“사이버 공격으로부터
계정과 데이터를 안전하게 보호하는 방법“
(정부부처 및 금융권 사례를 중심으로)

2022. 04.

(주)이스톰
우종현 대표

Contents

누구나 사이버 공격에 노출될 수 있다

전자신문 1982+40

망분리 환경까지 해커 침투...사이버 안전지대 없다

발행일 : 2019.07.29 11:00 지면 : 2019-07-30 8면

올 상반기 안전하다고 여겨지던 망분리 환경을 침투한 공격이 발생했다. 악성 이메일을 타고 들어온 해커가 중앙관리(AD) 서버를 장악한 후 랜섬웨어를 유포한 사례도 발견됐다.

이재광 한국인터넷진흥원(KISA) 침해사고분석 팀장은 올해 상반기 국내 기업 침해사고 현장조사를 바탕으로 '기업 침해사고 대응 프로세스' 부족을 지적했다. 기업과 기관이 방화벽, 안티바이러스(백신) 등 공격 예방체계를 갖췄지만 해커 침투 후 내부 정보 수집 활동을 잡아내는 체계가 소홀했다.

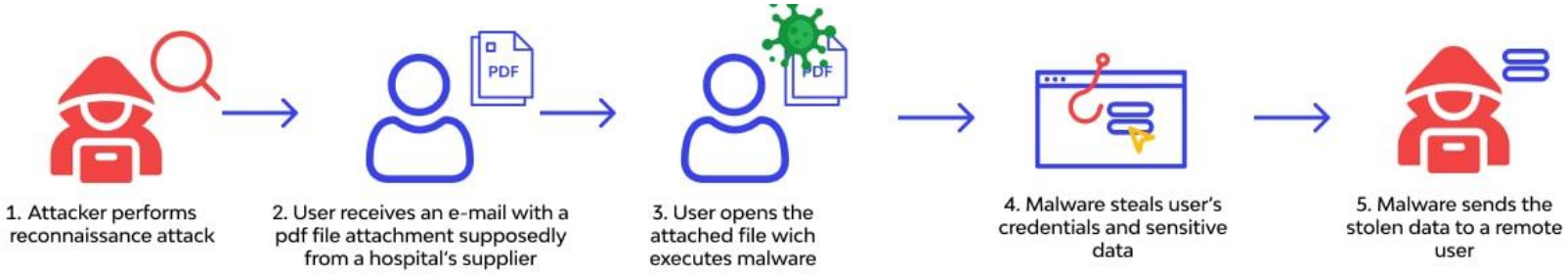
이 팀장은 “해킹위협을 사전에 막는 것만큼 공격이 시작된 후 해커 행동을 추적하는 내부 관리 관리가 중요하다”면서 “해커가 침투 후에 마음 놓고 정보를 수집할 수 없도록 위협식별 체계를 마련해야 한다”고 말했다.

올해 상반기 워너크라이, 대형 디도스 공격 등 침해사고는 발생하지 않았지만 알려지지 않은 개별기업 침해는 심각했다. 악성 이메일을 타고 들어온 해커가 AD서버를 장악 후 랜섬웨어를 유포하는 새로운 공격방법까지 등장했다. 소위 안전하다고 여겨지던 망분리 환경에 대한 공격도 발생해 '사이버 안전지대'가 없다는 것을 다시 한 번 증명했다.

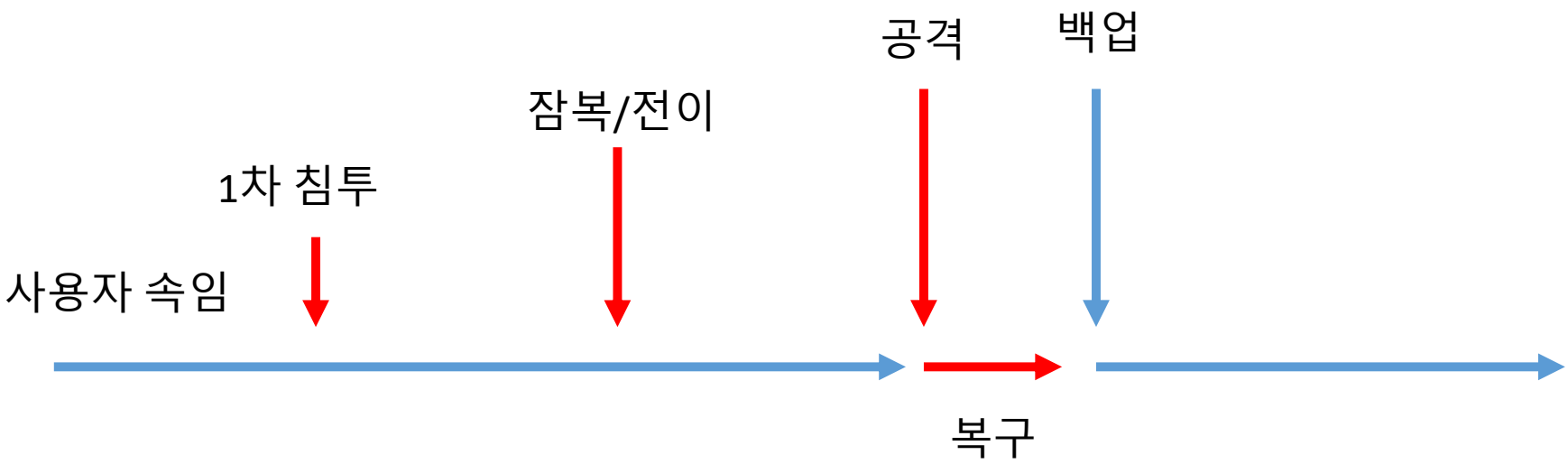

LOGIN
User Name
Password
Forgot password
Remember password


APT

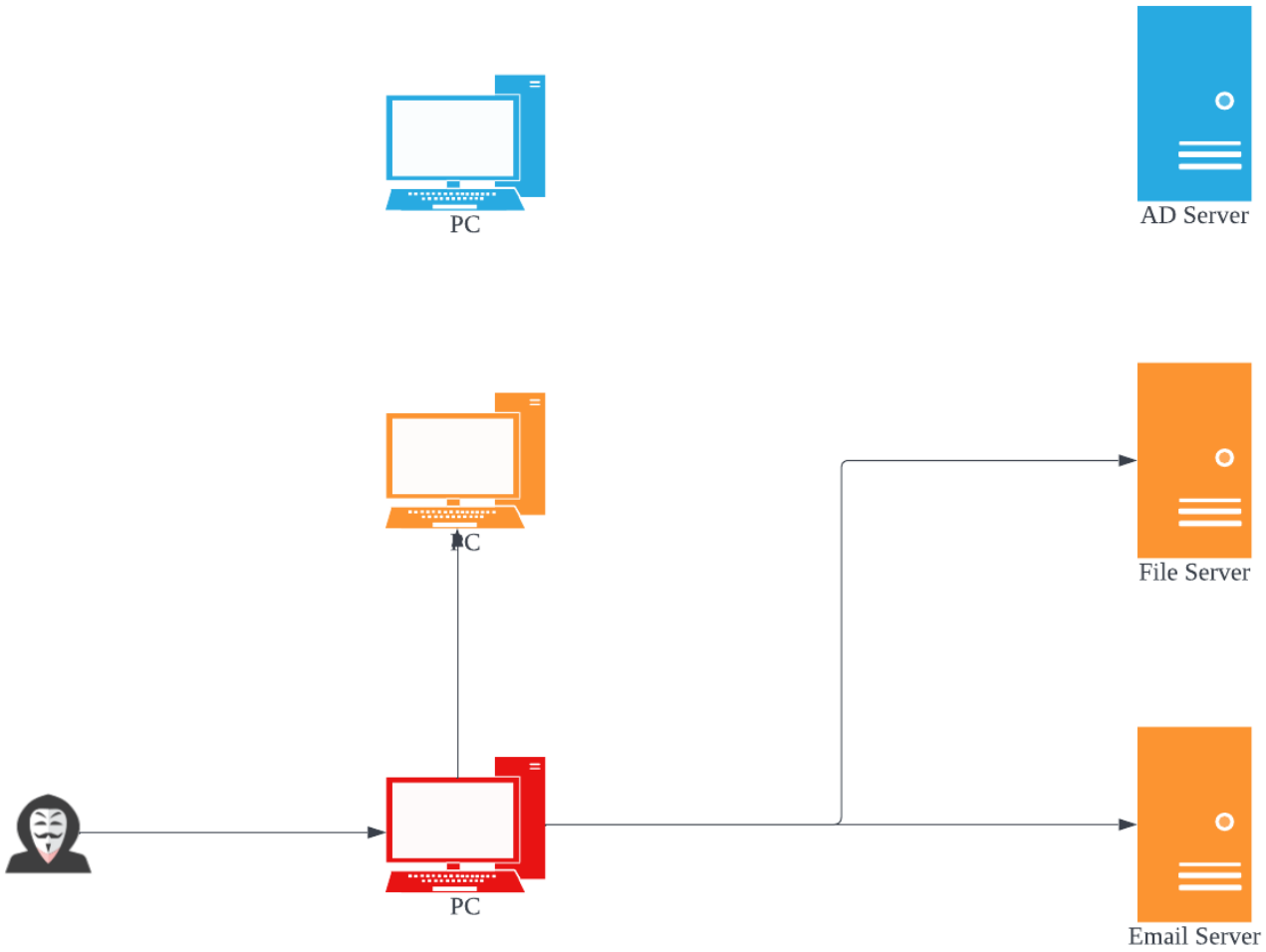
사용자나 관리자가 속아서
실수로 악성코드 구동하면?



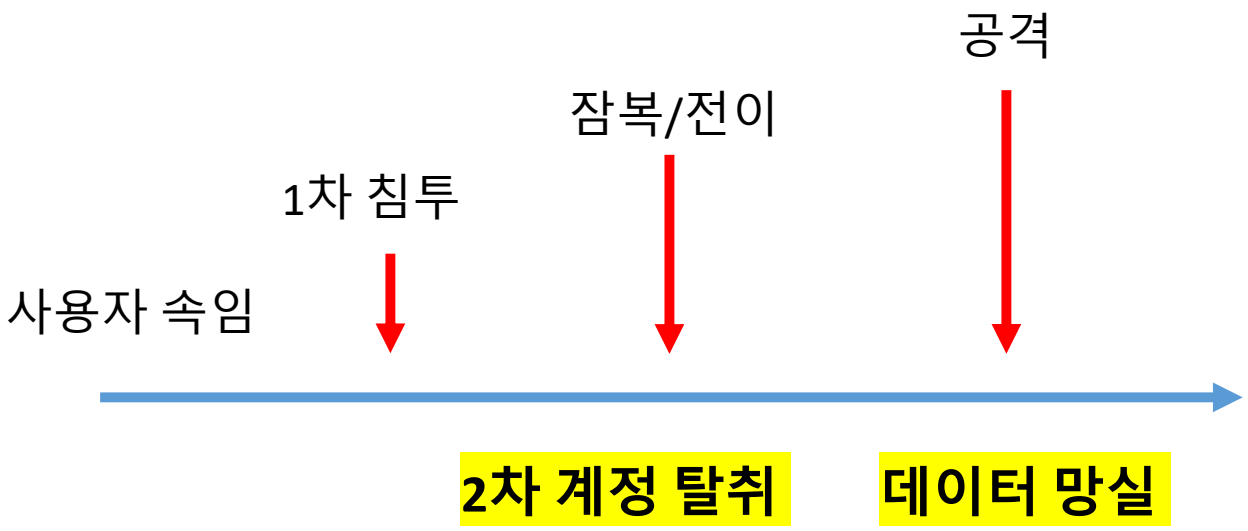
사이버 공격의 시작은?



