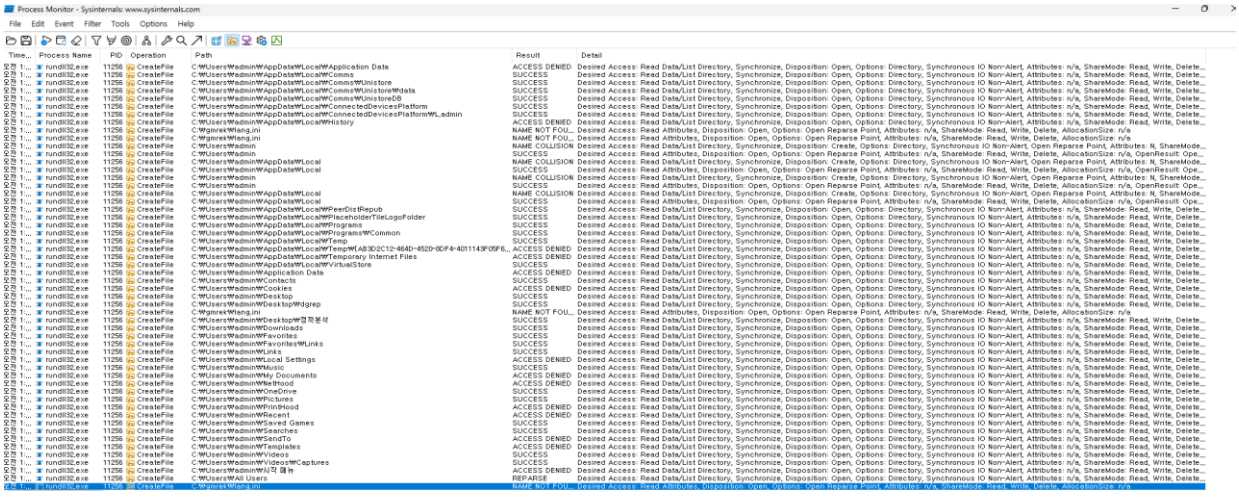
복사본 실행 후 PING.EXE가 2초간 실행된 뒤 복사본은 원본 파일을 삭제하였다. 복사본 파일은 rundll32가 페이로드 DLL을 로드한 뒤 삭제되었다. 결론적으로 디스크 상에 악성 exe 파일 흔적은 완전히 제거되고 정상 서명된 rundll32.exe만 메모리에 남게 된다.



[그림 11] 원본 및 복사본 삭제 행위

■ 추가 파일 탐색 시도

Process Monitor 로그에서 rundll32.exe가 다수의 파일 및 디렉터리에 접근하는 행위가 확인되었다.



[그림 13] rundll32.exe 파일 접근 로그

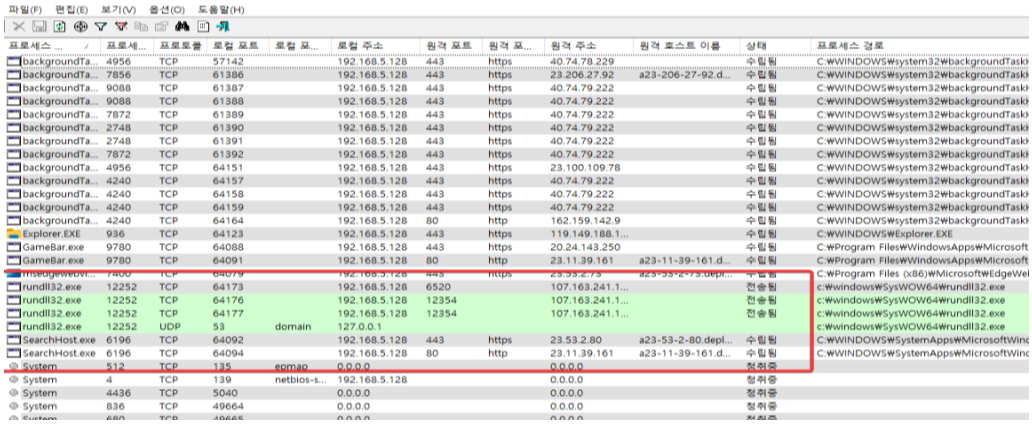
5.4 네트워크

네트워크 분석에서는 CurrPorts로 어떤 포트를 통해 어떤 IP와 통신하는지 확인하였다. SmartSniff로 실제 통신 내용을 확인하였으나 캡처가 되지 않았고 Wireshark로 어떤 상황인지 더 자세히 확인하였다.

■ 통신 대상 확인

CurrPorts로 확인한 결과 rundll32가 2개의 IP와 TCP 통신을 시도하는 것을 확인하였다. rundll32는
107[.]163[.]241[.]198:6520 (TCP), 107[.]163[.]241[.]197:12354 (TCP)와 통신을 시도하였고 연결 수립이 아닌 연결 요청을 전송한 것으로 확인하였다. IP 확인 결과 두 IP의 국가는 미국으로 확인되고 동일 서브넷으로 보인다.

