APT40 지침

실전에 적용된 중국 국가안보부의 공작 기술

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

목차

개요

서론

본 지침은 호주 신호국(ASD) 산하 호주 사이버 보안 센터(ACSC), 미국 사이버 보안 및 인프라 보안국(CISA), 미국 국가안보국(NSA), 미국 연방수사국(FBI), 영국 국가사이버보안센터(NCSC-UK), 캐나다 사이버 보안 센터(CCCS), 뉴질랜드 국가사이버보안센터(NCSC-NZ), 독일 연방정보국(BND) 및 헌법수호청(BfV), 대한민국 국가정보원(NIS) 및 국가정보원 산하 국가사이버안보센터, 일본 사이버보안사건대처및전략본부(NISC) 및 경찰청(NPA)의 협업으로 제작되었으며, 이들 기관은 이하 "저작 기관들"로 통칭됩니다. 이 문서는 중화인민공화국(PRC) 정부가 지원하는 사이버 그룹과 이들이 호주 네트워크에 미치는 현재의 위협에 대해 설명합니다. 이 지침은 저작 기관들 간 공유된 위협에 대한 공통 이해와 ASD 산하 ACSC의 사고 대응 조사 결과를 바탕으로 작성되었습니다.

중화인민공화국(PRC) 정부의 지원을 받는 이 사이버 조직은 과거에 호주와 미국을 포함한 여러 국가의 기관들을 대상으로 공격을 수행했습니다. 아래에 소개된 기술들은 전 세계에 있는 다른 PRC 정부 지원 사이버 공격자들도 정기적으로 사용하는 기법입니다. 따라서 저작 기관들은 이 조직과 이와 유사한 기술들이 각자의 국가 네트워크에 여전히 위협이 되고 있다고 평가하고 있습니다.

저작 기관들은 이 조직이 PRC 국가안보부(MSS)를 위한 악의적인 사이버 작전을 수행하고 있다고 판단하고 있습니다. 이 조직의 활동과 기술은 산업 보고서에서 추적되고 있는 APT40(Advanced Persistent Threat 40, 또는 'Kryptonite Panda', 'GINGHAM TYPHOON', 'Leviathan', 'Bronze Mohawk'이라고도 불림)으로 알려진 그룹과 중첩됩니다. 이 그룹은 PRC 하이난성 하이커우시에 소재하고 있으며 PRC MSS 산하 하이난 국가안보부로부터 임무 지시를 받고 있는 것으로 이전에 보고되었습니다.[2] 다음 지침은 두 개의 피해 네트워크에 대해 공격자가 사용하는 기술에 대한 중요한 사례 연구들 샘플을 제공합니다. 이들 사례 연구는 사이버 보안 실무자가 자사 네트워크에 대한 APT40 침입을 식별, 예방 및 해결하는 데 중요한 역할을 합니다. 선택된 사례 연구는 해당 위협 행위자 또는 타인이 악용할 위험을 줄이기 위해 적절한 시정 조치를 이미 취한 사례들입니다. 따라서 이 사례 연구들은 이미 시간이 좀 지난 사례들이며 이는 해당 기관들이 복구할 충분한 시간을 갖도록 하기 위함이었습니다.

활동 요약

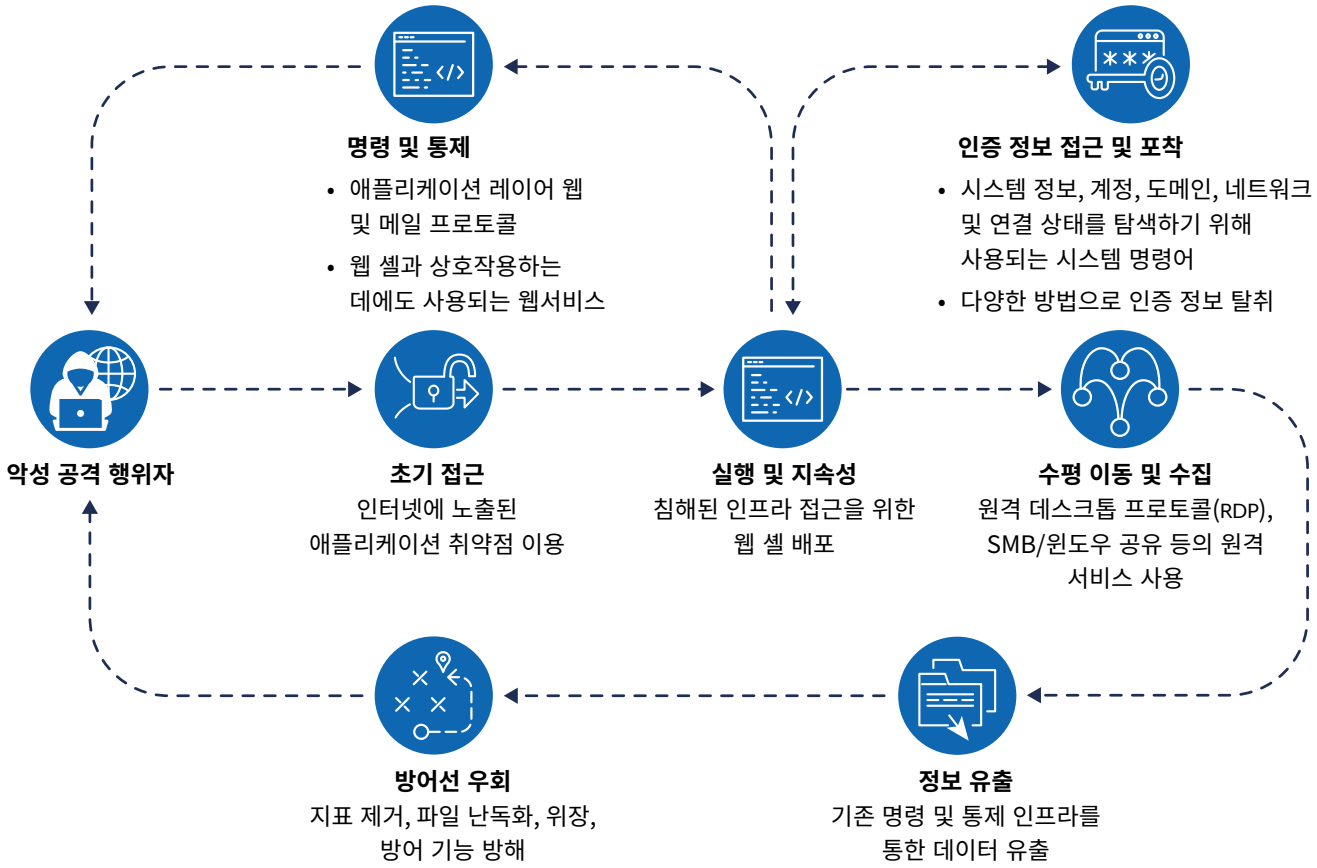
APT40은 호주의 네트워크뿐만 아니라 이 지역의 정부 및 민간 부문 네트워크를 반복적으로 공격해 왔으며, 그 위협은 현재도 지속되고 있습니다. 본 지침에 설명된 공작 기술은 호주 네트워크를 대상으로 한 활동에서 정기적으로 발견되고 있습니다.

특히, APT40은 새로운 취약점의 개념 증명(PoC)을 빠르게 변형 및 개작할 능력을 갖추고 있으며, 그들은 이를 관련 취약점을 가진 인프라가 존재하는 표적 네트워크를 즉시 공격하는 데 활용할 수 있습니다. APT40은 저작 기관 국가들의 네트워크를 포함해 관심 있는 네트워크를 대상으로 정기적으로 정찰 활동을 수행하며, 늘 표적 대상을 침해할 수 있는 기회를 탐색하고 있습니다. 이러한 정기적인 정찰 활동을 통해 APT40은 관심 네트워크 내의 취약한 기기, 수명이 다했거나 더 이상 유지관리되지 않는 기기를 식별하고, 해당 취약점에 대한 공격을 신속하게 실시할 수 있는 위치에 있습니다. APT40은 2017년까지 거슬러 올라가는 오래된 취약점들을 여전히 성공적으로 악용하고 있습니다.

APT40은 Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) 및 Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473)와 같이 널리 사용되는 소프트웨어의 새로 공개된 취약점을 빠르게 악용하고 있습니다. ASD 산하 ACSC 및 저작 기관들은 공개적으로 발표된 후 몇 시간 또는 며칠 내에 이 그룹이 계속해서 새로운 주요 취약점에 대한 POC를 사용할 것으로 예상하고 있습니다.

2 미국 법무부. 2021 감염병 연구 등 지적 재산권 및 기밀 비즈니스 정보를 표적으로 삼아 전세계 컴퓨터 침입 활동을 벌인 혐의로 국가안보부 소속 중국인 4명 기소.

