Fileless 악성코드 종류와 기법

(Fake) Fileless 악성코드 기법과 종류

2017.07.08

안랩 시큐리티대응센터(ASEC) 분석팀
차민석 (車珉錫, CHA Minseok, Jacky Cha) 수석 연구원

AhnLab

CodeEngn

www.CodeEngn.com

2017 CodeEngn Conference 14

Contents

AhnLab

01
Fileless 악성코드

AhnLab

Fileless Malware ?

AhnLab

• 관련 기사

-

"파일 없는 악성코드 공격 역대 최대치"

BY 이유지 on 2017년 1월 16일 • (0)

보안

지난 수년간 전

보안업체 하우리(대표 김희천)는 작년 한 해 동안 국내에서 발생한 '파일 없는(Fileless)' 악성코드 공격이 역대 최대치를 기록했다고 16일 밝혔다.

파일이 없는 악성코드 공격은 시스템상에 악성코드가 파일로 존재하지 않고 메모리 또는 레지스트리 상에서만 존재하며 동작하는 것을 말한다. 이같은 공격은 계속 급증세다.

최근 140개 이상의

ss malware attacks)은 현재 알려진 공격의 15%를 차지하며 지난 수년 간 다양한 형태로 존재했다.

SECURITY

Fileless malware: An undetectable threat

Fileless malware is a dangerous and devious threat--and it's gaining traction. Find out how it might affect your organization, network, and the devices connected to it.

By Jesus Vigo | June 15, 2017, 7:39 AM PST

* Source : http://www.itworld.co.kr/howto/103379 & https://byline.network/2017/01/1-531/ & http://www.techrepublic.com/article/fileless-malware-an-undetectable-threat/

Fileless

AhnLab

01

장점

- 사용자 발견이 좀 더 어려움
- 보안 제품 우회 가능성 높임

02

단점

- 일반 악성코드 보다 조금 더 제작 어려움
- 디스크 흔적을 남기지 않기 위해서 취약점을 이용 해야 함

03

결과

- 종류와 수가 적음
- 메모리에만 존재하는 형태 보다 디스크에 흔적이 남는 형태가 더 많음

Fileless Malware ?

AhnLab

- Wikipedia
  - Fileless 가 아니라 심지어 Disk 에 쓰지 않음 ?

Fileless malware

From Wikipedia, the free encyclopedia

Fileless malware is a variant of computer related malicious software that exists exclusively as a computer memory-based artifact i.e. in RAM. It is part of the family that has been defined as an Advanced Volatile Threat (AVT).[1]

It does not write any part of its activity to the computer's hard drive meaning that it's very resistant to existing Anti-computer forensics strategies that incorporate file-based whitelisting, signature detection, hardware verification, pattern-analysis, time-stamping, etc., and leaves very little by way of evidence that could be used by digital forensic investigators to identify illegitimate activity.

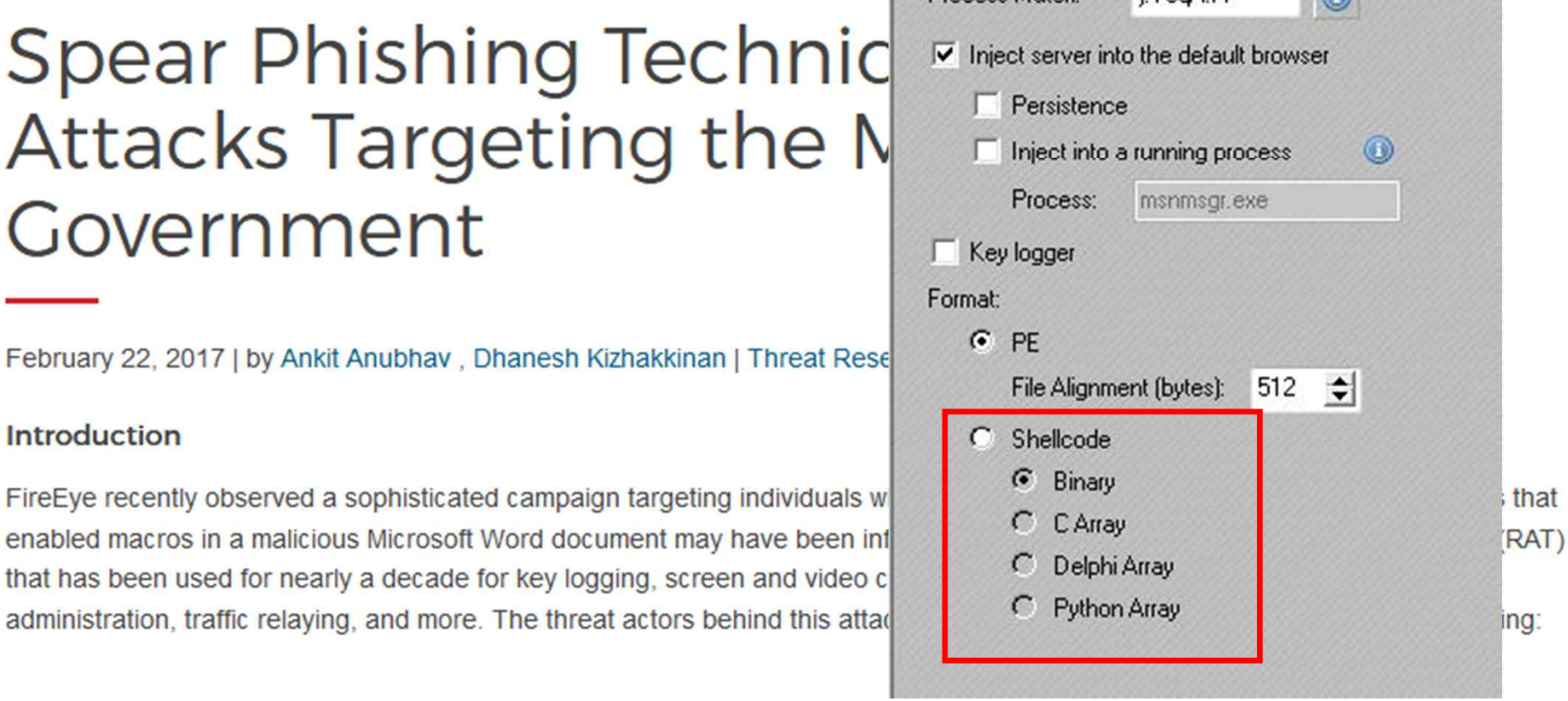
As malware of this type is designed to work in-memory, its longevity on the system exists only until the system is rebooted.

* Source : https://en.wikipedia.org/wiki/Fileless_malware

Why Fileless ?

AhnLab

- Whitelist 보안 제품 우회 가능
  - Poisonivy는 Shellcode 형태로도 제작 가능
  - Macro, Script 등을 통해 Shellcode 실행 가능

