

# Know Your **Cyber** Enemy

---

*sinflection*


*sinflection@gmail.com*



- **ch 1. Know Your Cyber Enemy**
- ch 2. Building a Hunting Infrastructures
- ch 3. Cyber Threat Hunting
- ch 4. Threat Actor Profiling

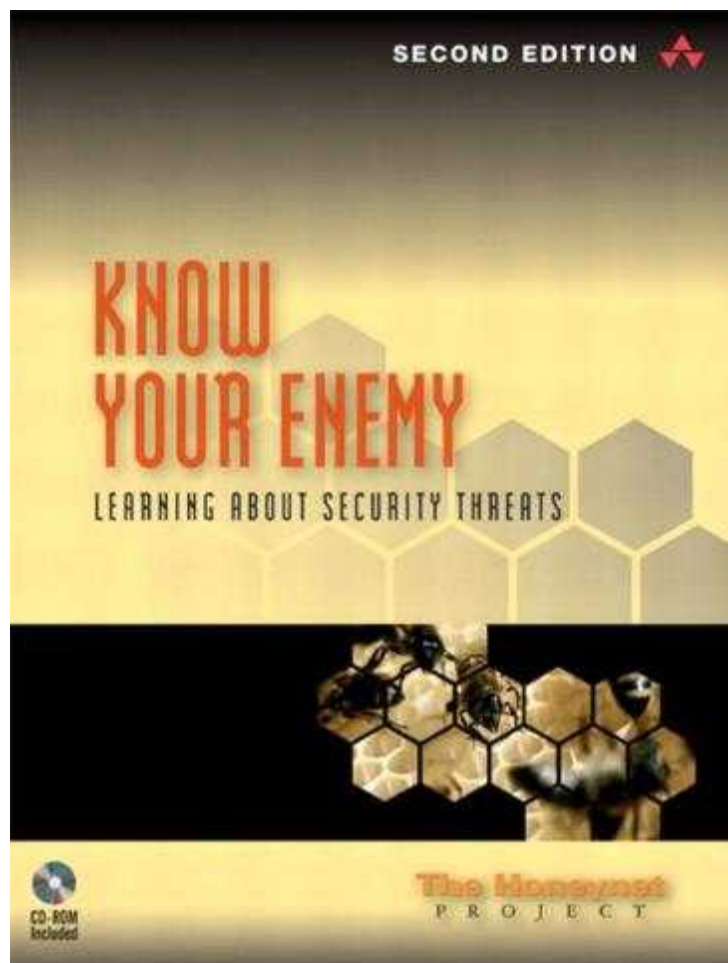
KISA 인터넷보호나라&KrCERT (<https://www.krcert.or.kr>)

- 자료실 - 보고서 - 202. 사이버 위협 동향 보고서(2018년 1분기) - 제 2 장. 전문가 컬럼

- 
- 1. Know Your Enemy ?**
  - 2. Know Your Enemy !**
  - 3. When you Know Your Enemy ?**
  - 4. How we know Cyber Enemy ?**
  - 5. What is Real Enemy ?**
  - 6. Why cybercrime is increasing Day by Day ?**
  - 7. How to Draw Cyber Enemy ?**
  - 8. 3 Easy ways to prevent your company from a cyber attack !**



# 1. Know Your Enemy ?



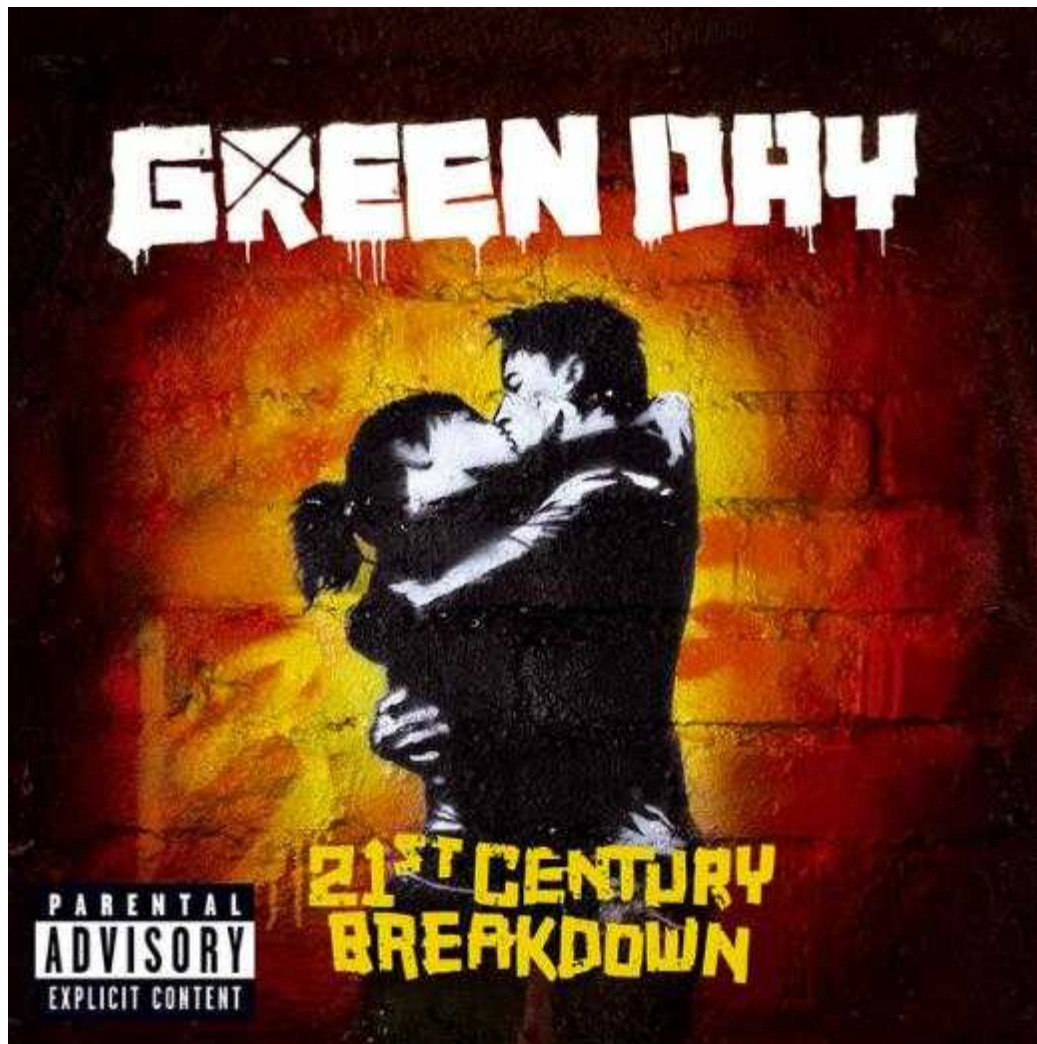
“Know Your Enemy” is the purpose of the HoneyNet Project.

