CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

2022년 3월 15일

2021 멀웨어 및 TTP 위협 경향 보고서

Recorded Future®

연례 위협 보고서는 레코디드 퓨처의 위협 연구 팀인 Insikt Group이 생성한 1년 동안의 인텔리전스를 요약하여 2021년 위협 환경을 평가한다. 이를 위해 언론사와 같은 공개 소스 및 다른 보안 그룹의 공개 연구와 다크웹 비공개 소스를 포함한 Recorded Future® 플랫폼 데이터를 기반으로 글로벌 동향, 멀웨어 동향, 주요 TTP(tactics, techniques, and procedures)를 분석한다. 이 보고서는 2021년 사이버 위협 환경에 대한 광범위하고 전체적인 관점을 원하는 모든 사람에게 흥미로운 정보를 제공할 것이다.

개요

2021년 파괴적인 대규모 공격과 최신 공격 툴 개발이 이어지면서 랜섬웨어 관련 위협이 보안 팀의 최우선 과제가 되었다. 랜섬웨어는 여러 산업 분야를 망라한 전 세계 조직들의 주요 위협으로 자리 잡았다. 2019년 말부터 2020년 전반에 걸쳐 랜섬웨어는 대규모 조직의 주요 위협으로 등극했다. 대규모 조직은 고수익을 위한 'Big Game Hunting'을 노리는 공격자들에게 주요 타깃이 되었다. 그러나 랜섬웨어 시장은 2020년과 2021년에 걸쳐 랜섬웨어 운영자가 증가하고 공격이 더욱 광범위해진 상품화된 시장으로 진화했다. 위협 행위자는 랜섬웨어 기능을 개발하기 위해 전문가를 고용하고, 랜섬웨어를 임대하고, 초기 액세스 브로커로부터 피해 조직의 네트워크 액세스를 구매했다. 2021년에도 랜섬웨어는 사이버 범죄 세계에서 성공적인 비즈니스를 계속했으며 Conti와 LockBit이 가장 많은 랜섬웨어 공격을 주도했다.

2020년 랜섬웨어 그룹들은 주로 이중 갈취(Double-Extortion) 방식을 사용했는데, 이는 피해자의 시스템 액세스를 잠글 뿐만 아니라 랜섬머니를 지불하지 않으면 데이터를 유출시키거나 판매하겠다고 위협함으로써 돈을 지불하도록 추가 압력을 가하는 것이다. 2021년에는 위협 행위자들이 전술을 변경하여 삼중 갈취(Triple Extortion) 기술을 구현했다. 삼중 갈취는 기업 네트워크를 침해할내부자를 모집하고, 피해 조직의 고객에게 연락하여 랜섬머니 지불을요구하고, DDoS(분산 서비스 거부) 공격으로 랜섬웨어 피해 조직을위협하고, 공급망과 관리 서비스 제공업체를 대상으로 피해를 확대하는 방식이다. 또한 일부 랜섬웨어 그룹이 Linux 시스템을 타깃으로삼기 시작하면서 빠른 취약점 익스플로잇과 제로데이 취약점 악용이공격에 추가되었다.

2021년 다크웹 시장에서는 계정 도용 거래가 활발히 이루어졌다. 랜섬웨어 운영자가 공격 초기 액세스에 유출된 계정 정보를 사용하는 경우가 많기 때문에 이러한 다크웹 시장의 활성화는 랜섬웨어 공격에도 기여했다. 인포스틸러(Infostealer)를 사용하여 훔친 계정 정보들이 다크웹에서 유통되었다. 이렇게 노출된 암호는 회사 계정이 유출된 로그에 포함되거나 직원이 개인 계정과 직장 계정에서 암호를 재사용할 경우에 네트워크를 위험에 빠뜨린다.

랜섬웨어와 더불어 멀웨어, Cobalt Strike와 같은 악성 툴들 또한 설치 시 탐지가 어렵고 더욱 위험하게 진화했다. 특히 2021년 후반에 지금까지 발견된 최악의 보안 결함 중 하나로 알려진 Log4Shell이 공개되면서 멀웨어 공격에서 급속한 취약점 익스플로잇이 계속되는 추세가 확인되었다.

마지막으로, Insikt Group은 2021년 주요 MITRE ATT&CK TTP 조사를 통해 상위 5가지 기술을 파악했다. 상위 5가지 기술은 다음과 같다.

T1486 (Data Encrypted for Impact), T1082 (System Information Discovery), T1055 (Process Injection), T1027 (Obfuscated Files or Information), T1005 (Data from Local System)

2021년 랜섬웨어 동향

2021년 미국 식품가공업체 JBS와 IT 관리 회사 Kaseya를 비롯한 유명 기업들이 랜섬웨어 공격을 받았다. 그 중에서도 가장 파급력이 컸던 것은 미국 가스회사 Colonial Pipeline을 타겟으로 한 공격이다. 이 공격은 해당 기업의 정상적인 운영을 중단시켰을 뿐만 아니라 미 동부 해안 전역의 가스 유통 및 가격에 심각한 타격을 입혔다. 이 공격은 랜섬웨어로 인해 발생할 수 있는 막대한 피해를 실제로 보여주었고, 미국 정부와 전 세계 법집행 기관들이 보다 적극적인 랜섬웨어 단속에 나서는 계기가 되었다.