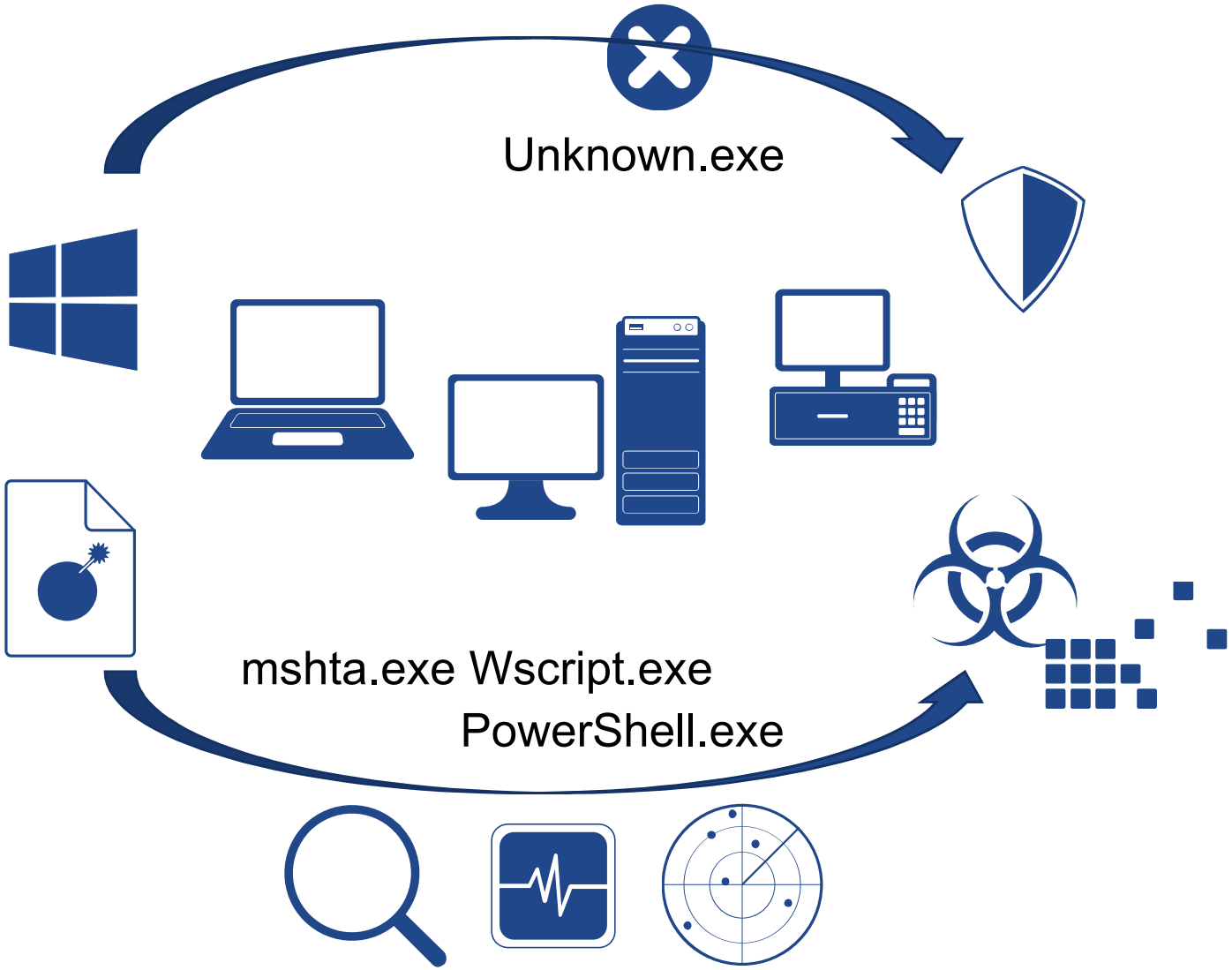


* Source : https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

Bypass Security Product

AhnLab

- 정상 파일을 통한 보안 프로그램 우회 시도
  -



02
정말 Fileless 일까?

AhnLab

기준이 필요

AhnLab

- Fileless 기준 필요
  - Disk ? File ? Dropper 가 있다면 ? Registry 에 저장된 형태는 ?
- 본 발표자료에서는 언론 등을 통해 Fileless 로 알려진 악성코드를 분석
- Fileless 기준에 대해서는 토론 중

