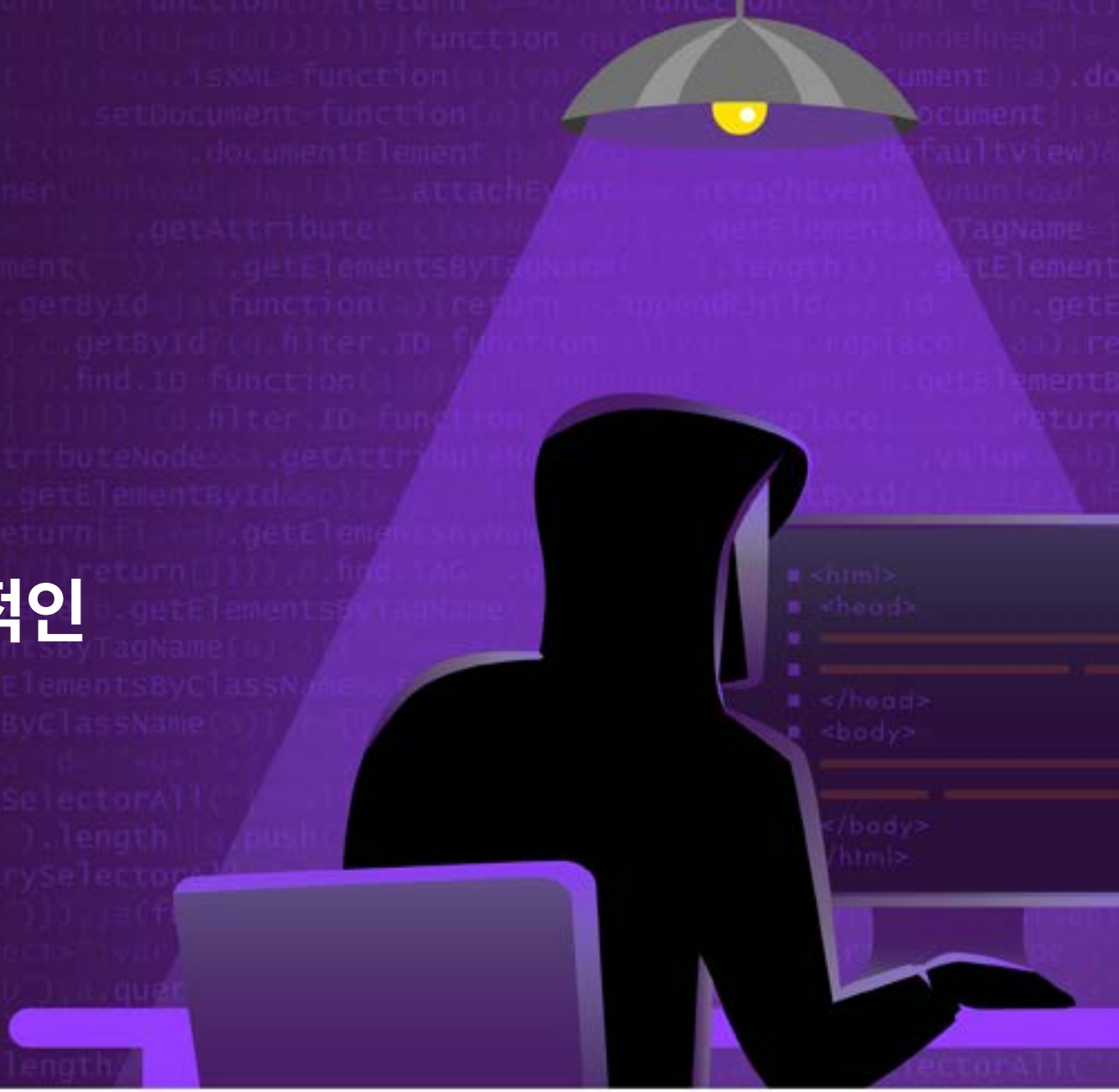
