

·||· Recorded Future®

ASM 고객 도입 사례

2024년 2월 6일

윤광택 상무/Recorded Future Korea



공격접점(Attack Surface)

External ASM

External Attack Surface Management

인터넷에 노출된 자산을 식별하고 위험을 관리에 도움을 주는 솔루션

북한 라자루스 해킹 그룹 최근 1년 TTP

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire (0/7)	Drive-by (0/9)	Command and Control (0/13)	Account (0/19)	Abuse Elevation (0/13)	Abuse Elevation (0/42)	Adversary-in- (0/17)	Account (0/30)	Exploitation of (0/9)	Adversary-in- (0/17)	Application (0/16)	Automated (0/9)	Account Access (0/13)
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application (0/7)	Interpreter (0/13)	BITS Jobs (0/19)	Mechanism (0/13)	Mechanism (0/42)	Brute Force (0/17)	Application Window Discovery (0/30)	Services (0/9)	Archive Collected Data (0/17)	Protocol (0/16)	Data Transfer Size Limits (0/9)	Data Destruction (0/13)
Gather Victim Identity Information (0/4)	Compromise Infrastructure (0/7)	External Remote Services (0/9)	Container Administration Command (0/13)	Boot or Logon Autostart Execution (0/19)	Access Token Manipulation (0/13)	Access Token Manipulation (0/42)	Credentials From Password Stores (0/17)	Browser Bookmark Discovery (0/30)	Internal Spearphishing (0/9)	Communication Through Removable Media (0/17)	Exfiltration Over Alternative Protocol (0/16)	Data Encrypted for Impact (0/9)	Data Encrypted for Impact (0/13)
Gather Victim Network Information (0/6)	Develop Capabilities (0/7)	Hardware Additions (0/9)	Deploy Container (0/13)	Boot or Logon Initialization Scripts (0/19)	Boot or Logon Autostart Execution (0/13)	BITS Jobs (0/42)	Exploitation for Credential Access (0/17)	Cloud Infrastructure Discovery (0/30)	Lateral Tool Transfer (0/9)	Audio Capture (0/17)	Data Encoding (0/16)	Data Manipulation (0/9)	Data Manipulation (0/13)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/9)	Exploitation for Client Execution (0/13)	Browser Extensions (0/19)	Boot or Logon Initialization Scripts (0/13)	Build Image on Host (0/42)	Forced Authentication (0/17)	Cloud Service Dashboard (0/30)	Remote Service Session Hijacking (0/9)	Automated Collection (0/17)	Data Obfuscation (0/16)	Exfiltration Over C2 Channel (0/9)	Defacement (0/13)
Phishing for Information (0/3)	Obtain Capabilities (0/7)	Replication Through Removable Media (0/9)	Inter-Process Communication (0/13)	Native API (0/19)	Create or Modify System Process (0/13)	Debugger Evasion (0/42)	Forge Web Credentials (0/17)	Cloud Service Discovery (0/30)	Remote Services (0/9)	Browser Session Hijacking (0/17)	Dynamic Resolution (0/16)	Disk Wipe (0/9)	Disk Wipe (0/13)
Search Closed Sources (0/2)	Stage Capabilities (0/7)	Supply Chain Compromise (0/9)	Scheduled Task/Job (0/13)	Compromise Client Software Binary (0/19)	Domain Policy Modification (0/13)	Diobfuscate/Decode Files or Information (0/42)	Input Capture (0/17)	Cloud Storage Object Discovery (0/30)	Replication Through Removable Media (0/9)	Clipboard Data (0/17)	Encrypted Channel (0/16)	Endpoint Denial of Service (0/9)	Endpoint Denial of Service (0/13)
Search Open Technical Databases (0/5)	Trusted Relationship (0/7)	Valid Accounts (0/9)	Serverless Execution (0/13)	Create Account (0/19)	Escape to Host (0/13)	Direct Volume Access (0/42)	Modify Authentication Process (0/17)	Container and Resource Discovery (0/30)	Data from Cloud Storage (0/9)	Data from Configuration Repository (0/17)	Fallback Channels (0/16)	Firmware Corruption (0/9)	Firmware Corruption (0/13)
Search Open Websites/Domains (0/3)	Valid Accounts (0/7)	System Services (0/9)	Software Deployment Tools (0/13)	Event Triggered Execution (0/19)	Event Triggered Execution (0/13)	Execution Guardrails (0/42)	Multi-Factor Authentication Interception (0/17)	Debugger Evasion (0/30)	Software Deployment Tools (0/9)	Data from Information Repositories (0/17)	Ingress Tool Transfer (0/16)	Network Denial of Service (0/9)	Network Denial of Service (0/13)
Search Victim-Owned Websites (0/3)	User Execution (0/7)	User Execution (0/9)	Windows Management Instrumentation (0/13)	External Remote Services (0/19)	Hijack Execution Flow (0/13)	File and Directory Permissions Modification (0/42)	Multi-Factor Authentication Request Generation (0/17)	Domain Trust Discovery (0/30)	Taint Shared Content (0/9)	Data from Local System (0/17)	Multi-Stage Channels (0/16)	Scheduled Transfer (0/9)	Resource Hijacking (0/13)
				Hijack Execution Flow (0/19)	Process Injection (0/13)	Hide Artifacts (0/42)	Network Sniffing (0/17)	File and Directory Discovery (0/30)	Use Alternate Authentication Material (0/9)	Data from Network Shared Drive (0/17)	Non-Application Layer Protocol (0/16)	Transfer Data to Cloud Account (0/9)	System Shutdown/Reboot (0/13)
				Implant Internal Image (0/19)	Scheduled Task/Job (0/13)	Hijack Execution Flow (0/42)	OS Credential Dumping (0/17)	Group Policy Discovery (0/30)		Data from Removable Media (0/17)	Non-Standard Port (0/16)		
				Modify Authentication Process (0/19)	Valid Accounts (0/13)	Indicator Removal (0/42)	Network Sniffing (0/17)	Network Service Discovery (0/30)		Data Staged (0/17)	Proxy (0/16)		
				Office Application Startup (0/19)	Masquerading (0/13)	Indirect Command (0/42)	Steal Application Access Token (0/17)	Network Share Discovery (0/30)		Email Collection (0/17)	Remote Access Software (0/16)		
				Pre-OS Boot (0/19)	Modify Authentication Process (0/13)	Modify Authentication Process (0/42)	Steal or Forge Kerberos Tickets (0/17)	Password Policy Discovery (0/30)		Input Capture (0/17)	Traffic Signaling (0/16)		
				Scheduled Task/Job (0/19)	Modify Cloud Compute Infrastructure (0/13)	Modify System Image (0/42)	Steal Web Session Cookie (0/17)	Peripheral Device Discovery (0/30)		Screen Capture (0/17)	Web Service (0/16)		
				Server Software Component (0/19)	Modify Registry (0/13)	Network Boundary Bridging (0/42)	Unsecured Credentials (0/17)	Permission Groups Discovery (0/30)		Video Capture (0/17)			
				Traffic Signaling (0/19)	Network Boundary Bridging (0/13)	Obfuscated Files or Information (0/42)	System Information Discovery (0/17)	Query Registry (0/30)					
				Valid Accounts (0/19)	Obfuscated Files or Information (0/13)			Remote System Discovery (0/30)					
								Software Discovery (0/30)					
								System Information Discovery (0/30)					