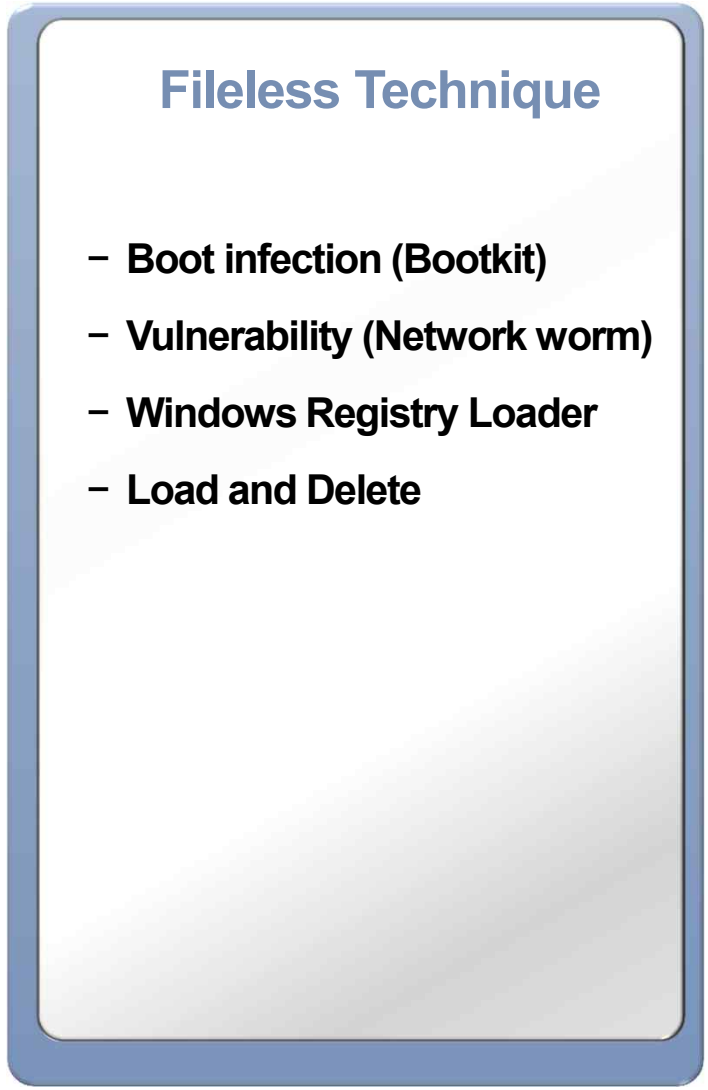
03
(Fake) Fileless Technique

AhnLab

Fileless Technique

AhnLab

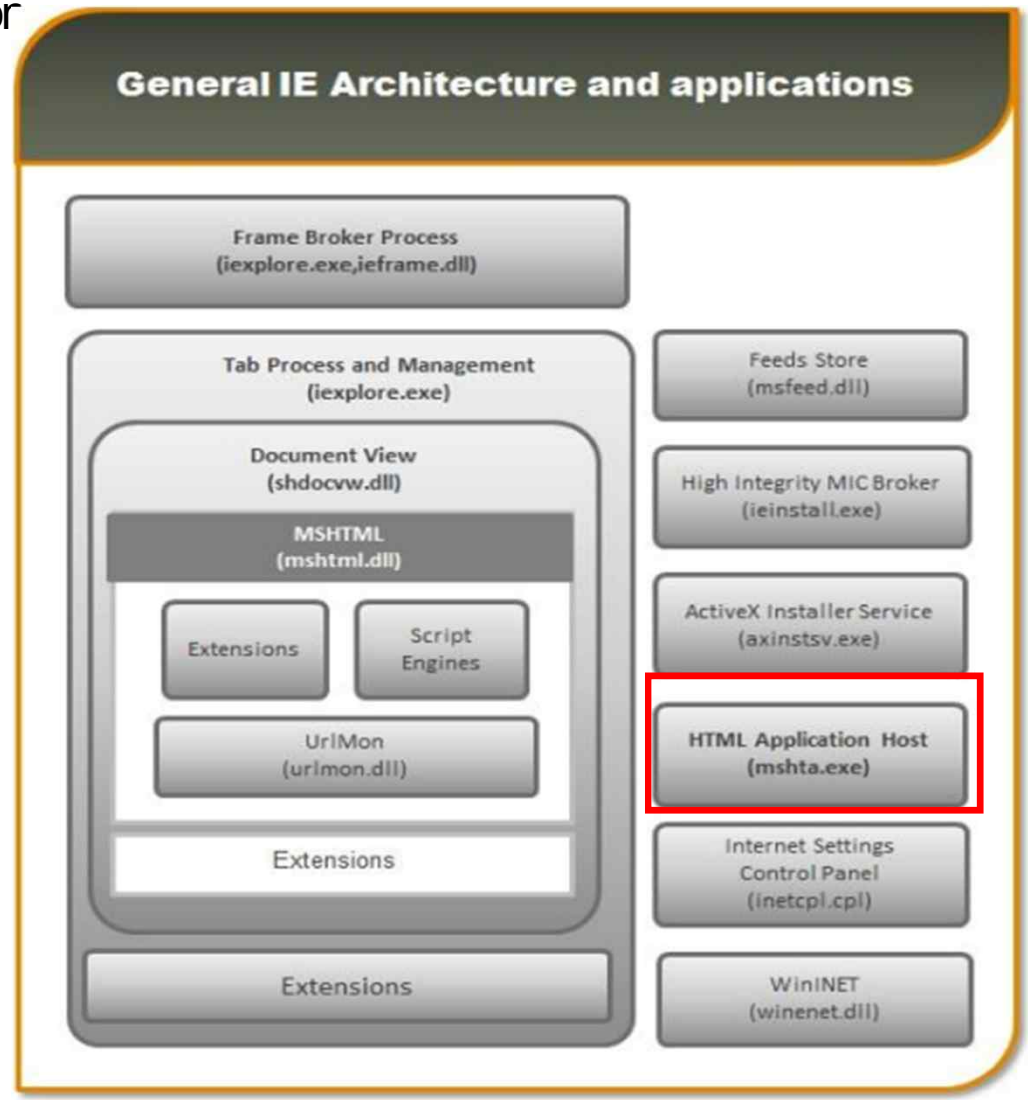
- Fileless Technique



Background

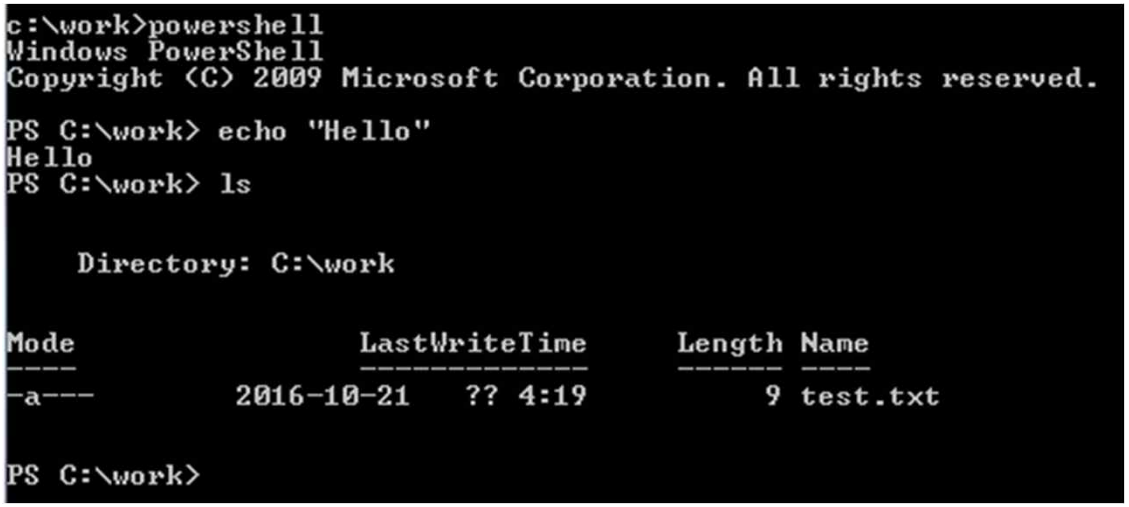
- One-click Fileless infection

  - HTA는 IE 외부 보안 정책



* Source : One-Click-Fileless (2016)(Himanshu Anand & Chastine Menrige)

- PowerShell
  - 2006년 공개된 Script Language
  - Windows Vista 이후 기본 탑재
  - 앞으로 명령 프롬프트 대체 가능



What is PowerShell?

PowerShell is an automation platform and scripting language for Windows and Windows Server that allows you to simplify the management of your systems. Unlike other text-based shells, PowerShell harnesses the power of the .NET Framework, providing rich objects and a massive set of built-in functionality for taking control of your Windows environments.

PowerShell Desired State Configuration (DSC)

PowerShell Desired State Configuration (DSC) is a platform for testing and ensuring the declarative state of a system. DSC allows you to scale complex deployments across environments, enables collaboration of management, and corrects for configuration drift.

* Source : https://msdn.microsoft.com/en-us/powershell

- WMI (Windows Management Instrumentation)
  -

Windows Management Instrumentation

Purpose

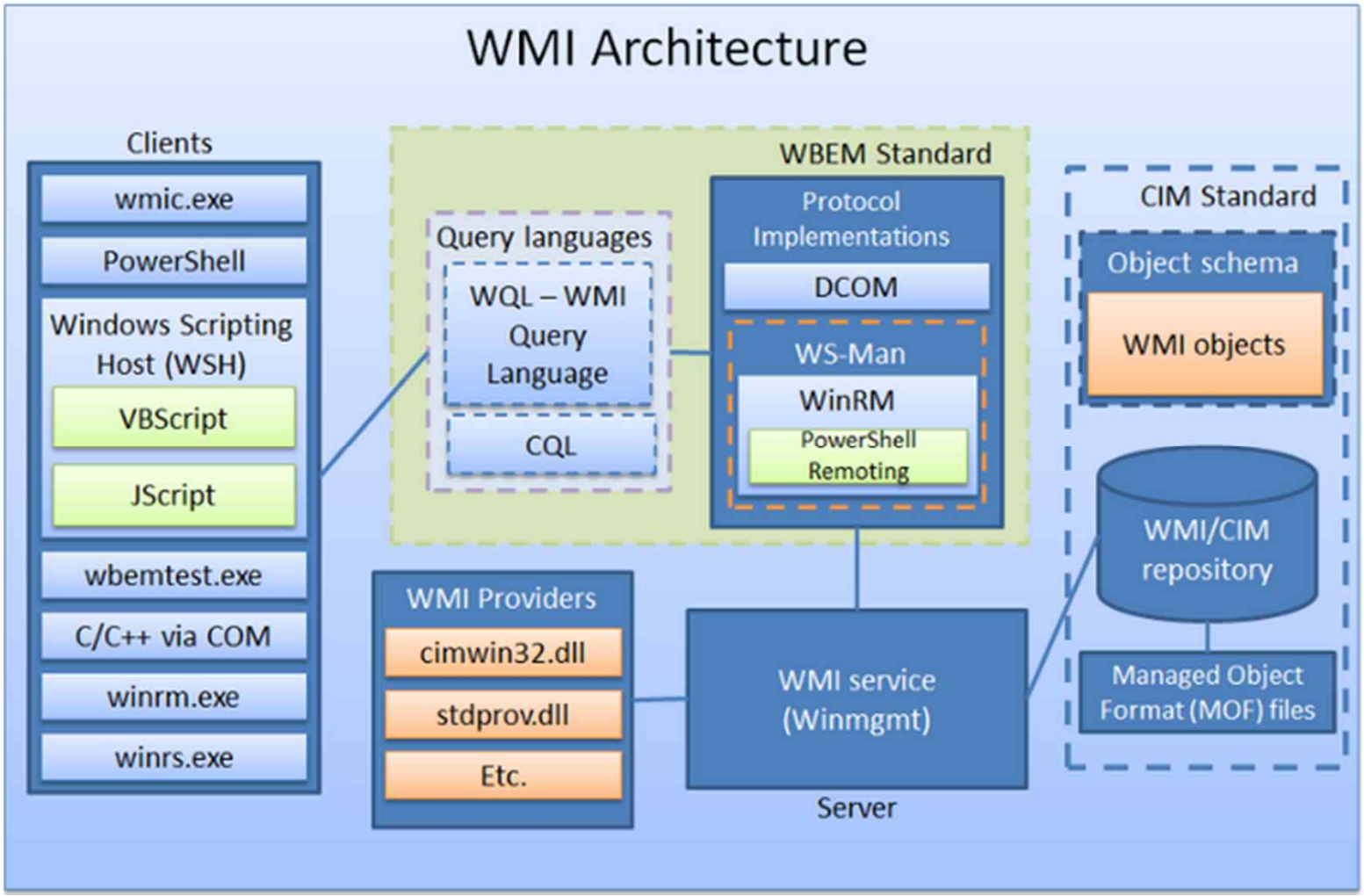
Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems. You can write WMI scripts or applications to automate administrative tasks on remote computers but WMI also supplies management data to other parts of the operating system and products, for example System Center Operations Manager, formerly Microsoft Operations Manager (MOM), or Windows Remote Management (WinRM).

Note The following documentation is targeted for developers and IT administrators. If you are an end-user that has experienced an error message concerning WMI, you should go to Microsoft Support and search for the error code you see on the error message. For more information about troubleshooting problems with WMI scripts and the WMI service, see WMI Isn't Working!

Note WMI is fully supported by Microsoft; however, the latest version of administrative scripting and control is available through the Windows Management Infrastructure (MI). MI is fully compatible with previous versions of WMI, and provides a host of features and benefits that make designing and developing providers and clients easier than ever. For more information, see Windows Management Infrastructure (MI).

* Source : https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx

- WMI Architecture
  -



* Source : http://oversitesentry.com/blackhat-presentation-wmi-architecture-used-to-attack/

- PowerShell + WMI
  - 가상 환경 검사 : Get-WmiObject –Class Win32_ComputerSystem

```
c:\work>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\work> Get-WmiObject -Class Win32_ComputerSystem


Domain                  : WORKGROUP
Manufacturer            : Gigabyte Technology Co., Ltd.
Model                   : To be filled by O.E.M.
Name                    : U[illegible]
PrimaryOwnerName        : u[illegible]
TotalPhysicalMemory     : 17062051840
```

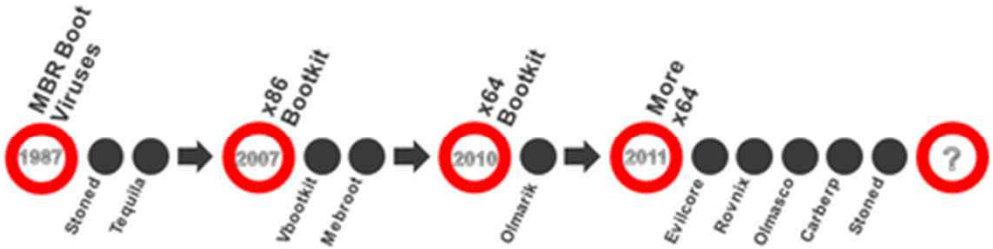
```
c:\work>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\work> Get-WmiObject -Class Win32_ComputerSystem


Domain                  : WORKGROUP
Manufacturer            : VMware, Inc.
Model                   : VMware Virtual Platform
Name                    : WIN[illegible]
PrimaryOwnerName        : Windows ???
TotalPhysicalMemory     : 4294434816
```

