

시스코 2011년 2분기 글로벌 위협 보고서

Cisco Security Intelligence Operation 자료 포함



목차

주요 내용	3
도입	4
지능형 지속 해킹 공격(APT)	5
Cisco ScanSafe: 웹 상의 악성코드 이벤트 동향	6
IPS는 마법이 아닙니다 – 그러나 효과적인 해결책을 제시합니다.	8
Cisco 침입 방지 시스템과 원격 관리 서비스	10
신속한 조사를 통한 정보 입수	12
Cisco IronPort: 글로벌 스팸 동향	13
결론	14

주요 내용

- 악성코드 발생 건수가 2011년 3월 105,536건에서 2011년 6월 287,298건으로 늘어나 2분기 동안 악성코드 발생률이 2배 이상 증가했습니다.
- 2분기 평균 악성코드 발생률은 회사당 매월 335건으로 3월(455건)과 4월(453건)에 최고치를 기록했습니다.
- 회사 규모당 발생 건수 측면에서는 5,001명 ~ 10,000명의 직원을 보유한 기업과 25,000명 이상의 직원을 보유한 기업에서 다른 규모의 기업에 비해 상당히 높은 악성코드 발생률을 기록했습니다.
- 침입 방지 시스템(IPS, Intrusion Prevention System), 침입 탐지 시스템 (IDS, Intrusion Detection System) 및 NetFlow와 같은 툴은 조기에 위협을 탐지할 수 있게 해주는 지속적인 경고 및 포렌식(Forensics) 기능을 제공합니다.
- SQL 인젝션 공격 보고가 증가한 것과 맞물려 2분기 동안 Brute-force SQL 로그인 시도가 크게 증가했으며, 결과적으로 2분기에 걸쳐 데이터 침해사고가 발생했습니다.
- 2분기 동안 DoS(Denial of Service) 시도를 나타내는 IPS 이벤트가 증가했습니다.
- 전 세계적으로 스팸메일의 규모가 2분기에는 약간 감소한 것으로 관찰되기는 했지만 2011년도 상반기 동안에는 꽤 일정한 수준을 유지했다고 할 수 있습니다.
- 2분기 동안 전체 스팸메일 대비 피싱메일이 차지하는 비율이 감소해 2011년 5 월에는 총 스팸메일 양의 4%에 이르렀습니다.

도입

2011년 상반기에는 주로 기업을 대상으로 데이터 침해사고가 끊임 없이 발생했으며, 다양한 분야의 특정 개인을 대상으로한 공격도 발생하였습니다. 목표 대상이 다양한 만큼 공격 의도 또한 다양했습니다. 많은 침해 사고에서 고객 데이터가 도난되어 공공연하게 공개되었습니다. 일부 사례에서는 보안 문제에 대한 경각심을 불러 일으키기 위해 일부러 공격했다는 공격자들의 주장도 있었으며, “재미(Lulz)”를 위해서 고객의 데이터를 훔치고 공개하는 공격사례도 발생하였습니다.

지적 자산이 도난되거나 훼손되는 결과를 가져온 일부 공격은 디지털 인증서 및 암호화 기술과 연관되어 있었습니다. 다른 사고에서는 공격자들이 민감한 정보에 대한 접근 권한은 얻었지만, 그들이 접근한 정보를 훔쳤는지 여부는 바로 명확하게 확인되지 않았습니다.

지능형 지속 해킹 공격(APT)이 많은 데이터 침해사고 사례에서 핵심적인 역할을 했습니다. APT는 일반적으로 루트킷(Rootkit)을 통해 실행되고, 감염 증상이 외부로 드러나지 않으며, 종종 권한 상승을 비롯하여 다른 악용된 형태로 감염된 네트워크를 통과합니다. 이와 같은 유형의 공격에서 사용되는 악성코드는 시그니처 탐지 및 기타 표준 보안 체계를 우회할 수 있습니다. 따라서 APT는 수동적인 방식으로는 거의 발견되지 않기 때문에 트래픽을 분석하고 사내 보안 데이터 소스를 능동적으로 끊임 없이 분석하는 것이 요구됩니다.

이번 시스코의 글로벌 위협 보고서에서는 APT에 대해 자세히 살펴보고, 여러분의 네트워크 내 APT나 침입 이벤트를 보다 효과적으로 식별하는 데 사용할 수 있는 몇 가지 방법에 대해 설명하고 있습니다.

2011년 2분기 시스코 글로벌 위협 보고서의 작성에 기여해주신 다음 분들께 감사의 말씀을 전합니다.

Jay Chan
Gregg Conklin
Raymond Durant
John Klein
Mary Landesman
Armin Pelkmann
Shiva Persaud
Gavin Reid
Clad Skipper
Ashley Smith

지능형 지속 해킹 공격(APT)

인터넷과 오늘날의 보더리스 네트워크가 등장하기 전까지는 어떤 개인이 기업의 기밀을 훔치기 위해서는 먼저 정보가 보관되어 있는 장소에 물리적으로 접근해야 했습니다. 하지만 이제 민감한 데이터는 더 이상 물리적 설비에만 한정되어 있지 않으며, 공격자들은 원격지에서도 익명으로 접근할 수 있습니다.

악성코드는 인터넷과 함께 진화해 공격자들이 가장 선호하는 수단이 되었습니다. 무엇보다도 중요한 것은 악성코드가 은밀하게 숨어 있을 수 있다는 것입니다. 악성코드는 일반적인 방어 체계에는 보이지 않는 상태에서 공격자들이 원격적으로 시스템을 조작할 수 있도록 되어 있습니다. 이 특수한 유형의 악성코드는 “지능형 지속 해킹 공격(APT)”라고 불리는 것으로 알려졌지만 아직 많은 부분이 밝혀지지 않고 있는 보안 문제입니다.

