KIWONTECH

정보보안 트렌드 및 보안 위협에 대한 대응방안

표적형 이메일 공격 선제대응을 위한 이메일 보안 표준 방침

(주)기원테크 김충한 팀장

CONTENTS

이메일 보안의 새로운 기준

KIWONTECH

01 Chapter

이메일 보안 현황

02 Chapter

이메일 사이버 공격 대응 방안

03 Chapter

기업 소개

CHAPTER

KIWONTECH

01
Chapter
이메일 보안 현황

| 01 | 기존 이메일 사이버 공격 유형

| 02 | 시그니쳐 기반 패턴 분석 방식의 한계

| 03 | 이메일 사이버 공격 최근 이슈

| 04 | 최근 이메일 사이버 공격 유형

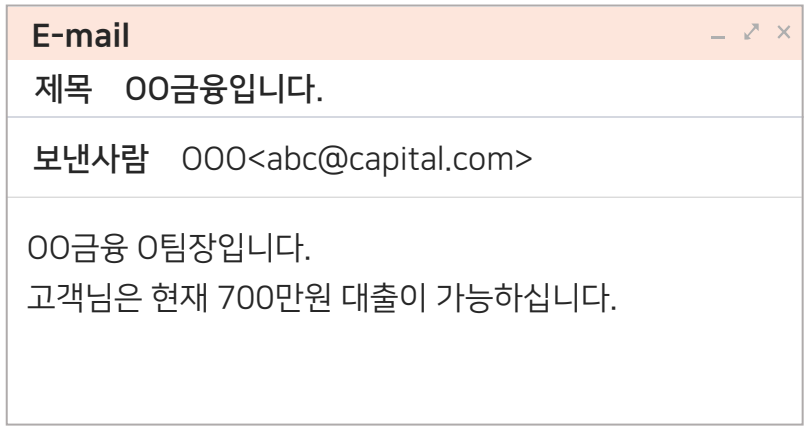
|01| 기존 이메일 사이버 공격 유형

광고성 SPAM 메일


Home > 전체기사

"인터넷 이용자 3명 중 1명은 스팸 메일 피해"

좋아요 73개 입력: 2001.06.04


E-mail

제목 OO금융입니다.

보낸사람 OOO<abc@capital.com>

OO금융 O팀장입니다.
고객님은 현재 700만원 대출이 가능하십니다.

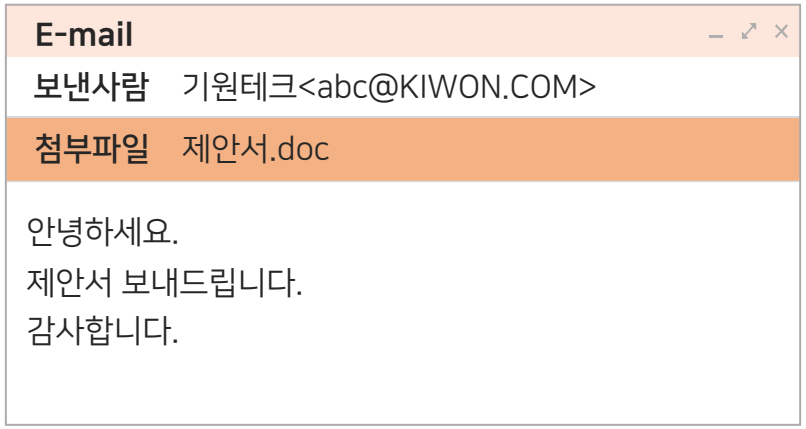
단순 광고 목적의 대량 스팸 메일

첨부파일 바이러스


Home > 전체기사

악성 PDF 파일 첨부된 '결제 송장' 위장 이메일 유포

좋아요 73개 | 입력: 2003.08.10


E-mail

보낸사람 기원테크<abc@KIWON.COM>

첨부파일 제안서.doc

안녕하세요.
제안서 보내드립니다.
감사합니다.