Boot infection (Bootkit)

AhnLab

- Bootkit

  - 부팅 관련 영역 감염



- Bootkit PoC evolution:
  - ✓eEye Bootroot (2005)
  - ✓Vbootkit (2007)
  - ✓Vbootkit v2 (2009)
  - ✓Stoned Bootkit (2009)
  - ✓Evilcore x64 (2011)
  - ✓Stoned x64 (2011)
- Bootkit Threats evolution:
  - ✓Mebroot (2007)
  - ✓Mebratix (2008)
  - ✓Mebroot v2 (2009)
  - ✓Olmarik (2010/11)
  - ✓Olmasco (2011)
  - ✓Rovnix (2011)
  - ✓Carberp (2011)

Stoned Bootkit – 2009 Another example of MBR-based bootkit infection.	Olmarik (TDL4) – 2010/11 The first 64-bit bootkit in the wild.
Stoned Bootkit x64 – 2011 MBR-based bootkit supporting the infection of 64-bit operating systems.	Olmasco (TDL4 modification) – 2011 The first VBR-based bootkit infection.
DeepBoot – 2011 [9] Used interesting tricks to switch from real-mode to protected mode.	Rovnix – 2011 The evolution of VBR-based infection with polymorphic code.
Evil Core – 2011 [10] This concept bootkit used SMP (symmetric multiprocessing) for booting into protected-mode	Mebromi – 2011 The first exploration of the concept of BIOSkits seen in the wild.
VGA Bootkit – 2012 [11] VGA-based bootkit concept.	Gapz – 2012 [12] The next evolution of VBR infection
DreamBoot – 2013 [13] The first public concept of UEFI bootkit.	OldBoot - 2014 [14] The first bootkit for the *Android* operating system in the wild.

* Source : https://www.welivesecurity.com/2012/01/03/bootkit-threat-evolution-in-2011-2/ &

https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-RodionovMatrosov.pdf

Network worm

AhnLab

- Memory Only
  - 2001년 7월 CodeRed, 2003 년 1월 SQL Slammer, 2004년 3월 19일 : Witty
  - 보통 취약점 공격해 감염

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

* Source : https://en.wikipedia.org/wiki/Code_Red_(computer_worm)

Cross-Site Scripting worm

AhnLab

- Fileless ?

  - Cache에 Script가 남는다면 ?

Cross-Site Scripting Worm Hits MySpace

By Nate Mook | Published 12 years ago | Follow @natemook

52 Comments | Like 1 | Share | G+1 3 | Tweet

With the advent of social networking sites, becoming more popular is as easy as crafting a few lines of JavaScript code, it seems.

Technical explanation of The MySpace Worm
Also called the "Samy worm" or "JS.Spacehero worm"

Click here to read the entertaining story of the development, release, and ensued hilarity of The MySpace Worm

Full source code of worm at bottom.

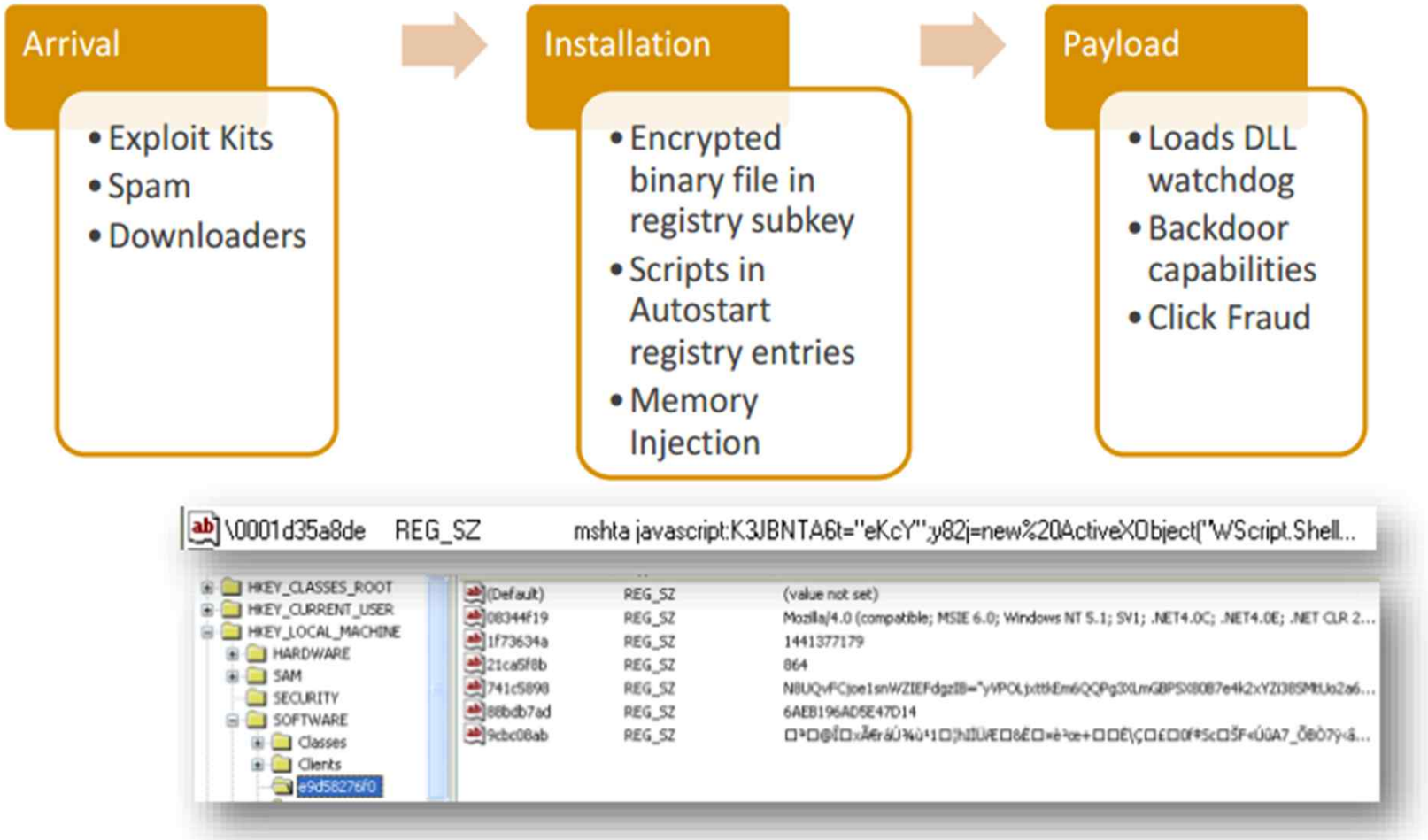
Please note that this code and explanation was only released AFTER MySpace resolved this.
None of this would work on MySpace at the time it was released and it will not work now. Otherwise, there would have been mayhem.
Now, let's talk more about the problems encountered, workarounds, and how it worked in general.

* Source : https://betanews.com/2005/10/13/cross-site-scripting-worm-hits-myspace & https://samy.pl/popular/tech.html

Registry Loader

AhnLab

- Fileless Infection
  -

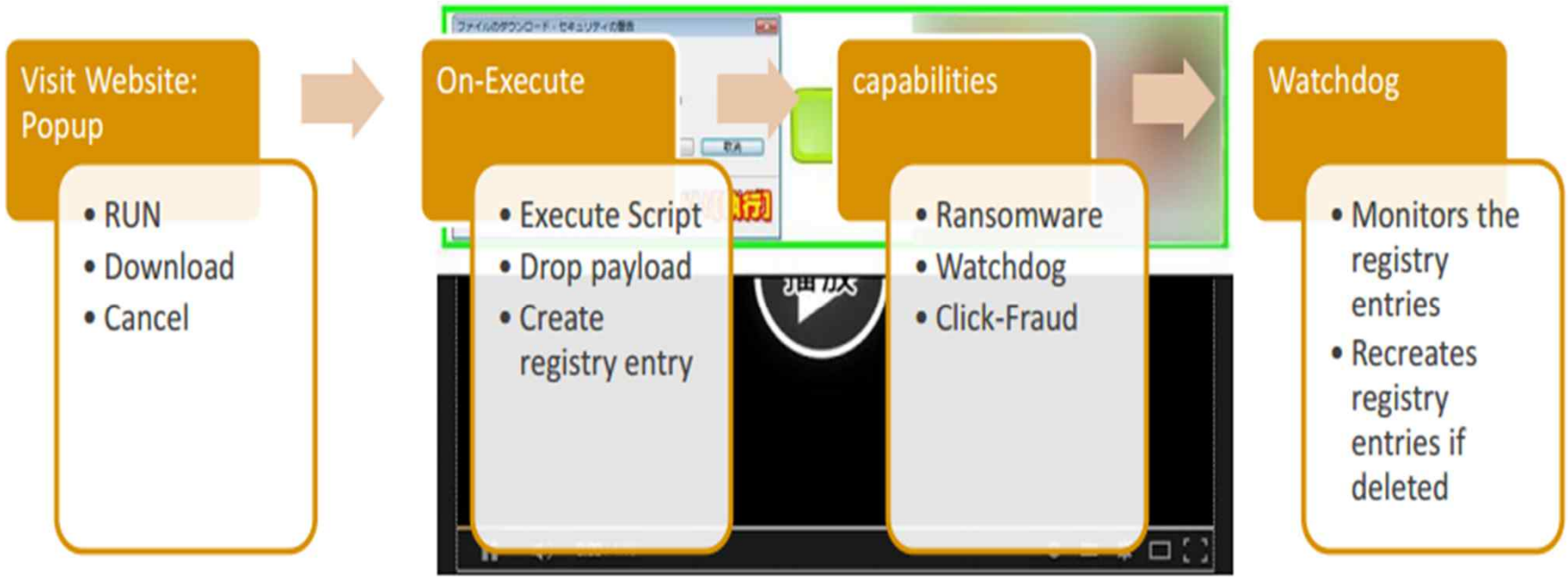


* Source : One-Click-Fileless (2016)(Himanshu Anand & Chastine Menrige)

