랜섬웨어로부터 안전한

AD(Active Directory) 보안과 DR 구축 전략

Solutions Consultant / Hongso Chae

hongso.chae@quest.com

Quest

Where Next Meets Now.

AD관련 사고

국내에서 발생한 랜섬웨어 에서
AD는 주요한 공격 대상

How Ryuk Ransomware operators made $34 million from one victim

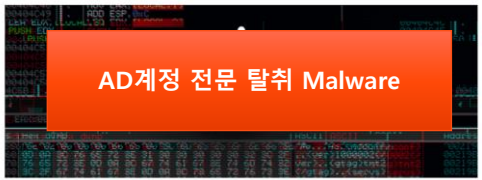
By Ionut Ilascu
November 7, 2020 03:44 AM

1. Examine domain admin via "Invoke-DACheck" script
2. Collect host passwords via Mimikatz "mimikatz's sekurlsa::logonpasswords"
3. Revert token and create a token for the administrative comment from the Mimikatz command output
4. Review the network of the host via "net view"
5. Portscan for FTP, SSH, SMB, RDP, VNC protocols
6. List accesses on the available hosts
7. Upload active directory finder "AdFind" kit with the batch script "adf.bat" from the "net view" and portscanned hosts
8. Display the antivirus name on the host via "WMIC" command
9. Upload multi-purpose password recovery tool "LaZagne" to scan the host
10. Remove the password recovery tool
11. Run ADFind and save outputs
12. Delete AdFind tool artifacts and download outputs
13. Grant net share full access to all for Ryuk ransomware
14. Upload remote execution software "PSExec" and prepared network hosts and uninstall the anti-virus product
15. Upload execution batch scripts and the parsed network hosts and run Ryuk ransomware as via PsExec under different compromised users

글로벌 TOP
Ryuk Ransomware >
AD 공격(계정탈취)

TrickBot Now Steals Windows Active Directory Credentials

By Lawrence Abrams



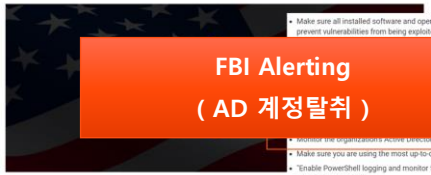
AD계정 전문 탈취 Malware

A new module for the TrickBot trojan has been discovered that targets the Active Directory database stored on compromised Windows domain controllers.

TrickBot is typically download and installed on a computer through other malware. This most common

FBI Issues Alert For LockerGoga and MegaCortex Ransomware

By Lawrence Abrams



FBI Alerting
(AD 계정탈취)

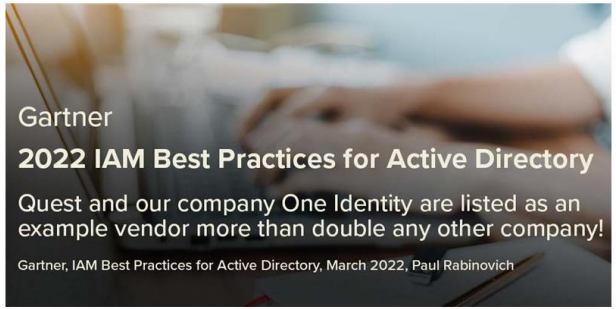
The FBI has issued a warning to private industry recipients to provide information and guidance on the LockerGoga and MegaCortex Ransomware.

Both LockerGoga and MegaCortex are ransomware infections that target the enterprise by compromising the network and then attempting to encrypt all its devices.

Quest

Where Next Meets Now.

Quest는 AD보안 리더



11개 Categories

- Active Directory migration
- AD monitoring, reporting and analytics
- Active Directory threat detection and response
- Active Directory backup
- Specialized AD management
- Access management
- Least privilege & separation of duty
- General-purpose PAM tools
- Active Directory bridging software to integrate non-Windows systems
- Identity governance and administration (IGA)
- Architectures for multiforest environments

"Quest는 AD 11개분야에 모든 솔루션을 제공하는 유일한 회사"

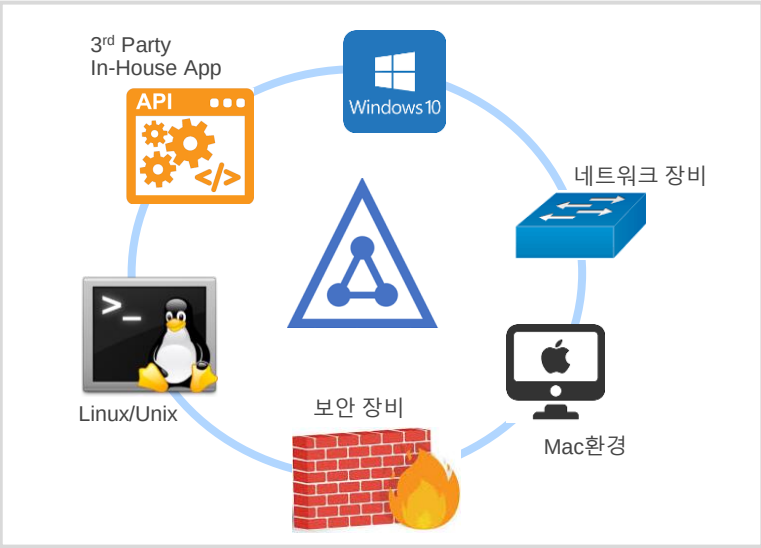
Quest

Where Next Meets Now.

Active Directory는 ?

