

2024.3Q

KARA 랜섬웨어 동향 보고서



KARA 랜섬웨어 동향 보고서

EQST Lab 팀 이호석, 정민수, 조효제, 이현아

- 랜섬웨어 트렌드2
 - 1. 3분기 Insight.....2
 - 2. 3분기 랜섬웨어 활동 통계3
 - 3. 랜섬웨어 트렌드5
 - Cloud 환경을 노리는 랜섬웨어 공격5
 - 랜섬웨어 그룹의 취약점 악용6
 - 4. 신규 랜섬웨어 및 그룹 활동7
- Meow Ransomware 그룹 상세 분석9
 - 1. Meow 개요.....9
 - 2. Meow 랜섬웨어 공격 시나리오11
 - 3. Meow 랜섬웨어 심층 분석12
 - 기능 분석12
 - 1) 분석 체크 사항12
 - 2) 기능 상세 분석13
 - 4. IoCs18
- 랜섬웨어 Mitigations19
 - 1. Meow 랜섬웨어 대응방안 안내.....19
 - 2. SK 쉐더스 MDR 서비스20



■ 랜섬웨어 트렌드

1. 3분기 Insight

TREND

- Embargo : **Active Directory 동기화**를 이용한 클라우드 침해
- RansomEXX : **Jenkins 취약점(CVE-2024-23897)**을 악용한 공격

THREAT

- 3분기 Top5 랜섬웨어 : RansomHub, Play, LockBit, Meow, Hunterse
- Conti 기반 랜섬웨어 : Meow, Mimic, Monti, BlueSky, Putin, ScareCrowe

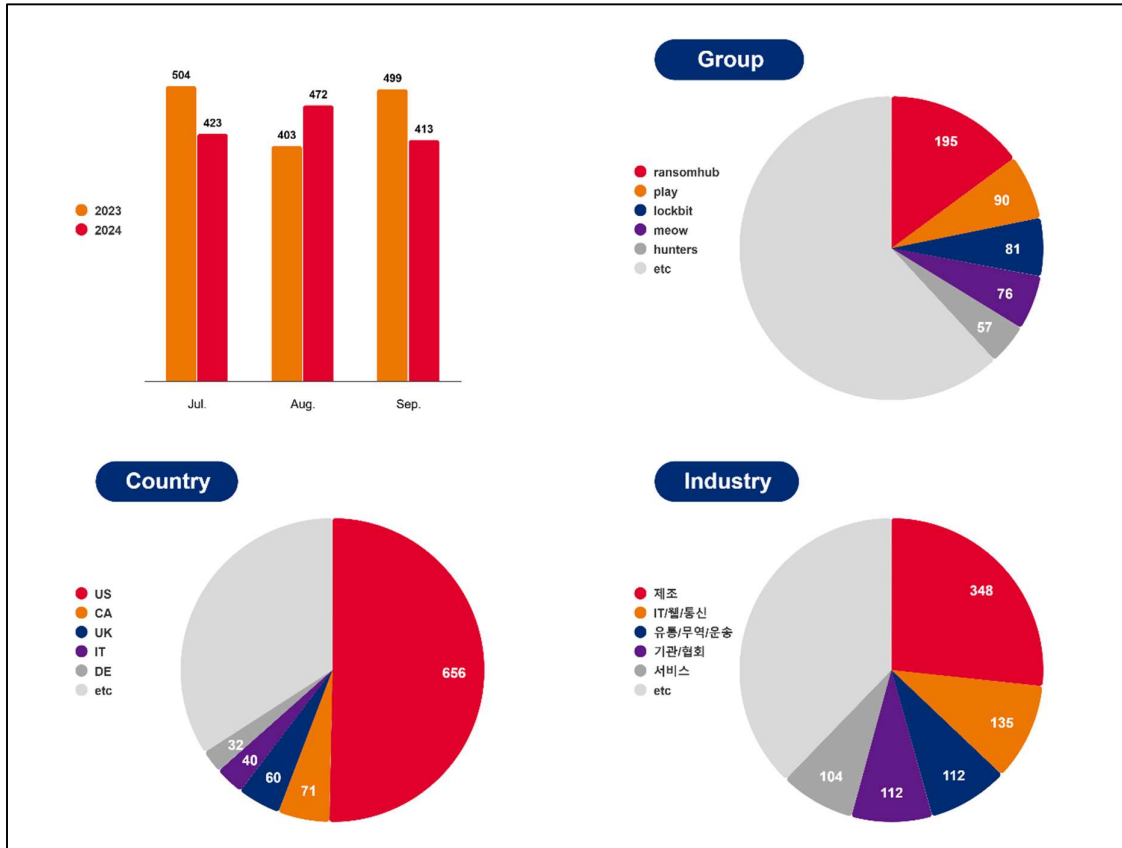
EXPLOIT

- 0-day : CVE-2024-23897, CVE-2024-40766
- 1-day : CVE-2023-48788

TARGET

- FortiEMS, Jenkins, SonicWall 취약점을 통한 초기 침투
- 전체 공격 중 **제조업** 26%, **미국** 50%

2. 3 분기 랜섬웨어 활동 통계



[랜섬웨어 그룹 활동]

2024년 3분기 랜섬웨어 피해 건수는 1,314건으로 작년 동기 대비 약 7%가량 감소한 수치를 보이고 있으며, 2분기 대비 약 3% 감소하였다. 이는 법 집행 기관의 처벌과 끈질긴 수사로 심리적 압박을 느낀 공격자들이 활동을 종료하거나 인프라를 압수당해 공격 수치가 줄어든 것으로 보인다. 특히 해티비스트 그룹으로 알려진 SiegedSec의 경우 수사 기관의 압박에 두려움을 느껴 활동을 종료하였고, Dispossessor 랜섬웨어 그룹은 인프라를 압수당해 폐쇄됐다. 압수당한 인프라에는 24개의 서버와 9개의 도메인이 포함되어 있으며, FBI의 조사 결과 총 43개의 기업이 공격받은 것으로 확인됐다. 이번 분기의 랜섬웨어 공격은 전체적으로 미국과 제조업에 대한 공격이 주를 이루고 있으며 RansomHub가 가장 많은 피해 건수를 기록했다.

피해 건수는 약간 감소한 모양새지만 3분기에도 랜섬웨어 공격자들은 고도화된 전략을 통해 공격을 이어나가고 있다. 특히 최근 가장 활발한 활동을 보이고 있는 RansomHub 그룹은 스피어 피싱이나 Zerologon¹ 취약점 등을 악용해 초기 침투 후, 탐지 회피를 위해 BYOVD(Bring Your Own Vulnerable Driver)² 기법을 활용해 EDR 솔루션을 무력화시키는 EDRKillShifter를 사용하기도 했다. RansomHub는 LockBit의 영향력이 줄어든 이후 가장 활발한 활동을 보이는 랜섬웨어 그룹으로 서비스형

¹ Zerologon: 마이크로소프트 윈도우 및 Samba 의 인증 프로토콜인 Netlogon 의 취약점

² BYOVD: 신뢰할 수 있는 인증서로 서명된 드라이버의 취약점을 악용해 공격하는 기법

랜섬웨어를 제공해 Scattered Spider, Noname 그룹 등 많은 계열사를 확보하며 랜섬웨어 생태계를 장악하고 있는 모습을 보이고 있다.

한편, Play 랜섬웨어 그룹은 RaaS 그룹은 아니지만 꾸준히 많은 피해자를 만들고 있으며 최근에는 ESXi 타깃 변종을 출시하여 공격 범위를 넓히고 있다. 해당 변종을 호스팅하는 데 사용된 도메인은 Prolific Puma라는 공격자와 연관이 있으며, Play 랜섬웨어 그룹이 이전에 사용했던 PsExec, NetScan, WinSCP와 같은 합법적인 도구들도 포함하고 있어 탐지 회피를 위해 공격에 악용하는 것을 알 수 있다.