#### Papers

- Know Your Enemy: Containing Conficker
- Know Your Enemy Lite: Proxy Threats - Socks v666
- Know Your Enemy: Malicious Web Servers
- Know Your Enemy: Fast-Flux Service Networks
- Know Your Enemy: Behind the Scenes of Malicious Web Servers
- Know your Enemy: Web Application Threats
- Know Your Enemy: A Forensic Analysis
- Know Your Enemy: Defining Virtual Honeypots
- Know Your Enemy: GenII Honeynets
- Know Your Enemy: Honeynets
- Know Your Enemy: Honeynets In Universities
- Know Your Enemy: Honeywall CDROM
- Know Your Enemy: Learning with User-Mode Linux
- Know Your Enemy: Passive Fingerprinting
- Know your Enemy: Phishing
- Know Your Enemy: Sebek
- Know Your Enemy: Statistics
- Know Your Enemy: The Social Dynamics of Hacking
- Know your Enemy: Tracking Botnets
- Know Your Enemy: Trends
- Know Your Enemy: Worms at War
- Know Your Tools: Glastopf - A dynamic, low-interaction web application honeypot
- Know Your Tools: Qebek - Conceal the Monitoring
- Know Your Tools: use Picviz to find attacks
- Know Your Enemy: Automated Credit Card Fraud
- Know Your Enemy: Motives

<http://www.honeynet.org/book/>

By HoneyNet Project, The Published May 17, 2004 by Addison-Wesley Professional.



Silence is an enemy

Against your urgency

So rally up  
the demons of your soul

Singles from 21st Century Breakdown "Know Your Enemy"

Released: April 16, 2009



I know my enemies!  
They're the teachers who  
taught me to fight me!

Compromise! conformity!  
assimilation! submission!  
(타협! 순응! 동화! 굴복!)

Ignorance! hypocrisy!  
brutality! the elite!  
(무지! 위선! 잔인함! 엘리트 계층!)

All of which are "American  
dreams"!

"Know Your Enemy " Song by RATM from the album Rage Against the Machine

November 3, 1992



SUN - TZU

# THE ART OF WAR

Realidad B



기원전 496년, 춘추시대 말기 손자가 10년동안 은둔하며 지음





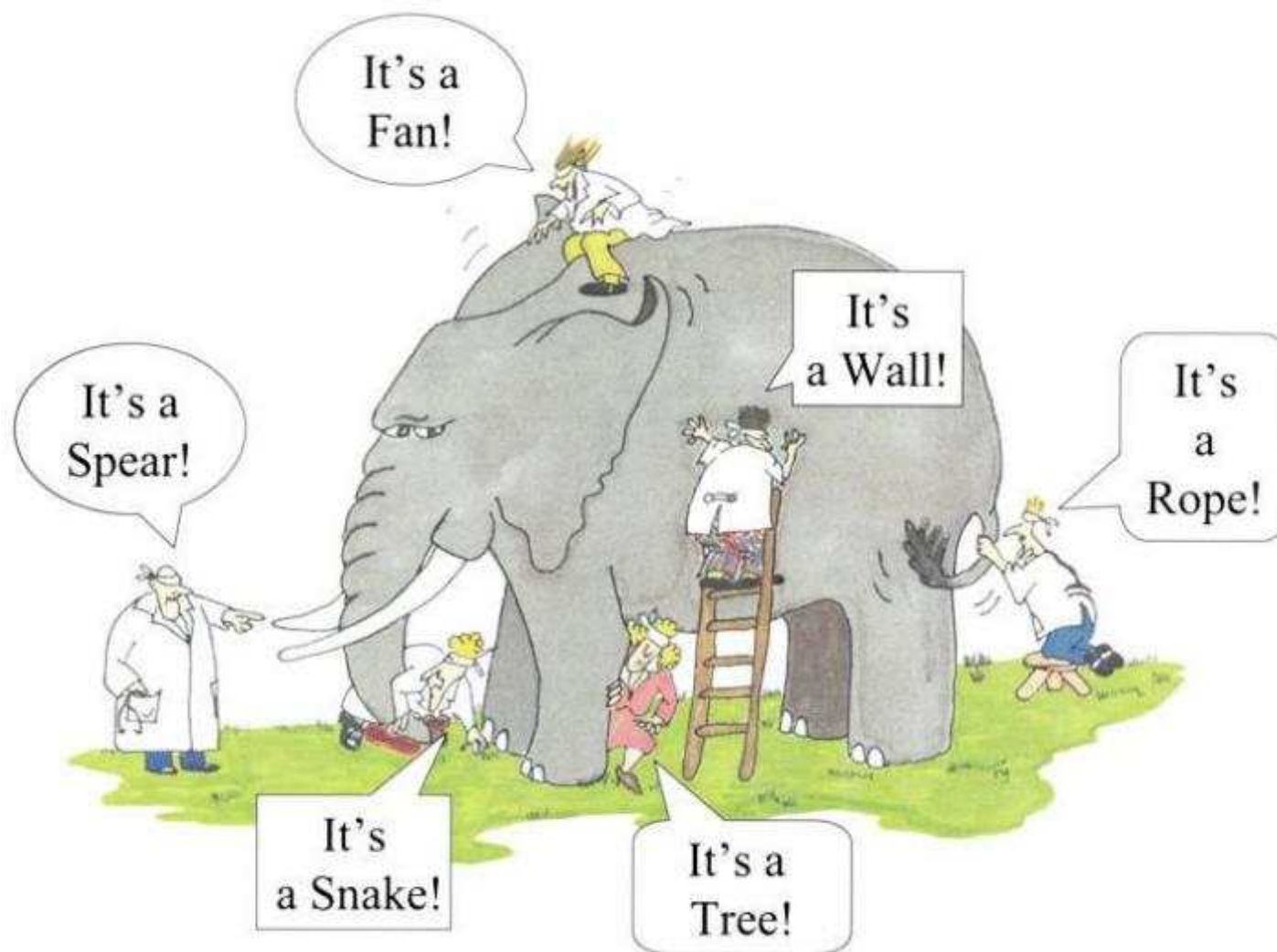
## 2. Know Your Enemy !!!