통합 인증

통합인증(계정통합)



표준 인증을 지원하는 대부분의 서비스/장비에

- 통합인증
- 권한관리
- ID단위 인증

대부분의 VDI에서 AD를 통합인증으로 사용

단말 통합관리

단말(Windows 10/11, Server) 통합관리

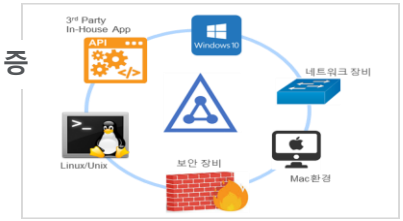
연결된 모든 장비들을 중앙에서 통합관리 / 거의 모든 작업을 수행

- 보안정책(GPO)일괄 배포
- 브라우저에 링크를 추가
- 패스워드 정책 설정
- 방화벽 설정
- NIC/프린트 관리

AD 보안과 DR?

AD 보안 및 DR

통합인증



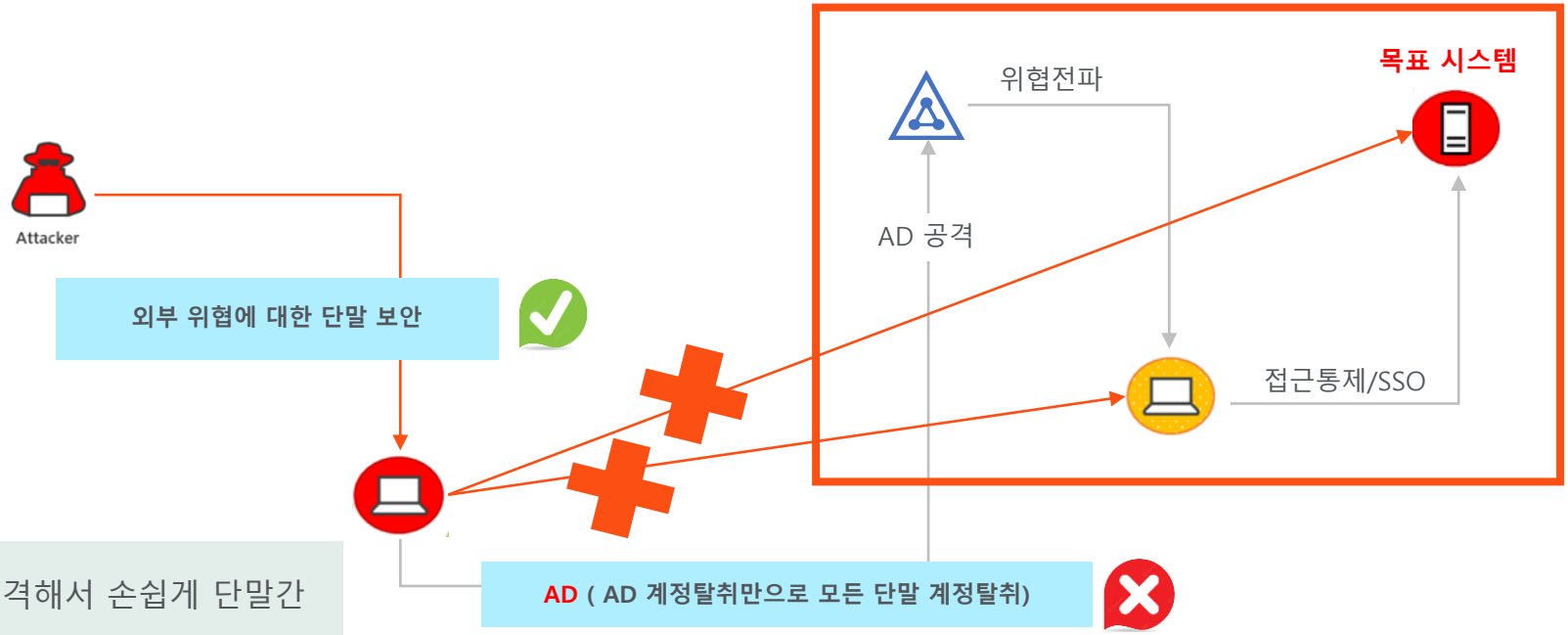
단말통합

보안	침해 가능성	낮음	감사(내부 위협)	높음	침해 탐지 및 보호(외부위협)
	업무 영향도	높음		높음	
DR	복구 시간 영향도	높음	빠른 복구	낮음	정확한 복구
	복구 난이도	높음		높음	

침해 가능성은 낮으나 **업무 영향도나 복구 시간이 중요**

침해 가능성이 높고 업무 영향도도 높으나 복구는 시간보다 **정확성 필요**

AD보안이 되지 않으면?



AD를 공격해서 손쉽게 단말간 전파를 통해서 목표 시스템 공격

AD DR 체계가 없다면?

Maersk

- NotPetya로 150개 DC중 149개 유실
- AD복구에 9일이 걸림
- $$ Millions 손실
- 뉴스 해드라인 장식

Global Manufacturer

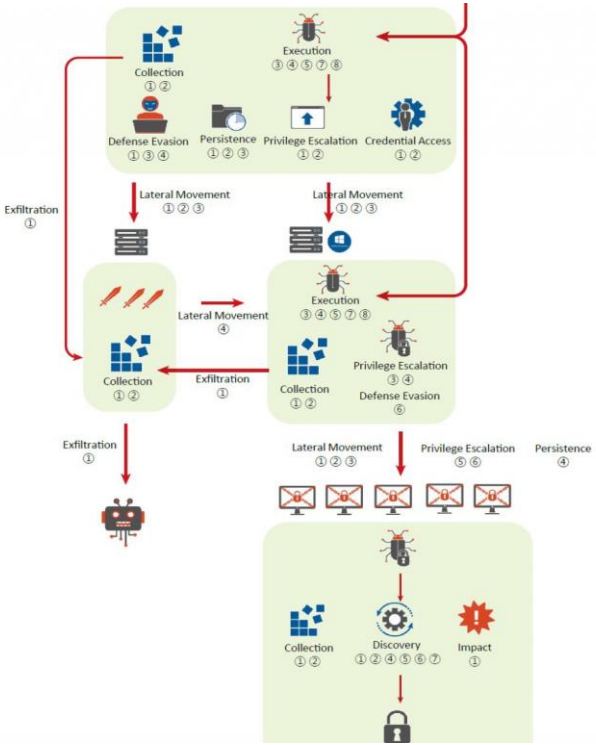
DRE로 다운시간 최소화: 1시간이내 서비스 복구

"Quest Tool이 없었다면 이렇게 빠르게 복구가 가능할 수 없었을 거다"