사이버 범죄자들이 고가치 표적을 공격하여 큰 이익을 얻는 것이 알려지면서 새로운 랜섬웨어 그룹이 속속 등장했다. 이들은 거의 모두 이중 갈취(Double-Extortion)라는 새로운 데이터 탈취 모델을 활용하여 한층 공격적으로 피해자를 압박한다.

우리는 위협 행위자들이 Linux 시스템을 노리는 전술로 전환하고 있음을 확인했다. 이러한 동향은 조직의 위험을 증가시킨다. 민감한 주요 정보를 호스팅하는 가상 머신과 컨테이너가 Linux 시스템을 기반으로 하는 경우가 많기 때문이다. 또한 랜섬웨어 그룹들은 ProxyShell과 Log4Shell 취약점에서 확인된 바와 같이 신속하게 취약점 익스플로잇을 자행했으며, Kaseya를 타격한 REvil 랜섬웨어 공격에서 나타난 것처럼 제로데이 취약점도 악용했다.

최신 랜섬웨어 전술에는 기업 네트워크에 침투하기 위해 내부자를 모집하고, 랜섬머니 지불을 요구하기 위해 피해 기업의 고객에게 연락하고, DDoS 공격으로 랜섬웨어 피해 기업을 위협하고, 공격의 파급력을 강화하기 위해 공급망 및 관리 서비스 제공업체를 표적으로 삼는 것이 포함된다.

정부와 민간 차원의 지속적인 개입과 압박으로 일부 랜섬웨어 그룹이 와해되었다. Avaddon, REvil, DarkSide, BlackMatter 등의 주요 랜섬웨어 그룹들이 활동을 중단했다. 그러나 이들 랜섬웨어 그룹의 활동이 중단된 후에 해당 그룹과 관련된 계열사들이 Conti와 LockBit으로 이동하는 것이 꾸준히 관찰되었으며, 결과적으로 Conti와 LockBit은 올해 가장 활발한 RaaS(ransomware-as-a-service) 플랫폼으로 등극했다.

2021년 한 해 동안 랜섬웨어로 인한 비용이 단순히 기업의 수익 손실에만 그치지 않는다는 것이 입증되었다. Springhill Medical Center를 상대로 제기된 소송에 따르면, 이 병원의 랜섬웨어 공격 피해는 결과적으로 유아 사망으로까지 이어졌다. Springhill이 사이버 공격을 받아 전산이 중단되면서 태아 심박수 증가에 대한 데이터, 즉 제왕절개로 신속한 분만이 이루어졌어야 할 중요한 정보가 의사에게 제공되지 않았다는 주장이다. 해당 병원은 잘못을 부인하고 있으나 이 사건은 랜섬웨어 공격과 관련하여 미국에서 처음 보고된 사망 사례이며, 랜섬웨어로 인한 운영 중단으로 발생할 수 있는 법적, 더 중요한 인명 피해를 보여준다.