Windows 기본 프로그램인 rundll32는 원래 네트워크 통신을 하지 않는 프로그램이다.



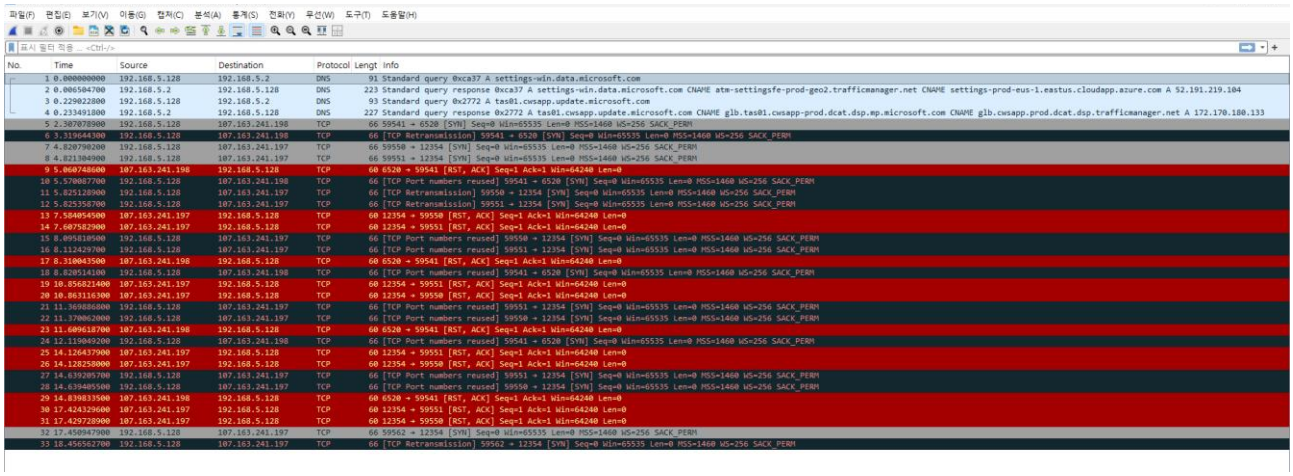
[그림 14] CurrPorts 분석

■ 실제 송수신 여부

SmartSniff로 네트워크 송수신 내용을 캡처한 결과 CurrPorts에서 발견된 IP와 실제 통신을 주고받은 내용을 확인할 수 없었다. 이를 통해 앞서 CurrPorts에서 전송됨의 상태가 실제 수립으로 이어지지 않아 실제 네트워크 통신이 이루어지지 않았다는 것을 확인할 수 있다.

■ 패킷 분석

Wireshark로 한 번 더 정밀하게 패킷을 캡처해 본 결과 로컬 IP(내 PC)에서 CurrPorts에서 발견된 원격 IP(C&C 서버)로 TCP 연결을 시도(SYN 플래그 전송)하였지만 연결이 거절되는 패킷(RST)을 확인할 수 있다. 중요한 것은 통신에 실패하였지만 로컬 IP에서 계속 연결을 재시도한다는 점이다.



[그림 15] Wireshark TCP SYN/RST 패킷 확인

6. 공격 흐름 정리 (Kill Chain)

단계	Kill Chain 구분	관찰된 행위
2	Exploitation (실행)	explorer.exe에서 dgrep.exe 더블클릭 실행. 별도 취약점 없이 사용자 실행에 의존
3	Installation (설치)	%TEMP%에 자기 복사본(qayhfh.exe) 드롭 → C:₩gmrek₩vpytm.pyv 페이로드 DLL 드롭
4	Defense Evasion (회피)	원본 및 복사본 자기 삭제, rundll32.exe에 DLL 로드하여 메모리 상주 (LotL)
5	Persistence (지속성)	HKCU₩...₩Run₩EvtMgr 등록 → 재부팅 후에도 rundll32.exe가 악성 DLL을 다시 로드
6	C2 (명령제어)	107[.]163[.]241[.]197:12354 / 107[.]163[.]241[.]198:6520 로 반복 접속 시도 (현재는 RST 응답)
7	Lateral Movement (확산)	이동식 드라이브(D:₩)에 자기 복사 시도 → Worm 특성
8	Collection (정보수집)	Desktop / Documents / Downloads / AppData 등 사용자 주요 폴더 열람

7. 결론

이번에 분석한 dgrep.exe는 분석 결과 **자가 복제, 전파 시도, 지속성 확보**, 윈도우 기본 프로그램을 사용하여 **외부 서버와 연결 시도, 셀프 삭제** 등의 행위를 보여 악성코드로 판별되었다.