9일 ⟷ **1시간**

KISA 권고

KISA권고 : AD 모니터링 필요



【Defender's Insight】

'한국인터넷진흥원'은 본 보고서를 통해 AD환경에서 발생하였던 랜섬웨어 감염 공격 유형에 대해 살펴보았다. 공격자는 스피어피싱을 통한 내부 침투, 계정 탈취 후 DC 서버 장악, SMB기능을 통한 내부 이동의 과정을 통해 랜섬웨어에 감염시켰다. 이러한 사고는 공격자가 요구한 대가 지불액, 기업의 이미지 손상에 따른 피해, 시스템 복구 비용 등 막대한 손실이 발생할 뿐 아니라 AD의 특성상 시스템 전체가 장악되어 기업 주요 정보 유출 등 추가 피해가 발생할 수 있다.

앞으로도 기업들을 대상으로 한 해킹사고는 끊임없이 발생할 것이고 AD를 사용하는 기업들도 타겟이 될 것이다. 기업마다 망 구성방식, 권한 관리, 보안 정책 등이 다르기 때문에 침투 방식이나 세부적인 공격 방법은 변경될 수 있으나 권한상승, 계정 탈취, SMB를 통한 내부 이동 등은 대부분의 AD사고에서 확인되는 공통적인 특성이다.

따라서 AD환경을 사용하는 기업 입장에서는 계정 관리 및 모니터링이 제일 중요하다.

최초 침투에 성공한 공격자는 관리자 계정 탈취를 목표로 내부망을 탐색하고 이동할 것이고 이때 일반 사용자 계정을 아무리 많이 탈취하더라도 내부망 장악에 도움이 되지않는다. 때문에 계정이 탈취되더라도 AD DC(Domain Controller)서버를 장악할 수 없도록 사용자 및 서비스 계정들의 권한을 분리하여 관리하여야 한다. 관리자 그룹 계정 사용을 최소화하고 불가피하게 관리자 계정을 사용하는 시스템들은 주기적으로 모니터링하여야 한다. 특히 AD DC의 경우 등록된 서비스와 그룹 정책 목록에 의심스러운 사항은 없는지 주의를 기울여야한다. 또한 주요 시스템 로그는 주기적으로 백업하고 계정 탈취 도구가 탐지되거나 파이프 통신 발견 시 즉시 전사 시스템을 점검해보아야한다.

AD 보안 전략

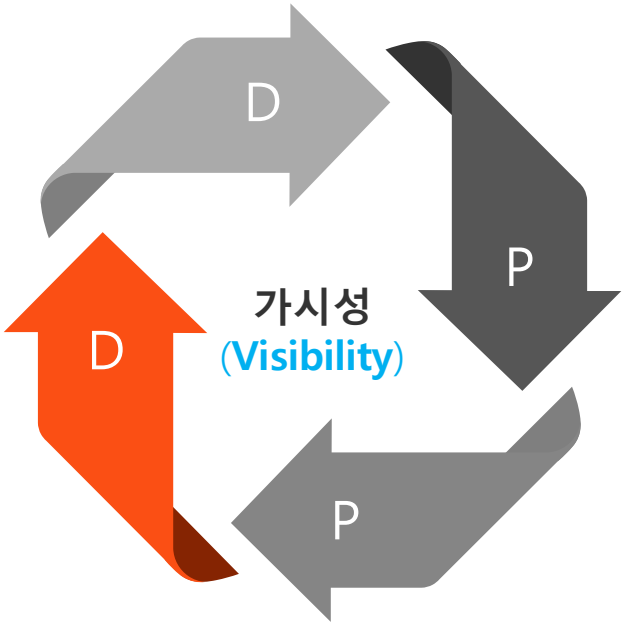
Quest

Where Next Meets Now.

AD 보안전략(2P2D)

Diagnostic(분석)

운영과정에서의 분석 및 위협발생에 대한 원인분석을 위한 데이터 및 검색 체계



Prevent(예방)

위협이 될 수 있는 정책위반에 대한 탐지를 통해서 사전에 위협 탐지 및 대응

Detect(탐지)

AD에 알려진 위협 등을 통한 공격을 실시간으로 탐지하여 피해를 최소화

Protect(보호)

