원격 액세스 툴 확산에 따른 문제점

기업들은 OT 환경에 원격 액세스 솔루션을 지나치게 많이 배포한 결과, 과도한 리스크와 운영 부담을 떠안게 되었습니다.

CLAROTY

TEAM82

요약

보안이 취약한 원격 연결이 ICS(산업 제어 시스템)와 같은 인터넷 연결 OT(운영 기술) 자산 및 IT 네트워크에 대한 초기 거점을 마련하기 위한 위협 행위자들의 진입 경로로 인기를 얻고 있습니다. 이러한 노출이 기업에게 중대한 위험을 야기한다는 것은 명백한 사실입니다. 내부 직원뿐만 아니라 벤더, 공급업체, 기술 파트너 등 원격 액세스에 대한 제3자의 과도한 수요로 인해 그 위험은 더욱 가중되고 있습니다.

기업은 로컬 네트워크와 클라우드 액세스를 보호해야 할 뿐만 아니라 공급망 파트너의 사이버보안 태세도 함께 고려하여 리스크 평가 및 우선순위 설정을 수행하고 시스템에 대한 권한 있는 액세스를 평가해야 합니다.

지금까지 사용되어 온 접근법 중 하나는 문제 해결을 위해 기술을 과도하게 투입하는 것이었습니다. 일부 기업이 6개~16개의 원격 액세스 툴을 배포하기도 하는 OT 환경에서 이러한 접근법이 특히 두드러집니다. 2가지 이상의 (IT 및 OT용) 원격 액세스 툴을 배포하는 사례가 종종 목격되지만 이러한 무분별한 확산은 위협 행위자가 악용할 수 있는 공격 표면을 넓히고 툴 관리 및 보호 측면에서 상당한 운영 부담을 가중합니다.

본 보고서에서는 원격 액세스 툴의 확산 현상 및 이러한 확산이 야기할 노출을 OT 환경을 중심으로 탐색합니다. 또한 OT 자산 및 네트워크 리소스에 대한 액세스를 제공하는 배포된 툴의 유형과 이러한 툴이 제공하는 보안 기능에 대해서도 살펴봅니다.

주요 조사 결과

1. 클래로티의 Team82 연구자들은 전용 OT 하드웨어에서 실행되는 알려진 산업 네트워크에 설치된 애플리케이션을 중심으로 특정 고객 범주에 걸쳐 5만 개 이상의 원격 액세스 기반 장치로 구성된 데이터세트를 조사했습니다.

2. 일부 기업에서는 원격 액세스 툴이 과도한 확산을 보이고 있습니다. 조사 결과, 기업의 55%가 OT 환경에서 원격 액세스 툴을 4개 이상 사용하고 있으며 33%는 6개 이상 사용하는 것으로 나타났습니다.

3. 이러한 툴은 대부분이 엔터프라이즈급 보안 제품이 아니므로 권한 있는 액세스에 대한 관리 기능을 지원하지 않습니다. 기업의 79%가 OT 네트워크에서 실행되는 장치에 이러한 비엔터프라이즈급 툴을 2개 이상 설치하여 위험한 노출과 추가적인 운영 비용을 초래하고 있습니다.

