

Keep up with Ransomware

암호화로 탐지 회피하는 Cactus, 다크웹 활동 개시

■ 개요

2023년 7월 랜섬웨어 공격으로 인한 피해 사례 발생 건수가 487건으로 나타났다. 이는 전월(439건) 대비 48건 증가한 수치로, 지난달 감소세를 보였던 랜섬웨어의 피해 사례가 다시 증가세로 전환됐다.

이번 달에 눈여겨볼 랜섬웨어 이슈는 Clop에 의한 피해 사례가 꾸준히 증가하고 있다는 것이다. Clop은 올해 2월 GoAnywhere MFT 취약점(CVE-2023-0669¹)을 시작으로 4월 PaperCut 취약점(CVE-2023-27350²), 6월 MOVEit Transfer 취약점(CVE-2023-34362³)을 악용하여 광범위한 공격을 펼치고 있으며, 탈취한 데이터를 다크웹 유출 사이트에 지속적으로 게시하는 등 많은 피해를 일으키고 있다.

한편, Clop은 최근 유출사이트 공격 대상 목록에 글로벌 코스메틱 기업 에스티로더사를 공개했다. 또 다른 랜섬웨어 그룹인 BlackCat(Alphv)도 유출 사이트에 에스티로더를 공격했다는 글을 게시했는데, 이들은 에스티로더 경영진에게 직접 연락을 취했으나 답신을 받지 못했다고 회신 없이 유출과 관련한 정보를 공개하겠다고 협박성 문구를 올렸다. 또한, 이들은 Clop이 이번 공격에서 MOVEit Transfer 취약점을 통해 공격을 수행했다면서, 자신들의 공격이 Clop과는 독립적인 공격이라고 밝혔다.

LockBit에 의한 랜섬웨어 피해 건수는 지난달에 이어 이번달에도 소폭 감소했다. 이는 LockBit에 대한 지속적인 수사와 공격에 가담한 관련자들이 체포되는 등 수사기관의 압박이 강화되자 활동을 줄이고 있는 것으로 추측된다. 그러나, LockBit의 활동이 멈춘 것은 아니다. 이들은 지난 7월 일본의 나고야 항을 제어하는 통합 터미널 시스템을 공격했다. 이로 인해 항구에 막대한 재정적 손실을 발생시켰으며, 일본을 오가는 물품 유통에도 심각한 차질이 생기는 등 업무가 일시 마비되기도 했다. LockBit에 의한 피해 건수의 절대적인 수치는 감소하는 모습을

¹ CVE-2023-0669 : GoAnywhere MFT에서 발생한 원격 코드 실행 취약점

² CVE-2023-27350 : PaperCut에서 발생한 원격 코드 실행 취약점

³ CVE-2023-34362 : 웹 셸 업로드를 가능하게 하는 SQL Injection 취약점

보이고 있으나, 이들에 의한 대규모 피해 사례는 꾸준히 발생하고 있어 여전히 위협적인 그룹으로 지켜볼 필요가 있다.

이번 달 주목할 만한 랜섬웨어 그룹은 5월부터 활동을 개시한 8Base 와 7월부터 다크웹 유출 사이트를 운영한 Cactus 다. 8Base 는 전월에 이어 36 건의 피해 사례를 게시했는데, 이는 대형 랜섬웨어 그룹인 LockBit 의 피해 사례인 49 건과 유사한 수준으로 간과하기 어려운 수치다. Cactus 는 지난 7 월 다크웹 유출 사이트를 개설하며 18 건의 피해 사례를 게시했다. 이들이 사용하는 Cactus 랜섬웨어는 몇 가지 주목할 만한 특징이 있다. Cactus 랜섬웨어는 Fortinet VPN⁴ 장치의 취약점을 이용해 초기 침투한 뒤 배치 스크립트를 활용하여 7-Zip 으로 랜섬웨어를 실행시킨다. 이때 탐지를 회피하기 위해 자체적으로 암호화한 ntuser.dat 이라는 구성 파일을 보유하고 있거나, 특정 키를 입력해야 랜섬웨어가 실행된다. 이는 제작자가 랜섬웨어 바이너리 암호화를 통해 분석과 탐지를 방해하는 효과를 노린 것으로 보인다.

특색 있는 신규 랜섬웨어들도 발견됐다. 특히, 최근 비주류 언어(Go, Rust, Nim 등)로 제작된 랜섬웨어들이 계속해서 등장하고 있다. 비주류 언어는 랜섬웨어의 암호화 속도, 분석 및 탐지 우회 등의 이점이 있어 이를 채택하는 움직임이 지속되고 있는 것으로 보인다. Rust 언어로 제작된 SophosEncrypt 는 정보 보안 업체 Sophos 의 이름을 사칭하고 있으며, 일반적인 랜섬웨어 행위인 시스템 암호화뿐만 아니라 키 입력을 로깅하고 시스템을 원격으로 제어할 수 있는 RAT 의 기능 또한 포함하고 있다. Nim 언어로 제작된 Kanti 랜섬웨어도 발견됐다.

이외에도 Surtr 랜섬웨어와 동일한 이메일을 사용해 일부 연관성이 확인된 Black Hunt2.0 랜섬웨어와 암호화 프로세스를 진행하는 동안 Windows 업데이트가 진행되는 것처럼 가장하여 피해자를 속이는 Big Head 랜섬웨어가 발견됐다. 또한, Proxima 랜섬웨어와 소스코드 유사도가 99% 이상인 Black Berserk 랜섬웨어, RanzyLocker 와 94% 이상의 코드 유사도를 보여주는 Architects 랜섬웨어 등이 발견됐다. 최근 새롭게 발견되는 랜섬웨어 대부분은 기존 랜섬웨어와 상당한 연관성을 가진 형태로 발견되고 있다.

⁴ VPN : 인터넷을 사용하여 개인적인 통신망처럼 안전하게 데이터를 주고받을 수 있는 서비스

국내에서는 또다시 Magniber 랜섬웨어가 유포되고 있다. 이번엔 Drive-by Download⁵ 방식으로 유포되는 만큼 웹 서핑 중 사용자가 특정 광고나 페이지에 접속할 경우 Redirection⁶이 될 수 있고, 설치 파일 혹은 보안 파일로 위장한 msi 파일을 다운로드 시켜 실행을 유도하기도 하므로 주의가 필요하다.

요즘 화두인 IAB⁷ (Initial Access Broker)의 등장으로 랜섬웨어 생태계는 한층 더 조직적이고 치밀해지고 있다. 서비스형 랜섬웨어 그룹은 계열사를 고용하고 초기 침투 경로를 IAB에게 구매하여 공격을 수행한 뒤 얻은 수익을 믹싱 서비스⁸를 통해 세탁하는 등 체계화된 양상을 띠고 있다. 이러한 변화로 인해 전문적인 지식이 없어도 랜섬웨어 공격이 가능하게 되어 피해 사례 역시 증가하고 있다. 또한, 과거 랜섬웨어 그룹들은 데이터 암호화를 통해 몸값을 요구하는 것이 대부분이었지만, 요즘은 전략적으로 데이터 탈취만 수행하여 몸값을 요구하는 그룹들이 하나둘씩 등장하고 있다.