APT를 탐지하는 것은 결코 쉬운 일이 아닙니다. 이와 같은 위협이 작동하는 방식을 감안하면, 네트워크 내에서 이를 식별할 수 있는 “특효약”은 없습니다. 시스코의 CSIRT(Computer Security Incident Response Team)의 매니저인 개빈 리드는 APT에 대해 이렇게 말하고 있습니다. “소프트웨어 시그니처로 APT를 식별할 수 있었다면, ‘APT’라고 부르지도 않았을 것입니다. 누군가 저희 회사에 APT를 처리하는 하드웨어 또는 소프트웨어 솔루션을 판매하려고 한다면, 그는 분명 APT에 대해 알지 못하거나, 컴퓨터가 작동하는 방식에 대해 제대로 이해하지 못하고 있거나, 거짓말을 하는 것입니다. 아니면 이들 셋 모두에 해당될 수도 있지요.”

이처럼 APT 탐지가 매우 어렵기 때문에, 초기에는 APT가 실제로 존재하기는 하는가에 대해 많은 의문이 제기되었습니다. 하지만 이와 같은 회의적인 시각은 2010년 1월 구글의 CLO(Chief Legal Officer)인 데이비드 드루몬드가, 구글의 네트워크 상에서 APT가 발생했으며 “최소한 20개 이상의 다른 대기업들”도 공격 대상이 되었다고 발표하면서 사라지게 되었습니다.

특정 공격의 세부적인 내용은 밝혀지지 않았지만, 이러한 구글의 솔직한 발표는 APT가 널리 퍼져 여기 저기 침투해 있음을 확인시켜 주었습니다. 이제 문제는 APT의 존재를 증명하는 것이 아니라, 다른 악성코드와 APT를 분별하고 포렌식 절차를 통해 이를 신속하게 식별하는 것입니다. 리드는 “쉬운 해결책은 없습니다. 여타 어려운 보안 문제들과 마찬가지로 APT 문제의 해결 방법은 복잡할 것입니다. 하지만 그 방법론은 단순합니다. 현재 이용할 수 있는 옵션들을 파악하고 실행하십시오.”라고 말하고 있습니다.

리드에 따르면, 조직의 APT 탐지 및 대응 능력은 철저한 이해를 토대로 다음과 같은 컴퓨터 보안 공격 대응 기능이 제대로 배포되었을 때 향상될 수 있습니다.

- 보안 관점에서 중요한 로그를 최대한 많이 작성, 수집 및 질의할 수 있는 기능 (예: 호스트 로그, 프록시, 인증 및 속성 로그)
- 네트워크 상의 모든 중요한 “관문방화벽(Choke Point)” 트래픽에 대한 정밀 패킷 검사 기능
- 전체 네트워크의 문제 트래픽에 대해 NetFlow(또는 유사한 서비스)를 통한 외부 네트워크 연결 또는 트래픽 흐름을 신속하게 파악할 수 있는 기능
- 이벤트에 대한 정보를 공유하기 위해 다른 조직과 신뢰 기반의 관계로 발전할 수 있는 능력. 예를 들어 이러한 유형의 정보를 쉽게 공유할 수 있도록 지원하는 Forum of Incident Response and Security Teams(FIRST.org)와 같은 조직에 참여하는 것
- 일정 수준의 악성코드 분석 기능 (사내 또는 외부)

리드는 또한 그의 팀이 APT 탐지를 위한 접근 방식을 어떻게 향상시켰는지 보여주는 2가지 사례를 제시했습니다.

1. 리드는 “저희는 3년 전 APT의 대상이 될 가능성이 있는 특정 직원 그룹, 즉 범죄자들이 원하는 데이터에 접근할 수 있는 권한을 가진 사람들에게 보다 깊이있는 분석 네트워크 및 시스템 포렌식을 제공하는 프로그램을 도입했습니다. 그리고 이 그룹에 대해 후속 조치를 취하면서 보다 엄격한 감시 및 조사를 수행하고 있습니다.”라고 설명했습니다.

2. "가능하다면 이메일을 통해 여러분의 회사 내로 들어오는 모든 PDF파일과 이와 관련된 이메일 헤더를 함께 수집하고 저장하십시오. 그리고 회사에 설치한 바이러스 차단 솔루션에서 추가적인 자동 검사를 주기적으로 실행하여 필요한 콘텐츠 외의 것을 포함하고 있는 PDF파일을 탐지하도록 하십시오. 일반 바이러스 차단 시스템이 이와 같은 위협을 탐지하거나 중단시키지 못할지라도, 단순한 문자열 검색을 이용하거나 여러 바이러스 검색 프로그램을 실행함으로써 그러한 위협들을 확인하고 조치할 수 있습니다.

마지막으로 리드는 "만약 여러분이 흥미로운 무언가를 보유하고 있는데 여러분의 조직 내에서 APT 공격이 보이지 않는다고 해서, 공격이 일어나고 있지 않거나 여러분이 안전하다는 것으로 해석해서는 안 됩니다. 그런 경우에는 여러분의 탐지 능력을 다시 한 번 생각해 볼 필요가 있습니다."라고 덧붙였습니다.

2011년 3월에 게시된 개인 리드(Gavin Reid)의 블로그 기사 "APT에 대한 시스코 CSIRT의 견해(Cisco CSIRT on Advanced Persistent Threat)"에서 인용.

(<http://blogs.cisco.com/security/cisco-csirt-on-advanced-persistent-threat/>)

Cisco ScanSafe: 웹 상의 악성코드 이벤트 동향

모든 악성코드의 감염은 APT로 이어질 수 있으며, APT는 주로 특정 대상에 대한 공격을 목적으로 하고 있습니다. 공격자들은 감염된 컴퓨터를 관심 대상으로 특별히 선택하여 자신들의 공격방식을 그 컴퓨터에 맞도록 변경할 수 있습니다. 예를 들어 공격대상 컴퓨터가 일반적인 다운로드 프로그램인 트로이 목마(Trojan) 프로그램에 의해 감염되면, 감염된 시스템에서 추가적인 정보를 수집하여 어떤 시스템이 민감한 데이터로 접근할 수 있는 지를 알아냅니다. 그리고 그러한 "관심" 시스템에는 "비 관심" 컴퓨터와는 완전히 다른 악성코드가 전달됩니다.

