



사이버 위협 정보공유를 위한 국내외 노력

위협정보공유센터 김정희

September , 2018



We Will be a Global Leader in the Internet & Security Field

01 사이버 위협 (Cyber Threats)

02 사이버 위협 정보공유 (Cyber Threat Information Sharing)

03 사이버위협정보분석·공유(C-TAS) 시스템



사이버 위협(Cyber Threats)

1 사이버 위협 (Cyber Threats)

개념 (Concept)

Possibility of a malicious attempt to damage or disrupt a computer network or system

- 정보시스템, 통신망에 연결된 디바이스 또는 통신망 자체를 손상시키거나 파괴할 수 있는 잠재적 요인
- 악의적 시도, 공격 행위 등

① (협의) 정보시스템, 통신망에 대한 직접적인 공격 정보로 공격IP, 악성코드 등 기술적 침해사고지표 (IoC)

- 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단을 이용하여 정보통신망과 정보통신기기를 침입·교란·마비·파괴 하거나 정보를 절취·훼손·왜곡 전파할 수 있는 행위

② (광의) 기술적 침해사고지표 (IoC) 뿐 아니라 전략적 분석(예측 트렌드), 상황인지(공격 실시간 정보), 취약점, 조치·대응 방안, 사고 분석결과 등

- 사이버공격 방법에 관한 정보, 악성프로그램 및 이와 관련된 정보, 정보통신망·정보통신기기 및 S/W의 보안상 취약점에 관한 정보, 그 밖에 사이버공격의 예방을 위한 정보

1 사이버 위협 (Cyber Threats)

정보 유형 (Information Type)

사이버 위협 정보를 생산, 소비하는 이해관계자(CEO/CISO, 관리자, 기술자)에 따라 다양한 유형이 존재

■ 사고 예방 및 사고 대응 측면

구분	유형	종류	이용자	활용 예	기한	Source
예방	전략	* 위협 글로벌 트렌드, 위협 전망 * 침해사고 News	C-Level 의사결정권자	조직 보안 전략 수립	장기	외부
예방	관리	* 침해사고 조사결과 * 취약점 조치 방안, 사고 대응복구 방안 * 중앙관리 S/W IoT 보안 가이드 * 시큐어코딩 지침	CISO, 보안관리자	보안 실행계획, 보안 조직운영	중기	외부
대응	기술	* 침해사고지표(IoC) (공격IP, C&C IP, 악성URL, 악성코드 등) * 악성코드 상세분석서 (공격자 IP, 공격유형, 취약점, 악용기술, 조치절차 등)	사고대응팀	공격방어, 공격증거 수집	즉시	내·외부



**사이버 위협 정보공유
(Cyber Threat Information Sharing)**

2 사이버 위협 정보 공유

KISA's Role

1. 침해사고 대응 조치 (Cyber Incident Response)

- 침해사고에 관한 정보의 수집·전파, 침해사고의 예보·경보, 침해사고에 대한 긴급조치
- 주요정보통신서비스제공자, 집적정보통신시설 사업자와 공동 대응
- 소프트웨어 제작/배포자의 보안취약점 수정·보완
- 국가 정보통신망 안전에 필요한 경우 관계 기관에게 침해사고 관련정보 제공

2. 이용자 정보보호 (Information Protection)

- 이용자의 정보보호에 필요한 기준을 정하여 권고
- 침해사고 예방 및 확산 방지를 위한 취약점 점검, 기술 지원 등 조치

3. 침해사고 대응 국제협력 (International Cooperation)