이미지 1: APT40 활동을 위한 전략, 기술 및 절차(TTP) 플로차트



이 그룹은 일반적으로 피싱 활동과 같이 사용자 상호작용이 필요한 기술보다, 취약한 공개 인프라를 악용하는 것을 선호하는 것으로 보이며, 이후 다양한 후속 활동이 가능하도록 유효한 인증 정보를 확보하는 데 중점을 두고 있습니다. APT40은 특히 침해 초기 단계에서, 지속성을 유지하기 위해 웹 셸(web shell)(T1505.003)을 정기적으로 사용합니다. 초기에 접근권을 획득한 이후, APT40은 대개 피해자의 환경에 대한 지속적인 접근을 확보하는 데 주력합니다. 단, 지속적 접근 확보는 침해 초기 단계에 이루어지기 때문에, 침해의 규모나 후속 침해 활동 여부와 관계없이 대부분의 침해 사례에서 관찰될 가능성이 높습니다.

핵심 공작 기술

APT40이 과거에 침해된 호주 웹사이트를 명령 및 통제(C2) 호스트로 활용했었지만, 지금은 이 기술을 더욱 발전시켰습니다(T1594).

현재 APT40은 세계적인 추세에 따라, 호주 내 활동에도 소규모 사무실/가정용(SOHO) 기기를 포함한 침해된 기기를 운영 인프라 및 최종 연결 은닉 지점(last-hop redirector)으로 사용하고 있습니다(T1584.008). 이를 통해 저작 기관들이 해당 그룹의 움직임을 더 효과적으로 식별하고 추적하게 되었습니다.

이러한 SOHO 기기의 대부분은 수명이 다했거나 보안 패치가 적용되지 않은 상태로, N-day 악용을 위한 소프트 타겟이 됩니다. 이 SOHO 기기들이 침해되면, 공격자는 이를 통해 합법적인 트래픽으로 위장된 공격을 실행하며, 네트워크를 방어하는 이들의 보호 활동을 어렵게 만듭니다(T1001.003).

이러한 기법은 APT40뿐만 아니라, 전 세계적으로 활동 중인 다른 PRC 정부 지원 사이버 행위자들도 정기적으로 사용하고 있으며, 저작 기관들은 이를 공통된 위협으로 간주하고 있습니다. 더 자세한 정보는 다음의 공동 제작 지침을 참조하세요: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices(중화인민공화국 국가 지원 사이버 공격자들, 네트워크 제공업체 및 기기 악용) 및 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (중화인민공화국 국가 지원 사이버 공격자들, 미국 주요 인프라를 침해하고 지속적인 접근 유지).

APT40은 때때로 구매하거나 임대한 인프라를 피해자와 연결되는 C2 인프라로 사용하기도 하지만, 이와 같은 공작 기술은 상대적으로 감소하는 추세입니다.

툴

ASD 산하 ACSC는 아래 설명된 조사 기간에 식별한 악성 파일들 일부를 공유하고 있습니다. 이들 파일은 VirusTotal에 업로드 되었으며 이는 광범위한 네티워크 방어 및 사이버 보안 공동체들이 자사가 어떤 위협에 대비해야 하는지를 보다 잘 이해할 수 있도록 하기 위함입니다.

사례 연구

ASD 산하 ACSC는 위협 행위자들이 어떤 방식으로 자신들의 도구와 공작 기술을 사용하는지 알리기 위해 두 개의 익명 처리된 조사 보고서를 공유합니다.

MD5	파일명	추가 정보
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

사례 연구 1

이 보고서는 대중적인 정보 공유 목적으로 익명 처리되었습니다. 피해 조직은 이하 '조직'으로 언급됩니다. 피해자의 신원을 보호하고 ASD 산하 ACSC의 사고 대응책을 기밀로 유지하기 위해 일부 세부 내용은 제거되었습니다.

개요서

이 보고서는 2022년 7월부터 9월까지 조직의 네트워크가 성공적으로 침해된 사건에 대해 ASD 산하 ACSC가 수행한 조사 결과를 설명합니다. 이 조사 보고서는 관찰된 악의적 공격 활동을 요약하고, 대응 및 복구 권고사항을 제시하기 위해 조직에 제공되었습니다. 조사 결과에 따르면, 침해 활동은 APT40 그룹에 의해 수행되었습니다.

8월 중순, ASD 산하 ACSC는 8월 말 해당 그룹이 사용한 침해된 가능성이 있는 기기를 통해 조직의 네트워크 내 악의적 활동이 발생한 사실을 조직에 통보했습니다. 조직의 동의를 받아, ASD의 ACSC는 조직 네트워크 내 영향을 받았을 가능성이 있는 호스트에 호스트 기반 센서를 배포했습니다. 이 센서들을 통해 ASD 산하 ACSC의 사고 대응 분석가들이 정밀한 디지털 포렌식 조사를 수행할 수 있었습니다. 사용 가능한 센서 데이터를 활용해 ASD 산하 ACSC 분석가들은 그 그룹의 활동을 성공적으로 추적한 후 관찰된 사건들을 상세 타임라인으로 진열했습니다.

ASD 산하 ACSC가 관찰한 7월부터 8월까지의 주요 악의적 행위는 다음과 같습니다:

- 네트워크 지도를 작성할 수 있도록 하는 호스트 열거;
- 네트워크에 초기 접근을 제공하고 명령 실행 능력을 확보하는 웹 셸 사용; 그리고
- 악의적인 목적으로 사용된 기타 툴의 배포.

조사 과정에서 대량의 민감 데이터가 접근되었음을 뒷받침하는 증거와 공격 행위자들이 네트워크 내에서 수평적 이동을 한 것이 발견되었습니다. (T1021.002) 침해의 상당 부분은 그 그룹이 네트워크에 여러 접근 경로를 확보한 점, 네트워크가 평면적 구조였던 점, 임의로 파일 업로드가 가능한 취약한 내부 개발 소프트웨어를 사용한 점 등으로 인해 촉진되었습니다. 유출된 데이터에는 공격 그룹이 로그인에 사용할 수 있는 관리 권한이 있는 인증 정보와 첫 접근 경로가 차단되더라도 무단 접근이 다시 가능하도록 하는 네트워크 정보가 포함되어 있었습니다. 초기 침해된 장비 외에는 추가적인 악성 툴이 발견되지는 않았으나, 앞서 설명했듯이 이 그룹이 관리 권한이 있는 유효 인증 정보를 확보함으로써 추가 툴 사용의 필요성이 상쇄되었습니다. 조사 결과는 이 조직이 공개적으로 알려진 취약점에 우연히 피해를 입은 것이 아니라 APT40 의
의도적인 표적이 되었을 가능성이 높음을 시사합니다.

조사 결과

2022년 8월 중순, ASD 산하 ACSC는 국가 지원 사이버 그룹과 연계된 것으로 확인된 악성 IP 주소가 최소 7월부터 8월 사이 조직의 컴퓨터 네트워크에 접근한 사실을 조직에 통보했습니다. 침해된 기기는 소규모 사업체 또는 개인 사용자의 것으로 추정됩니다.

8월 말, ASD 산하 ACSC는 침해된 것으로 의심되는 조직 네트워크 내 호스트에 호스트 기반 에이전트를 배포했습니다.

일부 조사에 도움이 될 수 있는 디지털 흔적은 로깅 설정이나 네트워크 설계로 인해 확보되지 못했습니다. 그럼에도 불구하고, 조직은 모든 가능한 데이터를 제공하는 데 적극적으로 협조했고, 덕분에 ASD 산하 ACSC 사고 대응 팀은 정밀한 분석을 수행하고 네트워크 내에서 발생한 것으로 추정되는 APT40 활동에 대한 이해를 구체화할 수 있었습니다.

