CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0107

2020년 공격자 인프라 보고서:
방어자의 관점

Recorded Future®

레코디드 퓨처의 연구기관인 Insikt Group®은 2020년 Proactive Scanning 방식을 사용하여 악성 C2(command and control) 인프라에 대한 조사를 실행했다. 모든 데이터는 Recorded Future® 플랫폼에서 소싱되었다. 이 보고서의 데이터는 2020년 11월 15일 기준이다.

요약

레코디드 퓨처는 다양한 포스트 익스플로잇(post-exploitation) 툴킷, 커스텀 멀웨어 프레임웍, 오픈소스 RAT(remote access trojans)와 관련된 신규 악성 인프라의 생성과 변경을 추적한다. 이러한 작업은 Insikt Group이 오픈소스 RAT의 배포를 파악하기 위한 방법론을 만든 2017년부터 계속되어 왔다. 레코디드 퓨처는 2020년 한 해 동안 80개 이상의 멀웨어 계열에서 10,000 개 이상의 C2 서버를 추적했다.

주요 내용

- 탐지된 서버의 55% 이상(5,740개 서버)이 오픈소스에서 전혀 참조되지 않았다. 이 서버들은 레코디드 퓨처 C2 서버 목록(Recorded Future Command and Control List)에서만 파악되었다.
- 평균적으로 C2 서버 수명(즉, 서버가 악성 인프라를 호스팅한 시간)은 54.8일이었다.
- 2020년에 최초 이벤트가 탐지된 IP 주소에 대한 리드 타임(lead time)을 계산했다. 리드 타임은 C2 서버가 생성된 시점부터 그것이 다른 소스에서 보고되거나 탐지된 시점까지 걸린 시간(일)이다. 여기서 924개의 서버를 확인하였으며, 레코디드 퓨처 C2 목록에서 처음 발견된 시점과 다른 소스에서 후속 관찰된 시점을 비교하여 리드 타임을 도출하였다. 오픈소스에서 IP 주소가 발견되기까지 평균 리드 타임은 61일이었다.
- 의심스러운 호스팅 제공업체만 모니터링하는 방식은 맹점을 남길 수 있다. 왜냐하면 레코디드 퓨처가 확인한 C2의 33%가 미국에서, 그것도 대부분이 유명 호스팅 제공업체를 통해 호스팅되었기 때문이다.
- C2 서버가 가장 많은 호스팅 제공업체는 Amazon, Digital Ocean, Choopa 등 모두 미국 업체였다.
- OST(offensive security tool) 탐지는 커스텀 임플란트(implant)를 탐지하는 것만큼 중요하다. APT 그룹 운영자, 랜섬웨어 공격자,일반 범죄자들은 이러한 도구를 사용하여 레드팀이 하는 것처럼 비용을 절감한다. 탐지된 것 중 40% 이상이 오픈소스 도구였다.

배경

악성 서버를 파악하는 리드 타임은 위협을 무력화하기 위한 선제적 조치가 될 수 있다. 공격자가 서버를 사용하려면 탈취 또는 합법적인 구매를 통해 서버를 획득해야 한다. 그런 다음 소프트웨어를 설치하고 구성을 조정하여 서버에 파일을 추가해야 한다. 공격자는 패널 로그인, SSH, 또는 RDP 프로토콜을 통해 서버에 액세스한 다음 포트에서 멀웨어 컨트롤러를 노출시켜 피해자로부터 데이터가 전송되도록 만들고 감염 명령을 관리해야 한다. 여기까지 완료되어야만 공격자가 해당 서버를 악의적인 목적으로 사용할 수 있다.

그러나 서버의 노출, 구성, 액세스 과정에서 공격자는 지문을 남기게 된다. 때로는 서버에 배포된 소프트웨어에, 때로는 로그인 패널에, 때로는 SSL 등록 패턴에 공격자 지문이 남는다. 이런 것들을 활용하여 피싱 이메일 전송이나 임플란트 컴파일 전에 선제적으로 탐지할 수 있다.