- 다른 국가/국제기구와 상호 협력
- 정보통신망의 안전성 침해행위 방지 업무, 정보통신서비스의 안전한 이용에 관한 업무

2 사이버 위협 정보 공유

KISA's Role

침해사고 예방/대응 협력 네트워크의 이해당사자



2 사이버 위협 정보 공유

KISA-정보공유/협의 활동



3

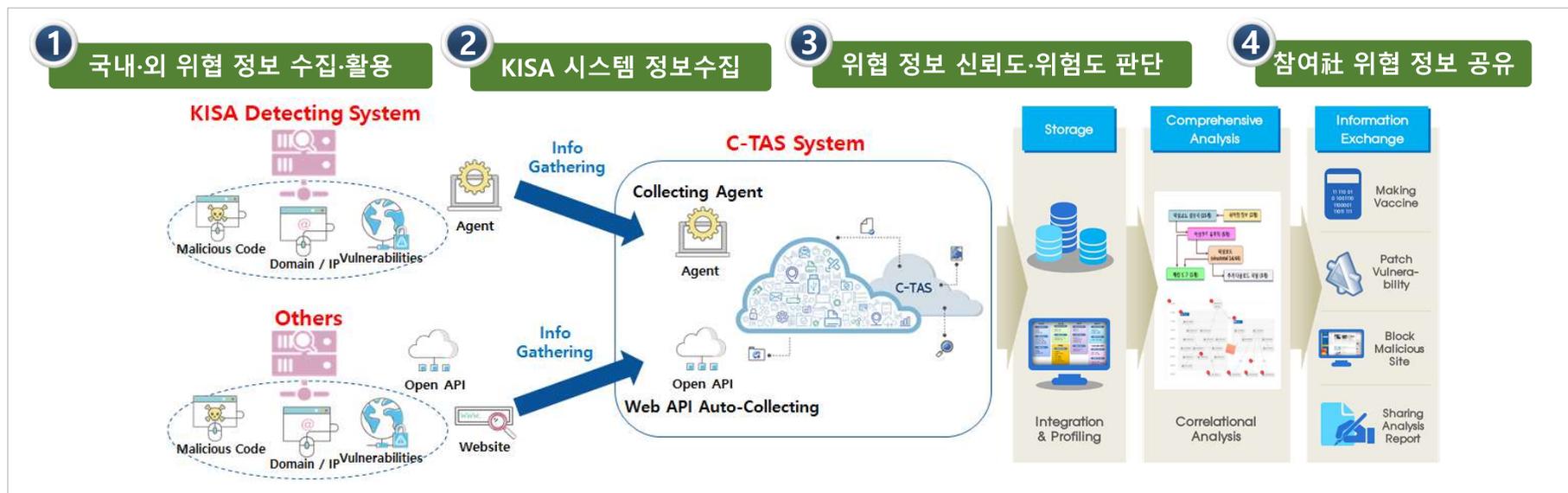
사이버위협정보 분석·공유(C-TAS) 시스템

3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템

민간분야 침해사고 확산 방지를 위하여 사이버 공격 시도 등을 수집분석하여 참여사와 함께 공유하는 플랫폼

- 악성도메인, 악성 IP, 악성코드 등 KISA 자체 시스템(DDoS 사이버대피소, MC-Finder 등), 글로벌 공격 정보(타 국가 CERT), 참여사 공유 정보
- 통신, 보안관제/장비, 호스팅, 게임, 포털 등 분야의 222개사 참여 ('18.8)