legend

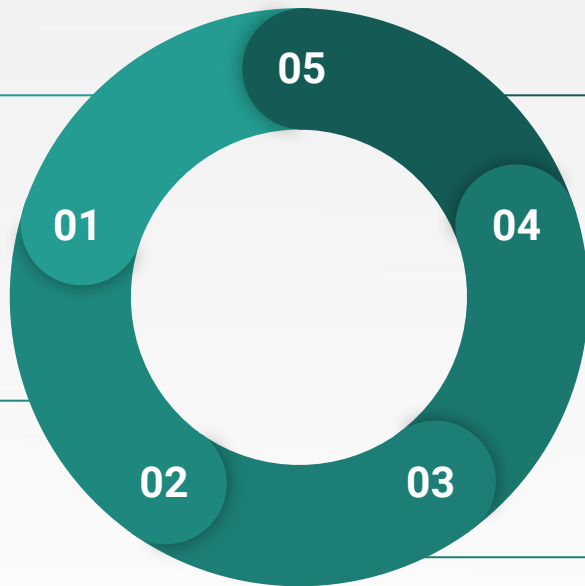
ASM Lifecycle

1. 자산대상식별

기업의 자산 식별 (데이터센터/클라우드)
Managed/Unmanaged
Shadow IT

2. 호스트/IP/Port

외부접근 가능여부
접근 가능한 포트



5. 조치

패치/설정변경/접근제어 등

4. 취약점/설정오류

CVE/Misconfiguration 스캐닝

3. 애플리케이션 식별

Version 식별에 따른 기술지원 종료 여부
확인

우리 회사의 자산중
외부에 노출된
자산은 무엇인가?

자산을 어떻게 찾아낼 것인가?

활용예) WHOIS 등록 정보

WHOIS도메인 대한민국 도메인 등록 1위 국내유일 일련치상위도메인 관리기관

DDoS 방어 초고성능 네임서버

신규등록 소유기간 연장 변경/이전 도메인 활용/부가서비스 브랜드관리/관심도메인 내 도메인 자산 관리 1:1 한일상담 전세계

로그인 회원가입 로그인 없이 도메인 연장하기 | 장바구니: 0

후이즈로 도메인 이전하면 스토릭스 커미 중징!

도메인 검색 / 등록

HOME > 신규등록 > 도메인 검색 / 등록

전화 안 통하면 신청서로 보내주세요! 1588-4259 (ARS 1:1)

● 등록할 도메인 선택

검색 도메인 선택 정보 입력 결제 신청 완료

- 전세계 실시간 검색결과로, 등록가능 도메인은 누구든지 먼저 등록할 수 있습니다.
- 도메인 선택 후 '할인가격 확인 / 등록신청' 버튼을 눌러 할인가격과 혜택을 확인하고 등록하세요.

검색결과	등록할 도메인 선택
등록불가	recordedfuture.kr 정보보기 바로가기 필수 2% 대한민국 대표 도메인
등록불가	recordedfuture.co.kr 정보보기 바로가기 필수 인기
등록불가	recordedfuture.com 정보보기 바로가기 필수 인기
등록불가	recordedfuture.net 정보보기 바로가기 필수 인기
등록불가	recordedfuture.io 정보보기 바로가기 추천 인기 글로벌 IT 스타트업 인기 도메인
등록불가	recordedfuture.ai 정보보기 바로가기 추천 인기 x 일론 마스크의 선택 x.ai

☒ 도메인 ☐ IP / 네임서버

검색 내역

recordedfuture.kr
recordedfuture.co.kr

Whois 정보 검색

도메인: **whois.co.kr** (www 없이 입력)
IP: **218.232.110.133** | 네임서버: **ns1.whois.co.kr**

recordedfuture.co.kr 후이즈 정보 검색 결과입니다.