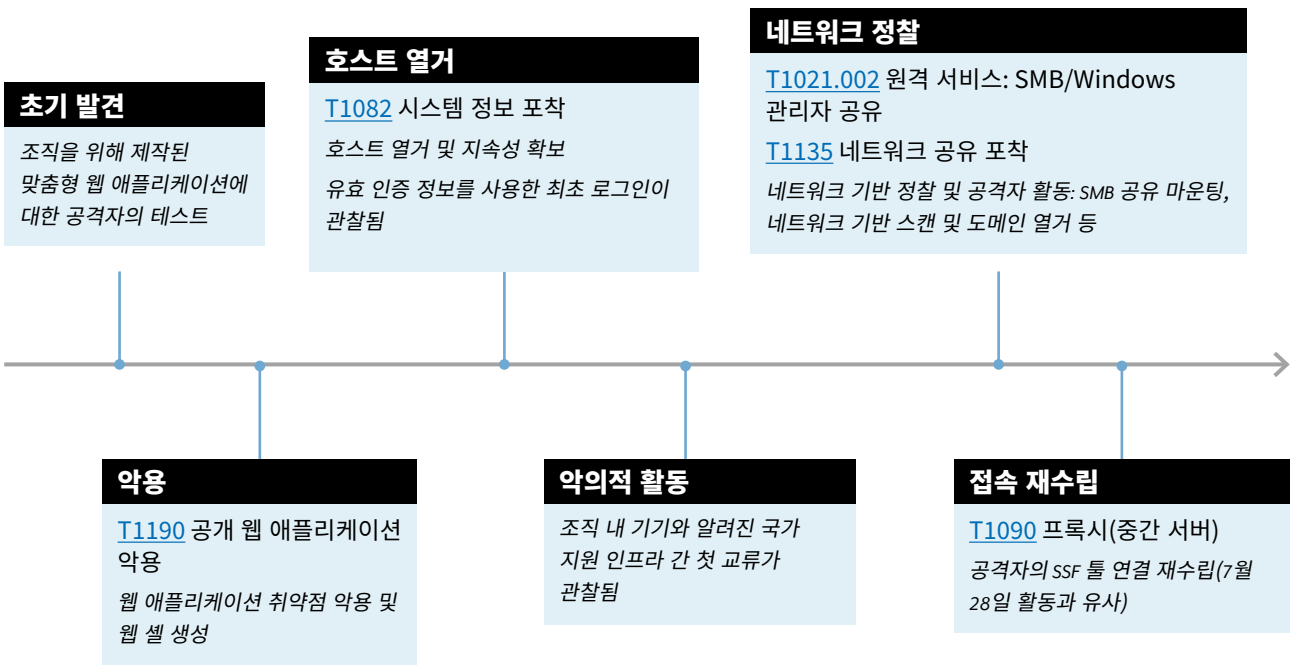
ASD 산하 ACSC와의 면담 후 9월, 조직은 최초 알림에서 파악된 IP 주소를 블랙리스트하기로 결정했습니다. 조직은 10월 대응책을 개시했습니다.

세부 내용

7월 초, 공격자들은 `<webapp>2-ext`에 운영되는 맞춤 웹 애플리케이션(T1190)을 검사 및 악용할 수 있었고, 이를 통해 네트워크 비무장 지대(DMZ)에 대한 발판을 확보할 수 있었습니다. 이는 네트워크는 물론 확인되는 모든 도메인을 나열하는 데 활용되었습니다. 이 그룹은 침해된 인증 정보(T1078.002)를 사용해 Active Directory(T1018)를 검사했으며 DMZ 내 여러 시스템에서 파일 공유를 마운트해(T1039) 데이터를 유출시켰습니다. 공격자는 서버에서(T1558.003) 유효 네트워크 인증 정보를 획득하기 위해 커버로스팅(Kerberoasting) 공격을 수행했습니다. 그룹은 DMZ나 내부 네트워크에서 추가적인 접근 지점을 확보하지 못한 것으로 관찰되었습니다.

시각적 타임라인

아래 타임라인은 악의적 공격 행위자가 조직의 네트워크에 대해 수행한 활동의 주요 단계를 포괄적으로 설명합니다.



세분화된 타임라인

7월: 공격자들은 조직을 위해 제작된 맞춤형 웹 애플리케이션(T1190)(이하 '웹 애플리케이션' 또는 '*webapp*') 1면에 전송 계층 보안(TLS) 연결(T1102)을 통해 초기 연결점을 확립합니다. 주목할 만한 다른 활동은 발견되지 않았습니다.

7월: 공격자들은 웹 애플리케이션의 웹사이트를 열거하기 시작하며, 추가 조사를 위해 엔드포인트를 탐색합니다[2].

7월: 공격자들은 특정 엔드포이트를 악용하기 위해 집중 시도합니다.

7월: 공격자들은 아마도 다른 페이지에 설치된 웹 셸을 통해 성공적으로 웹 서버에 포스팅을 합니다. 동일 공격자가 사용했을 가능성이 높은 두 번째 IP가 같은 URL에 포스팅을 하기 시작합니다. 공격자들은 여러 개의 웹 셸을 생성하고 테스트합니다.

정확한 악용 방식은 확인되지 않았지만, 특정 엔드포인트가 *<webapp>2*-ext 상에 파일을 생성하기 위해 표적이 된 점은 확실히 확인됩니다.

ASD 산하 ACSC는 두 IP 주소의 접속 시점이 몇 분 간격으로 발생하고 동일한 목표를 가졌다는 점에서 같은 공격 작업의 일부로 판단하고 있습니다.

7월: 그룹은 계속해서 호스트 열거를 수행하며, 권한 상승 기회를 엿보고 다른 웹 셸을 배포합니다. 공격자들은 탈취한 인증정보를 이용해 *<firstname.surname>@<organisation domain>* 계정으로 웹 애플리케이션에 로그인합니다.

공격자들의 활동은 *<webapp>2*-ext에서 권한 상승을 성공적으로 이루지 못한 것으로 확인됩니다. 그 대신 공격자들은 네트워크 기반 활동으로 전환합니다.

7월: 공격자는 내부 접근 가능한 바이너리에 아마 하드코딩되어 있었을 서비스 계정의 침해된 인증 정보[3]를 테스트합니다.

7월: 공격자들은 오픈 소스 툴인 Secure Socket Funnelling을 배포해 이를 악성 인프라에 연결하는 데 사용합니다. 이 연결은 공격자의 공격 머신에서 조직 내부 네트워크로 트래픽을 잇는 데 사용됩니다. 그리고 서비스 계정의 인증 정보를 사용하려 시도하는 과정에서 이벤트 로그에 머신 이름들이 노출됩니다.

8월: 공격자들은 서비스 계정을 사용한 접속 지점 확보에 실패하는 등 제한적인 활동을 수행한 것으로 확인됩니다.

8월: 공격자들은 광범위한 네트워크 및 Active Directory 열거 작업을 수행합니다. 이후 다른 탈취된 계정을 사용해 DMZ 내 Windows 머신에서 공유 마운트를 시도[4]하면서 성공적으로 데이터를 유출해 냅니다.

이는 DMZ 내 마운트 가능한 머신에서 탈취한 인증 정보를 악용한 사례로 보입니다. 방화벽은 공격자가 유사한 활동으로 내부 네트워크를 표적 삼는 것을 차단합니다.

8월 – 9월: SSF 도구가 악성 IP와 재연결하는 데 성공합니다. 접근이 차단될 때까지 그룹의 추가적인 활동 수행은 관찰되지 않았습니다.

9월: 조직은 방화벽에서 악성 IP를 차단 목록(denylist)에 등록해 차단합니다.

2 이 내용에서 엔드포인트는 웹 애플리케이션의 한 기능입니다.

3 서비스 계정은 개인 사용자에 연동되어 있는 것이 아니라 서비스에 연동되어 있습니다. Microsoft 기업 도메인에는 여러 유형의 계정이 있습니다.

4 공유 마운트는 파일 시스템 구조에 있는 파일들을 특정 사용자 또는 사용자 그룹에게 공유하는 절차입니다.

공격자 전략 및 기술

MITRE ATT&CK 프레임워크는 사이버 공간에서 악의적 공격자들이 사용하는 전술과 기법을 문서화한 모음집입니다. 이 프레임워크는 미국 비영리기관인 MITRE Corporation에서 수립했으며, 악의적 공격자들의 활동에 대한 세계 공통 언어입니다.

ASD 산하 ACSC는 다음의 기법과 전술이 공격자의 악의적 활동과 관련이 있다고 평가합니다.

정찰

T1594 – 피해자 소유 웹사이트 검색

공격자는 네트워크 접근 기회를 찾기 위해 맞춤형 웹 애플리케이션의 웹사이트를 열거했습니다.

최초 접근

T1190 – 공개 애플리케이션 악용(맞춤 웹 애플리케이션 악용 관련)

T1078.002 – 유효 계정: 도메인 계정(도난 인증 정보를 이용한 로그인 관련)

공격자는 인터넷에 노출된 맞춤형 웹 애플리케이션을 악용해 초기 접근 지점을 확보했습니다. 이후 공격자는 탈취한 인증 정보를 사용해 네트워크에 대한 접근권을 확대할 수 있었습니다.

실행

T1059 – 명령 및 스크립트 통역(웹 셸을 통한 명령 실행 관련)

T1072 – 소프트웨어 배포 툴(IP 연결을 위해 오픈 소스 도구인 Secure Socket Funnelling(SSF)를 사용하는 공격자 관련)

지속성

T1505.003 – 서버 소프트웨어 구성 요소: 웹 셸(접근권 확보를 위한 웹 셸 및 SSF 사용 관련)

인증 정보 접근

T1552.001 – 암호 저장소 내 인증 정보(건물 관리 시스템(BMS)에 연관된 비밀번호 파일 관련)

T1558.003 – Steal or Forge Kerberos Tickets: 커버로스팅(네트워크 인증 정보를 취득하기 위한 공격 관련)

시스템 내 수평적 이동

T1021.002 – 원격 서비스: SMB 공유(여러 기기에서 SMB 공유를 마운트하는 공격자 관련)

수집

T1213 – 정보 저장소의 데이터(BMS 서버에서 찾는 매뉴얼/문서 관련)

정보 유출

T1041 – C2 채널을 통한 유출(Active Directory 및 공유 마운팅을 통한 공격자의 데이터 유출 관련)

사례 연구2

이 보고서는 더 광범위한 배포를 목적으로 익명 처리되었습니다. 피해 조직은 이하 '조직'으로 언급됩니다. 피해자의 신원을 보호하고 ASD 산하 ACSC의 사고 대응책을 기밀로 유지하기 위해 일부 특정 내용은 제거되었습니다.