3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing (C-TAS) 시스템 – 공유 정보

총 36개 종류의 위협 정보를 구분하여 C-TAS 시스템을 통해 공유

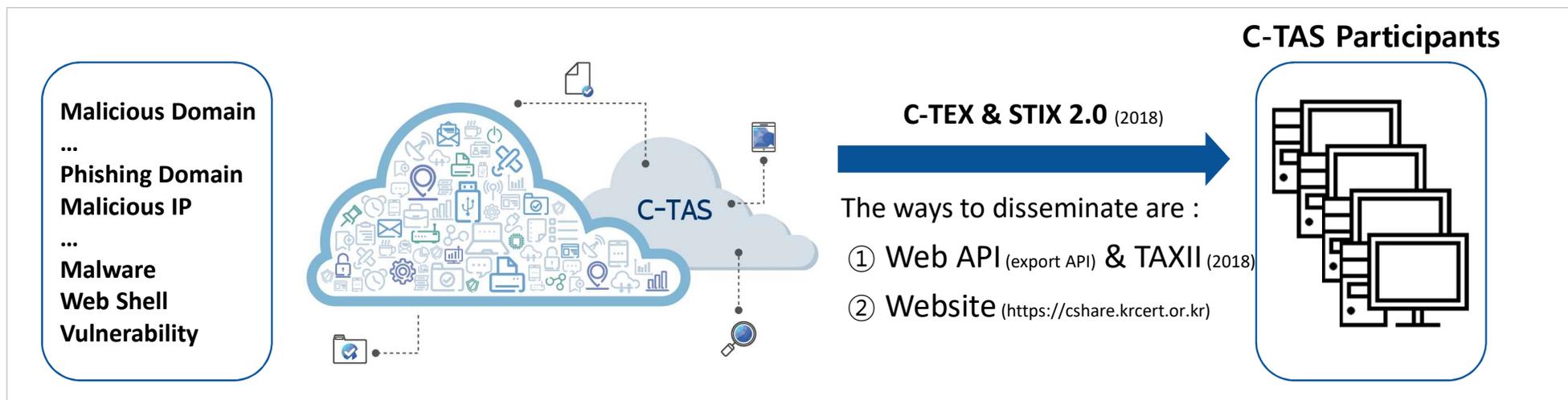
단일지표	악성코드, C&C, 감염IP, 공격시도IP, 유포지, 피싱, 파밍, 스미싱, 정보유출지 등	IoC (Indicator of Compromise)
분석보고	기술문서, 보안공지, 악성코드분석보고서, 악성모바이앱 분석보고서	-
추이정보	일간/주간/월간 추이	특정 관찰 기간 동안 전구간의 전체 지표와 비교하여 여러 수집처에서 발견한 정보, 해당 관찰시간에 재등장한 정보
지속정보	일간/주간/월간 지속	특정 관찰기간 동안 시간 기준으로 연속하여 등장하는 정보
중복정보	일간/주간/월간 중복	특정 관찰기간 동안 수집처 기준으로 여러 곳에서 등장하는 정보
동향정보	일간/주간/월간 동향	특정 관찰기간 동안 추이 또는 지속, 중복 등 다양한 속성의 최신경향 정보
핵심정보	일간/주간/월간 핵심	특정 관찰기간 동안 추이 및 지속, 중복성을 두루갖춘 고효동성 정보
중개지표	어뷰징IP, 상황전파/해제문, 원클릭서비스 등	-

3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템 – 공유 방식

API(실시간 자동 공유 가능) 및 홈페이지를 통한 다운로드 방식

- API를 이용할 경우 실시간으로 자동 공유 가능
- 홈페이지의 경우, 이용자가 필요시 접속하여 정보 조회 및 다운로드 가능



3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing (C-TAS) 시스템 – 활용사례

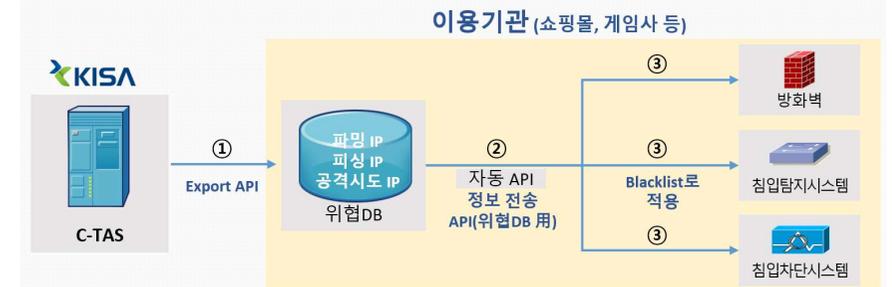
① 악성코드 차단

- 악성코드의 고유 식별값을 자사 백신 솔루션의 탐지률에 업데이트 하여 악성코드 차단



② 악성 IP 차단

- 악성 IP(파밍IP, 피싱IP, 공격시도IP 등)를 보안장비(방화벽, 침입 탐지시스템 등) 블랙리스트에 추가하여 공격 차단



③ 악성파일 업로드 탐지·차단

- 웹서비스를 통해 업로드 되는 파일과 고유식별값을 비교하여 악성 파일 차단



3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 - Incident Response with National CERTs

국가 간 CERT 협업(美, 中, 日, 英 등) - 침해사고 中心

- 국가 CERT 연락망을 통해 침해사고 중심의 정보를 TLP 규약에 따라 정보공유
- 사이버공격 비상대응 핫라인을 통해 단순 사고정보 뿐 아니라 사고 연관성 정보(공격분석보고서, 악성코드 등) 등 고품질 위협 정보 확보 (TLP 규약 준수)

Technical Analysis of Lazarus Group attacks on Polish and other institutions

Annex A
DNS data associated with 'tradeboard' and 'movis-es'

