

[인터넷 보안 현황 보고서]

5권, 1호

DDoS

및

애플리케이션

공격



Intelligent Security Starts at the Edge

편집자 인사말

2019년의 첫 번째 인터넷 보안 현황 보고서를 발표하게 되어 기쁘게 생각합니다. 2019년이 시작된 지 벌써 몇 주가 흘렀고 지난 연휴는 이미 과거가 되었습니다. 새해 첫날은 시간을 임의적으로 구획한 것에 불과하지만 과거를 되돌아보고 미래를 계획할 수 있는 좋은 시기이기도 합니다.

네트워크 보안 전문가는 이전 경험에서 배운 교훈을 토대로 앞으로 시스템 보안을 강화할 수 있는 체계를 구축할 책임이 있습니다. 간단한 프로세스일 수도 있지만 기업 운영에 필요한 일상적인 작업 때문에 복잡해지는 경우도 많습니다. 과거를 되돌아 보는 일은 우선 순위에서 밀리기 마련입니다.

핵심 요약

- '공격'이 실제 공격이 아니었던 경우도 있습니다. Akamai의 SOCC 전문가들은 사이트에 영향을 미치는 40억 건의 요청을 관측하고 실제 원인을 조사했습니다.
- 공격자들은 봇을 이용해 많은 수익을 거두고 있는데 이 봇은 새로운 방어 시스템을 우회하기 위해 지속적으로 진화하고 있습니다. 한 공격자는 Akamai의 방어 체계를 뚫어 본 경험이 있는 사람에게 큰 돈을 지불하겠다는 제안을 하기도 했습니다.
- 미국 기업들은 정신 건강 문제로 인해 매년 1,900억 달러의 손실을 겪고 있습니다. 본 보고서의 객원 저자인 아만다 베를린(Amanda Berlin)은 보안팀에서 모니터링해야 하는 문제에 대해 설명합니다.

2018년에 경험한 주요 인시던트와 도전과제를 살펴보고 이것이 2019년에 어떤 영향을 미칠 것인지에 대해 논의할 수 있는 시간을 별도로 정해 두셨나요? 관련성 없는 수많은 인시던트를 해결하느라 바빴셨나요? 중요한 의미를 갖는 경험이 있었나요?

많은 보안팀은 기업에서 발생한 모든 인시던트를 충실하게 검토하고 이를 통해 교훈을 얻고 있습니다. 하지만 역량 있는 보안팀이라 하더라도 한 걸음 물러서서 그동안의 경험을 전반적으로 살펴보지 않는 경우가 많습니다. 장기적인 글로벌 트렌드는 어느 정도 거리를 두고 관점을 전환할 때 비로소 뚜렷해집니다.

```
should: *) hostTokens := strings.Split(r.Host
ue("count"), 10, 64); if err != nil { fmt.Fpri
ue("target"), Count: count}; cc <- msg; fmt.Fp
tring(r.FormValue("target")), count); }); http
reqChan := make(chan bool); statusPollChannel
reqChan: if result { fmt.Fprint(w, "ACTIVE");
print(w, "TIMEOUT");}); log.Fatal(http.Listen
inpage", "deskwin10");</script></body></html>p
"strings"; "time" ); type ControlMessage struc
CompleteChan := make(chan bool); workerActive
channel, statusP
workerActive := <-controlCha
n: workerActive
func(w *http.ResponseWriter, r *http.Requ
they probably should. */ hostTokens :=
FormValue("count"), 10, 64); if err !=
r.FormValue("target"), Count: count}; cc
EscapeString(r.FormValue("target")), co
n bool); statusPo
http.HandleFunc("/admin", func(w *http.W
net/http"; "strconv"; "
ControlChannel := make
chan bool); workerActive
statusPollChannel: respChan <-
erCompleteChan); case status :=
statusPollChannel chan chan bo
anyone actually read this stu
err := strconv.ParseInt(
ControlMessage{targe
Target %s, count %d",
http.ResponseWriter, r *
After(time.Second); se
ACTIVE"); } return; c
"aaaa0f66-465f-4751-b
script></body></html>
```

2019년을 전망할 때 보안 분야에서 함께 근무하고 교류하는 사람들의 스트레스와 정신 건강을 확인할 것을 다시 한 번 강조하고 싶습니다. 부하 직원, 상사, 다른 조직의 동료 등에게 잠시 시간을 내어 연락하고 안부를 물어보시기 바랍니다.

최근 몇 년 동안 여러 컨퍼런스(BSides, RSA 등)에서 스트레스와 과로 문제가 의제에 추가되었습니다. 짧은 통화나 이메일이 동료의 하루에 큰 변화를 가져올 수 있습니다. 보안은 스트레스 수준이 높은 분야이기 때문에 자주 소통하려는 노력을 기울여야 합니다.

2019년에 변화를 가져올 수 있는 기회는 매우 많습니다. 여러분은 어떤 목표를 달성하고 싶으신가요?

목차

편집자 인사말

정신 건강: 해커를 위한 인지 교육

최신 연구 자료

jQuery 파일 업로드

UPnPProxy

AKAMAI 연구 자료

실제 공격이 아니었던 DDoS 공격

붐이 증가하면서 더 많은 문제 발생

향후 전망

부록 A: 방법론

저자 소개

1
2
5
11
11
11
15
22
23
24

```
g") {  
    () {  
        e(chan chan  
        <- statusPollChan  
        erCompleteChan  
        tatusPollChan  
        anyone actually  
        ; count, err :=  
        msg := ControlMessage{target  
        ed for Target %s",  
        .ResponseWriter, r *  
        time.Second); se  
        VE"); } return; case  
        ;("aeaa0f66-465f-4751-b  
        ain; import ("fmt"; "ht  
        ring; Count := int64(1);  
        l); statusPollChannel :=  
        { select { case respChan :=  
        e = true; go doStuff(msg, w  
        admin(cc chan ControlMessage,  
        , r *http.Request) { /* Does  
        Host, ":"); r.ParseForm(); count  
        .Printf(w, err.Error()); return  
        mt.Printf(w, "Control message %s",  
        http.HandleFunc("/status",func(w  
        nnel <- reqChan;timeout := time.After  
        E"); } else { fmt.Fprintf(w, "INACTIVE  
        istenAndServe(":1337", nil)); }>("aeaa0f66-465f-4751-b  
        tml>package main; import ("fmt"; "ht  
        struct { Target string; Count int64;  
        chan := makeCh[인터넷 보안 현황 보고서] DDoS 및 애플리케이션 공격: 5권, 1호  
        atusPollChannel), for { select { case respChan :=  
        olChannel: workerActive = true; go doStuff(msg, w  
        tive = status; }));unc admin(cc chan ControlMessage,  
        c(w http.ResponseWriter, r *http.Request) { /* Does  
        s := strings.Split(r.Host, ":"); r.ParseForm(); count
```

정신 건강:

해커를 위한 인지 교육

정보 보안 커뮤니티 종사자들은 인텔리전트하고, 추진력 있고, 열정적이고, 의견을 쉽게 굽히지 않습니다. 다른 분야와 비교하는 것이 어렵기는 하지만 연구, 학습, 강의 등으로 인한 스트레스와 압박감이 더해지면 상황은 빠르게 악화될 수 있습니다. 스스로 받는 압박감 외에도 우리는 직장 상사, 동료, 가족으로부터 매우 다양한 형태의 스트레스를 받게 됩니다.