위협이 될 수 있는 요소를 보호하여 위협요소 사전 차단

AD 보안 전략

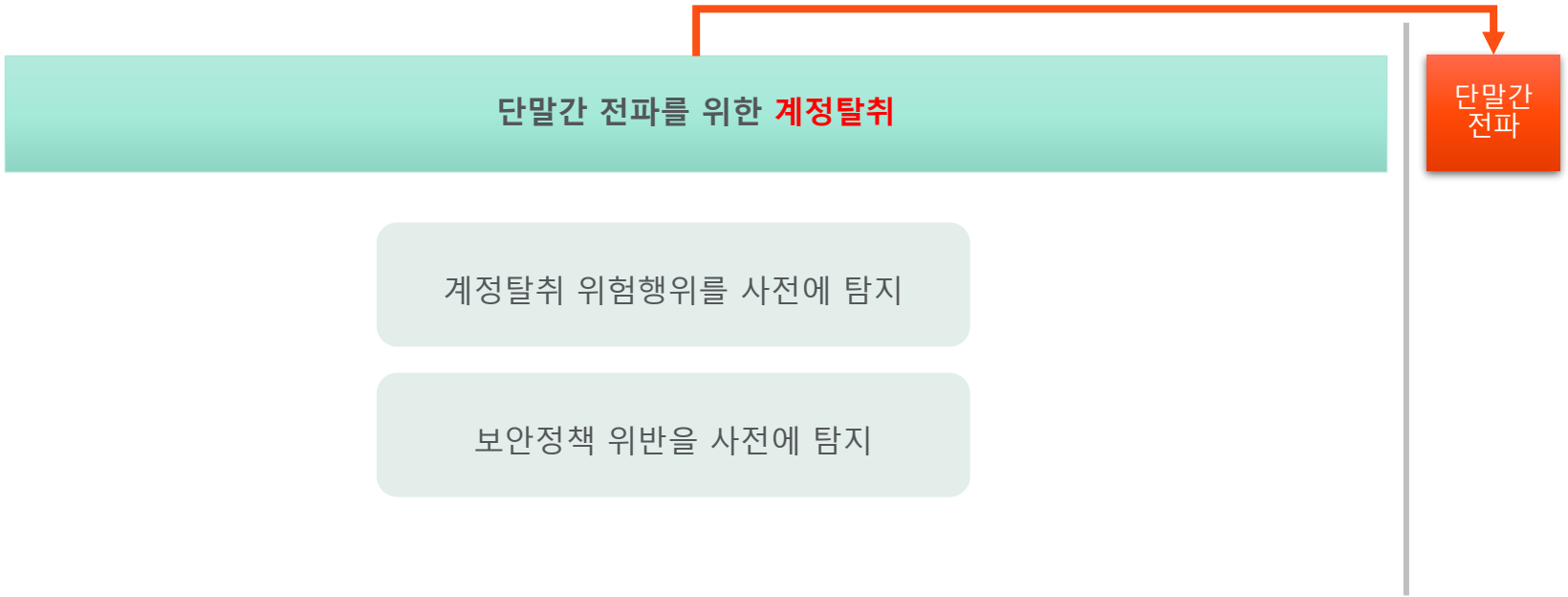
전략 #1. 예방

Quest

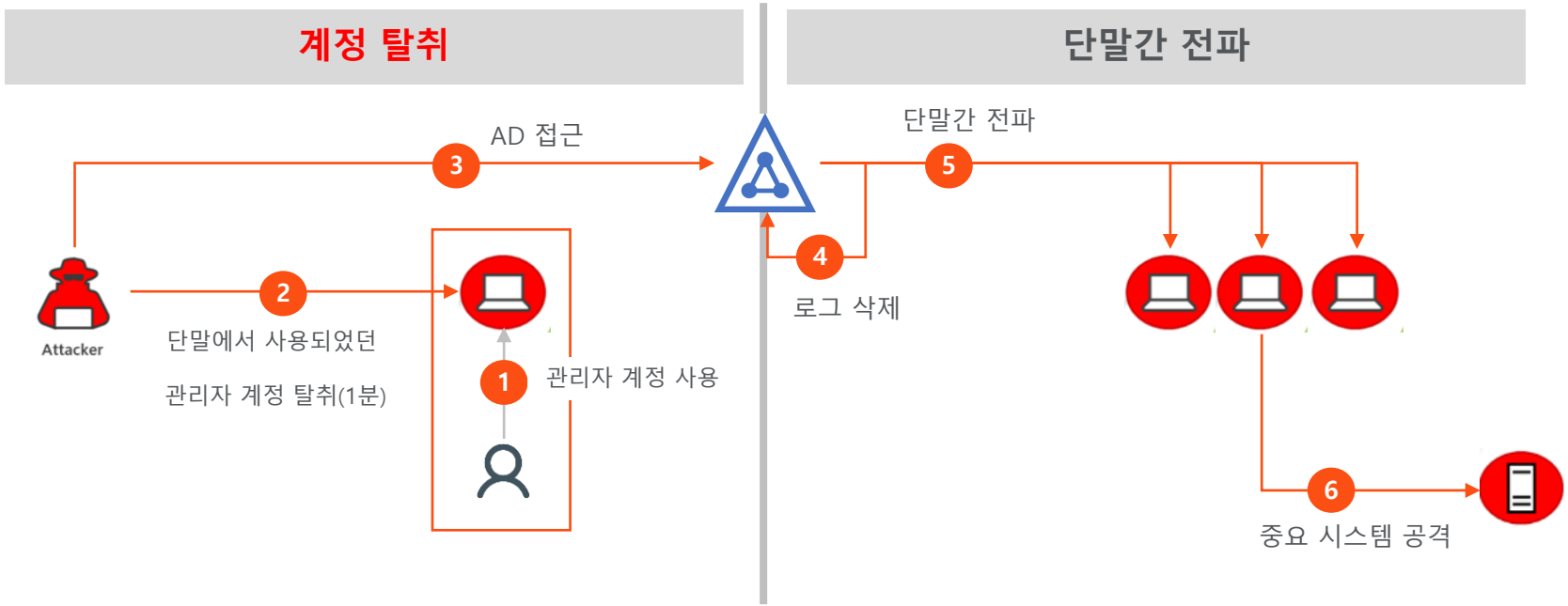
Where Next Meets Now.

취약점이나 정책위반 탐지를 통한 위협예방

계정탈취를 위한 공격에 많은 시간 소비가 되는 반면 계정탈취 후에 실제 단말간 전파는 손쉽게 수행됨



사례 : 단말에서 사용된 관리자 계정 탈취



사례 : 메모리 계정탈취는 손쉽게 수행

메모리로 부터 계정을 탈취하는 공격은
다양하며 손쉽게 탈취 가능합니다.