Domain	IP Address	Resolution
tradeboard.mefound.com	124.49.86.123	131.11.224.116
	18.133.51.74	36.61.133.78
	18.200.16.239	129.252.264.13
	244.16.166.3	0.174.0.74
	244.16.166.3	

Further domains hosted on IP addresses associated with 'tradeboard' and 'movis-es'

Domain
edonius.mibasic.com
hp.win7os.nso2.info
lgnews.kongmusic.com
win7os.nso2.info
www.win7os.nso2.info

Annex B
All indicators of compromise

101.102.225.236	129.221.154.15	18.200.16.237	244.16.155.3	58.43.86.123
203.85.140.183	151.11.224.116	180.211.191.114	36.61.133.78	68.95.25.140
109.184.247.169	133.242.88.44	196.39.166.218	43.243.207.145	73.245.147.162
113.29.189.133	150.214.190.118	203.236.192.108	40.243.207.150	79.174.241.188
117.238.176.3	170.160.135.6	210.51.109.22	50.203.97.150	82.144.131.5
117.252.113.22	175.45.178.222	216.54.224.59	58.177.238.32	9.173.0.74
125.214.195.17	175.45.24.76	218.224.129.66	59.3.127.132	96.32.213.51

edonius.mibasic.com	movis-es.ignorelist.com	tradeboard.mefound.com
eye-watch.in	sap.msaport.ch	win7os.nso2.info
hp.win7os.nso2.info	lgnews.kongmusic.com	www.win7os.nso2.info

Backdoor in Android mobile devices

After the announcement of Kryptowire about the several models of Android mobile devices that contained firmware which collects sensitive personal data about users and the data to third-party servers without users' consent, CERT.LV and CERT-EE conducted joint research on the Android mobile phones used in the government networks. Affected devices will most likely be extended after researchers will finish the analysis of mobile network operators.

The list of affected devices for now:
The list is TLP:

```

"oem=Acer" "model=B3-A20B"
"oem=alps" "model=VK800X"
"oem=asus" "model=ASUS_Z00V"
"oem=Blackview" "product=relax"
"oem=Coolpad" "model=Coolpad"
"oem=CUBOT" "model=CUBOT_T"
"oem=HTC" "model=V177"
    
```

18-16-2023B-Indicators of Compromise Associated with Mirai Botnet
TLP: US-CERT
Department of Homeland Security
Reference Number: 18-16-2023B
Report Date: 2018-10-23T22:25:29Z

Notification:
DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is distributed as TLP:GREEN. Limited disclosure, restricted to the community. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp>.

Summary:
US-CERT was notified by a trusted third party of indicators of compromise associated with Mirai botnet.

Analysis:
Host: report.laataazaittenjoh.cf
Killchain Phase: Command and Control
Characterization: CC

Host: netxrk.org
Killchain Phase: Command and Control
Characterization: CC

Registry Keys

As well as inserting itself as a scheduled task into the infected system, the malware writes to the following registry keys:

```

HKLMSOFTWARE\Wbem\Microsoft\Windows NT\CurrentVersion\Wbem\Trickbot
HKLMSOFTWARE\Wbem\Microsoft\Windows NT\CurrentVersion\Wbem\Trickbot
    
```

Command & Control Infrastructure

Each binary typically has nine IP addresses associated with it. These IP addresses change and can be updated by the malware. The list of IP addresses can be found below along with a domain name that is used for updating the Trickbot executable:

- <http://zalehanmal.temo.safest.com>

Malware Analysis

Trickbot Banking Trojan

Version 1.0
Reference: NCSC Ops05-17
16th March 2017
© Crown Copyright 2017

IP addresses identified by NCSC infrastructure analysis infrastructure:

IP Address	IP Address	IP Address
83.9.28.24	43.241.244.167	74.56.177.32
82.46.107.110	5.107.95.37	80.79.114.179
82.5.50.55	5.20.186.52	82.79.202.214
115.174.41.163	88.81.102.171	82.79.219.253
77.209.51.162	62.99.66.210	88.43.158.100
109.92.62.46	36.66.107.162	81.219.23.77
109.92.62.46	36.66.209.21	200.119.236.96
221.179.156.39	85.25.3.13	200.120.214.150
84.42.159.138	61.7.8.24	203.76.105.82

C2 servers using the encrypted HTTPS port 443. These servers follow the format: `rd_id/command_parameters`. The user-agent strings stand out from the rest as they are used by the NCSC, the user-agent strings stand out consistent over a lengthy period of time; these may be identified by NCSC infrastructure analysis infrastructure.