우리가 맡은 업무를 처리하려면 쉬지 않고 몇 시간 동안 키보드 앞에 앉아있어야 하는데 이로 인해 많은 사람들이 정신적으로 무너지게 됩니다. 무너지는 방법, 시간, 이유는 다양합니다.

이번 인터넷 보안 현황 보고서의 객원 저자인 아만다 베를린(Amanda Berlin)은 다른 외부 저자와는 다른 관점을 제시합니다. 인터넷 보안 현황 보고서는 인터넷의 어두운 이면에 대해 경각심을 일깨우는 데 중점을 두고 있습니다. 정보 보안 업계의 스트레스와 과로가 이미 높은 수준임에도 불구하고 계속 높아지고 있다는 것을 보여주는 증거가 끊임 없이 나오고 있습니다. 이로 인해 보안 담당자의 신체적 건강뿐만 아니라 감정적, 정신적 건강을 지키는 방법이 무엇인지에 대해 질문하게 됩니다. 저는 다행히 직원의 건강을 핵심 가치로 여기는 Akamai에 근무하고 있지만 모든 사람들이 다 저와 동일한 환경에서 지원을 받으면서 일하고 있는 것은 아닙니다. 몇 페이지 분량의 짧은 논의로는 이 문제를 해결할 수 없지만, 저와 나머지 SOTI 팀원들은 보안 커뮤니티 구성원으로서 베를린의 관점이 공개적으로 다뤄지지 않는 문제에 대한 해결의 실마리를 제공한다고 느꼈습니다. 우리 모두가 인터넷을 보다 좋은 공간으로 만드는 데 전념할 수 있도록 직원 건강 향상에 더 많은 노력을 기울이고 지원을 아끼지 않을 것을 기업에 권장합니다.

이 보고서의 내용은 의학 자문이나 전문 상담으로 해석해서는 안 됩니다. 본인 또는 지인이 여기에서 설명한 증상을 보이고 있다면 전문가의 도움을 받으시기 바랍니다.

- 마틴 맥케이(Martin McKeay), 편집 책임자

세계보건기구(WHO)에 따르면 **매년 80만 명이 자살로 사망**하며 자살은 15~29세의 사망 원인 2위를 차지합니다. 자살을 하기 전에 20번 이상의 자살 시도가 있었다는 결과가 있습니다. 사람들에게 필요한 관심을 제공하려면 조기 발견과 효과적인 관리가 중요합니다.

비즈니스 목표로서의 정신 건강:

미국은 **심각한 정신 질환으로 인해 연간 1,932억 달러의 손실**을 입고 있고, 매년 성인 25명 중 1명(980만 명 또는 인구의 4%)이 하나 이상의 주요 일상 생활을 제한하거나 지장을 주는 심각한 정신 질환을 경험합니다.

현재 많은 기업들은 정신 건강 치료와 인지를 일상 활동의 일부분으로 포함시키고 있습니다. 행복하고 균형 잡힌 삶을 사는 직원의 업무 성과가 더 우수하고 근무 기간 역시 더 깁니다. 또한 일반적으로 우수한 근무 환경을 만드는데 일조합니다.

MHH(MENTAL HEALTH HACKERS):

정신 건강에 대한 요구사항은 사람마다 다릅니다. 온전한 정신 건강을 유지하기 어렵게 만드는 조건도 하나의 요인이 될 수 있습니다. 신체적 건강을 위해 매일 헬스클럽에 가는 것처럼 정신 건강을 의사 결정의 최우선 기준으로 삼으면 일상 생활에 큰 변화를 가져올 수 있습니다.

스스로의 정신 건강 상태를 들여다 보거나 친구 또는 가족을 도우려고 할 때, 일반적인 행동과 정신 건강 문제의 징후 사이의 차이점을 구분하는 것은 쉽지 않습니다. 정신 건강 문제를 확인할 수 있는 간단한 테스트는 없습니다. 또한 행동과 생각이 일반적인 것일 수도 있고 신체적 질환의 결과일 수도 있습니다.

각각의 정신 질환 문제는 그 특유의 증상을 동반합니다. 일반적인 증상은 다음과 같습니다.

- 과도한 걱정 또는 두려움
- 극도의 슬픔 또는 우울감
- 사고의 혼란 또는 집중 및 학습의 장애
- 통제 불가능한 감정의 고조 또는 극도의 행복감 등 극심한 감정 기복
- 오래 지속되는 심한 짜증과 분노

- 대인관계 기피
- 타인에 대한 이해 또는 관계 형성의 어려움
- 수면 습관의 변화 또는 피로감과 무력감
- 식욕 증대 또는 식욕 부진과 같은 식습관의 변화
- 성욕의 변화
- 현실 인지 장애(망상, 환각, 환청)
- 스스로의 감정, 행동, 성격의 변화를 인지하는 능력 부족
- 약물 남용(술, 마약 등)
- 원인 모를 여러 신체적 질환
- 자살 충동 또는 자살 계획
- 일상 생활을 하거나 일상적인 문제와 스트레스를 해결할 수 있는 능력 부족

본인이 도움이 필요하거나 도움이 필요한 사람을 알고 있다면 주저 없이 도움을 요청해야 합니다. 정신 건강 문제에 대응하는 것이 첫 번째 중요한 단계입니다. 건강 보험, 1차 의료진, 국가 및 지역 정신 건강 당국에 연락하면 더 많은 도움을 받을 수 있습니다.

개인적으로 정신 건강 문제를 겪고 있지 않더라도 [Mental Health First Aid 수업](#)을 찾아보기를 권장합니다. 여러분 주위에 누군가가 정신 건강 문제를 겪고 있을 가능성이 큼니다. 정신 건강 문제는 직접적 혹은 간접적으로 우리 모두에게 영향을 미칩니다. 실제로 4명 중 1명은 정신 건강 문제를 겪고 있습니다. 우리는 우리가 생각하는 것만큼 외롭지 않고 살아있는 것만으로도 사회에 큰 기여를 할 수 있습니다.

정신 건강 문제를 극복하려면 지원 시스템이 반드시 필요합니다. 지원 시스템은 정신 질환으로 인한 피해를 최소화하고 사랑하는 사람의 생명을 구할 수 있습니다. 본인 또는 다른 사람을 도울 수 있는 방법들이 많습니다.

