사이버
위협
분석

Recorded Future®

By Insikt Group®

December 15, 2022

2022 Adversary Infrastructure Report

레코디드퓨처 Insikt Group®은 2022년 한 해 동안 선제적 스캐닝 및 취합 메쏘드를 이용해서 파악한 악성 커맨드-앤-컨트롤(C2) 인프라스트럭처에 대한 연구를 진행했습니다. 모든 데이터의 출처는 레코디드퓨처® 플랫폼이며 2022년 9월 1일 기준 최신입니다.

요약

레코디드퓨처는 수많은 후속 공격(post-exploitation) 툴킷, 커스텀 멀웨어, 오픈소스 RAT(원격 액세스 트로이목마)와 관련된 새로운 악성 인프라스트럭처의 생성과 변경을 추적합니다. 2017년 이래 저희는 RAT, APT 멀웨어, 봇넷 패밀리, 기타 상용 툴을 포함한 108개 패밀리를 탐지했습니다. 2022년 동안 17,000대 이상의 고유 커맨드-앤-컨트롤(C2) 서버를 관찰했는데 이것은 작년보다 30% 증가한 수치입니다. 2021년과 마찬가지로 2022년 취합 결과도 Cobalt Strike 팀 서버와 IcedID 및 QakBot을 포함한 봇넷 패밀리, 그리고 PlugX 같은 인기 있는 RAT가 장악했습니다.

주요 결론

- 탐지된 서버(5,481대)의 32%는 레코디드퓨처의 커맨드-앤-컨트롤 소스에 의해서만 독점적으로 확인됐습니다.
- 저희 스캐닝의 결과로 C2 서버를 탐지한 후 해당 서버가 다른 소스에서 보고되기까지 평균 33일이 소요됩니다.
- 탐지되는 C2 서버 수가 2021년 13,629대에서 2022년 17,233대로 30% 증가했습니다.
- PlugX의 "후속 제품(successor)"으로 ShadowPad가 부상했다고 알려져 있지만 PlugX가 여전히 많이 쓰이고 있습니다.
- 2021년과 아주 유사하게 봇넷 멀웨어 중 주로 Emotet과 Qak Bot이 계속 C2 인프라스트럭처를 확장하면서 한 해 동안 널리 퍼졌습니다.
- 러시아 정부가 후원하는 C2 인프라스트럭처의 변화로 특정 세력을 추적하는 일이 다른 정부 후원 집단에 비해 어려워질 수 있습니다.
- 최대 호스팅 업체에서 예상대로 가장 많은 C2 서버가 관측됩니다.하지만 C2 서버를 위해 이용하는 업체가 바뀌기도 했습니다. Shenzhen Tencent Computer Systems의 호스팅이 300% 이상 증가하면서 저희 조사에서는 C2의 가장 인기 있는 업체가 됐고 중국이 미국을 제치고 가장 많은 C2 서버를 호스팅하는 국가가 됐습니다.
- 2021년 저희는 보다 다양한 C2 환경을 예상하면서 새로운 툴링의 탐지가 늘어날 것으로 봤습니다. 하지만 다양성은 새로운 툴의 사용보다는 기존 툴링이 보다 광범위하게 확산되는 관점에서 나타났습니다.

배경

곧 활성화될 C2 서버를 공지하는 리드타임이 길어질수록 방어자들이 보다 선제적으로 위협을 무력화할 수 있습니다. 그림 1에서 보듯 C2 서버가 운영을 시작하기 전 위협 행위자가 수행해야 할 몇 가지 절차가 있습니다.
우선 침해를 하든 합법적으로 구매하든 서버 인프라스트럭처를 확보해야 합니다. 다음으로는 C2 커뮤니케이션을 위해 도메인 네임이 필요하다면 이를 확보하고 등록해야 합니다. 그런 다음 소프트웨어를 설치하고 구성을 튜닝하고 (해당하는 경우) TLS(transport layer security) 인증서를 등록하고 파일을 서버에 추가해야 합니다. 행위자들이 반드시 패널 로그인, 시큐어 쉘(SSH) 또는 원격 데스크탑 프로토콜(RDP)로 접속해서 포트 상에 멀웨어 컨트롤러를 노출시켜야 피해 시스템에서 데이터를 전송하고 감염 시스템에 커맨드를 보낼 수 있습니다. (작전에 따라 추가적 액션이 필요할 수도 있습니다.) 이런 절차가 모두 끝난 후에야 서버를 악의적으로 사용할 수 있습니다.

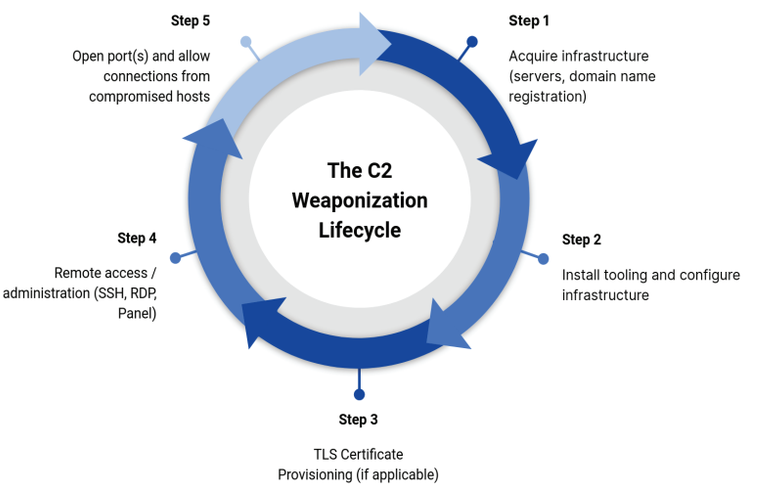


그림1: C2 무기화 라이프사이클 (출처: 레코디드퓨처)

하지만 서버를 세우고 구성, 접속하는 과정에서 서버가 피싱 캠페인이나 악성 툴과 함께 사용되기 전에 탐지 가능한 아티팩트(artifact)가 남게 됩니다. 이런 아티팩트는 방어자 입장에서 탐지 기회를 만들어 주는데 서버에 적용된 소프트웨어 버전, 로그인 패널, TLS 인증서 패턴이나 간단한 탐사로 돌아오는 디폴트 메시지 등을 예로 들 수 있습니다.