VT를 참고한 결과 **65/71의 탐지 점수**를 받았고 **pepatch / farfli의 패밀리 유형**으로 트로이목마, 웜, 백도어 태그를 많이 확인할 수 있었다. 실제 자체 분석 결과도 **트로이목마와 웜, 백도어** 유형의 악성코드로 판단된다.

dgrep.exe(이하 원본)는 실행 직후 임시 폴더에 랜덤한 이름으로 자신의 복사본을 생성한다(이하 복사본). 원본은 cmd를 실행 후 ping 127.0.0.1 -n 2로 2초간의 시간을 확보한 후 원본 프로세스는 종료되고 복사본 프로세스가 실행된다. 그 후 복사본은 원본 파일을 삭제한다. 복사본은 C:₩ 경로에 랜덤한 폴더를 생성하여 페이로드 DLL을 가짜 확장자로 드롭한다. 이때 생성된 폴더와 페이로드는 모두 랜덤한 이름으로 탐지를 어렵게 한다. 또한 복사본은 D:₩ 경로에 접근을 시도하여 전파를 시도한다. 복사본은 Windows 정상 프로세스인 rundll32를 호출(LotL 기법)하여 페이로드 DLL을 실행시킨다. 또한 ReadMe.txt를 드롭한다. 이후 악성 행위의 주체는 rundll32가 되고 복사본은 프로세스 종료 후 rundll32에 의해 삭제된다.

rundll32는 HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩EvtMgr에 EvtMgr라는 이름의 **레지스트리를 등록하여 지속성을 확보**하였다. 또한 107[.]163[.]241[.]198:6520, 107[.]163[.]241[.]197:12354의 **IP 주소와 지속적인 접속**을 시도한다. 네트워크 분석에서 rundll32가 네트워크 연결을 위해 SYN 플래그를 보냈지만 연결이 수립되지 않고 RST 응답으로 거절되어 실제 패킷을 확인하지 못하였다.

현재 기준으로 다소 오래된 악성코드로 C&C 서버가 중단되어 연결이 안 되는 것으로 판단된다 하지만 네트워크 분석에서 rundll32.exe가 C&C 서버로 추정되는 IP에 지속적인 연결을 시도하기에 C&C 서버가 살아난다면 언제든지 네트워크 통신이 이루어지고 악성 행위가 **증가할 수 있다** 따라서 **현재도 매우 높은 위험성을 가지고 있는 악성코드이다**

8. 대응방안

■ 감염 확인

1. 최근 출처가 불분명한 파일을 실행한 적이 없는지 확인한다.

해당 악성코드의 파일명은 dgrep.exe 이지만 VT에서 확인할 수 있듯이 다른 이름으로도 유포된 이력이 있다 또한 파일명은 쉽게 변경이 가능하기에 출처가 불분명한 파일을 실행한 적이 있는지 확인해본다 실행했던 파일이 보이지 않는다면 더욱 의심해볼 수 있다

2. C:₩ 바로아래 또는 다른 드라이브 루트 경로에 출처 불명의 폴더가 있는지 확인한다.

해당 악성코드의 주요 행위 중 하나는 드라이브 루트 경로에 랜덤한 이름의 폴더를 생성하고 그 안에 가짜 확장자를 가진 페이로드를 생성하는 것이다 파일 탐색기 설정을 숨김 파일 모두 보기로 설정한 후 C:₩와 같은 경로에 의심스러운 폴더와 페이로드가 있는지 확인한다.

3. rundll32.exe가 실행 중인지 확인한다.

해당 악성코드는 정상적인 프로그램인 rundll32를 사용하여 악성 행위를 하는 것으로 확인되었다. 작업관리자를 사용하여 rundll32가 실행 중인지 확인한다. 다만 rundll32는 정상적인 상황에서도 사용할 수 있어 이것만으로 감염이 되었다고 판단하지 않고 위 행위들과 같이 확인되었을 때 감염 가능성이 높아진다.

■ 감염 시 대응

1. 네트워크를 차단한다

C&C 서버가 살아있다면 언제든지 네트워크 통신을 통해 악성 명령어를 받을 수 있다 네트워크 차단을 통해 추가적인 명령어 수신을 차단한다

2. 악성 프로세스 종료

작업관리자를 통해 rundll32가 실행 중이라면 프로세스를 강제 종료한다 프로세스를 종료하지 않으면 사용 중인 악성 파일들을 삭제하지 못할 수 있다

3. 레지스트리 제거

레지스트리 편집기(regedit) 실행하여 HKEY_CURRENT_USER₩Software₩Microsoft ₩Windows₩CurrentVersion₩Run 경로에 EvtMgr 항목을 삭제한다