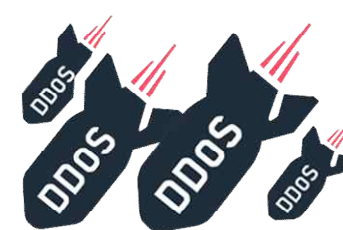
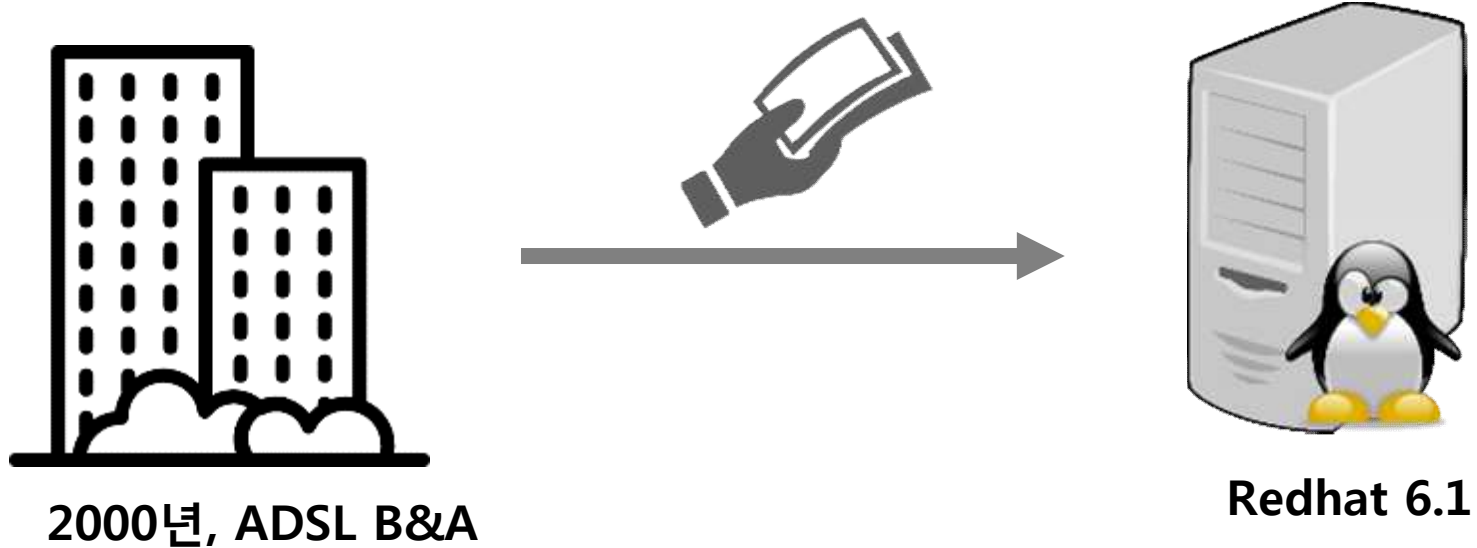








### 3. When you Know Your Cyber Enemy?



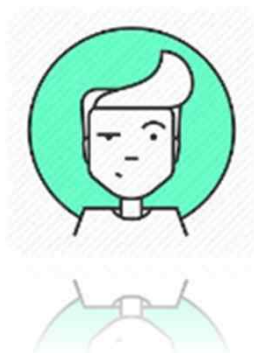








1) Distrust



2) Curiosity



3) Anger





## 4. How we know cyber Enemy ?





MBC뉴스

## 금융정보보안업체 코드서명 해킹 사건, 검찰 "북한 해킹조직..

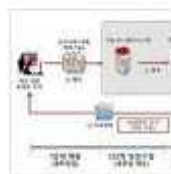
한국일보 - 2016. 5. 31.

검찰이 국내 금융정보 보안업체를 해킹해 악성 프로그램을 공공기관에 유입한 사건이 북한 해킹조직의 소행으로 추정된다고 결론 내렸다. 개인정보범죄 정부합동수...

## 검찰 "보안업체 전자인증서 해

심증 뉴스 - MBC뉴스 - 2016.

관련 기사 보기 (기사 38개 더보기)



## SK·한진 등 대기업 北해킹에 뚫렸다...F-15 무인정찰기 정보 유출

조선일보 - 2016. 6. 12.

북한이 국내 대기업 전산망을 해킹해 군(軍) 관련 정보 등 최소 4만여 건의 문서와 전산망 통제권을 탈취한 것으로 경찰 조사결과 밝혀졌다. 북한은 2013년 '3·20 방송·금융 전산망 사이버테러' 이후 최대 규모의 전산망 마비 공격을 준비해 온 사실도 드러났다.



## 북한, 대규모 사이버 공격 준비 확인...대기업 문서 4만여건 해킹(종합)

연합뉴스 - 2016. 6. 12.

SK네트웍스서비스 등 피해 업체에서 자체 대응팀을 가동하고 경찰 수사에 적극 협조, 관리망의 결함을 신속히 밝혀낸 덕분에 보안 패치작업이 빠르게 이뤄져 추가 피해를 막았다고 경찰은 전했다. 북한이 이번 해킹 이후 실제 사이버 공격을 감행했다면 규모는...



## "'워너크라이' 배후는 북한"...미 정부, 첫 공식 인정(종합) 연합뉴스 | 2017.12.19.

네이버뉴스 |

보서트 국토안보보좌관 "어떤 공격이든 최대 압박 전략 구사하겠다" 미국 정부가 올해 초 전 세계 병원과 은행, 기업의 네트워크를 마비시킨 '워너크라이'(WannaCry) 사이버 공격의 배후로 북한을 공식 지목했다. 토머스...

美 정부, 전 세계 강타한 '워너크라이'... 공감신문 | 2017.12.19.

"전세계 컴퓨터 감염시킨 '워너크라이'... 한국경제 | 2017.12.19. 네이버뉴스

美 정부, '워너크라이' 공격 배후로... 연합뉴스 | 2017.12.19. 네이버뉴스

'워너크라이' 북한 소행' 발표에 가려... 프레시안 | 2017.12.19. 네이버뉴스

관련뉴스 22건 전체보기 >



[개인정보 노린 악성코드 기승... "1주새 PC 2만5천대 감염"](#) 연합뉴스 | 2017.08.18,  
네이버뉴스 | [🔗](#)

경유지 악용 웹사이트 400개 이상...접속만 해도 위협 개인정보를 노리는 **파밍 악성코드**가 무차별 유포되고 있어 이용자의 주의가 요구된다. 18일 보안업계에 따르면 지난 12~13일 국내에서 **파밍 악성코드**가...