LockBit 그룹은 관계자의 체포와 수사 기관의 압박, 계열사 이탈 등으로 이전과 같은 모습을 보이고 있지 않지만 여전히 위협적인 그룹으로 자리매김하고 있다. LockBit 그룹의 위협과 영향력이 커지면서 이를 모방하거나 유출된 빌더를 사용한 랜섬웨어들이 꾸준히 발견되어 왔으며, 2024년 10월 LockBit 2.0과 동일한 바탕화면 이미지를 사용하고 MacOS를 겨냥한 NotLockBit 랜섬웨어가 발견됐다. LockBit을 모방해 개발된 NotLockBit 랜섬웨어는 Apple Silicon MacOS에서 동작하는 ARM 바이너리가 아닌, x86-64 기반의 바이너리로 작성되어 인텔 CPU를 사용하는 MacOS거나, Rosetta를 사용하는 MacOS에서만 감염된다. 현재까지 이 랜섬웨어가 유포된 정황이 확인되지 않았지만, Windows 혹은 Linux 보다 상대적으로 안전하다고 느꼈던 MacOS 역시 랜섬웨어 공격자들의 관심 대상이 되고 있음을 시사한다.

Meow 랜섬웨어 그룹은 Conti 랜섬웨어 그룹의 유출된 소스코드를 악용하여 만든 변종 랜섬웨어로 2022년 8월부터 활동을 시작했으며, 2023년 3월에 복호화 도구가 출시되어 잠시 종적을 감췄다. 이후 2023년 11월에 데이터 유출 사이트를 개설한 뒤 피해자를 게시하기 시작했는데, 그 수가 매월 큰 폭의 상승세를 보여 위협적인 랜섬웨어 그룹으로 자리 잡았다. 다크웹 유출 사이트에서는 정보의 가치에 따라서 가격을 다르게 책정해 기재하기도 하는 모습을 보이고 있다.

Hunters International 그룹은 Hive 랜섬웨어를 기반으로 한 그룹으로, SharpRhino RAT(Remote Access Trojan)를 최근 공격에 사용하기 시작했다. SharpRhino는 사용자의 오타를 유도하기 위해 정상 도메인의 일부를 변형한 타이포스쿼팅³ 도메인을 통해 웹사이트를 구축했다. 사용자가 해당 도메인에 잘못 접속하면, 정상적인 오픈소스 프로그램인 Angry IP Scanner로 위장한 악성코드가 존재하며, 사용자는 이를 정상 프로그램으로 착각해 파일을 다운로드 받아 실행한다. 이 악성코드는 정상 프로그램처럼 보이도록 유효한 인증서로 서명되어 있어 보안 솔루션을 우회할 수 있으며, 사용자의 의심 없이 시스템에 상주하며 악성 행위를 수행한다. 이처럼 랜섬웨어 그룹들은 공격에 인포스틸러나 RAT와 같은 악성코드도 함께 사용하는 전략을 취하고 있는 추세이다.

³ 타이포스쿼팅: 정상 URL의 일부를 변경해 등록된 뒤 사용자의 도메인 입력 실수를 통해 웹사이트에 접속하도록 유도하는 기법

3. 랜섬웨어 트렌드

✓ Cloud 환경을 노리는 랜섬웨어 공격

기업들의 클라우드 도입이 늘어남에 따라, 온프레미스⁴의 보안성과 클라우드의 유연성을 모두 활용할 수 있는 하이브리드 클라우드가 주목받고 있다. 이러한 변화로 기업의 핵심 자산과 데이터가 점점 더 클라우드로 이전됨에 따라, 사이버 공격자의 표적도 자연스럽게 기업 내부에서 클라우드 환경으로 확대되고 있다.

Embargo 랜섬웨어를 유포하는 공격 그룹은 최근 특정 기업에 침투해 내부 계정 정보를 탈취하고 내부 이동을 통해 시스템을 장악한 뒤, 계정 정보를 기반으로 기업의 클라우드 환경까지 침해한 뒤 정보를 탈취했다. 공격 그룹은 내부에서 탈취한 계정 정보를 기반으로 온프레미스 Active Directory와 클라우드 상의 Entra ID간의 동기화를 수행하는 Microsoft Entra Connect Sync⁵ 서비스를 악용해 패스워드를 동기화 한 후 클라우드 서비스에 접속했다. 추가적으로, 시스템 내에서 탈취한 계정과 동일한 계정을 사용하는 클라우드 계정 중 다중 인증이 적용되지 않은 계정을 찾아 기업의 클라우드 환경에 접속해 공격을 수행했다.

탈취한 계정 정보를 악용한 공격 외에도 Web Service 환경을 침해하는 랜섬웨어 공격 사례도 확인됐다. AWS(Amazon Web Services) 서비스를 사용하는 서비스 사용자의 잘못된 설정으로 인해 환경 설정 파일인 .env 파일이 외부에 노출되었고, 공격자는 이 파일을 수집해 AWS IAM(Identity and Access Management)⁶ 액세스 키를 무단으로 수집해 호스팅 된 클라우드 서비스에 접속한 뒤 시스템을 장악하고 랜섬웨어를 유포했다.

⁴ 온프레미스: 기업 내에서 자체적으로 서버를 보유해 자체 클라우드를 운영하는 방식

⁵ Microsoft Entra Connect Sync: 온프레미스 Active Directory와 Microsoft Entra ID를 연동 및 동기화 하는 도구

⁶ AWS Identity and Access Management: AWS 리소스에 대한 사용자 및 그룹의 접근 권한을 관리하는 서비스

✓ 랜섬웨어 그룹의 취약점 악용

3분기에도 취약점을 악용한 공격이 이어지고 있다. Medusa 랜섬웨어 그룹은 FortiClientEMS⁷ 시스템에서 임의 명령 실행이 가능한 CVE-2023-48788 취약점을 활용해 공격하고 있으며, RansomEXX 그룹은 CVE-2024-23897 취약점을 악용하고 있다. 2024년 1월 공개된 CVE-2024-23897 취약점은 소프트웨어 빌드 및 배포 자동화 시스템인 Jenkins에서 명령어를 파싱하는 과정 중 잘못된 인자 처리로 인해 시스템 내부의 파일들을 읽어들 수 있는 취약점이다. RansomEXX 그룹은 지난 8월 1일 Jenkins 취약점을 악용해 은행 서비스 기술 제공업체인 Brontoo Technology Solutions에 침투 후 랜섬웨어를 유포했고, 이로 인해 Brontoo의 솔루션을 사용 중이던 인도의 한 은행에서 결제가 중단되는 사고가 발생했다.

2024년 8월에 공개된 SonicWall 제품의 취약점인 CVE-2024-40766 또한 공격에 사용되었다. 이 취약점은 SonicWall SonicOS 관리 액세스 및 SSLVPN⁸ 장비에서 부적절한 액세스 제어로 인해 무단 접근이 가능한 취약점이다. 지난 분기 CVE-2023-27532 취약점을 이용해 공격을 수행하던 Akira 랜섬웨어 그룹이 SonicWall 제품의 취약점을 통해 공격을 수행하는 정황이 발견됐다.