인쇄하기 파일로 저장 웹사이트 확인 정보노출 차단

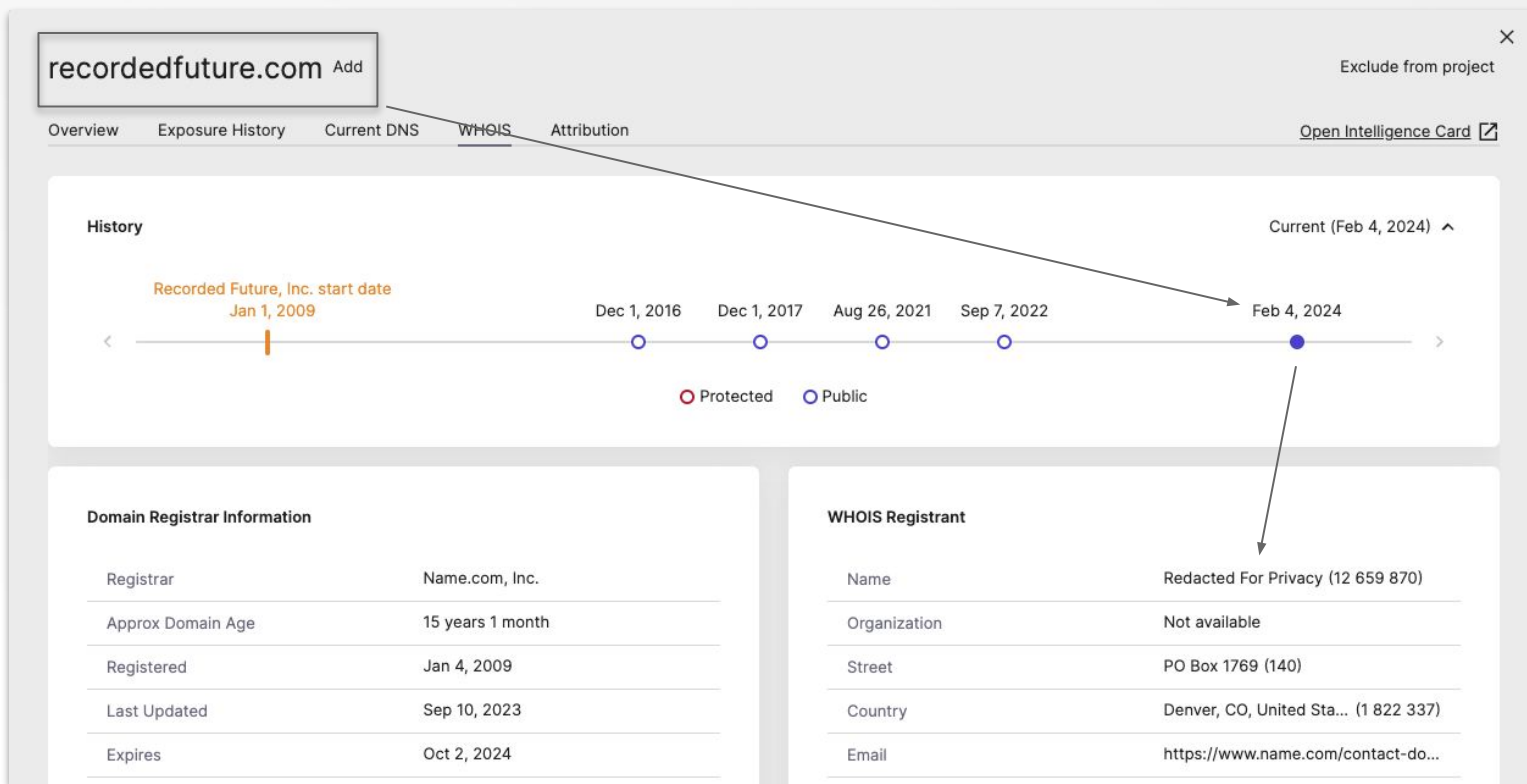
query : recordedfuture.co.kr

KOREAN(UTF8)

도메인이름 : recordedfuture.co.kr
등록인 : 도메인 관리자
등록인 주소 : 경기도 성남시 분당구 대왕판교로 660, 유스페이스1 B동 4층
등록인 우편번호 : 13494
책임자 : 도메인 관리자
책임자 전자우편 : gre0629107816@whoisprivacyservices.domains
책임자 전화번호 : +82.215444370
등록일 : 2017. 06. 29.
최근 정보 변경일 : 2017. 06. 29.
사용 종료일 : 2024. 06. 29.
정보공개여부 : Y
등록대행사 : (주)가비아(http://www.gabia.co.kr)
DNSSEC : 미서명

자산을 어떻게 찾아낼 것인가?

활용예) WHOIS 등록 정보



자산을 어떻게 찾아낼 것인가?