또한 이러한 지문을 통해 공격자에 대한 많은 것을 밝힐 수 있다. 생성된 C2 서버 수를 파악하면 공격자의 캠페인 범위를 측정하는 데 도움이 될 수 있다. 이러한 데이터를 해당 멀웨어 계열과 관련된 침입 보고와 비교하면 얼마나 많은 침입이 포착되었고, 일반에 알려지지 않은 이벤트 수는 어느 정도인지를 파악할 수 있다. 그리고 공격자 지문을 통해 공개 영역에서 찾을 수 없는 새로운 지표와 정보를 확인할 수 있다.

위협 분석

가장 일반적으로 관찰되는 멀웨어 계열은 주로 오픈소스 또는 상용 도구를 활용했다. 파악된 전체 C2 서버의 13.5%가 변형되지 않은 Cobalt Strike(사전 구성된 TLS 인증서, Team Server 관리 포트, 또는 telltale HTTP 헤더) 구축이었다. 레코디드 퓨처가 확인한 또 다른 주요 오픈소스 C2 서버는 Metasploit과 PupyRAT였다.

Top 5 Most Prolific C2 Families	
Family	**2020 C2s**
Cobalt Strike	1441
Metasploit	1122
PupyRAT	454

표 1: C2 인프라에서 가장 많이 탐지된 멀웨어 계열 (이 수치에는 분석 당시 작동 중이었고 2020년 신규 서버가 아닌 기존 서버들이 포함됨).

파악된 C2 서버 수를 기준으로 한 가장 일반적인 상위 10대 OST(offensive security tool)에는 신규/기존 멀웨어 계열이 포함되었다. 특히 레코디드 퓨처는 일반적인 탐지 메커니즘을 벗어난 393개의 Cobalt Strike 서버를 확인했다. 탐지된 것은 전체 Cobalt Strike 사용의 일부에 불과할 것으로 판단된다. PWC와 Blackberry는 페이로드가 관찰된 대부분의 Cobalt Strike 구축에서 상용화된 도구의 크랙 버전 또는 시험 버전을 사용한다는 사실을 발견했다.

Top 10 Observed Offensive Security Tools	
Family	**Notable Users**
Cobalt Strike	APT41, Mustang Panda, Ocean Lotus, FIN7
Metasploit	JointWorm (EVILNUM), Turla
PupyRAT	APT33, COBALT ILLUSION
Powershell Empire	Sandworm, GADOLINIUM
Meterpreter	MuddyWater, TA505
Covenant	APT34 (GreenBug)
Armitage	WIZARD SPIDER (UNC1878)[1]
Octopus C2	Unnamed Chinese APT
Sliver	N/A
Responder	APT28, APT40 (TEMP.Periscope)
PoshC2	UNC1945

표 2: 레코디드 퓨처가 추적한 오픈소스 멀웨어 계열의 예 (이 수치에는 분석 당시 가동 중이었고 2020년 신규 생성된 서버가 아닌 기존 서버가 포함된다.)

레코디드 표처가 탐지한 거의 모든 OST가 APT 또는 하이엔드 금융 행위자와 연결되었다. 이러한 도구는 구하기 쉽고 사용하기 쉬우며 배후를 특정하기 어렵기 때문에 무단 침입과 레드 팀 모두에게 인기있다. 또한 랜섬웨어 공격자들도 이러한 프레임웍을 사용한다. 따라서 이에 대한 탐지가 최우선이 되어야 한다.

C2 서버가 가장 많은 호스팅 제공업체

레코디드 퓨처 C2 데이터를 통해 가장 인기있는 C2 서버 호스팅 제공업체를 파악할 수 있었다. 576개 호스팅 제공업체에서 C2 인프라가 생성된 것이 확인되었다. 이것은 60,000 개가 넘는 전체 AS 사업자 가운데 매우 적은 비율에 불과하다.