⁵ Drive-by Download : 사용자가 인지하지 못하게 웹사이트를 방문하거나 이메일을 열 때 악성 소프트웨어가 자동으로 다운로드 되는 공격 기술

⁶ Redirection: 웹 사이트 주소를 다른 주소로 연결시키는 기능

⁷ IAB : 초기 침투 경로를 판매하는 개인 혹은 집단

⁸ 믹싱 서비스 : 보내는 코인 지갑 주소와 받는 지갑 주소와의 연결점을 확인하기 어렵도록 정상거래 코인들과 섞어서 코인을 거래하는 기술

Clop과 BlackCat, 글로벌 코스메틱 기업 에스티로더 공격 주장

- Clop 그룹, MOVEit Transfer의 취약점 CVE-2023-34362 악용하여 공격
- Clop 그룹, 131GB 이상의 데이터를 탈취했다고 주장
- BlackCat 그룹, 경영진 개인 이메일로 연락했으나 회신이 없었다고 주장
- BlackCat 그룹, 에스티로더 측이 협상에 응하지 않을 경우 탈취한 데이터에 대한 정보를 공개할 것이라고 협박

Clop, MOVEit Transfer 공격을 통해 약 1억 달러 이상 수익 창출 가능성

- 한 랜섬웨어 복구 회사는 Clop이 MOVEit 해킹을 통해 최대 1억 달러를 벌 수 있다고 주장
- 이전 Clop 캠페인 보다 더 많은 금전을 지불했으며, 평균 몸값 금액에 훨씬 웃도는 금액을 지불
- 현재까지 MOVEit 해킹으로 인한 피해자는 약 400여명으로 밝혀짐

랜섬웨어 공격자, 삼중 협박 방식 사용

- 삼중 협박은 데이터 암호화와 유출에 더불어 DDos 공격을 수행
- 삼중 협박 랜섬웨어는 정보 탈취형 악성코드의 로그를 사용하기도 하여 연관성이 깊음

BlackCat(Alphv), 다크웹 유출 사이트 데이터 API 사용

- BlackCat, 다크웹 유출 사이트에 피해자들의 데이터를 쉽게 악용할 수 있도록 API 게시
- 랜섬웨어 공격을 받은 피해자들의 금전 지불 비율이 줄어들자, 공포심을 조성해 압박을 가하려는 의도로 API를 공개한 것으로 추정

다크웹에서 판매되는 RaaS 빌더 NoBit

- 현재 다크웹에서 NoBit 랜섬웨어 빌더가 인기를 끌고 있음
- AES-128, SHA-128 알고리즘을 활용해 빠르고 효율적인 암호화 보장
- 200달러에 빌더를 사용할 수 있으며, 1000달러를 지불하면 소스 코드 제공

* RaaS : Ransomware as a Service의 약자로 랜섬웨어를 계열사에 제공하여 금전적 이익을 얻는 형태

BlackCat, Malvertising을 통해 WinSCP로 위장한 랜섬웨어 유포

- BlackCat은 최근 온라인 광고를 통해 랜섬웨어 페이로드를 유포
- 랜섬웨어 뿐 아니라 방어 회피 도구 및 지속성 유지 도구 설치

FIN8, Sardonic 변종을 사용하여 BlackCat 랜섬웨어 유포

- FIN8으로 식별되는 그룹, Sardonic 백도어 변종을 사용하여 BlackCat 랜섬웨어 유포
- FIN8, 최근 PoS(결제 및 매출 관리 시스템) 공격에서 랜섬웨어 공격으로 범위 확장

랜섬웨어 페이로드를 배포하는 TrueBot 악성코드 확산 주의

- 시스템 정찰 및 데이터 수집, 랜섬웨어 페이로드를 배포하는 TrueBot 확산 중
- 대표적으로 Clop 그룹은 초기 침투 후 TrueBot을 배포하여 데이터를 탈취 및 암호화
- TrueBot은 초기 침투 브로커가 즐겨 사용하는 악성코드 중 하나
- 예방하기 위해 시스템과 소프트웨어를 최신 상태로 유지하는 것이 필요

Big Head 랜섬웨어, 가짜 Windows 업데이트 가장

- Big Head 랜섬웨어는 암호화 과정이 진행 중일 때 Windows 업데이트 중인 것으로 가장하여 피해자를 속임
- 스크린 샷을 캡처하고 설치된 드라이버를 확인할 수 있는 변종 존재
- Microsoft Word로 가장한 변종 존재

Mallox, 취약한 MS-SQL 서버 침입

- Mallox는 이중 협박 방식을 따르며 주로 제조 및 법률 등의 분야를 공격
- 취약한 MS-SQL 서버를 통해 침투하며 전년 대비 174%의 활동 증가량을 보임

Nim 언어 기반 악성코드, Kanti 발견

- Kanti 제작자, 탐지 우회 및 분석 방해를 노리고 비주류 언어를 채택
- 암호화폐 지갑, 특히 비트코인과 관련된 파일명을 사용하므로 암호화폐 사용자를 타겟으로 한다고 추측

보안 업체 Sophos를 사칭하는 SophosEncrypt 발견

- SophosEncrypt는 Rust 언어로 작성되어 있으며 보안 업체 Sophos를 사칭함
 - 이메일과 Jabber 인스턴트 메신저 플랫폼을 통해 운영자와 통신 가능, 키 입력을 기록 가능
- * Jabber : 실시간 채팅과 메시징을 하게 하는 오픈 소스 프로토콜 및 서비스