개요서

이 보고서는 2022년 4월에 조직의 네트워크가 성공적으로 침해된 사건에 대해 ASD 산하 ACSC가 수행한 조사 결과를 설명합니다. 이 조사 보고서는 관찰된 악의적 공격 활동을 요약하고, 대응 및 복구 권고사항을 제시하기 위해 조직에 제공되었습니다. 조사 결과에 따르면, 침해 활동은 APT40 그룹에 의해 수행되었습니다.

2022년 5월, ASD 산하 ACSC는 2022년 4월부터 조직의 컴퓨터 네트워크에 영향을 미칠 것으로 의심되는 악의적 공격에 대해 조직에 통보했습니다. 이후 조직은 인터넷에 노출된 서버(조직의 기업용 원격 접속 솔루션 로그인 포털을 제공하는 서버)에서 악성 소프트웨어를 발견했다고 ASD의 ACSC에 알렸습니다. 이 서버는 원격 접속 로그인 및 신원 관리 제품을 사용했으며 본 보고서에서 '침해된 장치'로 언급됩니다. 본 보고서는 ASD 산하 ACSC가 수행한 조사 결과와 조직에 제공된 복구 권고사항을 상세히 설명합니다.

증거에 따르면 조직의 네트워크 일부가 최소 2022년 4월부터 조직의 원격 접속 로그인 포털을 통해 악의적 사이버 공격자에 의해 침해된 것으로 확인되었습니다. 이 서버는 여러 행위자에 의해 침해되었을 가능성이 있으며, 침해 시점에 널리 알려진 원격 코드 실행(RCE) 취약점으로 인해 피해를 봤을 확률이 높습니다.

ASD 산하 ACSC가 관찰한 주요 공격자 활동의 예는 다음과 같습니다:

- 공격자가 네트워크에 대한 전반적인 이해를 할 수 있게 하는 호스트 열거;
- 공격자가 네트워크에 대해 초기 발판을 확보하고 명령을 실행할 수 있게 하는 인터넷에 노출된 애플리케이션의 악용 및 웹 셸 사용;
- 공격자의 권한 상승을 가능케 하는 소프트웨어 취약점 악용; 그리고
- 시스템 내 수평적 이동을 가능하게 하는 인증 정보 수집.

ASD 산하 ACSC는 2022년 4월 침해된 장치에서 수백 개의 고유 사용자 이름과 비밀번호 페어는 물론, 원격 접속 세션과 관련된 다량의 다중인증 코드와 디지털 흔적이 악성 공격자에 의해 유출된 사실을 발견했습니다. 조직이 검토한 결과, 해당 비밀번호들은 유효한 것으로 확인되었습니다. ASD 산하 ACSC는 공격자가 이러한 기술적 디지털 흔적을 수집해 정상 사용자로서 원격 로그인 세션을 하이재킹하거나 생성하고, 유효 사용자 계정을 이용해 조직 내부 기업용 네트워크에 접근했을 수도 있다고 판단합니다.

조사 결과

조사 요약

ASD 산하 ACSC는 공격자가 조직 직원들의 원격 접속 세션이 가능한 장치(들)를 침해하고, 이 취약점을 악용하는 추가 활동을 수행하려고 했다고 판단했습니다. 이들 장치는 세 대의 로드 밸런싱된 호스트로 구성되어 있었으며 최초 침해 증거도 여기에서 감지되었습니다. 조직은 최초 침해 이후 곧바로 세 대 중 두 대의 로드 밸런싱된 호스트를 즉시 운영 중단시켰습니다. 그 결과로 모든 후속 활동은 하나의 호스트에서 이뤄졌습니다. 침해된 기기와 관련된 다른 서버들 또한 유사한 방식으로 로드가 밸런싱되어 있었습니다. 더 쉬운 이해를 위해 본 보고서에서는 침해된 장치가 대부분 '단일 장치'로 언급됩니다.

공격자는 대중에 공개된 취약점을 이용해 2022년 4월부터 침해된 장치에 웹 셸을 배포한 것으로 추정됩니다. 그룹의 위협 공격자들은 장치에 대해 상향된 권한을 획득한 것으로 판단됩니다. ASD 산하 ACSC는 로그 기록의 부재로 인해 활동의 전체 범위를 판단할 수는 없었습니다. 그러나 기기에 남은 증거에 의하면, 공격자는 다음을 성공적으로 수행했습니다:

- 몇 백개의 유효 사용자 이름과 비밀번호 페어 수집; 그리고
- 악의적 공격자가 유효 사용자로서 가상 데스크톱 인프라(virtual desktop infrastructure, VDI) 세션에 접근할 수 있도록 도움이 되었을 수도 있는 디지털 흔적의 수집.

ASD 산하 ACSC는 공격자가 조직의 네트워크를 더 깊게 침해하려는 의도가 있었을 것이라고 판단합니다. 공격자가 유출한 디지털 흔적은 해당 공격자가 정상 사용자(관리자 포함), 그리고 어쩌면 자신들이 선택한 사용자의 권한으로 가상 데스크톱 세션을 하이재킹하거나 개시할 수 있도록 했을 가능성이 있습니다. 공격자는 이 접근 벡터를 이용해 조직의 서비스를 추가로 침해하고, 지속적 접근을 확보하고, 기타 목적을 달성했을 가능성도 있습니다.

해당 호스팅 제공업체가 관리하는 환경 내의 다른 조직의 장치들에서는 침해의 증거가 발견되지 않았습니다.

접근

침해된 장치가 탑재된 호스트는 VDI 세션에 연결하는 사용자에게 Active Directory 및 웹서버를 통한 인증 기능을 제공했습니다. (T1021.001).

위치	침해된 장치 호스트명 (로드 밸런싱된 호스트)
데이터센터 1	HOST1, HOST2, HOST3

이 장치 인프라는 또한 사용자가 장치에서 인증 토큰을 생성 및 다운로드한 경우, VDI로의 터널을 제공하는 액세스 게이트웨이 호스트를 포함하고 있었습니다.

이들 호스트 중 어느 것도 침해된 정황이 발견되지 않았습니다. 그러나 액세스 게이트웨이 호스트의 로그에서는 알려진 악성 IP 주소들과의 많은 교류가 확인되었습니다. 이는 해당 호스트에서 발생한 활동 또는 악의적 공격자 인프라와의 네트워크 연결이 이 호스트에 도달하였음을 시사할 가능성이 높습니다. 수집된 증거로 해당 활동의 성격은 확인할 수 없었지만, 이 그룹이 조직의 네트워크 내에서 수평적 이동을 시도했음을 알 수 있었습니다. (TA0008)

내부 호스트

ASD 산하 ACSC는 조직 내부 네트워크 세그먼트에서 수집된 제한된 데이터를 조사했습니다. 조직 내부 네트워크 세그먼트에 영향을 미친 것으로 확인된 악의적 활동 시도 및 성공 사례에는 공격자의 VDI 관련 디지털 흔적 접근, 내부 SQL 서버의 데이터 스크래핑(scraping) (T1505.001), 그리고 액세스 게이트웨이 장치 내에서 알려진 악성 IP 주소에서 시작된 설명되지 않은 트래픽 (TA0011) 등이 있었습니다.

그룹은 침해된 장치에 대한 접근을 통해 실제 사용자 이름, 비밀번호(T1003), 그리고 MFA 토큰 값(T1111)을 수집했습니다. 이 그룹은 가상 데스크톱 로그인 세션 개시에 사용되는 인증 정보인 JSON Web Token(JWT) (T1528)도 수집했습니다. 공격자는 이를 통해 가상 데스크톱 세션을 개시하거나 하이재킹하고(T1563.002), 유효 사용자로서 조직 내부 네트워크 세그먼트에 접근했을 가능성이 있습니다(T1078).

또한 행위자는 침해된 장치에 대한 접근을 활용해 조직 내부 네트워크에 위치한 SQL 서버를 스크래핑(scraping)했습니다(T1505.001). 공격자가 이 데이터에 대한 접근권이 있었을 확률이 높습니다.

알려진 악성 IP 주소가 이 장치를 통해 또는 이 장치로 네트워크 트래픽을 발생시켰던 것이 액세스 게이트웨이 장치 증거를 통해 확인됐습니다. 위에서 설명했듯이 이는 악의적인 사이버 공격자가 이 장치에 영향을 미치거나 이를 활용했음을 의미할 수도 있으며, 그 목적이 내부 네트워크로 침투하기 위한 것일 가능성이 있습니다.