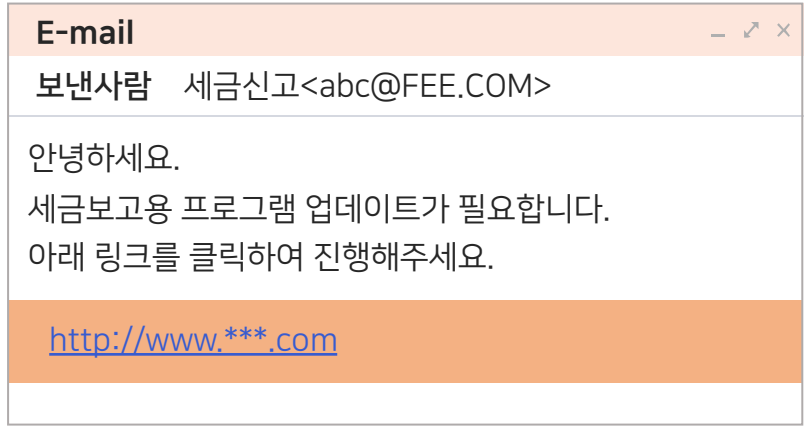
신종 악성코드 및 랜섬웨어

악성 URL


Home > 전체기사

"월급 계좌 신청서 작성해주세요"…사칭 이메일 늘었다."

좋아요 73개 입력: 2017.08.03


E-mail

보낸사람 세금신고<abc@FEE.COM>

안녕하세요.
세금보고용 프로그램 업데이트가 필요합니다.
아래 링크를 클릭하여 진행해주세요.

http://www.***.com

악성 및 피싱 사이트

| 02 | 시그니쳐 기반 패턴 분석 방식의 한계

HACKER

- 도메인 평판, 파일, URL 검사결과, 정상으로 판단하여 보안솔루션 통과

- 정상적인 경로로 도메인 구매
- 정상 메일 서비스 사용하여 메일 발송
- 본문 및 파일 내 URL 비활성화

- 메일 내 URL과 악성 피싱 사이트 연결
- 악성코드 다운로드, 개인정보 유출 등, **악성 URL 공격 피해 발생**

- 각종 스팸 분석 솔루션, RBL, 백신 등 시그니쳐 패턴 업데이트

알려지지 않은 위협에 취약

- 신종 악성코드, 신종 랜섬웨어, 신고되지 않은 URL 등, 패턴 분석으로 비교 불가능한 공격 방식에 취약
- 능동적인 방식의 분석 방식과 병행 하여 다중 보안체계 구축

한 발 늦은 대응

- 누군가는 반드시 피해를 당해야 패턴이 업데이트
- 피해를 당하기 전에 예방하는 선제적인 대응이 필요

| 03 | 이메일 사이버 공격 최근 이슈

수신 보안 이슈

"이 계좌로 송금하세요"…
이메일 해킹 무역사기 '또' 2020. 08. 24 뉴스1

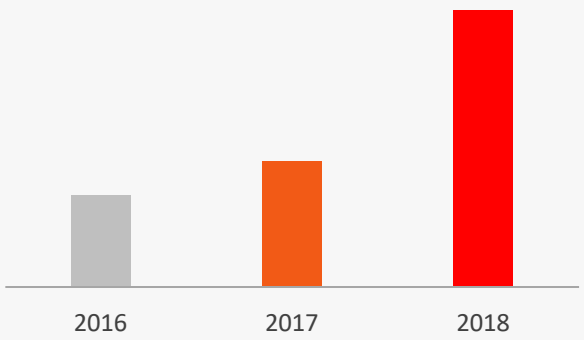
"피싱 URL만 3만개 이상"…
코로나19 악성메일 공격 2020. 04. 14 뉴스핌