- ↳ [주간 악성링크] '록키' 랜섬웨어부... 보안뉴스 | 2017.08.18,
  - ↳ 개인 정보 빼돌리는 '파밍 악성코드'... 공감신문 | 2017.08.18,
  - ↳ **파밍 악성코드**로 PC 2만5000대 감... 국제신문 | 2017.08.18,
  - ↳ '접속만 해도 감염' 개인정보 노린 악... 서울경제 | 2017.08.18, | 네이버뉴스
- [관련뉴스 6건 전체보기 >](#)

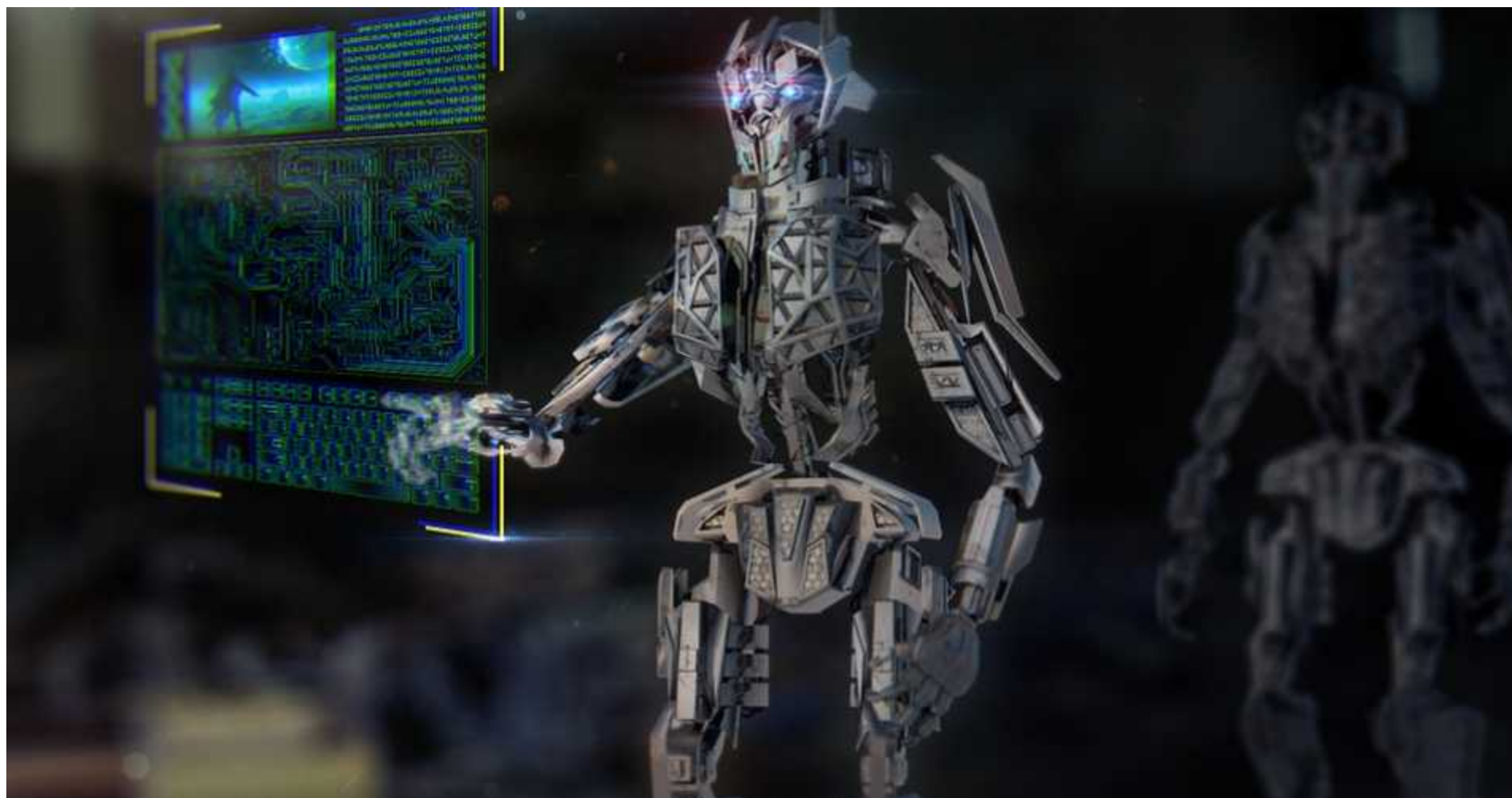


["가상화폐거래소, 해킹·개인정보유출 사고 무방비"](#) 뉴데일리 | 2018.01.24, | [🔗](#)

[뉴데일리-김동식 기자] 최근 뜨거운 감자로 떠오르고 있는 가상화폐거래소가 **해킹** 및 개인정보유출 사고에 무방비로 노출돼 있는 것으로 드러났다. 국회 과학기술정보방송통신위원회 더불어민주당 변재일 의원(청주 서원구)...

- ↳ 가상화폐거래소, 해킹·개인정보유출... 중부매일 | 2018.01.24,
- ↳ 변재일 "가상화폐거래소 보안 취약, ... 동양일보 | 2018.01.24,
- ↳ 가상화폐거래소, 보안 취약...해킹 개... EBN | 2018.01.24,
- ↳ 가상화폐거래소 해킹·개인정보유출... 여성소비자신문 | 2018.01.24,

[관련뉴스 31건 전체보기 >](#)





## 5. What is Real enemy?





- **2017 Major Cyber Incidents**

Case	Threat Actor	Target	Method	Purpose
WannaCry (May 12)	North Korea	Indiscriminate (like worm)	Existing Vulnerabilities	Disruptive
Erebus (Jun 10)	Chinese-speaking actors	Targeted	Server Hacking	Money
Nyetya (NotPetya) (Jun 27)	Russia	Targeted	Supply chain attack (M.E.Doc)	Destructive
Netsarang Xshell (Aug 15)	Chinese hacking group ( PlugX and Winnti)	Targeted	Server Hacking	Steal data? Foothold
Ccleaner (Sep 18)				



- Wannacry : SMB 취약점을 랜섬웨어와 결합한 원격 전파형 악성코드







- NotPetya: 우크라이나 타겟 랜섬웨어 (and PlugX)





## 6. Why cybercrime is increasing Day by Day?





## How Many Websites Are Active?

The size of the Internet can be measured in various ways, including totals such as: How many websites are there? How many domains are registered? How many websites are being used? What are the most popular web sites? How much storage is required to hold all the web data? How much data is transmitted? Etc., etc. The trouble is the Internet is so big that these totals and numbers change all the time. For this brief look at the size of the Internet the total number of websites is examined. In other words you can type a unique domain name into your browser's address bar and you will get a response.