- 현재 겪고 있는 질병에 대해 가능한 많은 정보를 파악합니다.
- 가족 및 친구와 논쟁이 아닌 대화를 시작합니다.
- 급성 정신 질환(정신증, 자살 충동)에 시달리는 경우 병원을 찾는 것이 가장 현명한 방법입니다.
- 어떤 도움이 필요한지 추측하지 말고 직접 물어봅니다.
- 지원 그룹을 찾습니다.
- 가족 또는 친구가 걱정하지 않도록 안심시킵니다.
- 일상적인 업무를 처리할 수 없는 사람들을 도와줍니다.
- 초대를 거절하더라도 부담스럽지 않게 계속 초대하고 계획에 포함시킵니다.
- 스스로를 잘 챙깁니다. 지나침은 장기적으로 다른 문제의 원인이 될 수 있습니다.
- '해결사' 또는 '구원자' 역할에 몰입되지 않습니다. 누군가를 많이 사랑하더라도 그 사람을 구할 수 없습니다.
- 객관성, 연민, 포용은 매우 큰 가치입니다.
- 여러분의 행동과 사랑이 별 영향을 미치지 않는 것처럼 보일지라도 결국에는 변화를 이끌어 냅니다.
- 현실적인 수준의 기대치를 갖습니다. 회복은 단계적으로 이루어지지 않고 한 번에 회복되지도 않습니다.



커뮤니티 봉사 활동:

*Hackers, Hugs & Drugs*에 대해 들어본 적이 없는 분들을 위해 먼저 저에 대해 말씀드리겠습니다.

저는 10대 중반부터 불안감과 우울감에 시달려 왔습니다. 좋지 않은 대인관계는 상황을 더 악화시켰습니다. 약 6년 전에 정보보안 커뮤니티와 교류하면서 소속감을 느끼기 시작했습니다. 다양한 의약품과 방어 기제를 시도하면서 저의 정신 건강에 대해 좀 더 분명히 이해하고 적어도 인지할 수 있게 되었습니다.

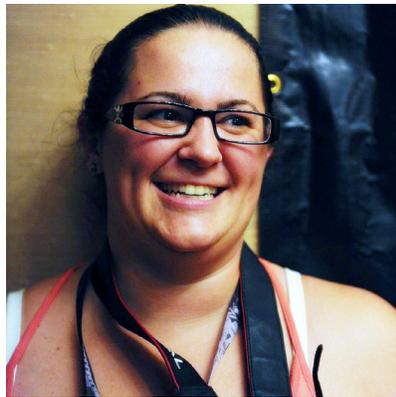
1년 반 동안 여러 컨퍼런스와 모임에서 저에 대한 이야기를 했는데 긍정적인 반응이 계속 쏟아져서 크게 놀랐습니다. “좋아. 이제 이 발표도 이만하면 됐겠지”라고 생각할 때마다 누군가 제게 와서 제 연설 덕분에 상담을 받게 되었고 자해나 자살에 대한 생각을 바꾸게 되었다고 말했습니다.

계속 이야기를 듣다가 저는 이런 노력을 확대해 나가는 것이 좋겠다고 생각했습니다. 저는 말하는 것을 좋아하지만 제 얘기를 들을 수 있는 사람들은 한정적이었습니다. 보안 커뮤니티는 다른 방법을 모색해야 했습니다. 그러다가 DerbyCon에서 Mental Health & Wellness 워크숍에 대한 아이디어가 떠올랐습니다. Derbycon은 단순히 소규모 워크숍이 열리는 곳이 아니었습니다.

```
should := hostTokens := strings.Split(r.Host
ue("count"), 10, 64); if err != nil { fmt.Fpri
ue("target"), Count: count}; cc <- msg; fmt.Fp
tring(r.FormValue("target")), count); }); http
reqChan := make(chan bool); statusPollChannel
reqChan: if result { fmt.Fprint(w, "ACTIVE");
print(w, "TIMEOUT");}); log.Fatal(http.Listen
inpage", "deskwin10");</script></body></html>p
"strings"; "time"); type ControlMessage struc
erCompleteChan:
Channel, statusP
eChan := <-controlCha
workerActive
func(w h
ld. */ hostTokens :=
), 10, 64); if err !=
Count: count}; cc
escapeString(r.FormValue("target")), co
reqChan := make(chan bool); statusPo
if result { fmt.Fprint(w
); log.Fatal(ch
b3d1c614f5", "Lo
controlChannel := make
chan bool); workerActive
statusPollChannel: respChan <-
erCompleteChan); case status :=
statusPollChannel chan chan bo
anyone actually read this stu
count, err := strconv.ParseInt(
msg := ControlMessage{targe
for Target %s, count %d",
http.ResponseWriter, r *
time.Second); se
ACTIVE"); }); return; c
"aaaa0f66-465f-4751-b
script"></body></html>
```

이 곳에서 제가 구상했던 것 이상으로 아이디어가 발전했습니다. 열정적인 정보 보안 전문가들이 힘을 합쳐 스스로를 치유할 수 있는 커뮤니티를 만들었습니다. 우리는 여기서 멈추지 않았고, 이 편안한 교육 환경을 더 많은 컨퍼런스에 확산하기 위해 MHH(Mental Health Hackers)를 출범시켰습니다.

우리는 한 팀이고 새로운 것을 배우는데 열정적입니다. 이제 취약점, 프로토콜, 패치에 대해 얘기하는 것만큼 우리의 정신 건강에 관해 진솔한 대화를 시작할 수 있도록 우리의 커뮤니티와 가족 내에서 변화를 시작할 때입니다.



- 아만다 베를린(Amanda Berlin), Mental Health Hackers
2018년 11월

```
g");
() { count
eChan chan
<- statusP
erCompleteChan
statusPollChan
anyone actual
); count, err :=
msg := ControlM
ed for Target %s,
.ResponseWrit
time.Second); se
VE"); }); return; case
);("aaaa0f66-465f-4751-b
ain; import ("fmt"; "ht
ring; Count int64; );
l); statusPollChannel
( select { case respChan
e = true; go doStuff(msg, w
admin(cc chan ControlM
, r *http.Request) { /* Does W
Host, ":"); r.ParseForm(); count
.Fprintf(w, err.Error()); return;
mt.Fprintf(w, "Control message %s",
http.HandleFunc("/status", func(w h
nnel <- reqChan; timeout := time.After
E"); } else { fmt.Fprint(w, "INACTIVE
istenAndServe(":1337", nil)); });("aaaa0f66-465f-4751-b
tml>package main; import ("fmt"; "ht
struct { Target string; Count int64;
han := makeCh
atusPollChannel), for { select { case respChan
olChannel: workerActive = true; go doStuff(msg, w
tive = status; }); }); func admin(cc chan ControlM
c(w http.ResponseWriter, r *http.Request) { /* Does W
s := strings.Split(r.Host, ":" ); r.ParseForm(); count
```

최근 연구 자료

Akamai 연구원들은 2018년 4분기에 jQuery 파일 업로드의 취약점과 UPnP에 대한 새로운 공격을 자세히 설명하는 연구 결과를 발표했습니다.