Registry Loader

AhnLab

- One-click Fileless Infection
  -



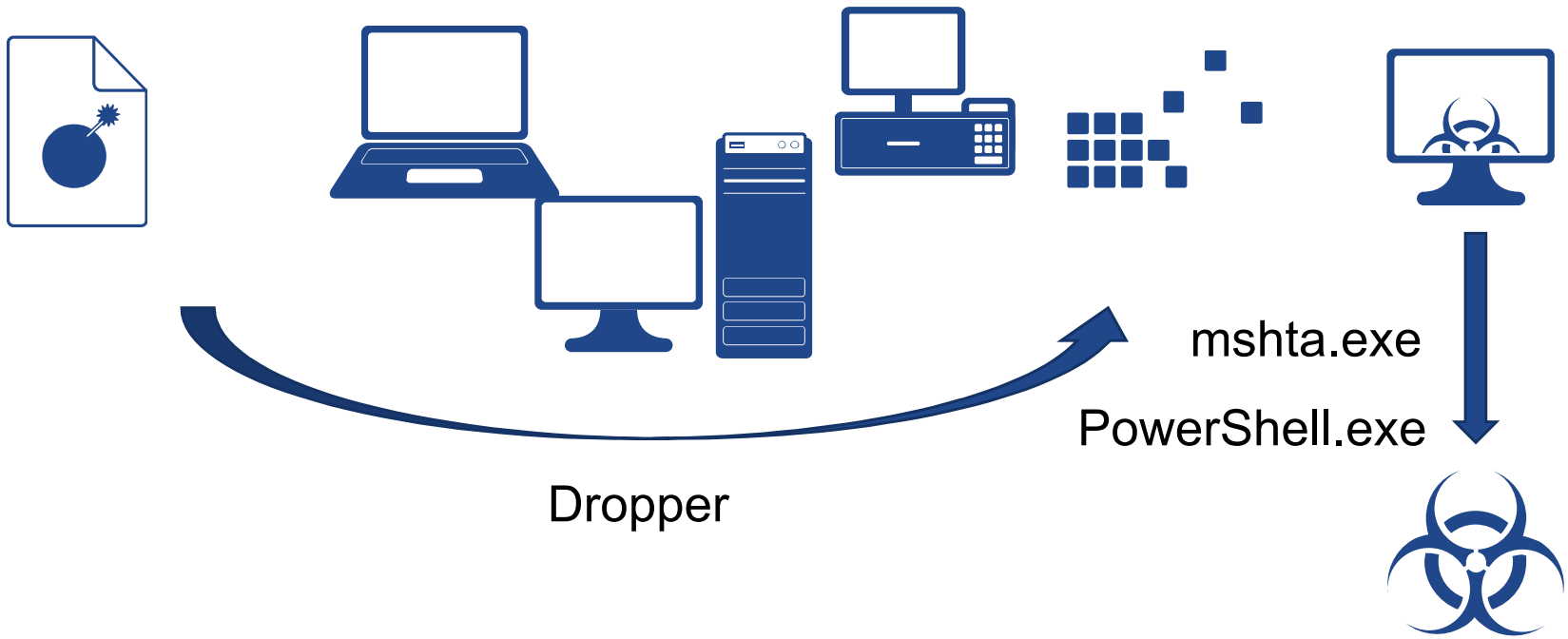
* Source : One-Click-Fileless (2016)(Himanshu Anand & Chastine Menrige)

Registry Loader

AhnLab

- 일반적 Semi-Fileless 기법

  - Dropper -> 보통 Registry 에 악성코드 데이터 저장 -> Script 로 Load



- Fileless Technique으로 이용

  - Poweliks

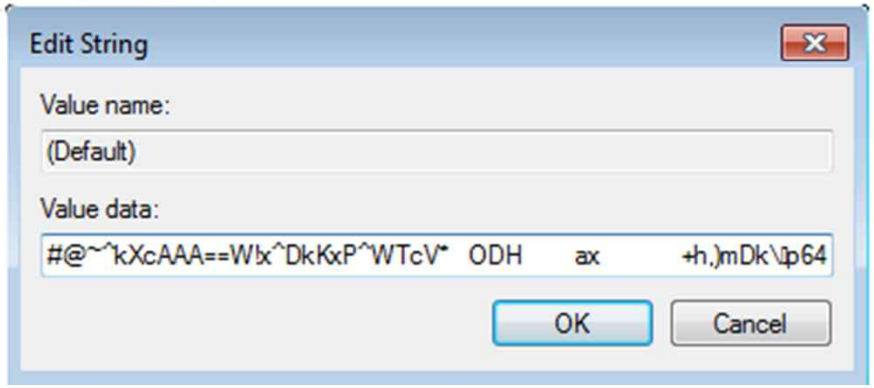
Autostart feature

To start at every boot-up of the system, the malware must create an autostart mechanism. In this case, the malware creates the following registry key:

```
\\HKCU\Software\Microsoft\Windows\CurrentVersion\Run\温
```

Note that the character used for the key's name is not an ASCII character. We will come back to this fact, later. The mentioned entry contains:

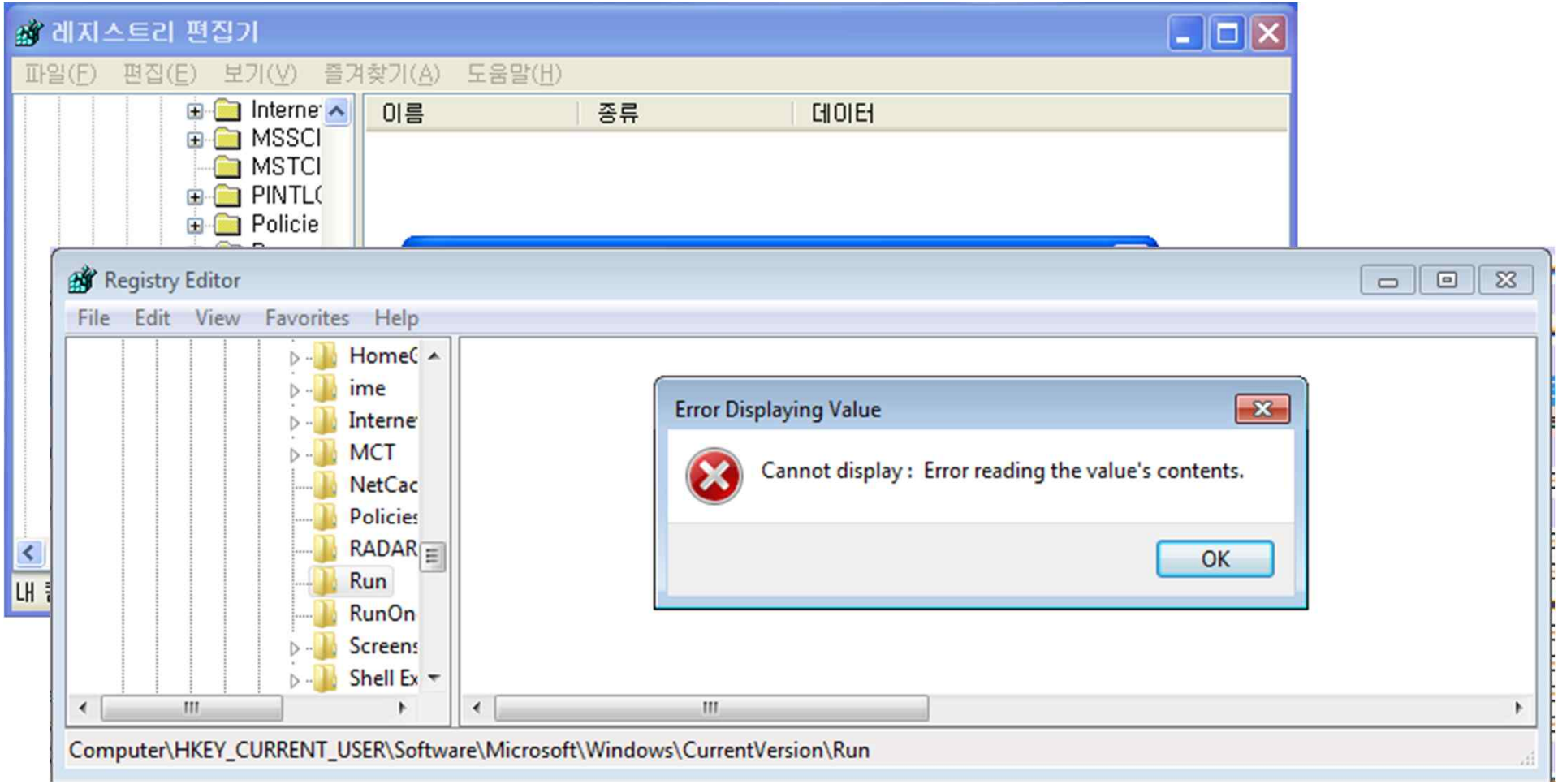
```
rundll32.exe  javascript:"\..\mshtml,RunHTMLApplication";
document.write("<script language=jscript.encode>"+
   (new ActiveXObject("WScript.Shell")).
   RegRead("HKCU\\software\\microsoft\\windows\\currentversion\\run\\")+
   "</script>")
```