Avaddon, NoEscape로 리브랜딩

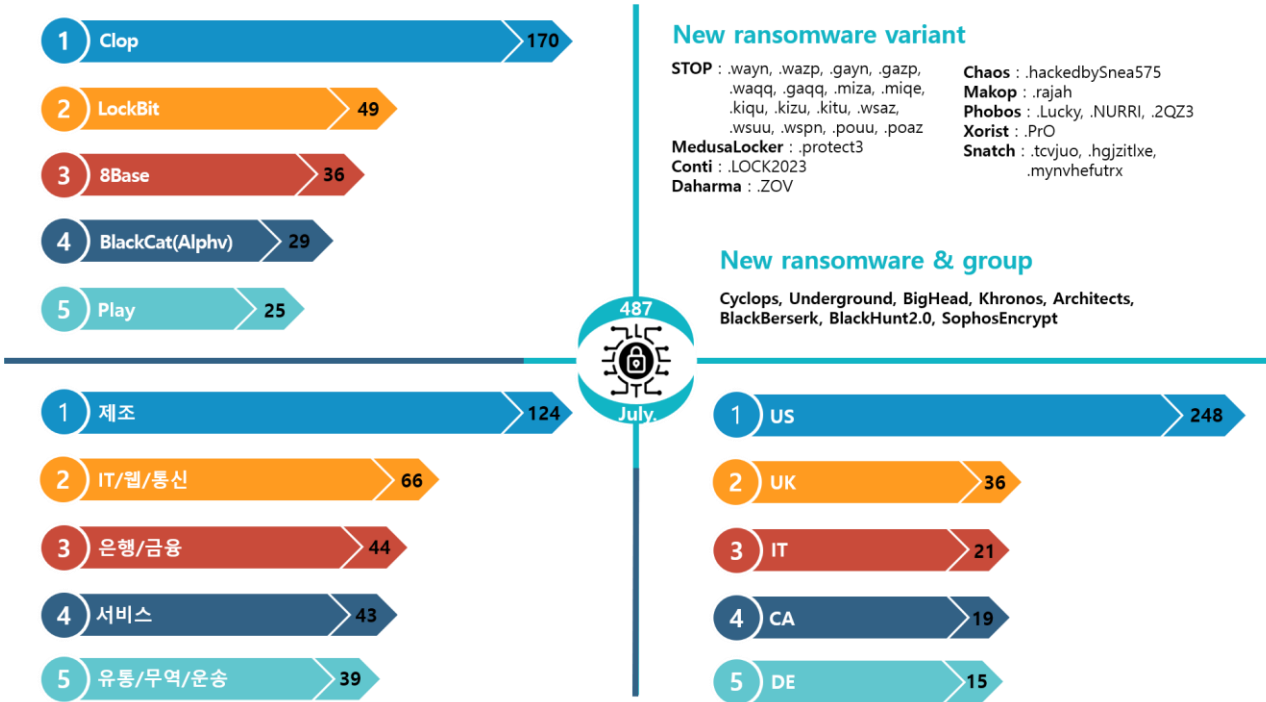
- NoEscape는 2021년 6월에 작전을 중단한 Avaddon의 리브랜딩, NoEscape 측은 Avaddon과 아무런 상관이 없다고 주장했으나 암호화 루틴, 구성 파일 형식 등이 상당 부분이 유사
- 리브랜딩을 진행하며 암호화 방식을 AES에서 Salsa20으로 전환

VMware ESXi를 타겟으로 하는 Linux 버전의 AbyssLocker 랜섬웨어

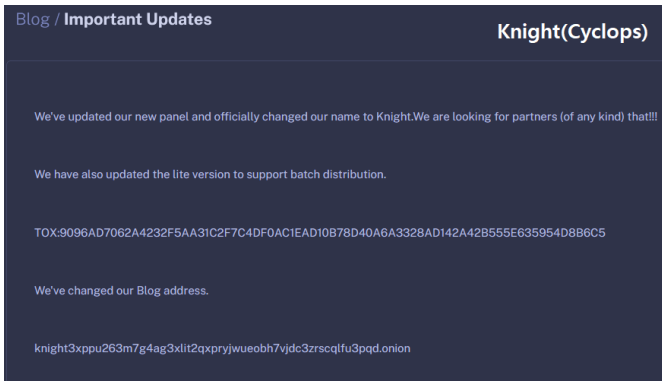
- 기업이 더 나은 리소스 관리, 성능 및 복구 등을 위해 ESXi 시스템으로 전환함에 따라 ESXi 타겟 랜섬웨어 증가
- 일각에서는 암호화 루틴이 Hellokitty 랜섬웨어를 기반으로 하며 대신 Chacha20 방식을 사용한다고 주장

■ 랜섬웨어 위협

infosec



새로운 위협



WELCOME TO THE UNDERGROUND

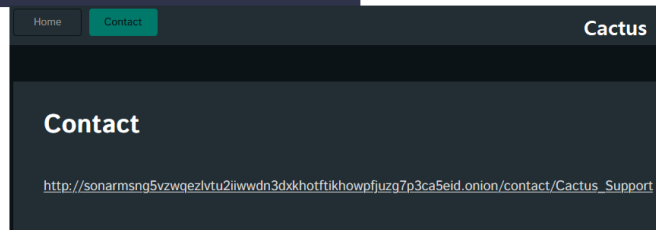
Username

Password

CAPTCHA

Login

[Create your account](#)



*출처: Knight(Cyclops), Underground, Cactus 랜섬웨어 그룹 사이트 이미지

2023 년 7 월 랜섬웨어 공격에 의한 피해 사례는 487 건으로 나타났다. 피해 사례 중 대부분이 Clop(170 건)에 의한 것으로 확인되고 있는데, 이는 Progress MOVEit Transfer 캠페인 피해자들의 자료를 점차 게시하고 있기 때문이다. 지난달부터 해당 캠페인의 피해자들이 지속적으로 속출하고 있어 앞으로의 동향이 주목되고 있다.

RedEnergy 라는 Stealer as a Ransomware⁹와, SophosEncrypt 라는 RAT as a Ransomware¹⁰가 발견됐다. 정보 탈취형 악성코드와 랜섬웨어가 결합한 RedEnergy 는 신뢰할 수 있는 프로그램인 Google Installer 로 위장하여 바이너리를 실행시키고 외부로 정보를 유출시킨 뒤 시스템을 암호화한다. SophosEncrypt 랜섬웨어는 파일 암호화 후 변경되는 확장자를 '.sophos'로 변경하고 바탕화면을 Sophos 와 관련된 이미지로 변경하는 등 보안 업체 Sophos 를 연상하도록 속이려는 행보를 보이기도 했다. 이 랜섬웨어는 비주류 언어(Go, Rust, Nim 등)인 Rust 로 제작됐으며, 키 입력 로깅을 위한 키보드 드라이버 후킹과 WMI¹¹(Windows Management Instrumentation) 명령을 사용한 시스템 프로파일링 등 RAT¹²(Remote Access Trojan) 기능 등도 포함하고 있다.

마찬가지로 비주류 언어인 Nim 언어로 제작된 Kanti 랜섬웨어는 비트코인 지갑이 잠겨 있는 상태인 것처럼 속여 공격을 수행한다. 스팸 메일 또는 피싱 사이트를 통해 유포된 것으로 추측된다. 압축 파일로 유포된 Kanti 는 LNK 파일을 클릭하도록 유도해 'Locked_253_BTC.zip' 이름의 랜섬웨어를 실행하여 암호화 시킨 뒤 확장자를 '.kanti' 로 변경한다.

랜섬웨어들이 Nim 과 같은 비주류 언어를 채택하고 있는 이유는 주류 언어에 비해 보안 메커니즘이나 탐지 확률이 떨어질 수 있기 때문이다. 또한, 분석가들이 C 계열의 언어에 비해 상대적으로 자주 접해보지 못한 언어이므로 분석을 방해하려는 목적 또한 가지고 있다. 비주류 언어의 크로스 플랫폼 지원으로 인해 랜섬웨어 제작자의 편의성 또한 증대되어 BlackCat(Alphv), BianLian, Nokoyawa, Chaos 등의 여러 랜섬웨어 그룹들이 Go, Rust, Nim 과 같은 비주류 언어를 채택하고 있다.