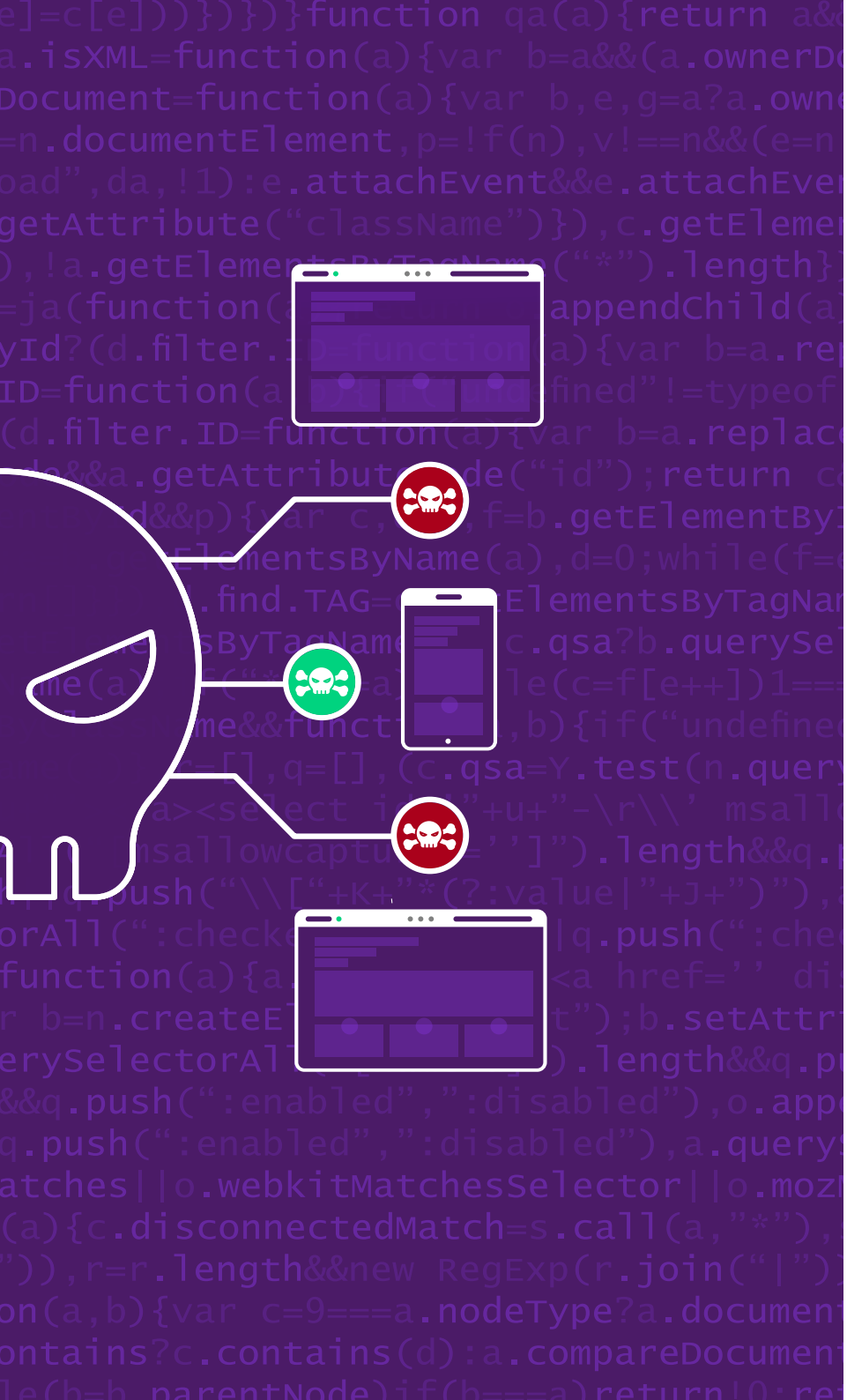
MENLO SECURITY