CVE	악용 공격자	설명	영향 버전
CVE-2023-48788	Medusa	SQL Injection 공격으로 xp_cmdshell 함수를 실행해 원격 코드 실행 가능	FortiClientEMS 7.0.1 ~ 7.0.10, 7.2.0 ~ 7.2.2
CVE-2024-23897	RansomEXX	CLI ⁹ 명령 파싱 과정에서 @ 문자를 해당 파일의 내용으로 변경해 임의 파일 읽기 가능	Jenkins (< 2.441) LTS 2.426.2
CVE-2024-40766	Akira	SonicWall SonicOS Management Access 와 SSLVPN 에서 부적절한 접근 가능	SOHO Gen 5 (<5.9.2.14-13o) Gen6 Firewalls (<= 6.5.4.14-109n) Gen7 Firewalls (<= 7.0.1-5035)

[3 분기에 랜섬웨어 그룹이 악용한 취약점 목록]

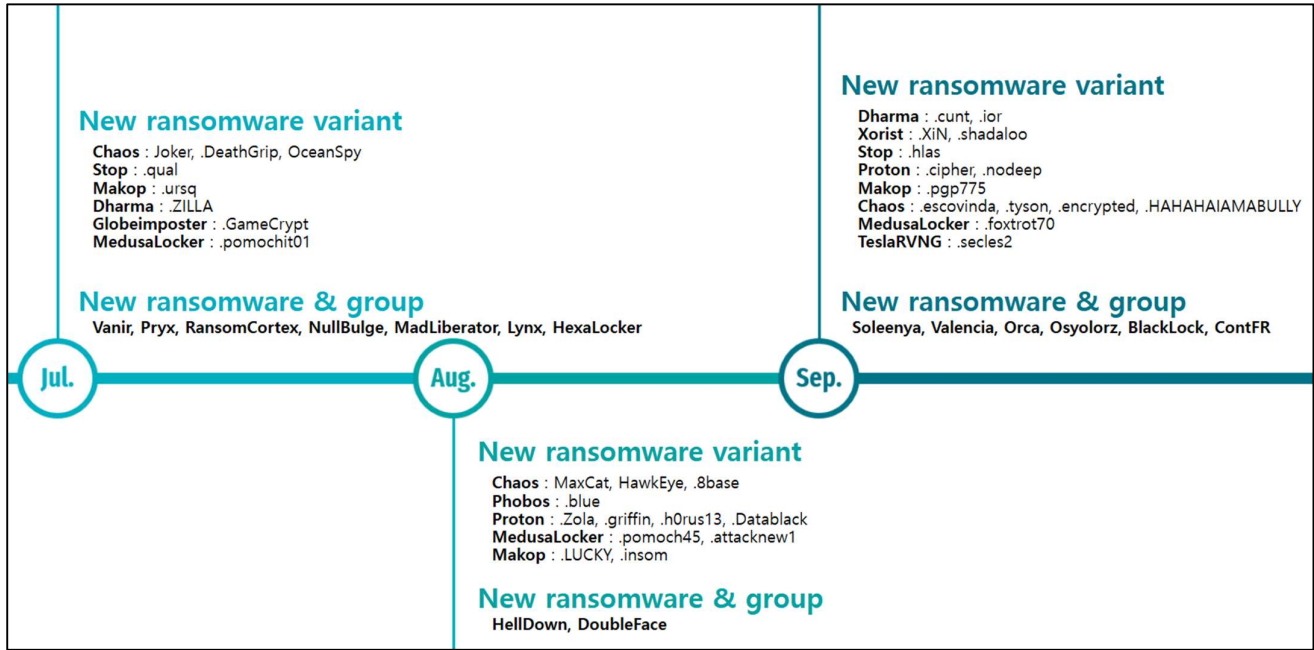
⁷ FortiClientEMS : Fortinet 사의 FortiClient 중앙 관리 콘솔 프로그램

⁸ SSLVPN: 인터넷을 통한 원격 접근시 암호화된 터널을 제공해 안전한 통신을 제공하는 가상 사설망 기술

⁹ CLI: Command Line Interface 로 명령줄 실행을 의미



4. 신규 랜섬웨어 및 그룹 활동



[신규/변종 랜섬웨어]

3분기에는 15개의 신규 랜섬웨어 그룹이 발견되었다.

7월에 등장한 NullBulge 랜섬웨어 그룹은 AI 중심 애플리케이션과 게임 커뮤니티를 타겟으로 삼고 있다. 이들은 가짜 개발자 계정을 통해 악성코드를 유포하며, 최근에는 디즈니의 내부 Slack¹⁰ 채널에서 1테라바이트 이상의 데이터를 유출했다고 주장했다. 현재 NullBulge의 웹사이트는 일시적으로 폐쇄된 상태이다.

HexaLocker는 LAPSUS\$ 그룹의 전 관리자가 운영하는 새로운 랜섬웨어 그룹으로, Golang으로 작성된 랜섬웨어를 이용해 파일 공격을 수행하며 파일 암호화와 탈취한 데이터 공개를 빌미로 금전을 갈취한다. 그러나 이 그룹은 최근 텔레그램 채널을 통해 LAPSUS\$를 포함한 그룹들과 제휴 탈퇴를 공지하며 HexaLocker 및 LAPSUS\$ 랜섬웨어의 소스코드를 판매한다고 밝히며 활동 중단을 선언했다.

8월에 발견된 신규 랜섬웨어 그룹 HellDown은 활동 시작 후 10일 만에 17건의 피해자를 게시하며 활발한 활동을 예고했으나, 8월 24일 이후로 활동을 중단한 상태이다. 8월 5일 텔레그램 채널을 개설해 활동을 시작한 Doubleface 랜섬웨어 그룹은 다양한 랜섬웨어 그룹들과 제휴를 맺으며, 랜섬웨어 유포 및 웹사이트 변조 공격 등을 감행하고 있다.

9월에는 총 6개의 신규 랜섬웨어 그룹이 발견되었다. 이 중 LockBit 3.0을 기반으로 한 Soleenya 랜섬웨어와 ZEPPELIN 랜섬웨어를 기반으로 한 Orca 랜섬웨어는 기존 랜섬웨어를 활용한 사례이다. 아래는 3분기에 발견된 주요 랜섬웨어 그룹에 대한 설명이다.

¹⁰ Slack: 기업내 협업을 위한 클라우드 기반 협업 도구 및 메신저

- **Lynx**

7월에 활동을 시작한 Lynx 랜섬웨어 그룹은 주로 북미와 유럽 전역의 소매, 부동산, 건축, 금융과 같은 다양한 산업 분야를 타겟으로 20곳 이상의 피해자를 데이터 유출 사이트에 공개했으며, 현재까지 꾸준히 활동하고 있다. Lynx 랜섬웨어는 AES-128 알고리즘과 Curve25519¹¹를 사용해 파일을 암호화하며, 암호화된 파일에는 .lynx 확장자를 추가한다. 또한 실행시 인자에 따라 프린트 관련 기능이 동작하며, 옵션이 활성화된 경우 감염된 시스템에 연결된 프린트 장치를 찾아 랜섬 노트를 출력한다.

- **Vanir**

Vanir 랜섬웨어는 2024년 7월 새롭게 등장한 그룹으로 3개의 기업을 데이터 유출 사이트에 공개하며 등장했다. Vanir 그룹의 다크웹 데이터 유출 사이트는 Akira 랜섬웨어 그룹의 명령줄 도구 스타일의 인터페이스와 유사한 형태로 구성되어 있어 Akira 그룹과의 연관성이 의심되지만 단순 모방의 가능성도 존재한다. Vanir 그룹을 운영하던 BlackEyedBastard는 Karakurt, LockBit 및 Knight와 같은 랜섬웨어 그룹의 전 계열사라 주장하며 자신들이 운영중인 랜섬웨어 서비스의 제휴사를 찾고 있다고 광고해왔다. 그러나 이들의 데이터 유출 사이트는 지난 9월 독일 사법기관에 의해 폐쇄되었고, 이후 추가적인 활동은 확인되지 않고 있다.