⁹ Stealer as a Ransomware : 인포스틸러와 랜섬웨어 기능이 결합된 악성코드로, 데이터 탈취와 암호화로 금전을 요구함

¹⁰ RAT as a Ransomware : RAT와 랜섬웨어 기능이 결합된 악성코드로, 원격으로 피해자의 시스템을 제어하고 데이터를 암호화하여 금전을 요구함

¹¹ WMI : Windows에서 시스템 구성 요소를 관리하고 모니터링하기 위한 인터페이스와 도구 모음

¹² RAT : 원격에서 컴퓨터나 시스템에 침투하여 제어하고 데이터를 수집하거나 다른 악의적인 활동을 수행하는 악성코드

BlackHunt2.0 랜섬웨어는 이전에 등장한 BlackHunt 랜섬웨어의 후속으로 보이며, 'dectokyo@onionmail.org'라는 Surtr 랜섬웨어와 동일한 메일 주소를 사용하는 것으로 보아 연관성이 있을 것으로 의심된다. Surtr 그룹은 RaaS¹³를 제공하며 REvil¹⁴에 경의를 표하는 문구로 피해자의 시스템 제조업체 이름을 변경하거나, 피해자가 CIS 국가¹⁵ 언어를 사용할 경우 랜섬웨어가 실행되지 않게 설계했다. 이러한 현상을 보아 Surtr 그룹이 REvil 과 관련이 있거나, REvil 의 유명세를 이용하고자 하는 의도가 있을 것으로 추측된다. 또한, BlackHunt2.0 은 'ryuksupport@yahooweb.co'라는 메일 주소도 사용하고 있는데, ryuk¹⁶ 와 직접적인 연관성은 확인되지 않으나 ryuk 를 언급함으로써 마찬가지로 유명세를 얻거나 ryuk 의 후속작으로 위장하여 수사기관을 따돌리려는 의도가 있을 것이라고 추측된다.

BigHead 랜섬웨어는 Windows Update 및 Microsoft Word 로 위장하여 유포되고 있다. '.NET'으로 작성되었으며 행위는 다른 랜섬웨어들과 크게 다르지 않다. 다만, 특이한 점은 시스템을 암호화하는 과정에서 사용자가 눈치채고 시스템을 종료하지 못하게 Windows Update 와 유사한 화면을 꾸며 사용자를 속이고 있다는 것이다. 이를 접하면 피해자가 쉽게 속을 수밖에 없으므로 신뢰도가 떨어지는 사이트에서 프로그램을 다운로드 하거나 실행하지 않도록 주의할 필요가 있다.

한편, Sardonic 백도어를 이용해 FIN8¹⁷로 식별되는 그룹이 BlackCat 랜섬웨어를 유포하고 있다. 이 백도어는 정보를 수집하고 명령을 실행하며 추가 페이로드를 DLL 플러그인으로 배포할 수 있는 기능을 가지고 있다. FIN8 은 원래 PoS(결제 및 매출 관리 시스템) 시스템에서 카드 데이터를 탈취하는 것을 목표로 활동했으나, 수익성을 극대화하기 위하여 랜섬웨어 공격까지 손을 뻗은 것으로 추정된다. 또한, 이들은 Ragnar Locker 랜섬웨어도 공격에 사용한 전적이 있는데 두 랜섬웨어는 모두 서비스형 랜섬웨어다. 이러한 사례를 보았을 때, 누구나 손쉽게 마음만 먹으면 랜섬웨어를 구매하여 공격에 사용할 수 있는 만큼 서비스형 랜섬웨어의 위험성을 다시 한번 확인할 수 있는 대목이다.

¹³ RaaS : 서비스형 랜섬웨어, 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태

¹⁴ REvil: Sodinokibi 로도 알려졌으며, 서비스형 랜섬웨어를 제공하는 그룹(현재는 활동 종료)

¹⁵ CIS 국가 : 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

¹⁶ Ryuk: 서비스형 랜섬웨어를 제공하는 그룹으로 주로 피싱 메일이나 बैं킹 악성코드를 통해 유포됨(현재는 활동 종료)

¹⁷ FIN8 : 소매 및 엔터테인먼트 산업을 대상으로 하는 금전을 목적으로 활동하는 공격 그룹

7 월 새롭게 등장한 랜섬웨어 그룹으로는 Underground 그룹이 있다. Underground 그룹의 랜섬웨어는 22 년 5 월에 발견된 Industrial Spy 랜섬웨어와 상당한 코드 유사성을 보여 같은 그룹으로 의심된다. 이 랜섬웨어는 Microsoft Office 및 Windows HTML RCE 취약점인 CVE-2023-36884 를 악용해 배포되었으며, 배포 시 그들이 제작한 백도어인 RomCom 의 변종을 사용했다. 특이점은 Industrial Spy 랜섬웨어에 기재된 공격자들의 이메일이 Cuba 랜섬웨어에 기재된 것과 일치하는 것으로 보아 Industrial Spy, Cuba 랜섬웨어 간의 일부 연관성 또한 확인된다.

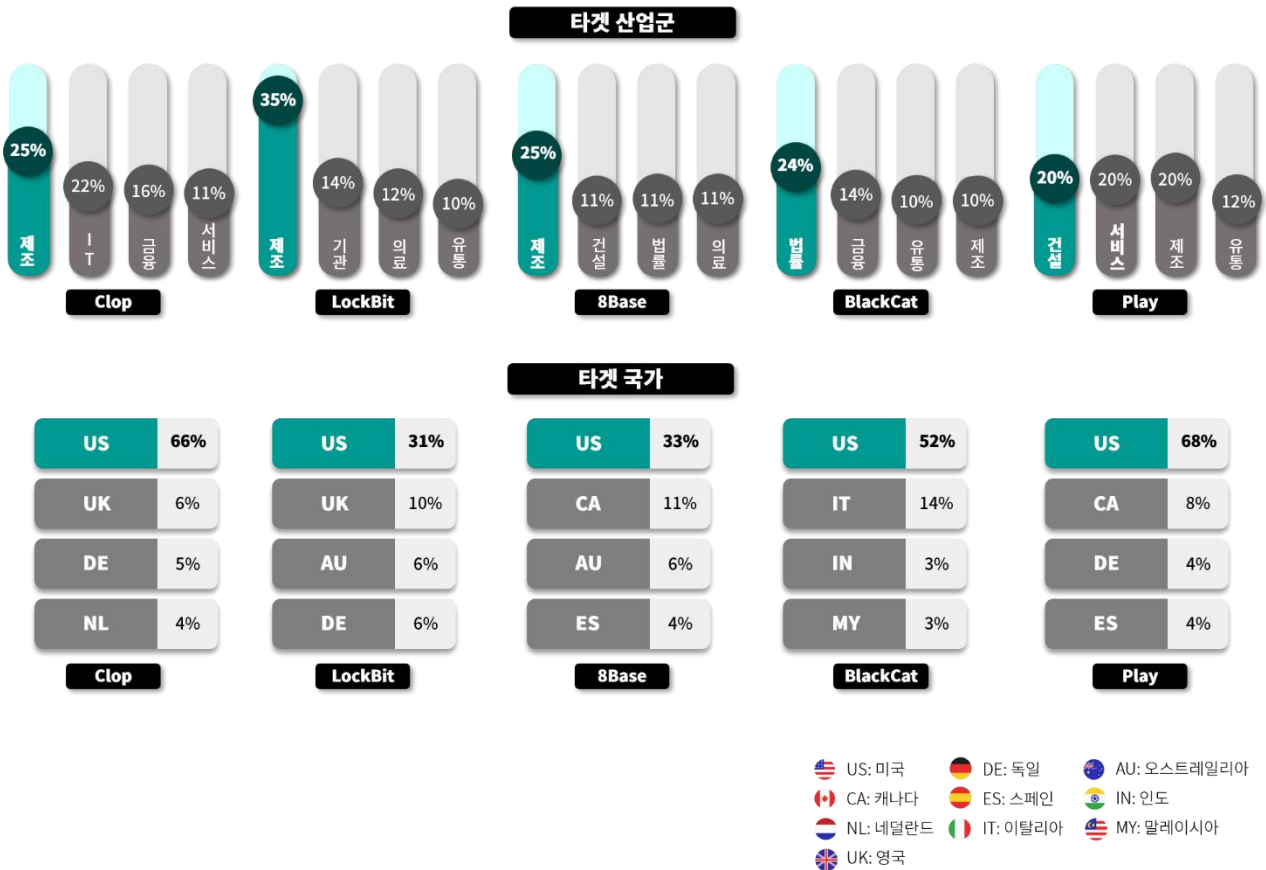
또한, 새롭게 유출 사이트 운영을 시작한 그룹으로는 Cyclops 와 Cactus 가 있다. Cyclops 는 Go 언어 기반의 인포스틸러¹⁸ 와 랜섬웨어를 사용하였으며 시스템에서 특정 확장자와 일치하는 파일들을 압축하여 공격자의 서버로 전송하는 인포스틸러가 윈도우, 리눅스 버전으로 존재한다. Babuk 랜섬웨어와 암호화 루틴이 유사하여 유출된 Babuk 소스코드를 차용한 것으로 추측된다. 최근 Cyclops 는 다크웹 주소 및 그룹명을 Knight 로 변경하는 동시에 파트너를 모집하는 공지를 하는 등 빠르게 변화하는 움직임을 보이고 있다.