교묘하게 숨어드는 보안 공격 찾아내기 : 예시 및 분석 매우 회피적인 위협 캠페인



eBook

페이지 내용



재택근무와 함께 늘어난 HEAT 공격

오늘날의 기업은 10년 전과 매우 다르게 보이고 작동합니다. 기업 네트워크를 가속화하고 어디에서나 작업을 수행할 수 있는 직원들을 위해 기술이 홍수처럼 들어와 무궁무진한 기회가 있지만, 그만큼 위험도 높아졌습니다. 많은 기업들이 인식하지 못하는 것은 기업 네트워크를 보호하는 데 투자한 보안 기술에서 주요한 문제가 있습니다. 이는 비즈니스와 함께 발전하지 못한 것 중에 하나입니다.

우리가 믿고 있는 기술 자체가 조직을 보호하지 못하는 것은 위협 행위자들이 알고 있기 때문입니다. 그 이유는 이러한 해결책이 주로 위협을 감지하고 제거하며 악성 코드를 차단하는 규칙을 작성하는 개념에 기반하고 있기 때문입니다. 이것이 보안 기술보다 훨씬 더 빠르게 적응하는 이유입니다. 따라서 이것이 사이버 보안 콘텐츠에서 종종 사용되는 끝없는 '고양이와 쥐' 비유입니다.

공격자들이 집중적으로 노리는 분야 중 하나는 지식 근로자들을 위한 가장 큰 생산성 도구 인 웹 브라우저를 이용한 공격입니다. 그 방법은 고도로 회피적인 적응형 위협(HEAT)으로, 웹 브라우저를 공격 벡터로 이용하고 현재 보안 스택의 여러 계층을 회피하기 위해 다양한 기술을 사용합니다. 이 공격은 많은 경우 랜섬웨어, 고급 피싱 및 제로데이 악성 코드의 출발점 역할을 합니다. HEAT 공격으로 분류되기 위해서는 다음과 같은 회피적 특성 중 하나 이상이 있어야 합니다.

- URL 필터링 회피
- 이메일 보안 도구 회피
- 파일 기반 검사 회피
- HTTP 콘텐츠 / 페이지 검사 회피

이 전자책은 Menlo Labs 연구팀이 분석한 다양한 HEAT 공격 예시를 살펴보며, 그들이 관찰한 것과 이 자료 외의 연구 세부사항을 탐색할 기회를 제공합니다.

멘로팀의 결과 분석

Menlo Labs 연구팀은 보안 팀에 도움이 되는 통찰력, 전문지식, 맥락 및 도구를 제공하는 데 초점을 맞추고 있습니다. 연구팀은 다양한 위협 캠페인에서 HEAT 공격을 분석해 왔습니다. 완전히 이해되면, Menlo Labs 팀은 위협 속성, 전술, 기술, 절차(TTPs) 및 타협 지표(IOC) 등 다양한 통찰력을 포함한 연구 결과를 게시합니다. 가장 중요한 것은, 조직이 미래의 HEAT 공격으로부터 자신을 보호하기 위한 조치를 제공한다는 것입니다.

HEAT 공격

50%

관찰된 HEAT 공격의 50%가 카테고리화된 웹사이트에서 발생했습니다.

분석된 500만 개 이상의 악성 URL 중에서 말입니다.

73%

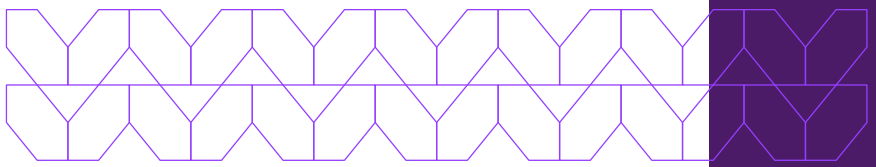
분석된 500만 개 이상의 악성 URL 중에서 말입니다. 카테고리화된 웹사이트에서 발생한 HEAT 기술인 레거시 URL 평판 회피(LURE) 공격의 73%가 발생했습니다.

팀에서 분석한 100만 개가 넘는 urlscan.io 기록을 기반으로 합니다.

70%

2022년에는 LURE 공격이 70% 증가했습니다.

2021년 7월부터 2022년 7월까지 분석된 고객 기록에서, 기존 방어를 우회하는 HEAT 회피 기술이 신뢰에 기반한 도메인을 분류하려는 웹 필터를 피했습니다.



최근 연구를 바탕으로, 연구팀은 HEAT 공격에 대한 몇 가지 의미 있는 통찰력을 발견했습니다. 다음 위협 캠페인 예시는 그들의 발견에 대한 스냅샷을 제공합니다. 완전한 내용을 보려면 연관된 연구 블로그 게시물을 참조하십시오.