활용예) WHOIS 등록 정보

recordedfuture.com

Add

Exclude from project

OverviewExposure HistoryCurrent DNSWHOISAttribution

Open Intelligence Card

History

Dec 1, 2017

Recorded Future, Inc. start date
Jan 1, 2009

Dec 1, 2016Dec 1, 2017Aug 26, 2021Sep 7, 2022Feb 4, 2024

ProtectedPublic

Domain Registrar Information

Registrar	Name.com, Inc.
Approx Domain Age	
Registered	Dec 1, 2017
Last Updated	Nov 17, 2015
Expires	Oct 2, 2018

WHOIS Registrant

Name	Martin Forssen
Organization	Recorded Future
Street	Vstra Hamngatan 24
Country	Gteborg, n/a, SWEDEN
Email	operations@recordedfuture.com

자산을 어떻게 찾아낼 것인가?

활용 예) SSL 인증서의 등록 정보

The image shows a web browser window displaying the Recorded Future website. The URL in the address bar is recordedfuture.com/ko/. The website has a dark header with the Recorded Future logo and navigation links. The main content area features the text '위협 인텔리전' (Threat Intelligence) and '하기' (Doing). A popup window titled '인증서 뷰어: *.recordedfuture.com' (Certificate Viewer: *.recordedfuture.com) is overlaid on the page, showing detailed information about an SSL certificate. The popup includes tabs for '일반(G)' (General) and '세부정보(D)' (Details), with '일반(G)' selected. It lists the following information:

- 발급 대상 (Issued To):**
 - 일반 이름 (CN): *.recordedfuture.com
 - 조직 (O): Recorded Future, Inc
 - 조직 구성 단위 (OU): <인증서에 속하지 않음>
- 발급 기관 (Issued By):**
 - 일반 이름 (CN): DigiCert TLS RSA SHA256 2020 CA1
 - 조직 (O): DigiCert Inc
 - 조직 구성 단위 (OU): <인증서에 속하지 않음>
- 유효성 기간 (Validity Period):**
 - 발급일 (Issued): 2023년 2월 3일 금요일 오전 9:00:00
 - 만료일 (Expires): 2024년 3월 6일 수요일 오전 8:59:59
- SHA-256 지문 (SHA-256 Fingerprint):**
 - 인증서 (Certificate): 40d04c5828dc5dd8b70a332293cde38a42e72a97d5cb6161b8074a1d4f711944
 - 공개 키 (Public Key): d004ee033b0cd60872139749253599500f319e558f050d1b9211a3d0368dd171

자산을 어떻게 찾아낼 것인가?

Total Internet Inventory™ 에서 자산 식별

- **2억4천+ 호스트** 실시간 트래킹
- 580M+ 도메인 트래킹
 - 1500 TLDs 지원
 - gTLD/ccTLD
- 세계 최대 과거/현재 **DNS** 히스토리 아카이빙
- 지속적으로 IP 주소 스캔
- **10+ 년**, 아래 정보를 포함하는 구조화된 데이터 보유:
 - WHOIS
 - SSL Certificates
 - 현재 및 과거 DNS
 - IP 등록



IP 블록

기업에 등록된 IP블록 찾아보기
(모든 RIRs: ARIN, APNIC, 등등.)



SSL 인증서

인증서 투명성 로그 및 대량
스캔 인증서에 대해 쿼리



관련 도메인

회사 전체의 도메인
포트폴리오 확인



열려진 포트

노출된 앱 및 서비스에서
사용하는 열린 포트를 즉시
검색



Reverse DNS

PTR 레코드를 사용하여 더
많은 회사 인프라를 자동으로
검색




Forward DNS

어떤 도메인과 하위 도메인이
어떤 자산을 가리키는
포괄적인 목록을 가져오기

외부에 노출된 호스트명 **/IP/Port**

식별된 호스트명, **IP, Port**









































*recordedfuture.com

Inventory					
Hosting Report (63) <u>Inventory Tree</u> Hostnames pointing local (2) Remote Access (0) Admin Pages (0) VPNs (0)					
Domain	Total Hostnames	Total Active	Total Inactive	Total Recently Updated	Total Recently Discovered
 recordedfuture.com	96	<u>65</u>	<u>31</u>	2	0