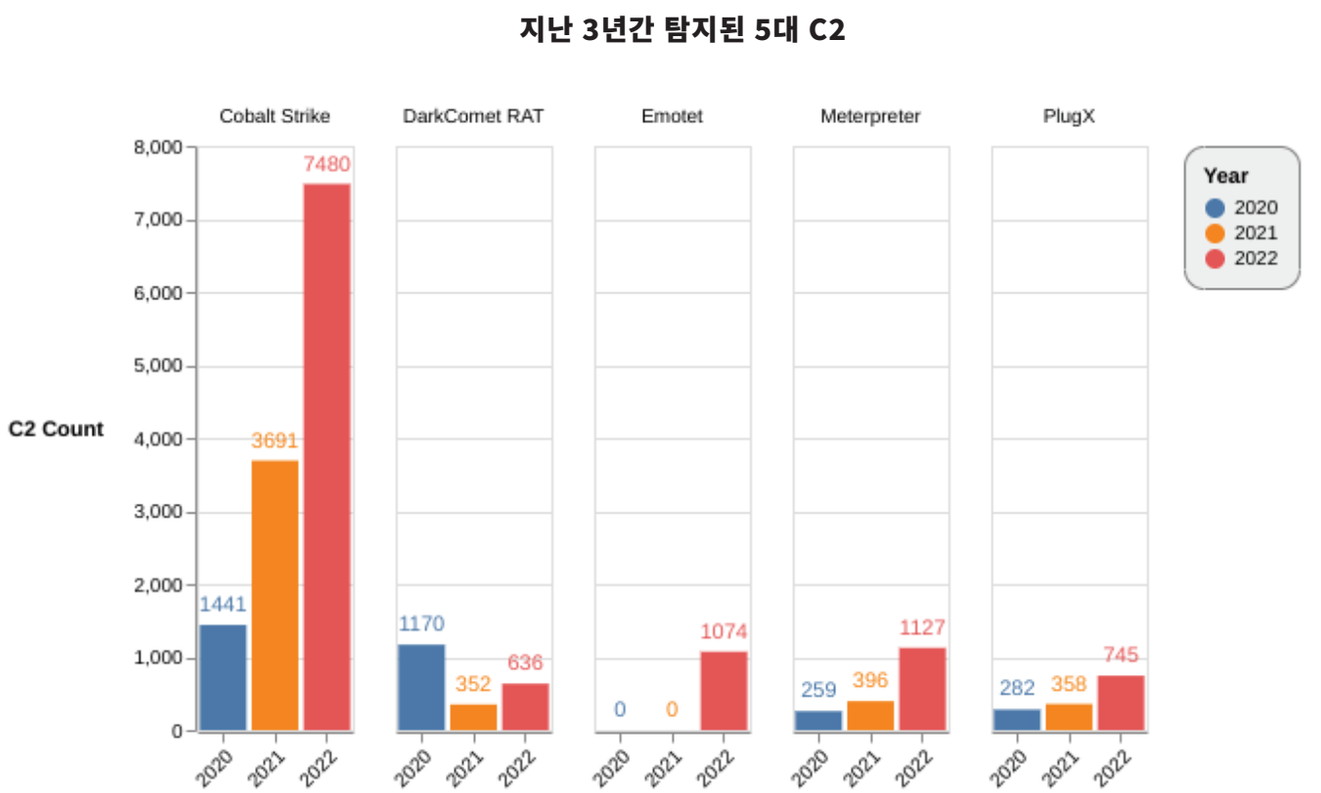


그림2: 레코디드퓨처가 관찰한 상위 5개 C2의 3년간 추이 (출처: 레코디드퓨처)

C2 서버의 생성부터 무기화 과정을 감지하면 적이 어떻게 악의적 공격을 감행하는지 다음과 같은 인사이트를 얻을 수 있습니다.

- 감지된 C2 서버를 해당 패밀리 관련 침해 리포트와 비교하면 실제로 적발된 침해 사고 대비 잠재적으로 얼마나 많은 사건이 비공개로 남았는지 파악할 수 있습니다.
- 서버 생성 속도를 측정하면 향후 활동의 증가나 감소에 대한 인사이트를 얻을 수 있습니다.
- 공개적으로 알 수 없는 지표나 첩보를 포착할 수 있습니다.

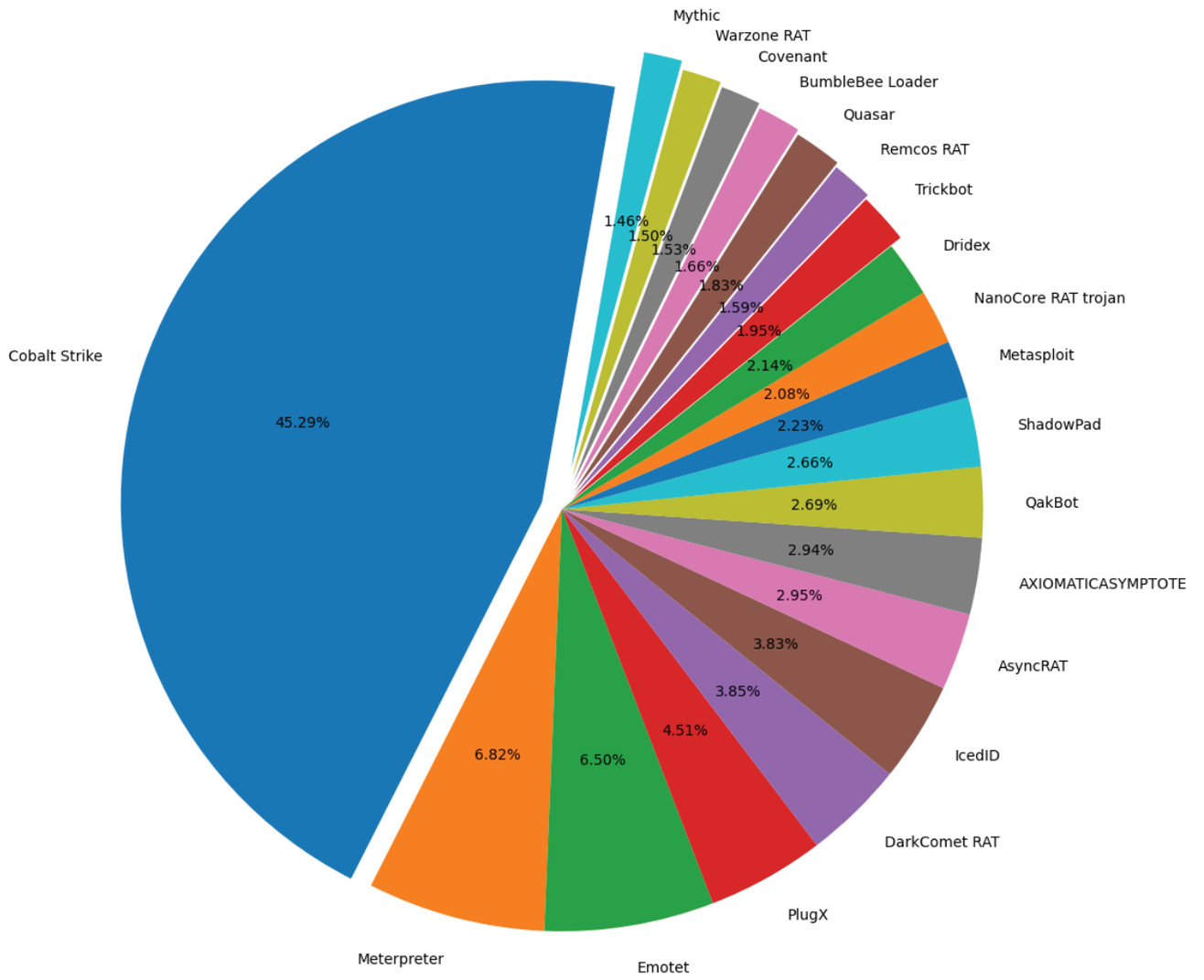
정보 취합 편향에 대해

레코디드퓨처는 알려진 멀웨어 패밀리와 그들의 서버 소프트웨어의 특성을 기반으로 C2 서버 정보를 취합합니다. 이런 취합 정보들은 알려진 커맨드-앤-컨트롤 프레임웍과 그 파생물이나 지원 인프라스트럭처를 파악하는데 집중하며 수동적, 능동적 인터넷 스캔 데이터를 포함합니다. 저희는 C2 서버에서 악의적 행위가 일어났다는 증거가 있을 때 IP 주소가 C2 서버라는 사실만 검증합니다. 따라서 알려진 위협을 감행하는 서버를 보고하는 편향성이 있고 해당 서버에 대해 취합한 정보도 편향성을 갖게 됩니다. 이런 방법론이 네트워크 이상을 확인하거나 예외적 트래픽을 감지하는 대안으로 쓰여서는 안됩니다.