보안 공격 내용

라자루스 그룹은 북한 정부가 운영하는 사이버범죄 조직입니다. 이 그룹에게는 2010년부터 2021년까지 많은 사이버 공격이 귀속되었으며, 그 중 가장 주목할 만한 공격은 2014년 소니 픽처스 해킹으로 소니 네트워크에서 훔친 데이터 덩어리와 악명 높은 워너크라이 2.0 글로벌 랜섬웨어 공격으로 전 세계적으로 20만 대 이상의 시스템에 영향을 미쳤습니다.

최근에는 라자루스 그룹이 Menlo Lab 연구팀의 고객 기반에서 HEAT 기술을 활용하여 현재 사용 중인 보안 기술을 우회하여 피해자 조직을 손상시키는 것으로 관찰되었습니다. 그들이 선호하는 방법은 무엇일까요? 바로 브라우저 취약점을 활용한 것입니다. 왜냐하면 웹 브라우저는 오늘날 지식 노동자의 생산성에 있어서 중추적인 역할을 하기 때문입니다.

이 그룹은 브라우저 취약점을 활용하여 최종적으로 악성 소프트웨어와 랜섬웨어를 설치하여 금전적 이익과 지식 재산 도용을 할 수 있도록 알려져 있습니다. 해당 활동은 그룹이 이용한 치명적인 크롬 브라우저 취약점에 의존했으며, 구글 엔지니어들이 결국 이를 패치하였습니다.

타켓

구글은 2021년부터 이 그룹이 유사한 취약점을 뉴스 미디어, IT, 암호화폐 및 핀테크 분야의 조직을 대상으로 활용해 왔다고 지적했습니다. Menlo Lab에서 Menlo Security 고객 기반에 대한 추가 연구를 통해 미국 정부 기관 및 일본 기반 암호화폐 거래소를 포함한 추가 목표가 발견되었습니다.

HEAT 공격 방법

탈취 표적을 나타내는 첫 번째 사례는 2021년 10월까지 거슬러 올라갑니다. 당시 위협 행위자들은 giantblock.org 도메인을 생성하여 이들 작전에 대한 기존 URL 평판 회피(LURE) 도구로 사용하였습니다. 이는 알려진 HEAT 기술 중 하나입니다. 이러한 LURE 공격은 신뢰에 기반한 도메인을 분류하려는 웹 필터를 회피하여 기존 방어를 우회합니다. 공격자들은 이러한 보안 시스템에 이미 신뢰를 받고 있는 약하게 보호된 웹사이트를 침해하거나, 경우에 따라 처음부터 만들어서 악성 소프트웨어를 전송하거나 사용자 자격 증명을 훔칩니다. 이는 초기 세대의 안전한 웹 게이트웨이(SWG)와 전통적인 URL 필터에 의존하는 조직이 점점 위험에 처하게 됨을 의미합니다.

The Lazarus 그룹에 대하여 더 알아보기

VIP3R 스피어 피싱 공격 캠페인

캠페인

위협 행위자들의 공격 무기고와 관련하여, 그들은 성공적인 것에 대해서는 계속 사용하는 것에 익숙합니다. 이것이 바로 이메일 기반 공격이 사용자를 침해하는 그들의 검증된 방법 중 하나인 이유입니다. 최근 한 연구에 따르면, 조직은 2021년 하반기에 비해 2022년 상반기에 이메일 공격이 48% 더 많았습니다. 그 중 대다수(68%)는 자격 증명을 침해하는 것을 목표로 했습니다.

위협 행위자들의 목적에 따라 사용자 자격 증명은 현금과 마찬가지로 귀중할 수 있습니다. 그들에게는 네트워크에 원활하게 접근하여 민감한 정보를 빼내거나, 땅에서 생활하며 결국 그들이 원하는 최고의 보석에 접근할 수 있게 됩니다. 당연히, 2022년에 Menlo 랩 연구팀이 사용자 이름과 비밀번호로 가득한 오픈 디렉토리를 발견했을 때, 그들은 즉시 정보를 파헤쳤습니다.

디렉토리 내용을 추가 분석한 결과, 여러 조직의 164명의 사용자의 자격 증명을 침해하기 위해 회피적인 HEAT 기술을 활용한 단일 캠페인의 결과물이라고 판단했습니다. 캠페인과 관련된 익스플로잇 키트를 분석한 결과, 연구팀은 독특한 문자열 - DH4 VIP3R L337 -을 발견하여 캠페인을 VIP3R로 명명했습니다.