91% 사이버 공격 이메일에서 시작
출처 : KISA

62% 지능형공격 (APT)
출처 : 밸리메일 보고서

90% 악성코드 없이 발송
출처 : 취재K

랜섬웨어 피해 경험



출처 : 과학기술정보통신부

발신 보안 이슈

6년간 기술 121건 해외유출…
국가핵심기술도 29건 빼돌려 2020. 09. 17 매일경제

국내 기업 데이터 유출 피해액
평균 38억원… 작년보다 증가 2020. 07. 30 바이라인네트워크

이메일 데이터 침해 발생 원인
출처 : IBM

악의적인 공격 **50%**
직원 단순 실수 **21%**

| 04 | 최근 이메일 사이버 공격 유형

정상적인 메일로 위장하여 패턴으로 검출 불가능한 지능형 사기 메일

E-mail

제　　목 ! 결제 계좌 변경 안내

보낸사람 거래처<abc@KIWON.COM>

받는사람 구매팀<purchase@company.com>

첨부파일

안녕하세요.
세금 계산 문제로 계좌가 변경되었으니,
아래 계좌로 대금 입금 요청합니다.

SWISS BANK 256-78901-859-3452

대금 결제, 물품 선적 등 중요한 순간을 노린 지속형 범죄

- 거래 과정을 지속적으로 지켜본 후, 결제 시점에서 사기 메일을 발송하여 결제 대금을 가로채는 방식

기업 특정 부서의 실무자를 노린 표적형 범죄

- 구매팀, 재무팀 등, 특정 부서의 실무자를 표적으로 삼기 때문에 성공률 및 피해 금액이 상당히 큼

악성코드, 랜섬웨어 등, 첨부파일이 없어 패턴 검출 불가능

- 악성코드와 랜섬웨어가 포함되어 있지 않기 때문에 엔드포인트 보안 및 백신 등으로 검출 불가능