오늘날 발견되는 악성코드의 대부분은 웹을 통해 발생하고 있습니다. 2011년 상반기동안 기업 사용자들은 웹 상에서 매월 평균 335건의 악성코드 공격을 경험했으며, 3월(455건) 및 4월(453건)에 최고치를 기록했습니다(그림 1 참조).

하지만 이와 같은 평균 수치는 실제 사용자의 경험을 반영하지 못할 수 있다는 사실을 염두에 두어야 합니다. 직원 수, 산업 부문 및 기타 여러 요인에 따라 각 기업의 실제 발생 건 수는 매월 수십 건에서 수만 건에 이르기까지 상당한 차이가 납니다.

웹 악성코드 발견 건수는 1월 72,294건에서 6월 287,298건으로 늘어나 2011년 상반기 전반에 걸쳐 크게 증가했습니다(그림 2 참조). 하지만 발견 건수가 증가했음에도 불구하고 악성코드 호스트 및 IP 주소의 수는 2011년 3월부터 2011년 6월까지 비교적 일정한 수준을 유지했습니다(그림 3 참조).

제약 및 화학 부문과 에너지 및 오일 부문의 기업들은 2011년 상반기 동안 웹 악성코드의 위험이 최고 수준인 것으로 나타났습니다. 해당 분기 동안 비교적 높은 위험도를 나타낸 시장으로는 교통 및 운송, 농업 및 광업, 그리고 교육 등이 포함됩니다. 모든 산업 부문에 대한 평균 비율을 100%라고 할 때 100% 이상인 경우에는 평균 산업 비율보다 높고 100% 이하인 경우에는 전체 산업 평균보다 낮다는 것을 의미합니다(그림 4 참조).

그림 1 2011년 상반기 기업당 평균 웹 악성코드 발생 건수
출처: Cisco ScanSafe

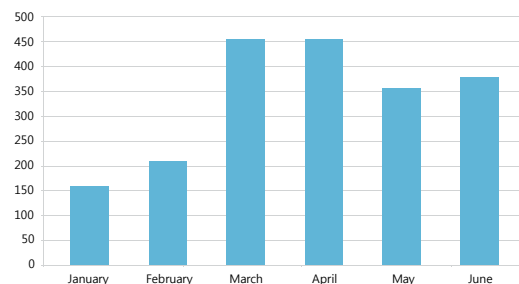


그림 2 2011년 상반기 고유 웹 악성코드 발생 건수
출처: Cisco ScanSafe

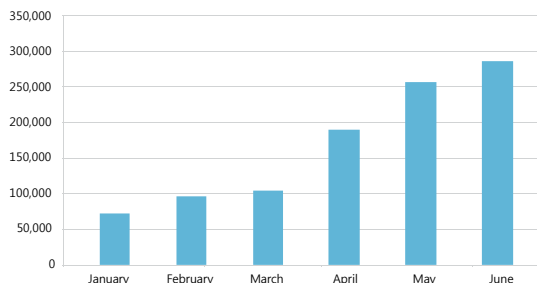


그림 3 2011년 상반기 고유 악성코드 도메인 및 IP 수
출처: Cisco ScanSafe

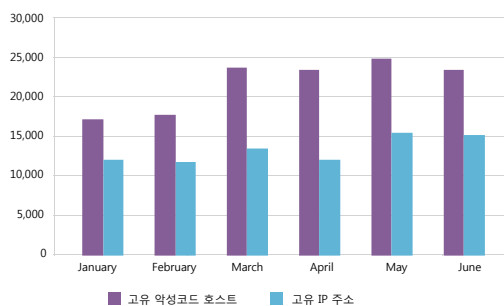
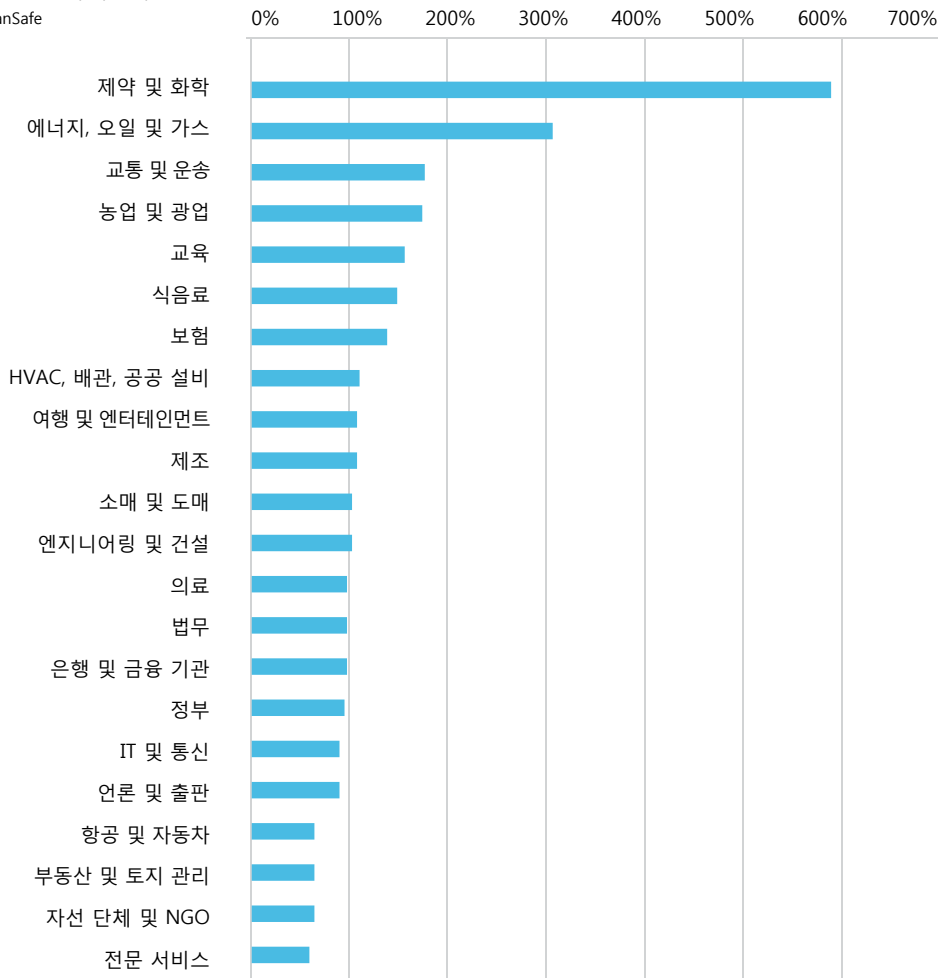
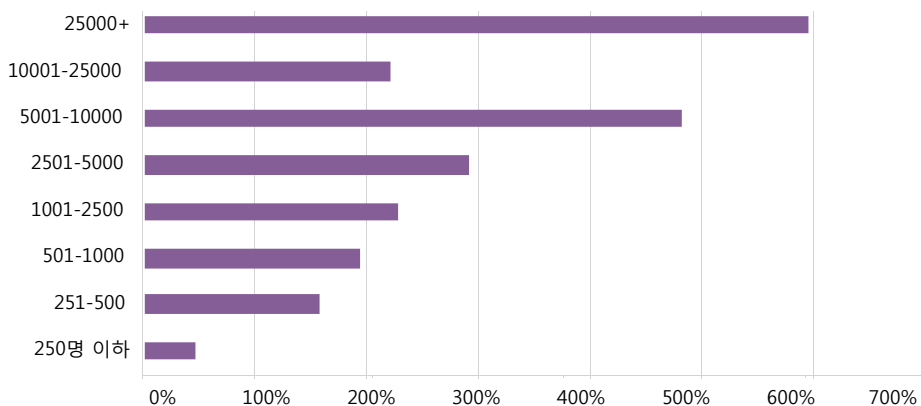