Metasploit

Koadic

Impacket

Mimikatz

PowerShell Empire

Python Script

MeterPreter

사례 : 메모리로부터 계정탈취 수행

Meterpreter로 run 명령어 수행

Hash정보 탈취

```
[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3be07e8131a02ffdfa8aa2859f6af5df...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

ladmin:"la"

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ladmin:1000:aad3b435b51404eeaad3b435b51404ee:2663c51dac03ec3347943696b33f29cb:::
```

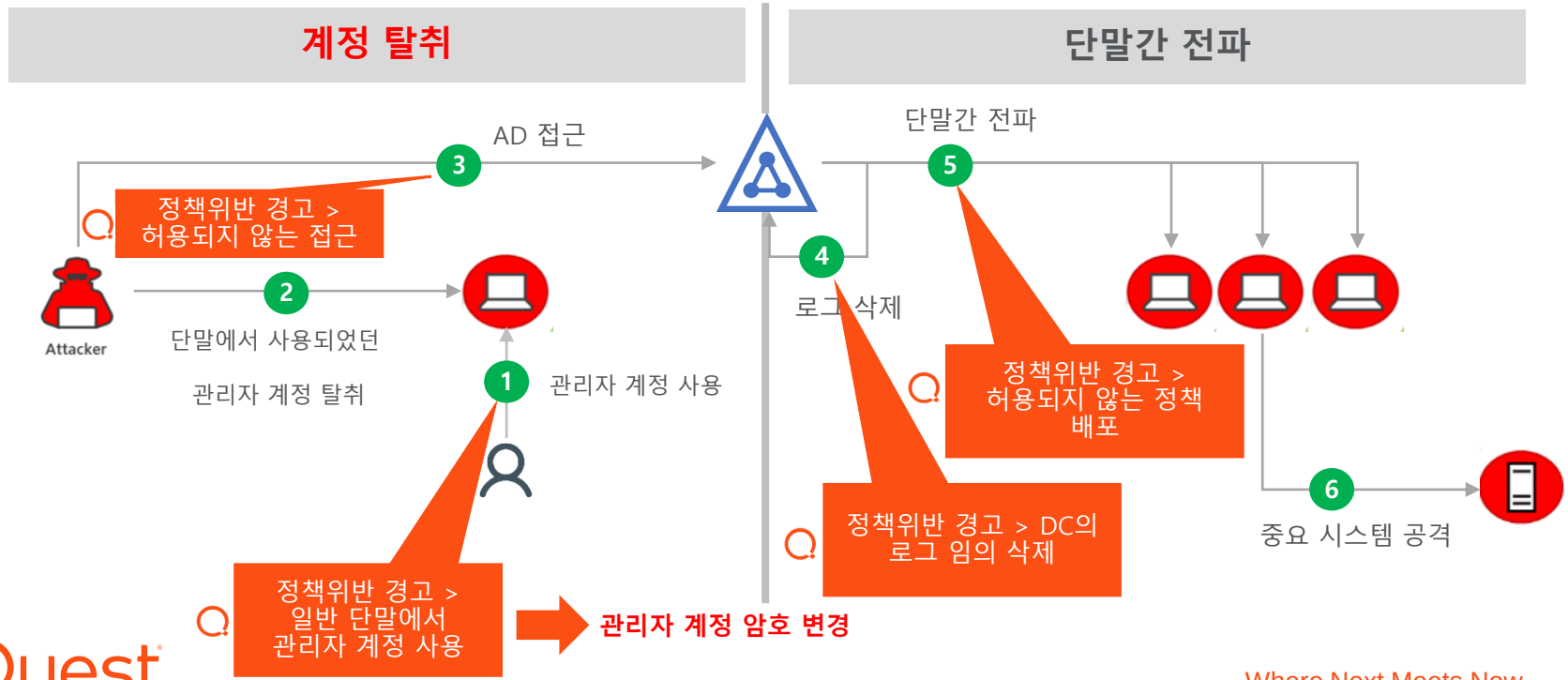
Meterpreter로 sekurlsa::logonpasswords 수행

패스워드 탈취

```
tspkg :
 * Username : dadmin
 * Domain   : ADSEC
 * Password : P@ssw0rd
wdigest :
 * Username : dadmin
 * Domain   : ADSEC
 * Password : P@ssw0rd
kerberos :
 * Username : dadmin
 * Domain   : ADSEC.DOM
 * Password : P@ssw0rd
ssp :
credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2022-09-04 오후 7:04:34
SID               : S-1-5-19
```

1분 안에 계정탈취 완료

사례 : 계정탈취 위협예방



Quest

Where Next Meets Now.