3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 - Incident Response with National CERTs

국가 간 CERT 협업 - 중점 협력국 확대

- 유럽 (영국, 에스토니아, ENISA), 아시아 (대만, 홍콩) 권역에 사이버 위협정보 공유를 위한 협력 파트너 확보
- (다국적) 국제사고침해대응협의회(FIRST), 아태침해사고대응협의회(APCERT) 공동모의훈련 등



The collage features logos for several national CERTs: CIRCL (@circl_lu), CERT Estonia (@CERT_EE), CERT-RO (@CERT_RO), NCSC-FI (@CERTFI), CERT Polska (@CERT_Polska_en), NorCERT (@NorCERT), and CCN-CERT (@CCNCERT). Each logo includes a brief description of the organization's role. To the right, two photographs show participants in a control room during a joint simulation exercise, with one photo showing a presentation slide for APCERT.

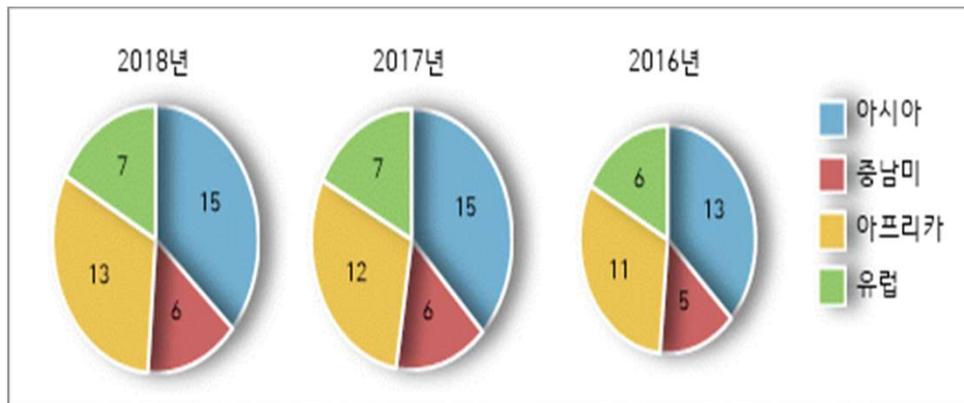
3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 – GCCD와 CAMP

글로벌 사이버보안 협력 네트워크 (CAMP, Cybersecurity Alliance for Mutual Progress)

- 국경없이 발생하는 고도화, 지능화된 사이버위협에 공동 대응하고, 사이버 보안 협력 사안을 함께 논의, 발전시켜 나가기 위한 협의체
- 다양한 침해사고 대응 경험과 정보보호 노하우, 사이버보안 전략과 경험을 국제사회에 공유·전파
- 정보공유, 사고 공동대응, 역량강화 등 사이버보안 발전을 서로 돕는 글로벌 사이버보안 허브 기능

< CAMP 플랫폼을 통한 사이버보안협력 >



구분	사이버보안 기술	사이버보안 정책	사이버보안 역량강화
정보 공유	· 신규 위협정보 · IoT 등 융합환경 보안기술 · CERT 구성·운영 가이드	· 사이버보안전략표준 · 사이버보안 법령/체계 · 회원국 시장 트렌드 등	· 전문가 교육(K-Shield) · 자격인증(정보보안기사 등) · 인식제고 캠페인
공동 활동	· 침해사고 모의훈련 · 취약점 컨설팅 (GCCD) · PKI, CSIRT 등 F/S	· 사이버보안 공통보안수칙 · 공동세미나 (GCCD) · 정책 컨설팅 (외부기관)	· APISC CSIRT 교육 · 역량진단 (WB-OXF-GCCD) · 초청연수

CAMP(Cyber security Alliance for Mutual Progress) 플랫폼



안전한 사이버 세상을
만들기 위해 노력하겠습니다

국민 안심, 국가 안전

한국인터넷진흥원이 함께 합니다!