그림 4 2011년 상반기 시장 위험 현황
출처: Cisco ScanSafe



어떤 회사는 직원 수가 200명도 채 되지 않는 반면, 또 어떤 회사는 수만 명 이상의 직원들을 보유하고 있습니다. 그림 5은 악성코드 발생 위험 상황(Context)에 대한 이해를 돕기 위해 고객 규모를 기준으로 평균 공격 발생률을 나타낸 것입니다.

그림 5 2011년 6월 고객 규모 별 공격 발생 위험
출처: Cisco ScanSafe



IPS는 마법이 아닙니다 - 그러나 효과적인 해결책을 제시합니다.

작성자: 개빈 리드(Gavin Reid)/Cisco CSIRT의 매니저

대부분의 CSIRT 팀들은 모래 사장에서 모래알을 세고 건조 더미에서 바늘을 찾는 격으로 여러 책임을 떠안게 됩니다. 많은 사람들은 오직 중요한 부분에 대해서만 직관적인 경고를 해주는 그런 "마법"과도 같은 보안 제품을 찾고 있으며, 그렇게 할 수 있다고 주장하는 제품을 사곤 합니다.

저는 한 번도 그런 그럴듯한 마법을 본 적이 없기 때문에 그것에 의존하지 않습니다. 대신, 올바른 쿼리를 통해 제대로 모니터링하고 확인하는 방법을 권하고 싶습니다. 여러분이 조치를 취할 수 있는 가능한 이벤트로 시작해 거기서부터 풀어나가십시오. 마법과 같은 알고리즘은 필요하지 않으며, 약간의 노력과 상식만이 필요할 뿐입니다.

"사람이 판독할 수 있는" 경고 생성

첫 번째 팁은 IDS location (시스코 IPS에서는 locale) 변수를 지정하는 것입니다. 시스코 IPS에서는 모든 의미있는 대상에 대해 변수를 지정하여 튜닝하고 사용자 정의 시그니처에서도 사용하고 있습니다. 무엇보다 중요한 것은 그러한 변수를 이용해 "사람이 판독할 수 있는" 경고를 만드는 것입니다. 다음은 그 예입니다.

```
Assign "locality" to the source ip and destination ip.  
sigDetails=STOR command on dst ports 20 and 21"src=64.104.X.X srcDir=DC_OTHER_DC_NETS srcport=41507  
dst=210.210.X.X dstDir=OUT dstport=21
```

만약 시스코의 모니터링 팀이 위와 같은 경고를 보게 되면, 이들은 호스트 lookup을 수행하지 않고도, 회사의 데이터 센터 중 한 곳에 설치된 호스트(DC_OTHER_DC_NETS)가 외부 사이트(OUT)로 아웃바운드 FTP를 연결했다는 것을 즉시 확인할 수 있습니다. 시스코는 자체 데이터 센터에서 인터넷으로 이루어진 모든 아웃바운드 전송에 대해 조사하기 때문에 모니터링팀이 추가 조사를 수행할 필요없이 이 경고를 즉시 에스컬레이션하게 됩니다.