악성 피싱 사이트 URL 없는 본문으로 보안 솔루션을 통과

- 본문에 악성 사이트로 연결되는 URL을 포함하고 있지 않아 URL검출 또한 불가능

CHAPTER

KIWONTECH

02
Chapter

이메일 사이버 공격 대응 방안

| 01 | 메일 발송지 및 경유지 역추적

| 02 | 악성 메일 다중 분석 검사 체계

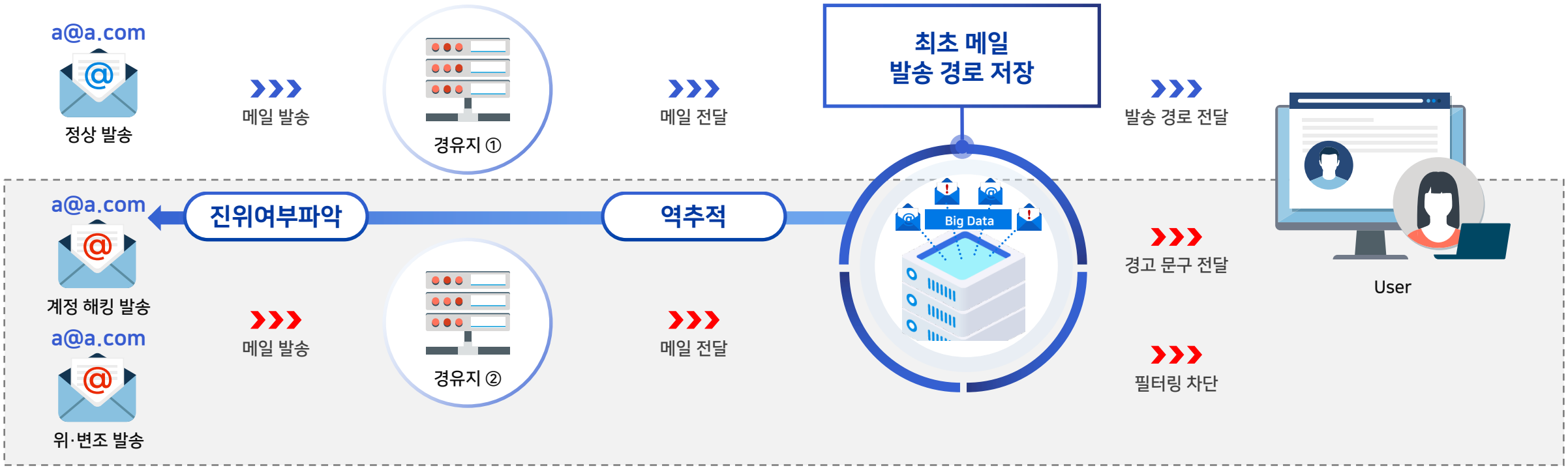
| 03 | URL End-Point 추적 검사

| 04 | 비활성 URL 실시간 검사

| 05 | 사기성 유사 도메인 선별 검사

| 01 | 메일 발송지 및 경유지 역추적 검사

기존 발송 경로 데이터와 다른 변경된 발송 경로 역추적 검출



- 기존 메일 발송 경로 저장 후, 이후 메일 발송 경로가 변경 시에 해당 메일 차단
- 변경된 발송 경로를 사용자에게 전달하여 해당 메일에 대한 경각심과 발송지 변경에 대해 발신자에게 확인

| 02 | 악성 메일 다중 분석 검사 체계

신종 바이러스 및 랜섬웨어 검출

- 메일에 첨부된 파일과 URL에 대해 검사 진행
- 사용자 PC에 변화되는 환경 검사

첨부파일 ——— CUBE ①

URL ——— CUBE ②

➡ 3단계 검사

악성 메일일 경우, 차단

1단계 | 백신(패턴) 검사

- 백신 프로그램(정적 검사)으로 패턴 바이러스 검출
- 기존에 검출되어 백신에 등록되어 있는 바이러스를 검출

2단계 | 환경 변화 검사

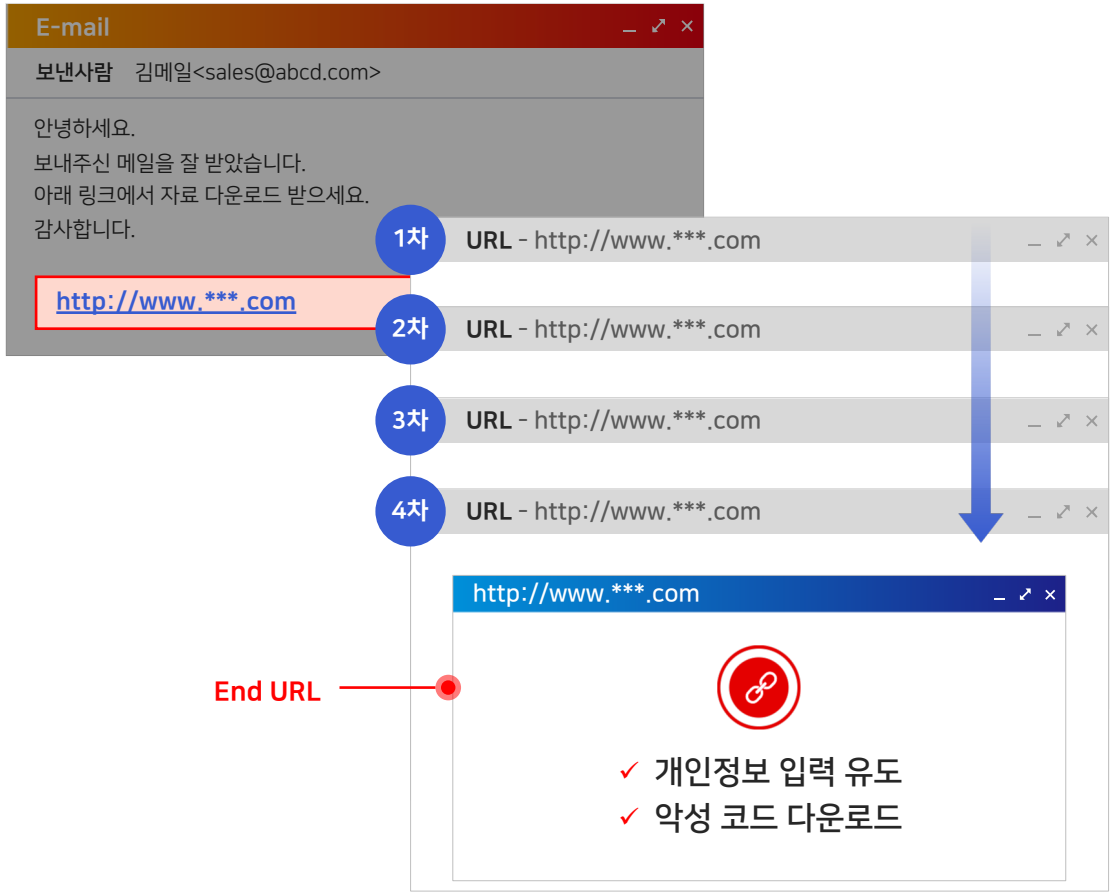
- 백신 프로그램으로 스파이웨어, 바이러스 검출
- 윈도우 환경 변화를 감지