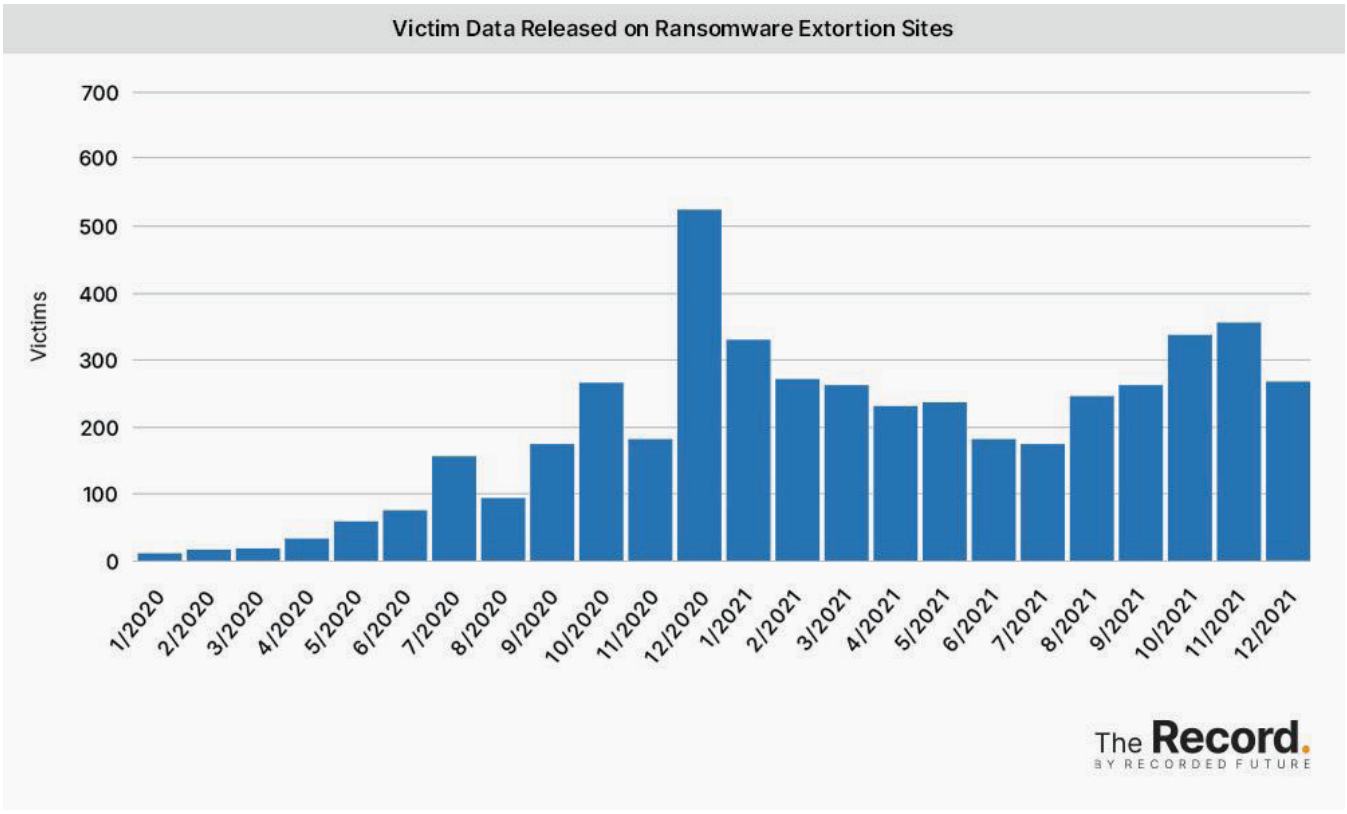

그림 1: 2020년에서 2021년 사이 갈취(Extortion)사이트에 게시된 피해자의 양(출처: The Record)

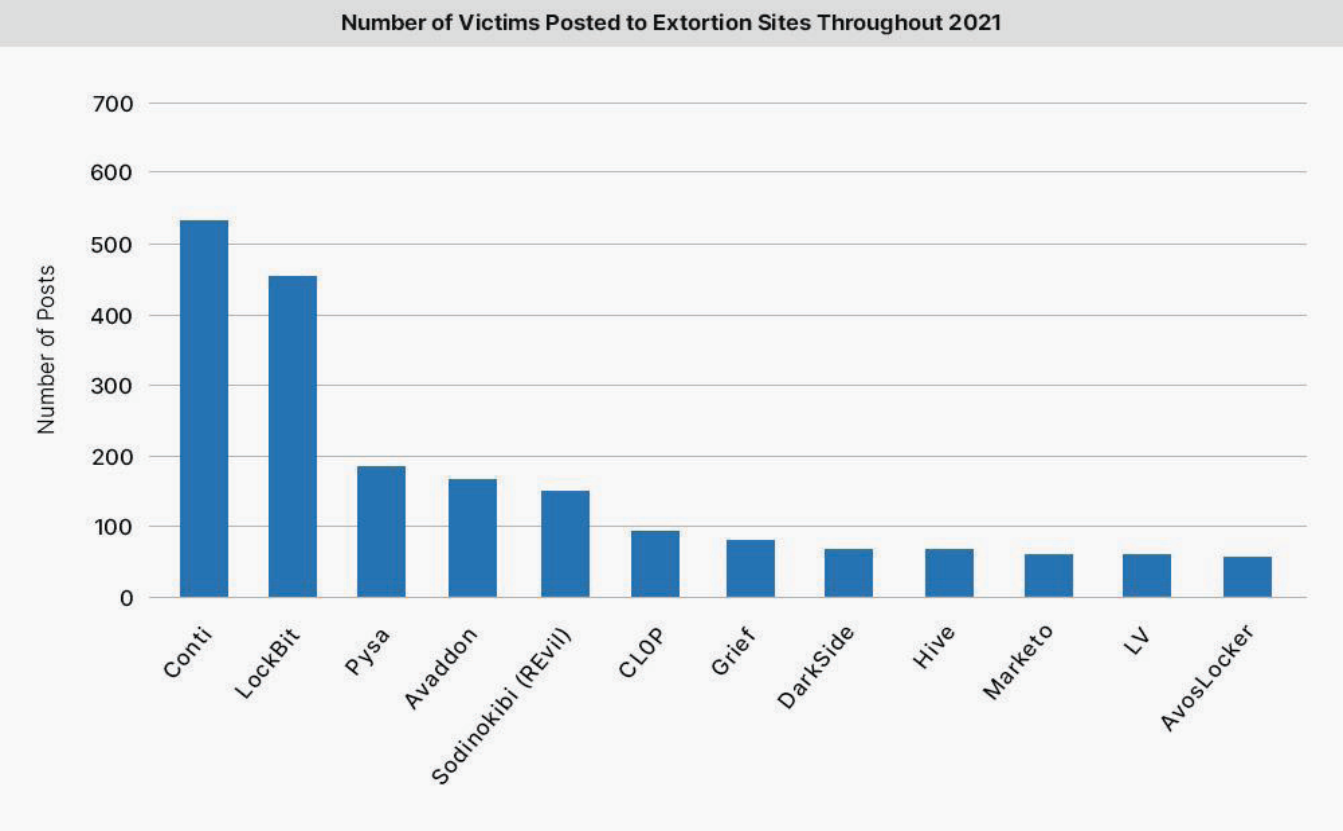

그림 2: 2021년 각 랜섬웨어 운영자의 갈취 사이트에 게시된 피해자 수(출처: Recorded Future)