경고를 이해하기 쉽게 만드는 것은 맞춤 IPS 시그니처를 작성할 때에도 매우 유용합니다. 예를 들어, 네트워크 관리 위치 정보를 통해 보안 담당자는 관리시스템을 즉시 튜닝하여 일-대-다(one-to-many) 연결(웜에서의 스캔 활동 등)을 찾아내는 IPS 시그니처로부터 적절하게 이런 연결을 찾아낼 수 있도록 할 수 있습니다. 아래를 보면 위치 변수에 일부 시스템이 추가된 것을 확인할 수 있습니다.

```
xxx-dc-nms-1# conf t  
xxx-dc-nms-1(config)#  
service event-action-rules rules0  
variables MGT_SYSTEMS address 10.6.30.5,10.6.30.6,10.30.6.7,10.50.1.5,10.50.1.6,10.50.1.7
```

그리고 여기서 아래와 같이 필터를 이용하여 여러 IPS 시그니처에서 이들 관리 시스템을 튜닝합니다.

```
filters insert drop_mgt_system_alerts  
signature-id-range 4003,3030,2100,2152  
attacker-address-range $MGT_SYSTEMS  
victim-address-range $IN  
actions-to-remove produce-alert|produce-verbose
```

주로 탐지활동을 통해 (때로는 IT 팀을 통해) 새로운 관리 시스템을 발견하더라도, 변수를 업데이트하는 것은 쉽습니다. 이에 따라, 해당 변수를 사용하는 모든 IPS 시그니처도 쉽게 업데이트할 수 있습니다. 따라서 MGT_SYSTEMS에서 일-대-다 스캐닝이 이루어졌다고 하면, 저희 모니터링 팀은 그와 같은 행위가 매우 정상적인 것이란 것을 알고 있을 것입니다.

여기에서 다른 것 중 아주 장황하거나 어려운 것은 하나도 없습니다. 분명한 것은 그 어느 것도 마법과 같이 모든 것을 해결하거나 완벽하지 않다는 것입니다. 하지만 이들 모두는 IPS 를 통해 효과적으로 위험 부담을 줄일 수 있습니다.

2011년 3월 게시된 개빈 리드(Gavin Reid)의 블로그 기사 "IPS 는 마법이 아닙니다 - 그러나 효과적인 해결책을 제시합니다."에서 발췌하여 수정함.

(http://blogs.cisco.com/security/ips_isnt_magic_but_thats_okay/)

대규모 공격 확산을 탐지하기 위한 기준 설정

네트워크 상에서 공격이 발생했는지 또는 "정상(Normal)" 상태인지 여부를 확인할 수 있도록 돕는 실용적인 제로-데이(Zero-day) 공격 탐지 방법이 있습니다. 바로 기준(baseline)을 지정하는 것입니다. 이를 "마법이 아닌" 제로 데이 대규모 공격 탐지 방법으로 고려해 보십시오.

기준 설정은 어떤 유형의 IPS에도 적용될 수 있습니다. 보안 담당자는 탐지 벡터 별로 감염된 호스트 수를 도식화하고, 임계치를 설정하며, 트렌드를 분석해야 합니다. 임계치를 넘어서는 경우, 이는 대규모 공격 발생을 나타내는 중요한 지표가 됩니다.

신속하게 공격 발생을 탐지할 수 있도록 돕는 또 다른 기준 설정 방법은 각종 보통의 악성코드 보고서마다 발견되는 IP 주소의 수를 기록한 다음, 정상적인 값과의 차이를 확인하는 것입니다.

Cisco 침입 방지 시스템과 원격 관리 서비스

지속적인 데이터 분석은 회사의 정상 상태에 대한 기준을 설정하는 데 유용한 것으로, 새로운 공격이나 지금까지 한 번도 확인되지 않은 공격을 쉽게 식별하기 위한 중요한 첫 번째 단계입니다. 그림 6과 7은 2011년 4월 1일부터 6월 30일까지 Cisco 원격 관리 서비스(Remote Management Services)와 Cisco 침입 방지 시스템(Intrusion Prevention System)에서 발견된 IPS 이벤트 발생 현황을 나타냅니다.

그림 6 2011년 2분기 상위 10대 시그니처
출처: Cisco RMS

시그니처	이벤트
일반적인 SQL인젝션	64.21%
잘못된 형식의 SIP 패킷	10.04%
Cisco Unified Videoconferencing 원격 명령 인젝션	6.95%
TCP 하이재킹	2.27%
Cisco CDS Internet Streamer Web Server 취약점	1.67%
웹 뷰 스크립트 주입 취약점	1.62%
TCP SYN/FIN 패킷	1.56%
Gbot 명령 및 HTTP 제어	1.48%
불가능한 IP 패킷	1.33%
SNMP Community Name Brute-Force 시도	1.04%

그림 7 2011년 2분기 상위 25개 포트 활동
출처: Cisco RMS

포트	%
80	72.27%
5060	16.11%
443	1.85%
161	1.67%
40436	1.57%
25	0.83%
22	0.82%
4500	0.80%
455	0.67%
20	0.63%
1935	0.47%
554	0.39%
1433	0.30%
8080	0.19%
7654	0.13%
1836	0.11%
3985	0.09%
7777	0.06%
500	0.06%
8000	0.05%
1583	0.05%
7717	0.04%
42810	0.04%
50354	0.04%
53	0.04%

그림 8에서 볼 수 있듯이 DoS(Denial of Service) 공격은 2011년 상반기 동안 지속적으로 나타났으며, 2011년 5월과 6월에 그 발생률이 최고 수준에 도달했습니다. 한때, 대부분이 장난 의도를 가지고 있던 DoS 공격은 점차 정치적이고 금전적 의도를 가지고 감행되었습니다.

Brute-force SQL 서버 로그인 시도 또한 2분기 동안 증가했는데 이는 같은 기간 동안 SQL 인젝션 공격이 증가한 것과 관련되어 있습니다(그림 9 참조).