Cactus 그룹은 다크웹 유출 사이트를 개시한 동시에 18 건의 피해 사례를 게시했다. 이 그룹의 활동은 3 월부터 시작한 것으로 확인되며, 다크웹을 개시하며 그동안 누적된 피해자 정보를 한 번에 올린 것으로 추측된다. Cactus 그룹은 내부 시스템에 침투하여 같은 네트워크에 속한 사용자들을 탐색하여 접근 가능한 시스템을 확인한다. 그 후 새로운 사용자 계정을 생성하여 미리 준비한 스크립트를 활용해 7-Zip 으로 랜섬웨어 페이로드를 해제한 다음 해당 압축 아카이브를 삭제한다. Cactus 는 소규모 기업보다 대형 기업들을 위주로 공격을 수행한 것으로 나타났다. 이는 더욱 많은 수익을 얻기 위한 목적으로 추측된다.

¹⁸ 인포스틸러 : 자격증명 혹은 가상화폐 지갑 주소 등을 탈취하는 정보 탈취형 악성코드

Top5 랜섬웨어

infosec



주요 랜섬웨어 그룹 중에서는 지난달에 이어 이번달에도 Clop 그룹이 가장 많은 피해 사례를 발생시켰다. Clop 그룹은 다크웹 유출 사이트에 MOVEit Transfer 캠페인으로 인한 피해 사례를 170건 게시했는데, 해당 사건으로 인한 이슈는 당분간 지속될 것으로 보인다.

LockBit 그룹의 활동은 전월과 마찬가지로 소폭 감소했으나, 두 번째로 많은 피해자를 발생시켰다. LockBit 그룹 공격에 가담한 자들이 계속해서 체포되고 있고 걸으로 드러나는 피해 사례가 감소하고 있어 영향력이 줄어들었다고 생각할 수 있으나, 여전히 이들의 공격으로 인한 대규모 피해 사례와 피해자가 발생하고 있어 LockBit 그룹으로 인한 위협이 줄어들었다고 보기는 어렵다.

8Base 그룹은 주로 다양한 분야의 중소기업을 타겟으로 공격을 수행하고 있어, 일각에서는 데이터 탈취 그룹 RansomHouse 와 유사하다는 추측이 나오고 있다. 이 외에도 8Base 그룹은 유출된 Babuk 빌더로 빌드 되었다는 특징이 있으며, 피싱 이메일과 익스플로잇 키트를 통해 확산되는 것으로 알려져 있다.

BlackCat(Alphv) 그룹은 이번 달에도 여러 특색 있는 행보를 보였다. 이들은 Windows 용 WinSCP¹⁹ 파일 전송 애플리케이션의 공식 웹사이트로 가장한 가짜 페이지로 유인하여 악성코드가 포함된 설치 프로그램을 배포하는 Malvertising²⁰ 캠페인을 진행하고 있다. WinSCP 는 인기 있는 무료 오픈 소스 SFTP, FTP, S3, SCP 클라이언트 및 SSH²¹ 파일 전송 기능이 있는 파일 관리 시스템으로, 파일 공유 사이트에서 매주 400,000 회 다운로드 되는 만큼 이러한 캠페인은 많은 피해자를 야기할 수 있으므로 주의가 필요하다.

또한 BlackCat(Alphv) 그룹은 글로벌 코스메틱 기업 에스티로더를 공격한 후 에스티로더 경영진에게 연락을 취했으나 회신이 없었다며 다크웹 유출 사이트에 불만을 드러냈다. 덧붙여 Microsoft 의 DART(Detection and Response Team)와 Mandiant 가 에스티로더의 보안을 담당하고 있음에도 불구하고 여전히 네트워크는 취약하며 접근이 가능하다고 주장하며, 시스템을 암호화하지는 않았지만 협상에 응하지 않을 경우 탈취한 데이터에 대한 자세한 정보를 공개하겠다고 이야기했다. 이 외에도 피해자들의 유출된 데이터에 액세스하기 쉽게 유출 사이트에서 API 를 제공하며 사용법에 대해 상세하게 안내하는 페이지를 추가하였다. 이러한 API 제작 동기에 대해서는 밝혀진 바가 없으나, 랜섬웨어로 인한 침해 사고 발생 시 몸값을 지불하는 피해자들이 줄어들고 있어 유출 데이터에 대한 접근성을 높여 피해자에게 데이터 유출에 대한 부담을 가중시켜 수익을 올리기 위한 새로운 전략으로 보인다.

Play 그룹도 꾸준히 유출 사이트에 피해자를 게시하고 있다. ProxyNotShell²², OWASSRF²³, Microsoft Exchange Server RCE 취약점 관련하여 다양한 도구와 익스플로잇으로 공격을 수행하고 있으며, 최근에는 네트워크 스캐너 및 인포스틸러인 Grixba 와 오픈 소스 VSS²⁴ 관리 도구인 AlphaVSS 와 같은 새로운 도구도 사용하기 시작했다. 이를 통해 공격의 효율성을 높이고 백업 파일에 더 쉽게 접근할 수 있게 되어 위험성이 크게 증가하고 있다.