2021년 랜섬웨어 개요

레코디드 퓨처는 2021년 141개국 2,865명의 피해자를 갈취 사이트에 게시한 58종의 랜섬웨어 제품군을 추적했다.

2020년에서 2021년 사이에 갈취 사이트에 올라온 피해자의 양을 비교해 보면 2021년의 총 숫자는 106% 증가했다.

레코디드 퓨처 데이터에 따르면 Conti 랜섬웨어가 2021년 한 해 동안 530명으로 가장 많은 피해자를 갈취 사이트에 게시했으며, LockBit이 그 다음으로 많은 467명의 피해자를 게시했다. Pysa, Avaddon, REvil 피해자가 각각 150명 이상으로 그 뒤를 이었다.

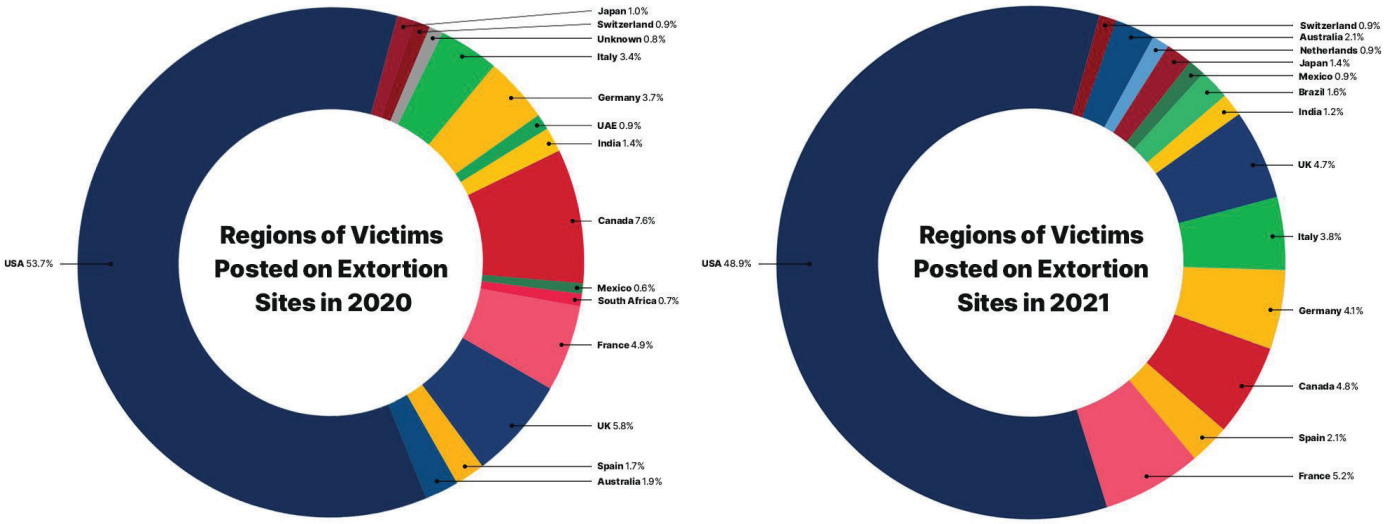

그림 3: 2020년과 2021년 갈취 사이트에 게시된 피해자 지역(출처: 레코디드 퓨처)

레코디드 퓨처 분석가들이 파악한 2020년 피해 지역 분포는 다음과 같다.

- 53.7% 미국
- 7.6% 캐나다
- 5.8% 영국
- 4.9% 프랑스
- 3.7% 독일
- 3.4 % 이탈리아

레코디드 퓨처 분석가들이 파악한 2021년 피해 지역 분포는 다음과 같다.