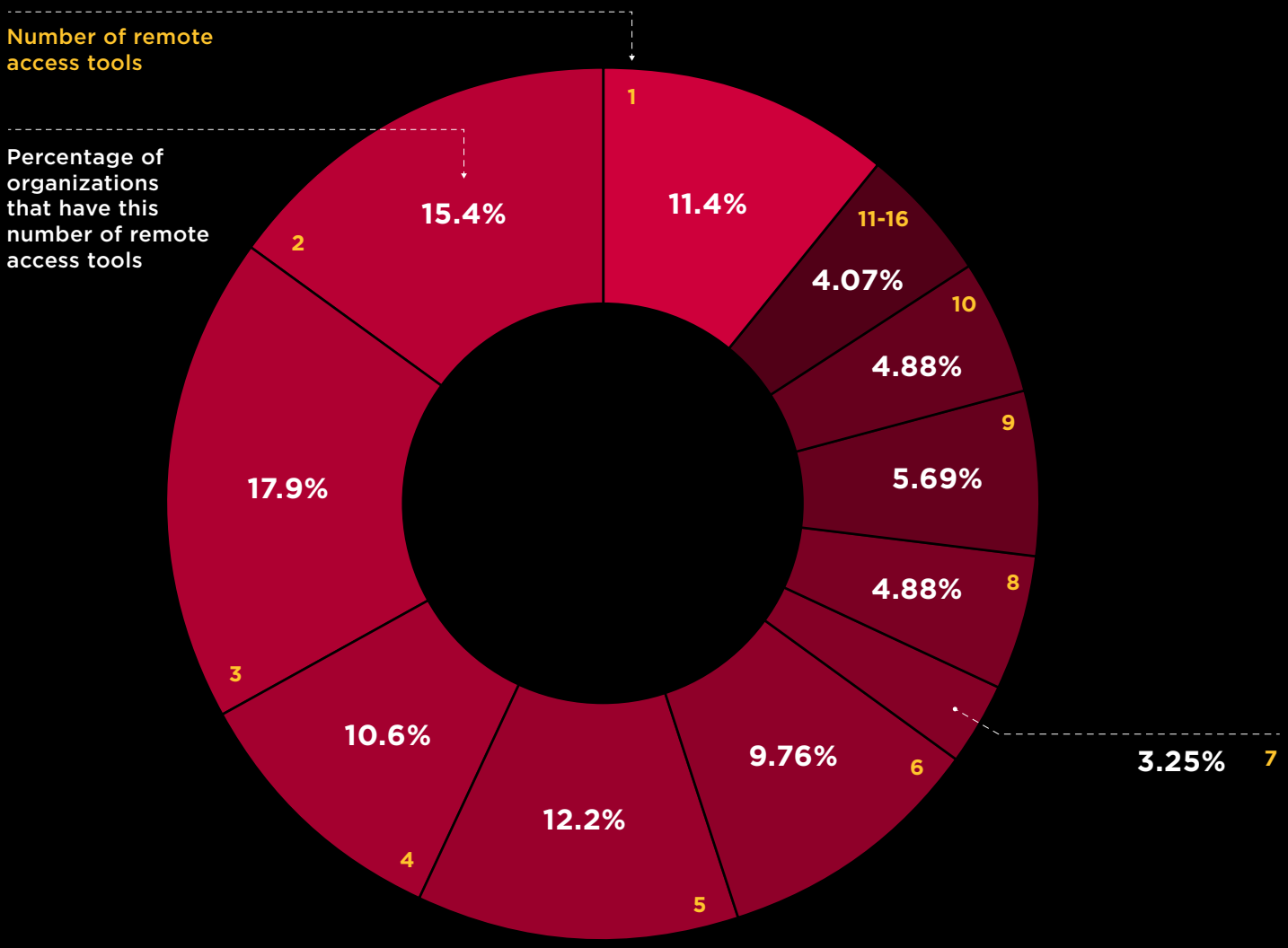
무분별한 확산이 초래하는 보안 및 운영 부담

지난 5월에 발행된 이전 Team82 조사에 따르면 기업들은 보안 모범 사례에 반하는 방식으로 운영을 지속하면서 전용 보안 액세스 솔루션을 이용하지 않고 인터넷에 OT 자산을 직접 연결하는 것으로 나타났습니다. 이러한 장치는 인터넷 스캐닝 서비스로 손쉽게 발견할 수 있고, 강력한 인증을 통해 보호되지 않으며, 악용 가능한 취약점이 있는 경우에는 공격자들이 이러한 액세스를 이용해 OT 및 엔터프라이즈 네트워크에 깊숙이 침투할 수 있습니다.