96 vs. 65

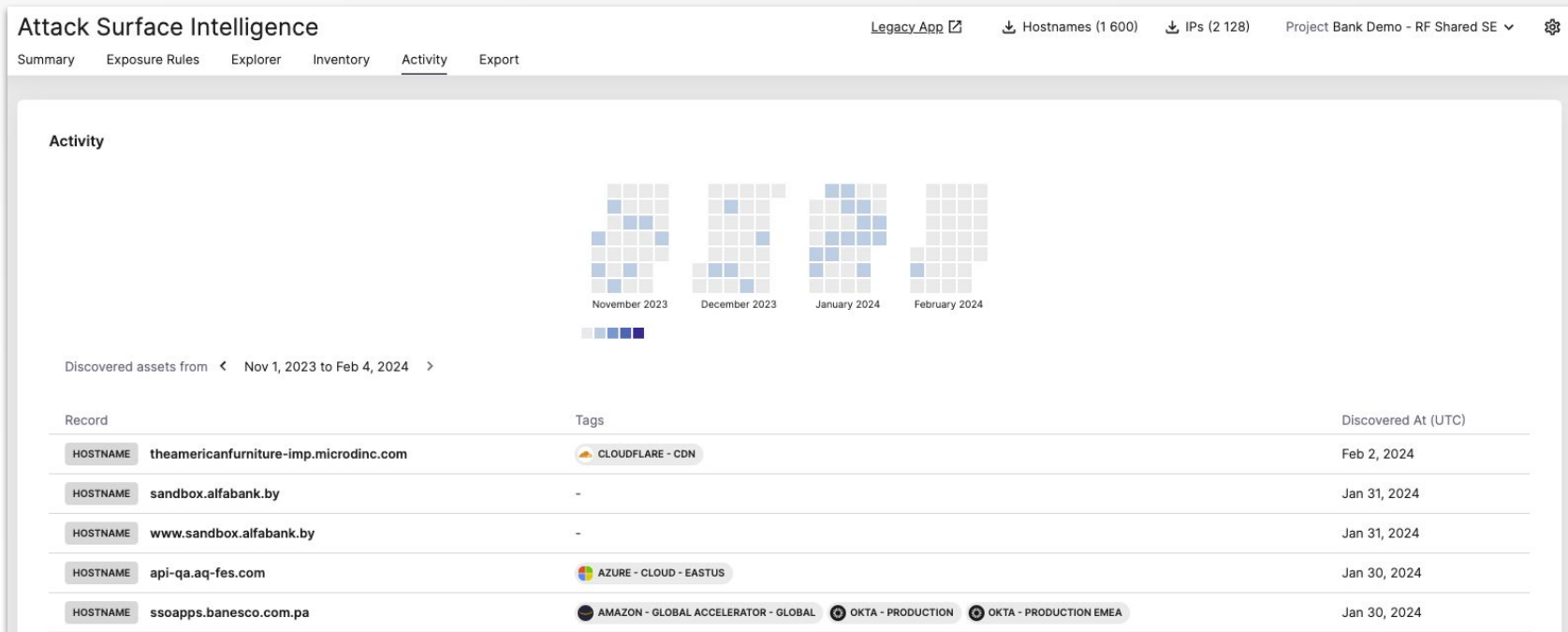
식별된 호스트명, IP, Port

다양한 방법으로 호스트식별(다크웹, 코드저장소, 인터넷스캐닝 등등)

Explorer						
Hosts		IPs				
Show Filters (0)		Table	Screenshots	View Bulk Jobs (0)	Filter by Hostname or IP	Add to Downloads + View Downloads
<input type="checkbox"/>	Hostname	Rank	Tags		IPs	Ports
<input type="checkbox"/>	 recordedfuture.com	13 613	 CLOUDFLARE - CDN Add	 1	104.18.43.111	80  443   CLOUDFLARE >
					172.64.144.145	80  443   CLOUDFLARE >
<input type="checkbox"/>	 go.recordedfuture.com	132 626	 HUBSPOT - MARKETING	 1	199.60.103.2	80  443   CLOUDFLARE >
<input type="checkbox"/>	 blog.recordedfuture.com	1 690 953	 CLOUDFLARE - CDN	 1	104.18.43.111	80  443   CLOUDFLARE >
<input type="checkbox"/>	 support.recordedfuture.com	3 480 699	 ZENDESK - CUSTOMER SERVICE SUITE  CLOUDFLARE - CDN	 1	104.16.51.111	80  443   CLOUDFLARE >
<input type="checkbox"/>	 app.recordedfuture.com	4 941 191	 CLOUDFLARE - CDN	 1	104.18.43.111	80  443   CLOUDFLARE >
<input type="checkbox"/>	 api.recordedfuture.com	9 717 047	 CLOUDFLARE - CDN	 1	162.159.128.62	80  443   CLOUDFLARE >

식별된 호스트명, IP, Port

다양한 방법으로 호스트식별(다크웹, 코드저장소, 인터넷스캐닝 등등)



식별된 호스트명, IP, Port

다양한 방법으로 호스트식별(다크웹, 코드저장소, 인터넷스캐닝 등등)

Attack Surface Intelligence

Legacy App [Hostnames \(1 600\)](#) [IPs \(2 128\)](#) Project Bank Demo - RF Shared SE

Summary Exposure Rules Explorer **Inventory** Activity Export

Inventory [Export as CSV](#)

[Hosting Report \(1 503\)](#) [Inventory Tree](#) [Hostnames pointing local \(38\)](#) [Remote Access \(59\)](#) [Admin Pages \(20\)](#) [VPNs \(12\)](#)

Counts by Panel All

Hostname	IP	Port	Service	Target
www[redacted]nesco.com Open Exposed Credentials (1)	34[redacted]	443	Fiori Launchpad Login Panel - Detect	Target
www[redacted]nesco.com Open Exposed Credentials (1)	34[redacted]	443	SAP NetWeaver Portal - Detect	Target
www[redacted]nesco.com Open Exposed Credentials (1)	34[redacted]	443	SAP Fiori Login Panel - Detect	Target
1 162[redacted]	66[redacted]	443	Fortinet FortiOS Management Interface Panel - Detect	Target
activesync.sberbank.hr	21[redacted]	443	Microsoft Exchange Admin Center Login Panel - Detect	Target

어떤 서비스를 수행하는 애플리케이션

애플리케이션 식별

취약점 DB에서 CVE 조회

Attack Surface Intelligence

ASN Owner (8)

Hosts by ASN C

- ☐ Cloudflare
- ☐ Amazon.co
- ☐ Fastly, Inc.
- ☐ Google LLC
- ☐ SendGrid, Inc.

Show 1 more

All Screenshot

Filter by hostname

Hostname

- ☒ recordedfuture.com
- ☐ go.recordedfuture.com
- ☐ blog.recordedfuture.com

1,690,953 Cloudflare - CDN

104.38.43.111 80 443 Cloudflare Cloudflare, Inc.

go.recordedfuture.com

2024-01-29 05:01 PM (5 days ago) 200 OK

<http://go.recordedfuture.com>

Strengthen Your Defenses with Threat Intelligence

Detected Technologies (15)

Product	Version	Category
Cloudflare	-	CDN
Facebook Pixel	2.9.143	Analytics
Fastly	-	CDN
Google Analytics	-	Analytics
Google Hosted	-	CDN
WAF detected as Cloudflare by Cloudflare Inc.		

Active Exposures Exposure History Current DNS

No issues found.

애플리케이션 식별

취약점 DB에서 CVE 조회 결과가 내 시스템에도 동일하게 존재하는가?

The screenshot shows the CVE Details website with a search for 'PHP » PHP » 5.4.16 : Security Vulnerabilities, CVEs'. The results show 212 vulnerabilities found. A table lists several CVEs with their details:

CVE ID	Description	Max CVSS	Published	Updated	EPSS
CVE-2022-31629	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a 'Host-' or 'Secure-' cookie by PHP applications.	6.5	2022-09-28	2023-01-20	0.13%
CVE-2022-31628	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar compressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.	5.5	2022-09-28	2023-07-21	0.07%
CVE-2019-9641	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in TIFF.	9.8	2019-03-09	2022-04-05	2.17%
CVE-2019-9639	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in MAKERNOTE because of mishandling the data_len variable.	7.5	2019-03-09	2022-04-05	0.34%
CVE-2019-9638	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in MAKERNOTE because of mishandling the maker_note->offset relationship to	7.5	2019-03-09	2022-04-05	

PHP V. 5.4.16을 사용하면 취약점이 212개 존재?

RF에는 224개의 취약점 기록 보유

실제 노출된 취약점/설정오류

우선순위에 따른 취약점 스캔 CVE-2024-21887

therecord.media/ivanti-vpn-vulnerabilities-exploited-devices-worldwide

ivanti

조나단 그레이그
2024년 1월 17일

기술 뉴스 소식

분석가가 1,700개의 장치가 악용된 것을 발견함에 따라 Ivanti는 VPN 표적으로 '급격한 증가'를 발견했습니다.

Ivanti는 사이버 보안 연구원들이 피해 규모를 파악함에 따라 최근 Connect Secure VPN 제품에서 공개된 두 가지 취약점을 표적으로 삼는 해커가 급증하고 있다고 말했습니다.

Ivanti 대변인은 The Record와의 논평에서 지난 주 경고를 발표한 이후 버그와 관련된 "위험 행위자 활동과 보안 연구원 검색이 급격히 증가하는 것을 확인했습니다"라고 말했습니다.

Volexity의 연구원들은 월요일 예 IT 대변인이 대중에게 이 문제를 알린 이후 전 세계적으로 1,700개 이상의 장치가 악용되었다고 밝혔습니다. Volexity는 12월 초에 CVE-2023-46805 및 CVE-2024-21887로 추적되는 문제를 발견하여 Ivanti에 보고했습니다.

Ivanti 대변인은 1월 10일에 발표된 완화 조치와 기타 도구가 취약점 악용을 중단하는데 관리자에게 도움이 될 것이라고 말했습니다. Ivanti는 아직 이 문제에 대한 공식 패치를 개발하는 중입니다.

다음은 통해 더 많은 통찰력을 얻으세요.
기록됨에
인텔리전스 클라우드로,
더 알아보기.

24년 1월17일
기사

Recorded Future

VULNERABILITY in Ivanti Connect Secure and 1 Other

CVE-2024-21887

Notes
References 1 000+
First Reference Jan 3, 2024
Latest Reference Feb 4, 2024
Curated
Recorded Future Community Vulnerability C2

Used in List CISA Known Exploited Vulnerabilities Catalog

Affected Products 2 of 2
Ivanti Connect Secure
Ivanti Policy Secure
Show All Versions

99
VERY CRITICAL
RISK SCORE

14 of 23 Risk Rules Triggered

Rise in cyber references in the last 60 Days
Show recent events or cyber events

Recorded Future AI Insights

Narrative View

CVE-2024-21887 취약점은 상당한 주목을 받았으며 심각한 위험을 가하고 있습니다. 다양한 출처의 여러 보고서와 링크 지점에서 볼 수 있듯이 위험 행위자들이 이를 적극적으로 악용하고 있습니다. 이 취약점은 Ivanti Connect Secure 및 Policy Secure VPN 장치에 영향을 미치므로 RCE (원격 코드 실행) 공격에 취약됩니다. 이 취약점을 악용하면 KrustyLoader 페이로드가 전파되고 손상된 시스템에 GIFTEDVISITOR 붙박이 존재하게 됩니다. 이 취약점의 중요성과 활발한 악용을 고려할 때 조직 자산에 대한 잠재적인 위험을 완화하기 위해 가능한 한 빨리 이 CVE 패치를 우선적으로 적용하는 것이 좋습니다.

Generated based on 14 Risk Rules | Analyst: Patrick Youn

Share feedback?