- 49% 미국
- 5.2% 프랑스
- 4.8% 캐나다
- 4.7% 영국
- 4.1% 독일
- 3.8% 이탈리아

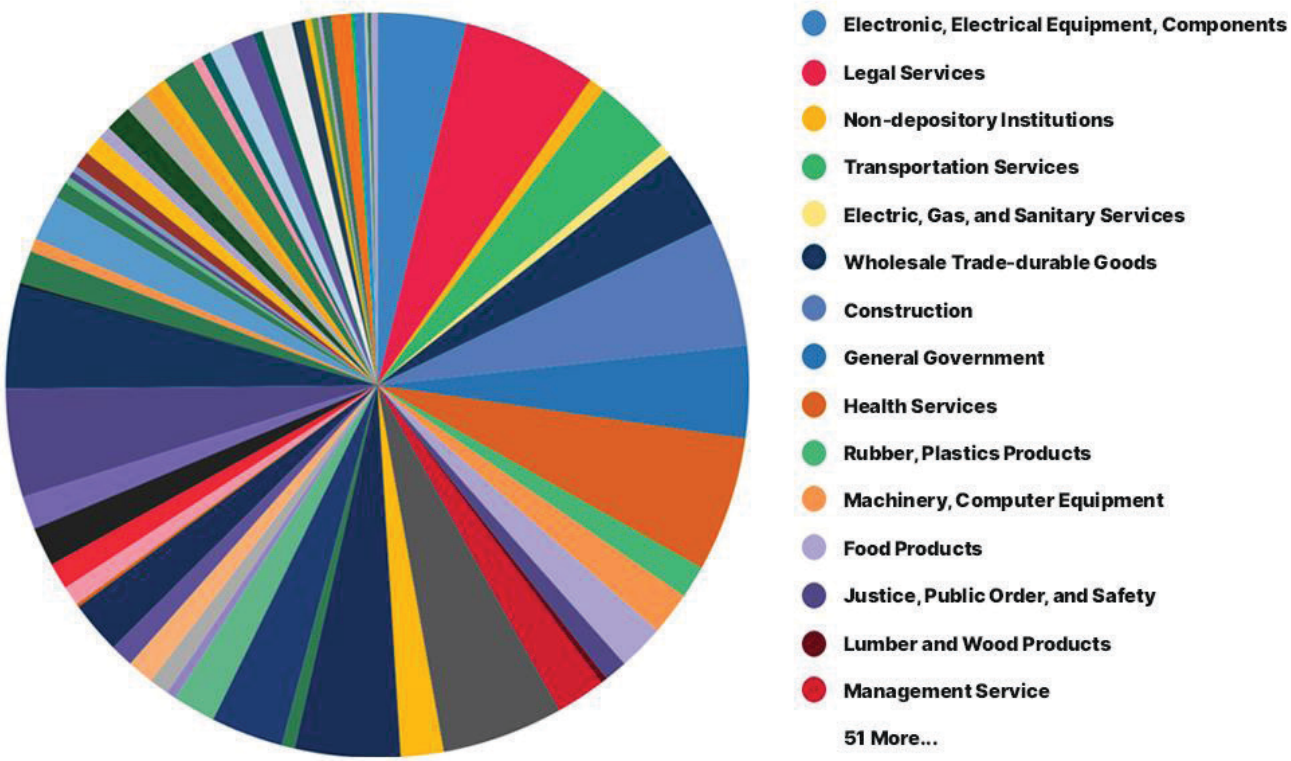

그림 4: 2021년 랜섬웨어의 표적이 된 산업 분포 (출처: Recorded Future)

2021년 랜섬웨어는 주요 인프라, 특히 Colonial Pipeline과 JBS를 타겟으로 한 공격으로 주류 언론의 주목을 받았다. 그러나 2021년 랜섬웨어 공격 데이터를 추적한 검토에서 레코디드 퓨처 분석가들은 랜섬웨어 운영자와 관련 공격자들이 본질적으로 기회주의적이라고 판단한다. 랜섬웨어 공격자들은 일반적으로 특정 산업이나 특정 지역을 중점적으로 노리는 것이 아니라 접근성, 기회, 그리고 유출된 데이터 유형과 같은 다양한 요인과 고액의 랜섬머니 지불 능력(회사 매출로 판단)을 기반으로 대상 조직을 선택한다. 위의 그림 4에서 볼 수 있듯이 랜섬웨어의 영향을 받는 산업은 매우 광범위하다.

랜섬머니 요구 및 지불

랜섬머니 요구와 지불은 대개 프라이빗 채널에서 이루어지기 때문에 추적이 어렵다. Prodraft의 리포트에 따르면 2021년 11월 중순 기준으로 Conti 랜섬웨어는 5개월 간 수행된 공격과 후속 랜섬머니 요구로 최소 2,550만 달러를 벌어들였다. 그러나 Insikt Group이 다양한 출처의 자료를 내부적으로 분석한 결과에 따르면 Conti는 2017년 설립 이후 2억 달러 이상을 갈취한 것으로 추정된다.

2021년 한 해 동안 북한 해커들이 훔친 4억 달러 상당의 암호화폐와 랜섬웨어 공격으로 지불된 막대한 랜섬머니를 생각해 보면 이는 일반 기업에서 사이버 범죄 조직으로 막대한 자금이 이동한 것이다. 이렇게 이전된 자금은 2022년 공격에 사용될 인프라 재정비에 투자될 것이다.