위협 분석

저희가 파악한 상위 5개 C2 패밀리에는 특정 멀웨어 카테고리가 압도적이지 않고 후속 공격 프레임웍(Cobalt Strike), 원격 접속 툴/백도어(PlugX, Dark Comet), 봇넷(Emotet)이 혼합돼 있습니다.

지난 3년간 상위 5개 패밀리를 면밀히 관찰한 결과 확인된 Cobalt Strike, Meterpreter 및 PlugX 서버 수가 오래된 툴임에도 불구하고 지속적으로 증가했습니다. Emotet을 본격 감지한 것은 1년 정도인데 그간 확인된 것을 기준으로 볼 때 Emotet이 다시 완전히 활성화됐음을 알 수 있습니다. DarkComet은 지난 한 해 약 47% 증가한 것으로 알 수 있듯 여전히 위협적입니다. 새로운 멀웨어와 레드팀 툴이 매년 출시되지만 그림2에서 보듯 이전 세대의 고착된 툴에 비해 많이 이용되진 않고 있습니다.



범위를 상위 20개 C2로 넓혀보면 Brute Ratel (BRc4), BumbleBee와 같은 새로운 패밀리가 PlugX, AsyncRAT, IcedID, DarkComet 등의 주류와 함께 섞인, 보다 균형 잡힌 C2 환경을 확인할 수 있습니다. 저희가 2021년에 "C2 환경이 계속 다변화될 것이다. 새로운 멀웨어 패밀리와 C2 프레임웍이 출시되면서 이 중 일부는 자기들의 서버를 스캔하고 탐지하는 위협 인텔리전스 기법을 인지하게 될 것으로 예상한다"라고 예측했습니다. 이것이 사실로 드러났지만 2022년에는 작년의 5대, 20대 리스트에 포함되지 않는 다른 툴을 가진 C2가 상당히 증가했음을 확인했습니다. 올해 증가분의 대부분은 다양한 행위자들이 PlugX, Remcos, DarkComet, QuasarRAT 같은 "고착된" 툴링을 사용한데 기인합니다. 저희 데이터셋에 따르면 2021년에 비해 2022년에 이용이 증가한 6대 툴은 다음과 같습니다.

1. PlugX (51% increase)
2. Remcos (51% increase)
3. DarkComet (44% increase)
4. QuasarRAT (40% increase)
5. Mythic (33% increase)
6. AsyncRAT (24% increase)

상용화 툴이 많이 사용되는 이유는 점점 많은 위협 행위자들이 탐지를 피하는 것보다는 잘 섞여들어서 용의자로 지목되지 않는 것을 더 중시하거나 또는 공격 대상이 이런 잘 알려진 툴조차도 탐지할 가능성이 없다고 판단했기 때문입니다. 그리고 맞춤 툴을 개발하는데 드는 비용과 전문성을 고려하면 위협 행위자 입장에서 상용 툴을 구매하거나 무료 오픈소스 툴을 사용하는 것을 선호할 수 있습니다.

PlugX vs. AXIOMATICASYMPTOTE 월별 활성 C2 수

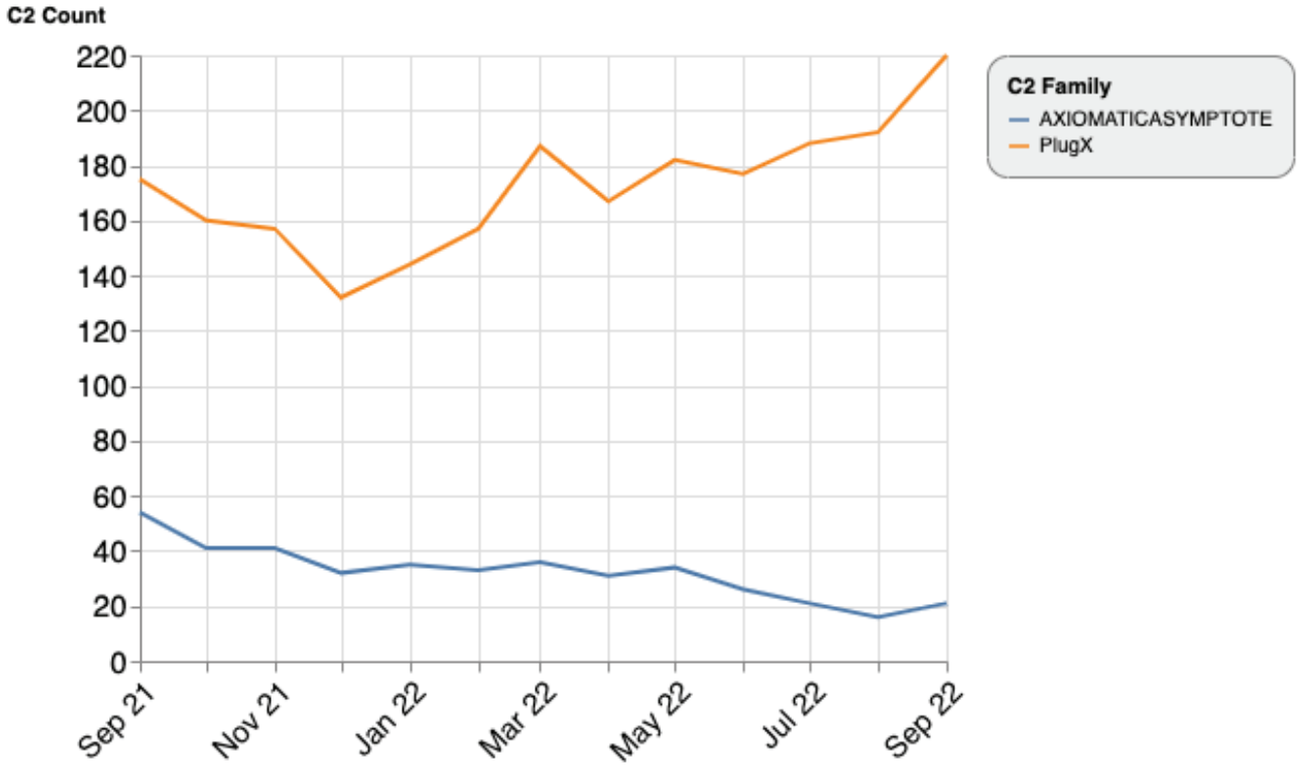


그림4: 지난 12개월간 탐지된 PlugX 및 AXIOMATICASYMPTOTE의 C2 서버 수 (출처: 레코디드퓨처)

예를 들어 BRc4를 사용하면 더 많은 EDR 회피 테크닉을 쓸 수 있지만 유저 베이스가 비슷하기 때문에 공격자로 지목 당할 위험이 커집니다. 반면 DarkComet은 BRc4만큼 잘 숨거나 회피할 수는 없지만 많은 위협 행위자들이 사용하는 오픈소스 RAT입니다.

2022 Adversary Infrastructure 테마

2022년 저희가 C2에 대해 확인한 내용을 종합하면 세 가지 테마로 정리할 수 있습니다.

1. 후속 제품 등장에도 불구하고 PlugX는 여전히 성공적: ShadowPad가 "후속 제품"이라고 불리지만 PlugX가 여전히 널리 사용되고 있습니다.

2. 다시 봇으로 (다시, 또 다시): 2021년 만큼은 아니지만 많은 봇넷이 여전히 아주 활동적입니다. Emotet, IcedID, QakBot, Dridex, TrickBot 모두 2022년 20대 리스트에 들었습니다.