타겟

타겟의 대다수(19%)는 의료 서비스 사용자에게 속했습니다. 전문 서비스를 제공하는 회사(16%)와 교육 부문(11%)의 사용자가 그 뒤를 바짝 뒤따랐습니다. 그러나 20개 이상의 업종이 영향을 받았다는 점을 감안할 때 캠페인은 상당히 넓은 그물을 던졌습니다.

HEAT 공격 방법

IHEAT 기술 "VIP3R 캠페인에서 공격자는 피싱 이메일을 통해 맞춤형 HTML 첨부 파일 페이로드를 피해자에게 전송하여 파일 기반 검사를 피할 수 있었습니다. 피해자가 첨부 파일을 열면 수신자가 일반적으로 사용하는 서비스를 가장한 피싱 페이지가 나타납니다. . 피해자가 비밀번호를 입력하고 "제출" 버튼을 선택하면 서버 측에서 발생하는 비밀번호 유효성 검사 및 검증을 거쳐 궁극적으로 자격 증명이 손상됩니다. 캠페인에 사용된 HTML 파일은 파일 기반 분석을 회피합니다. 피싱 페이지의 URL도 또 다른 HEAT 기술인 LURE(Legacy URL Reputation Evasion)로 인해 URL 필터링을 회피합니다.

VIP3R 캠페인에 대하여 더 알아보기

캠페인

맬웨어 가계도와 관련하여 뱅킹 트로이 목마는 뱅킹 고객이 온라인 거래라는 아이디어에 익숙해지면 실제로 영향을 미치기 시작했습니다. 온라인 뱅킹이 일반화되자 디지털 범죄자들은 재빨리 행동에 나서 은행 자격 증명을 손상시키는 것을 목표로 하는 맬웨어를 제작했습니다. 뱅킹 트로이 목마를 입력하십시오. Trickbot, Dridex 및 Emotet을 포함하여 가장 악명 높은 일부 뱅킹 트로이 목마는 쉽게 탐지를 피하고 민감한 정보를 훔치며 조작할 수도 있습니다 사용자 데이터.

오늘날의 위협 환경에서 뱅킹 트로이 목마는 돈을 노리는 사이버 사기꾼들 사이에서 인기 있는 도구입니다. 연구 결과에 따르면 1년에 100,000개의 변종을 탐지할 수 있다고 합니다. 말할 필요도 없이 뱅킹 트로이 목마는 효과적이며 곧 아무데도 가지 않을 것입니다. 이것이 이 특정 캠페인이 Menlo Labs 연구팀의 레이더에 포착된 이유입니다. QBot 또는 Pinkslipbot이라고도 하는 Qakbot은 지난 10년 동안 널리 퍼진 저명한 뱅킹 트로이 목마입니다. 주로 피싱 이메일을 통해 전달되는 공격자들은 2007년부터 멀웨어를 유지 관리하고 변경하여 전 세계 최고의 뱅킹 트로이 목마 중 하나가 되었습니다.

오늘날 Qakbot은 은행 자격 증명을 손상시킬 수 있을 뿐만 아니라 금융 기관을 염탐하고 자신을 확산시키고 랜섬웨어를 설치할 수 있습니다. Menlo Labs 연구팀은 피해자 조직을 성공적으로 손상시키기 위해 다양한 HEAT 기술을 사용하는 몇 가지 Qakbot 캠페인 변종을 관찰했습니다.

타겟

앞서 언급한 바와 같이 Qakbot 캠페인에는 일반적으로 경계가 없으며 피해자 조직과 사용자는 전 세계에 있습니다. 가장 최근에는 미국 조직을 대상으로 한 공격적인 캠페인이 보고되었으며 랜섬웨어 집단인 Black Basta가 운영하고 있습니다.