2021년 기업에 요구된 랜섬머니에 대한 오픈소스 데이터를 분석한 결과[1, 2], **평균적으로 피해 기업 연매출의 0.16%가 랜섬머니로 요구된 것**으로 확인됐다. 이 수치는 0.02%에서 0.37%까지 다양하지만 확인된 기업 연 매출이 수백억 달러에 달하는 것을 감안하면 랜섬머니가 상당한 액수임을 알 수 있다. 피해 조직의 유명세나 감염된 데이터의 유형과 같은 다른 요인이 영향을 미칠 수 있으므로 이 수치가 반드시 랜섬머니 요구액과 일치하는 것은 아니지만 조직이 랜섬머니 요구액을 추정하는 데 도움이 될 수 있다. 아래 표에 나열된 조직 모두가 공격자가 요구한 랜섬머니를 지불한 것은 아니다.

다크웹 노출: Infostealer Malware를 사용하여 계정 정보 수집

2021년 계정도용(Credential Theft) 시장이 활성화되면서 랜섬웨어 공격 증가에 일조했다. 랜섬웨어 운영자는 공격 초기 액세스에 여러 방법을 사용하는데, 특히 도용한 계정 정보가 네트워크 액세스 권한을 획득하는 데 악용되었다.

유출된 계정 정보는 Genesis Store, 2easy Shop, Russian Market, Amigos Market과 같은 다크웹에 정기적으로 광고된다. 2021년 6월 Insikt Group은 Amigos Market과 Russian Market이 연관되어 있음을 확인했다. 이들이 타임스탬프, 사용된 인포스틸러(Infostealer) 변종, 감염된 장치의 지리적 위치, ISP가 모두 일치하는 완전히 동일한 목록을 게시했기 때문이다.

이러한 다크웹들은 인포스틸러에 감염된 피해자로부터 수집된 계정 정보가 포함된 로그를 광고하고 판매한다. 인포스틸러(Infostealer) 악성코드는 RAT(remote access trojan)로 작동하여 사용자의 시스템 정보와 계정 로그인 크리덴셜, 브라우저 쿠키, 자동 완성 정보를 훔친다. 이러한 정보는 공격자가 다단계 인증(multi-factor authentication, MFA)을 비롯한 특정 보안 프로토콜을 통과하도록 해준다. 일반적으로 사용되는 인포스틸러에는 RedLine, Vidar, Taurus, AZORult, Raccoon Stealer, FickerStealer 등이 있다.

사이버 범죄자는 도용한 계정을 사용하여 네트워크에 무단 액세스하고, 랜섬웨어 공격을 수행하고, 멀웨어를 업로드하고, 피해 조직의 호스트에서 데이터를 추출하고, 권한 상승을 수행할 수 있다. 유출된 계정의 대다수는 개인 계정이지만, 경우에 따라 이러한 로그에 회사 계정이 포함되어 조직의 네트워크에 심각한 위험을 초래할 수 있다. 또한 동일한 암호를 재사용하는 경우가 많기 때문에 MFA가 설치되어 있지 않은 경우 위협 행위자가 개인 계정 로그인 정보를 사용하여 기업 네트워크에 침투할 수 있다. 그리고 직원이 인포스틸러에 감염된 개인용 컴퓨터를 업무에 사용하는 경우 해당 정보가 도용되어 기업 데이터 무단 액세스와 유출이 발생할 수 있다.

2021년 5월 Colonial Pipeline을 타격한 DarkSide 랜섬웨어 공격이 바로 이런 경우이다. Colonial Pipeline이 공격을 받으면서 미국 동부 해안 지역 전체에 연료 공급이 중단되었다. 2021년 6월 4일 보고서에 따르면 공격자는 유출된 VPN 휴면 계정 암호를 사용하여 Colonial Pipeline의 네트워크에 원격으로 액세스한 것으로 확인되었다.

조사관에 따르면 DarkSide가 어떻게 비밀번호를 얻었는지는 불분명하지만, 다크웹에 게시된 비밀번호 모음에 해당 비밀번호가 포함된 것이 확인됐으며, 직원이 외부의 다른 계정 비밀번호를 Colonial Pipeline 네트워크 비밀번호로 사용했을 가능성이 있다. 또한 조사에서 직원을 대상으로 한 피싱 공격의 증거는 확인되지 않았다고 밝혔다.

피해조직	랜섬웨어	추정 연매출	지불액 및 랜섬머니 요구액	연매출 대비 랜섬머니 요구액 비율
Acer	REvil	277$billion	50$million	0.018
Brenntag	DarkSide	13.4$billion	7.5$million	0.056
CNA Financial Corp	Phoenix CryptoLocker	10.8$billion	40$million	0.37
Colonial Pipeline Company	DarkSide	1.32$billion	4.4$million	0.33
JBS	REvil	53$billion	11$million	0.02

최신 멀웨어 TTP

레코디드 퓨처는 TTP Instance 노트에서 멀웨어 또는 사이버 공격과 관련된 TTP 개발을 추적한다. 2021년 이 노트의 6%를 차지하는 가장 많이 등장한 악성코드는 Cobalt Strike였다. 이는 C2 인프라 로그에서 Cobalt Strike가 우세하다는 올해 관찰과 일치했다. 그리고 Active Directory 오브젝트 익스플로잇, DNS 트래픽 마스킹(traffic masking), 랜덤 C2 프로필 생성, 도메인 차용, .NET 환경 개발, Blowfish Cipher 암호화, Mimikatz Kit 액세스, Windows 방화벽 조작, 피해자 DLL File Enumeration 등 새로운 기능을 가진 Cobalt Strike BOF(Beacon Object Files)의 몇 가지 신규 버전이 릴리즈되었다.