So let us look at the size of the Internet according to the [Netcraft January 2017 Web Server Survey](#). How many websites are there? There are **1,800,047,111** (over 1.8 billion web sites). This is a rise on the number of websites compared to last year.

### A Yearly Table of the Number of Websites in the World

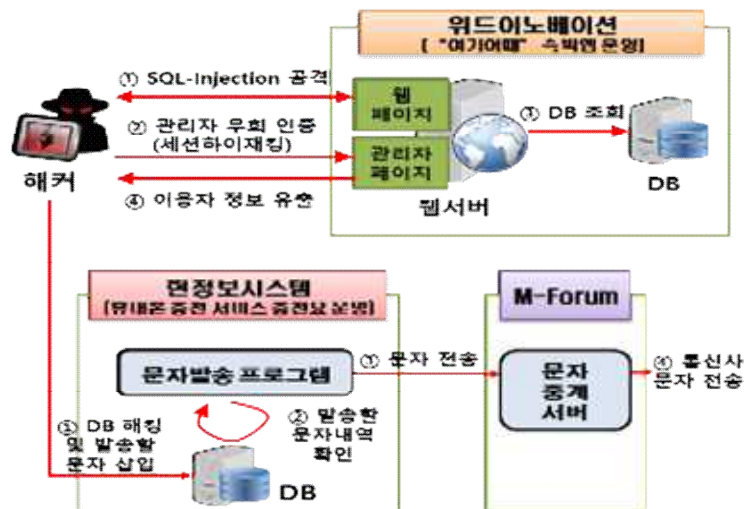
Month and Year	Number of Websites
January 2017	1,800,047,111
January 2016	906,616,188
January 2015	876,812,666
January 2014	861,379,152

## 신규 서비스 사이버 공격 및 피해 사례

### ■ ‘여기어때’이용고객 개인정보 유출(‘17.3)

- 유출규모 : 990,584건 개인정보 유출 (숙박 예약 정보, 제휴점 정보, 회원정보)
- 유출경위 : DB내 정보탈취 공격으로 관리자 인증정보 탈취 → 서비스 관리 서버에 접속 후,

개인정보 탈취 → 문자발송업체를 이용한 불법문자 발송 (4,457건, 3.21~23) 및 피해 유발



### ■ 야피존(‘17.4)

- 피해규모 : 55억 규모의 가상화폐 해킹

### ■ 빗썸(‘17.6)

- 이용자 3만6000여명의 개인정보가 유출

### ■ 코인이즈(‘17.7)

- 피해규모 : 21억원

### ■ 유빗(구야피존)(‘17.12)

- 피해규모 : 172억원

### ■ 코인레일(‘18.6)

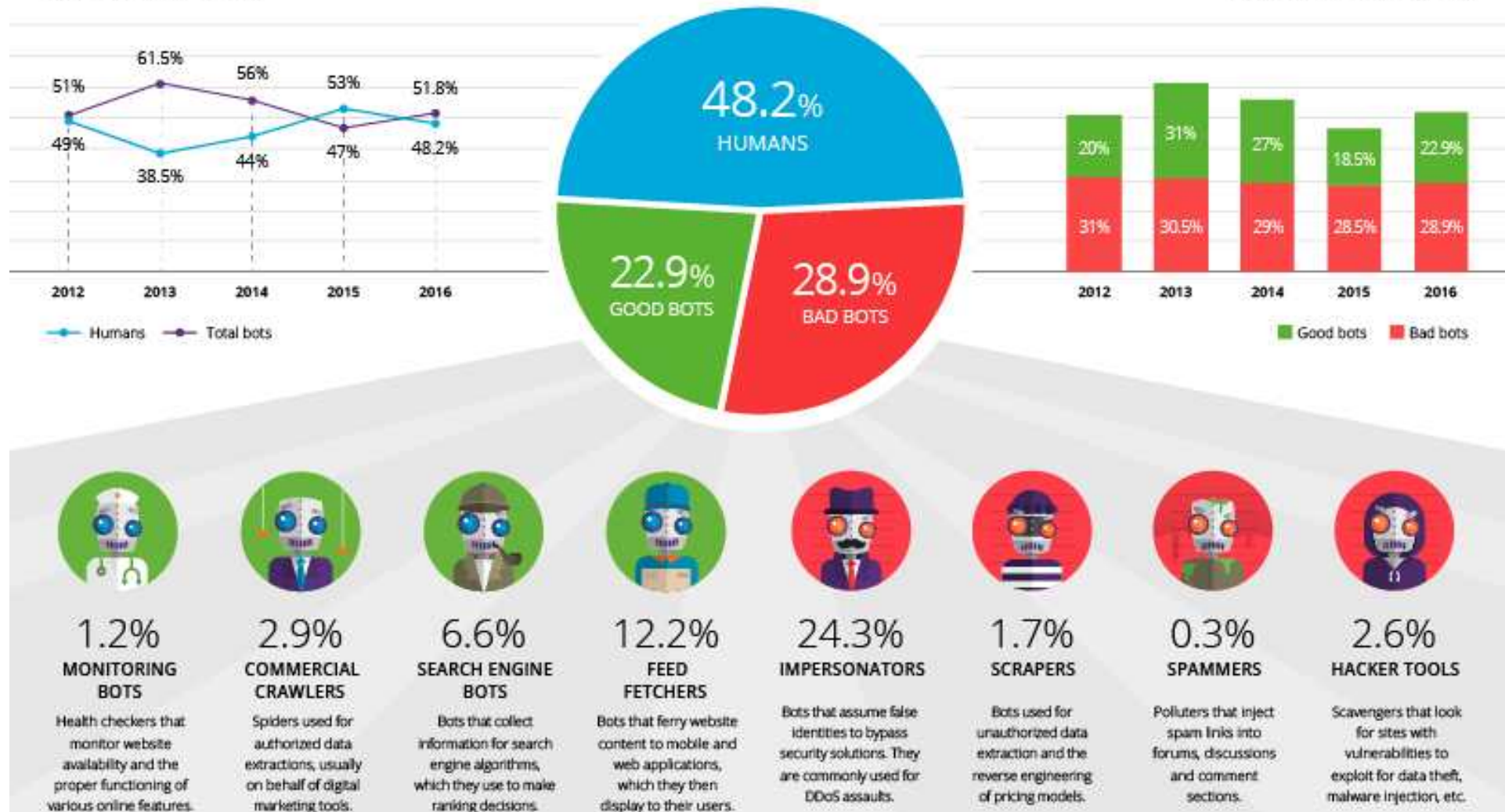
- 피해규모 : 535억원

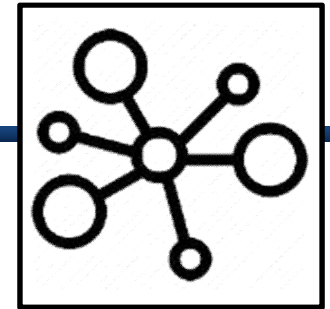
# BOT TRAFFIC REPORT 2016

BOTS ONCE AGAIN COMPRISE THE MAJORITY OF ONLINE TRAFFIC AMID AN INCREASE IN GOOD BOT ACTIVITY.