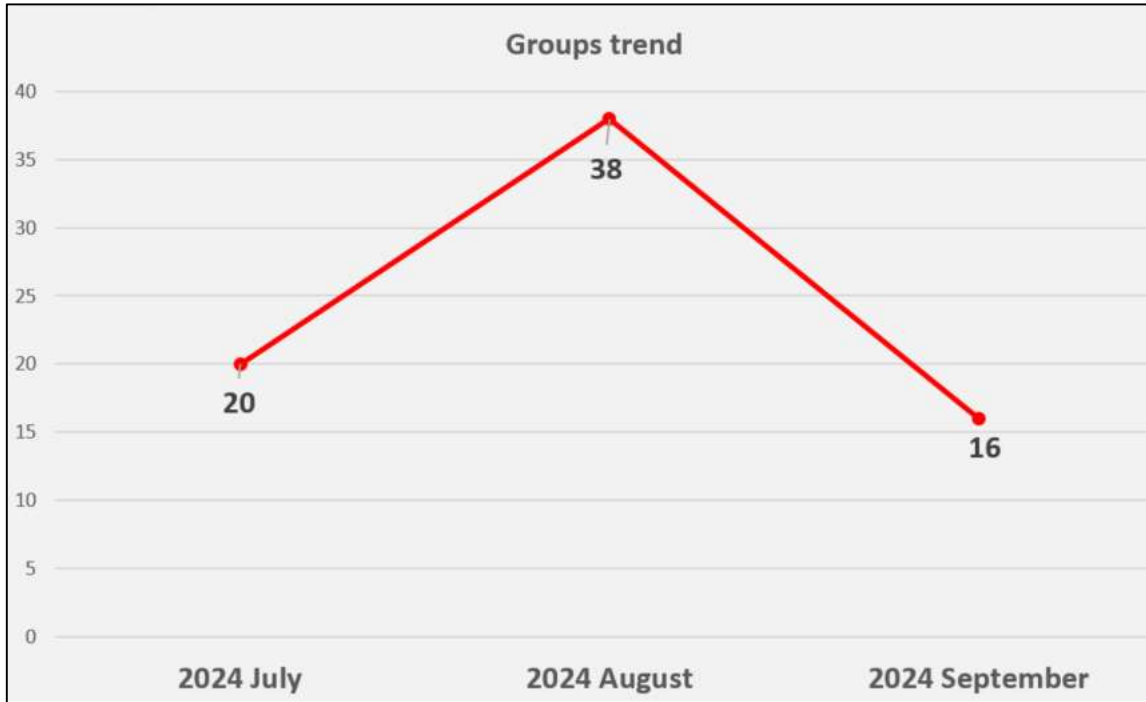
- **RansomCortex**

RansomCortex 그룹은 2024년 7월 11일 데이터 유출 사이트에 첫 게시물을 올리며 활동을 시작했다. 흥미로운 점은, 한 언론사에서 RansomCortex의 멤버 중 한 명과 인터뷰를 진행했는데, 인터뷰에 의하면 이들은 독립국가, 이란, 북한, 중국, 경찰서는 공격하지 않는다는 규칙을 가지고 있으며 주요 공격 대상으로 가장 민감하고 중요한 데이터를 다루는 병원들 중 영어, 이탈리아어, 스페인어, 포르투갈어를 구사하는 곳이라 밝혔다. RansomCortex 그룹은 취약점을 악용하기도 하지만 자체적으로 정보를 수집하고 공격을 수행하기 위한 다양한 전문가들과 함께 하고 있다고 밝혔다.

¹¹ Curve25519 : 빠른 속도와 보안성을 제공하는 타원곡선 기반의 비대칭키 암호화 알고리즘

■ Meow Ransomware 그룹 상세 분석

1. Meow 개요



[Meow 랜섬웨어 그룹의 3 분기 공격 건수]

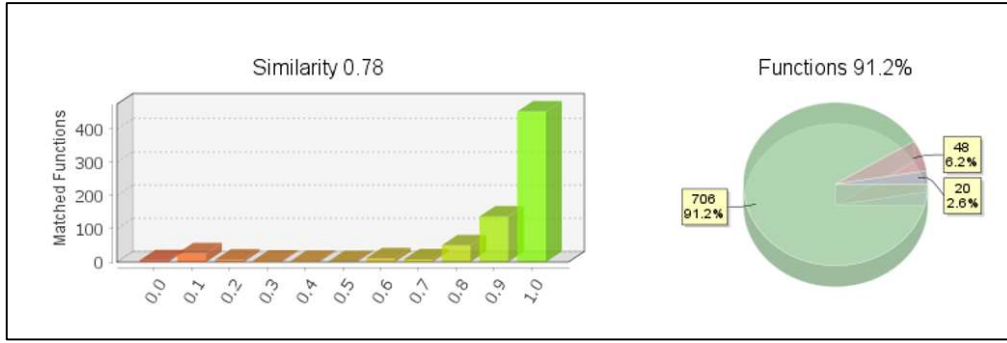
2022 년 3 월, Conti Ransomware 의 소스코드가 유출되는 사건이 발생했다. 러시아의 우크라이나 침공 이후 러시아 기반의 사이버 범죄 그룹으로 추정되는 Conti 그룹이 러시아를 지지하는 메시지를 공개하면서, 이에 대한 보복으로 우크라이나의 한 연구원에 의해 Conti, Ryuk 랜섬웨어 갱단의 채팅 서버의 메시지와 랜섬웨어 암호화, 빌더 등이 포함된 랜섬웨어 자료가 유출되었다.

소스코드가 유출되자 공격자들은 이 소스코드를 기반으로 새로운 변종 랜섬웨어를 개발하고 유포해 다양한 공격을 수행했다.

Ransomware	확장자	발견일
Mimic	.QUIETPLACE	2022-06
Monti	.monti	2022-06
Meow	.meow	2022.09 ~
BlueSky	.bluesky	2022-06 ~
Putin	.PUTIN	2022-08 ~2022-11
ScareCrow	.CROW	2022-11

[Conti 파생 랜섬웨어]

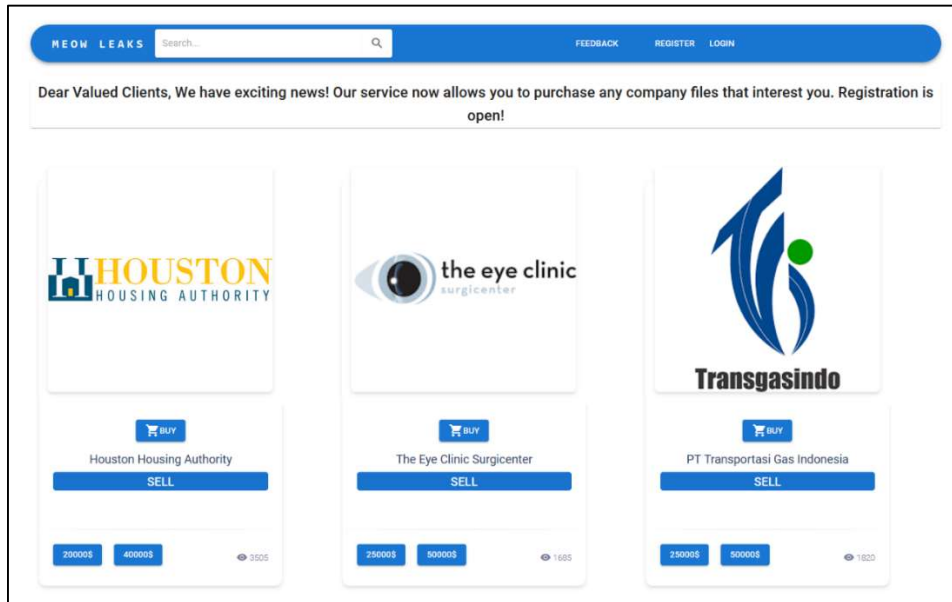
Meow 랜섬웨어는 유출된 Conti 소스코드로 개발된 변종 랜섬웨어 중 하나로 다른 변종 랜섬웨어들과 비슷한 시기인 2022 년 8 월부터 활동을 시작했고 이후 다양한 공격을 수행하며 257 여 명의 피해자를 감염시키는 등 활발하게 활동하고 있다.