4. 생성파일 제거

C:₩루트 경로와 %TEMP% 경로에 있는 출처 불명의 폴더와 파일을 삭제한다

*%TEMP% 경로는 윈도우 검색창에 입력하면 열 수 있다

5. 백신 프로그램 사용

신뢰할 수 있는 백신을 사용하여 전체 검사를 진행하여 발견하지 못한 악성 행위를 정리한다

■ 예방

- 출처 불명한 파일(.exe, .dll)을 실행하지 않는다
- 파일 확장자 표시 설정을 권장한다
- IP 107[.]163[.]241[.]197, 107[.]163[.]241[.]198을 방화벽에 추가한다
- 비표준화 포트 12354, 6520을 방화벽에 추가한다
- 백신을 최신 버전으로 항상 유지한다

부록. IOC 정리

본 IOC는 분석 환경에서 직접 확인한 행위 기반 지표와 VT 조회 결과를 함께 정리한 것이다. 파일명, 폴더명, 확장자 일부는 실행 시점마다 랜덤하게 생성될 수 있으므로 단일 값보다 행위 패턴을 함께 확인해야 한다.

1. 파일 해시

종류	값	확인 경로
MD5	68af0599e74d36bc2f39a2710754082c	VirusTotal
SHA-1	c63f22e2d6feecbe9801c76a76f81589bce1b9a3	VirusTotal
SHA-256	d3e4a46b95a3a54c762f0e1696e9167528bd1cf30b190e4893b44f0259e7893c	VirusTotal

2. 호스트 기반 IOC

2.1 파일 및 경로

구분	값	확인 경로
원본 파일	dgrep.exe	직접 분석
별칭 / 유포명	vbscript.dll / output.123910684.txt	VirusTotal
드로퍼 복사본	%TEMP%₩[랜덤].exe	Process Monitor
드로퍼 복사본 예시	%TEMP%₩qayhfh.exe	Process Monitor
페이로드 DLL	C:₩[랜덤폴더]₩[랜덤파일].[가짜확장자]	Process Monitor / System Explorer
페이로드 DLL 예시	C:₩gmrek₩vpytm.pyv	Process Monitor / System Explorer
드롭 파일	C:₩[랜덤폴더]₩ReadMe.txt	System Explorer
삭제 대상	원본 dgrep.exe, %TEMP%₩[랜덤].exe	Process Monitor / Process Explorer
전파 시도 경로	D:₩	Process Monitor
탐색 시도 경로	C:₩wiseman.exe, C:₩gmrek₩wlang.ini, C:₩stov.exe	Process Monitor

2.2 레지스트리

구분	값	확인 경로
Run 키	HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩EvtMgr	Autoruns / System Explorer / Process Monitor
등록명	EvtMgr	Autoruns
실행 명령 패턴	rundll32.exe "[랜덤경로]₩[랜덤파일].[가짜확장자]",XML_MemFree	Autoruns / Process Monitor
고정 함수명	XML_MemFree	Autoruns / Process Monitor

3. 네트워크 IOC

구분	값	확인 경로
C&C IP:Port	107.163.241.198:6520	CurrPorts / Wireshark
C&C IP:Port	107.163.241.197:12354	CurrPorts / Wireshark
연결 상태	SYN 전송 후 RST 응답	Wireshark
C&C 도메인	api.wisemansupport.com	VirusTotal / BinText
관련 도메인	admatching.co.kr, api.admatching.co.kr	VirusTotal
C&C URL 패턴	/wms/inf.php, /wms/log.php, /wms/upd.php	VirusTotal / BinText
참조 IP	114.114.114.114, 123.126.45.92	VirusTotal

4. 기타 분석 지표

구분	값	확인 경로
공격자 이메일	RedTom21@HotMail.com	BinText / VirusTotal
위장 메타데이터	FileDescription: Microsoft (r) VBScript	PEview
패커	UPX 3.03	ExeinfoPE / DIE
프로텍터	SVK-Protector v1.11	ExeinfoPE / DIE
EP 섹션명	.mmmym	PEview
관련 패밀리	pepatch, farfli, zebyvhki	VirusTotal

5. IOC 확인 시 주요 패턴

확인 대상	주요 확인 패턴
파일 생성	%TEMP%₩[랜덤].exe 생성
페이로드 드롭	C:₩[랜덤폴더]₩[랜덤파일].[가짜확장자] 생성
실행 방식	rundll32.exe를 통한 페이로드 실행
지속성 확보	HKCU₩...₩Run₩EvtMgr 등록
자기 삭제	원본 파일 및 임시 복사본 삭제
전파 시도	D:₩ 경로 접근 시도
네트워크 행위	외부 C&C IP로 반복 연결 시도
위장 및 회피	VBScript 메타데이터 위장, UPX/SVK-Protector 사용, EP 섹션명 변조