가장 많이 사용되는 ASN은 분명히 호스팅 제공업체의 규모와 관련이 있다. 이들이 반드시 방탄 호스팅 사업자(bulletproof hosting – 서버 내에 고객이 뭘 저장하든 묻지 않고 상관도 하지 않는 회사)이거나 공격 행위에 연루된 것은 아니다. 가장 많이 사용되는 도구는 민군겸용(Dual-Use)으로 간주되어 평판 좋은 AS 영역에서 이러한 서버 수가 증가한다.

미국에서 운영되는 Amazon.com, Inc.는 레코디드 퓨처가 관찰한 ASN의 C2 대부분을 호스팅했다. 여기서 호스팅된 C2 서버는 471개로 전체의 약 3.8%를 차지했다. Amazon.com, Inc.에서 가장 흔하게 관찰된 멀웨어 계열은 Cobalt Strike로 167개의 서버가 확인되었다. 그 다음으로 규모가 큰 호스팅 제공업체는 역시 미국에서 운영되는 Digital Ocean이었다.

C2 서버가 많은 미국 내 다른 호스팅 제공업체들은 아래와 같다. 이들 호스팅 제공업체에 Cobalt Strike와 Metasploit 컨트롤러가 구축된 것은 위법 행위나 부주의에 의한 것이라기 보다는 클라우드 인프라에서 이러한 도구를 사용하는 레드 팀 때문일 가능성이 높다.

[1] 레코디드 퓨처는 2020년 10월 29일 IP 179.43.128[.]5에서 Armitage 인증서를 발견했다. 이 인증서는 Ryuk 랜섬웨어를 배포할 의도로 UNC1878에서 사용하는 Cobalt Strike 서버도 호스팅하고 있었다.

Top 10 C2 Hosting Providers				
Hosting Provider	**ASN**	**Country**	**Top Family**	**Total C2s**
Amazon.com, Inc.	AS16509	United States	Cobalt Strike	471
Digital Ocean	AS14061	United States	Metasploit	421
Choopa, LLC	AS20473	United States	Cobalt Strike	368
Zenlayer Inc	AS21859	United States	Roaming Mantis	358
Hangzhou Alibaba Advertising	AS37963	China	Cobalt Strike	335
ICIDC Network	AS136800	China	Cobalt Strike	277
OVH SAS	AS16276	France	PupyRAT	273
Shenzhen Tencent Computer Systems	AS45090	China	Cobalt Strike	262
Google LLC	AS15169	United States	Bozok RAT	241
Space-IX - RECONN LLC	AS6870	Russia	DarkComet	205

표 4: 2020년 가장 많은 C2 서버를 호스팅한 호스팅 제공업체들

OST에서 널리 사용되는 가장 일반적인 ASN은 레드 팀 활동과 무단 침입에서 쉽게 구할 수 있으므로 추정이 어렵다.

Top OST Hosting Providers				
Family	**Hosting Provider**	**ASN**	**Country**	**C2s**
Cobalt Strike	ICIDC NETWORK	AS136800	China	259
Metasploit	Shenzhen Tencent Limited	AS45090	China	124
PupyRAT	Digital Ocean	AS14061	United States	85
Powershell Empire	Digital Ocean	AS14061	United States	43
Covenant	Amazon.com, Inc.	AS16509	United States	29

표 5: 각 OST의 주요 호스팅 제공업체.

RAT(Remote Access Trojans)로 퍼블리싱된 공개 툴 또한 선호하는 호스팅 제공업체를 예측하기가 어렵다.

RATs' Favorite Hosting Providers				
Family	**Hosting Provider**	**ASN**	**Country**	**C2s**
QuasarRAT	Internap Corporation	AS19024	United States	175
DarkComet	RECONN LLC	AS6870	Russia	89
Bozok RAT	Google LLC	AS15169	United States	62
njRAT	Crnogorski Telekom	AS8585	Montenegro	32
REMCOS	Taiwan Academic Network	AS1659	Taiwan	14

표 6: 각 RAT의 주요 호스팅 제공업체.