[Meow 랜섬웨어와 Conti 랜섬웨어의 유사도]

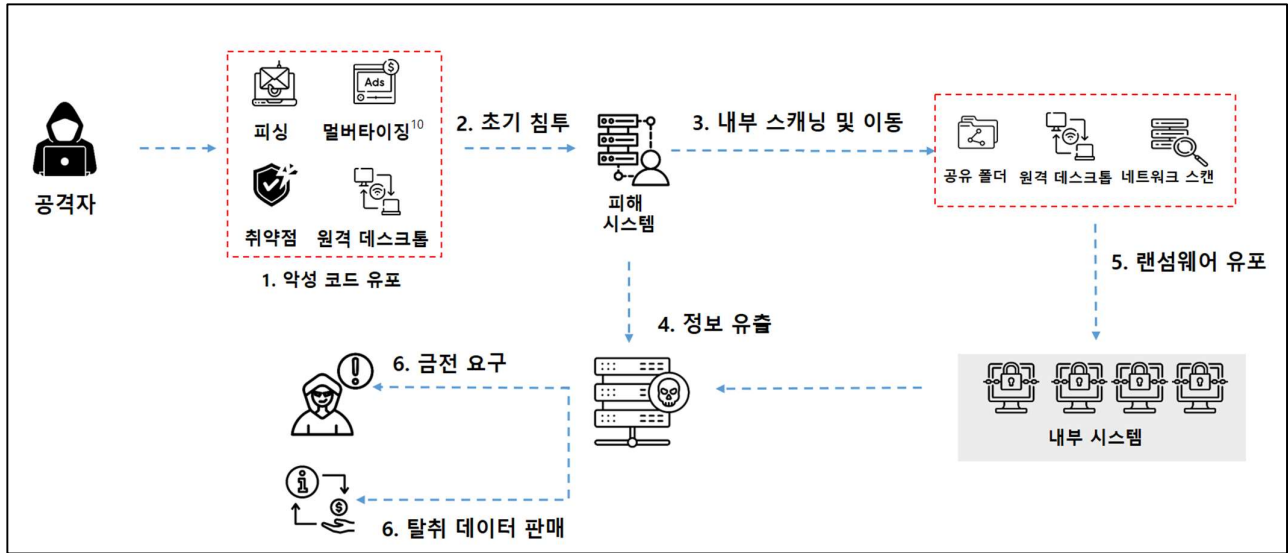
2023 년 2 월경 Meow 랜섬웨어 그룹은 포럼을 통해 활동 중단을 선언한 뒤 모든 개인 키와 복호화 도구를 공개했다. 이후 카스퍼스키는 이 데이터를 기반으로 복호화 도구를 개발해 유포했으며 이후 Meow 그룹은 더 이상 활동하지 않았다. 카스퍼스키는 공개된 정보들을 분석해 복호화 도구를 개발해 배포하면서, 약 257 여개의 그룹 또는 개인이 피해를 당했으며 14 명의 피해자가 몸값을 지불한 것으로 보인다고 밝혔다.

잠적했던 meow 랜섬웨어 그룹은 2023 년 11 월 활동을 재개했다. Vanderbilt 대학 메디컬 센터를 다크웹 데이터 유출 사이트에 게시하면서 다시 활동을 시작했다. 활동 재개 이후 이들의 공격 방식은 과거 랜섬웨어를 통한 파일 암호화를 이용한 협상에서, 데이터 유출을 중심으로 방향을 선회했다. Meow 랜섬웨어 그룹은 시스템에 침투해 정보를 탈취하고 랜섬웨어를 감염시킨 후 사용자를 협박하거나, 유출한 데이터를 다크웹에 게시해 협상에 실패할 경우 데이터를 판매하는 방식으로 수익을 올렸다.



[Meow 랜섬웨어의 데이터 유출 사이트]

2. Meow 랜섬웨어 공격 시나리오



[Meow 랜섬웨어 공격 시나리오]

Meow 랜섬웨어 공격자는 다양한 방식을 통해 초기 침투를 수행하며 주로 네 가지 방식을 사용하고 있다.

첫번째는 방식은 멀버타이징(Malvertising)¹² 공격으로 광고 사이트를 공격해 악성 스크립트를 삽입하고 광고가 노출될 때 취약점을 이용해 기업 내 시스템에 침투하는 방식이다. 이 방식은 스피어 피싱¹³과 같은 대상을 특정 지어 공격하는 케이스와 달리 불특정 다수를 대상으로 하는 공격 방식이며 공격자는 취약점을 통해 감염된 사용자가 랜섬웨어 공격에 큰 영향을 받을 수 있는 기업일 경우 추가적인 침투를 수행한다.

두번째는 고전적인 공격 방식인 피싱 이메일을 이용한 공격으로 공격자는 이메일 등에 악성 링크 등을 첨부하고 기업들의 공개된 이메일로 전송한 뒤 사용자의 클릭이나 파일 다운로드를 통해 악성코드를 실행해 시스템을 감염시키고 초기 침투를 수행한다.

세번째 공격 방식은 취약점을 이용한 공격으로, 외부 인터넷에 접점이 있는 서버나 서비스 등의 취약점을 이용해 악성 스크립트를 설치 후 초기 침투를 수행하는 방식이다.

마지막으로 공격자는 원격 접속인 RDP(Remote Desktop Protocol)를 이용한 최초 접근을 수행한다. 공격자는 외부에 알려지거나, 다크웹 등에서 판매되는 기업의 RDP 계정 정보를 획득해 접근하거나, 혹은 공개된 원격 접속 취약점을 통해 기업에 침투한다.

공격자의 최초 침투 이후, 내부 네트워크 전체를 장악하기 위해 내부 네트워크를 스캔하고, 원격 공유 폴더 내 파일들을 조작하거나, 내부 시스템의 원격 연결 시스템 등을 악용해 전체 시스템 장악을 수행한 후 침투한 네트워크 내 중요 정보를 공격자의 C2로 탈취한 후 Meow 랜섬웨어를 유포해 암호화를 수행한 뒤 금전을 요구한다.

¹² 멀버타이징(Malvertising): 광고 내 악성코드를 삽입해 악성코드를 유포하는 기술

¹³ 스피어 피싱: 특정 개인이나 단체를 표적으로 지정해 피싱을 수행하는 공격 방식

3. Meow 랜섬웨어 심층 분석

✓ 기능 분석

1) 분석 체크 사항

- 문자열 복호화

Meow 랜섬웨어가 실행될 때, 악성 행위에 필요한 모든 문자열을 암호화해 가지고 있으며 문자열을 사용할 때 복호화 후 악성행위에 사용한다.

```
v26[66] = 96;
v26[67] = 95;
v26[68] = 31;
qmemcpy(v27, "_2_2_1_2_E_e_E_9'_w___", sizeof(v27));
v28 = v7;
for ( i = 0; i < 0x5C; ++i )
    v26[i] = (11 * (95 - v26[i]) % 127 + 127) % 127;
```

[문자열 복호화 로직]

```
#Decrypt routine 1
dec = (((key1 - enc) * key2) % 0x7F) + 0x7F) % 0x7F
#Decrypt routine 2
dec = (((enc - key1) * key2) % 0x7F) + 0x7F) % 0x7F
```

[문자열 복호화 파이썬 코드]

- API 동적 로드

프로그램은 동적 API 테이블을 재구성해 사용하며 이를 위해 Windows API를 호출하기 전 특정 함수를 호출한다. 함수는 전달 받은 테이블 내 API 오프셋 위치에 주소가 존재할 경우 이를 반환하고, 저장된 주소가 없을 경우 함께 전달받은 4Byte 해시를 통해 API 주소를 검색하고 테이블에 저장한 뒤 반환한다.

```
addr = *(g_api_table_43939C + 4 * a3);
v8 = addr + 6035901;
v4 = ((addr + 6035901) & 0x80000003) == 0;
if ( addr + 6035901 < 0 )
    v4 = (((addr - 67) & 3) - 1) | 0xFFFFFFFF;
if ( v4 )
{
    do
        ++v8;
    while ( !(v8 % 4) );
}
if ( addr )
    return addr;
addr = GetApiAddr_4044B0(0, hash);
```

[문자열 동적 로드]

2) 기능 상세 분석

- 실행 인자 설정

랜섬웨어는 초기 실행 단계에서 프로그램 실행 시 전달받은 인자를 기반으로 실행을 위한 설정 값을 저장한다. 함수를 기반으로 실행 단계에서 전달받은 인자 정보를 가져와 인자들과 비교한 후 실행 플래그를 설정한다. 실행 인자는 총 다섯 개로 각각의 옵션 정보는 아래와 같다.