HEAT 공격 방법

Menlo Labs 연구팀이 보고한 바와 같이 Qakbot 캠페인은 Lazarus Group에서도 사용했던 LURE(Legacy URL Reputation Evasion)와 같은 HEAT 기술과 사이버 범죄자가 정적 및 동적 콘텐츠 검사를 피할 수 있게 해주는 HTML 밀수를 활용한 것으로 관찰되었습니다. 이러한 공격에서 공격자는 JavaScript BLOB(Binary Large Object) 요소를 생성하고 콘텐츠로 동적으로 채웁니다. Menlo Labs에서 목격한 공격에서 멀웨어 생성에 사용된 콘텐츠는 사용자가 요청한 HTML 페이지 내에 인코딩되었습니다. 콘텐츠는 웹 페이지 내의 요소에서 동적으로 생성되기 때문에 파일 요청은 인터넷을 통해 전송되지 않습니다.

Qakbot 공격에 대하여 더 알아보기

Template 주입 공격

공격

일반 사무 직원들에게 전자 문서 파일은 매우 중요합니다. 매일 직원들은 근무 시 PDF, Excel, Word 또는 기타 Microsoft Office 문서등으로 컴퓨터에서 작업 결과물을 공유하기위해 가장 많이 사용합니다. 그렇기 때문에 위협 행위자들은 이러한 문서를 무기화하여 맬웨어, 트로이 목마 및 심지어 릴리스할 수 있는 코드 및 링크를 포함합니다. 랜섬웨어. Menlo Labs 연구팀은 모든 것을 면밀히 주시하였습니다. 최근에 관찰된 활동의 경우 악성 문서를 포함할 때 템플릿 삽입을 활용한 여러 무기화된 미끼 문서 공격기법이 발견되었습니다.

위협 행위자는 템플릿 주입 기술에 열중하고 있습니다. 매크로와 같은 의심스러운 지표가 문서에 있어야 합니다. 악성 템플릿을 가져올 때까지. 관찰한 내용을 보면 Menlo Labs 연구팀은 템플릿 주입 공격이 인기가 높아지고 있으며 익스플로잇을 로드하는 데 사용될 수도 있다고 합니다.

멘로 팀은 또한 고유한 특성을 지닌 여러 무기화된 문서를 관찰했습니다. 눈에 보이는 URL을 숨기는 위장 기술, IP 주소를 포함하거나 모호한 URL을 사용한 문서 원격으로 호스팅되는 템플릿을 가져오기 위한 다양한 형식입니다.