권고 사항

- 선제적 탐지는 방어자에게 추가적인 파일/네트워크 기반 탐지를 위한 준비 시간을 제공하는 이점이 있다.
- 레코디드 퓨처 고객은 Recorded Future Command and Control List에서 확인된 IP 주소를 탐지하여 신속하게 감염을 파악할 수 있다.
- 레코디드 퓨처 사용자는 Recorded Future Command and Control List를 사용하여 모든 멀웨어 엔티티를 쿼리하고 자체 조사를 수행할 수 있다.
- SIEM에서 의심 활동, YARA에서 의심 파일 콘텐츠, SNORT에서 의심/악성 네트워크 트래픽에 대한 상관관계 검색(correlation search)를 통해 일반적인 오픈소스 툴링(tooling)에 대한 심층 탐지를 수행해야 한다.
- 각 멀웨어 계열에 대한 탐지 결과는 주류 멀웨어 외에서도 오픈소스 툴 사용이 증가했음을 보여준다. 따라서 엔터프라이즈 환경에서 이러한 비주류 멀웨어 계열에 대한 네트워크/호스트 기반 탐지를 강화해야 한다.
- APT와 범죄집단들이 OctopusC2, Mythic, Covenant와 같이 비교적 덜 알려진 오픈소스 툴을 사용하고 있다. 따라서 위협 인텔리전스 실무자는 이러한 도구의 사용을 추적하고 평가해야 한다.

향후 전망

레코디드 퓨처의 전망에 따르면 2021년 한 해 동안 최근 인기를 얻은 오픈소스 도구들(특히 Covenant, Octopus C2, Sliver, Mythic)이 더욱 광범위하게 사용될 것으로 보인다. 이 도구들 중 3개에는 GUI가 있어서 초보적인 사용자도 쉽게 사용할 수 있다. 또한 4개 모두 자세한 사용 설명서가 있다. 이 도구들은 릴리즈 후 빠르게 도입되어 레드 팀과 무단 행위자 모두에게 애용되었다. 하지만 이러한 오픈소스 프레임웍의 이점에도 불구하고 Cobalt Strike가 편재성과 유용성 덕분에 선두를 유지할 가능성이 높다. 더욱이 해당 프레임웍의 소스코드가 유출되었기 때문에, 위협 행위자들이 전방위적으로 Cobalt Strike를 더 많이 채택할 것으로 전망된다.

또한 다양한 발표에서 탐지 방법이 자세히 소개되었음에도 불구하고 스파이 행위자가 서버 측 구성요소를 수정할 가능성은 적을 것으로 예상된다. 국가 차원의 스파이 활동에 개입된 위협 행위자는 목표 달성을 위해 무엇이든, 어떤 도구라도 사용할 것이다. 표적으로 삼은 조직이 공개된 도구로부터 네트워크를 방어하지 못한다면 위협 행위자 입장에서는 굳이 최신 기능에 눈을 돌릴 이유가 없다. 그러나 재정적 이익을 목적으로 커스텀 도구를 사용하는 행위자는 구성요소를 재설계하거나(BazarBackdoor와 TrickBot 행위자의 경우) 완전히 새로운 도구를 도입하여(FIN7의 방식) 탐지에 대응할 가능성이 매우 높다.

이와 같은 요인들이 존재하기 때문에 이러한 멀웨어 계열에 대한 보안 컨트롤 및 방어를 구현하는 것이 중요하다. C2 서버를 선제적으로 탐지하는 것이 사고 방지에 도움이 될 수 있다. 하지만 피해 호스트, 네트워크 경계, 전송망에서 침입 행위를 탐지하기 위해서는 심층 방어(defense-in-depth) 방식을 사용하는 것이 좋다.

레코디드 퓨처에 대하여

레코디드 퓨처(Recorded Future)는 보안 팀에 특허 받은 머신러닝을 기반으로 한 업계 유일의 완전한 보안 인텔리전스 솔루션을 제공합니다. 레코디드 퓨처의 기술은 타의 추종을 불허하는 방대한 소스로부터 자동으로 정보를 수집하고 분석합니다. 그리고 전문가 분석 또는 기존 보안 기술과의 통합을 위한 귀중한 컨텍스트를 실시간으로 제공합니다.