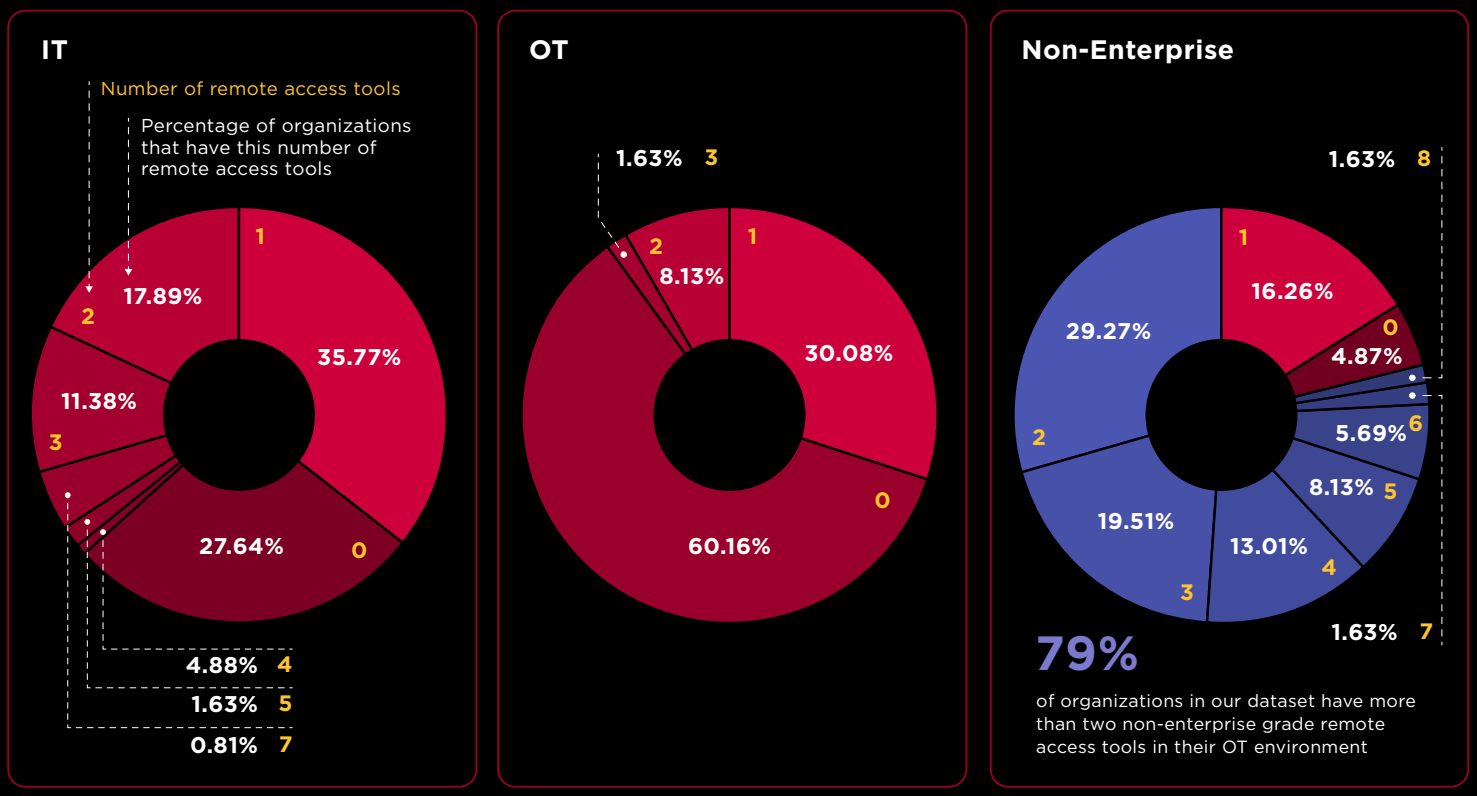
본 보고서는 이전 조사를 확장하여 원격 유지보수에서 소프트웨어 및 펌웨어 업데이트에 이르는 전 영역에서 직원, 파트너 및 공급업체에게 원격 액세스를 제공하는 데 사용되고 있는 각종 툴을 살펴봅니다.

당사 조사 결과에 따르면 기업들은 과도한 원격 액세스 요구에 대응하기 위해 다양한 수준의 보안을 제공하는 툴을 필요 이상으로 사용하고 있는 것으로 나타났습니다. 클래로티의 데이터세트에 속한 기업 중에는 단일 환경에 원격 액세스 툴을 최대 16개 배포한 곳도 있었습니다.

아래 도표를 보면 기업의 55%가 OT와 외부 환경을 연결하는 원격 액세스 툴을 4개 이상 배포한 것을 알 수 있습니다. 이에 따라 넓은 공격 표면으로 인해 관리가 복잡하고 많은 비용이 소요되는 환경을 가진 기업이 우려할 만한 수준으로 증가했습니다. 더 심각한 점은 원격 액세스 툴을 8개 이상 보유하고 있는 비율이 약 16%에 달하며, 15~16개의 툴을 관리하고 있는 경우도 있다는 사실입니다.



OT 환경에서 찾을 수 있는 원격 액세스 툴



이러한 툴 중 일부는 엔터프라이즈급 솔루션이지만 IT 원격 액세스에 상당한 수의 툴이 사용되고 있는 것은 사실입니다. 대부분의 툴은 OT 환경을 적절히 보호하는 데 필요한 세션 기록, 감사 및 역할 기반 액세스 제어 기능이 부족합니다. 또한 이 중 일부는 MFA(다단계 인증) 옵션과 같은 기본적인 보안 기능을 제공하지 않거나 관련 벤더의 서비스가 중지되어 기능 또는 보안 업데이트를 받지 못하는 상태입니다.