3. 러시아, '읽은 즉시 파기하세요': 러시아 소행으로 의심되는 C2 탐지의 한계

후속 제품 등장에도 불구하고 PlugX는 여전히 성공적

2020 Adversary Infrastructure 리포트에서 저희는 ShadowPad를 PlugX의 후속 제품으로 설명한 Doctor Web의 기사를 참고했습니다. 중국 정부의 후원을 받는 많은 집단이 ShadowPad를 점점 많이 도입하기 시작했지만 저희는 2020년 후에도 계속 PlugX 감염을 관측했습니다.
(레코디드퓨처는 ShadowPad 컨트롤러를 관리하는 인프라스트럭처를 AXIOMATICASYMPTOTE라는 이름으로 추적하고 있습니다). 2022년에도 PlugX는 계속 사용되고 있고 아래 그래프에서 보듯 심지어 사용이 증가했습니다.

PlugX는 지난 십년 간 주로 중국 기반 위협 행위자들이 사용해왔습니다. 2015년 Airbus가 보고한 바에 따르면 이전 PlugX 변종의 빌더가 공개적으로 유출됐습니다. 이로 미루어 볼 때 PlugX 사용은, 제한적인 중국 지원 위협 행위자를 상대로 사적으로 판매될 가능성이 높은 ShadowPad에 비해 통제가 약할 가능성이 높습니다. 저희는 RedDelta 및 RedFoxtrot 위협 행위자 집단과 연관된 것으로 보이는 PlugX 변종을 적극적으로 추적하고 있습니다.

월별 봇넷 활성화 C2 개수

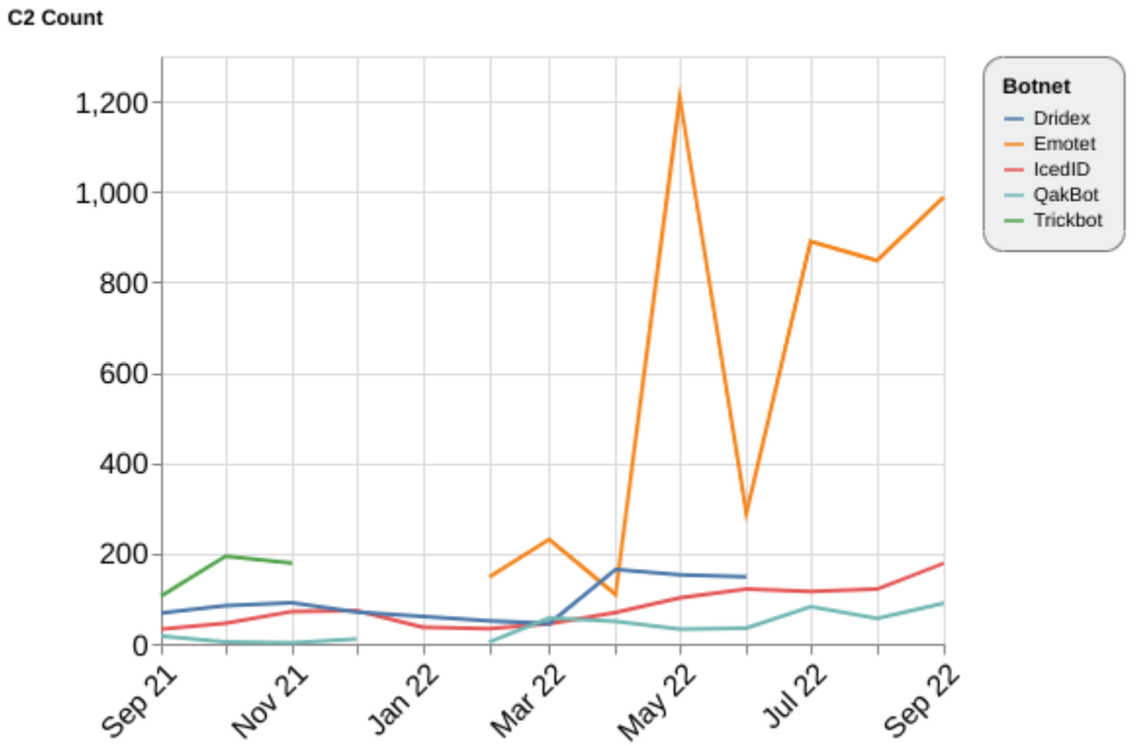


그림5: 탐지된 Dridex, Emotet, IcedID, QakBot, TrickBot C2 수 (출처: 레코디드퓨처)

다시 봇으로 (다시, 또 다시)

2021년 Emotet 검거 후로 봇넷 활동이 급격히 증가했으며 TrickBot, QakBot, Bazar, IcedID, Dridex가 탐지된 C2의 과반수 이상을 차지했습니다. 2022년에는 봇넷이 저희 C2 데이터를 장악하지는 않았지만 여전히 5대, 20대 리스트에 포함됐습니다. 그림 5에서 보듯 Dridex, Emotet, IcedID, QakBot, TrickBot은 저희가 확인한 봇넷 패밀리 중 가장 많은 C2가 탐지됐습니다.

TrickBot과 Dridex

탐지되는 TrickBot C2 수(194개 활성 C2)가 2021년 10월 갑자기 폭증했다가 몇 달 후 사라졌습니다. 마찬가지로 Dridex 활동도 매월 45~80대의 활성 C2가 꾸준히 탐지되다가 2022년 6월 급증하더니 (150대 활성 C2) 곧 휴면기에 접어들었습니다.

TrickBot 활동 흐름은 TrickBot 운영자들이 TrickBot 멀웨어 사용을 점차 줄이고 있다는 올해 초 리포트와 일치합니다. Dridex의 경우 3월부터 사용이 증가해서 6월에 정점을 찍었는데 Dridex가 RIG 익스플로잇 키트에 사용된다는 리포트와 관련이 있습니다. Dridex가 갑자기 잠잠해진 것도 IcedID와 QakBot이 널리 쓰이고 Emotet이 재부상하면서 이 봇넷이 밀려났기 때문일 수 있습니다.

QakBot

작년 말부터 올해 초까지 확인된 QakBot C2는 월별 활성 C2가 10대 정도로 상대적으로 적었습니다. 2022년 3월부터 탐지되는 QakBot C2가 상당히 증가했는데 2022년 9월에는 활성 C2가 90대로 최고치를 기록했습니다. 가장 최근에는 SentinelOne에서 QakBot이 Black Basta 랜섬웨어 전송에 사용되는 것을 확인했다고 합니다.

IcedID

2022년 5월까지 IcedID는 매월 활성 C2가 30에서 60대까지 들쭉날쭉했습니다. 5월부터 102대로 증가하더니 계속 늘어서 2022년 9월에는 활성 C2가 178대에 달했습니다. 아래의 주요 사건이 이런 증가에 기여한 원인일 수 있습니다.

- 2022년 4월, CERT-UA가 IcedID 멀웨어를 설치하는 XLS 문서의 대량 배포를 경고했습니다.
- 가장 최근에는 IcedID가 Quantum Locker 랜섬웨어를 다운받아 실행시키는데 사용됐다고 알려졌습니다.

Emotet

2021년 초 Emotet 인프라스트럭처 검거 후 오래 활동이 없자 Emotet이 영구히 운영을 중단할 수도 있다는 추측이 있었지만 틀린 예측으로 판명됐습니다. Emotet이 2021년 후반, 알려지기로는 Conti 랜섬웨어 세력과 함께 돌아왔습니다. Emotet의 빠른 재부상은 TrickBot 인프라스트럭처를 재사용한 덕분인 것으로 알려졌습니다. 그림 5를 보시면 우연히도 TrickBot이 운영을 중단한 직후 저희가 TrickBot을 추적한 똑같은 수만큼의 활성 C2로 Emotet이 시작을 합니다.