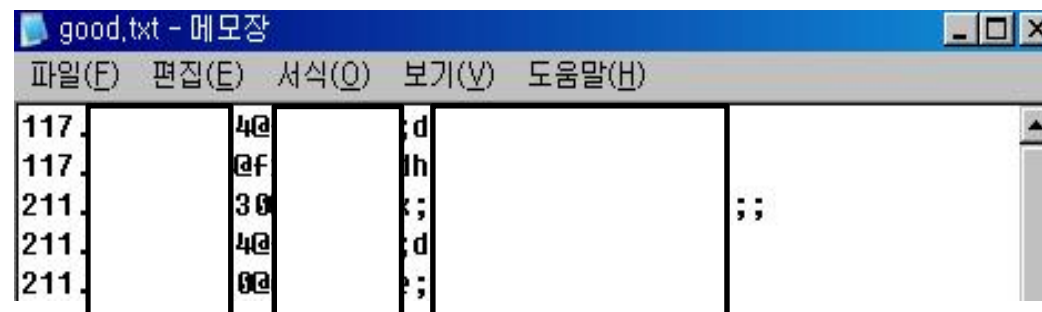
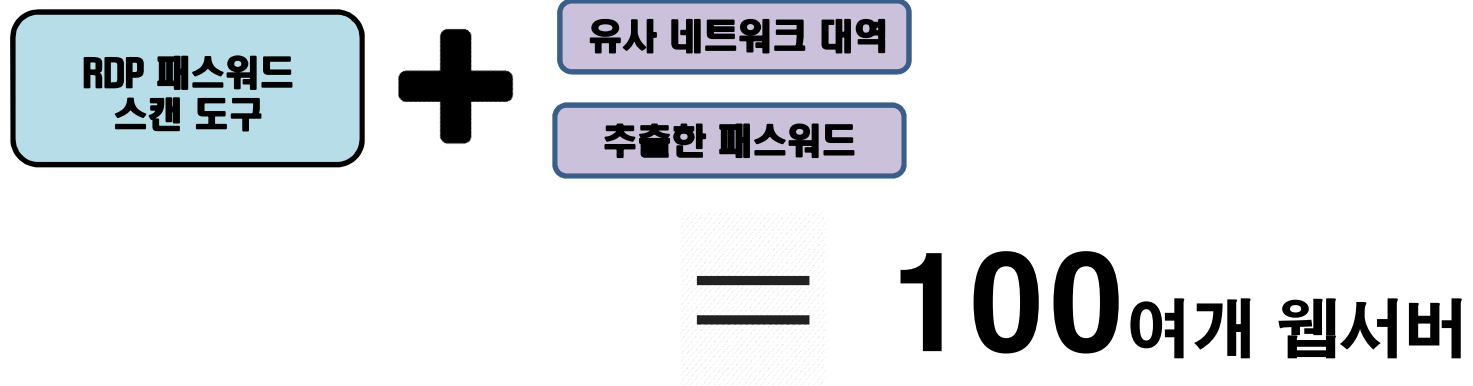
BOT ACTIVITY IS IN AN UPTREND, after a three year decline.

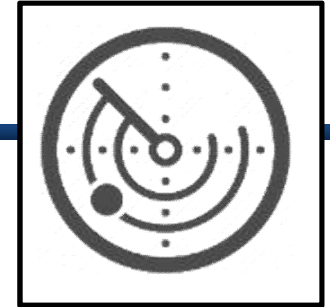
INCREASE IN GOOD BOT ACTIVITY, which went up by 4.4 percent.



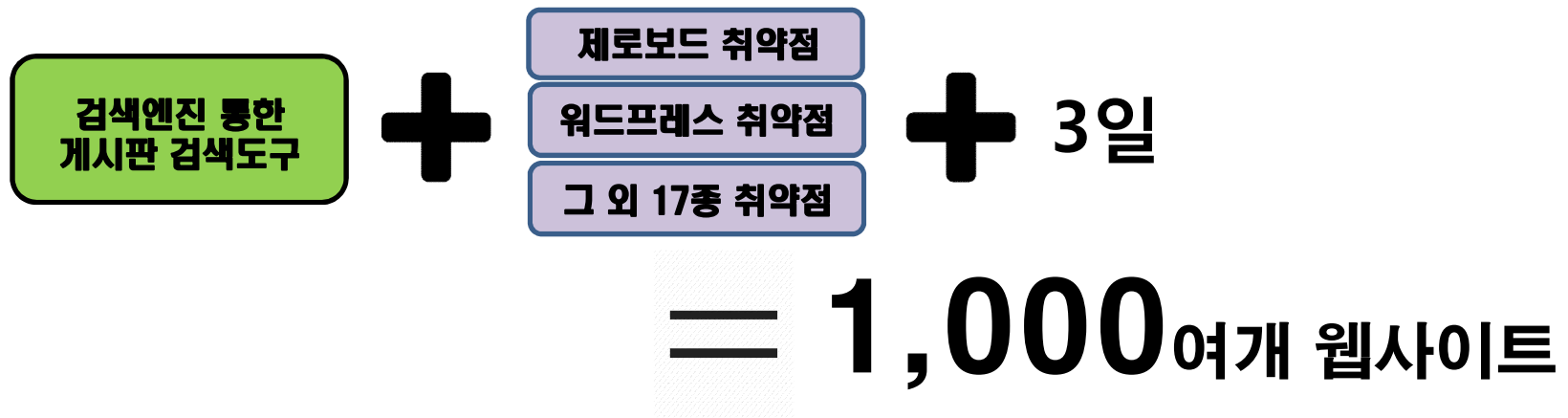


## 내부 동일 취약점을 통한 내부 전파 사례





## 취약한 웹사이트 스캔 및 해킹 사례



```
http://www. co.kr///userfiles/file//1.asp/\\20150302183727.jpg  
http:// tech.com///files/upload/file//1.asp///20150302183728.jpg  
http://hs co.kr///UploadFiles/UserFiles/File//20150302183735.asp  
http://www. .or.kr///kirsfFiles/File//20150302184215.asp  
http://www. housing.com///board/data/ FCKeditor/file//20150302185220.asp
```