¹⁹ WinSCP : Windows 환경에서의 SFTP, FTP, SCP 클라이언트

²⁰ Malvertising : 온라인 광고 서버를 해킹하여 광고를 통해 악성코드를 유포하는 기법

²¹ SSH : 안전하게 원격 컴퓨터에 접속하고 명령을 실행할 수 있는 프로토콜

²² ProxyNotShell : Microsoft Exchange Server 를 이용해 원치 않는 요청을 보내게 하는 취약점인 SSRF(CVE-2022-41040)와 원격 코드 실행 취약점(CVE-2022-41082)을 통한 익스플로잇

²³ OWASSRF : Microsoft Exchange Server 권한 상승 취약점(CVE-2022-41080), 원격 코드 실행 취약점(CVE-2022-41082)을 통한 익스플로잇, ProxyNotShell 완화 조치를 우회함

²⁴ VSS : Windows 에서 파일이나 데이터 변경 상태를 백업하여 이전 상태로 복원할 수 있게 하는 기능

■ 랜섬웨어 집중 포커스

Cactus 랜섬웨어 개요

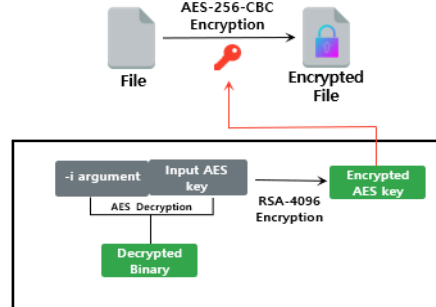
Cactus는 지난 3월 처음 발견됐지만, 이번달부터 첫 다크웹 유출 사이트를 개설하여 활동하고 있는 랜섬웨어 그룹이다. 유출 사이트 개설과 동시에 18건의 피해 사례를 게시하며 화제가 됐다. 다양한 분야의 기업을 대상으로 공격을 수행했지만, 여태까지 알려지지 않았던 이유는 다크웹 유출 사이트를 운영하지 않기도 했지만, 랜섬웨어 동작에 필요한 데이터가 암호화되어 있어 커맨드 라인 인자로 복호화 키를 전달하거나 ntuser.dat 파일이 존재해야만 Cactus 랜섬웨어가 실행되기 때문에 쉽게 발견되기 어려웠을 것으로 추측된다. 파일 이름은 고유한 피해자 ID와 동일하게 지정되며, 이는 정규 표현식 `[a-z1-9]{4}-[a-z1-9]{4}`로 랜덤하게 생성된다.



Cactus Ransomware

암호화 키

입력된 키(인자)를 RSA-4096으로 암호화한 뒤, 해당 키로 AES-256을 통해 파일 암호화



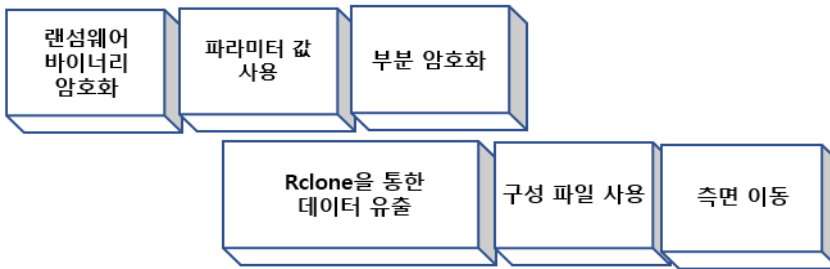
암호화 제외

- .exe
- .dll
- .sys
- .lnk
- .cts0
- .cts1
- .msi
- .bat

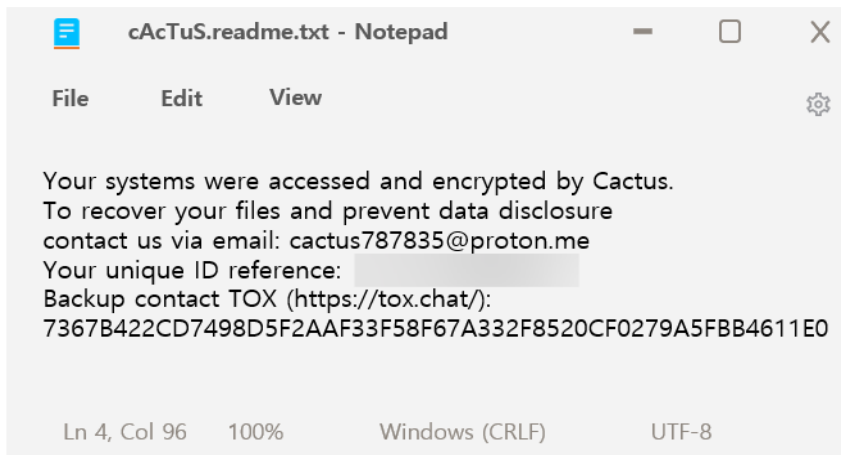
암호화 방식

파일 크기 7.74MB 이상 : 파일을 특정 크기의 블록으로 나눈 뒤, 간헐적으로 160KB 암호화
 파일 크기 7.74MB 이하: 파일 전체 암호화