JQUERY 파일 업로드:

래리 캐시달러(Larry Cashdollar)는 10월에 [Blueimp jQuery File Upload 프로젝트에 존재하는 취약점을 보고](#)했고 이 취약점은 곧바로 해결되었습니다. 하지만 다른 프로젝트에서도 Blueimp의 기본 코드를 사용하고 있었기 때문에 문제는 거기서 끝나지 않았습니다. 래리는 이 프로젝트 담당자들에게 연락을 시도했습니다. 결국 몇몇 프로젝트가 업데이트되었지만, GitHub의 가시성과 연락처 문제 등으로 인해 연락하지 못한 프로젝트가 수천 개에 달했습니다.

UPNPROXY:

11월에 [채드 시먼\(Chad Seaman\)](#)은 자신의 기존 UPnP 연구를 업데이트하고 Eternal Blue 및 Eternal Red를 이용한 새로운 공격을 발견했습니다. 채드는 취약점이 있는 상태로 UPnP를 구현한 277,000대의 디바이스와 45,000건 이상의 활성 인젝션 공격을 발견했습니다. 채드의 연구 자료가 출간된 당시 인젝션이 확인된 45,113개의 라우터가 170만 대의 시스템을 공격자에게 노출시켰습니다.

Akamai 연구 자료

실제 공격이 아니었던 DDOS 공격

Akamai는 2018년 초에 아시아 고객사의 URL로 비정상적인 수준의 트래픽이 수신되는 것을 확인했습니다. 지나치게 많은 트래픽이 발생했고 트래픽이 정점에 도달했을 때는 Akamai가 활동을 로그하기 위해 사용하던 데이터베이스 용량이 부족할 정도였습니다.

Akamai의 다른 부서에서 이 트래픽에 대한 조사가 필요하다고 결정했을 때, 초기 보고서와 관련 데이터에 대규모 DDoS 공격의 특징이 모두 나타났습니다. 특정 시점에 초당 875,000건의 요청이 발생했습니다. 인시던트 기록에 따르면 트래픽이 광범위하게 분산되어 있었고 초기 로그에 5.5Gbps의 기록적인 트래픽이 나타났습니다.

방대한 트래픽:

이 인시던트는 처음에 정상적인 채널이 아니라 Akamai의 다른 부서를 통해 SOCC (보안운영관제센터)로 보고되었습니다. 무언가 크게 잘못되었다는 의미입니다.

SOCC에서 분석을 시작하자마자 그림 1에 나온 것처럼 고객사의 URL로 대용량 HTTP 요청이 유입되는 것을 발견했습니다. 곧바로 공격이라는 가정을 세웠습니다. 갑작스런 트래픽 폭증을 설명할 수 있는 다른 이유가 없었기 때문입니다.



그림 1: 초기에 40억 개 이상의 요청이 발생하면서 트래픽이 폭증했고 로깅 시스템을 거의 마비시킬 정도였습니다.

SOCC의 임무는 공격을 차단하고 해결하는 것인데 이 과정에서 고객사의 다운타임을 최소화해야 했습니다. 보안 인시던트 대응팀(SIRT)이 고객사의 URL로 유입되는 트래픽 폭증의 근본 원인을 파악하는 동안 SOCC는 고객사의 운영을 정상적으로 되돌리는 데 주력했습니다.

세부 정보 정리:

SIRT는 트래픽 폭증의 실제 원인을 파악하기 위해 이 인시던트가 발생하기 며칠 전에 해당 URL로 유입되는 트래픽을 조사했는데 흥미로운 사실을 발견했습니다.

트래픽이 급증하기 며칠 전에 139개의 IP 주소가 고객사의 URL에 접속했는데 정확하게 동일한 공격 특징을 보였습니다. URL로 유입되는 요청 건수가 1주일 안에 643개에서 40억개로 폭증했습니다. 그림 2의 데이터는 이러한 요청이 얼마나 광범위하게 분산되어 있는지 보여줍니다.

초기 분석에 따르면 Akamai는 IP 주소의 절반을 NAT 게이트웨이로 분류했습니다. 추가적으로 패킷 및 헤더를 분석한 결과 문제의 트래픽은 Windows COM Object(WinHttpRequest)에서 발생한 것으로 확인되었습니다.

원래 공격 이전에 고객사 URL에 유입되는 트래픽은 GET 및 POST 요청 방식을 포함했습니다. 현재는 수천 개의 IP 주소가 지속적인 POST 스트림으로 URL을 마비시키고 있었습니다.

고객사의 URL로 유입되는 모든 POST 요청을 조사한 결과 트래픽을 차단해도 User Agent 항목이 위조 또는 변경되지 않았습니다. 따라서, SIRT 연구원들이 내렸던 결론, 즉 Windows 기반의 툴이 이 대규모 요청을 일으켰다는 결론에 더욱 무게가 실렸습니다.

SOCC는 이후 28시간에 걸쳐 15,582 개의 IP 주소에서 발생하는 40억 건 이상의 요청을 방어했습니다. 고객이 사용하는 기본 플랫폼이 전송률 제어만으로 악성 트래픽의 98%를 차단할 수 있다는 사실이 판명되었습니다.

Akamai의 플랫폼은 적응형 전송률 제어를 통해 DDoS 공격으로부터 고객을 보호합니다. 이러한 제어 기능은 행동 기반 룰을 사용해 애플리케이션에 대한 요청 비율을 모니터링하고 제어합니다.

이 경우 전송률 제어 기능은 고객사 URL로 유입되는 POST 요청을 차단하는 데 사용되었습니다. 나머지 2%의 트래픽은 새로운 룰 세트를 개발해 차단했습니다.

시장에 출시된 다른 DDoS 솔루션과 마찬가지로 Akamai의 전송률 제어 기능 역시 제대로 튜닝되고 설정되었을 때 가장 큰 효과를 발휘합니다. 이 사례에서는 사고가 발생하기 전에 고객사가 Akamai와 협력하여 고유한 요구 사항에 부합하는 룰을 개발했습니다.

국가	IP 주소	요청
미국	13,996	4,558,664,071
캐나다	659	261,733,710
영국	538	25,930,858
호주	93	11,042,026
덴마크	49	21,818,410
아일랜드	37	3,133,283
인도	17	2,589,683
중국	12	243,448
독일	12	997,701
남아프리카공화국	11	2,121,635

그림 2: 이 그래프는 인시던트가 발생했을 때의 지역별 IP 주소와 요청 건수를 보여줍니다.

버그가 있는 코드가 배포되어 일어난 DoS 공격

SIRT가 분석을 완료하고 SOCC가 상황을 정리하고 난 후에 모든 관련된 사람들은 이 인시던트가 공격이 아니었다는 사실을 깨달았습니다.