그림 8 2011년 상반기 DoS 이벤트 발생 현황
출처: Cisco IPS

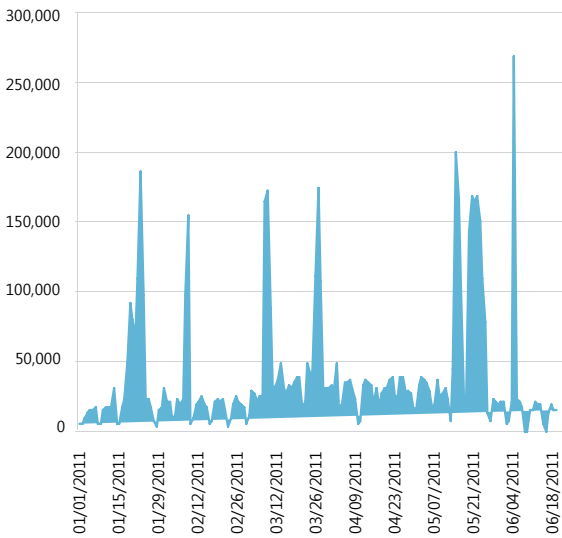
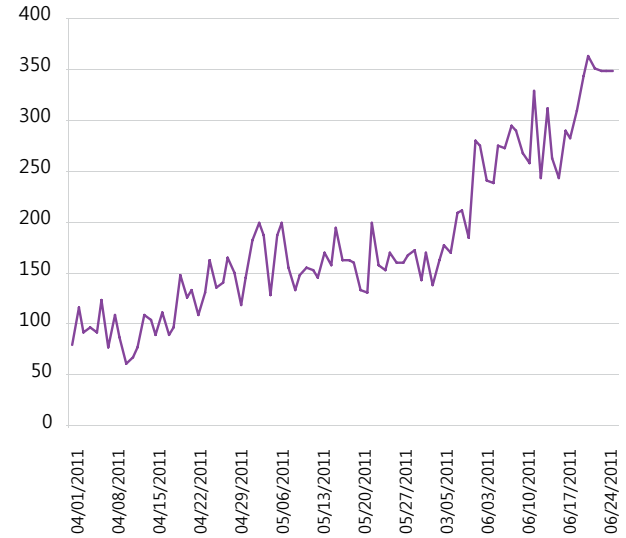


그림 9 2011년 2분기 Brute-Force SQL 로그인 시도, 센서 카운트
출처: Cisco IPS



사건 대응을 위한 NetFlow 활용

보안 담당자들은 트래픽 플로우 기록을 수집해 검색 가능한 데이터베이스에 저장함으로써 침입 및 기타 잠재적인 위험 활동의 발견 능력을 강화할 수 있습니다. 다음 몇 가지 예는 사건 대응을 지원하기 위해 어떻게 NetFlow가 사용될 수 있는지를 설명한 것입니다.

감염된 시스템 확인. NetFlow에 질의하는 방식으로 관리자는 공격이 어디에서 시작되었으며 다른 어떤 시스템이 감염되었는지 확인할 수 있습니다. 예를 들어 봇넷 활동이 탐지되면, 관리자들은 악성 서버의 포트와 IP 주소에 대한 모든 연결에 대해 NetFlow 데이터베이스에 질의할 수 있습니다.

정책 기반 경고 또는 보고. 관리자들은 회사 네트워크 내의 영역을 목적지로 하는 연결이 회사 네트워크 및 보안 정책과 일치하는지 확인할 수 있습니다. 이는 직원들이 데이터 센터 시스템에서 웹 서핑과 같은 작업을 수행하지 않도록 하는 데 도움이 됩니다.

방화벽 ACL(Access Control List) 확인. 예를 들어, 네트워크가 DMZ 내에 웹 서버 및 DNS 서버를 보유하고 있으며 관리자들이 기타 모든 트래픽을 차단하기 위해 ACL을 적용했다면, 포트 80 또는 53으로 들어오지 않는 모든 트래픽에 대해 경고를 설정할 수 있습니다.

은닉 채널 및/또는 웹 기반 업로드 탐지. 이는 심지어 데이터가 암호화되어 있는 영역에서도 유용할 수 있습니다. 업로드 vs. 다운로드의 비율이 예상 동작과 일치하지 않는 웹 트래픽에 대해 질의할 수 있습니다. 예를 들어, 사용자가 웹 서버에 연결하여 20MB의 데이터를 업로드하면서 200K를 다운로드한다면, 이 사용자는 아마도 웹 서버에 파일을 업로드하고 있거나 트래픽을 터널링하고 있는 것입니다.

2011년 1월 게시한 개빈 리드의 블로그 기사 "[공격 대응을 위한 NetFlow\(NetFlow for Incident Response\)](http://blogs.cisco.com/security/netflow-for-incident-response/#utm_source=rss&utm_medium=rss&utm_campaign=netflow-for-incident-response)"에서 발췌함.
(http://blogs.cisco.com/security/netflow-for-incident-response/#utm_source=rss&utm_medium=rss&utm_campaign=netflow-for-incident-response)

신속한 조사를 통한 정보 입수

작성자: 시바 퍼사우드(Shiva Persaud)

보안 사고를 조사할 때 제기되는 의문 중에는 직관적인 정보를 토대로 바로 답을 제시할 수 없는 경우가 많이 있습니다. 하지만 다행히도 건조 더미 속에서 바늘을 찾을 수 있도록 돕는 많은 툴이 개발되었습니다.

트래픽 캡처를 분석할 때 저는 다양한 프로토콜 디섹터(Dissector)와 유연한 명령줄 툴을 제공하는 Wireshark를 이용합니다. TShark는 대용량의 트래픽 캡처를 손쉽게 검색하여 원하는 것을 정확하게 찾아 낼 수 있도록 도와줍니다. 예를 들어, 다음과 같은 명령은 Conficker 변형에서 사용되는 shellcode를 포함하고 있는 RPC 트래픽을 찾아냅니다.

```
$tshark -r traffic_sampel.pcap tcp contains \  
e8:ff:ff:ff:ff:c2:5f:8d:4f:10:80:31:c4:41:66:81 and tcp.dstport eq 445
```

그리고 해당 프로토콜이 어떻게 분석되었지는 보기 위해 저는 TShark의 PDML(Packet Details Markup Language) 결과물을 탐색하는 방법을 선호합니다. 그러한 결과물에서 대량의 정보가 제공되기 때문이지요. PDML를 읽으면서 부수적으로 해당 프로토콜에 대해 더 많은 것도 배우게 됩니다. 다음은 DNS 쿼리를 포함하고 있는 트래픽 캡처에 대한 PDML 결과물을 vim으로 전달하는 명령입니다.

```
$tshark -r dns.pcap -T pdml dns | vim -
```