The median "dwell-time", the time an APT attack goes undetected. FireEye reported the mean dwell-time for 2018 **in APAC as 204 days**.


PC
AD Server
PC
File Server
PC
Email Server

1차 침투 이후 주요 과정



사용자가 많으면 많을 수록 사고 확률이 높아진다

사용자나 관리자가 속아도

사용자 계정과 데이터를

보호할 수 있는 방법은?

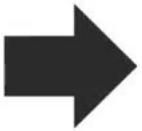
실수를 하더라도

계정을 보호할 수 있는 방법

PC에 잠복중인 멀웨어가 설치되어 있다면?

Input-Based User Credential

User Password

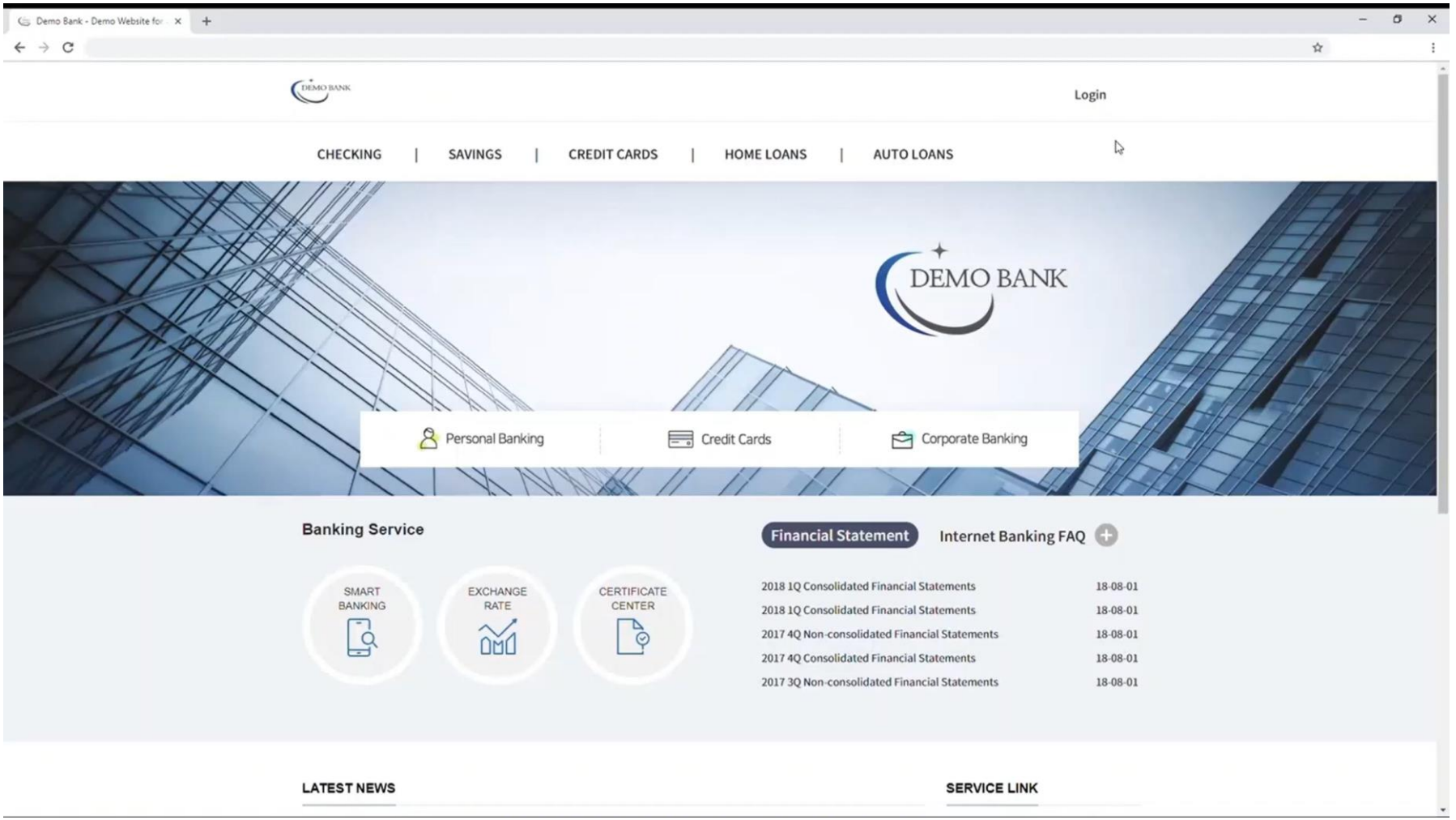


사이버 공격의 90%는 계정탈취에서 시작된다

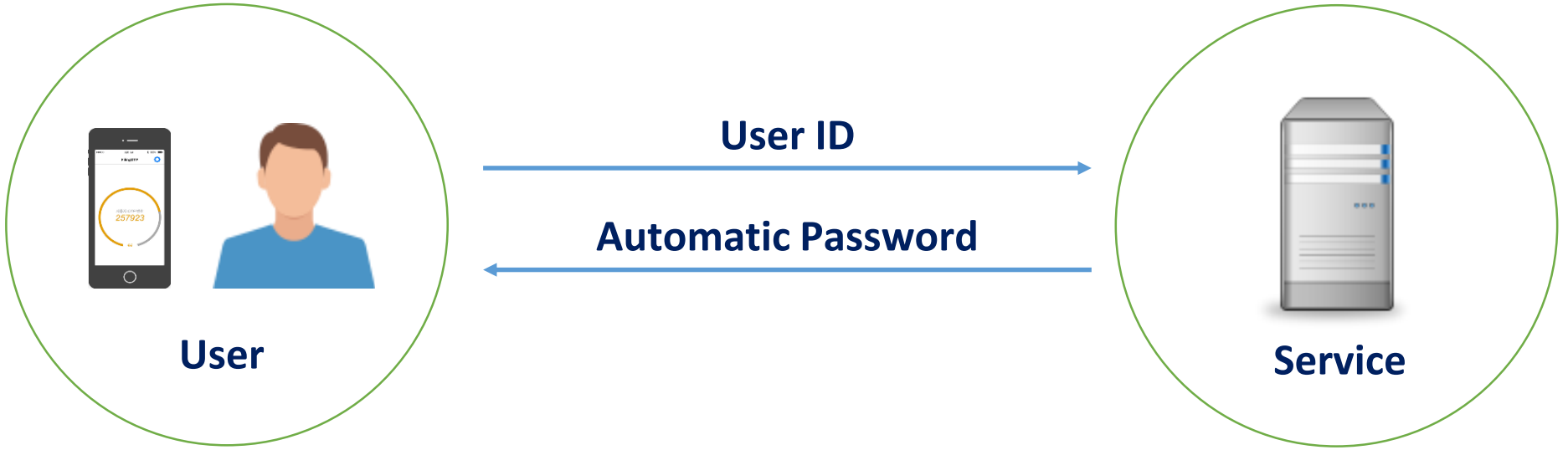
혼자서 몇 대의 서버와 PC를 관리하나요?

얼마나 자주 패스워드를 변경하나요?

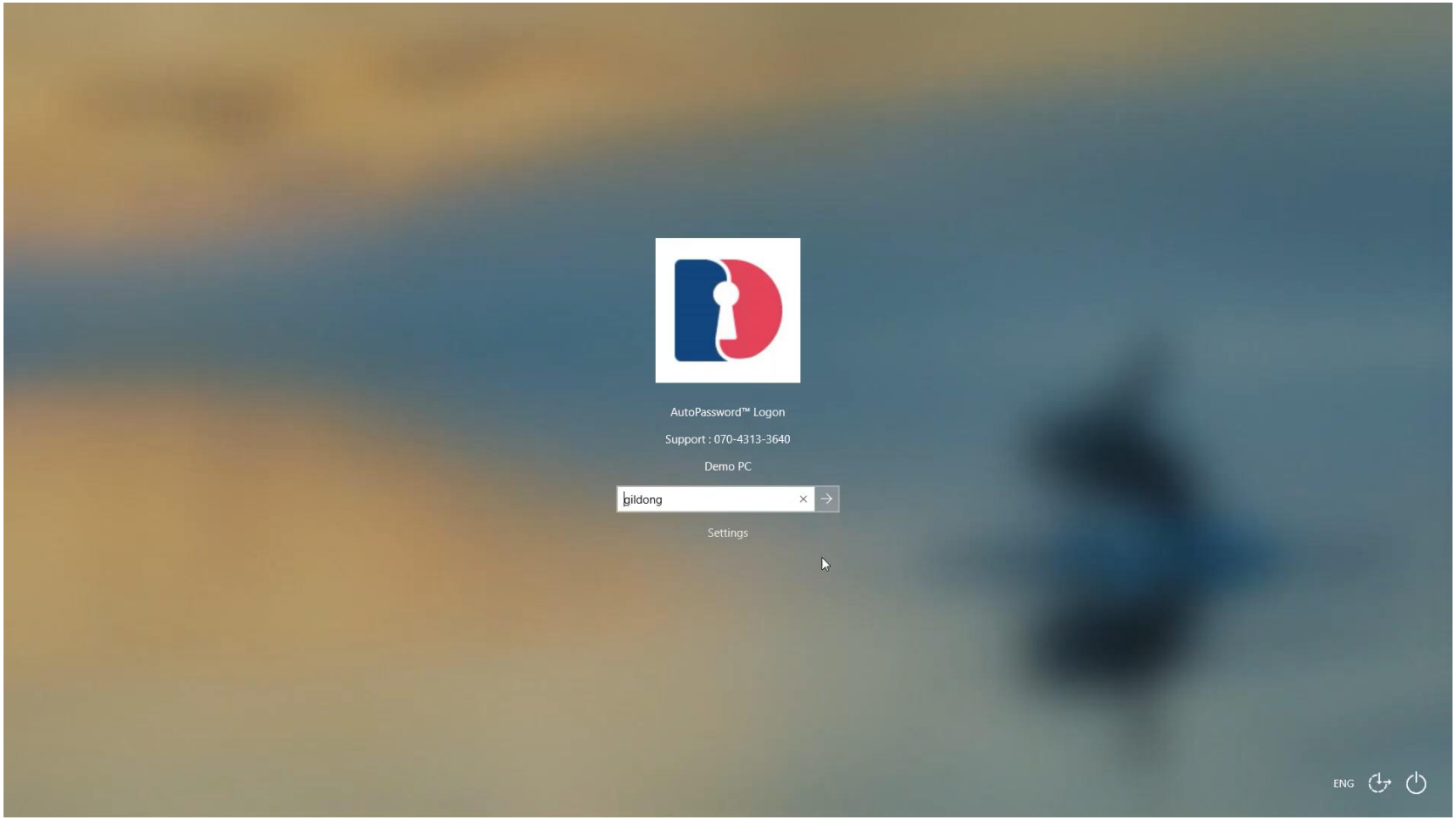
AutoPassword™


Demo Bank - Demo Website for
DEMO BANK
Login
CHECKING | SAVINGS | CREDIT CARDS | HOME LOANS | AUTO LOANS
DEMO BANK
Personal Banking
Credit Cards
Corporate Banking
Banking Service
SMART BANKING
EXCHANGE RATE
CERTIFICATE CENTER
Financial Statement
Internet Banking FAQ
2018 1Q Consolidated Financial Statements 18-08-01
2018 1Q Consolidated Financial Statements 18-08-01
2017 4Q Non-consolidated Financial Statements 18-08-01
2017 4Q Consolidated Financial Statements 18-08-01
2017 3Q Non-consolidated Financial Statements 18-08-01
LATEST NEWS
SERVICE LINK