초기 분석과 SIRT의 추가 분석에 따라 고객사의 URL로 유입되는 대규모 트래픽은 워런티 툴의 오작동으로 인한 것으로 결론 내렸습니다.

SOCC가 트래픽을 필터링하기 시작한 후에도 워런티 툴은 해당 URL을 계속 방문했습니다. 하지만 이 때 User Agent같은 헤더를 변경하지 않았습니다. 헤더를 변경하면 방어를 우회할 수도 있었기 때문에 이 인시던트는 결국 악성 공격이 아닌 것으로 밝혀졌습니다.

고객사 뿐만 아니라 이 툴을 만든 벤더사 역시 이 결론에 동의했습니다. 버그가 있는 시스템은 단 몇 시간 안에 모두 수정되었습니다.

교훈:

연중무휴 24시간 운영되는 SOCC는 중요한 이슈만 다룹니다. 하지만 모든 인시던트가 이번 경우처럼 상황에 대한 이해와 대응 조치를 필요로 하는 것은 아닙니다.

이 인시던트는 Akamai의 다른 부서에서 발견했는데 그렇다고 해서 SOCC 직원들이 이 인시던트의 우선 순위를 낮게 두는 것은 아닙니다. 실제로는 SIRT 연구원들과의 긴밀한 협조를 통해 SOCC가 문제를 신속히 해결할 수 있었습니다.

이 사건을 통해 얻은 교훈은 강력한 방어 체계 개발의 중요성입니다. 문제가 발생하기 전에 미리 조치를 취하는게 가장 좋습니다. 이 경우 고객사는 자사의 요구사항에 따라 설정 및 파인 튜닝을 진행했습니다.

봇이 증가하면서 더 많은 문제 발생

분산형 컴퓨팅은 기업과 소비자의 삶을 편리하게 만들었습니다. 하지만 동시에 새로운 공격 기법이 발생하기도 했습니다. 네트워크 및 애플리케이션에 대한 가장 일반적인 위협 중 하나는 봇입니다. Akamai 연구에 따르면 악성 봇은 끊임 없이 진화하고 있고 봇을 개발하는 사람들은 방어를 우회할 수 있는 방법을 적극적으로 찾고 있습니다. 특히, 특정 브랜드와 특정 벤더사의 솔루션을 우회할 수 있는 개발자를 고용하기도 합니다.

봇이 어떻게 작동하고 봇을 어떻게 방어하는지 이해하는 것이 중요합니다. 일반적으로 봇을 어떻게 방어하는지, 그리고 봇이 방어 기술을 어떻게 우회하는지 이해해야 하고 이 정보를 기업의 비즈니스와 리스크 모델에 적용하는 방법도 이해해야 합니다.

만약 온라인 비즈니스 사이트로 유입되는 대부분의 트래픽이 봇에서 발생한다면 이로 인한 파급효과는 상당합니다.

업계	전체 봇 트래픽	전체 요청 건수(봇 및 HTTP)	요청 비율(봇/HTTP)
미디어 & 엔터테인먼트	6,385,268,181	94,607,069,792	6.75%
교육	126,485,194	2,920,230,414	4.33%
호텔 & 여행	17,213,912,273	403,734,977,420	4.26%
기타	1,070,980,172	25,252,564,668	4.24%
리테일	107,301,948,091	2,768,895,396,390	3.88%
제조	1,398,829,764	41,430,063,364	3.38%
부동산	130,157,772	4,006,237,916	3.25%
소비재	2,737,855,414	103,710,648,491	2.64%
공공 분야	3,185,738,438	138,246,823,219	2.30%
SaaS	1,624,107,871	77,066,649,310	2.11%
계약/의료	307,249,702	15,373,210,108	2.00%

그림 3: Akamai 네트워크에서 관측된 봇을 업계별로 구분했습니다. 좋은 봇과 악성 봇이 모두 포함됩니다.

이 파급 효과는 성능 문제(예: 웹사이트 속도 저하로 인한 고객 불편)와 IT 비용 증가 등 봇 트래픽과 관련된 여러 리스크로 확대됩니다. 이 밖에도 재고 자산, 가격 데이터 또는 콘텐츠를 확보하기 위해 웹사이트를 스크레이핑하는 봇과 같이 브랜드 관련 리스크도 존재합니다. DDoS 공격, 광고 사기, SEO 스팸, 크리덴셜 스테핑에 이용되는 봇에도 대응해야 합니다.

알려진 좋은 봇은 일반에게 공개된 콘텐츠를 스캔하고, 합법적인 기업에서 운영하며, 흔히 웹 페이지 URL 등 User-Agent 헤더에 자신의 정체성을 밝힙니다.

알려진 좋은 봇은 다음과 같은 카테고리를 기준으로 분류됩니다.

- **검색 엔진 크롤러** - 웹 검색 엔진은 여러 가지 목적으로 사용됩니다. 글로벌 검색 엔진(Google, Bing), 직업 검색 엔진, 미디어 및 엔터테인먼트, 커머스 중심의 검색 엔진, 학술 및 연구(출간물, 인용문 검색, 시맨틱 분석)와 같은 맞춤형 엔진 등이 포함됩니다.
- **웹 아카이브** - 주기적으로 웹을 스캔하여 해당 콘텐츠를 검색 가능한 데이터베이스에 기록합니다.
- **검색 엔진 최적화, 시청자 분석, 마케팅 서비스** - 포지셔닝, 논평, 레퍼런스 등 시장 인사이트를 제공하는 콘텐츠를 확보하기 위해 웹사이트와 소셜 미디어를 스크레이핑합니다.
- **사이트 모니터링 서비스** - 사이트의 상태, 가용성, 부하에 따른 성능을 모니터링하는 자동화된 툴입니다.
- **콘텐츠 애그리게이터** - 웹에서 뉴스, 트렌드, 제품 업데이트, 가격 변동, 주식 시세 등 여러 소스를 스캔합니다.

많은 기업들은 봇을 사용해 웹사이트를 스크레이핑하는 파트너를 보유하고 있습니다. 이 봇은 제품군 또는 동적 광고 목록에 변경사항이 있는지 확인하는데 특히 서비스 및 여행 업계에서 많이 사용됩니다. 하지만 이런 좋은 봇도 기업 웹사이트에 과도한 부하를 일으킬 수 있습니다.

대부분의 봇 방어 시스템의 목적은 분명합니다. 악성 봇 트래픽은 차단하고 실제 사용자와 좋은 봇 트래픽은 허용하는 것입니다. 또한, 알려진 좋은 봇과 악성 봇을 구별해야 하고 알려진 좋은 봇이 기존의 룰과 제한사항을 준수하는지 확인해야 합니다.

봇의 영향 분류

보다 유연한 접근 방식은 기업에게 미치는 봇의 영향을 기반으로 봇을 관리합니다.



그림 4: 기업마다 봇으로 인해 받는 영향은 큰 차이를 보이기 때문에 기업은 봇의 영향을 개별적으로 평가해야 합니다.