다음은 위 명령에서 나온 PDML 일부분입니다.

```
<field name="dns.qry.name" showname="Name: cisco.com" size="11" pos="54"  
show="cisco.com" value="05636973636f03636f6d00"/>
```

이제 저는 Wireshark이 DNS 이름 필드를 dns.qry.name으로 명명했음을 알 수 있습니다. 그리고 다음을 실행하여 질의되는 호스트를 제한할 수 있습니다.

```
$tshark -r dns.pcap -T field -e dns.qry.name cisco.com
```

디스플레이 필터를 이용하여 여러분이 관심을 가지고 있는 트래픽만 포함하는 트래픽 캡처 파일을 생성하는 것도 가능합니다. 다음 스크립트는 패킷 캡처(pcap) 파일명을 input으로 받아들이고 TCP 트래픽만 포함하는 새로운 pcap으로 해당 파일을 덮어씁니다.

```
$cat tcp_only.sh  
#!/bin/bash  
  
tshark -r ${1} -w tcp_${1} tcp  
mv tcp_${1} ${1}
```

제가 TShark를 포함하도록 작성한 모든 스크립트에서 가장 많이 사용한 방법은 트래픽 캡처 파일을 각각 단 하나의 TCP 스트림을 포함하고 있는 작은 파일들로 분할하는 것입니다. 이는 연습 문제로 남겨 두도록 하겠습니다.

보안 연구를 수행할 때 결론에 도출하기 위해 필요한 정보는 멀리 있지 않습니다. 올바른 툴을 이용하면, 유용한 정보를 즉시 찾아낼 수 있을 것입니다.

즐겁게 찾아 보십시오!

Cisco IronPort: 글로벌 스팸 동향

2010년에 여러 차례 스팸 봇넷 공격이 발생한 데 이어, 2011년에도 Rustock 봇넷 공격이 발생하여 전체 스팸의 양이 증가했습니다. 그림 10은 Cisco SenderBase Network 참가자들이 보고한 전체 스팸 양을 나타냅니다.

그림 10 2011년 상반기 전체 스팸 양

출처: Cisco IronPort

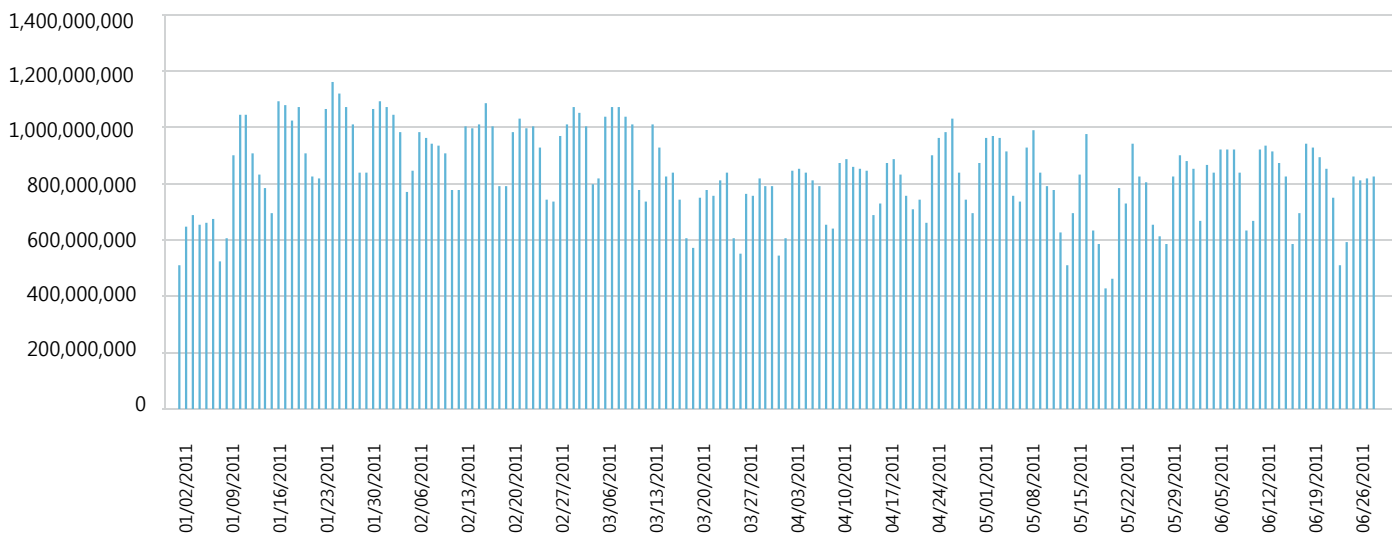
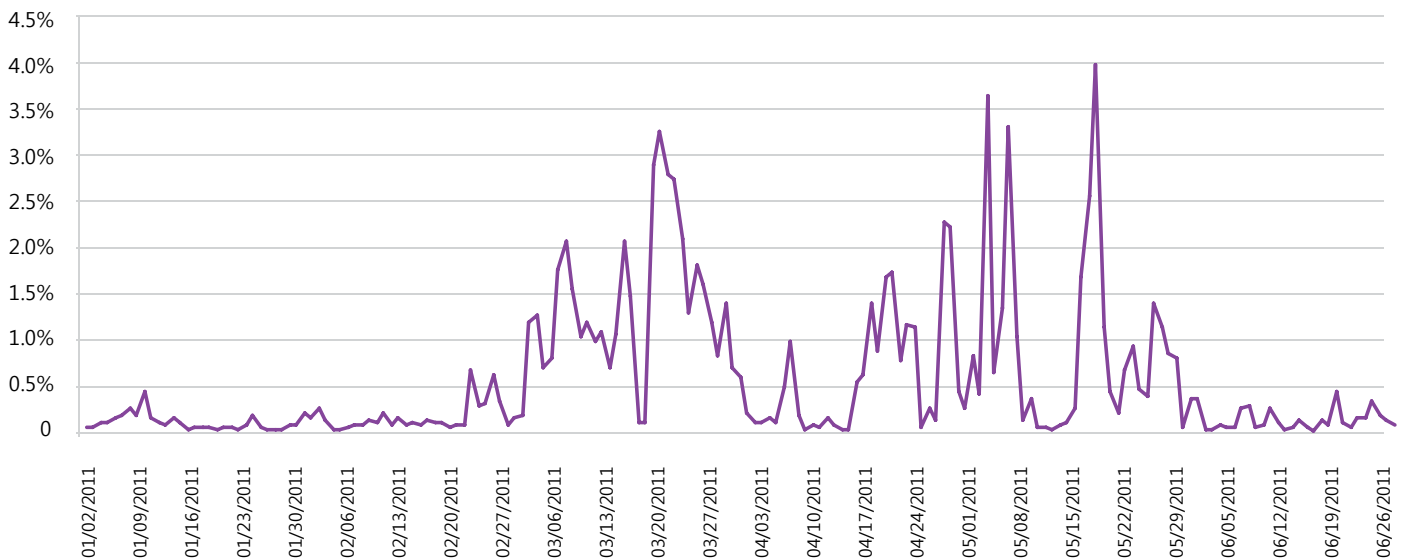