Menlo Labs 연구 팀 최신 분석에 따르면 이러한 캠페인 중 위협 행위자 일부는 배후에 북한이 연루되어 있을 수도 있

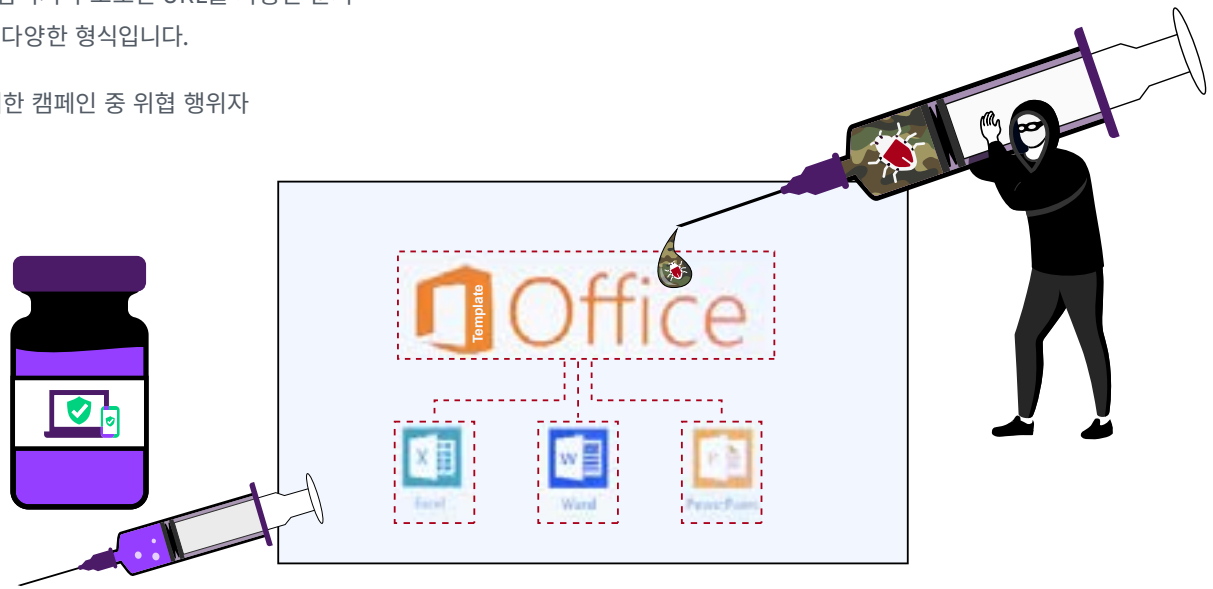
타겟

유사한 TTP가 북한 APT인 BlueNoroff에서 사용되는 것으로 관찰된 점을 감안할 때 일부 대상에는 암호화폐 회사가 포함되지만 이에 국한되지는 않습니다. Menlo Labs 연구팀이 여전히 연구를 수행하는 동안 다른 대상에는 외교 및 정부 기관이 포함될 수 있습니다. 유사한 TTP를 활용하는 위협 행위자에 대해 수행된 연구에 대해.

HEAT 기술

템플릿 주입 공격은 그 자체로 기술로 간주되지만 웹 필터에 의해 평판이 좋은 것으로 분류된 웹 사이트를 사용하여 맬웨어를 전달하는 레거시 URL 평판 회피(LURE) 기술을 활용하여 보안 도구 및 솔루션을 회피하기도 합니다.

Menlo Labs 연구팀은 아래와 같은 공격을 이야기하였고,이 기사 시리즈의 1부, 2부 및 3부 에 자세하게 다루웠습니다.



조직을 보호하는 방법

The infection vectors of HEAT attacks have been plaguing organizations for years, but given the recent evolution of the threat market resulting in part from accelerated cloud migration and the proliferation of remote work, these relatively unknown attacks pose the greatest threat for enterprises today. As mentioned before, all traditional security capabilities–including Secure Web Gateways, sandboxing, URL reputation, and filtering – are rendered ineffective against HEAT attacks. The challenge is that because HEAT characteristics have legitimate uses, simply blocking them won't work. Preventing the use of these techniques altogether is key.

One proven preventative approach is leveraging isolation technology, which delivers on the true promise of Zero Trust security. Separating an enterprise network from the public web–while still allowing users to access the Internet seamlessly– results in a Zero Trust Internet. One key characteristic that makes isolation technology appealing to organizations is that it ensures user productivity, while granting open access to the Internet–making security invisible to the end user. Additionally, it allows businesses to scale globally to support roaming users without impacting user performance.

Isolation moves the viewing of email attachments and web browsing from a user's device to the cloud. By isolating Internet content in the cloud, users are protected from HEAT attacks that bypass legacy security solutions and result in malware and ransomware. Not only would isolation technology have prevented each of the malware and phishing examples outlined in this ebook, but it's also proven to eliminate the most prolific sources of breaches.