Emotet C2 수가 2021년 후반과 2022년 초에는 상대적으로 적었지만 2022년 5월 활성 C2가 1,200대 이상으로 급증한 것을 확인했습니다. Netskope Threat Labs 리포트에 따르면 이 기간 중 LNK 파일과 마이크로소프트 오피스 문서를 이용해서 Emotet을 퍼뜨린 두 가지 공격이 있었다고 합니다.

6월에는 다시 낮은 수준으로 돌아왔지만 2022년 7월에 Emotet 숫자가 다시 증가하기 시작했습니다. 현재 파악되는 활성 Emotet C2는 5월에 폭증했던 수준과 비슷해서 2022년 9월에는 1,000대가 조금 넘습니다. 2022년 7월 이후 최근 급증한 Emotet 활성 C2는 Emotet에 대한 가장 최신 리포트의 내용을 뒷받침합니다.

- Emotet이 Quantum과 ALPHV 랜섬웨어를 로드하는데 사용되고 있습니다.

- Proofpoint는 11월에 Emotet이 매일 “수만 통”의 피싱 이메일을 발송하면서 IcedID를 로드 및 실행하는데 사용된다고 밝혔습니다. Emotet을 통한 IcedID 배포가 최근 저희의 IcedID 탐지 증가에 기여했을 수 있습니다.

러시아, ‘읽은 즉시 파기하세요’

저희가 관찰한 바에 따르면 러시아 정부가 후원하는 행위자들이 다른 정부 지원 세력에 비해 더 좋은 C2 인프라스트럭처 운영 보안을 사용하는 경우가 많습니다. 예를 들면 1:1 기준으로 C2 서버를 운영하면서 단일 표적 조직의 임플랜트하고만 인터랙션을 합니다. 또 그들의 C2 인프라스트럭처가 공개적으로 알려지면 신속하게 폐기되는 것을 확인했습니다. 러시아의 후원을 받는 일부 행위자의 경우 앞장서서 상용 멀웨어와 인기 있는 C2 프레임웍으로 전환하는 트렌드를 이끌기도 했습니다. 일반적인 상용 소프트웨어를 첩보 작전에 사용하는 위협 행위자들의 경우 연구원이나 조사원들이 책임 소재를 파악하기가 더 어려울 수 있습니다.

이와 반대로 중국, 이란, 그 외 국가의 소행으로 보이는 작전들은 멀웨어 및 인프라스트럭처 운영 보안에 부주의한 경우가 많아 대외적으로 공개된 후에도 여러 표적에 대해 특정 C2를 사용하거나 여러 작전팀이 수년 동안 (PlugX 같은) 동일한 멀웨어를 공유하면서 쓰기도 합니다.

러시아 정부가 후원하는 C2 인프라스트럭처는 자주 변경되기 때문에 특정 작전을 추적하기가 더욱 어렵습니다. GRAVITYWELL은 레코디드퓨처가 러시아 해외 첩보 서비스(SVR)와 연계된 WellMess 백도어를 호스트하는 일반적 서버 기술과 TLS 인증서 구성을 묶어서 지칭하는 용어인데 이것이 그런 일시적인 인프라스트럭처의 예라고 할 수 있습니다.

저희는 여러 단계에 걸쳐 GRAVITYWELL을 추적했는데 각 단계 사이에서 GRAVITYWELL 활동이 대외적으로 알려진 직후에 인프라스트럭처가 분명히 달라지는 것을 확인했습니다.

2020년 7월, 영국 국립사이버보안센터(NCSC)가 WellMess를 이용한 APT29 작전에 대한 리포트를 발간했습니다. 이 리포트에는 해당 작전에 사용된 것으로 알려진 C2가 포함됐습니다. 2020년 8월, 이 인프라스트럭처가 새로운 C2 셋으로 교체됐는데 이전 단계의 작전과 구분되는 TLS 인증서로 파악할 수 있었습니다. 2021년 7월 발행된 RiskIQ 리포트는 TLS 인증서 내역을 제공하는 30대 이상의 C2 서버를 확인했습니다. 1년 전과 마찬가지로 해당 리포트가 공개된 후 한 달 내에 C2 변경이 확인됐습니다.

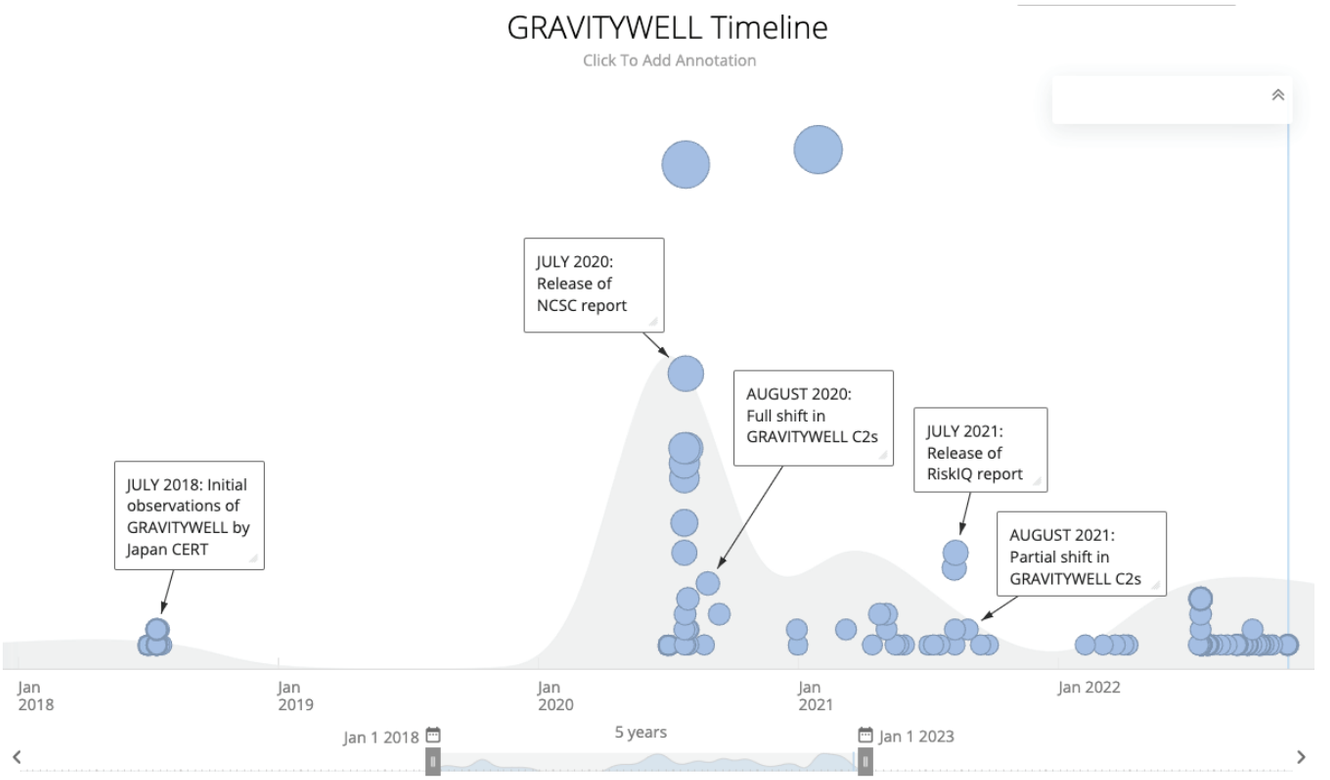


그림6: GRAVITYWELL에 대한 공개 리포트와 인프라스트럭처 변경 연대표 (출처: 레코디드퓨처)

후속 공격(post-exploitation) 프레임웍

저희가 탐지한 후속 공격 프레임웍 중 어느 정도가 합법적 레드팀 작전에 쓰였고 어떤 것들이 범죄 혹은 첩보 세력에 이용됐는지 추측하기는 어렵습니다. 전체적인 수량의 변화는 여러 작전에 쓰이는 경우 외에도 시그니처가 개선되거나 취합 노력이 강화된 덕분일 수 있습니다.