3단계 | 행위 분석 검사

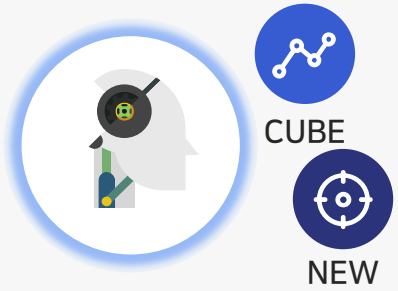
- 행위 분석 검사로 패턴이 없는 신종 바이러스를 검출
- CUBE에서 직접 열어보고 시스템에 대한 위험 행위 검출
- 패턴 검사의 한계를 극복한 능동형 선제 대응 검사

| 03 | 악성 URL 검출 – URL End-Point 추적 검사

메일 본문, 첨부파일 내의 모든 URL의 End-Point까지 추적 검사

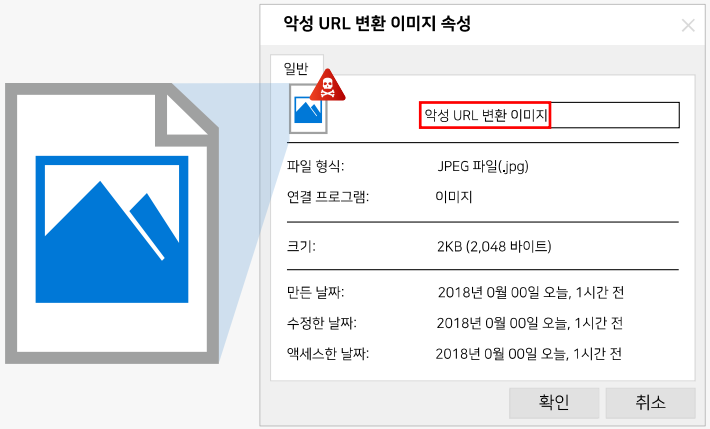


자동 실행 스크립트, 다운로드 파일 등 행위 기반 검사 실행



- ✓ 1단계 | 백신(패턴) 검사
- ✓ 2단계 | 피싱 사이트 알고리즘 검사
- ✓ 3단계 | 행위 분석 검사

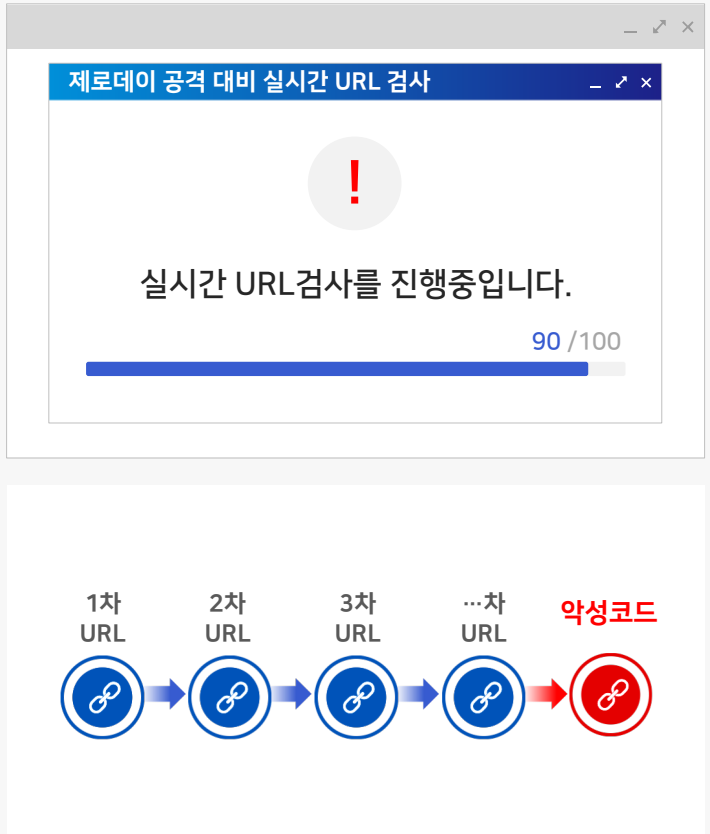
악성 URL 검출 시, 이미지로 변환하여 안전하게 전달



| 04 | 사후 악성URL 활성 검출 – 비활성 URL 공격 차단 (실시간 검사)

본문 내 URL 비활성화, 재검사 전용 URL로 변경

URL End-Point 추적 및 행위 기반 동적 검사



비활성 URL 변경 공격 차단 및 피해 예방

정상 URL로 위장한 악성 URL
행위 기반 End-Point 검사로
사후 공격 실시간 대응!

| 05 | 사기성 유사 도메인 선별 검사

KIWONTECH

유사한 문자열을 사용했을 경우 사기성 및 유사성 판단

abc@KIWONTECH.COM — 대문자 i

abc@KIWONTECH.COM — 소문자 L

[유사성 검출]
눈으로 구분하기 어려운 문자열을 사용한 기업대상 사기메일 검출

유사성 필터링(상·중·하) 사용자 경고 알림

[유사성-위험] 의심스러운 메일 주소와 메일을 주고 받았을 경우 경고 알림

[유사성-상] 1@KIWONTECH.com ->1@KIWONTECH.com (1개 검출)

[유사성-중] 1@KIWONTECH.com -> 1@KIWONTECH.com (2개 검출)

[유사성-하] 1@KIWONTECH.com -> 1@KIWOMTECH.com (3개 검출)

정확한 판단을 위하여 **개인별 DB화 색인 분석**

선제 대응이 가능한 실시간 Memory 조회 방식

History 분석 및 비교

E-mail	E-mail
보낸사람 기원테크<abc@KIWON.COM> 1월 1일	보낸사람 기원테크<abc@KIWON.COM> 1월 2일

이전 수신 History를 학습하고 데이터로 저장하여 수신 도메인과 **비교**

선제 대응이 불가능한 패턴 등록 방식보다 진화된 검출

유사 도메인 패턴 등록 목록

1. GOWONTECH.COM
2. MAVER.COM
3. DOUM.NET
4. GOOGLE.OR.KR

...

CHAPTER

KIWONTECH

03
Chapter
기업 소개

| 01 | 기업 소개

KIWONTECH

- 기 업 명 주식회사 기원테크
- 주 소 서울시 구로구 디지털로31길 53 E&C 5차 509호
- 대표이사 김동철
- 설 립 일 1994년 최초 설립
- 홈페이지 www.kiwontech.com
- 대표전화 T)02-6012-7406 / F)02-6085-4330
- 운영 IDC 서울시 양천구 목동로 233-5 KT ICC

| 02 | 사업 소개

이메일 수신부터 발신까지 완전한 통합 보안 제공
차세대 메일 보안 전문 All-in-One 솔루션 “EG-Platform”

이메일 전 구간 보안

수신 메일 보안 구간

SpamGUARD

STEP 01

스팸메일 검사

- 학습형 스팸 필터링으로
- 기업 맞춤 스팸 정책 제공

ReceiveGUARD

STEP 02

APT 사기메일 검사

- 사기 메일 선제 대응

  오송금 사기, 랜섬웨어 예방

발신 메일 보안 구간

SendGUARD

STEP 03

발신메일 관리

- 차세대 발신 메일 제어

  조직도 연계 승인 관리

| 03 | 기술력 인증

Gartner | 이메일 보안 시장조사 리포트 등재

글로벌 최대 규모의 IT부문 최대 시장 조사 기관인 Gartner 보고서에 따르면, Gartner는 이메일 보안의 4대 핵심기술을 발표하고 이를 모두 보유하여 향후 이메일 보안시장을 선두할 것으로 예상되는 Vender List 중 기원테크가 아시아 지역 유일하게 2019년 선정되었음.

Regionally focused SEGs (see Table 2) have their predominant business bases in the same geographic regions, particularly in Europe. Gartner ai will continue to expand their geographic reach.

Table 2. Representative Vendors for Regionally Focused SEGs

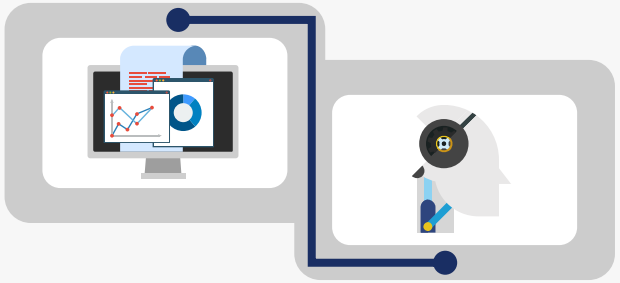
Vendor
Clearswift
Kiwontech
Retarus
Spamina (part of the Hornetsecurity Group)

Source: Gartner (June 2019)

대한민국 최초, 지역을 대표하는 이메일 보안 벤더 선정!

자체개발 메일 엔진, 머신러닝 AI 보유 기업

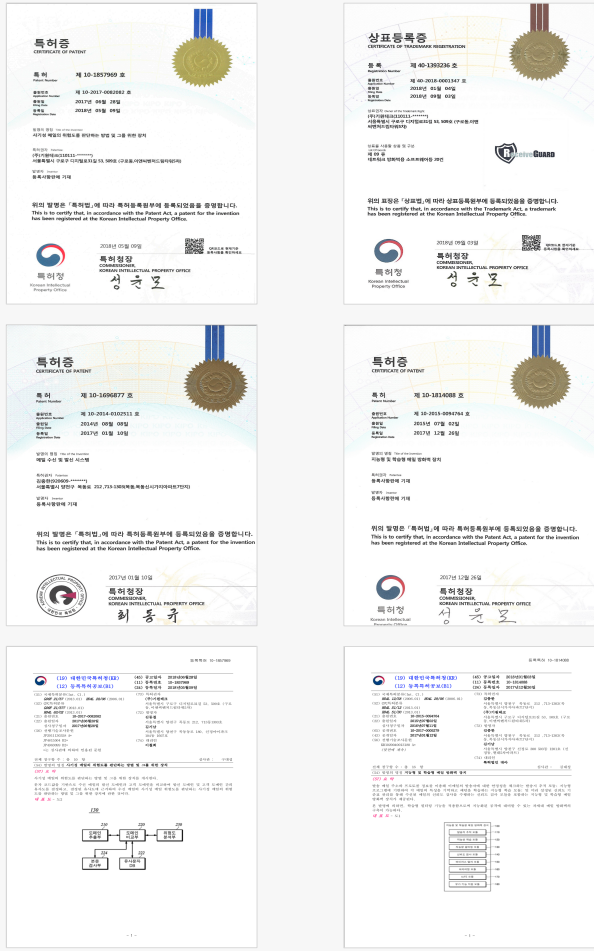
독자적인 기술로 자체 개발한 메일 엔진 보유!
이메일 원본 자체를 분석할 수 있는 AI기술과 머신러닝의 결합



IT보안인증사무국 CC인증 획득

Receive GUARD는 보안 제품에 대한 국제공통평가 기준을 만족하여 정부 및 공공기관이 정보보안 제품을 도입할 때 필수적으로 요구되는 CC인증(EAL2)을 획득하였습니다.

국내·외 지식재산 확보 현황



표적형 이메일 공격 선제대응을 위한 이메일 보안 표준 방침

이제는 한 발 빠른 선제 대응이 필요합니다.

THANK YOU

From the Beginning to the End of Mail Service
One stop Mail Platform with AI