Verify Automatic Password by User



Windows Demo

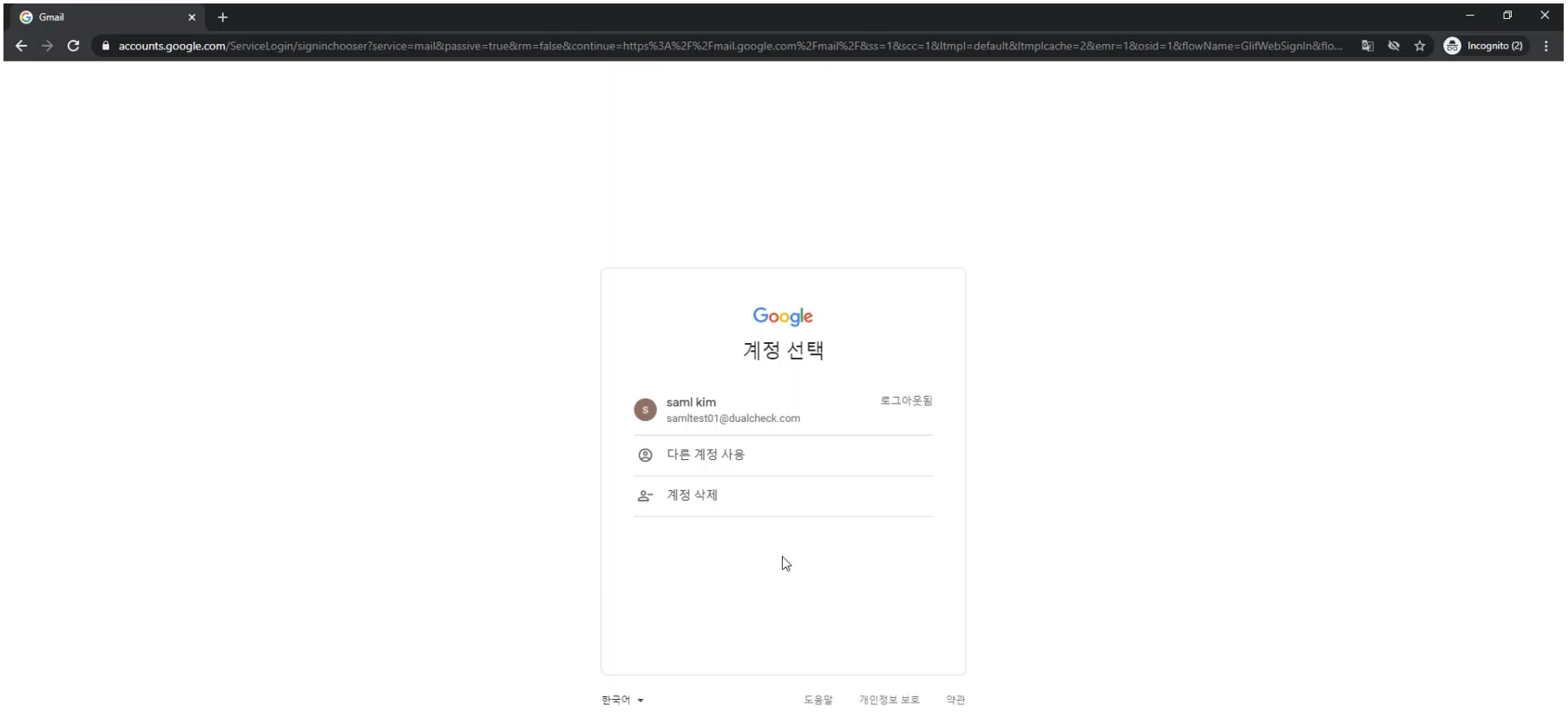


https://youtu.be/cjmjBDwgw00

Linux Demo

https://youtu.be/FDt0i06otUI

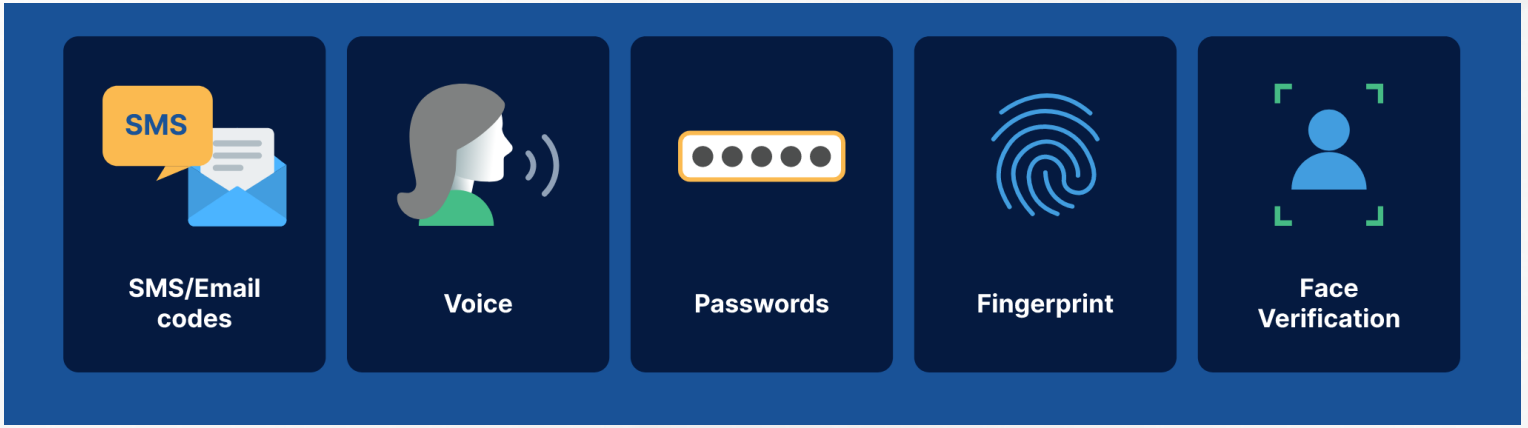
Cloud Demo

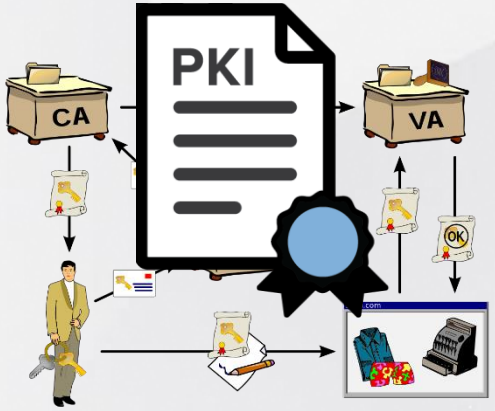


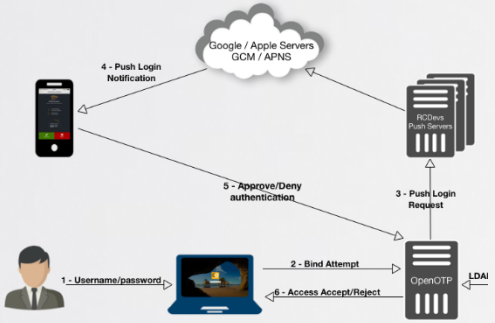
https://youtu.be/FDt0i06otUI

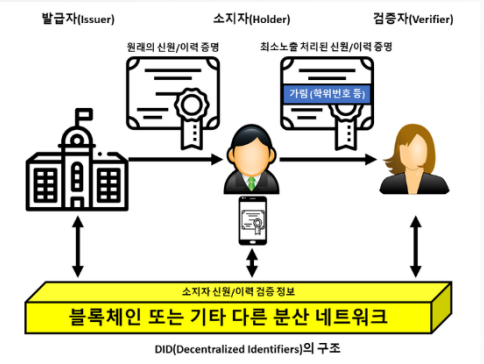

Service
Verification
1. Service Authentication by User
AutoPassword™
User
Service
2. User Authentication by Service

다른 인증기술과 무엇이 다르지?