지난 3년간 확인된 상위 10대 공격적 보안 툴

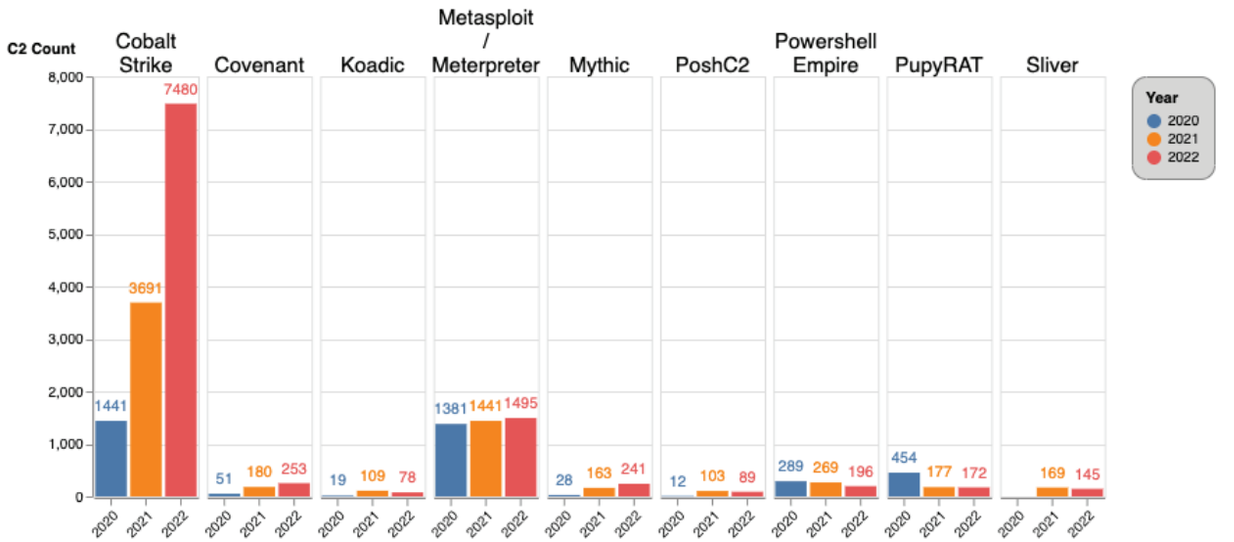


그림7: 지난 3년간 확인된 공격적 보안 툴에 쓰인 C2서버 (출처: 레코디드퓨처)

작년 한 해 동안 확인된 상위 10대 공격 보안 툴을 그 전 2년과 비교하면 한 가지를 분명히 알 수 있습니다. Cobalt Strike C2 활동이 계속 빠른 속도로 증가한다는 사실입니다. Cobalt Strike는 확실히 여러 행위자들이 선호하는 공격 보안 툴이고 Cobalt Strike 탐지 건 수가 작년에 상당히 증가했습니다. 이렇게 두 배나 증가한 이유는 탐지되는 경우가 늘어나고, 탐지 기간이 길어지고, Cobalt Strike를 사용하는 행위자가 많아졌기 때문이라고 보고 있습니다.

그 외 10대 프레임웍 중 수량이 증가한 경우는 Covenant, Mythic, Metasploit/Meterpreter(올해는 이 두 개를 합쳤습니다)가 있습니다. 하지만 Cobalt Strike만큼 크게 급증한 경우는 없습니다. Covenant의 오픈소스 프로젝트는 2021년 이래로 업데이트되지 않았지만 이용은 계속 증가하고 있습니다. Mythic은 계속해서 코드 베이스에 업데이트를 받고 있습니다. 일부 Mythic 인프라스트럭처가 Botleggers Club이라는 이름을 참조하는데 이것은 Conti 유출 사고에서도 언급된 적이 있어 적어도 일부 랜섬웨어 운영자들이 사용했다고 추측할 수 있습니다.

Brute Ratel(BRc4)과 BeEF는 모두 탐지율이 높지 않아서 안타깝게도 10대 리스트에 들지 못했습니다. BRc4의 개발자는 EDR 개발 경력이 있는 사람으로 EDR이 탐지를 피하는 방식을 구체적으로 활용해서 해당 툴의 탐지를 어렵게 만들고 있습니다. BRc4 버전 중 하나가 크랙돼서(cracked) 범죄자들 사이에서 번지고 있으며 Black Basta 랜섬웨어 집단이 사용하는 것이 확인됐습니다.

세계적 규모

2022년(17,233대)에는 2021년(13,268대)에 비해 30% 더 많은 C2 서버를 탐지했습니다. 이유는 새로운 멀웨어 탐지 기술이 개발됐고 기존 멀웨어 패밀리에 대한 탐지력이 강화됐으며 Cobalt Strike, Meterpreter, PlugX 등을 탐지하는 툴의 활용이 증가했기 때문입니다.

저희는 C2 인프라스트럭처가 116개 국가에 걸쳐 1,419개 호스팅 업체에서 구축된 것을 확인했습니다. 지리적으로 전 세계의 과반을 차지하지만 악용되는 서버 수는 70,000개 이상의 업체보다 많은 전체 자율 시스템(AS) 운영자 중 아주 적은 비중을 차지할 뿐입니다.