특징



랜섬노트



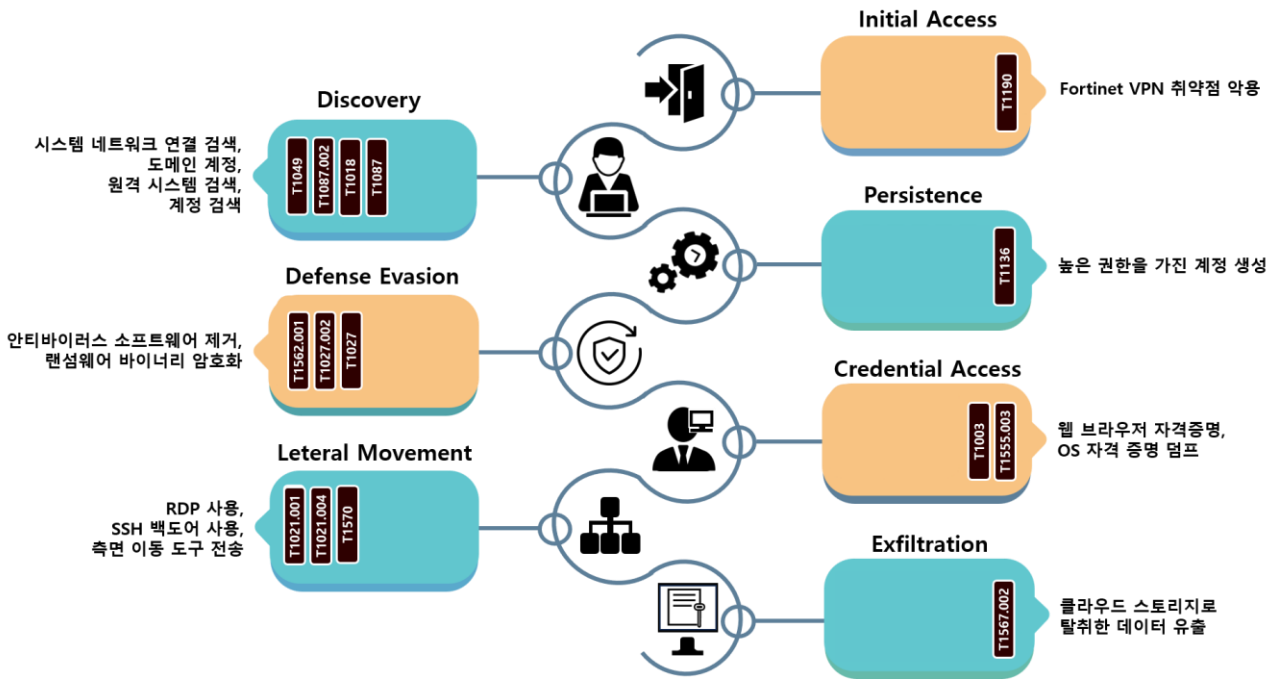
cAcTuS.readme.txt

변경 확장자

cts0, cts1

제작 언어

C++



Cactus 랜섬웨어는 Fortinet VPN의 취약점을 이용해 시스템에 침투한 후, SSH 백도어로 지속적인 액세스를 확보한다. SoftPerfect²⁵ 스캐너로 내부 호스트를 탐색하며 감염시키고, PowerShell 과 Windows 이벤트를 통해 호스트와 계정 접근성을 파악하는데, 이러한 활동은 텍스트 파일로 로깅된다. 다양한 도구를 사용해 백도어의 지속성을 유지하며, msixec²⁶로 안티바이러스를 제거한 후 자격 증명을 탈취하고 권한을 상승시킨다. 높은 권한의 계정으로 RDP²⁷와 Super Ops²⁸를 이용한 측면 이동 수행 후, Rclone²⁹을 통해 데이터를 MEGA 클라우드 서버로 전송한다. 마지막으로, PowerShell 을 사용하여 랜섬웨어를 배포하고 7-Zip 으로 페이로드를 추출하여 시스템을 암호화한다.

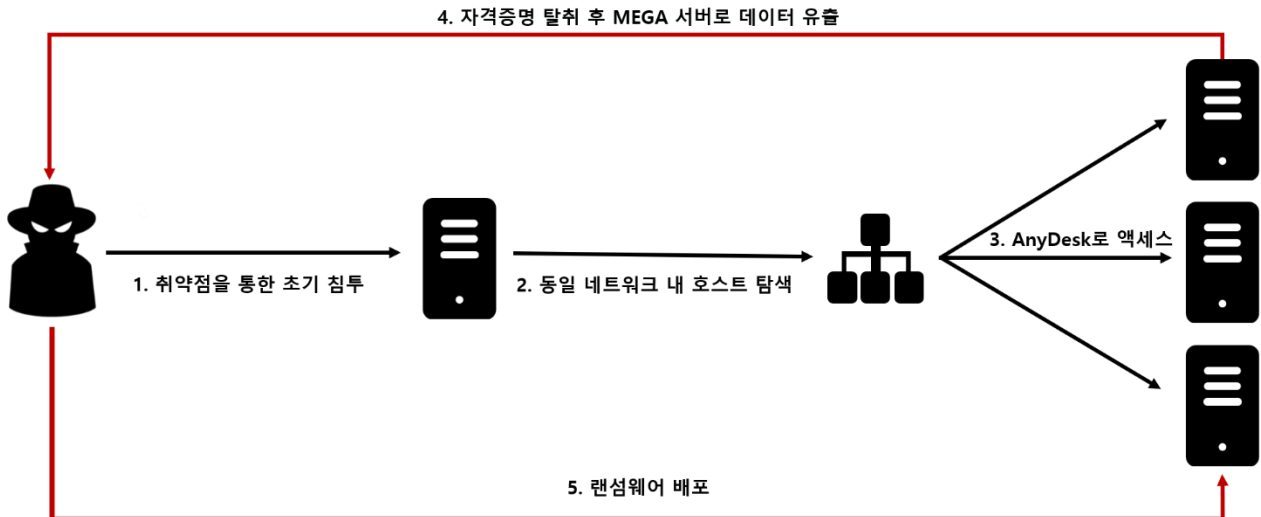
²⁵ SoftPerfect : 시스템에 접속할 수 있는지 확인하고 사용 가능한 포트를 스캔하는 도구

²⁶ msixec : Windows에서 MSI 패키지를 설치하거나 관리하는 도구

²⁷ RDP : 컴퓨터를 원격으로 조작할 수 있게 해주는 프로토콜

²⁸ Super Ops : Splashtop, Teamviewer 와 같은 원격 접속 도구를 통합 관리하는 플랫폼

²⁹ Rclone : 클라우드 스토리지에서 데이터를 관리하거나 마이그레이션 하는 도구



Cactus 랜섬웨어 공격 시나리오

Cactus 랜섬웨어의 공격 과정 중 하나는 공격자가 초기 침투를 한 뒤, 지속적으로 시스템에 액세스하기 위해서 SSH 백도어를 설치하는 것으로 시작한다. 이후 동일한 네트워크 대역에 있는 모든 호스트를 감염시키기 위해 SoftPerfect 네트워크 스캐너를 통해 내부 정찰을 수행한다. 이때 PowerShell 명령어를 실행하여 호스트를 나열하고, Windows Security 4624 이벤트³⁰ 확인을 통해 사용자 계정을 식별하여 접속 가능한 상태인지 확인하는 작업을 수행한다. 이러한 행위의 기록은 침해된 호스트 시스템의 텍스트 파일로 저장된다.

공격자는 백도어가 삭제될 경우를 대비하여 여러 방식으로 지속성을 유지하는데 Cobalt Strike³¹나 프록시 도구인 Chisel³², 합법 원격 액세스 도구인 Splashtop³³, AnyDesk³⁴와 같은 도구를 사용하여 대상 시스템에 액세스한다. 그리고 나서 msieexec 를 활용하여 안티바이러스 소프트웨어를 제거하는 배치 스크립트를 실행한다.