한편 유명한 보안 침해 사건에 노출된 툴도 있었습니다. TeamViewer의 경우, 최근 러시아 APT 위협 행위자 집단의 소행으로 추정되는 침입 공격을 공개했습니다. APT29와 CozyBear로 알려져 있는 이 집단은 탈취한 직원의 자격증명을 이용해 TeamViewer의 기업 IT 환경에 접근했습니다.

또 다른 원격 데스크톱 유지보수 솔루션인 AnyDesk는 2024년 초에 프로덕션 시스템을 손상시켰던 보안 침해 사건을 보고했습니다. 이에 예방조치로 AnyDesk는 사용자의 기기에 전송되는 업데이트 및 실행파일 서명에 사용되는 모든 사용자 비밀번호와 코드 서명 인증을 폐지했습니다.

이중적인 문제

보안

- 원격 액세스 툴의 확산이 조직의 공격 표면과 노출을 증가시킴
- 16가지 툴 전반에 걸쳐 소프트웨어 취약성과 공급망 취약점을 관리해야 함
- IT 기반의 원격 액세스 솔루션은 MFA, 감사, 세션 기록 및 OT 원격 액세스 툴 고유의 액세스 제어 기능 등 보안 기능이 대체로 부족함

운영

- 통합 툴 세트의 부재가 모니터링 및 탐지의 비효율성을 증가시키고 대응 기능을 최소화
- 중앙화된 제어 및 보안 정책 시행의 부재가 구성/배포 오류 및 악용 가능한 노출을 야기하는 일관성 없는 보안 정책을 초래
- 툴의 수가 늘어날수록 초기 툴 및 하드웨어 비용뿐만 아니라 각종 툴을 관리 및 모니터링하는 데 시간이 소요되어 총 소유비용이 크게 증가

권고 사항

원격 액세스 툴의 확산에 따른 리스크와 비효율성에 대응하기 위해서는 다음과 같은 권고 사항을 따라야 합니다.

먼저 조직의 OT 네트워크에 대한 완전한 가시성을 확보하여 OT 자산과 ICS에 액세스를 제공하는 솔루션의 개수 및 종류를 파악합니다.

엔지니어와 자산 관리자는 특히 알려진 취약점이 있거나 MFA와 같은 필수 보안 기능이 없는 OT 환경에서 보안 수준이 낮은 원격 액세스 툴의 사용을 없애거나 최소화하도록 적극 노력해야 합니다.

기업은 특히 공급망의 보안 요건에 부합하도록 조정을 실시하고 가능한 경우 타사 벤더에게 보안 표준을 요구해야 합니다.

OT 보안팀은 OT와 ICS에 연결된 원격 액세스 툴의 사용을 제어해야 하며, 통합 액세스 제어 정책에 따라 작동하는 중앙화된 관리 콘솔을 통해 이를 적절히 관리해야 합니다. 이를 통해 보안 요건을 충족하고, 가능한 경우 이러한 표준 요건을 공급망의 타사 벤더로 확장할 수 있습니다.

클래로티 소개

클래로티는 산업, 의료, 상업, 공공 부문 전반의 환경에 걸쳐 기업이 확장형 사물 인터넷(XIoT)인 사이버 물리 시스템을 보호할 수 있도록 지원합니다. 클래로티의 통합 플랫폼은 고객의 기존 인프라와 통합되어 가시성, 위험 및 취약점 관리, 위협 탐지 및 보안 원격 액세스를 위한 총체적인 제어 기능을 제공합니다. 세계 최대 투자회사와 산업 자동화 업체가 후원하는 클래로티는 전 세계 수백 개의 기업이 운영하는 수천 개의 현장에 배포되고 있습니다. 본사는 미국 뉴욕에 있으며 유럽, 아시아 태평양 및 중남미 지역에서 지사를 운영하고 있습니다. 자세한 내용은 claroty.com에서 확인하실 수 있습니다.

TEAM82 소개

사이버 물리 시스템 보호 기업 클래로티의 연구팀인 Team82는 위협 조사, OT 및 의료 프로토콜 분석, 산업, 의료 및 상용 취약점의 탐색 및 공개로 널리 알려진 수상 경력을 자랑하는 연구자 그룹입니다. Team82는 업계에서 가장 폭넓은 테스트 랩을 갖추고 CPS 사이버보안 강화를 위해 노력하고 있으며 선도적인 업계 벤더들과의 긴밀한 협력을 통해 자사 제품의 보안을 평가하고 있습니다. 2024년 5월 기준, Team82는 570개 이상의 취약점을 발견 및 공개했습니다. 클래로티 웹사이트 Claroty.com/Team82

CLAROTY

TEAM82