※ 파일명 규칙 : [년월일시분초].[asp, jpg, asp;(1).jpg]





## xDedic 사이버 블랙마켓, 70,624개 서버 판매 중(Kaspersky, '16.6.15)





## 워너크라이, 150개국 30만여대 랜섬웨어 감염('17. 5.12~)

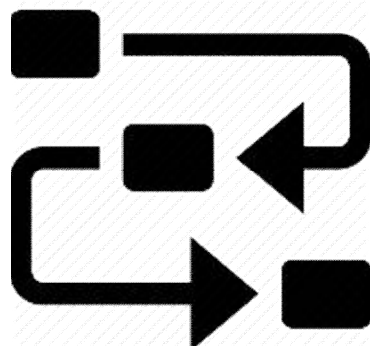
- NSA Eternal blue, SMB remote vul, CVE MS17-010



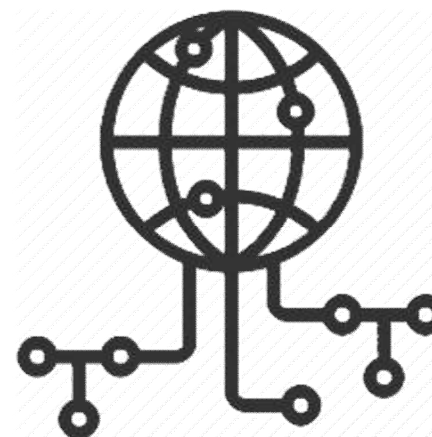




↻ **AS-IS** ↻



**TO-BE**



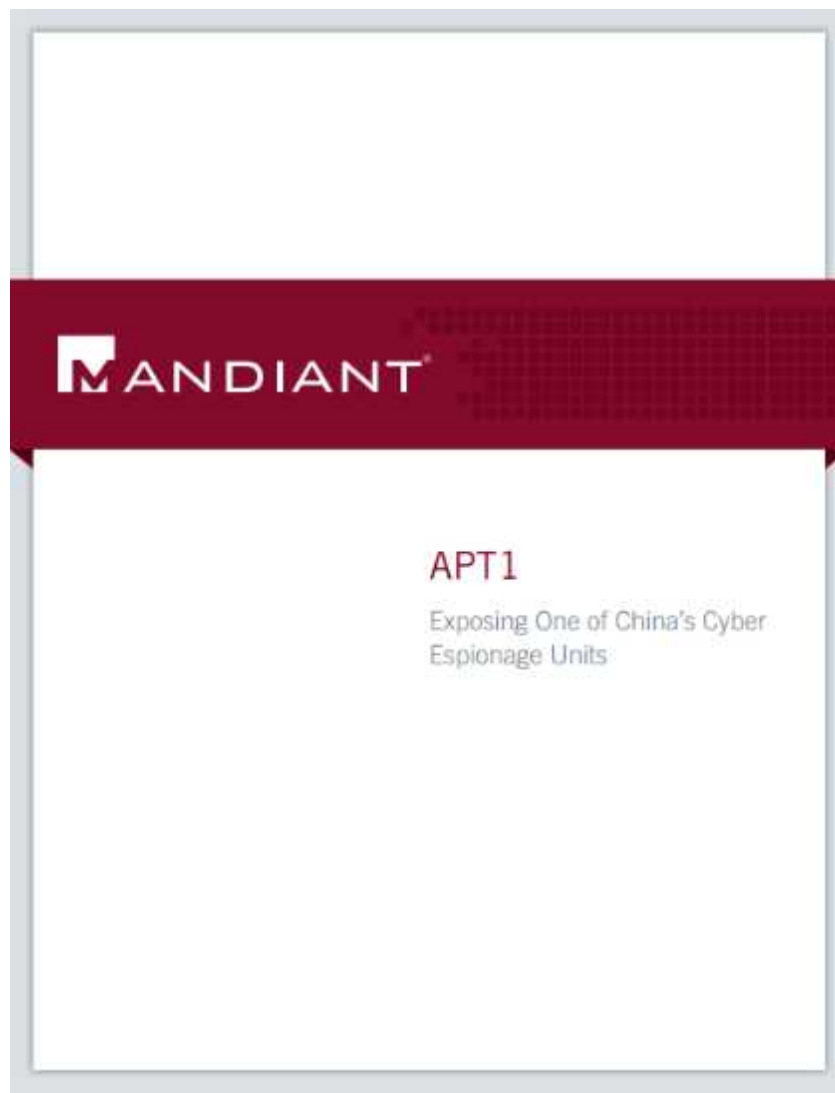


## 7. How to Draw Cyber Enemy ?



## A Type Report

2013.2





## C Type Report

2014.10

NOVETTA 

### Operation SMN:

Axiom Threat Actor Group Report  
公理队

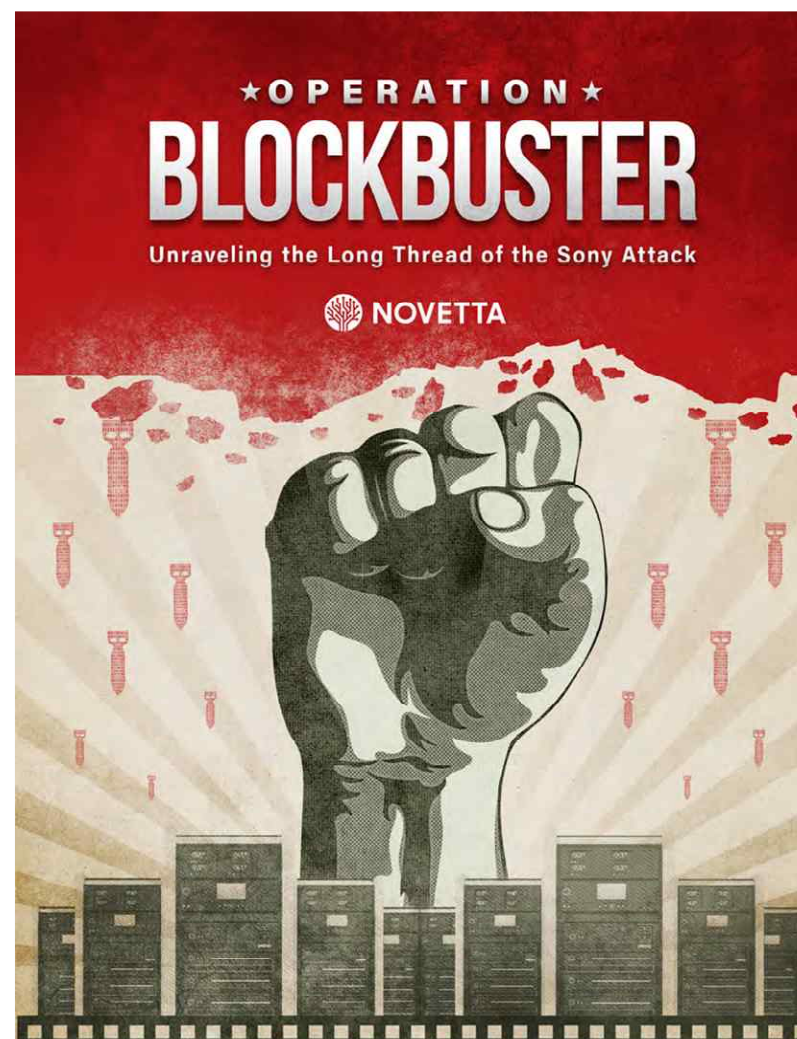
Thank you to our public partners:

Bit9+CARBON BLACK ARM YOUR ENDPOINTS. CISCO F-Secure FireEye

iSIGHTPARTNERS tenable THREATCONNECT

ThreatTrack SECURITY VOLEXITY

2016.2





## Contents

Key Findings – pg. 4
Operation SMN Background – pg. 5
Operational Impact – pg. 6
Axiom Targeting – pg. 8
Targeting and China's Strategic Goals – pg. 10
Semiconductor and Networking Technology – pg. 10
Human Intelligence – pg. 11
Non-Governmental Organizations – pg. 11
Previous Public Reporting – pg. 12
Domestic Targeting – pg. 15
Tactics, Techniques, and Procedures of Axiom – pg. 18
Structure of Adversary – pg. 20
Command and Control (C2) Infrastructure – pg. 21
Hikit Command and Control (C2) Configuration – pg. 22
Remediation – pg. 23
Kudos – pg. 26
Appendix A: Malware Key Findings – pg. 27
Hikit Generation 1 – pg. 27
Hikit Generation 2 – pg. 28
Zox Family – pg. 28
Derusbi (Server Variant) – pg. 29
Appendix C: Signatures – pg. 30
Yara Signature Links – pg. 30
IDS signatures – pg. 30
Appendix D: Malware Names Index – pg. 30
Appendix E: Malware Hashes – pg. 31

## CONTENTS

Executive Summary .....	2
China's Computer Network Operations Tasking to PLA Unit 61398 (61398部队) .....	7
APT1: Years of Espionage .....	20
APT1: Attack Lifecycle .....	27
APT1: Infrastructure .....	39
APT1: Identities .....	51
Conclusion .....	59
Appendix A: How Does Mandiant Distinguish Threat Groups? .....	61
Appendix B: APT and the Attack Lifecycle .....	63
Appendix C (Digital): The Malware Arsenal .....	66
Appendix D (Digital): FQDNs .....	67
Appendix E (Digital): MD5 Hashes .....	68
Appendix F (Digital): SSL Certificates .....	69
Appendix G (Digital): IOCs .....	70
Appendix H (Digital): Video .....	74

Mandiant APT1

www.mandiant.com

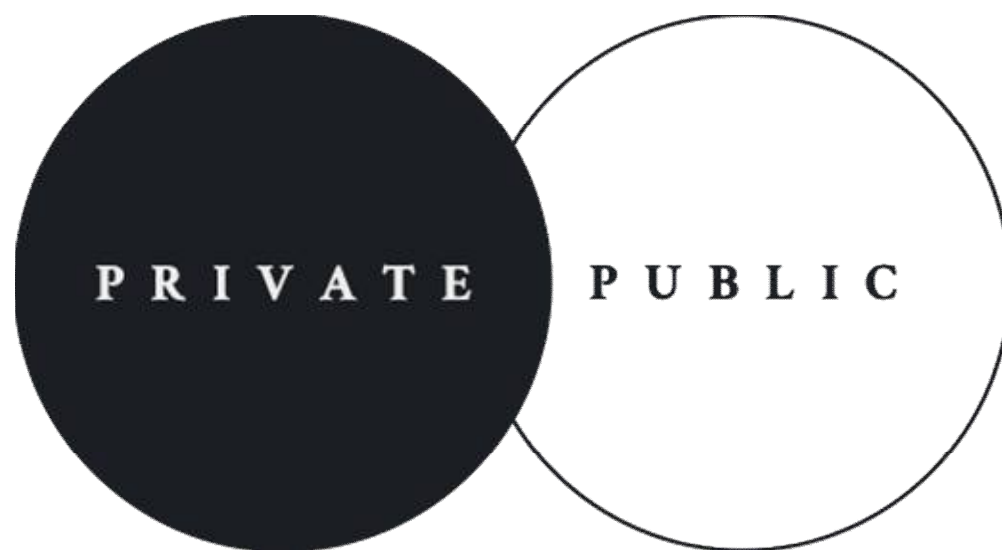
## TABLE OF CONTENTS

Executive Summary .....	4
1. Executive Summary .....	5
1.1 Key Takeaways .....	7
2. Operation Details .....	8
2.1 Hunting Method .....	9
3. Lazarus Group Details .....	11
3.1 The SFE Attack and Conflicting Attribution .....	12
3.2 Tactics, Techniques, and Procedures (TTPs) .....	14
3.3 Targeting .....	16
3.4 Links to Previous Reporting .....	20
The Lazarus Group Timeline .....	20
4. Malware Tooling .....	24
4.1 Naming Scheme .....	25
4.2 Infrastructure .....	27
4.3 Code Relationships .....	28
4.3.1 Encryption .....	28
4.3.2 Dynamic API Loading .....	34
4.3.3 Network Functionality .....	35
4.3.4 Directory Hierarchy Verification and Generation .....	46
4.3.5 Secure File Delete .....	47
4.3.6 Target File Identification .....	47
5. Conclusion .....	48
YARA Rules .....	50
Hashes .....	50
6. Appendix .....	51
7. Glossary of Terms .....	55









Malware VS Incident



## 8. 3 Easy ways to prevent your company from a cyber attack

## If you don't wanna cry?

- 1) Hunting Infra    2) Hunting&Profiling    3) Cooperative Net



KISA 인터넷보호나라&KrcERT (<https://www.krcert.or.kr>)

- 자료실 - 보고서 - 202. 사이버 위협 동향 보고서(2018년 1분기) - 제 2 장. 전문가 컬럼