* Source : https://blog.gdatasoftware.com/2014/07/23947-poweliks-the-persistent-malware-without-a-file

• Kovter

- Run 항목 읽을 수 없음

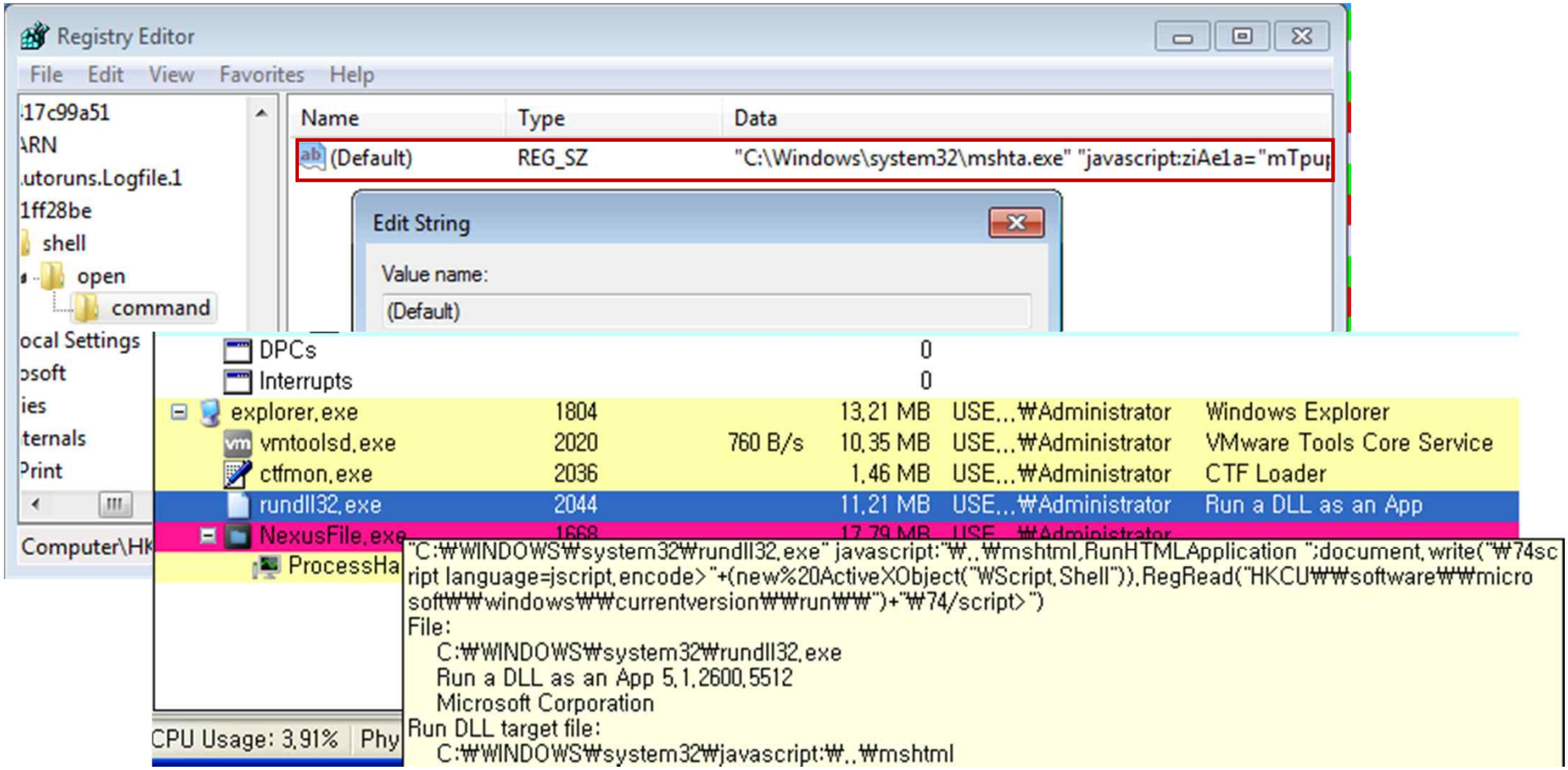


Registry Loader

AhnLab

- Kovter

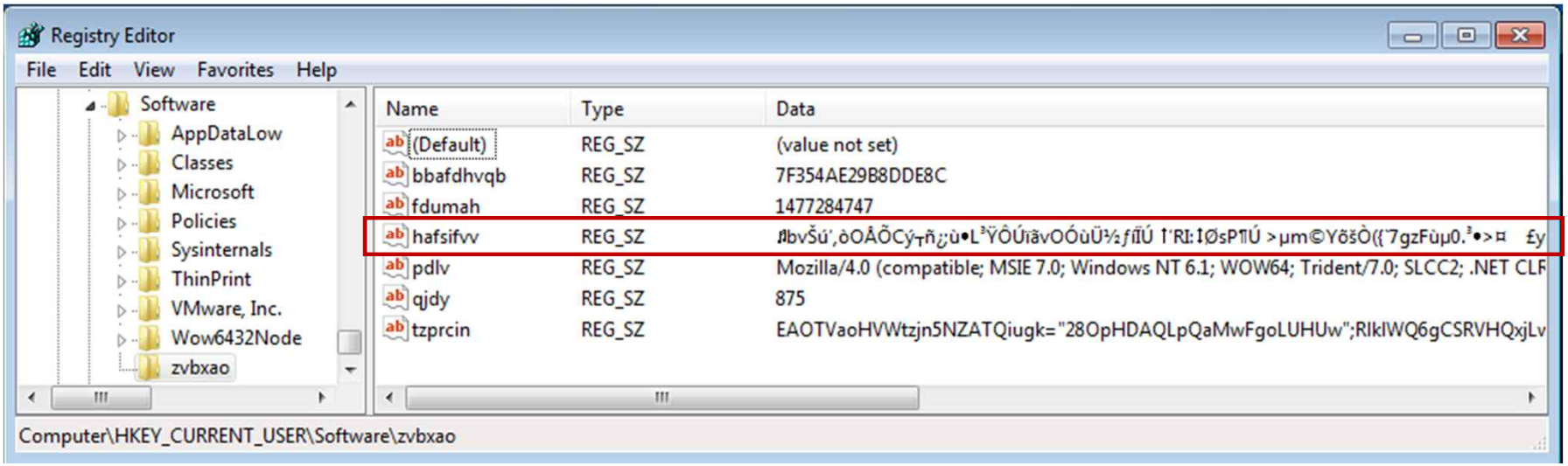
  - mshta.exe를 통해 Script 실행



Registry Loader

AhnLab

- Kovter
  - 인코딩 된 데이터



Registry Loader

AhnLab

- Fileless Technique으로 이용

  - Poweliks

Step 2 (PowerShell script and its purpose)

The PowerShell script contains a variable $p, which contains Base64-encoded shellcode. It uses VirtualProtect() to render the memory executable and CallWindowProcA() to execute the shellcode in $p.

Step 3 (ASM shellcode)

The shellcode realizes several actions:

- It allocates memory, using VirtualAlloc();
- it copies data, including itself (at the offset 0x1104);
- It executes the copied code.