그림 11에서 볼 수 있듯이 스팸이 2분기에 약간 감소하기는 했지만 거의 일정한 수준을 유지하고 있으며, 피싱 공격은 동일 기간 동안 증가했습니다.

그림 11 2011년 상반기 전체 스팸 양에서 피싱이 차지하는 비율

출처: Cisco IronPort (스팸 함정/사용자 제출)



결론

사이버 범죄자들은 보다 타깃화되고, 지속 가능하며, 탐지하기 어려운 공격을 실행하고 있습니다. 하지만 기업들도 이와 같은 침입에 무방비한 상태로 있지는 않습니다. 모든 것을 해결해 주는 만능 특효약은 없지만, 모니터링, 탐지 및 사건 대응을 위한 많은 접근 방식들을 쉽게 이용할 수 있게 되었으며, 많은 경우 무료로 제공되고 있습니다. 이 보고서에서 논의되고 있는 것처럼, 보안 담당자들은 다음과 같은 전략을 수용하는 방안을 고려해야 합니다.

- NetFlow를 이용하여 일반적인 보안 통제를 우회하는 제로 데이 악성코드 식별하고, 감염된 시스템을 노출시키며, 회사 네트워크 내부의 영역을 목적지로 하는 연결이 회사의 네트워크 및 보안 정책을 준수하는지 확인하는 것은 물론, 방화벽 ACL을 평가하고, 은닉 채널 및/또는 웹 기반 업로드를 탐지함으로써 사건 대응을 지원합니다.
- APT를 탐지하고 잘 알려진 컴퓨터 보안 사건 대응 기능을 배치 적용하는 분석적 접근 방식을 채택합니다. 여기에는 로그를 생성, 수집 및 질의하고, 주요 네트워크 "관문(Choke Point)"을 발견하기 위해 정밀 패킷 검사를 실시하며, NetFlow 또는 유사 서비스를 통해 네트워크 연결이나 흐름에 대해 신속하게 질의하고, 다른 조직과 신뢰 기반의 정보 공유 관계를 구축하며, 악성코드 분석하는 것 등이 포함됩니다.
- IPS 위치 변수를 할당하여 "사람이 더욱 쉽게 판독할 수 있는" 경고를 만들어서, 보안 팀이 경고에 대한 1차 해독 과정 없이 즉시 공격을 식별 및 에스컬레이션할 수 있도록 합니다.
- 비정상적인 이벤트를 탐지하는 기준을 설정합니다. 접근 방식에는 탐지 벡터별 감염된 호스트 수를 기록하고, 임계치를 설정하며, 악성코드 보고서를 실행할 때마다 발견된 IP 주소의 수를 기록한 다음, 정상값과의 편차를 확인하는 것 등이 포함됩니다.
- 협업하고 지식을 공유합니다. 다른 조직과 신뢰 기반의 관계를 구축하여 이벤트에 대한 인텔리전스를 공유합니다. 이는 의도적으로 자원을 제공하고 관리해야 하는 장기적인 프로세스입니다. FIRST.org와 같은 조직에 가입하는 것이 좋은 출발점이 될 수 있습니다.

공격자의 의도가 데이터를 훔쳐가기 위한 것이든, 자신의 주장을 증명하기 위한 것이든, 아니면 단순한 장난이든 간에 데이터 침해사고는 막대한 손실을 발생시키며, 공격은 지속적으로 증가하고 있습니다. 위에서 설명한 접근 방식들을 함께 사용할 경우 보안팀이 보다 신속하게 침입을 식별 및 해결하고 잠재적인 비용 손실을 방지하는 데 도움이 될 것입니다.



미주 지역 본사
Cisco Systems, Inc.
San Jose, CA

아시아 태평양 지역 본사
Systems (USA) Pte. Ltd.
Singapore

유럽 지역 본사
Cisco Systems International BV Amsterdam,
The Netherlands

시스코는 전 세계에 200여 개의 사무소를 두고 있습니다. 주소, 전화 번호 및 팩스 번호는 시스코 웹 사이트(www.cisco.com/go/offices)를 참조하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 상표입니다. 시스코 상표 목록은 www.cisco.com/go/trademarks에 나와 있습니다. 여기에 언급된 타사 상표는 해당 소유주의 재산입니다. 본 문서에 사용된 파트너라는 단어는 시스코와 다른 회사 간의 파트너 관계를 의미하지는 않습니다. C02-681613-00 7/11