조사 타임라인

아래 리스트는 조사로 발견된 주요 활동을 설명하는 타임라인입니다.

시간	사건
2022년 4월	알려진 악성 IP 주소가 액세스 게이트웨이 호스트인 HOST7과 접속했으나 구체적인 접속 내용은 확인되지 못했습니다.
2022년 4월	모든 호스트(HOST1, HOST2 및 HOST3)가 악의적 공격자(들)에 의해 침해되었고, 그들은 이들 호스트에 웹 셸을 배치했습니다. HOST2에는 로그 파일이 생성 또는 개정되었습니다. 해당 파일에는 인증 정보가 포함되어 있었고, 악의적 공격자가 이를 취득했을 가능성이 높습니다. HOST1과 HOST3에 /etc/security/opasswd 및 /etc/shadow 파일이 변경되었고 이는 비밀번호가 수정되었음을 의미합니다. HOST1에서 찾은 증거에 의하면 사용자 'sshuser'의 비밀번호가 수정되었음을 추정할 수 있습니다.
2022년 4월	조직은 HOST2를 운영 중단했습니다. HOST1과 HOST3에 추가 웹 셸(T1505.003)이 생성되었습니다. HOST1은 HOST3으로부터 SSH 무차별 대입 공격을 받았습니다. HOST3에서 하나의 로그 파일(T1070)이 개정되었습니다. 해당 파일에는 인증 정보(T1078)가 포함되어 있었고, 악의적 공격자가 이를 취득했을 가능성이 높습니다. JWT가 캡처되어(T1528) HOST3에 파일로 저장되었습니다. 조직은 HOST2를 운영 중단했습니다. 이 시점 이후의 모든 활동은 HOST1에서 이뤄졌습니다.
2022년 4월	HOST1에 추가 웹 셸이 생성되었습니다(T1505.003). JWT가 캡처되어 HOST1에 파일로 저장되었습니다.
2022년 4월	HOST1에 추가 웹 셸이 생성되었고(T1505.003), 알려진 악성 IP 주소가 호스트와 교류했습니다(TA0011). 알려진 악성 IP 주소가 액세스 게이트웨이 호스트인 HOST7과 교류했습니다.
2022년 5월	알려진 악성 IP 주소가 액세스 게이트웨이 호스트인 HOST7과 교류했습니다(TA0011). HOST1 로그에서 특정 사용자의 인증 이벤트가 어떤 알려진 악성 IP 주소와 연결되었습니다. 해당 호스트에 추가 웹 셸이 생성되었습니다(T1505.003).
2022년 5월	HOST1에 있는 스크립트가 공격자에 의해 개정되었습니다(T1543). 해당 스크립트는 내부 SQL 서버에서 데이터를 스크래핑할 수도 있는 기능을 갖추고 있었습니다.
2022년 5월	HOST1에 있는 다른 로그 파일이 마지막으로 개정되었습니다(T1070). 해당 파일에는 조직 네트워크에 대한 사용자 이름과 비밀번호 페어들이 포함되어 있었고 이 정보는 유효한 것으로 판단됩니다(T1078).
2022년 5월	추가 로그 파일이 마지막으로 개정되었습니다(T1070). 해당 파일에는 HOST1에서 수집된 JWT가 포함되어 있었습니다.
2022년 5월	HOST1에 추가 웹 셸이 생성되었습니다(T1505.003). 이 날, 조직은 2022년 4월에 생성된 웹 셸을 발견한 사실을 ASD 산하 ACSC에 보고했습니다.
2022년 5월	HOST1에 여러 개의 스크립트가 생성되었고 이 중 하나의 명칭은 'Log4jHotPatch.jar'였습니다.
2022년 5월	'iptables-save' 명령어가 액세스 게이트 호스트에 2 개의 오픈 포트를 추가하기 위해 사용되었습니다. 그 포트는 각각 9998과 9999였습니다(T1572).

공격자 전략 및 기술

아래 기술된 내용은 조사 과정에서 파악된 여러 전략 및 기술입니다.

최초 접근

T1190 공개된 애플리케이션 취약점 악용

이 그룹은 원격 액세스 로그인 및 ID 관리 제품의 RCE, 권한 상승 및 인증 우회 취약점을 악용해 네트워크에 대한 초기 접근권을 얻었을 가능성이 높습니다.

해당 초기 접근 방식이 가장 가능성이 높은 것으로 판단되는 이유는 다음과 같습니다:

- 당시 서버는 이러한 CVE에 취약했던 점;
- 알려진 공격자 인프라가 이러한 취약점을 악용하려 시도한 정황이 있었던 점; 그리고
- 악용을 시도한지 얼마 지나지 않아 첫 내부 악의성 활동이 파악된 점.

실행

T1059.004 명령 및 스크립트 통역: 유닉스 셸

이 그룹은 위의 취약점을 성공적으로 악용해 침해된 기기에서 사용 가능한 유닉스 셸을 통해 명령을 실행할 수 있었을 가능성이 있습니다. 공격자들이 실행한 명령에 대한 완전한 정보는 기기에 기록되지 않았기 때문에 제공될 수 없습니다.

지속성

T1505.003 서버 소프트웨어 구성 요소: 웹 셸

공격자들은 침해된 기기에 여러 웹 셸을 배포했습니다. 여러 명의 다른 공격자가 웹 셸을 배포했으나 이들 중 소수의 공격자만 해당 웹 셸을 사용해 악의적 활동을 수행했을 가능성도 있습니다. 웹 셸은 침해된 기기에서 공격자가 임의의 명령을 실행할 수 있도록 했을 것입니다.

권한 상승

T1068 권한 상승 악용

수집된 증거로는 공격자들이 어느 수준의 권한을 취득했는지 파악할 수 없습니다. 하지만 그들은 웹 셸을 사용해 침해된 기기의 웹서버에 상응하는 수준의 권한을 취득했을 것으로 짐작됩니다. 침해된 기기가 갖고 있는 것으로 추정되는 취약점으로 인해 공격자들은 루트 권한을 취득할 수 있었을 것입니다.

인증 정보 접근

T1056.003 인풋 캡처: 웹 포털 캡처

침해된 기기에서 나온 증거에 따르면 공격자는 유효한 것으로 추정되는 수백 개의 사용자 이름과 비밀번호 페어를 분명한 텍스트로 탈취했습니다. 이러한 탈취 내용물은 인증 정보를 파일에 출력하는 실제 인증 프로세스를 일부 수정해 포착했을 가능성이 높습니다.

T1111 다중인증(MFA)에 대한 개입

공격자는 유효 로그인 정보에 상응하는 MFA 토큰 값도 획득했습니다. 이러한 값은 실제 인증 프로세스를 수정해 해당 값을 파일에 출력함으로써 포착되었을 가능성이 높습니다. MFA 토큰의 보안을 제공하는 고유 값을 저장하는 '비밀 서버'가 침해되었다는 증거는 없습니다.

T1040 네트워크 스니핑(Network Sniffing)

공격자는 침해된 기기에서 HTTP 트래픽을 캡처해 JWT를 캡처한 것으로 추정됩니다. 침해된 기기에서 tcpdump 유틸리티가 실행되었다는 증거가 있으며, 공격자는 이를 통해JWT를 캡처했을 수도 있습니다.

T1539 웹 세션 쿠키 탈취

위에서 설명한 대로, 공격자는 웹 세션 쿠키와 유사한 JWT를 캡처했습니다. 공격자는 이를 재사용해 더 많은 접근권을 확보하려 했을 수도 있습니다.

발견

T1046 네트워크 서비스 발견

침해된 기기에서 네트워크 스캐닝 유틸리티 nmap이 실행되어 동일한 네트워크 세그먼트에 있는 다른 기기를 스캔했다는 증거가 있습니다. 이는 공격자에게 수평 이동의 기회를 제공할 수 있는 다른 접근 가능한 네트워크 서비스를 발견하는 데 사용되었을 가능성이 높습니다.

수집

수집된 증거는 공격자가 침해된 기기나 다른 시스템에서 어떻게 데이터를 수집했고 정확히 무엇이 수집되었는지 보여주지 않습니다. 그러나 공격자는 위에서 설명한 캡처된 인증정보(T1003), MFA 토큰 값(T1111) 및 JWT를 포함해 침해된 기기의 모든 파일에 접근했을 가능성이 높습니다.

명령 및 통제

T1071.001 애플리케이션 레이어 프로토콜: 웹 프로토콜

공격자들은 명령 및 통제를 위해 웹 셸을 사용했습니다. 웹 셸 명령은 기기의 기존 웹 서버를 사용하는 HTTPS로 전달되었을 것입니다(T1572).

T1001.003 데이터 난독: 프로토콜 가장

공격자는 합법적인 트래픽에 섞이도록 설계된 공격을 위한 시작점으로 침해된 기기를 사용했습니다.