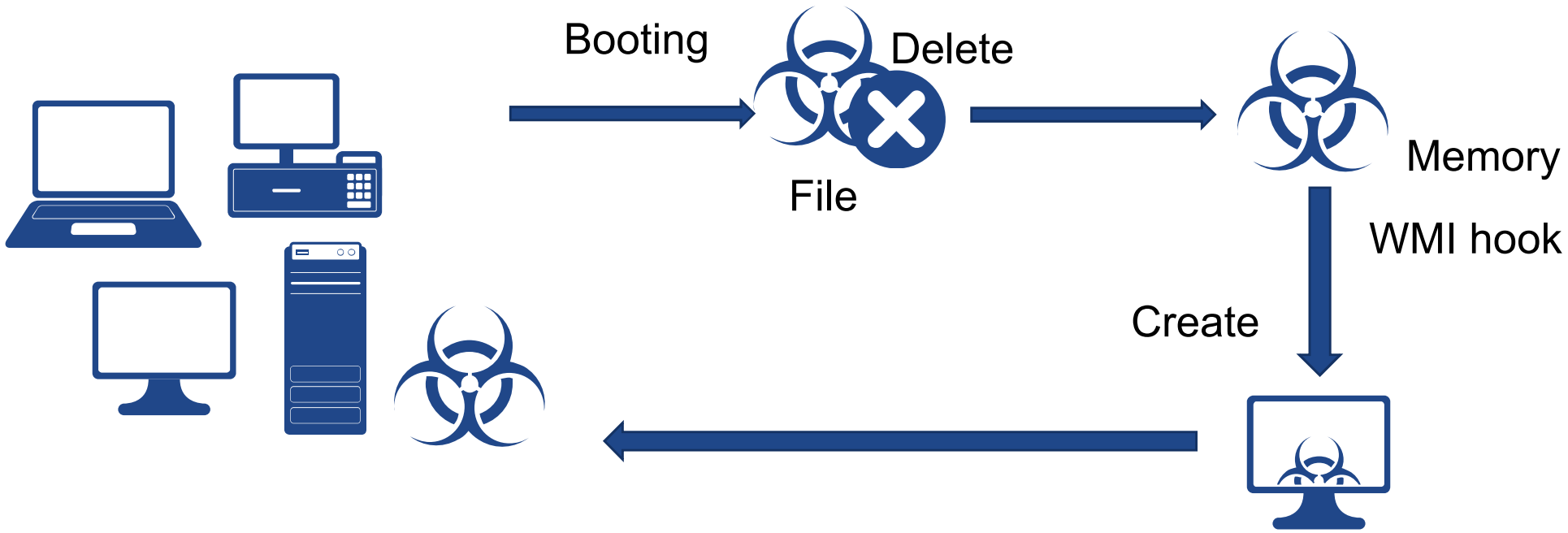
Have a look at the data copied to the offset 0x11

```
00001100  00 00 00 00 4d 5a 40 00  01 00 00 00 02 00 00 00  |....MZ@.........|
00001110  ff ff 00 00 b8 00 00 00  00 00 00 00 0a 00 00 00  |................|
00001120  00 00 00 00 0e 1f ba 0e  00 b4 09 cd 21 b8 01 4c  |............!..L|
00001130  cd 21 57 69 6e 33 32 20  2e 44 4c 4c 2e 0d 0a 24  |.!Win32 .DLL...$|
00001140  40 00 00 00 50 45 00 00  4c 01 02 00 c3 39 37 53  |@...PE..L....97S|
00001150  00 00 00 00 00 00 00 00  e0 00 02 23 0b 01 0a 00  |...........#....|
00001160  00 14 00 00 00 84 32 02  00 00 00 00 5c c2 32 02  |......2.....\.2.|
00001170  00 10 00 00 00 30 00 00  00 00 00 10 00 10 00 00  |.....0..........|
00001180  00 02 00 00 05 00 01 00  00 00 00 00 05 00 01 00  |................|
00001190  00 00 00 00 00 d0 32 02  00 02 00 00 4f 4b 00 00  |......2.....OK..|
000011a0  02 00 00 01 00 00 10 00  00 10 00 00 00 00 10 00  |................|
000011b0  00 10 00 00 00 00 00 00  10 00 00 00 00 00 00 00  |................|
000011c0  00 00 00 00 00 c0 32 02  5c 02 00 00 00 00 00 00  |......2.\.......|
000011d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001210  00 00 00 00 00 00 00 00  00 00 00 00 dc c0 32 02  |..............2.|
00001220  50 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |P...............|
00001230  00 00 00 00 00 00 00 00  00 00 00 00 2e 4d 50 52  |.............MPR|
00001240  45 53 53 31 00 b0 32 02  00 10 00 00 00 22 00 00  |ESS1..2......"..|
00001250  00 02 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00001260  e0 00 00 e0 2e 4d 50 52  45 53 53 32 17 05 00 00  |.....MPRESS2....|
00001270  00 c0 32 02 00 06 00 00  00 24 00 00 00 00 00 00  |..2......$......|
00001280  00 00 00 00 00 00 00 00  e0 00 00 e0 00 00 00 00  |................|
00001290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```

Load and Delete

AhnLab

- Load and Delete
  - 시스템이 꺼져 있을 때는 File 존재
  - 시스템이 켜지면 Load 후 삭제
  - 시스템 종료 때 파일 생성

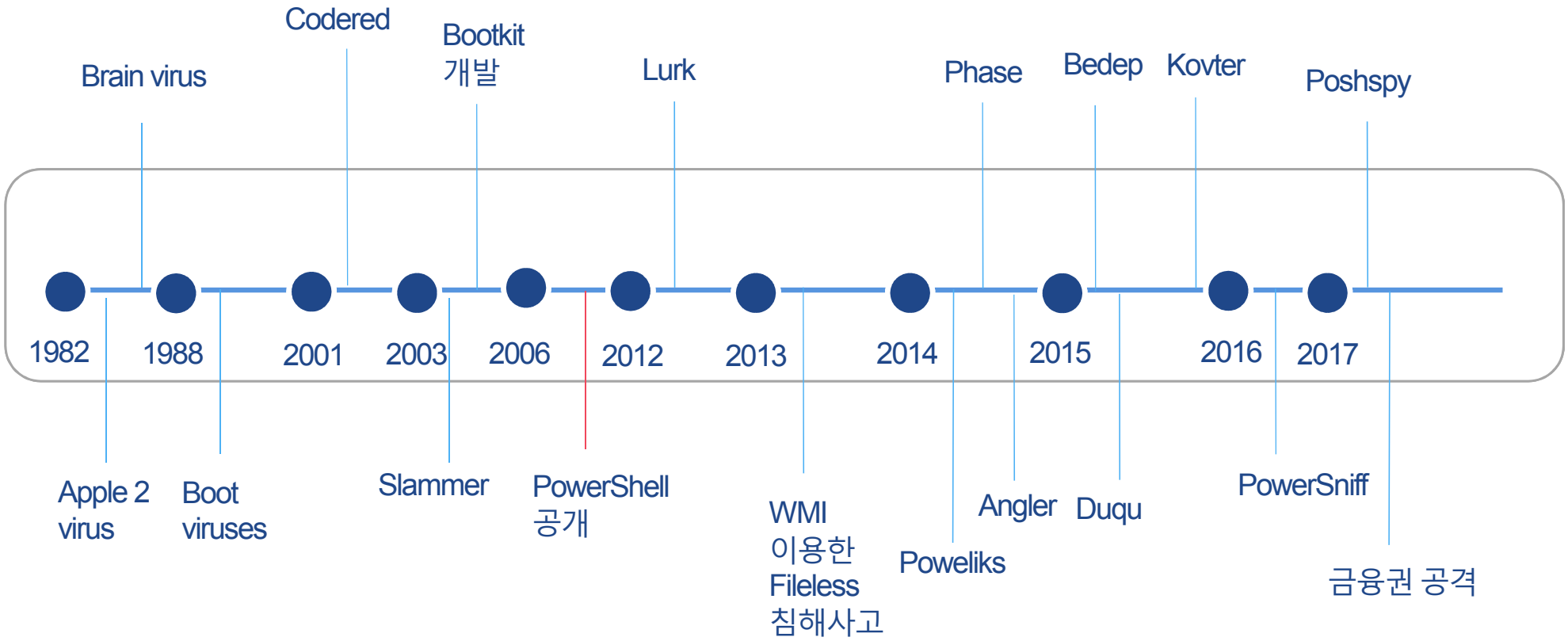


04
주요 악성코드

AhnLab

Timeline

AhnLab



2013 – 게임회사 침해사고

AhnLab

- WMI이용한 Backdoor
  - WMI 설정 변경해 시스템 종료 때 코드 실행 돼 악성코드 감염
  - 부팅 시 악성코드 로드 후 파일 삭제
  - 결과적으로 악성코드가 메모리 상에만 존재

2014 - Poweliks

AhnLab

- Poweliks

  - Registry 내 저장

Home » Malware » POWELIKS: Malware Hides In Windows Registry

POWELIKS: Malware Hides In Windows Registry

Posted on: August 1, 2014 at 4:50 am **Posted in:** Malware **Author:** Roddell Santos (Threats Analyst)

168 61

We spotted a malware that hides all its malicious codes in the Windows Registry. The said tactic provides evasion and stealth mechanisms to the malware, which Trend Micro detects as TROJ_POWELIKS.A. When executed, TROJ_POWELIKS.A downloads files, which can cause further system infection. Systems affected by this malware risk being infected by other malware, thus causing further system infection. In addition, it has the capability to steal system information, which may be used by cybercriminals to launch other attacks.