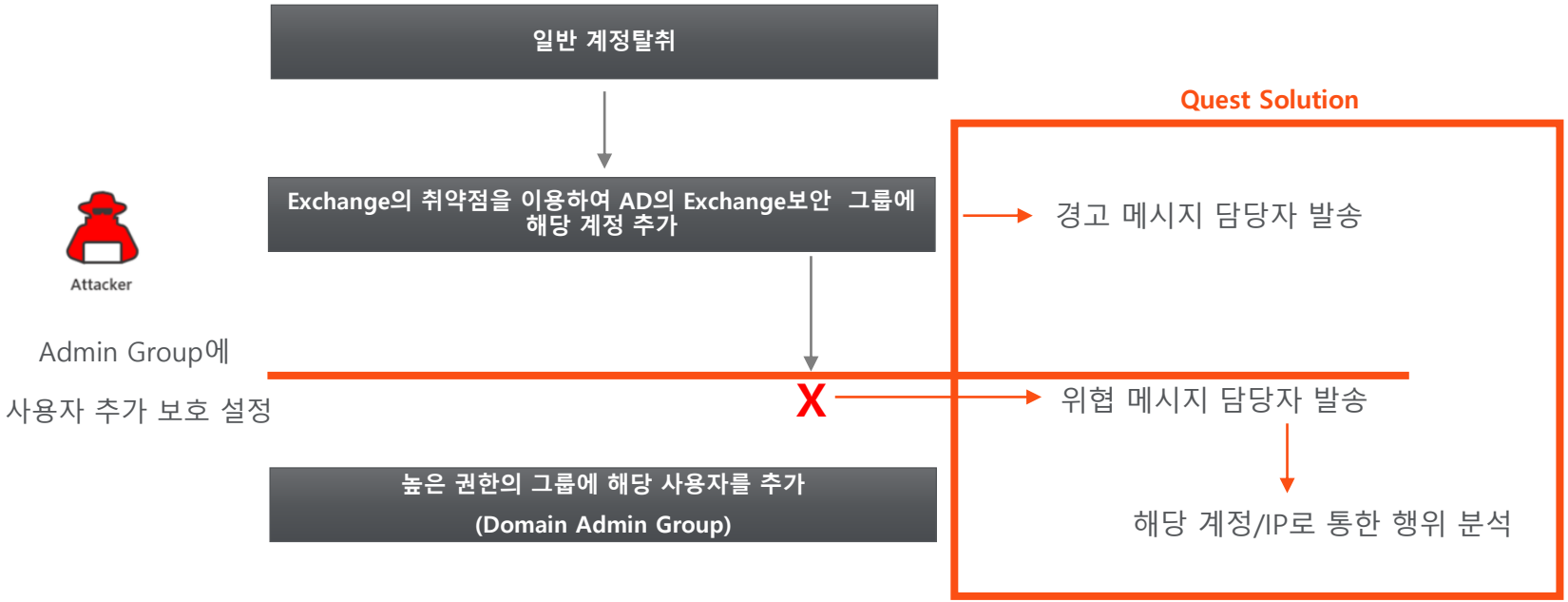
AD 보안 전략

전략 #2. 보호

Quest

Where Next Meets Now.

고객 사례 : 취약점을 통한 계정 탈취 후 권한 상승



AD 보안 전략

전략 #3 위협탐지

Quest

Where Next Meets Now.

알려진 위협 탐지

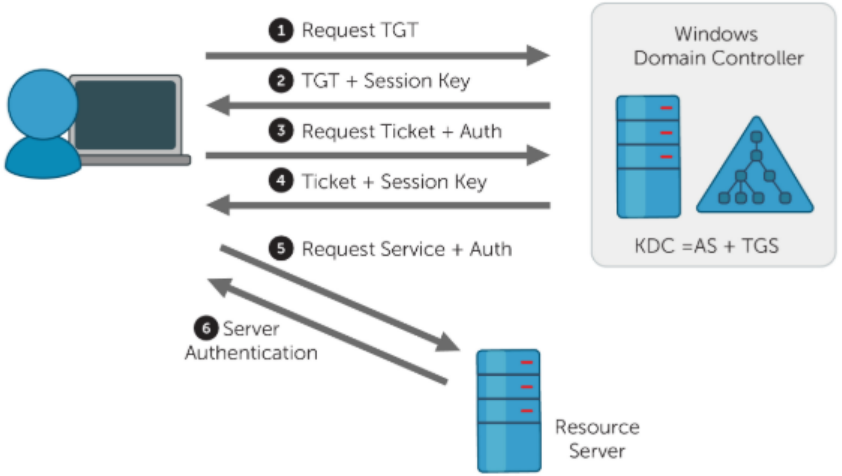
Golden Kerberos Ticket	SID History Injection
DC Sync	DC Shadow
NTDS.dit Attack	AdminSDHolder
Kerberos Roasting	NTML V1.0

계정탈취 공격

(모든 AD환경에서 위협)

