FAQ (자주묻는질문)

개인

1. 우리회사의 IP 중에 위험한 이력이 있다고 하는데 무엇인가요?
   A. 사용중인 IP가 감염 기록 있을 경우 내부 APT 감염 가능성 있으므로 높은 주의가 필요합니다.
   B. 실시간 악성링크 차단 장비 이용 또는 차단주소를 이용한 추가감염예방 및 감염 PC 제거가 필요합니다.

2. 그렇다면, 현재에도 위험한 건가요?
   A. 과거에 감염된 기록이 있다는 것이며, 최신 업데이트 적용된 백신을 이용한 검사를 부탁 드립니다.
   B. 감염여부를 확인할 수 있으며, 윈도우, 자바, 플래시 최신 업데이트 유지 등을 통해서 감염가능성을 줄일 수 있습니다.

3. 유출됐다고 하는 정보가 100% 믿을 수 있는 건가요?
   A. 다년간 PCDS를 통해 수집, 탐지, 분석된 악성링크 정보와 바이너리 정보를 분석하여 나온 공격자 수집서버에서 확인된 내용입니다.

4. 우리회사 IP가 알려지고 있어 평판에 문제가 있습니다. 삭제해 주세요.
   A. ip를 식별할 수 있는 정보가 없습니다.

5. 유출된 정보를 수집해서 보관하고 계신가요?
   A. 정보 수집은, 과거에 공공의 목적으로 유관 기관의 요청에 따라 수집하여 제공한 적이 있으며, 파일 원본은 전송 후 삭제 및 파기하였습니다.
      다만, 관련 데이터의 통계 목적으로 IP와 시각 정보를 보관하고 있으며, IP 정보는 개별적으로 암호화되어 보관되어 있으므로 안심하셔도 됩니다.

6. 우리회사 홈페이지는 robot.txt에 검색을 허용하지 않는데 PCDS 라고 하는 것은 로봇을 통해서 정보를 수집하나요?
   A. 사람이 웹 서핑을 하는것처럼, 프로그램을 통해서 비정상적인 악성 URL만 검색합니다.
   B. 정보를 수집하지 않으며, 비정상적인 악성 URL만 검색합니다.

7. 시간이 많이 경과된 과거의 이력은 별로 의미 없는 것이 아닌가요?
   A. 만약 오래 전에 유출된 기록이 있는 경우 참고 용도로 이용해 주시고, 최근에 발생한 경우라면 면밀히 검토하여, 회사의 보안을 강화하는
      방안으로 이용해 주십시오.
   B. 와이파이를 통해서 접속시 해당 와이파이를 통해 접속한 사용자중에서 감염 이력이

있을 수 있습니다.

8. 이 서비스를 쓰면 무엇이 좋은가요?
   A. 감염 확인: 파밍 감염이 최근 1달 이내에 발생한 경우, 해당 공인 IP를 통해 인터넷 접속한 내부 PC들에 실제 악성코드 감염이 발생 되었다는 점을 의미합니다. 내부 PC 감염을 전체적으로 염두에 두시고 대응하셔야 합니다. 감염 확인 메시지가 나타날 경우 점검 IP와 확인 기간에 대해 필요 시 C&C 및 악성코드 분석 정보를 제공하여 위험 확인에 도움 되실 수 있도록 하겠습니다.

   B. 파일 유출 확인: 내부 사용자의 인증서까지 유출이 확인된 부분이며, 명백한 감염과 정보유출이 확인된 심각한 사안입니다. 만약 기업용 인증서 유출이 있었다면, 즉시 폐기와 절차적인 대응을 시행하여야 합니다. 악성코드 추적중 확인된 인증서 파일은 모두 인증기관에 전달되어 처리하도록 하고 있습니다. 저희 쪽에서는 디렉토리명에 나타난 사용자명 혹은 사업체 명은 확인할 수 있으므로, 만약 유출 확인 메시지 확인 시에 추가 정보가 필요하시면 정보를 전달해 주세요. 감염확인과 동일한 수준에서 동기간의 악성코드 분석과 C&C 정보를 제공하도록 하겠습니다.

   C. 파밍서버: 악성코드에 의해 공인IP가 직접 파밍서버로 이용된 기록이며, 이미 공격자에 의해 권한획득이 된 상황에서 이용된 상황입니다. 침해사고 대응 절차에 따라 해당 서버에 대해 정밀한 조사와 동일 네트웍 영역의 시스템들에 대해 사고 분석을 권고 드립니다.

9. 비트코인하고 무슨 관련이 있나요?
   A. 당사는 비트코인과는 전혀 관련이 없는 웹 보안 업체이며, 빛스캔(bitscan)이라는 사명으로 각종 서비스에 "bit"라는 명칭을 사용하고 있습니다.

10. 정보 유출은 어떻게 확인했어요?
    A. 다년간 PCDS를 통해 수집, 탐지, 분석된 악성링크 정보와 바이너리 정보를 분석하여 나온 공격자 수집서버에서 확인된 내용입니다.

11. 무슨 내용인지 모르겠어요. 제 컴퓨터 좀 봐주세요.
    A. 과거 파밍 악성코드에 감염된 것으로 의심되는 IP 리스트를 보여주는 사이트 입니다.
    B. 1번 문항의 가이드를 따라서 진행해 보시기 바랍니다.

12. 감염 이력이 있다고 하네요. 제 컴퓨터 고쳐주세요.
    A. 당사에서는 개개인의 컴퓨터를 확인하는 서비스를 제공하지 않으며, 1번 문항의 가이드를 따라서 진행해 보시기 바랍니다.

13. 이웃집 와이파이 접속해서 쓰는데 감염 이력이 있다고 하네요. 제 컴퓨터가 이상이 있는 건가요?
    A. 비밀번호가 걸려있지 않은 오픈된 와이파이의 경우 보안에 취약한 경우가 많습니다.
    B. 가능한 오픈된 와이파이 사용은 자제하시기 바라며 vpn을 사용하거나, 로그인을 필요로 하는 웹사이트 접속은 피해주시기 바랍니다.
    C. 1번 문항의 가이드를 따라서 진행해 보시기 바랍니다.

기업

1. 우리회사의 IP 중에 위험한 이력이 있다고 하는데 무엇인가요?
    A. 사용중인 IP가 감염 기록 있을 경우 내부 APT 감염 가능성 있으므로 높은 주의가 필요합니다.
    B. 실시간 악성링크 차단 장비 이용 또는 차단주소를 이용한 추가감염예방 및 감염 PC 제거가 필요합니다.

2. 그렇다면, 현재에도 위험한 건가요?
    A. 과거에 감염된 기록이 있다는 것이며, 최신 업데이트 적용된 백신을 이용한 검사를 부탁 드립니다.
    B. 감염여부를 확인할 수 있으며, 윈도우,자바, 플래시 최신 업데이트 유지 등을 통해서 감염가능성을 줄일 수 있습니다.

3. 유출됐다고 하는 정보가 100% 믿을 수 있는 건가요?
    A. 다년간 PCDS를 통해 탐지된 악성링크 정보와 바이너리 정보를 분석하여 나온 공격자 수집서버에서 확인된 내용입니다.

4. 우리회사 IP가 알려지고 있어 평판에 문제가 있습니다. 삭제해 주세요.
    A. ip를 식별할 수 있는 정보가 없습니다.

5. 유출된 정보를 수집해서 보관하고 계신가요?
    A. 정보 수집은, 과거에 공공의 목적으로 유관 기관의 요청에 따라 수집하여 제공한 적이 있으며, 파일 원본은 전송 후 삭제 및 파기하였습니다.
       다만, 관련 데이터의 통계 목적으로 IP와 시각 정보를 보관하고 있으며, IP 정보는 개별적으로 암호화되어 보관되어 있으므로 안심하셔도 됩니다.

6. 우리회사 홈페이지는 robot.txt에 검색을 허용하지 않는데 PCDS 라고 하는 것은 로봇을 통해서 정보를 수집하나요?
    A. 사람이 웹 서핑을 하는 것처럼, 프로그램을 통해서 비정상적인 악성 URL만 검색합니다.
    B. 정보를 수집하지 않으며, 비정상적인 악성 URL만 검색합니다.

7. 시간이 많이 경과된 과거의 이력은 별로 의미 없는 것이 아닌가요?
   A. 만약 오래 전에 유출된 기록이 있는 경우 참고 용도로 이용해 주시고, 최근에 발생한 경우라면 면밀히 검토하여, 회사의 보안을 강화하는
      방안으로 이용해 주십시오.
   B. 와이파이를 통해서 접속 시 해당 와이파이를 통해 접속한 사용자중에서 감염 이력이 있을 수 있으며,
      공용 와이파이 사용시에는 VPN을 사용하는 것이 좋습니다.

8. 이 서비스를 쓰면 무엇이 좋은가요?
   A. 감염 확인: 파밍 감염이 최근 1달 이내에 발생한 경우, 해당 공인 IP를 통해 인터넷 접속한 내부 PC들에 실제 악성코드 감염이 발생 되었다는 점을 의미합니다. 내부 PC 감염을 전체적으로 염두에 두시고 대응하셔야 합니다. 감염 확인 메시지가 나타날 경우 점검 IP와 확인 기간에 대해 필요 시 C&C 및 악성코드 분석 정보를 제공하여 위험 확인에 도움 되실 수 있도록 하겠습니다.

   B. 파일 유출 확인: 내부 사용자의 인증서까지 유출이 확인된 부분이며, 명백한 감염과 정보유출이 확인된 심각한 사안입니다. 만약 기업용 인증서 유출이 있었다면, 즉시 폐기와 절차적인 대응을 시행하여야 합니다. 악성코드 추적 중 확인된 인증서 파일은 모두 인증기관에 전달되어 처리하도록 하고 있습니다. 저희 쪽에서는 디렉토리명에 나타난 사용자명 혹은 사업체 명은 확인할 수 있으므로, 만약 유출 확인 메시지 확인 시에 추가 정보가 필요하시면 정보를 전달해 주세요. 감염확인과 동일한 수준에서 동기간의 악성코드 분석과 C&C 정보를 제공하도록 하겠습니다.

   C. 파밍서버: 악성코드에 의해 공인IP가 직접 파밍서버로 이용된 기록이며, 이미 공격자에 의해 권한획득이 된 상황에서 이용된 상황입니다. 침해사고 대응 절차에 따라 해당 서버에 대해 정밀한 조사와 동일 네트웍 영역의 시스템들에 대해 사고 분석을 권고 드립니다.

기관

1. 이 사이트를 만든 목적이 무엇인가요?
   A. 감염여부를 알 수 없이 당하는 다수의 개인 사용자들에게 위험성을 인지할 수 있는 공익수단으로 제공하고 있습니다.
   B. 모르면 사고가 되지만, 알게 되면 관리가 가능한 위험이 되는 수단으로 제공하고 싶습니다.

2. 정보를 수집한 경로는 무엇인가요? (불법성문의 등)
   A. 준비된 동영상 통해 분석을 통해 수집되었음을 알 수 있습니다.