³⁰ Windows Security 4624 이벤트 : 시스템에 성공적으로 로그인하려는 모든 시도 기록

³¹ Cobalt Strike : 상용 침투 테스트 도구

³² Chisel : C2 통신을 제공하고 추가 스크립트 혹은 도구를 피해 시스템으로 가져오는 역할

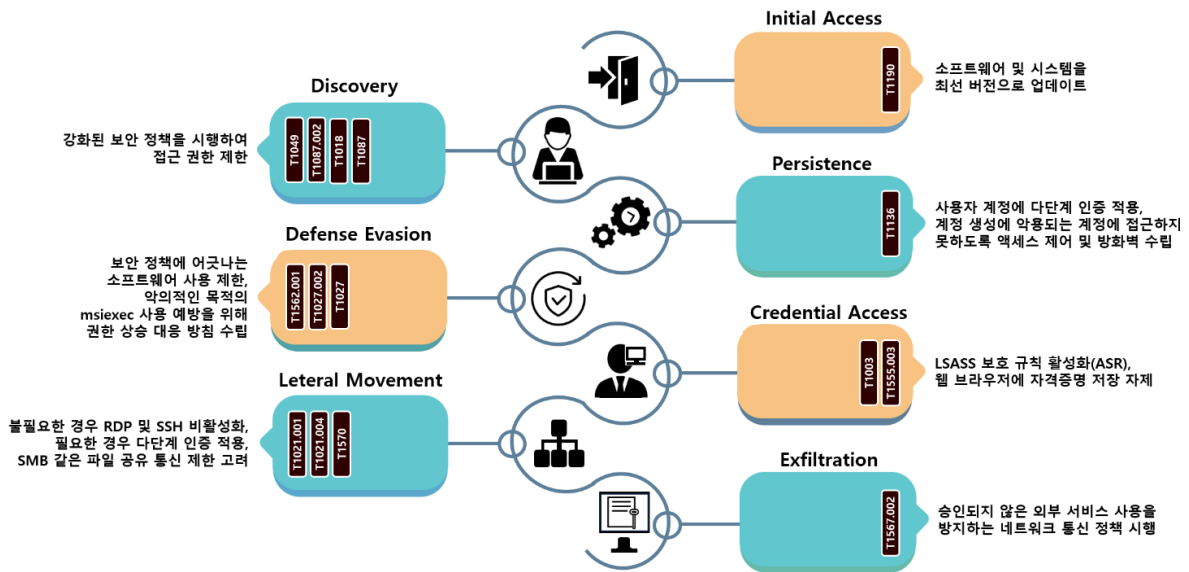
³³ Splashtop : 원격 데스크톱 소프트웨어 및 원격 지원 소프트웨어

³⁴ AnyDesk : 원격 데스크톱 소프트웨어로, 원격 제어 및 파일 전송, VPN 등의 기능 제공

특정 호스트에 액세스한 뒤 안티바이러스 소프트웨어를 성공적으로 제거하고 나면, 유출시킬 자격 증명을 디스크나 웹 브라우저에서 탈취하고 권한 상승을 위해 LSASS³⁵ 메모리를 덤프 한다. 탈취한 자격 증명 중에 높은 권한을 가지고 있는 계정과 RDP, Super Ops 와 같은 원격 관리 도구를 사용하여 내부 확산을 수행한다.

공격자는 탈취한 데이터를 Rclone 과 같은 합법적인 도구를 통해 MEGA 클라우드 서버로 자동 추출시켜 손에 넣는다. 데이터가 유출되고 난 것을 확인한 공격자는 BlackBasta 그룹에서도 자주 사용하는 PowerShell 스크립트를 통해 랜섬웨어의 배포를 자동화하고 바이너리 실행을 위해 7-Zip 으로 페이로드를 추출한 다음 시스템을 암호화한다.

³⁵ LSASS : Windows 시스템 유저들의 로그인을 검사하며 비밀번호 변경을 관리하는 프로세스



랜섬웨어의 초기 침투는 취약점을 통해 이루어지므로, 소프트웨어와 시스템을 항상 취약점이 패치된 최신 버전으로 유지하는 것이 중요하다. 만약 초기 침투가 발생해도 시스템과 계정에 대한 정보를 검색하지 못하도록 접근 권한을 관리하고, 계정이 악용되는 것을 예방하기 위해 접근을 막는 정책이나 방화벽 등을 수립하는 방안이 필요하다.

또한 Cactus 공격자가 msixexec 를 악용하여 안티바이러스 소프트웨어를 제거하거나, Cobalt Strike 등 침해 사고에서 많이 발견되는 소프트웨어를 사용하는 것을 고려하여 해당 도구를 제한하는 정책을 마련하고, 권한 상승이 발생하지 않도록 계정 보안에 만전을 기해야 한다. 웹 자격 증명 브라우저에 저장을 자제하고, OS 자격 증명 탈취에 가장 빈번하게 악용하는 LSASS 메모리 덤프를 예방하기 위해 Windows10 에서부터 적용된 ASR³⁶(Attack Surface Reduction) 규칙을 활성화하여 LSASS 를 보호하고 자격 증명 도용을 예방해야 한다. RDP 와 SSH 는 사용하지 않을 시에 비활성화해야 하고, 만약 사용해야 할 경우에는 다단계 인증을 통해 공격자가 쉽게 접근하지 못하도록 막아야 한다.

또한, SMB 와 같은 파일 공유 통신 프로토콜을 통해 공격에 사용되는 도구들을 전송하는 경우가 있기 때문에 이를 제한하는 정책 또한 고려할 필요가 있다. 공격자는 탈취한 데이터를 클라우드 스토리지로 전송하여 손에 넣는 경우가 많은데, 이러한 과정을 손쉽게 자동화할 수 있는 Rclone 과 같은 외부 서비스 사용을 제한하는 것만으로도 데이터 유출을 예방할 수 있다.

³⁶ ASR : 악성코드의 공격 경로를 차단하는 기술

Indicator Of Compromise

[a-z1-9]{4}-[a-z1-9]{4}.exe : SHA256

```
509A533ADE43406EB50FA9CB8984B2E10D008AD0EA8C22D0652F3EE101125BB7
D7429C7ECEA552403D8E9B420578F954F5BF5407996AFAA36DB723A0C070C4DE
78C16DE9FC07F1D0375A093903F86583A4E32037A7DA8AA2F90ECB15C4862C17
C52AD663FF29E146DE6B7B20D834304202DE7120E93A93DE1DE1CB1D56190BFD
69B6B447CE63C98ACC9569FDCC3780CED1E22EBD50C5CAD9EE1EA7A4D42E62CC
0933F23C466188E0A7C6FAB661BDB8487CF7028C5CEC557EFB75FDE9879A6AF8
9EC6D3BC07743D96B723174379620DD56C167C58A1E04DBFB7A392319647441A
```

File Name

ntuser.dat : Configuration File
[a-z1-9]{4}-[a-z1-9]{4}.exe : Binary of Cactus Ransomware

■ 참고 사이트

URL : <https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/analysis-of-cactus-ransomware>

URL : <https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection>

URL : <https://thehackernews.com/2023/07/blackcat-operators-distributing.html>

URL : <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-pushes-cobalt-strike-via-winscp-search-ads/>

URL : <https://thehackernews.com/2023/07/redenergy-stealer-as-ransomware-threat.html>

URL : <https://www.bleepingcomputer.com/news/security/ransomware-affiliates-triple-extortion-and-the-dark-web-ecosystem/>

URL : <https://thehackernews.com/2023/07/beware-of-big-head-ransomware-spreading.html>

URL : <https://www.securityweek.com/blacklotus-uefi-bootkit-source-code-leaked-on-github/>

URL : <https://www.bleepingcomputer.com/news/security/meet-noescape-avaddon-ransomware-gangs-likely-successor/>

URL : <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor>

URL : <https://www.bleepingcomputer.com/news/security/cybersecurity-firm-sophos-impersonated-by-new-sophosencrypt-ransomware/>

URL : <https://www.bleepingcomputer.com/news/security/est-e-lauder-beauty-giant-breached-by-two-ransomware-gangs/>

URL : <https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/>

URL : <https://thecyberexpress.com/nobit-raas-new-generation-ransomware-builder/>