설정 값	설정 정보
-p	특정 디렉토리를 지정해 암호화 수행
-m	local/net/all 옵션과 함께 사용해 암호화 대상 파일을 지정 (로컬/네트워크/전체)
-size	대용량 파일 암호화를 위한 Chunk 크기 지정
-log	암호화 정보를 저장할 log 파일을 지정
-nomutex	Mutex ¹⁴ 를 생성하지 않고 악성행위 수행

[랜섬웨어 실행 인자]

전달받은 인자를 비교하기 위해 문자열을 복호화해 비교를 수행한다.

```

v43[11] = 29; // -log
LogFlag = CheckArgv_41C600(v5, NumberOfArgv, v44);
for ( m = 0; m < 0xC; ++m )
    v43[m] = (36 * (29 - v43[m]) % 0x7F + 127) % 0x7F;
v37 = 0;
v9 = CheckArgv_41C600(v36, NumberOfArgv, v43);
v38 = 16;
qmemcpy(v39, "BcBpBVB?B2BmBfBBB", 17);
v45 = v9;
for ( n = 0; n < 0x12; ++n ) // -size
    v39[n - 1] = (39 * (66 - v39[n - 1]) % 0x7F + 127) % 0x7F;
v11 = v36;
p_NumOfArgv = NumberOfArgv;
    
```

[인자 비교를 위한 문자열 복호화]

¹⁴ Mutex: 중복 실행을 방지하기 위한 동기화 메커니즘

- 랜섬 노트 설정

파일 암호화 이후 감염 여부를 사용자에게 알리는 랜섬 노트 정보와, 암호화에 사용할 공개키를 특정 메모리 영역에 복사한다. 이 랜섬웨어의 노트를 구성하는 코드를 확인해보면 특정 메모리 영역에 사용자의 랜섬 노트를 입력하고 이후 나머지 공간을 0으로 채운 뒤 이를 다시 “_DECRYPT_NOTE_” 라는 문자열이 있는 메모리 영역으로 복사한다. 공격자의 공개키 또한 특정 공간에 존재하는 “_public_key_” 라는 문자열이 존재하는 영역으로 복사한다.

```
memset_422210(&ransom_note[283], 0, 0x3EF1u);
memcpy_4228D0(“_DECRYPT_NOTE_”, ransom_note, 0x400Cu);
memcpy_4228D0(“_public_key_”, &pubkey_430E40, 0x1000u);
return 1;
```

[랜섬 노트 및 공개키 복사]

- Mutex 생성

프로그램 실행 시 전달받은 인자 중 -nomutex 옵션에 따라 활성화되는 플래그를 확인한 후 플래그가 비 활성화되어 있다면 아래와 같은 이름으로 Mutex를 생성한다

- Mutex Name: hsfjuukjzloqu28oajh727190

```
v35[16] = 123;
v35[17] = 22;
qmemcpy(v36, “s,V,EN4”, sizeof(v36)); // Decrypt Mutex Name
for ( i = 0; i < 0x1A; ++i )
    v35[i] = (15 * (v35[i] - 125) % 127 + 127) % 127;
CreateMutexA = GetProcAddress_4052D0(15, 0x20D8FA8C, 84);
v8 = CreateMutexA(0, 1, v35); // v35 = “hsfjuukjzloqu28oajh727190”
WaitForSingleObject = GetProcAddress_4052D0(15, 0xE0C23134, 98);
```

[Mutex 설정]

- Volume Shadow Copy 삭제

윈도우 시스템은 특정 시점을 저장하고, 복원할 수 있는 Volume Shadow Copy를 제공한다. 이를 통해 감염된 시스템이 특정 시점으로 복구될 수 있어 랜섬웨어는 Volume Shadow Copy를 삭제하는 기능을 가지고 있다. WMIC를 이용하여 “SELECT * FROM Win32_ShadowCopy” 명령을 실행해 시스템 내부의 복구 이미지를 모두 가져온 뒤 아래 명령을 CreateProcess 함수 인자로 전달해 이미지를 삭제한다.

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where
“ID='{[VOLUME_SHADOW_ID]}” delete
```

[Volume Shadow Copy 삭제 명령어]

- 암호화 준비 단계

암호화를 수행하는 스레드가 실행되면, CryptImportKey를 통해 악성코드의 공개키를 암호화를 위해 등록한다. 이 값은 파일 암호화에 사용하는 키와 Nonce 값을 암호화하는 용도로 활용된다.