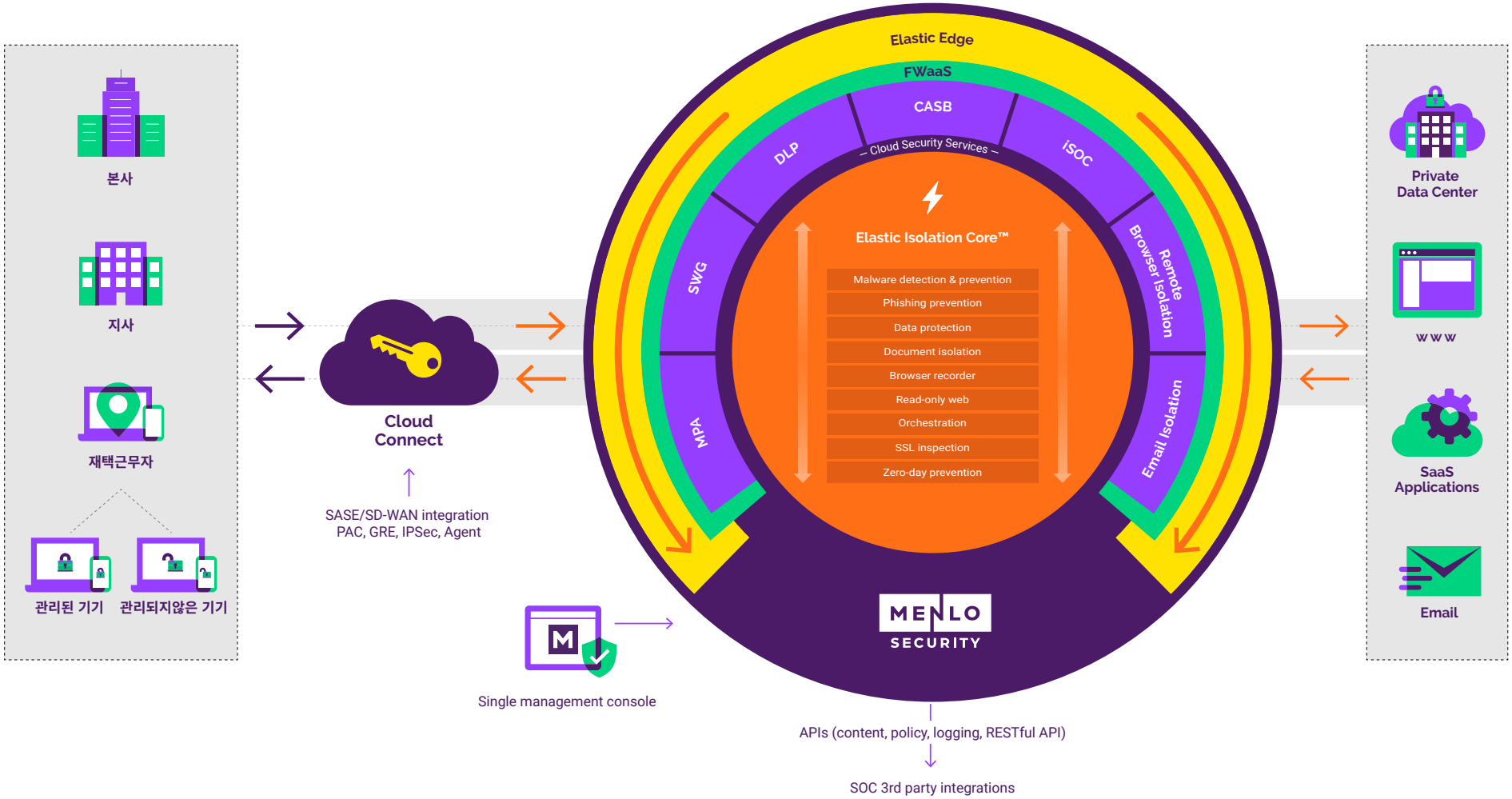
멘로 시큐리티에 대하여

Menlo의 Cloud Security Platform은 위협이 조직에 침입하는 것을 방지하고 단일 글로벌 클라우드 기반 제품에서 데이터 및 애플리케이션 액세스를 보호합니다. 당사의 Elastic Isolation CoreTM는 보안, 정책 및 가시성이 적용되는 사용자, 콘텐츠 및 애플리케이션을 분리합니다. By 조직은 위협이 발생하기 전에 감지하고 대응하는 것과는 달리 웹, 이메일, SaaS 애플리케이션 및 개인 애플리케이션 전반에서 HEAT(Highly Evasive Adaptive Threats)를 비롯한 모든 위협을 제거합니다.

HEAT 체크

Menlo Security는 조직이 다양한 HEAT에 대한 민감성을 더 잘 이해할 수 있도록 간단한 침투 평가를 제공합니다. 공격. 이 평가는 위협 행위자가 현재 사용하고 있는 다양한 실제 HEAT 공격을 활용하여 조직이 안전하게 수행할 수 있도록 합니다. 그들의 노출을 추론하십시오. Menlo의 Heat Check 도구는 실제 악성 콘텐츠를 전달하지 않습니다.

Menlo's Cloud Security Platform



궁금한 사항이 있으시면 언제든 연락부탁드립니다.

멘로시큐리티에 연락주시면 고객님의 조직이
현재 HEAT 공격에 취약한지를 확인하고 예방하여
처음부터 이러한 공격이 발생하지 않도록 하는 방법을
제안해드리겠습니다.

menlosecurity.com/heatcheck-korea

ask@menlosecurity.com

MENLO SECURITY