감지 및 완화 관련 권장사항

ASD 산하 ACSC는 조직들이 ASD의 필수 8가지 통제 기능과 관련된 사이버 보안 사고 완화 전략(Strategies to Mitigate Cyber Security Incidents)을 도입하기를 강력히 권장드립니다. 아래는 APT40 공격을 감지 및 방지하기 위해 필수적으로 실행해야 하는 네트워크 보안 조치 권장사항이며 이어지는 표1에는 4가지 주요 전략, 기술 및 절차(TTP)에 대한 특정 완화 전략이 요약되어 있습니다.

감지

위에서 파악된 파일 중 일부는 C:\Users\Public* 및 C:\Windows\Temp*와 같은 위치에 배치되었습니다. 이러한 위치는 일반적으로 모든 사용자가 쓸 수 있으므로 데이터를 쓰기에 편리한 장소입니다. 즉, Windows에 등록된 모든 사용자 계정이 이러한 디렉터리와 서브 디렉터리에 접근할 수 있습니다. 많은 경우에 모든 사용자가 이러한 파일에 접근할 수 있으며, 이는 시스템 내 수평적 이동, 방어 기능 우회, 낮은 권한 작업 실행, 그리고 데이터 유출을 위한 준비 등이 가능함을 의미합니다.

다음 시그마 규칙은 의심스러운 위치에서 실행되는 활동을 탐지하며 이를 비정상적인 활동의 지표로 인식합니다. 모든 경우에 후속 조사가 이뤄지며 이는 악의성 활동과 그 소속을 확인하기 위함입니다.

제목: World Writable Execution (전체 사용자에게 수정 권한 오픈) - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

설명: C:\Windows\Temp 경로에서 프로세스 실행을 탐지합니다.

배경:

이 규칙은 C:\Windows\Temp*에서의 실행만을 탐지합니다. Temp는 정상 애플리케이션에서 더 광범위하게 사용되므로 C:\Windows 내 전 사용자가 쓰기 가능한 다른 하위 디렉터리에서의 실행보다 신뢰도가 낮은 악성 지표입니다.

SYSTEM 또는 NETWORK SERVICE 사용자가 실행한 애플리케이션을 제거하면 이 규칙에서 선택되는 정상 활동의 양이 크게 줄어듭니다.

즉, 이 규칙은 더 높은 권한 수준에서 악의적인 실행을 놓칠 수 있습니다. 사용자가 SYSTEM으로 권한을 상승하려고 시도하는지 확인하기 위해서는 다른 규칙을 사용하는 것이 좋습니다.

조사:

1. 사용자 배경, 실행 무결성 수준, 직후 발생하는 활동, 그리고 파일에 의해 업로드된 이미지 등 해당 파일 실행과 직접 연관되어 있는 정보를 살핍니다.
2. 해당 활동의 악의성 여부를 평가하는 데 도움이 되는 호스트에서의 프로세스, 네트워크, 파일 및 기타 관련 데이터를 조사합니다.
3. 필요한 경우, 유효성을 확인하기 위해 역설계할 파일의 사본 수집을 시도합니다.

참조:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

작성자: ASD 산하 ACSC

날짜: 2024/06/19

상태: 실험

태그:

- tlp.green
- classification.au.official
- attack.execution

로그 출처:

카테고리: process_creation
상품: windows

감지:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    사용자:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

상태: temp and not (common_temp_path or system_user or dismhost or known_parent)

오탐지:

- 허용 목록(Allowlist) 감사 애플리케이션이 Temp에서 실행 파일을 실행하는 것이 관찰되었습니다.
- Temp에는 다양한 설치 애플리케이션과 실행 프로그램이 포함되어 있으므로 이 규칙을 배포하기 전에 모니터링되는 네트워크에서 이러한 동작이 얼마나 흔히 일어나는지(그리고 이를 허용 목록에 추가할 수 있는지 여부)를 고려하는 것이 좋습니다.

레벨: 낮음

제목: World Writable Execution - Non-Temp System Subdirectory

ID: 5b187157-e892-4fc9-84fc-aa48aff9f997

설명: Windows OS 설치 경로의 서브 디렉터리에 있는 전체 사용자 쓰기 가능 위치에서의 프로세스 실행을 탐지합니다.

개요:

이 규칙은 C:\, 특히 C:\Windows* 내의 전체 사용자 쓰기 가능한 디렉터리에서의 실행을 구체적으로 찾습니다. 단, C:\Windows\Temp는 제외되며 이는 이것이 정상 애플리케이션에서 더 널리 사용되므로 신뢰도가 낮은 악성 지표이기 때문입니다.

파일이 SYSTEM으로 실행되는 경우 AppData 폴더는 제외됩니다. 이는 많은 임시 애플리케이션 파일이 실행되는 정상 방법입니다.

초기 네트워크 베이스라인을 완성하고 이러한 경로에서 알려진 정상 실행을 식별한 후에는, 이 규칙이 거의 실행되지 않아야 합니다.

조사:

1. 사용자 배경, 실행 무결성 수준, 직후 발생하는 활동, 그리고 파일에 의해 업로드된 이미지 등 해당 파일 실행과 직접 관련되어 있는 정보를 살핍니다.
2. 해당 활동의 악의성 여부를 평가하는 데 도움이 되는 호스트에서의 프로세스, 네트워크, 파일 및 기타 관련 데이터를 조사합니다.
3. 필요한 경우, 유효성을 확인하기 위해 역설계할 파일의 사본 수집을 시도합니다.

참조:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

작성자: ASD 산하 ACSC

날짜: 2024-06-19
상태: 실험

태그:

- tlp.green
- classification.au.official
- attack.execution

로그 출처:

카테고리: process_creation
상품: windows

감지:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'

- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
사용자: 'SYSTEM'

상태: writable_path and not appdata

오탐지:

허용 목록(Allowlist) 감사 애플리케이션이 이들 디렉토리에서 실행 파일을 실행하는 것이 관찰되었습니다.

모니터링 대상 환경에서 사용된 스크립트와 관리 도구가 이러한 디렉토리 중 하나에 있을 가능성이 있으며, 이는 사례별로 다뤄져야 합니다.

레벨: 높음

제목: World Writable Execution - Users

ID: 6dda3843-182a-4214-9263-925a80b4c634

설명: C:\Users\Public* 및 Users 내 전체 사용자 쓰기 가능한 다른 폴더에서의 프로세스 실행을 탐지합니다.

개요:

파일이 SYSTEM으로 실행되는 경우 AppData 폴더는 제외됩니다. 이는 많은 임시 애플리케이션 파일이 실행되는 정상 방법입니다.

조사:

1. 사용자 배경, 실행 무결성 수준, 직후 발생하는 활동, 그리고 파일에 의해 업로드된 이미지 등 해당 파일 실행과 직접 관련되어 있는 정보를 살핍니다.
2. 해당 활동의 악의성 여부를 평가하는 데 도움이 되는 호스트에서의 프로세스, 네트워크, 파일 및 기타 관련 데이터를 조사합니다.
3. 필요한 경우, 유효성을 확인하기 위해 역설계할 파일의 사본 수집을 시도합니다.

참조:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

작성자: ASD 산하 ACSC

날짜: 2024-06-19

상태: 실험

태그:

- tlp.green
- classification.au.official
- attack.execution

로그 출처:

카테고리: process_creation
상품: windows

감지:

사용자:

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contains: '\\AppData\\'
사용자: SYSTEM'

상태: users and not appdata

오탐지:

- 모니터링 대상 환경에서 사용된 스크립트와 관리 툴은 공개 디렉토리 또는 서브 디렉토리에 위치해 있을 가능성이 있으며, 이는 사례별로 다뤄져야 합니다.

레벨: 중간

완화 조치

로깅

ASD 산하 ACSC 조사 기간에 조사 노력의 효과와 속도를 저하시키는 흔한 문제는 웹 서버 요청 로그, Windows 이벤트 로그, 인터넷 프록시 로그를 포함한 여러 영역에 있어 포괄적인 로깅 정보와 기록된 로그 데이터가 부족하다는 것입니다.

ASD 산하 ACSC는 Windows 이벤트 로깅 저장소 (Windows Event Logging Repository)의 구성 파일 및 스크립트와 정보 보안 매뉴얼의 시스템 모니터링 지침 (Guidelines for System Monitoring)을 포함하여 Windows 이벤트 로깅 및 전달에 대한 지침을 검토하고 구현할 것을 권장합니다. 이는 로그의 중앙 관리 및 적절한 기간 동안의 로그 보관을 위한 것입니다.

패치 관리

웹 서버, 웹 애플리케이션 및 원격 접근 게이트웨이를 비롯해 인터넷에 노출된 모든 기기와 서비스를 즉시 패치하세요. 프로세스를 자동화시켜 소요 시간을 단축시킬 수 있는 중앙 패치 관리 시스템 도입을 고려해 보세요. ASD 산하 ACSC는 적용 가능한 경우, ISM의 시스템 관리 지침(Guidelines for System Management), 특히 시스템 패치 통제 구현을 권장합니다.