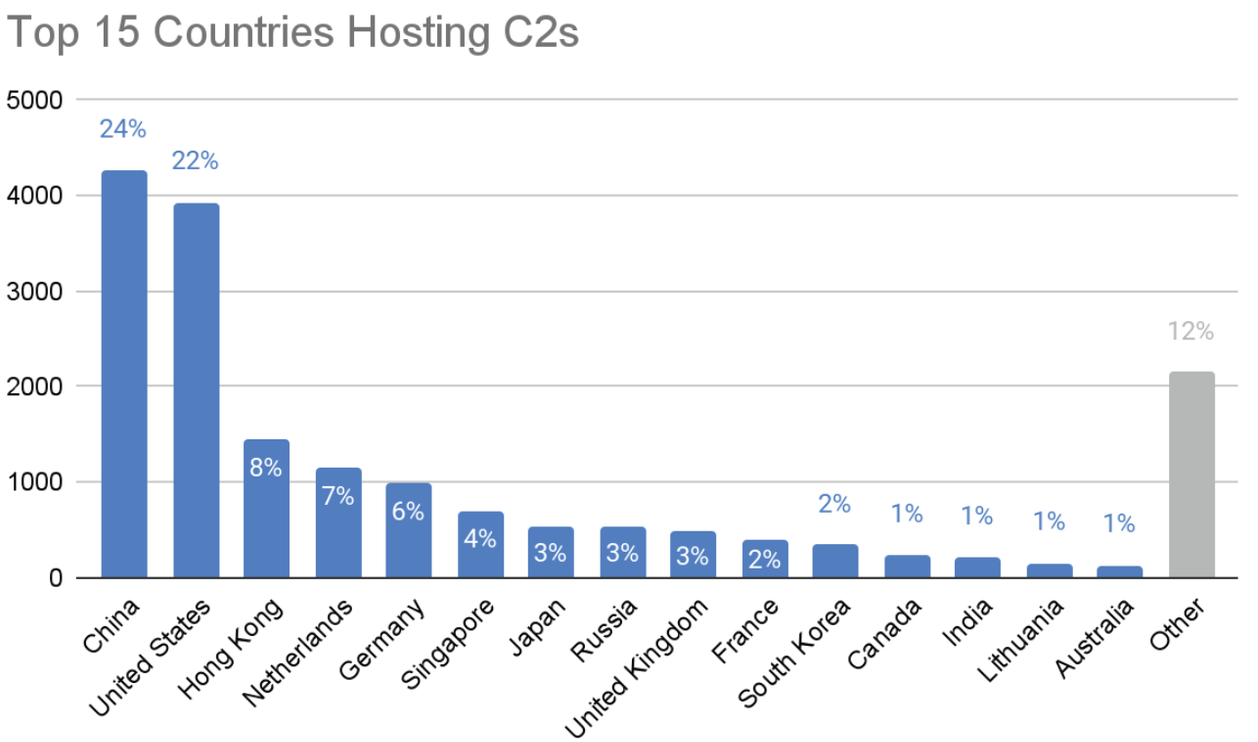


그림8: (자율 시스템 번호[ASN] 위치로 파악된) 국가별 C2 호스팅 (출처: 레코디드퓨처)

- 2021년과 마찬가지로 최대 호스팅 업체들이 C2 호스팅에 가장 많이 악용됩니다. 24개 AS 운영업체(확인된 전체 ASN의 1%)에서 2022년 동안 100대 이상의 C2 서버가 탐지됐습니다. (2021년에 AS 운영업체 수는 20개).

- 1,419개 AS 운영자가 2022년 동안 C2 서버를 호스팅하는 것을 확인했지만 과반수 이상이 100대 이하의 C2서버를 호스팅하고 있었고(98%) 1,225개의 AS 업체(확인된 총 ASN의 86%)가 10대 이하를, 그리고 682개의 AS 업체가 단 1대의 C2 서버를 호스팅했습니다.

순위에는 다소 변화가 있었지만 수량 기준으로 10대 C2 호스팅 업체의 구성은 2021년 이래 거의 변화가 없습니다. 유일하게 싱가폴 소재의 BGPNET Global(AS64050)만 C2 서버가 181대에서 147대로 감소하면서 Alibaba (US) Technology Co., Ltd.로 대체됐습니다. 전반적으로 모든 10대 C2 호스팅 업체에서 C2 서버 탐지가 상당히 증가했고 4개 업체는 2021년에서 2022년 사이 50% 이상 증가를 기록했습니다.

- 중국이 4,265대의 C2 서버를 2022년 호스팅했고 미국이 3,928대로 2위였으며 홍콩이 3위로 1,451대였습니다. 이 상위 3개 국가가 탐지된 모든 C2 서버의 55%를 차지했고 상위 10개 국가가 탐지된 모든 C2 서버의 88%를 차지했습니다.

- C2 서버를 호스팅하는 것으로 확인된 116개 국가 중 18개 국가는 2022년 단 1대의 C2 서버만 호스팅했습니다.

- 미국의 C2 서버 호스팅 비중이 34%에서 22%로 떨어진 반면 중국의 비중은 14%에서 24%로 증가했는데 중국 호스팅 업체인 Shenzhen Tencent Computer Systems의 C2 탐지가 크게 늘었기 때문입니다.

- 홍콩과 네덜란드에서 탐지된 C2 서버의 비중은 각각 3.3%에서 8%로, 2.1%에서 7%로 증가했습니다.

Top 10 C2 Hosting Providers by Volume					
Hosting Provider	ASN	Country	Total C2s (2021)	Total C2s (2022)	YoY Increase
Shenzhen Tencent Computer Systems	AS45090	China	571	2297	+302%
DigitalOcean, LLC	AS14061	United States	968	1421	+48%
Amazon.com, Inc.	AS16509	United States	624	1156	+85%
Hangzhou Alibaba Advertising Co., Ltd.	AS37963	China	574	1126	+96%
The Constant Company, LLC	AS20473	United States	700	834	+19%
Microsoft Corporation	AS8075	United States	205	411	+100%
OVH SAS	AS16276	France	267	338	+27%
Linode, LLC	AS63949	United States	208	291	+40%
M247 Ltd	AS9009	United States	171	228	+33%
Alibaba (US) Technology Co., Ltd.	AS45102	United States	95	192	+102%

도표1: 2021년 대비 2022년 확인된 C2 서버 수량 기준 최고 C2 호스팅 업체

- 중국 소재의 Shenzhen Tencent Computer Systems가 302%의 C2 서버 증가율을 기록, 2022년 레코디드퓨처가 확인한 모든 ASN 중 가장 많은 C2 서버를 호스팅했습니다. 이 업체는 2,297대의 개별 C2 서버(13%)를 운영했습니다. Shenzhen Tencent Computer Systems에서 가장 빈번하게 확인된 패밀리는 Cobalt Strike로 2,032대의 서버를 확인했습니다.

  그 다음은 미국에 기반한 DigitalOcean LLC로 2021년에는 1위를 차지했습니다. 이 업체는 48%의 증가율을 기록하면서 1,421대의 개별 C2 서버(8%)를 운영했습니다.
  DigitalOcean LLC에서 가장 많이 확인된 패밀리는 Cobalt Strike로 526대의 서버를 확인했습니다.

도표2를 보면 5대 멀웨어 패밀리가 10대 호스팅 업체의 C2 서버 중 상당 부분을 차지하고 있습니다. 저희가 파악한 5대 멀웨어 패밀리가 10대 호스팅 업체 중 절반에서 탐지한 모든 C2 서버의 최소 80%를 차지했습니다. “최대 멀웨어 %” 컬럼은 해당 호스팅 업체의 총 C2 중 5대 멀웨어 패밀리가 차지한 C2의 비중을 의미합니다.

Top 5 Malware Families by C2 Hosting Providers			
Hosting Provider	Top Families	Total C2s	Top Malware %
Shenzhen Tencent Computer Systems	Cobalt Strike, Meterpreter, AXIOMATICASYMPTOTE, Metasploit, PlugX	2178	95%
Hangzhou Alibaba Advertising Co., Ltd.	Cobalt Strike, Meterpreter, Sliver, PupyRAT, XtremeRAT	1041	92%
DigitalOcean, LLC	Cobalt Strike, YerLoader, IcedID, Meterpreter, Mythic	935	66%
Amazon.com, Inc.	Cobalt Strike, Meterpreter, Koadic, Sliver, Gh0st RAT	668	58%

Top 5 Malware Families by C2 Hosting Providers			
Hosting Provider	**Top Families**	**Total C2s**	**Top Malware %**
The Constant Company, LLC	Cobalt Strike, PlugX, AXIOMATICASYMPTOTE, Meterpreter, QakBot	669	80%
Microsoft Corporation	Cobalt Strike, Cerberus, Meterpreter, DarkComet, Empire Powershell	290	71%
M247 Ltd	Cobalt Strike, BumbleBee, IcedID, Meterpreter, PlugX	200	88%
OVH SAS	Cobalt Strike, BumbleBee, IcedID, Meterpreter, NanoCore RAT	178	53%
Alibaba (US) Technology Co., Ltd.	Cobalt Strike, Meterpreter, XtremeRAT, AXIOMATICASYMPTOTE, CROSSWALK	159	83%
Linode, LLC	Cobalt Strike, Meterpreter, AXIOMATICASYMPTOTE, Mythic, PlugX	125	43%

도표2: 2022년 확인된 C2 호스팅 업체 기준 최대 멀웨어 패밀리

도표2를 보면 Cobalt Strike가 모든 호스팅 업체에서 최대 멀웨어 패밀리였으며 많은 경우 Meterpreter가 그 뒤를 이었습니다. AXIOMATICASYMPTOTE와 PlugX는 일반적으로 동일한 호스팅 업체에서 발견됩니다. 레코디드퓨처 BumbleBee 탐지의 26%가 M247 Ltd와 OVH SAS 기반이었으며 Cerberus 탐지의 57%는 Microsoft Corporation infrastructure 기반이었습니다.