* Source : http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-malware-hides-in-windows-registry/

2014 - Phase

AhnLab

- Phase

  - 2013년 발견 된 Solarbot 변형

Without a Trace: Fileless Malware Spotted in the Wild

Posted on: April 20, 2015 at 1:03 pm **Posted in:** Malware
Author: Michael Marcos (Threat Response Engineer)

91 131

With additional analysis from David Agni

Improvements in security file scanners are causing malware authors to deviate from the traditional malware installation routine. It's no longer enough for malware to rely on dropping copies of themselves to a location specified in the malware code and using persistence tactics like setting up an autostart feature to ensure that they continue to run. Security file scanners can easily block and detect these threats.

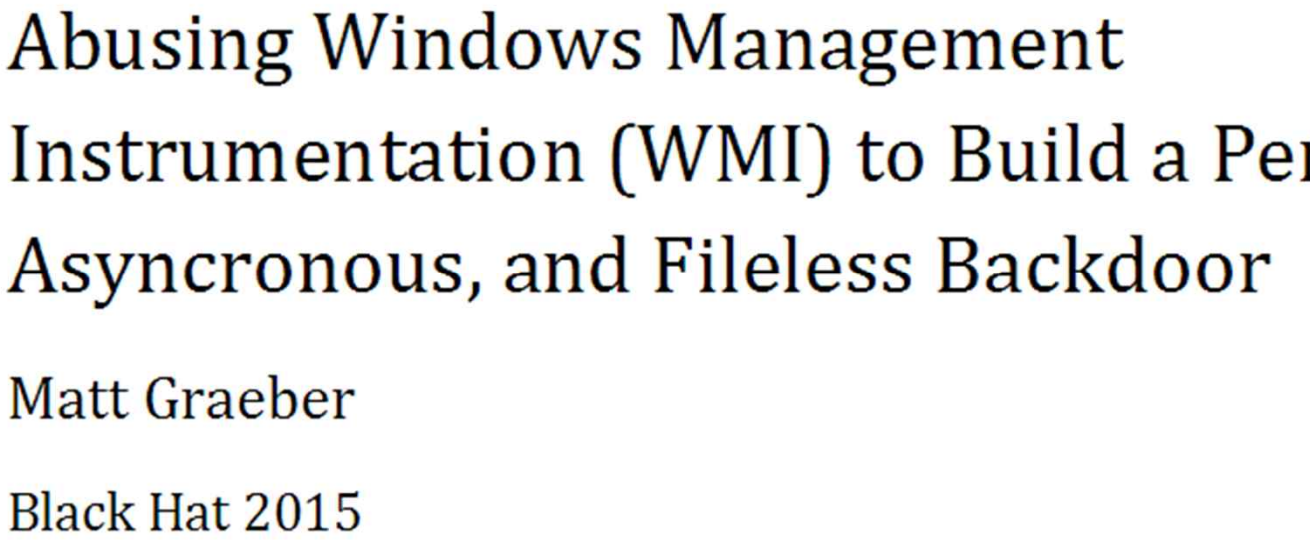
A tactic we have spotted would be using fileless malware. Unlike most malware, fileless malware hides itself in locations that are difficult to scan or detect. Fileless malware exists only in memory and is written directly to RAM instead of being installed in target computer's hard drive. POWELIKS is an example of fileless malware that is able to hide its malicious code in the Windows Registry. These use a conventional malware file to add the entries with its malicious code in the registry.

* Source : http://blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild/

2015 – WMI 악용

AhnLab

- Black Hat 2015
  -

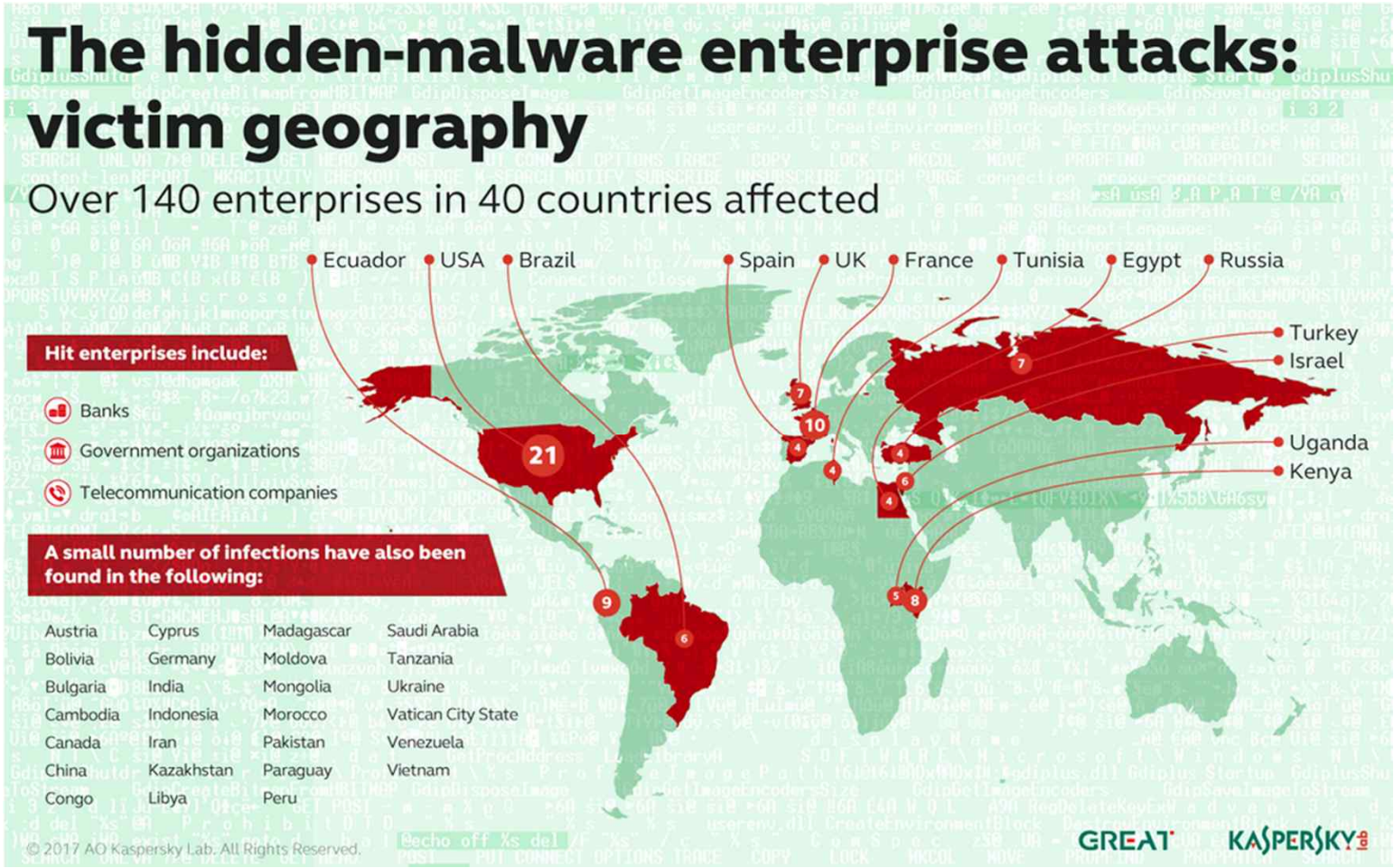


* Source : https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf

2017.2 – Enterprise 노린 공격

AhnLab

- Enterprise 노린 공격
  - 40 개 국 140곳 공격



* Source : https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks/

05
Case Study

AhnLab

06
진단법

AhnLab

가능한 진단법

AhnLab

-

가능한 진단법

- Dropper / 흔적
- 행위
- Network Packet
- Memory 등

07
맺음말 및 전망

AhnLab

Wrap up

AhnLab

- Fileless 악성코드
  - File 로 존재하지 않는 악성코드
  - 사용자 발견이 어려움
  - 보안 프로그램 탐지를 어렵게 할 목적
  - Fileless 악성코드 기준에 대해 논란 중
- Fileless Technique
  - Boot infection (Bootkit 등)
  - Vulnerability (Network worm 등)
  - Windows Registry Loader
  - Load and Delete
- 주요 악성코드
  - Windows Registry Loader 방식이 가장 흔함
- 진단 가능
  - Dropper , 행위, 흔적, Network Packet, Memory 등

Q&A

email : minseok.cha@ahnlab.com / mstoned7@gmail.com
http://xcoolcat7.tistory.com, https://www.facebook.com/xcoolcat7
https://twitter.com/xcoolcat7, https://twitter.com/mstoned7

More security, More freedom

AhnLab

CodeEngn

www.CodeEngn.com

2017 CodeEngn Conference 14