봇을 관리하는 일은 쉽지 않습니다. 가시성 문제도 발생할 수 있고 블랙리스트 같은 일반적인 방어 방법은 관리하는데 어려움이 많습니다.

우회 기법:

웹사이트를 방문하는 봇은 탐지를 피하기 위해 다양한 기법을 사용합니다. 가장 기본적인 우회 기법은 User-Agent 또는 HTTP 헤더값을 변경하는 것입니다. 이를 통해 봇은 일반적으로 사용되는 브라우저, 모바일 애플리케이션, 알려진 좋은 봇 등으로 위장할 수 있습니다.

또한 봇은 오리진을 감추기 위해 IP 주소를 변경하거나 여러 개의 IP 주소를 사용하기도 합니다. IP 주소 변경은 전송률 제한 기능을 우회하기 위해 사용되기도 합니다. '로우 앤 슬로우(low and slow)' 기법은 여러 개의 IP 주소에서 시간마다 적은 수의 요청 건수를 보내는 방법입니다.

전송률 제한 기능을 우회하기 위해 모바일 API 엔드포인트를 사용하기도 하고 프록시, VPN, Tor를 통해 IP 주소를 변경하기도 합니다.

브라우저 속성을 조작하고 주로 화이트리스트로 등록되는 알려진 핑거프린트 특징을 스푸핑(spoofing)하는 봇도 있습니다. 또한 탐지를 우회하기 위해 쿠키를 변조하는

봇도 있습니다. 쿠키를 삭제하거나 좋은 쿠키를 수집하고 좋은 쿠키를 이용하기도 합니다.

멀티레이어 공격:

최근에 Akamai의 몇몇 고객사에서는 여러 업계를 표적으로 삼은 봇 공격을

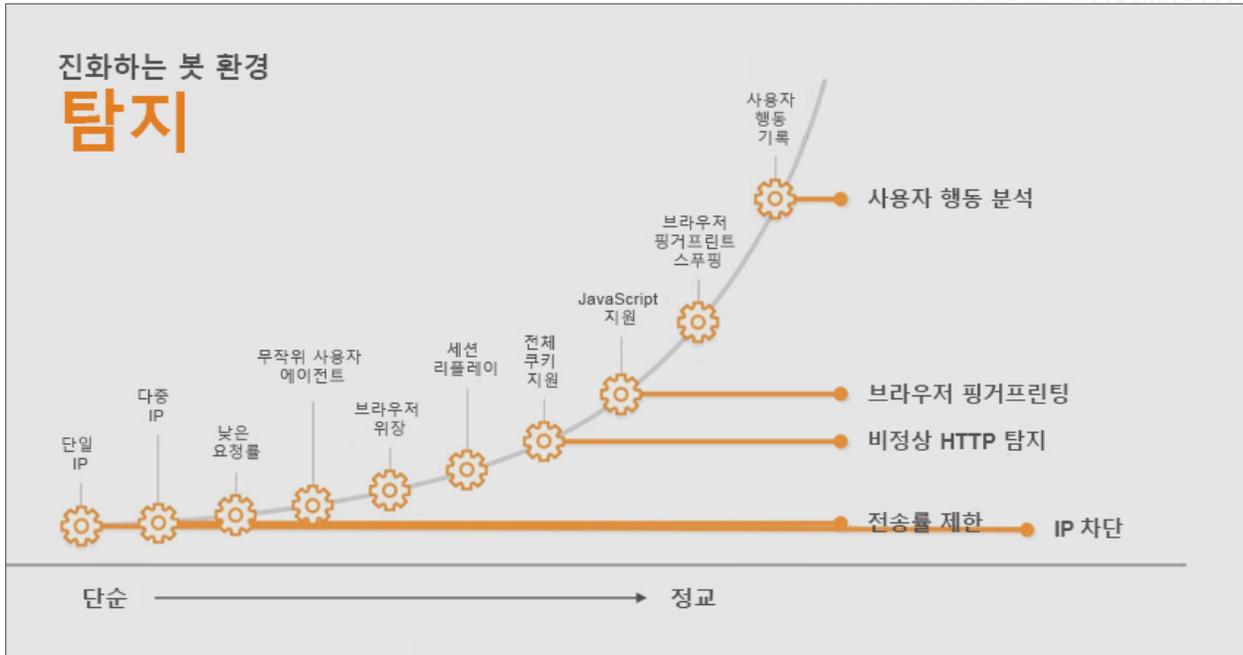


그림 5: 논리적 방어 매커니즘에 매핑된 일반적인 우회 기법(난이도 순으로 정렬)

경험했습니다. 공격자는 수천 개의 IP 주소와 여러 우회 기법을 활용하여 고객사들을 공격했습니다. 이 때, 한 가지 새로운 우회 기법이 광범위하게 사용되었는데 엔지니어들이 신속하게 해결하기 전까지 큰 문제로 이어지지는 않았습니다.

연구 관점에서 여러 업계를 표적으로 한 공격은 Akamai에서 보유한 인터넷 가시성의 힘을 보여주었다는 점에서 흥미로웠습니다. 이를 통해 식별 오류 또는 핑거프린트 충돌 같은 문제를 일으키지 않는 솔루션을 구현할 수 있었습니다.

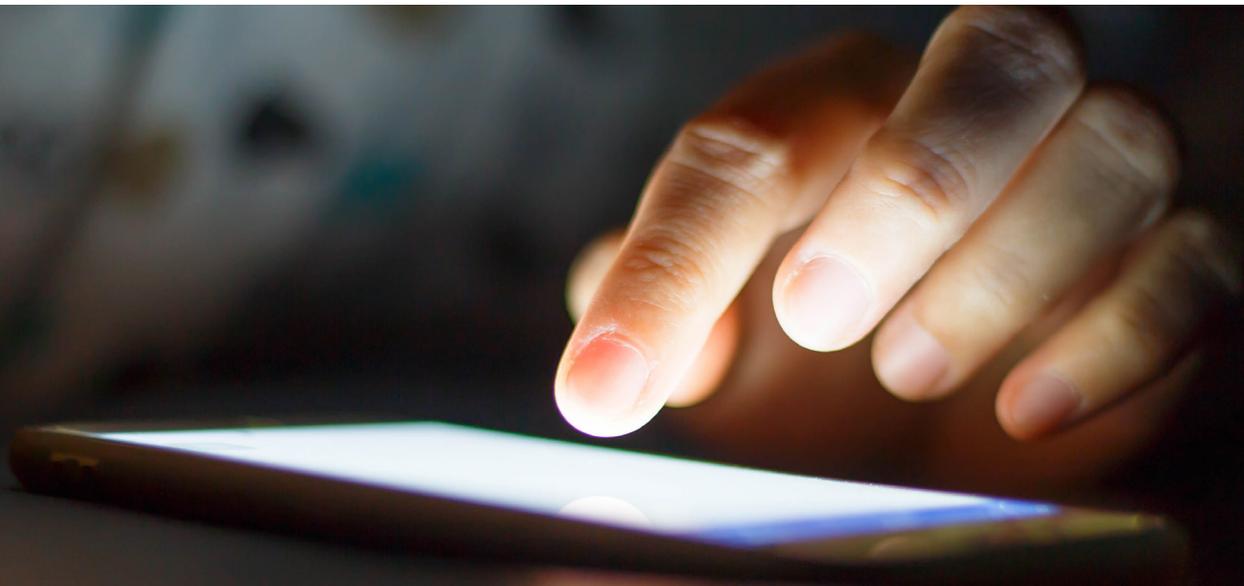
리테일 업계 사례:

리테일 분야에서 봇은 제품을 자동으로 구매하는데 사용됩니다. 주로 세일, 한정판, 프로모션 행사를 이용합니다. 봇 소유자는 구매한 제품에 높은 마진을 붙여 재판매합니다. 가격을 올릴 수 있는 이유는 구매한 제품의 희소성이 커졌기 때문입니다.

말씀드린 것처럼 봇 소유자는 탐지를 피하기 위해 우회 기법을 사용합니다. 방어 솔루션보다 앞서 나가려면 리소스 풀을 유지 관리해야 합니다. 기존의 우회 기법이 모두 실패할 경우 봇 소유자는 새로운 우회 기법을 개발하기 위해 상당한 돈을 투자할 것입니다.

한 봇 소유자는 "웹에서 제품을 구매하는 무차별 대입(brute force) 프로그램을 제작"하는 개발자에게 15,000 달러를 지불하겠다는 게시물을 올리기도 했습니다. 이 게시물은 특히 Akamai의 방어 체계를 우회한 경험이 있는 프리랜서를 찾고 있었습니다.

또한, 이 게시물은 저명한 스포츠 의류 브랜드에 대한 봇을 제작한 경험이 있는 개발자를 원했습니다. 봇은 안티 봇 우회, 쿠키 생성, 웹 스크레이핑, API 스니핑, reCAPTCHA 우회, reCAPTCHA 쿠키 가져오기 등 다양한 우회 기능을 갖추게 될 것입니다.



아래의 스크린샷이 캡처될 당시 개발 작업을 제안하는 사람은 28개 일자리에 10,000 달러 이상을 내걸면서 36개 이상의 구인 광고를 게시했습니다. 모두 봇 탐지를 우회할 수 있는 개발자를 찾는 게시물이었고 대부분은 코딩 기반의 작업을 요구했습니다. 다른 출처에 따르면 비슷한 개발 작업에 대해 500달러를 지불한 경우도 있었지만 프리랜서 개발자들의 관심을 거의 끌지 못했습니다.

탐지 우회 기술을 갖춘 리테일 봇을 개발하면 매달 1,000달러를 지급하고 최대 3명의 개발자에게 2,000달러를 지불하겠다고 제안한 경우도 있었습니다. 이 구인 광고에서도 리테일 웹사이트에서 Akamai 방어 체계를 우회한 경험이 있어야 한다고 요구했습니다.

web request/brute-force expert web automation

Other - Software Development

Posted 22 days ago

WE are a LLC looking to create brute force program to purchase items on the web.

Job length:
1-5 years with monthly paid after finishing software

Websites:
Shopify
Adidas
Supremenewyork
Nike

ANYONE WITHOUT EXPERIENCE WILL BE DENY!
PLEASE DON'T WASTE MY TIME AND I WON'T WASTE YOURS!

I don't want anyone who has never scraped or bypass akamai or cloudfare.

Payment:
We can discuss payment!

Skills require:

- MUST HAVE EXPERIENCE IN CREATNG BOTS FOR Footlocker,champssport,nike,supreme,adidas,solebox
- Solve Algorithm
- Generate Cookies
- Fast worker
- C#,Node.js, Python, expert in web cookies
- understand transferring cookies
- webscrapping
- web automation
- multi-threading
- find websites backend api using network sniffers
- http request
- recaptcha bypass/or importing recaptcha cookies
- bypass anti bots

We are looking for an individual with these skills set. You will help develop our bot to purchase item and other things. MUST HAVE EXPERIENCE

\$15,000
Fixed-price

Expert level
I am willing to pay higher rates for the most experienced freelancers

Post a Job Like This

Submit a Proposal

About the client

★★★★☆ (3.42) 9 reviews

United States
Oregon 11:54 pm

45 jobs posted
36% hire rate, 7 open jobs

Over \$10,000 total spent
28 hires, 8 active

\$24.53/hr avg hourly rate paid
100 hours

Member since Aug 12, 2017

그림 6: 특정 기업과 관련된 지식 및 경험을 보유한 개발자를 찾는 게시물 사례

핵심 교훈

봇은 사라지지 않습니다. 자동화가 간편해지면서 봇은 좋은 비즈니스 기회를 제공하기도 하고 리스크를 증가시키기도 합니다. 봇을 무조건 차단하거나 무시하는 것이 아니라 제대로 관리해야 합니다. 검색 엔진 크롤러, 애그리게이터 등 비즈니스에 도움이 되는 봇도 있고 비즈니스와 고객들에게 부정적인 영향을 끼치는 봇도 있습니다. 기업은 이 2가지 봇을 구분하기 위해 많은 노력을 기울여야 합니다.

봇이 운영되는 방식과 봇 행동에 대한 가시성이 있으면 봇을 보다 효율적으로 관리할 수 있습니다. 예를 들어, 알려진 좋은 봇은 이들의 오리진, 특성, 위장 트렌드를 식별하는데 큰 도움이 됩니다. 악성 봇의 경우 광범위한 가시성이 있어야 위협 인텔리전스를 확보할 수 있고 대규모 캠페인을 진행하는 교묘한 공격자들에 대응할 수 있습니다.

향후 전망

보안 분야에서 가장 중요한 법칙은 '자신의 환경을 알라'입니다. 정상적인 네트워크 상태에 대한 기본적인 이해가 없으면 비정상적인 상황을 이해할 수 없습니다. 기업의 요구 사항을 충족하기 위해 네트워크에 새로운 툴 및 기술이 적용되고 대규모 변화가 거의 매일 일어나는 상황에서 이는 매우 어려운 일이지만 그렇다고 노력을 중단해서는 안 됩니다.

첫 번째 사례에서 좋은 툴이 고장이 난 경우를 살펴봤는데 이미 이전 인터넷 현황 보고서에서도 언급했던 주제입니다. 새로운 파트너가 기업 API를 통해 접속한 다음 요청 건수를 제한하는 설정을 잊어버리는 경우도 있고, 검색 엔진을 지탱하는 사이트 크롤러는 종종 네트워크 중단의 원인이 되기도 합니다. 모든 공격이 악의적인 것은 아니며 가끔은 단순한 실수일 수도 있지만, 공격 대상에 동일하게 매우 부정적인 영향을 끼칩니다.