이러한 업데이트로 인해 Cobalt Strike Beacon의 탐지가 더 어려워지고, 기능이 증가하면서 위협 행위자가 수행할 수 있는 악성 작업이 다양화된다. 레코디드 퓨처는 2019년에 악성 Cobalt Strike 서버 탐지 방법에 대한 연구를 발표했으며 해당 보고서의 많은 권장 사항이 오늘날에도 유효하다. Insikt Group은 또한 2021년 위협 행위자의 Cobalt Strike 사용과 네트워크 및 호스트 기반 탐지 방법에 대한 연구를 발표했다.

다른 유형의 멀웨어들도 2021년 계속 업데이트되었다. 신규 사용자 인터페이스(예: 365-stealer), 새로 공개된 취약점 익스플로잇 지원(예: Mimikatz의 PrintNightmare), 탐지 회피 강화(예: Lilith Botnet 및 Qakbot) 등이 그것이다.

이러한 최신 멀웨어 변종들의 공통 기능으로 계정 도용, 암호화폐 마이닝, 권한 상승, 정상 파일/프로세스 위장이 포함된다. Insikt Group은 보안 도구에 대한 초기 액세스 경로 또는 회피 기술로 사용하기 위해 Microsoft 제품을 대상으로 하는 여러 업데이트 또는 광고를 관찰했다. 여기에는 악성 Office 문서에 대한 신규 TTP와 Windows UAC(User Account Control) 및 AMSI(Antimalware Scan Interface) 우회 기능 등이 포함된다.

TTP 트렌드

레코디드 퓨처 데이터에 따르면 2021년 상위 5개 MITRE ATT&CK 기술은 T1486 (Data Encrypted for Impact), T1082 (System Information Discovery), T1055 (Process Injection), T1027 (Obfuscated Files or Information), T1005 (Data from Local System)이다. 이러한 기술은 Discovery, Privilege Escalation, Defense Evasion, Collection, Impact의 5단계 공격 전반에서 실행된다. 2가지 기술은 Defense Evasion으로 분류된다.

TTP	설명
T1486 (Data Encrypted for Impact)	Data Encrypted for Impact 기술은 2021년 내내 대량의 랜섬웨어 공격에 가장 많이 사용된 기술이다.
T1082 (System Information Discovery)	System Information Discovery 기술은 위협 행위자가 운영 체제 및 하드웨어에 대한 자세한 정보를 얻으려고 시도할 때 발생한다. System Information Discovery는 일반적으로 감염된 장치에 대한 정보를 수집하기 위해 다양한 멀웨어에 의해 수행된다. Insikt Group은 2021년 내내 하급 및 고급 위협 행위자 모두가 이 기술을 사용하는 것을 확인했다.
T1055 (Process Injection)	Process Injection 기술은 다른 프로세스의 어드레스 공간 내에서 커스텀 코드를 실행한다. Process Injection은 방어 회피 이점(악성 작업을 정상적인 프로세스로 위장) 때문에 널리 사용되는 기술이다. 이 기술은 2021년 여러 쉘코드 로더 및 드로퍼(shellcode loader & dropper)와 함께 사용되었다.

TTP	설명
T1027 (Obfuscated Files or Information)	Obfuscated Files or Information 기술은 공격자가 시스템 상 또는 전송 중인 콘텐츠를 암호화, 인코딩하거나 난독화하여 실행 파일이나 파일을 탐색하거나 분석하기 어렵게 만드는 기법이다. 이는 다양한 플랫폼과 네트워크에서 방어를 회피하는 데 흔히 사용되는 작업이다. Insikt Group은 공격자가 탐지를 피하기 위해 이 기술을 사용하여 페이로드를 압축, 보관 또는 암호화하는 것을 확인했다. 공격자는 일반적으로 PowerShell 및 JavaScript와 같은 압축 또는 아카이브 스크립트를 사용한다.
T1005 (Data from Local System)	Data from Local System 기술은 갈취 사이트(extortion website)를 운영하는 랜섬웨어 그룹에 의해 연중 계속 사용되었다. 위협 행위자들이 대개 암호화 전에 데이터를 검색하고 유출하기 때문이다. 그런 다음 위협 행위자는 이 데이터를 사용하여 훔친 데이터를 유출하겠다고 위협하여 피해자에게 랜섬머니를 지불하도록 강요한다.

Insikt Group의 2019년 및 2020년 MITRE ATT&CK 전술 및 기술 보고서 결과와 마찬가지로 Defense Evasion 기술이 3년 연속 계속해서 우세하다. 2020년 상위 6개 MITRE ATT&CK 기술 목록과 비교해 보면 2021년에도 계속해서 T1082 (System Information Discovery), T1055 (Process Injection), T1027 (Obfuscated Files or Information)이 멀웨어가 가장 많이 사용하는 기술로 확인되었다.