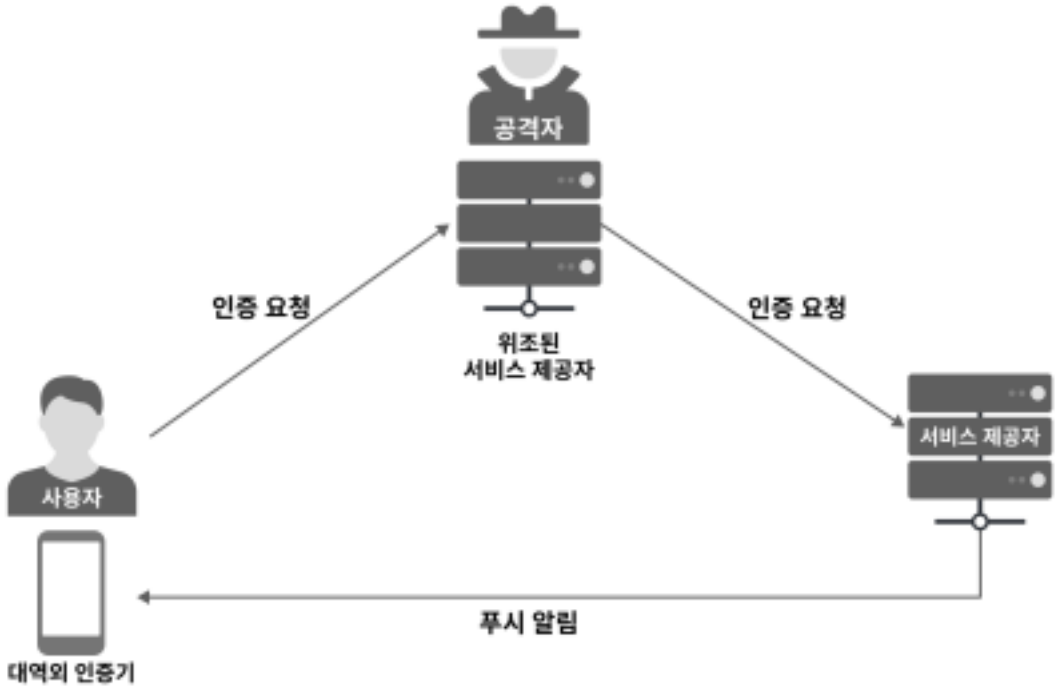


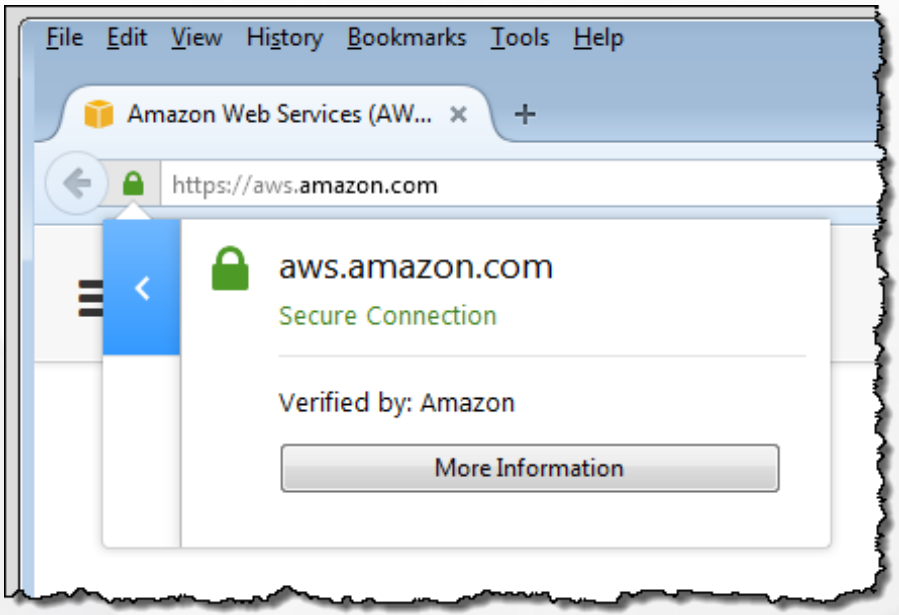
모든 사용자 인증 기술은

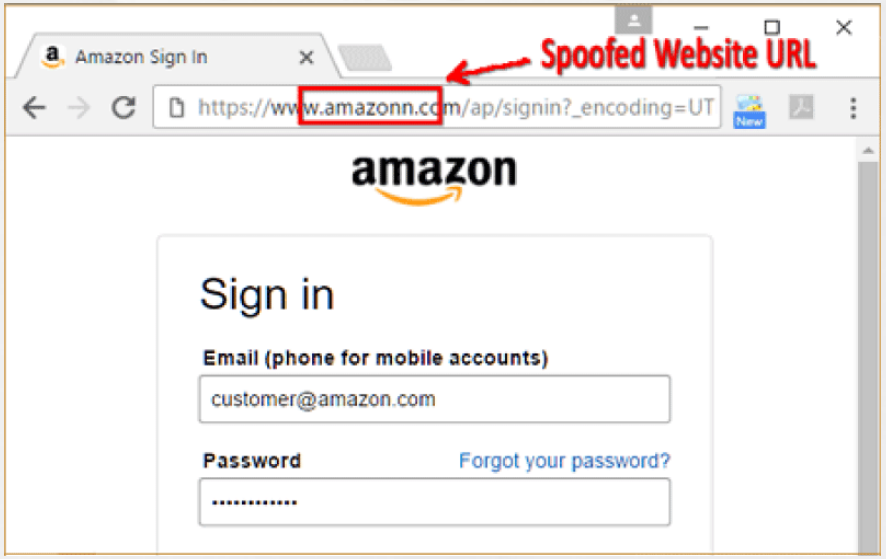
한가지 전제 조건하에서 작동한다

'파밍' 확산…해커에 넘어간 공인인증서

입력 2013.02.12 (07:11) | 수정 2013.02.12 (08:21) 뉴스광장

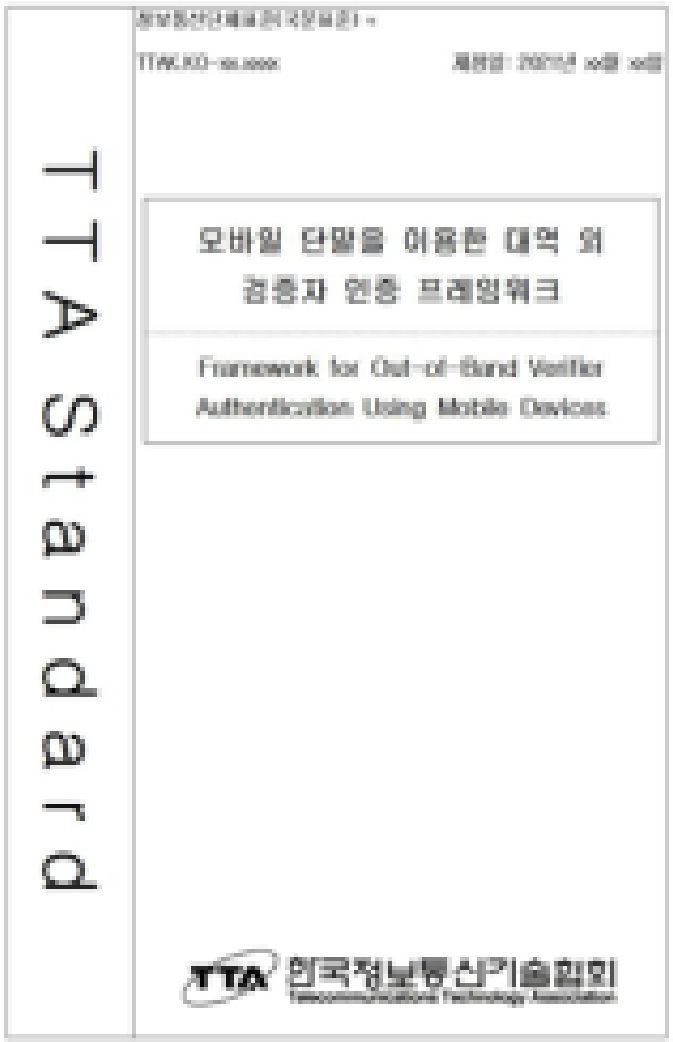

공격자
인증 요청
위조된
서비스 제공자
인증 요청
서비스 제공자
사용자
대역외 인증기
푸시 알림


File Edit View History Bookmarks Tools Help
Amazon Web Services (AW...
https://aws.amazon.com
aws.amazon.com
Secure Connection
Verified by: Amazon
More Information


Amazon Sign In
Spoofed Website URL
https://www.amazonn.com/ap/signin?_encoding=UT
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your password?


NAVER
KB국민은행
KB골든라이프
국민은행 정상 홈페이지는
주소창에 녹색음영이 확인됨

Figure 6 – Example of server verification information presentation


TTA Standard

정보통신단체표준(한국정보통신기술협회 표준)

TTAK.KO-xx.xxxx 제정일: 20xx년 xx월 xx일

모바일 단말을 이용한 대역 외
검증자 인증 프레임워크

Framework for Out-of-Band Verifier
Authentication Using Mobile Devices

TTA 한국정보통신기술협회
Telecommunications Technology Association


INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR

SG17-Cx
STUDY GROUP 17
Original: English

Question(s): 10/17 Virtual 24 August – 03 September 2021

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposed new work item: Framework for out-of-band verifier authentication using mobile devices

Purpose: Proposal

Contact: Jonghyun Woo
DataSeals
Korea (Republic of)
Tel: +82-10-3308-4017
Fax: +82-70-4313-3658
E-mail: jhwoo@dataseals.com

Contact: Heejun Shin
eStorm
Korea (Republic of)
Tel: +82-10-3367-3193
Fax: +82-70-4313-3658
E-mail: heeseo@estorm.co.kr

Contact: Il Ju Jung
eStorm
Korea (Republic of)
Tel: +82-10-7343-3602
Fax: +82-70-4313-3658
E-mail: ijjung@estorm.co.kr

Contact: Sejung Park
TTA
Korea (Republic of)
Tel: +82-10-3335-5998
Fax: +82-31-724-0109
E-mail: sjpark1@tta.or.kr

Keywords: authentication, verification, password, identification, phishing, pharming

Abstract: This Contribution proposes Q10/17 to consider establishing a new work item, about "Framework for out-of-band verifier authentication using mobile devices"

1. Overview

Authentication technologies are a fundamental technology that maintains trust between users and online service providers in the digital era. Diverse authentication technologies such as OTP, FIDO, and mobile push authentication have been developed and used widely considering secure, cost-effective, and convenient authentication. Accordingly, different authentication assurance levels have been classified for new authentication technologies in ITU-T X.1254, ISO/IEC 29115, and NIST 800-63-3.

As authentication technologies have been enhanced and standardized, providing verifier impersonation resistance is highly demanded to web or user authenticator. Authentication technologies that comply with the requirement are classified as the highest level.

However, since existing authentication technologies authenticate users only, there is a limitation providing only the user authentication information to the verifier without users to verify it explicitly for verifier impersonation resistance.

AutoPassword™

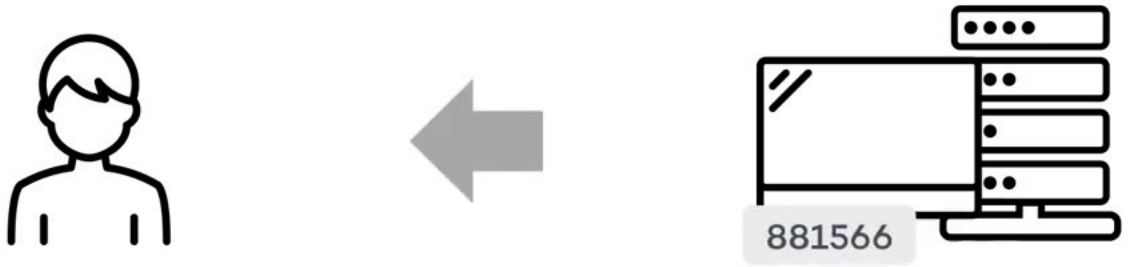
서비스 제공자를 확인 한 이후 사용자를 인증하는

상호인증기술

AutoPassword™

피싱이나 파밍 공격에 탈취나 도용 될 수 없는 기술

Output - Based Device Credential



one time code to the user first, and then makes users verify that code with the code on their smartphone.


대한민국
청 와 대


통계청


동두천시


우리은행

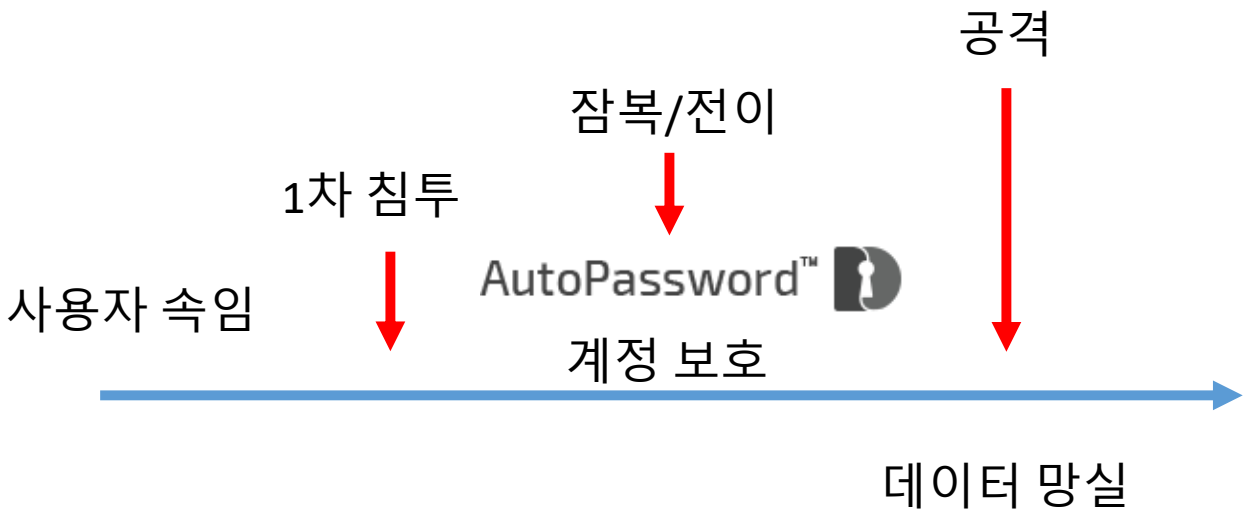

건설근로자공제회
Construction Workers Mutual Aid Association


브이피(주)

실수하더라도

데이터를 보호할 수 있는 방법

1차 침투 이후 직접 데이터를 공격하면?

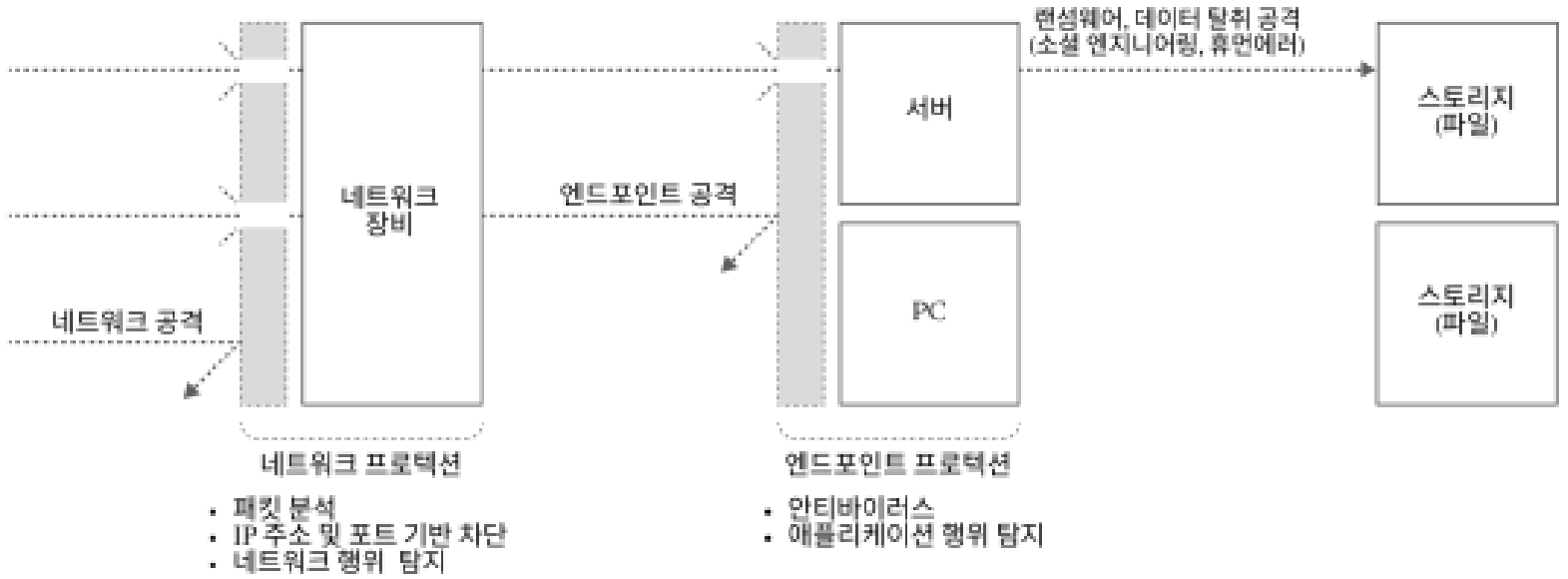


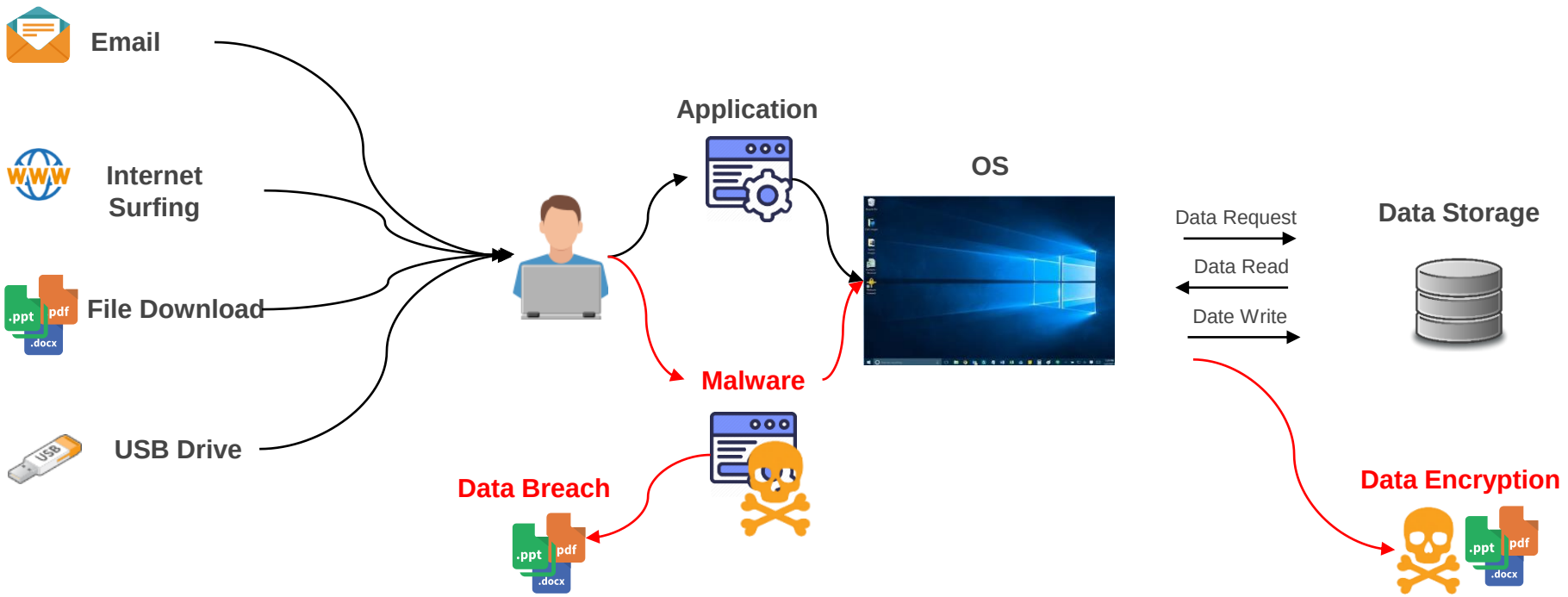
얼마나 자주 백업을 하나요?

임직원이 실수하더라도

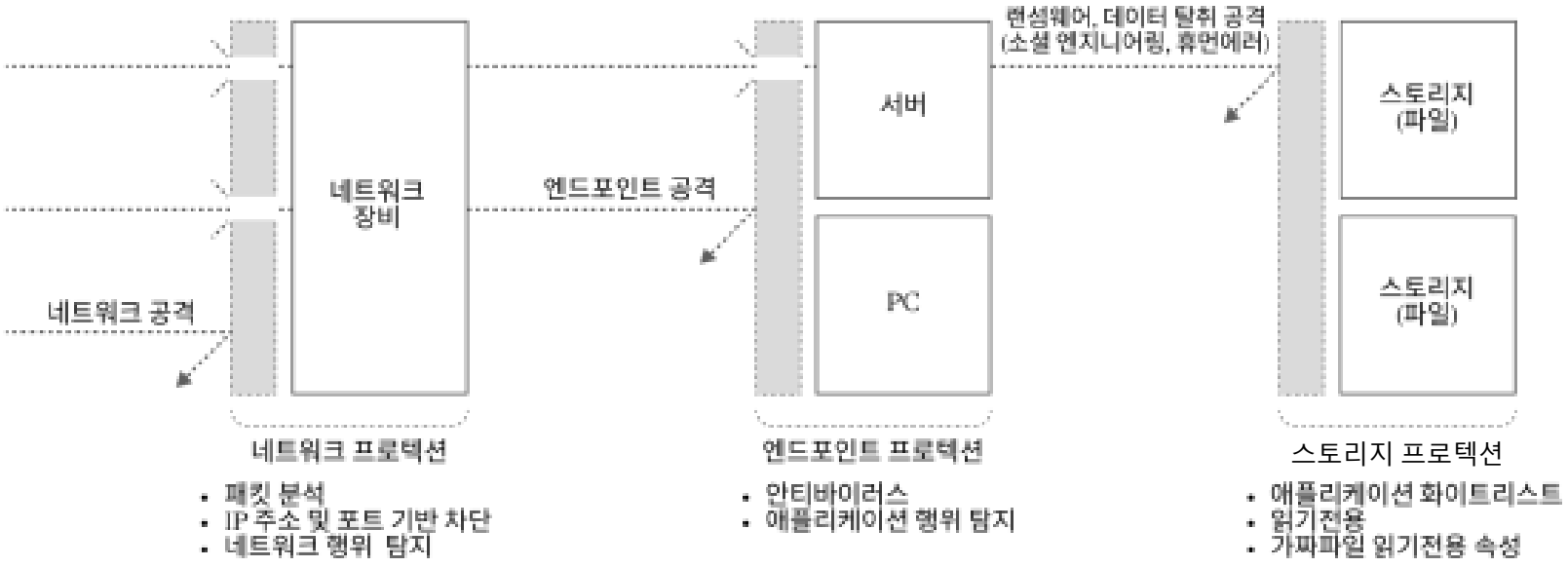
사전에 데이터를

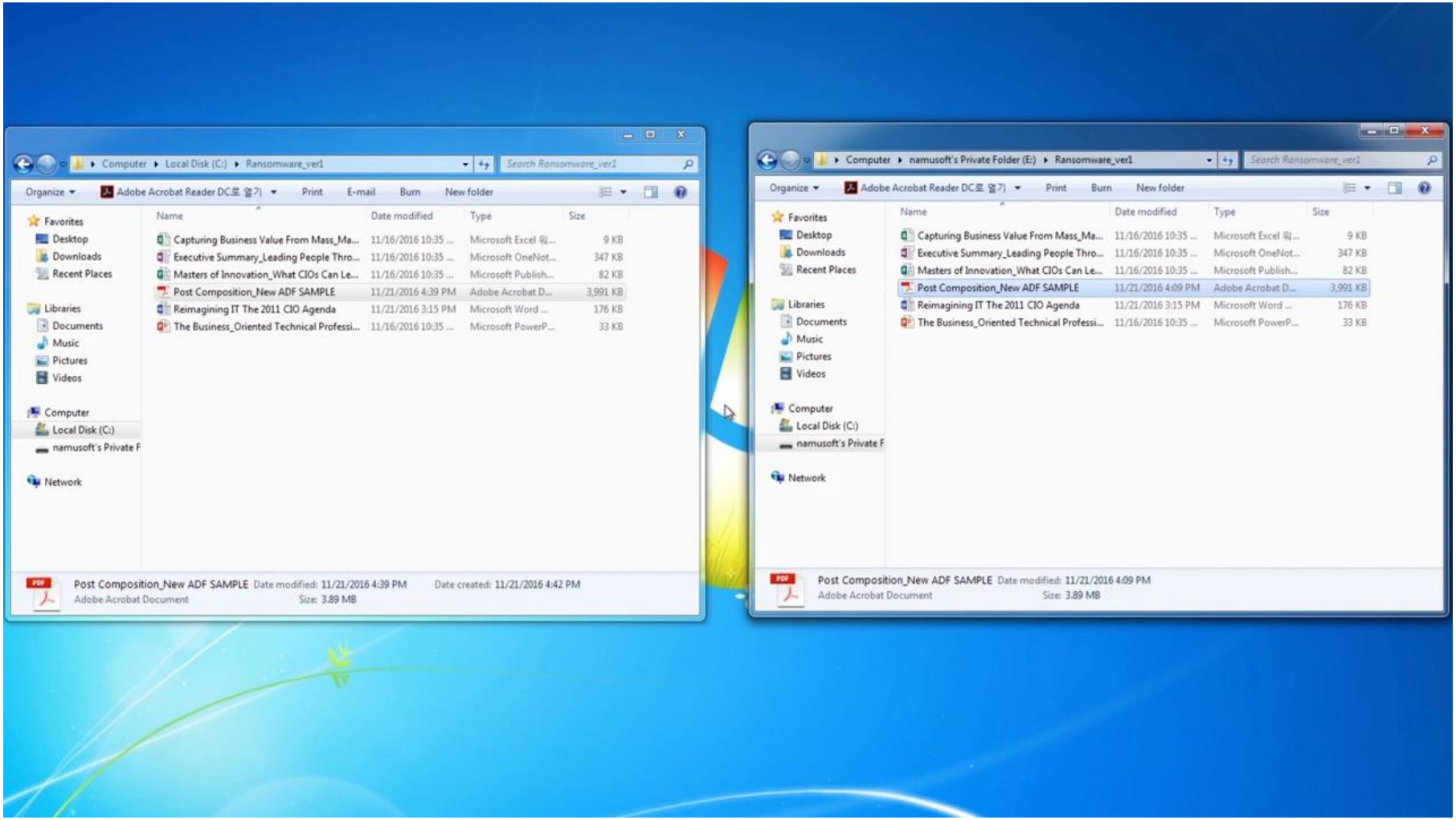
보호할 수 있는 방법은?

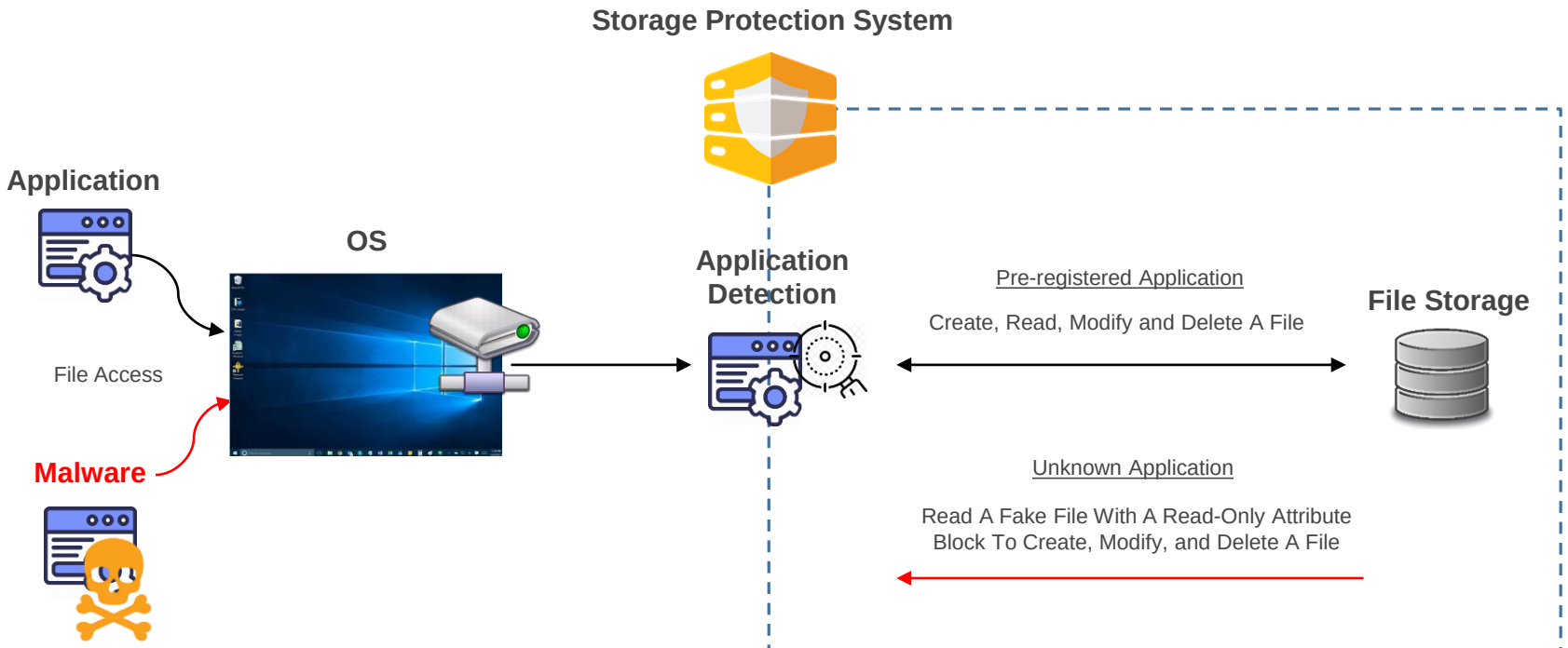

랜섬웨어, 데이터 탈취 공격
(소셜 엔지니어링, 휴먼에러)
네트워크
장비
엔드포인트 공격
서버
스토리지
(파일)
PC
스토리지
(파일)
네트워크 공격
네트워크 프로텍션
엔드포인트 프로텍션
• 패킷 분석
• IP 주소 및 포트 기반 차단
• 네트워크 행위 탐지
• 안티바이러스
• 애플리케이션 행위 탐지

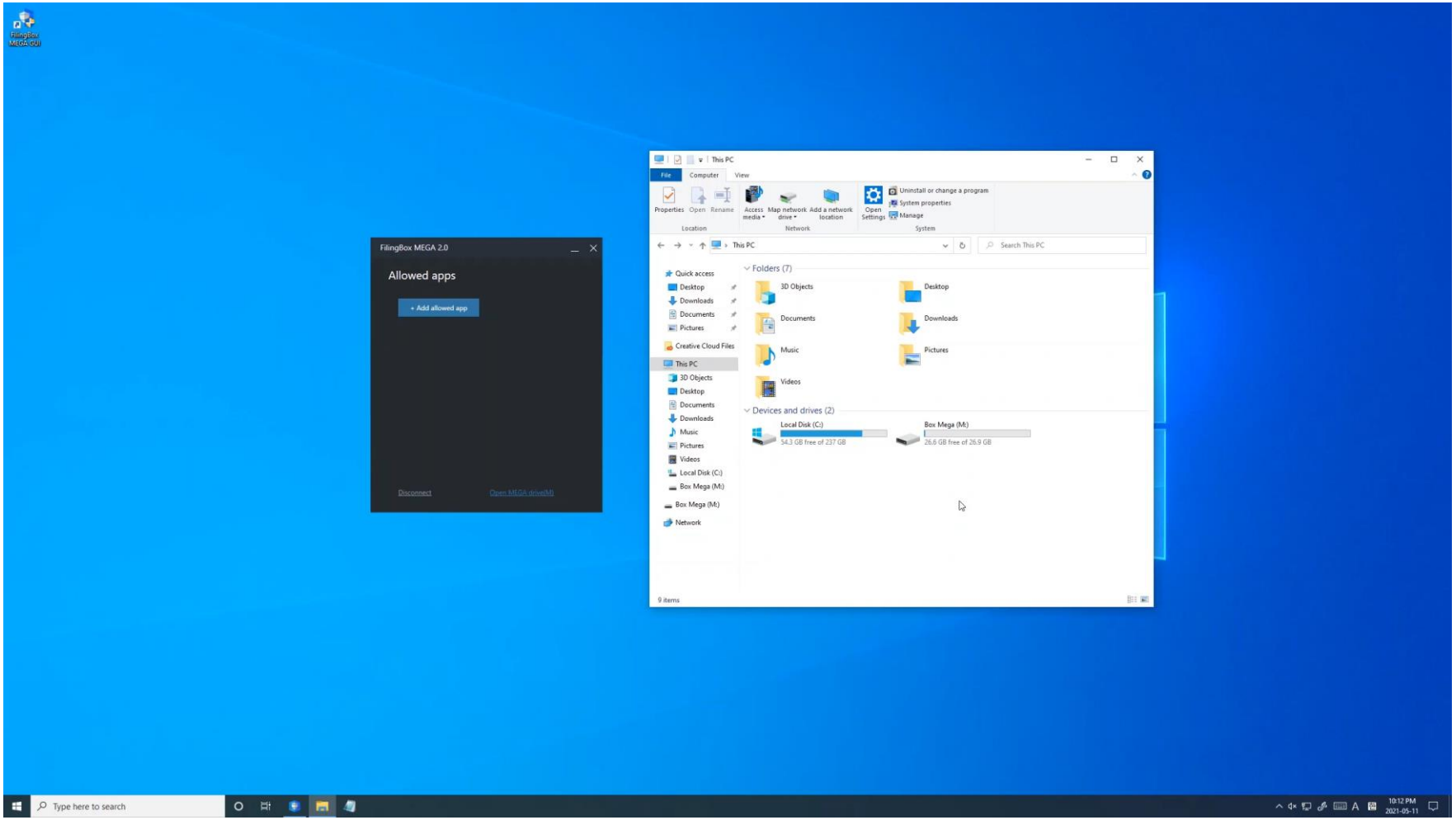

Email
Internet Surfing
File Download
USB Drive
Application
OS
Malware
Data Breach
Data Request
Data Read
Date Write
Data Storage
Data Encryption

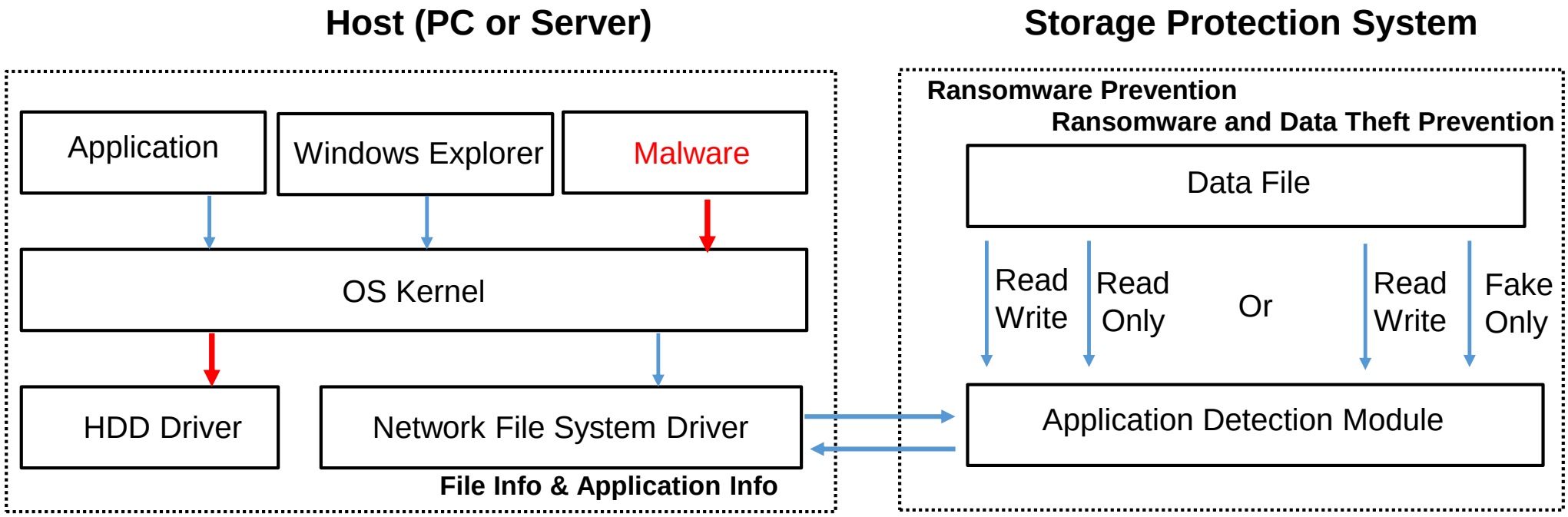

FILINGBOX


랜섬웨어, 데이터 탈취 공격
(소셜 엔지니어링, 휴먼에러)
네트워크
장비
엔드포인트 공격
서버
PC
스토리지
(파일)
스토리지
(파일)
네트워크 공격
네트워크 프로텍션
엔드포인트 프로텍션
스토리지 프로텍션
• 패킷 분석
• IP 주소 및 포트 기반 차단
• 네트워크 행위 탐지
• 안티바이러스
• 애플리케이션 행위 탐지
• 애플리케이션 화이트리스트
• 읽기전용
• 가짜파일 읽기전용 속성


Computer ▸ Local Disk (C:) ▸ Ransomware_ver1
Search Ransomware_ver1
Organize
Adobe Acrobat Reader DC로 열기
Print
E-mail
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
namusoft's Private F
Network
Name
Date modified
Type
Size
Capturing Business Value From Mass_Ma... 11/16/2016 10:35 ... Microsoft Excel 워... 9 KB
Executive Summary_Leading People Thro... 11/16/2016 10:35 ... Microsoft OneNot... 347 KB
Masters of Innovation_What CIOs Can Le... 11/16/2016 10:35 ... Microsoft Publish... 82 KB
Post Composition_New ADF SAMPLE 11/21/2016 4:39 PM Adobe Acrobat D... 3,991 KB
Reimagining IT The 2011 CIO Agenda 11/21/2016 3:15 PM Microsoft Word ... 176 KB
The Business_Oriented Technical Professi... 11/16/2016 10:35 ... Microsoft PowerP... 33 KB
Post Composition_New ADF SAMPLE Date modified: 11/21/2016 4:39 PM Date created: 11/21/2016 4:42 PM
Adobe Acrobat Document Size: 3.89 MB
Computer ▸ namusoft's Private Folder (E:) ▸ Ransomware_ver1
Search Ransomware_ver1
Organize
Adobe Acrobat Reader DC로 열기
Print
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
namusoft's Private F
Network
Name
Date modified
Type
Size
Capturing Business Value From Mass_Ma... 11/16/2016 10:35 ... Microsoft Excel 워... 9 KB
Executive Summary_Leading People Thro... 11/16/2016 10:35 ... Microsoft OneNot... 347 KB
Masters of Innovation_What CIOs Can Le... 11/16/2016 10:35 ... Microsoft Publish... 82 KB
Post Composition_New ADF SAMPLE 11/21/2016 4:09 PM Adobe Acrobat D... 3,991 KB
Reimagining IT The 2011 CIO Agenda 11/21/2016 3:15 PM Microsoft Word ... 176 KB
The Business_Oriented Technical Professi... 11/16/2016 10:35 ... Microsoft PowerP... 33 KB
Post Composition_New ADF SAMPLE Date modified: 11/21/2016 4:09 PM
Adobe Acrobat Document Size: 3.89 MB


Storage Protection System
Application
OS
Application Detection
File Storage
File Access
Malware
Pre-registered Application
Create, Read, Modify and Delete A File
Unknown Application
Read A Fake File With A Read-Only Attribute
Block To Create, Modify, and Delete A File


FilingBox MEGA GUI
FilingBox MEGA 2.0
Allowed apps
+ Add allowed app
Disconnect
Open MEGA drive(M)
This PC
File
Computer
View
Properties
Open
Rename
Access media
Map network drive
Add a network location
Open Settings
Uninstall or change a program
System properties
Manage
Location
Network
System
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Creative Cloud Files
This PC
3D Objects
Videos
Local Disk (C:)
Box Mega (M:)
Network
Folders (7)
Music
Devices and drives (2)
54.3 GB free of 237 GB
26.6 GB free of 26.9 GB
9 items
Type here to search
10:12 PM
2021-05-11


Host (PC or Server)
Storage Protection System
Application
Windows Explorer
Malware
OS Kernel
HDD Driver
Network File System Driver
File Info & Application Info
Ransomware Prevention
Ransomware and Data Theft Prevention
Data File
Read Write
Read Only
Or
Read Write
Fake Only
Application Detection Module

TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-xx.xxxx 제정일: 2022년 xx월 xx일

호스트 내 멀웨어 공격으로부터 스토리지를 보호하기 위한 보안 프레임워크

Security Framework for Storage Protection Against Malware Attacks on Hosts

한국정보통신기술협회
Telecommunications Technology Association

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-Cn
STUDY GROUP 17
Original: English

Question(s): 4/17 Virtual, 10-20 May 2022

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposal for new work item: Security framework for storage protection against malware attacks on hosts

Contact: Jonghyun Woo, DualAuth, Korea (Republic of) Tel: +82-10-3386-4017 E-mail: jhwoo@dualauth.com

Contact: Bongchan Kim, Namusoft, Korea (Republic of) Tel: +82-10-9530-5213 E-mail: kbchani@namusoft.co.kr

Contact: Heejun Shin, eStorm, Korea (Republic of) Tel: +82-10-5387-2153 E-mail: heejun@estorm.co.kr

Contact: Jonghyun Kim, ETRI, Korea (Republic of) Tel: +82-42-860-6576 E-mail: jhk@etri.re.kr

Contact: Sujung Park, TTA, Korea (Republic of) Tel: +82-10-5110-5098 E-mail: sjpark@tta.or.kr

Contact: Heung-Ryong Oh, TTA, Korea (Republic of) Tel: +82-70-7780-0083 E-mail: hroh@tta.or.kr

Abstract: This Contribution proposes Q4/17 to consider establishing a new work item about "Security framework for storage protection against malware attacks on hosts"

1. Overview

Malware attacks that encrypt, tamper, or steal data on hosts are on the rise. To protect data on hosts from such malware attacks, network protection and endpoint protection technologies have been adopted. But those protection technologies may not be enough against them.

Network protection technologies work based on whitelist-based and behaviour-based detection mechanism. Whitelist-based detection works by comparing every traffic on the network with the whitelist and inspecting every packet. If the attacks start with the approved network or encrypted data packets, it easily bypasses the whitelist-based detection mechanism. To overcome the limitations of whitelist-based mechanism, behaviour-based detection mechanism including AI technology has been adopted, but it is resource-intensive and inevitably less accurate.

If the network protection is compromised, endpoint protection should protect data on hosts. However, endpoint protection technologies work based on blacklist-based and behaviour-based detection


통계청


KNOC
한국석유공사


인천광역시 남동구
Namdong-Gu, Incheon


NH투자증권


MIRAE ASSET
미래에셋생명


광주광역시북구

정보 보안 예산 만드는 방법

사고가 안 나야 한다

1. 명분

2. 다른 보안 담당자의 구입 순서

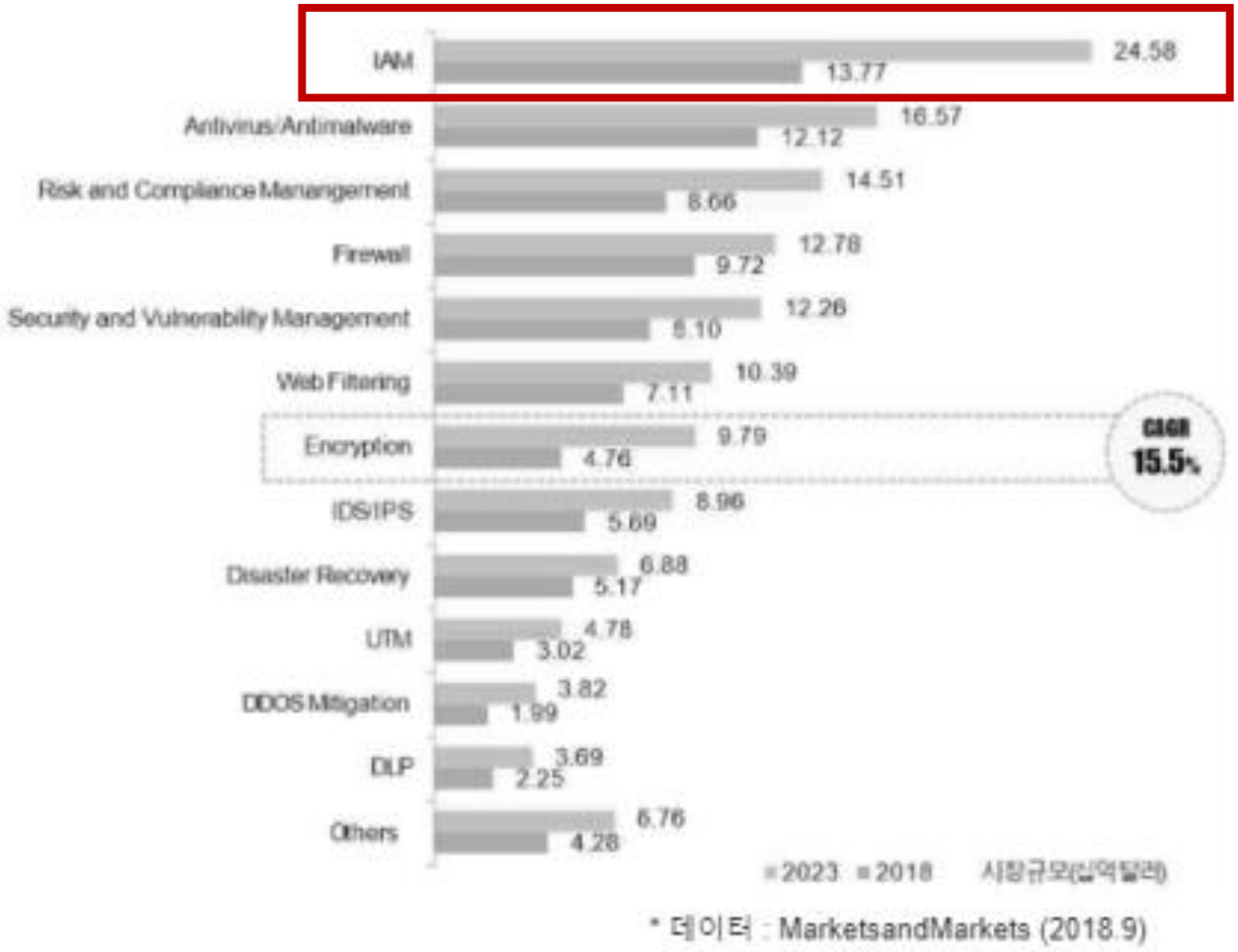
3. 공공기관/기업에서 할인 받는 방법

4. 무료로 사용하는 방법

사고는 보안담당자가 아닌 임직원 실수로 발생한다

실수하더라도 계정과 데이터를 보호하는 기술

정보 보안 제품별 시장 규모



파일링박스 조달 품목으로 등록

파일링박스는 기술의 혁신성을 인정받아 우선구매 조달 물품으로 등록되어 있으며, 습니다.

[조달 우선 구매 조달 물품]

[공공기관의 조달 제품 구매 혜택]

1. 수의계약 근거

혁신제품은 수의계약을 통해 구매할 수 있음

* 법적 근거 : 「국가계약법 시행령」 제26조 제1항 제5호 사목

「지방계약법 시행령」 제25조 제1항 제8호 다 · 자목

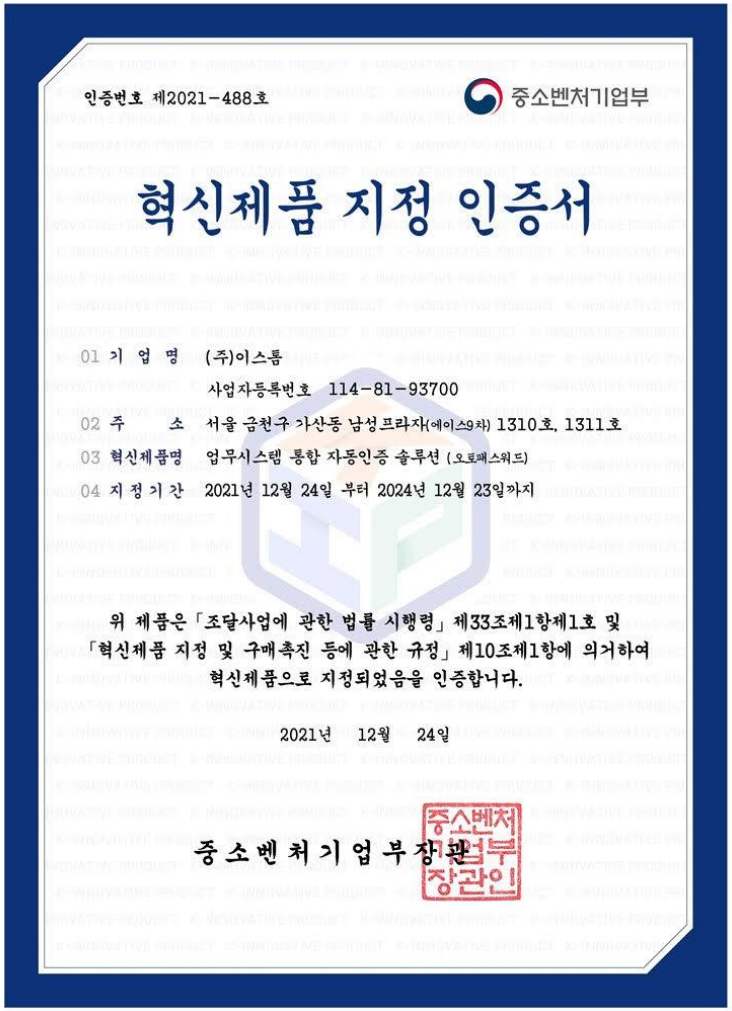
2. 구매 면책

혁신제품을 구매한 수요기관의 구매책임자는 고의나 중대한 과실이 입증되지 아니하면 그 제품의 구매로 생긴 손실에 대하여 책임을 지지 않음

* 법적 근거 : 「조달사업에 관한 법률」 제27조 제4항

오토패스워드 조달청 조달물품 및 혁신제품 지정

오토패스워드는 기술의 혁신성을 인정받아 2021년 12월 조달 혁신제품으로 지정되었습니다.



인증번호 제2021-488호

중소벤처기업부

혁신제품 지정 인증서

01 기 업 명 (주)이스룸
사업자등록번호 114-81-93700
02 주 소 서울 금천구 가산동 남성프라자(에이스9차) 1310호, 1311호
03 혁신제품명 업무시스템 통합 자동인증 솔루션 (오토패스워드)
04 지 정 기 간 2021년 12월 24일 부터 2024년 12월 23일까지

위 제품은 「조달사업에 관한 법률 시행령」 제33조제1항제1호 및
「혁신제품 지정 및 구매촉진 등에 관한 규정」 제10조제1항에 의거하여
혁신제품으로 지정되었음을 인증합니다.

2021년 12월 24일

중소벤처기업부장관

중소벤처기업부 장관인

[혁신제품 지정 인증서]

[공공기관의 혁신 제품 구매 혜택]

1. 수의계약 근거

혁신제품은 수의계약을 통해 구매할 수 있음

* 법적 근거 : 「국가계약법 시행령」 제26조 제1항 제5호 사목
「지방계약법 시행령」 제25조 제1항 제8호 다 · 자목

2. 구매 면책

혁신제품을 구매한 수요기관의 구매책임자는 고의나 중대한 과실이 입증되지 아니하면 그 제품의 구매로 생긴 손실에 대하여 책임을 지지 않음

* 법적 근거 : 「조달사업에 관한 법률」 제27조 제4항

3. 기관평가 반영

기관별 총 물품구매액의 1.6%(지자체 0.8%)를 혁신제품 구매에 활용하고 실제 구매실적을 기관평가에 반영

* 혁신구매액 인정범위 : 혁신제품 구매액 + 기타혁신구매(경진대회 · 공모사업 상금 및 공공부문 R&D 결과물구매액 등)
* 정부혁신평가(중앙부처), 지방자치단체 합동평가(지자체), 공기업 및 준정부기관 경영평가, 지방공기업 경영평가
* 평가항목 및 지표, 측정기준 등 세부사항은 기관별 평가계획 참조

수요 기업 가입 (사업신청) | 공급 기업 가입 신청 | 로그인

2022 클라우드서비스 지원포털

클라우드 솔루션 빨리 찾기

클라우드 서비스란 | 공급기업 가이드 | 수요기업 가이드 | 서비스검색 | 알림마당

2022 클라우드서비스 이용지원(바우처)사업

전국 중소기업 업무환경의 디지털 전환을 위해
클라우드서비스 “도입 컨설팅” 및 “전환 이용료”를 지원하여
클라우드 기반의 디지털 전환 촉진 등 국내 산업경쟁력 강화

자세히 보기

공지사항 더보기

- 2022년 클라우드 서비스 수요기업 사업 신청
- 수요기업 가입(사업신청) 매뉴얼
- 공급기업 가입신청 매뉴얼

홍보게시판 더보기

- 2021년 클라우드 서비스 우수사례 (영상)
- 2021년 클라우드 서비스 성과공유회 (영상)
- 2021년 클라우드 서비스 우수사례집

상담지원센터

031-628-9653
031-628-9656
031-628-9696

부정수급 신고 : help112@cloudsup.or.kr

과학기술정보통신부 | nipa 정보통신산업진흥원 National IT Industry Promotion Agency | INNOBIZ 이노비즈협회 | KACI 한국클라우드산업협회 Korea Association of Cloud Industry

정부지원 신청현황
신청접수금액 :
0원
신청가능금액 :
9,590,000,000원

파일링박스 (FilingBOx)

파일링박스 클라우드는 랜섬웨어에 의한 데이터 피해를 원천 차단하는 특허 기술을 기반으로 안

- 업체명 : (주)나무소프트
- 담당자명 : 김효동
- 연락처 : 02-6925-1304

업체 정보

업체명	(주)나무소프트	기업구분	중소기업
사업자등록번호	1078656191	웹사이트주소	
업종		분야	
대표자명	우종현	대표번호	02-6925-0471
담당자명	김효동	담당자직급	실장
담당자연락처	02-6925-0471	담당자이메일	biz@filingbox.com
기업소개			

오토패스워드 액세스 매니저

오토패스워드 액세스 매니저는 사용자가 암호를 입력할 필요가 없이, PC나 서버가 스스로 자

- 업체명 : (주)이스톰
- 담당자명 : 신희준
- 연락처 : 02-6925-0290

간략 정보 | 솔루션 상세 | 가격 정책 | 도입 사례

업체 정보

업체명	(주)이스톰	기업구분	중소기업
사업자등록번호	1148193700	웹사이트주소	www.estorm.co.kr
업종	지식서비스업	분야	
대표자명	우종현	대표번호	02-6925-0290
담당자명	신희준	담당자직급	실장
담당자연락처	02-6925-0290	담당자이메일	biz@autopassword.com
기업소개			

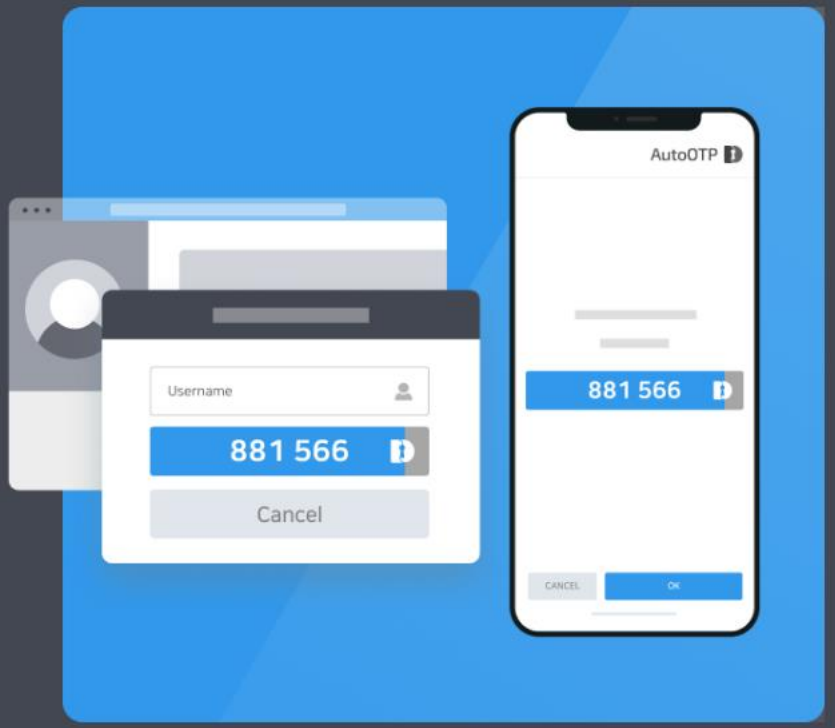
www.AutoOTP.com

AutoOTP

문의하기

아직도 OTP코드를 입력하나요?
OTP코드 입력 방식은 피싱이나 파밍 공격에 취약할뿐만 아니라 매번 입력하기 불편합니다.

자동으로 OTP가 제시되는 AutoOTP를 사용해 보세요 편리하고 안전한 AutoOTP는 모든 온라인 서비스에 무료로 제공됩니다.



감사합니다

Booth Q59

문의
02-6925-1304
support@filingcloud.co.kr