이는 기업 네트워크를 표적으로 삼는 툴과는 극명하게 대조됩니다. 특정 커머스 기업이나 특정 은행의 네트워크를 공격하는 것이 아니라 방어 체계를 무너뜨리기 위해서 기업의 환경과 시스템을 공격합니다. 인터넷의 지하세계에서 특정 타켓 리스트를 공격한다고 광고하는 툴이 점차 증가하고 있습니다. 이 툴을 구매하는 사람은 어떤 기업을 공격할 수 있는 툴인지 알 수 있습니다.

Akamai의 기술을 우회할 수 있는 개발자를 찾는 채용 광고문을 보면서 저희는 복잡한 감정을 느낍니다. 공격자들이 Akamai를 공격하고 있습니다. Akamai의 툴과 방어 체계를 극복하기 위해 더 많은 노력을 기울이고 있습니다. 하지만 동시에 이는 Akamai 봇 방어 솔루션의 효과를 분명하게 입증하는 것이기도 합니다. Akamai 기술이 효과적이지 않다면 공격자들이 특별히 더 많은 노력을 투입하지는 않을 것입니다. 어떤 면에서는 기분 좋은 일이기도 합니다.

보고서의 앞 부분에 있는 아만다 베를린의 에세이를 아직 읽지 않았다면 지금 조용한 곳을 찾아 바로 읽어보시기 바랍니다. 스트레스 없는 직업은 없습니다. 하지만 보안 전문가의 커리어는 특히 더 많은 스트레스를 받는 것 같습니다. 잠시 시간을 내어 아만다의 제안사항에 대해 고민해 보고 여러분이나 여러분의 팀에 적용할 수 있는지 확인하시기 바랍니다.

인터넷 보안 현황 보고서를 읽어주셔서 감사합니다.

부록 A: 방법론

인터넷 현황 보고서를 작성하는데 사용된 데이터는 Akamai의 여러 솔루션에서 수집되었고, 2가지 주요 네트워크로 분류할 수 있습니다. 이 솔루션에는 Kona WAF(Web Application Firewall), Prolexic DDoS, Bot Manager Premier 등이 포함됩니다. 이 솔루션은 Akamai 고객사를 보호하도록 설계된 복잡한 생태계를 구성합니다. Akamai는 광범위한 네트워크를 통해 상당량의 인터넷 트래픽을 관측하고 있습니다.

첫 번째 네트워크는 Akamai Intelligent Edge Security Platform으로, 전 세계 수천 개의 네트워크에 배치된 20만 대 이상의 서버로 구성되어 있습니다. 2018년 11월 Akamai 네트워크에서 전송하는 일일 최대 평균 트래픽은 50Tbps를 초과했습니다. 12월 초에는 여러 패치 및 게임이 출시되면서 트래픽이 거의 69Tbps에 육박했습니다. 이 트래픽을 보호하는 데 Kona WAF가 사용되며, 공격자에 관한 정보가 CSI(Cloud Security Intelligence)라는 내부 툴로 전달됩니다. 매달 페타바이트 수준의 데이터가 축적되고 이 데이터는 공격 연구, 트렌드 파악, Akamai 솔루션에 추가적인 인텔리전스 제공 등 다양한 용도로 사용됩니다.

Akamai가 사용하는 두 번째 주요 네트워크는 Prolexic Platform입니다. 광범위하게 분산된 Intelligent Edge Security Platform과 달리 Prolexic 솔루션은 고객사의 모든 트래픽을 Akamai 데이터 센터로 라우팅합니다. 이 곳에서 정상 트래픽과 악성 트래픽을 분류합니다. 각 데이터센터는 모든 지역의 고객에게 최상의 서비스를 제공하기 위해 물리적 위치, 고속 상호 연결 네트워크 접속, 기타 다양한 요인을 기반으로 선정되었습니다.

"실제 공격이 아니었던 DDoS 공격" 섹션에는 Akamai 팀에서 관측할 수 있는 트래픽 종류 및 용량과 여러 팀이 협력을 통해 문제를 파악하고 해결할 수 있는 방법이 요약 설명되어 있습니다. Prolexic 솔루션에서 캡처한 트래픽 정보를 사용하여 주요 문제들을 발견하고 해결했지만 문제를 완벽히 이해하기 위해서는 여러 팀의 전문 지식이 필요했습니다.

"봇이 증가하면서 더 많은 문제 발생" 섹션에 나와 있는 데이터는 Akamai의 Bot Manager Premier 솔루션에서 대부분 취합되었습니다. 하지만 이 툴은 웹 애플리케이션 방화벽 로그, IP 평판 툴 등 여러 곳에서 취합된 데이터를 기반으로 합니다. 이 밖에도 공격자가 트래픽을 조작하여 탐지를 회피하는 방법을 파악하기 위해 유의미한 트래픽 분석이 필요했습니다. 하지만 채용 과정에 대한 추가 연구에 나와 있는 것처럼 Akamai의 가장 강력한 툴은 우리의 경험과 인텔리전스입니다.

인터넷 보안 현황 보고서는 Akamai 모든 팀의 분석 내용을 담고 있으며, 팀원들의 전문 지식이 없었으면 발간이 불가능했을 것입니다.

인터넷 보안 현황 보고서] DDoS 및 애플리케이션 공격: 5권, 1호

저자 소개

인터넷 보안 현황 보고서 팀

벤 탕(Ben Tang), 데이터 과학자

엘라드 슈스터(Elad Shuster), 수석 보안 책임 연구원

채드 시먼(Chad Seaman), 보안 인텔리전스 대응 팀 수석 II

래리 캐시달러(Larry Cashdollar), 보안 인텔리전스 대응 팀 수석 II

모셰 지오니(Moshe Zioni), 위협 연구 책임자

가브리엘 벨라스(Gabriel Bellas), 글로벌 서비스 사례 매니저

편집부

마틴 맥키(Martin McKeay), 편집 책임자

아만다 파크레딘(Amanda Fakhreddine), 수석 테크니컬 라이터 겸 관리 편집자

스티브 레이건(Steve Ragan), 수석 테크니컬 라이터 겸 편집자

객원 저자

아만다 베를린(Amanda Berlin), Mental Health Hackers*

크리에이티브

베네딕트 반 홀트(Benedikt Van Holt), 아트 디렉션

브렌든 존 오하라(Brendan John O'Hara), 그래픽 디자인

조지나 모렐 햄프(Georgina Morales Hampe)/카일리 맥래(Kylee McRae)/무라리 베누쿠마 (Murali Venukumar), 프로젝트 관리

* 아만다 베를린의 관점은 Akamai Technologies의 관점과 반드시 일치하는 것은 아니며, 여기에 포함된 기고 내용을 의학 자문이나 전문 상담으로 해석해서는 안 됩니다.



Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2019년 1월 발행.