레코디드 퓨처 데이터에 따르면 전체 상위 5개 기술에 포함되지는 않았지만 2021년 초기 액세스 벡터로 가장 많이 사용된 기술은 T1190 (Exploit Public-Facing Application)과 T1566.001 (Spearphishing Attachment)이었다.

전망

멀웨어 그룹, 특히 랜섬웨어 운영자가 사용하는 다양하고 진화하는 TTP는 심층 방어 전략이 시급하게 필요함을 보여준다. 여기에는 비정상적인 활동을 탐지하기 위해 조직의 네트워크 전체에 로깅을 배치하고, 취약성 패치의 우선 순위를 지정하는 강력하고 효율적인 취약성 관리 프로그램을 구축하고, 알려진 악성 작업을 찾기 위해 헌팅 패키지를 구현하고, 위협 인텔리전스를 기존 보안 기술에 통합하여 경고 분류를 지원하는 것이 포함된다. 또한 조직은 체계적이고 상세한 직원 보안 교육 프로그램을 도입해야 한다. 직원이 제1선의 방어이기 때문이다. 특히 계정 도용을 방지하기 위해서는 이 부분의 노력의 더욱 절실하다.

랜섬웨어 시장의 수익성이 계속 유지되는 한 랜섬웨어는 연중 계속해서 공공 및 민간 조직에 중대한 위협이 될 것이다. 보안 팀의 패치 관리와 공격접점(Attack Surface) 개선으로 공격자 리소스가 줄어들더라도 랜섬웨어 운영자들은 계속해서 네트워크 침투를 위해 유출된 암호, 취약성 익스플로잇, 멀웨어 배포에 크게 의존할 것이다. 또한 Cobalt Strike는 랜섬웨어 배포를 비롯한 공격에서 C2 통신에 계속 사용될 것이다.

랜섬웨어는 계속해서 전 세계 조직을 타깃으로 삼겠지만 2021년에는 랜섬웨어 그룹에 대해 전례 없는 법적 조치가 단행되었다. 미국이 주도하는 30개국 랜섬웨어 태스크포스는 거의 매주 랜섬웨어 그룹에 대한 대응을 발표하며 초기 성공을 거두고 있는 것으로 보인다. 2021년 10월 미국 법무차관 리사 모나코(Lisa Monaco)는 암호화폐 및 디지털 자산의 범죄적 오용을 방지하기 위해 암호화폐 단속팀(National Cryptocurrency Enforcement Team) 출범을 발표했다. 가장 최근인 2022년 1월 14일, 러시아 연방 보안국(FSB)은 REvil 랜섬웨어 갱단을 급습하여 폐쇄했다고 발표했다.

정부 차원의 개입이 랜섬웨어 공격 감소로 이어졌는지 여부를 판단하기에는 아직 이르지만 체포, 암호화폐 거래소 제재, 암호화폐 압류를 통해 일부 산업과 지리적 영역에서 랜섬웨어 공격의 수를 줄일 수 있다는 초기 징후가 있다. 레코디드 퓨처의 앨런 리스카(Allan Liska)는 정부 개입과 더불어 공격 감소에 기여하는 다른 요인이 있을 수 있다고 주장한다. 사이버 보험 회사는 보험 계약자가 보험을 갱신하기 전에 더 엄격한 사이버 보안 보호를 시행할 것을 요구하기 시작했으며, Gartner에 따르면 2021년 기업 사이버 보안 지출이 12% 증가했다. 이러한 방어 전략에 대응하여 사이버 위협 그룹, 특히 랜섬웨어 운영자들 역시 공격 탐지를 회피하기 위한 기술을 계속 개발할 것이다.

Insikt Group®

레코디드 퓨처의 위협 연구 부서인 Insikt Group은 정부, 법 집행 기관, 군 기관, 정보 기관 경험이 풍부한 분석가와 보안 연구원으로 구성되어 있다. Insikt Group의 임무는 고객의 위험을 줄이고 실질적인 결과를 제공하며 비즈니스 중단을 방지하는 인텔리전스를 제공하는 것이다.

레코디드 퓨처에 대하여

레코디드 퓨처(Recorded Future)는 세계 최대 엔터프라이즈 보안 인텔리전스 제공업체이다. 레코디드 퓨처는 지속적이고 광범위한 자동 데이터 수집 및 분석에 전문가 분석을 결합하여 적시에 정확하고 실행 가능한 인텔리전스를 제공한다. 레코디드 퓨처는 끊임없이 증가하는 혼란과 불확실성의 세계에서 조직이 위협을 신속하게 파악하고 탐지하는 데 필요한 가시성을 제공한다. 조직은 이러한 가시성을 확보함으로써 선제적 대응을 통해 공격을 저지하고 사용자, 시스템, 자산을 보호하여 비즈니스를 안정적으로 수행할 수 있다. 레코디드 퓨처는 전세계 1,000개 이상의 기업과 정부 기관에서 신뢰받고 있다.

자세한 사항은 www.recordedfuture.com과 Twitter @RecordedFuture에서 확인할 수 있다.