이런 호스팅 업체들이 C2 서버 호스팅의 가장 큰 비중을 차지하긴 했지만 C2 서버는 이들이 관리하는 전체 서버 중 극소수를 차지할 뿐입니다. 도표3은 전체 보유 서버 대비 C2 서버 비중이 가장 높은 10대 업체를 정리한 것입니다. 이것은 AS가 밝힌 IPv4 prefix 개수를 기준으로 2022년 확인된 C2 서버 수와 비교한 것입니다.

- 도표3에서 두 개 호스팅 업체가 유일하게 2021년 호스팅한 C2 서버의 비중이 가장 높은 10대 호스팅 업체에도 포함됐는데 영국 소재 International Hosting Solutions LLP와 홍콩 소재 HDTIDC LIMITED입니다. Media Land LLC, Host Sailor Ltd.와 같은 방탄 호스팅(bulletproof hosting) 업체는 리스트에서 탈락했습니다.

- 오픈소스 데이터를 기준으로 도표3에 포함된 대부분의 호스팅 업체는 다음과 같은 특징을 갖습니다.

    - (예를 들면 UAB Cherry Servers, BL Networks, KURUN CLOUD INC와 같은) 위험한 웹 트래픽과 관련이 있습니다.
    - (예를 들면 HDTIDC LIMITED를 이용하는 TAG-26과 같은) 특정 위협 행위자들이 선호하는 호스팅 업체로 여겨져왔습니다.
    - (예를 들면 Flyservers S.A.나 Chang Way Technologies Co. Limited 같은) 알려진 방탄 호스팅 업체입니다.

Hosting Providers with Highest Percentage of C2s Hosted				
Hosting Provider	**ASN**	**Country**	**Top Detection**	**% of Servers Hosted Are C2s**
UAB Cherry Servers	AS59642	Lithuania	Cobalt Strike	3.91%
SteamVPS SRL	AS50578	Romania	IcedID	2.73%
KURUN CLOUD INC	AS395886	United States	Cobalt Strike	2.34%
Flyservers S.A.	AS48721	Panama	Cobalt Strike	1.56%
HDTIDC LIMITED	AS136038	Hong Kong	Roaming Mantis	1.20%
International Hosting Solutions LLP	AS213354	United Kingdom	YerLoader	1.17%
Flyservers S.A.	AS209588	Panama	Cobalt Strike	0.95%
Chang Way Technologies Co. Limited	AS57523	Hong Kong	Cobalt Strike	0.91%
BL Networks	AS399629	United States	Cobalt Strike	0.80%
BlueVPS OU	AS62005	Estonia	IcedID	0.78%

도표3: 2022년 전체 서버 대비 가장 높은 비중의 C2서버를 호스팅한 업체

전망

2023에도 여전히 Cobalt Strike와 봇넷이 저희가 파악하는 C2의 과반수를 차지할 것이라고 예측할 수 있습니다. Cobalt Strike가 저희의 내년 5대 탐지 멀웨어에도 포함될 것으로 예상하지만 또 다시 두 배나 증가할 것으로 보진 않습니다. 저희는 Cobalt Strike 사용이 BRc4에 잠식당할 것으로 예상합니다. 따라서 BRc4 사용과 C2 탐지가 증가할 것입니다. 위협 행위자들이 EDR 에이전트에 탐지가 덜 되고 Cobalt Strike의 유용한 대안인 BRc4로 옮겨가고 있기 때문입니다. 그리고 Sliver, DeimosC2, Alchimist, Manjusaka 같은 니치 C2 툴과 관련된 C2 탐지가 증가할 것으로 예상합니다.

Redline Stealer, QakBot, Nanocore 같은 멀웨어 패밀리가 무작위적으로 비표준 포트를 사용하면서도 성공을 하고 있습니다. 이로 인해 전통적인 풀 인터넷 스캐닝을 하지 못합니다. IPv4 영역에서 가능한 모든 비표준 포트를 스캔하기란 불가능하기 때문입니다. 한 때는 탐지가 더 쉽다고 여겨졌던 하이 포트(high ports) 사용이 여전히 적절한 C2 커뮤니케이션 채널인 것으로 보이고 저희는 더 많은 C2 운영자들이 C2 커뮤니케이션을 위해 하이 포트를 사용할 것으로 예상합니다.

2022년 6월, ShadowServer가 IPv6 인터넷 영역을 스캔하는 자체 방법론을 상세히 소개했습니다. 저희는 레코디드퓨처를 포함한 더 많은 조직이 IPv6 스캔을 하고 그 결과 IPv6 C2 탐지가 늘어날 것으로 예상합니다. 널리 알려지진 않았지만 Mandiant가 보고한 VirtualPie처럼 IPv6 커넥션으로 통신하는 멀웨어가 존재합니다.

About Insikt Group®

Insikt Group은 레코디드퓨처의 위협 리서치 부서로 행정부, 사법부, 군사 및 첩보 기관 경험이 풍부한 분석가와 보안 연구원들로 구성됩니다. 이들의 임무는 일련의 사이버 및 지정학적 위협에 대한 인텔리전스를 제공, 고객의 위험을 낮추고 실질적 성과를 내며 비즈니스 차질을 예방하는 것입니다. 정부 후원 위협 집단, 다크넷과 범죄 세계의 금전적 목적이 있는 위협 행위자, 새롭게 부상하는 멀웨어 및 공격자 인프라스트럭처, 전략적 지정학, 영향력 공작(influence operation)에 대해 연구합니다.

About Recorded Future®

레코디드퓨처(Recorded Future)는 세계 최대 인텔리전스 기업입니다. 레코디드 퓨처의 클라우드 기반 인텔리전스 플랫폼은 공격자, 인프라스트럭처, 타깃을 아우르는 가장 포괄적인 커버리지를 제공합니다. 레코디드 퓨처는 지속적이고 광범위한 자동 데이터 수집 및 분석과 전문가 분석을 결합하여 거대한 디지털 환경에 대한 실시간 가시성을 제공, 기업이 공격자에 대해 선제적 액션을 취하고 자사의 직원, 시스템, 인프라스트럭처를 안전하게 보호하도록 지원합니다. 레코디드 퓨처는 보스턴에 본사를 두고 전 세계 사무소 직원들과 함께 60여 국가에서 1,400여 기업 및 정부 기관과 협력하고 있습니다.

보다 자세한 사항은 recordedfuture.com에서 확인할 수 있습니다.
트위터에서 @RecordedFuture를 팔로우하세요.

문의처 : Korea-contact@recordedfuture.com