```
memcpy_4228D0(ransom_pubkey, "__public_key__", 0x1000u);
p_hCrypt = hCrypt;
CryptImportKey = GetApiAddress_4052D0(16, 1892860132, 55);
if ( !CryptImportKey(p_hCrypt, ransom_pubkey, 0x1000, 0, 0, &v28) )
{
    v5 = GetApiAddress_4052D0(15, -1480703512, 71);
    v5(1);
}
```

[Client ID 생성]

- 암호화 단계

공격자의 공개키를 등록하고 나면 디렉토리를 순회하며 예외 디렉토리 및 파일명, 암호화 대상 파일 확장자 등을 확인해 암호화를 수행한다. 랜섬웨어가 감염시키지 않는 디렉토리와 확장자는 다음과 같다.

폴더명	확장자
tmp	.MEOW
winnt	.exe
temp	.dll
thumb	.lnk
\$Recycle.Bin	.sys
\$RECYCLE.BIN	.msi
Boot	readme.txt
Windows	CONTI
Trend Micro	.bat
perflogs	

[암호화 제외 대상]

예외 디렉토리 및 파일 목록을 제외하고, 모든 파일에 대해 암호화를 수행한다. CryptGenRandom 함수를 통해 32바이트 암호화 키와 8 바이트의 Nonce를 생성하고 이 값을 기반으로 chacha8 암호화 알고리즘을 통해 파일 암호화를 수행한다.

랜섬웨어는 효율적인 파일 암호화를 위해 파일의 확장자 및 크기 등을 확인해 조건에 따른 암호화를 수행한다.



- 데이터 베이스 파일 암호화

랜섬웨어는 파일의 확장자가 데이터베이스 파일 형태인지 확인하며, 데이터베이스 파일인 경우에는 다른 조건을 확인하지 않고 파일 전체에 대한 암호화를 수행한다. 악성코드가 확인하는 데이터베이스 파일의 확장자는 다음과 같다.

4dd	4dl	acddb	accdc	accde	accdr	accdt	accft	adb	ade
adf	adp	arc	ora	alf	ask	btr	bdf	cat	cdb
ckp	cma	cpd	dacpac	dad	dadiagrams	daschema	db	db-shm	db-wal
db3	dbc	dbf	dbx	dbt	dbv	dbx	dcb	dct	dcx
ddl	dli	dp1	dqy	dsk	dsn	dtsx	dxi	eco	ecx
edb	epim	exb	fcd	fdb	fic	fmp	fmp12	fmpsl	fol
fp3	fp4	fp5	fp7	fpt	frm	gdb	grdb	gwi	hdb
his	ib	idb	ihx	itdb	itw	jet	jtx	kdb	kexi
kexic	kexis	lgc	lwx	maf	maq	mar	mas	mav	mdb
mdf	mpd	mrg	mud	mwb	myd	ndf	nnt	nrmlib	ns2
ns3	ns4	nsf	nv	nv2	nwdb	nyf	odb	oqy	orx
owc	p96	p97	pan	pdb	pdm	pnz	qry	qvd	rbf
rctd	rod	rodx	rpd	rsd	sas7bdat	sbf	scx	sdb	sdc
sdf	sis	spq	sql	sqlite	sqlite3	sqlitedb	te	temx	tmd
tps	trc	trm	udb	udl	usr	v12	vis	vpd	vvv
wdb	wmdb	wrk	xdb	xld	xmlff	abcddb	abs	abx	accdw
adn	db2	fm5	hjt	icg	icr	kdb	lut	maw	mdn
mdt									

[암호화 대상 데이터베이스 파일]

파일의 확장자를 확인해 디스크 이미지 파일 여부를 확인한다. 디스크 이미지의 경우 주로 사이즈가 커서 빠른 암호화를 위해 전체 암호화를 진행하지 않고 부분 암호화를 진행한다. 디스크 이미지 암호화를 위한 확장자 목록은 다음과 같다.

vdi	vhd	vmdk	pvm	vmem	vmsn	vmsd	nvr	vmx	raw
qcow2	subvol	bin	vsv	avhd	vmrs	vhd	avd	vmc	iso

[암호화 대상 디스크 이미지 파일]

디스크 이미지 파일인지 확장자를 확인하는 로직에 코딩 실수가 확인됐다. 대상 파일이 디스크 이미지 파일인 경우 함수는 1을 리턴해 파일 크기에 따라 부분 암호화를 진행해야 하지만, 랜섬웨어는 함수 내에서 확장자 비교 후 항상 0을 반환하도록 작성되어 있어 디스크 이미지 암호화 로직을 따르지 않고 일반 파일 암호화 로직에 따라 암호화가 진행된다.

```

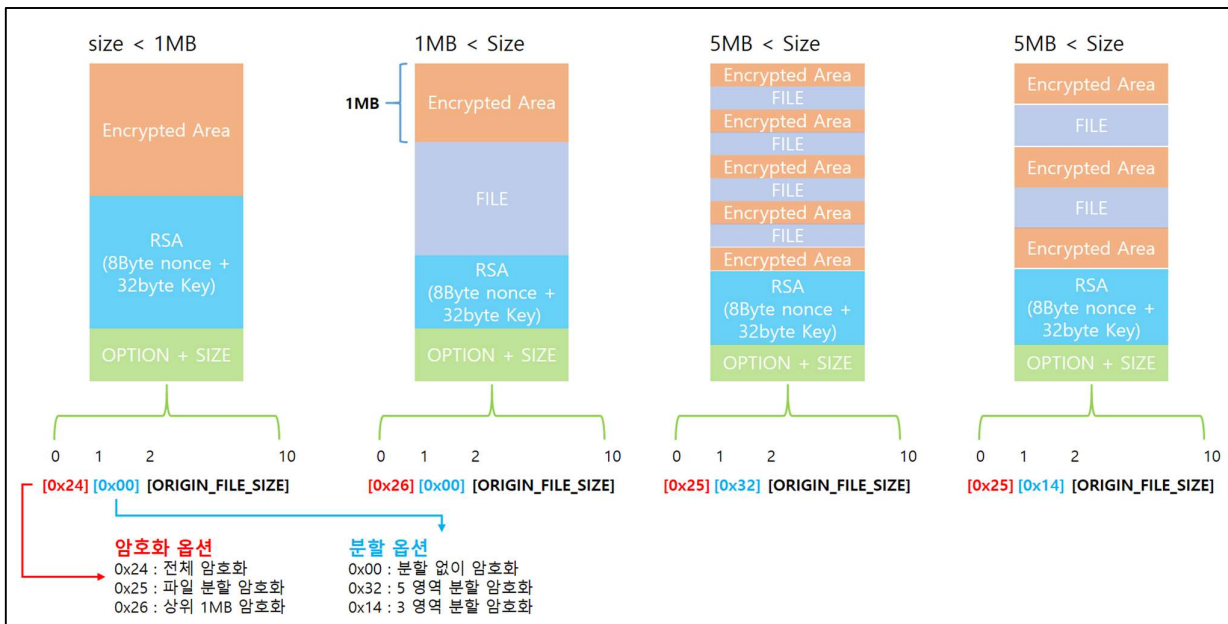
}
  strstrIA = GetApiAddress_4052D0(22, -122749343, 23);
  if ( strstrIA(extension, target_extension[v22]) )
    break;
  ++v22;
}
while ( v22 < 20 );
return 0;
}

```

[확장자 확인 여부와 관계없는 0 반환]

• 일반 파일 암호화

암호화 대상 파일이 데이터베이스 파일이나 디스크 이미지가 아닌 경우 파일 크기에 따라 암호화를 진행한다. 파일의 크기가 1MB 이하인 경우 파일 전체에 대한 암호화를 수행하고, 크기가 1MB 이상인 경우 상위 1MB만 암호화, 파일이 5MB 이상인 경우 파일을 다섯 개 영역으로 나눠 부분 암호화를 진행한다. 암호화를 완료하면 파일 끝부분에 RSA 알고리즘으로 암호화한 chacha8의 32바이트 Key와 8Byte Nonce 값을 추가하고, 이후 암호화 설정(1byte)과 암호화 영역 설정(1byte), 그리고 원본 파일의 크기(8byte)를 파일의 끝부분에 추가한 뒤 암호화를 종료한다.



[옵션별 암호화 방식]

- 랜섬노트 생성

암호화가 완료되면 해당 디렉토리에 redeme.txt 파일을 생성하고 랜섬노트를 작성한다.

```
"MEOW! MEOW! MEOW! \n"
"\n"
" Your files has been encrypted! \n"
"\n"
" Need decrypt? Write to e-mail: \n"
"\n"
" meowcorp2022@aol.com\n"
"\n"
" meowcorp2022@proton.me \n"
"\n"
" meowcorp@msgsafe.io \n"
"\n"
" meowcorp@onionmail.org\n"
"\n"
" or Telegram: \n"
"\n"
" @meowcorp2022 \n"
"\n"
" @meowcorp123 \n"
"\n"
" Uniq ID: 4d2942e6-49a6-410b-9a09-a02423f53e1c");
```

[Meow 랜섬노트]





4. IoCs

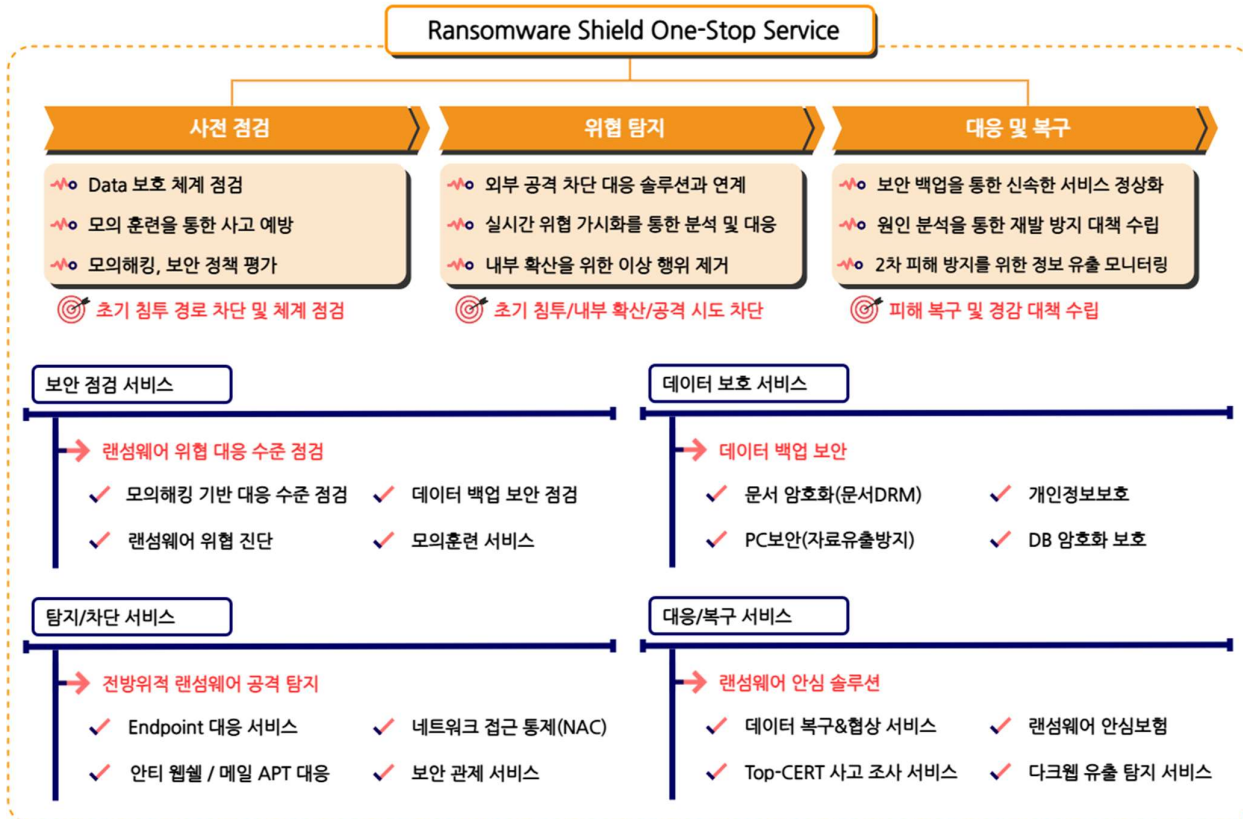
SHA256
222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853
7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099
0856ab4ba1732ffb7c98fbdf806b3af41ad5015ae6cc08f1c1fbb72bf44de7d8
8ba84d65308e49007860e339dc93c1c4304e39755ba00a4cb4373bee7df37e0f
d7573284c29cf5f68bb64860f1be0a696c852678fac36f176fd88f555ed853f2

■ 랜섬웨어 Mitigations

1. Meow 랜섬웨어 대응방안 안내

Meow 랜섬웨어는 피싱과 멀버타이징 등 다양한 공격 경로를 통해 초기 침투를 수행하며, RDP와 공유 폴더를 활용한 내부 전파로 시스템을 장악하는 특징을 보인다. 특히 중요 정보 유출 후 이를 다크웹에서 판매하는 방식을 사용하고 있어, 몸값 지불 여부와 관계없이 추가적인 피해가 발생할 수 있다는 점에서 각별한 주의가 요구된다. 따라서 기업은 외부 접점이 있는 시스템에 대한 철저한 보안 관리와 지속적인 업데이트를 수행해야 하며, RDP와 같은 원격 접속 서비스는 비활성화하거나 강력한 보안 정책을 적용하는 등 선제적인 보안 강화 조치를 실시해야 한다.

3Q Key Point			
	FortiGuard	CVE-2023-48788	(FortiClientEMS 7.0.1~7.0.10, 7.2.0~7.2.2)
	Jenkins	CVE-2024-23897	(Jenkins < 2.441, LTS 2.426.2)
	VMWare ESXI	CVE-2024-37085	(VMWare Cloud Foundation 4.x, 5.x)
	SonicWall	CVE-2024-40766	(SonicWall SOHO Gen6, Gen6/7 Firewalls)



2. SK 쉐더스 MDR 서비스

랜섬웨어에 전문적으로 대응하기 위해서 SK 쉐더스의 MDR(Managed Detection and Response) 서비스¹⁵를 사용하는 것이 효과적인 방안이 될 수 있다. 최근 랜섬웨어 공격자들의 치밀한 전략과 고도화된 탐지 회피 기법으로 인해 기존의 방어 체계만으로는 위협에서 벗어나기 어려운 상황이다. 이를 해결하기 위해 SK 쉐더스는 실시간으로 네트워크를 모니터링하고 이상 징후를 감지하며 필요시 즉각적으로 대응할 수 있는 MDR 서비스를 제공하고 있다. 랜섬웨어 공격은 사전 예방이 무엇보다 가장 중요하지만, 피해가 발생했을 경우 신속한 조치를 통해 피해를 최소화하는 것 또한 매우 중요하다. 따라서 기업에서는 전담 조직의 신속하고 정확한 사고 조사와 분석을 토대로 맞춤형 보안 솔루션을 제공하는 SK 쉐더스의 MDR 서비스를 고려하는 것을 추천한다.

SK 쉐더스 MDR Service 3가지 특징점

서비스 내용

01	EDR 전문가 운영 대행
Managed	<ul style="list-style-type: none"> • 24 X 7 관제 요청 접수 및 대응 • IoC 및 SK-Defined Rules 업데이트 • 정책 운영 및 예외처리 반영 • 이벤트 분석 & 대응 조치
02	SK 쉐더스 상세 분석 서비스
Detection	<ul style="list-style-type: none"> • EDR/악성코드 전문가 분석 서비스 • EDR 기능을 통한 악성행위 추적 지원 • 상세분석을 통한 정/오탐 대응 • 주기적 위협현황 수행
03	침해사고 관점 통찰력
Response	<ul style="list-style-type: none"> • 국내 최다 침해사고 분석 및 조사 노하우 적용 • 침해 흔적 점검 진행 • 국내 침해지표(IoC) EDR 우선 적용



EDR 전문가 관제서비스

- ✓ EDR 전문 관제 서비스
 - 다수 고객사 서비스 제공 중
 - 다양한 산업군별 레퍼런스 고객 요청 대응 가능
- ✓ 사용자 만족도 향상
 - 숙련된 운영 전문가 신속한 대응



전문가 서비스 활용

- ✓ TOP-CERT 활용 가능
 - 24X7 긴급 로컬 투입
 - 국내 최다 사고분석 및 조사 대응
- ✓ SK 쉐더스 보안 전문가 서비스 활용 가능
 - 분석 전문가 상시 대응
 - 보안 전문가 분석 서비스 (악성코드분석가 + CERT)
 - 전담 조직 체제로 정확/신속 서비스



국내 최대 보안 수준 대응

- ✓ 서비스 통한 정보유출 불가
 - 첨부파일 자사 망내 분석
 - 당사 전용 분석 환경 보유
- ✓ 사전 보안위협 대응역량 강화
 - 고객 보안 부서와 협업 위협 확산 선 차단 가능

¹⁵ MDR 서비스: 실시간 위협 감지와 대응을 통해 사이버 공격으로부터 조직을 보호하는 관리형 보안 서비스



안녕을 지키는 기술 |  SK 쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
<https://www.skshieldus.com>

발행인 : SK쉴더스 EQST/시솔루션사업그룹 & KARA(Korea Anti Ransomware Alliance)

제 작 : SK쉴더스 마케팅그룹

COPYRIGHT © 2024 SK SHIELDUS. ALL RIGHT RESERVED.

본 저작물은 SK쉴더스의 서면 동의 없이 사용될 수 없습니다.