공격자가 사용한 대부분의 악용 사례는 공개적으로 알려진 패치나 완화 지침이 제공된 패치였습니다. 조직에서는 보안 패치나 완화책을 48시간 이내에 인터넷 연결 인프라에 적용해야 하며, 가능한 경우 최신 버전의 소프트웨어와 운영 체제를 사용해야 합니다.

네트워크 세분화

네트워크 세분화는 공격자들이 조직의 민감한 데이터를 찾아 액세스하는 것을 훨씬 더 어렵도록 할 수 있습니다. 필요하지 않은 경우, 컴퓨터 간 트래픽을 거부하여 시스템 내 수평적 이동을 제한하거나 차단하기 위해 네트워크를 세분화하세요. 액티브 디렉토리(Active Directory) 및 기타 인증 서버와 같은 중요한 서버는 제한된 수의 중개 서버 또는 '점프 서버'에서만 관리할 수 있어야 합니다. 이러한 서버는 면밀히 모니터링되고 보안이 잘 유지되어야 하며, 서버에 연결할 수 있는 사용자와 기기는 제한되어야 합니다.

시스템 내 수평적 이동이 방지된 경우와 별개로 추가적인 네트워크 세분화를 통해 공격자가 접근하고 추출할 수 있는 데이터량을 더욱 제한할 수 있습니다.

추가 완화 조치

저작 기관들은 또한 APT40 및 타 공격자들이 아래 전략, 기술 및 절차(TTP)를 사용하는 것을 방지하기 위해 다음과 같은 완화 조치를 권장합니다.

- 사용되지 않는 혹은 불필요한 네트워크 서비스, 포트 및 프로토콜은 비활성화 시키세요.
- 웹 서버와 애플리케이션을 보호하기 위해 잘 설계된 웹 애플리케이션 방화벽(WAF)을 사용하세요.
- 서버, 파일 공유 및 기타 자원에 대한 접근 권한을 최소 권한 원칙에 따라 제한하세요.
- 누군가가 인증 정보를 해독하고 재사용하는 것을 더욱 어렵게 만들기 위해 다중인증(MFA)과 관리 서비스 계정을 사용하세요. 다중인증은 인터넷에 연결될 수 있는 모든 원격 접근 서비스에 적용되어야 하며 이는 다음을 포함합니다:
  - 웹 및 클라우드 기반 이메일
  - 콜라보레이션 플랫폼
  - 가상 개인 네트워크 연결
  - 원격 데스크톱 서비스
- 지원이 더 이상 제공되지 않는 장비는 교체하세요.

표 1: 완화 전략/기술

TTP	8가지 필수 완화 전략	ISM 통제
최초 접근 T1190 공개 애플리케이션의 악용	패치 애플리케이션 패치 운영 체제 다중인증(MFA) 애플리케이션 통제	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
실행 T1059 명령 및 스크립트 통역:	애플리케이션 통제 Microsoft Office 매크로 제한 관리자 권한 제한	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
지속성 T1505.003 서버 소프트웨어 구성 요소: 웹 셸	애플리케이션 통제 관리자 권한 제한	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
초기 접근 / 접근 권한 상승 / 지속성 T1078 유효 계정	패치 운영 체제 다중인증(MFA) 관리자 권한 제한 애플리케이션 통제 사용자 애플리케이션 강화	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

감지 및 완화 관련 더 많은 일반적인 조언이 필요하시면 본문 마지막 부분에 있는 MITRE ATT&CK 기술 웹 페이지의 Mitigations and Detection 섹션을 참조하세요. 여기에 MITRE ATT&CK 요약에 식별된 각 기술이 설명되어 있습니다.

면책 조항

이 보고서에서 제공되는 정보는 정보 제공 목적으로만 "있는 그대로" 제공됩니다. 저작 기관은 이 문서에 언급된 모든 단체, 제품 또는 서비스를 포함해 어떠한 상업적 단체, 제품, 회사 또는 서비스도 보증하지 않습니다. 서비스 마크, 상표, 제조업체 또는 기타 방법을 통한 특정 상업적 단체, 제품, 프로세스 또는 서비스에 대한 언급은 저작 기관의 지지, 권장 또는 선호를 구성하거나 암시하지 않습니다.

본 문서는 TLP:CLEAR로 지정되었습니다. 공개에는 제한이 없습니다. 대중 공개에 대한 관련 규정 및 절차에 따라, 정보의 예상 가능한 오용 위험이 미미하거나 전혀 없는 경우 정보 출처는 TLP:CLEAR를 사용할 수 있습니다. 표준 저작권 규칙에 따라 TLP:CLEAR 정보는 제한 없이 배포될 수 있습니다. 트래픽 라이트 프로토콜(Traffic Light Protocol)에 관한 더 자세한 정보를 원하시면 cisa.gov/tlp를 참조하세요.

MITRE ATT&CK – 관심 대상의 과거 APT40 공격 기법

정찰 (TA0043)	
피해자 소유 웹사이트 검색 (T1594)	피해자 신원 정보 수집: 인증 정보 (T1589.001)
액티브 스캐닝: 취약성 스캐닝 (T1595.002)	피해자 호스트 정보 수집 (T1592)
공개 웹사이트/도메인 검색 검색 엔진 (T1593.002)	피해자 네트워크 정보 수집: 도메인 특성 (T1590.001)
피해자 신원 정보 수집: 이메일 주소 (T1589.002)	

자원 개발 (TA0042)	
인프라 확보: 도메인 (T1583.001)	인프라 확보 (T1583)
인프라 확보: DNS 서버 (T1583.002)	계정 침해 (T1586)
기능 개발: 코드 서명 인증서 (T1587.002)	인프라 침해 (T1584)
기능 개발: 디지털 인증서 (T1587.003)	기능 개발: 악성코드 (T1587.001)
기능 획득: 코드 서명 인증서 (T1588.003)	계정 생성: 클라우드 계정 (T1585.003)
인프라 침해: 네트워크 기기 (T1584.008)	기능 획득: 디지털 인증서 (T1588.004)

초기 접근 (TA0001)	
유효 계정 (T1078)	피싱 (T1566)
유효 계정: 기본 계정 (T1078.001)	피싱: 스피어피싱 첨부파일 (T1566.001)
유효 계정: 도메인 계정 (T1078.002)	피싱: 스피어피싱 링크 (T1566.002)
외부 원격 서비스 (T1133)	공개 애플리케이션 악용 (T1190)
드라이브 바이 감염 (T1189)	

실행 (TA0002)	
Windows 관리 도구 (T1047)	명령 및 스크립트 통역: Python (T1059.006)
예정 태스크/작업: At (T1053.002)	명령 및 스크립트 통역: JavaScript (T1059.007)
예정 태스크/작업: 예정 태스크 (T1053.005)	네이티브 API (T1106)
명령 및 스크립트 통역 (T1059)	프로세스 간 통신 (T1559)
명령 및 스크립트 통역: Windows 명령 셸 (T1059.003)	시스템 서비스: 서비스 실행 (T1569.002)
명령 및 스크립트 통역: PowerShell (T1059.001)	클라이언트 실행 악용 (T1203)
명령 및 스크립트 통역: 비주얼 베이직 (T1059.005)	사용자 실행: 악성 파일 (T1204.002)
명령 및 스크립트 통역: 유닉스 셸 (T1059.004)	명령 및 스크립트 통역: Apple 스크립트 (T1059.002)
예정 태스크/작업: Cron (T1053.003)	소프트웨어 배포 툴 (T1072)

지속성 (TA0003)	
유효 계정 (T1078)	서버 소프트웨어 구성 요소: 웹 셸 (T1505.003)
오피스 애플리케이션 스타트업: 오피스 템플릿 매크로 (T1137.001)	시스템 프로세스 생성 또는 수정: 서비스 (T1543.003)
예정 태스크/작업: At (T1053.002)	부팅 또는 로그온 자동 실행: 레지스트리 런 키 / 시작 프로그램 폴더 (T1547.001)
예정 태스크/작업: 예정 태스크 (T1053.005)	부팅 또는 로그온 자동 실행: 단축 기능 수정 (T1547.009)
외부 원격 서비스 (T1133)	실행 플로우 하이재킹: DLL 검색 순서 하이재킹 (T1574.001)
예정 태스크/작업: Cron (T1053.003)	실행 플로우 하이재킹: DLL 사이드로딩 (T1574.002)
계정 조작 (T1098)	유효 계정: 클라우드 계정 (T1078.004)
유효 계정: 도메인 계정 (T1078.002)	

권한 상승 (TA0004)	
예정 태스크/작업: At (T1053.002)	시스템 프로세스 생성 또는 수정: Windows 서비스 (T1543.003)
예정 태스크/작업: 예정 태스크 (T1053.005)	부팅 또는 로그온 자동 실행: 레지스트리 런 키 / 시작 프로그램 폴더 (T1547.001)
프로세스 개입: 스레드 실행 하이재킹 (T1055.003)	부팅 또는 로그온 자동 실행: 단축 기능 수정 (T1547.009)
프로세스 개입: 프로세스 할로잉 (T1055.012)	실행 플로우 하이재킹: DLL 검색 순서 하이재킹 (T1574.001)