TRIGGERED RISK RULES

Learn More

Very Critical
Critical
High
Medium
Low

MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN FEB

Currently Triggered Risk Rules

Exploited in the Wild by Recently Active Malware - 1 sighting on 1 source
CISA Known Exploited Vulnerabilities Catalog, Ivanti Connect Secure and Policy Secure Command Injection Vulnerability from vendor Ivanti. The recommended action is to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Added Jan 10, 2024.
Security Control Feeds: Exploits in the Wild - Learn More

NIST Severity: Critical - 1 sighting on 1 source
Recorded Future Vulnerability Analysis via National Vulnerability Database. CVSS v3.1 Score (9.1) calculated using NIST reported CVSS Base Score (9.1) and Recorded Future Temporal Metrics. Base vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/CH/H/HA/H. Temporal vector string: E:H/RLX/RCC. Most recent link (Jan 12, 2024): https://nvd.nist.gov/vuln/detail/CVE-2024-21887

Recently Reported by Insikt Group - 1 sighting on 1 source
Insikt Group. 1 report: Ivanti Connect Secure VPN Vulnerabilities (CVE-2024-21887 and CVE-2023-46805) Exploited to Deliver Rust Payload "KrustyLoader", Sample Available on PolySwarm. Most recent link (Feb 02, 2024): https://app.recordedfuture.com/portal/analyst-note/docu/YN7N

Recently Linked to Malware - 80 sightings on 29 sources including
securonix.com, IoT Security News, Cybersecurity Help | Blog, SOCRadar Cyber Intelligence, Cybersecurity Dive | Home. 35 related malware families including WebShell, HermeticWiper, Zipline, Wiper Malware, Loader. Most recent tweet: "First world" Government owned Ivanti Secure Connect SSL VPN - vulnerable to CVE-2023-46805 -> CVE-2024-21887 -> RCE - vulnerable to CVE-2024-21893 -> CVE-2024-21887 -> RCE - backdoored with GIFTEDVISITOR - backdoored with JS credentialstealer - fully unpatched and pwned https://t.co/YX3HWMU7r. Most recent link (Feb 4, 2024): https://twitter.com/Gi7w0rm/statuses/1753965658930282731

Recently Linked to Ransomware - 12 sightings on 2 sources
Broadcom Protection Bulletin, GitHub. 4 related malware families: Akira Ransomware, Royal Ransomware, Kasseika

1월10일 CISA 공지
2월2일 공격샘플

우선순위에 따른 취약점 스캔 CVE-2024-21887

긴급을 요하는 공격 취약점을 중심으로
네트워크 스캐닝 시그니처 추가, 2월4일
현재 4,133개



우선순위에 따른 취약점 스캔

Shellshock (CVE-2014-6271)

취약점 경고시, 정탐? 오탐?

VULNERABILITY in GNU Bash

CVE-2014-6271 (Shellshock)

Notes [4 Insikt Group Notes](#)

References	100 000+
First Reference	May 19, 2014
Latest Reference	Apr 28, 2023
Curated	★
Recorded Future Community	Vulnerability Vulnerability

Affected Products 1 of 1

GNU Bash [Show All Versions](#)

79
HIGH RISK SCORE

14 of 23 Risk Rules Triggered

▲ Surge in cyber references in the last 60 Days
[Show recent events or cyber events](#)

Recorded Future AI Insights
Generated based on 14 Risk Rules

CVE-2014-6271, also known as Shellshock, is a vulnerability that affects Bash, a commonly used Unix shell. It allows attackers to execute arbitrary code remotely, which can lead to a complete compromise of the targeted system. The vulnerability has been exploited in the wild by multiple malware families, and there are a number of public exploits available. The severity of the vulnerability is high, with a CVSS score of 9.8 out of 10, and it has been included in CISA's list of known exploited vulnerabilities. As a vulnerability analyst responsible for managing patching, it is highly recommended to prioritize patching this vulnerability as soon as possible to prevent potential attacks.

[Recorded Future AI](#) summarizes insights, in part by using GPT, with intelligence sourced from the Recorded Future Intelligence Cloud

Was this useful? [👍](#) [👎](#)

ANALYST NOTES FROM PATRICK YOUN

[+ Create Analyst Note](#)

그외,

- 설정파일에서 DB접근 ID/PWD
- Cross Site Scripting
- Default ID/PWD

운영관리 조치 (**Mitigation**)

위험 완화 (Risk Mitigation)

Patch/Configuration 변경/네트워크 접근 제어

24 Exposures Found | Updated Jan 2, 2024

Search Exposures

Export Exposures by Issue

2 Critical

12 Moderate

10 Informational

Severity	Name	Number of Hosts
Critical	WordPress Contact Form 7 Plugin - Unrestricted File Upload (CVE-2020-35489) WordPress Contact Form 7 before 5.3.2 allows unrestricted file upload and remote code execution because a filename may contain special characters. View References References app.recordedfuture.com nvd.nist.gov contactform7.com web.archive.org wordpress.org www.insonvarghese.com	2

Host

www.se

www.ba

Target

External Link

External Link

Priority

99

99

Export

Evidence (JSON)

JSON

Raw Data

Headers

Save

Copy

Collapse All

Expand All

Filter JSON

0:

exposure_classification:

high

exposure_description:

WordPress Contact Form 7 before 5.3.2 allows unrestricted file upload and remote code execution because a filename may contain special characters.

exposure_id:

CVE-2020-35489

exposure_name:

WordPress Contact Form 7 Plugin - Unrestricted File Upload (CVE-2020-35489)

matched_at:

https://www.banescob.com.uy/contact-form-7/readme.txt

port:

443

request_data:

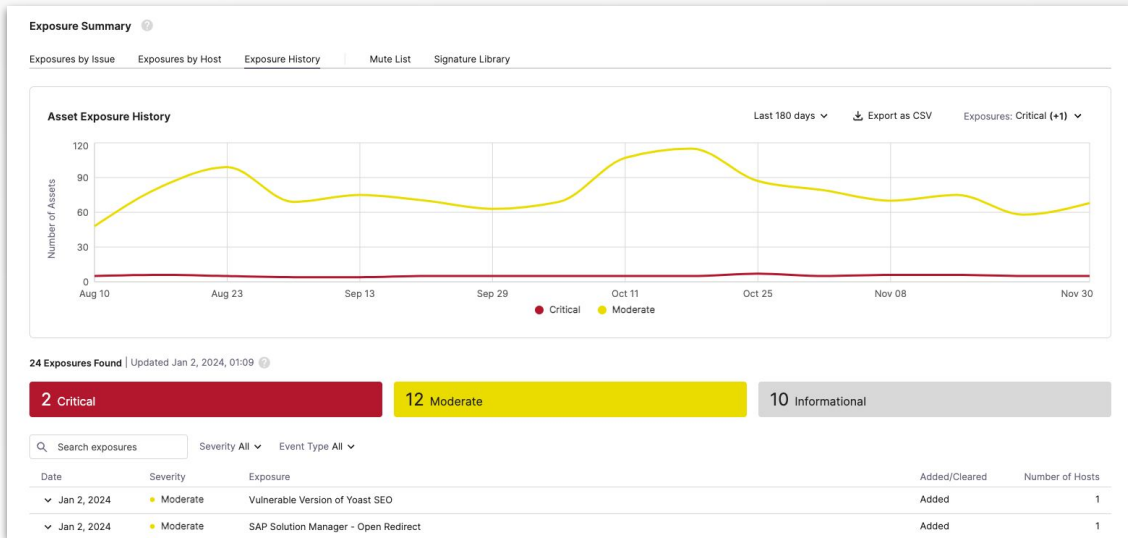
GET /wp-content/plugins/contact-form-7/readme.txt HTTP/1.1\r\nHost: www.banescob.com.uy\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; rv:68.0) Gecko/20100101 Firefox/68.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en\r\nAccept-Encoding: gzip, deflate\r\nConnection: close\r\nUpgrade-Insecure-Requests: 1\r\nReferer: https://www.banescob.com.uy/contact-form-7/readme.txt

response_data:

HTTP/1.1 200 OK\r\nConnection: close\r\nAccept-Ranges: bytes\r\nCache-Control: max-age=3600, public, must-revalidate\r\nContent-Type: text/html\r\nContent-Length: 12345\r\nExpires: Wed, 29 Nov 2023 14:25:34 GMT\r\nLast-Modified: 29 Nov 2023 13:25:34 GMT\r\nVary: Accept-Encoding, User-Agent\r\nX-Content-Type-Options: nosniff\r\nX-Frame-Options: DENY\r\nX-XSS-Protection: 1; mode=block\r\n\r\nContact Form 7 - Contributors: takayukister\nDonate Link: https://contactform7.com/donate/\nEmail: ajax, captcha, akismet, multilingual\nRequires at least: 4.8\nTested up to: 4.9\nStable tag: 5.0.5\nLicense: GPL2 or later\nLicense URI: http://www.gnu.org/licenses/gpl-2.0.html\n\nJust another contact form plugin. Simple but flexible.\n\nDescription\n\nContact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup. The form supports Ajax-powered submitting, CAPTCHA, Akismet spam filtering and so on.\n\nDocs & Support\n\nYou can find [docs](https://contactform7.com/docs/), [FAQ](https://contactform7.com/faq/) and more detailed information about Contact Form 7 on contactform7.com. If you were unable to find the answer to your question on the FAQ or in any of the documentation, you should check the [support forum](https://wordpress.org/support/plugin/contact-form-7) on WordPress.org. If you can't locate any topics that pertain to your particular issue, post a new topic for it.\n\nContact Form 7 Needs Your Support\n\nIt is hard to continue development and support for this free plugin without contributions from users like you. If you enjoy using Contact Form 7 and find it useful, please consider [making a donation](https://contactform7.com/donate/). Your donation will help encourage and support the plugin's continued development and better user support.\n\nRecommended Plugins\n\nThe following are other recommended plugins by the author of Contact Form 7.\n\n* [Flamingo](https://wordpress.org/extend/plugins/flamingo/) - With Flamingo, you can save submitted messages via contact form in the database.

지속적인 공격 접점 관리

패치여부/예외 처리 등



Exposures by Host | Exposure History | Mute List | Signature Library

	User	Created At	Comment
o.info	patrick.youn@recordedfuture.com	Feb 4, 2024	월말 서비스 개선 작업시 업데이트 예정
	drew.gidwani@recordedfuture.com	Oct 26, 2023	-

위험관리 라이프사이클

1. 자산대상식별

기업의 자산 식별 (데이터센터/클라우드)
Managed/Unmanaged
Shadow IT

2. 호스트/IP/Port

외부접근 가능여부
접근 가능한 포트

01

02

05

04

03

5. 조치

패치/설정변경/접근제어 등

4. 취약점/설정오류

CVE/Misconfiguration 스캐닝

3. 애플리케이션 식별

Version 식별에 따른 기술지원 종료 여부
확인

“데모 부스 방문하세요”

감사합니다.