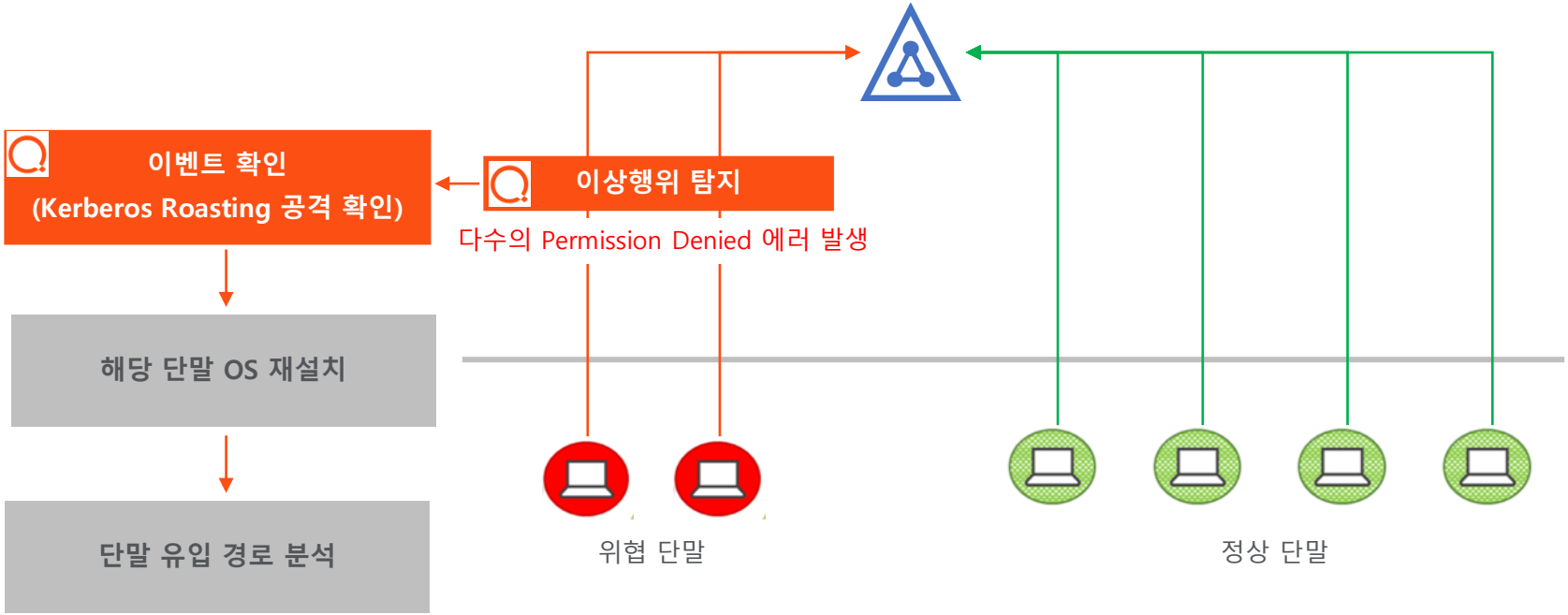
사례 : Kerberos Roasting

Kerberos Roasting 공격 : Kerberos를 통해서 계정탈취




```
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$krb5tgs$23$28dbc5e4e514a94b561156069953e0c8$e4ddac618c74978d7b0b2416b17884808f820a6585607d654a23d427c74c163ffdf4c3f1845
b15e2de199ff745ddf9ac8a118224c17439fc0fd8b1c82bc8c818418e370fab8722173ca7088791a832c36bc5e8bd23e25a9cfcb7cf57be728399e83
179fdeb8c9f9a11cd261c73d34e26ae76185a9abd9e9b18cefe98dad29c139a3aadf0573718f7e16ca4109594ca13f3fcd7cc868e79765d779d4b74f
1fd52f6c594ed33c129869a8b586d26f6de377c852e5afeb68a8c32c4d56cba5ffe52d84c1bbf8e59f7b5705becfa09110053f5930f717f004bcfd99a
0313ffb2befb83fae3372b0edca322073525c9af8aeab9813f950d953226bcb1dd5e02830a8d01022122b7d9cfd270f97008bf0be288baf75b53044a
5427bfde173288868db9a9b6afe667596bb198b609df52f809786f8105905c88478f1aa8c04b0d8421d89ce9d515a5bab7a4131723c2635c5c3db352
81cf9afd69cffcab7be73bee74aa74f62e53de097cdca120b67977a64dffcc5db4514a8cb4924146b2b436a5e70b70d59e4b3fc8929878a35c2e8991
ea9cc33dc92c04f8cf7e4c802a03fe8bf886bf2d89cea1d2a2a99b5eab9227ec01dd410cfec3c4e66613615d58c2a9072c3adfec5b25f9fadb14365b
0859463a6fbd543957c6798698f4a5b825fcf836ef731d10969fc186a101463e1698c9fa6a3b74ca320ed9d187c11c1aad10b766f6c2a8617eaecceb
5dce23d7fa620cb95d3248652e9bfb57de47bda652b078a258f6da7b6cfe6291f763ef01394d39f50e38f201ee34b08bad6eb550825236d9b2e6a71b
ff700474b18299db9fc6896f273e9882daeda312347fe9d4337283859fedf2bbdb5dba16f64906596ccd57278313e6078953e849af896e69363077 39
16d635af6de3a224d727a5a92379397fe166fe53d33cdbfae7b23fd5cfa284948ae3d925edcc51e163ace48d386db9924c022217068296b929ca7f24
e6004e7116b9b734519eed89bd8edf445af38b3a3407a2350f1bad8de558553ce87d64b11d7addfc6f978ae8fa39b8e2835d84028816c4ddf9a6d313
900121c95e9bfe2fe36b3558f7feb537ce1d5fe9f9065b3fe938f65f76e9542391f6568b25a01bcb5da96f8ddacae69db5a79cd005c4411940caeece
3c047d9e47c57442957279d76b492d361d1389e2e8b8498a3607a0c0c4d5e99c5220cb1619b751754dcc56399c05ac864c9e88f9972a91d4621df60b
77d3a1cfb70f113635936c15e38f217eae4152e1186d4f0e6e7fa222018c11d61b569f3c88e5aff36ed3a300518fa68584190e968d0273db69c00fe
602e3d773ce8d4870bf420f78bb40b3225b489eae791b44ee77f797576d638e47a96cfec73432c5072923273928fdda06464929243737b1891e3da3e
9fb2c63aa805ad297bf80f7ed200fdb7a766277017e2eeacc220c06f80b2dbc1edc3b963e04db4a706147476 92f26992dd30aadb570e0416a352e85d6
f3708616fadf3205c33d3931c76242c6bbe17c2003cdb41009726953 4d51475c98add3c14162b848d4e6cdfb1586db290243                    6
68efa8026e824abfc743fb61c20f7e237f68f26efed50614563a1b76148486a467c475fce403554b306863de59b38d764d0                3:Pa$$word1234

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$28dbc5e4e514a94b561156069953e0c8$e4ddac...64d068
Time.Started.....: Fri Jan 14 09:33:42 2022 (0 secs)
Time.Estimated...: Fri Jan 14 09:33:42 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/Users/matthewvinton/tmp/dict.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3105.9 kH/s (0.82ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 3109/3109 (100.00%)
Rejected.........: 0/3109 (0.00%)
Restore.Point....: 0/3109 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 12345 -> P@le0dsv
Hardware.Mon.SMC.: Fan0: 53%
Hardware.Mon.#1..: Temp: 65c

Started: Fri Jan 14 09:33:36 2022
Stopped: Fri Jan 14 09:33:44 2022
matthewvinton@charon ~ %
```

고객사례 : 내부망(망 분리) 일부 단말에서 공격



AD DR?

Quest

Where Next Meets Now.

Gartner 리포트

Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

Published 2 March 2022 - ID G00761039 - 11 min read

By Nik Simpson, Ron Blair

Challenges of Ransomeware Recovery

Scope of the Attack

- Unknown start date
- Unknown extent of the attack
- Compromised Active Directory
- Different systems affected at different times
- Malware and configuration changes

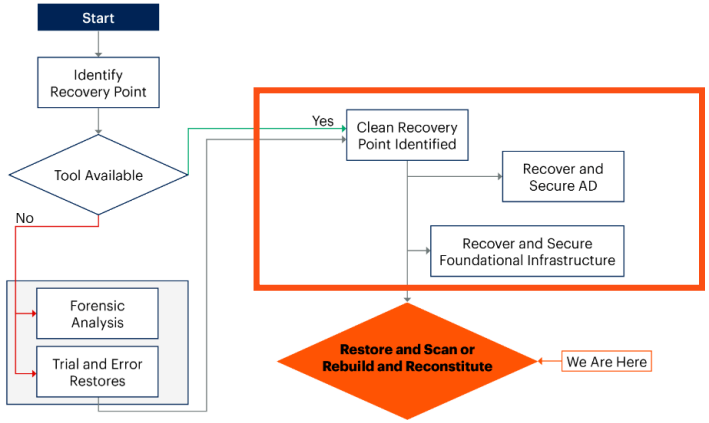
Unattainable RTO/RPO

- Replicated systems at DR site unusable
- Most recent backups may be unusable
- Large-scale recovery of systems from backup
- Lack of recovery automation
- Normal DR procedures can't be used

Source: Gartner
761039_C

- AD는 DR도 동시에 공격 가능하고
- 가장 최근 백업이 사용불가하고
- 복구 자동화가 미흡하고
- 일반적인 DR 프로시저가 사용될 수 없다

Recovery Flowchart



Source: Gartner
761039_C

- Active Directory threat detection and response
- Active Directory backup
- Specialized AD management

AD DR은 Restore뿐만 아니라 Rebuild도 필수
(기존 Legacy 백업은 Restore)

Quest

Where Next Meets Now.

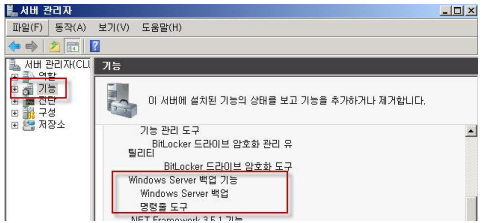
국내 고객 사례

기존에 전용 백업 솔루션으로 AD Backup하여 DR 구성

(Acronis)

Microsoft로부터 Acronis로는 DR구축이 안된다고 권고 받음

(윈도우 상태 백업 권고 받음)



DR개념으로는 한계 존재

- 랜섬웨어/ Datacenter 이슈 같은 DR상황에 대응 어려움
- 운영과정에서의 온라인 복구를 지원하지 못함

AD 백업/복구 전문 솔루션 필요

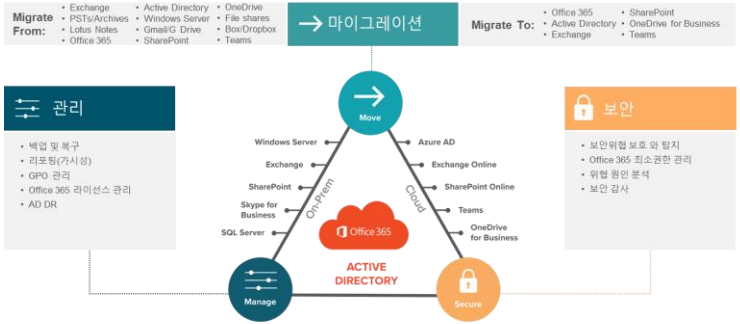
AD의 중요성이 증가하면서 중단이 되었을 때의 업무와 비즈니스 영향도 분석결과 빠른 복구의 필요성 대두

Quest는 ?

Quest

Where Next Meets Now.

Quest는 국내 / 글로벌 AD보안 리더



Microsoft와 진행한 AD보안 고객세미나

NIST Cybersecurity Framework

Identify
SpecterOps BHE / Enterprise Reporter Suite / Quadrotech Nova

Protect
Change Auditor / GPOADmin / Quadrotech Nova

Detect
Change Auditor / On Demand Audit Hybrid Suite

Respond
Change Auditor / IT Security Search / Enterprise Reporter Suite

Recover
Recovery Manager DRE / On Demand Recovery

퀘스트 AD 보안 솔루션 웨비나 보기
- Microsoft와 함께하는 Quest AD 보안이야기

웨비나 보기

국내 유일
금융/Enterprise/ 공공/제조 고객사 확보

국내에 처음으로 AD보안 영역을 만듬(개념, 전략)

Hybrid/O365 완벽 커버리지

Quest

Where Next Meets Now.

단말 보안의 중요성을 알고 계시다면 AD 보안은 필수적인 요소입니다.

AD가 구성되어 있다면 AD 활용이 낮아도	EDR이 있는데 AD보안이 없다면	AD보안 뿐만 아니라 AD서비스 문제에 대한	AD 가시성이 없다면, 보안 전략이 없다면 AD 위협을 어떻게 대응할지 고민이라면
AD 보안이 필수 입니다.	단말 보안의 마지막 퍼즐이 남아 있다고 볼 수 있습니다.	사전 대응, 감사 및 가시성을 제공합니다.	Quest의 솔루션이 최고의 선택지 입니다.

Quest

Where Next Meets Now.

전통적인 백업/복구 체계로 DR 구성을 하셨다면 **DR에 대해서 다시 고민해 봐야할 시점**입니다.

AD DR를 위한 Restore와 Rebuild를 모두 지원하는 솔루션 필요


Thank You
Quest
Where Next Meets Now.