권한 상승 (TA0004)	
유효 계정: 도메인 계정 (T1078.002)	권한 상승을 위한 악용 (T1068)
액세스 토큰 조작: 토큰 가장/도난 (T1134.001)	이벤트로 촉발된 실행 유닉스 셸 구성 수정 (T1546.004)
프로세스 개입: 동적 링크 라이브러리 인젝션 (T1055.001)	유효 계정: 도메인 계정 (T1078.002)
유효 계정: 로컬 계정 (T1078.003)	

방어 기능 우회 (TA0005)	
루트키트 (T1014)	간접 명령 실행 (T1202)
난독화된 파일 또는 정보 (T1027)	시스템 바이너리 프록시 실행: Mshta (T1218.005)
난독화된 파일 또는 정보: 소프트웨어 패킹 (T1027.002)	시스템 바이너리 프록시 실행: Regsvr32 (T1218.010)
난독화된 파일 또는 정보: 스테가노그래피(위장 삽입) (T1027.003)	신뢰 통제 기능 무력화: 코드 서명 (T1553.002)
난독화된 파일 또는 정보: 배포 후 컴파일(편집) (T1027.004)	파일 및 디렉토리 권한 변경: Linux 및 Mac 파일 및 디렉터리 권한 변경 (T1222.002)
위장: 정상 이름 또는 위치와 일치시키기 (T1036.005)	가상화/샌드박스 회피: 시스템 검사 (T1497.001)
프로세스 개입: 스레드 실행 하이재킹 (T1055.003)	위장 (T1036)
반사 코드 로딩 (T1620)	방어선 무력화: 시스템 방화벽 비활성화 또는 변경 (T1562.004)
프로세스 개입: 프로세스 할로잉 (T1055.012)	디지털 흔적 숨기기: 숨겨진 파일 및 디렉터리 (T1564.001)
지표 제거: 파일 삭제 (T1070.004)	디지털 흔적 숨기기: 숨겨진 창 (T1564.003)
지표 제거: 타임스템프 위조 (T1070.006)	실행 플로우 하이재킹: DLL 검색 순서 하이재킹 (T1574.001)
지표 제거: Windows 이벤트 로그 삭제 (T1070.001)	실행 플로우 하이재킹: DLL 사이드로딩 (T1574.002)
레지스트리 변경 (T1112)	웹 서비스 (T1102)
난독화 해제/파일 또는 정보 디코딩 (T1140)	위장: 위장 작업 또는 서비스 (T1036.004)
방어선 무력화 (T1562)	

인증 정보 접근 (TA0006)	
운영 체제 자격 증명 덤핑: LSASS 메모리 (T1003.001)	보호되지 않은 인증 정보 파일 내 인증 정보 (T1552.001)
운영 체제 자격 증명 덤핑: NTDS 데이터베이스 (T1003.003)	무차별 대입 공격: 비밀번호 추측 (T1110.001)
네트워크 스니핑 (T1040)	강제 인증 (T1187)

인증 정보 접근 (TA0006)	
암호 저장소 내 인증 정보: 키체인 (T1555.001)	커버러스(Kerberos) 티켓 탈취 또는 위조: 커버로스팅 (Kerberoasting) (T1558.003)
인풋 캡처: 키로깅 (T1056.001)	다중인증(MFA) 탈취 (T1111)
웹 세션 쿠키 탈취 (T1539)	애플리케이션 접근 토큰 탈취 (T1528)
인증 정보 접근을 위한 악용 (T1212)	무차별 대입 공격: 비밀번호 크래킹 (T1110.002)
인풋 캡처: 웹 포털 캡처 (T1056.003)	운영 체제 자격 증명 덤핑: DCSync (T1003.006)
암호 저장소 내 인증 정보 (T1555)	암호 저장소 내 인증 정보: 웹 브라우저 내 인증 정보 (T1555.003)

포착 (TA0007)	
시스템 서비스 포착 (T1007)	시스템 정보 포착 (T1082)
애플리케이션 창 포착 (T1010)	계정 포착: 로컬 계정 (T1087.001)
레지스트리 조회 (T1012)	시스템 정보 발견, 기술 T1082 – 엔터프라이즈 | MITRE ATT&CK®
파일 및 디렉터리 포착 (T1083)	시스템 시간 포착 (T1124)
네트워크 서비스 포착 (T1046)	시스템 소유자/사용자 포착 (T1033)
원격 시스템 포착(T1018)	도메인 간 신뢰 관계 포착 (T1482)
계정 포착: 이메일 계정 (T1087.003)	계정 포착: 도메인 계정 (T1087.002)
시스템 네트워크 연결 포착 (T1049)	가상화/샌드박스 우회: 시스템 검사 (T1497.001)
프로세스 포착 (T1057)	소프트웨어 포착 (T1518)
권한 그룹 포착: 도메인 그룹 (T1069.002)	공유 네트워크 발견, 기술 T1135 – 엔터프라이즈 | MITRE ATT&CK®
시스템 네트워크 구성 포착: 인터넷 연결 포착 (T1016.001)	

시스템 내 수평적 이동 (TA0008)	
원격 서비스: 원격 데스크톱 프로토콜 (T1021.001)	원격 서비스 (T1021)
원격 서비스: SMB/Windows 관리자 공유 (T1021.002)	대체 인증 자료 사용: 티켓 전달 (T1550.003)
원격 서비스: Windows 원격 관리 (T1021.006)	수평적 도구 전송 (T1570)

수집 (TA0009)	
로컬 시스템의 데이터 (T1005)	수집 데이터 보관: 라이브러리를 통한 보관 (T1560.002)
네트워크 공유 드라이브 데이터 (T1039)	이메일 수집: 원격 이메일 수집 (T1114.002)

수집 (TA0009)	
인풋 캡처: 키로깅 (T1056.001)	클립보드 데이터 (T1115)
자동 수집 (T1119)	정보 저장소의 데이터 (T1213)
인풋 캡처: 웹 포털 캡처 (T1056.003)	데이터 준비: 원격 데이터 준비 (T1074.002)
데이터 준비: 로컬 데이터 준비 (T1074.001)	수집 데이터 보관 (T1560)
이메일 수집 (T1114)	

유출 (TA0010)	
C2 채널을 통한 유출 (T1041)	대체 프로토콜을 통한 유출: 비대칭 암호화된 비C2 프로토콜을 통한 유출 (T1048.002)
대체 프로토콜을 통한 유출 (T1048)	웹 서비스를 통한 유출: 클라우드 스토리지로 유출 (T1567.002)

명령 및 통제 (TA0011)	
데이터 난독화: 프로토콜 가장 (T1001.003)	웹 서비스: 데드 드롭 리졸버 (T1102.001)
자주 사용되는 포트 (T1043)	웹 서비스: 한 방향 통신 (T1102.003)
앱 레이어 프로토콜: 웹 프로토콜 (T1071.001)	도구 유입 전송 (T1105)
앱 레이어 프로토콜: 파일 전송 프로토콜 (T1071.002)	프록시: 내부 프록시 (T1090.001)
프록시: 외부 프록시 (T1090.002)	비표준 포트 (T1571)
프록시: 멀티 홉 프록시 (T1090.003)	프로토콜 터널링 (T1572)
웹 서비스: 양방향 통신 (T1102.002)	암호화 채널 (T1573)
암호화 채널: 비대칭 암호화 (T1573.002)	도구 유입 전송 (T1105)
프록시, 기술 T1090 - 엔터프라이즈 | MITRE ATT&CK®	

영향 (TA0040)	
서비스 중단 (T1489)	디스크 삭제 (T1561)
시스템 종료/재부팅 (T1529)	자원 하이재킹 (T1496)

참조

면책 조항

본 지침의 자료는 일반적인 성격을 지니므로 법률 자문으로 간주되어서는 안되며, 혹은 특정 상황이나 긴급 상황에서 도움을 받기 위해 의존되어서도 안 됩니다. 모든 중요한 문제에 대해서는 자신의 상황과 관련해 적절하고 독립적인 전문가의 조언을 구해야 합니다.

호주 연방정부는 본 지침에 포함된 정보에 의존한 결과로 발생한 어떠한 손해, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

저작권

호주 연방정부 문장(Coat of Arms) 사용

호주 연방정부 문장의 사용 조건은 국무총리내각부(Department of the Prime Minister and Cabinet) 웹사이트에 자세히 기술되어 있습니다. Commonwealth Coat of Arms Information and Guidelines (호주 연방정부 문장 정보 및 지침) | pmc.gov.au.

더 자세한 정보를 원하시거나 사이버 보안 사고를 신고하시려면 다음으로 저희에게 연락주시기 바랍니다.

cyber.gov.au | 1300 CYBER1 (1300 292 371)

이 번호는 호주 내에서만 사용되는 번호입니다.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre