'인터넷 나야나' APT- 랜섬웨어 공격 분석 및 보안 권고

스마일서브 (www.iwinv.kr, www.cloudv.kr) 대표 김병철

지난 2017 . 6월 10일 01시 에 있었던 인터넷 나야나에 대한 공격이 있었습니다. 이와 관련해서 인터넷 상에 삼바 보안 헛점 같은 정확치 않은 정보들이 확대 재생산 되고 있습니다. 그러나 정확하지 않은 유언비어성 정보는 대략 세가지의 문제점을 발생 시킵니다.

첫째, 보안 위협에 대하여 엉뚱한 대응을 하게 됩니다. 동문으로 도둑이 들어 왔는데 서쪽문을 지키며 안도하게 됩니다.
둘째, 호스팅 서비스의 적정한 수준의 보안과 백업수준을 유지 하였음에도 불구하고, 상호 불신의 골을 깊게 하여 소송을 이르게 하여 기업과 고객이 서로 피해를 입게 합니다.
세째, 정확하지 않은 유언비어는 기업의 명예를 실추 시키고 나아가 전체 업계의 명예를 실추 시킵니다.

지난 월요일 이후 몇 차례에걸쳐 '한국 호스팅 도메인 협회' 임원진과 '인터넷 나야나' 황칠홍 대표와의 긴급 면담을 통해 사건 경위와 이에 대한 대책을 협의하게 되었습니다.

면담 결과, 익히 알려진 형태의 단편적 공격 아닌 신종 공격(APT+리눅스 랜섬웨어 등)형태로 향후 다양한 형태의 서버 공격으로 이어질 수 밖에 없다고 판단됩니다. DDOS, ARP SPOOF, APT 공격 등 지금까지 대부분의 공격 형태는 협회 차원에서도 인지하고 있었지만, 이번 신종 공격 방식을 통해 금품을 노린 제 3 제4의 공격이 아주 가까운 시일내에 빈번하게 발생 될 걸로 예견됩니다.

이에, 현 사태에 대한 부정확한 정보들이 인터넷에 확대 재생산되는 것을 막고, 이번 공격에 대한 나름의 분석, 어떠한 보안 헛점이 있었는지 그리고 미래 공격에 대하여 어떻게 준비하고 대응할 것인지에 대하여 보안 권고문 형태로 글을 작성합니다.

본 권고문은, 당장 당사 고객뿐아니라 협회 회원 및 서버운영 중인 분 및 보안 담당자들에게 좋은 참고 자료가되어 침해 사고 예방에 도움이 되기를 바랍니다.

1. 공격의 분류 : 신종 APT+ 리눅스 랜섬웨어

이번 공격은 기본적으로 APT 기획 공격으로 의심되고, 거기에 리눅스 랜섬웨어가 조합된 신종 공격으로 분류 할 수 있겠습니다.

2. 공격 상황에 대한 오해와 그 분석

- 피해를 받은 서버는 대략 150여대

‘나야나’에서 공격 받은 서버는 대략 150여대로 모두 리눅스 운영체제 서버이며, 그중 절반은 웹 호스팅 서버이며 나머지 절반은 전문 서버 관리 서비스를 제공 받는 ‘나야나’ 전문 엔지니어의 관리하에 운영되고 있는 서버였습니다. 한마디로 대부분 전문가의 관리로 최적의 보안상태였다고 판단됩니다.

- 발견된 랜섬웨어 특성: 리눅스 OS용 및 중국 문자 set포함

발견된 랜섬웨어 악성 코드는, 윈도우 운영체에서는 작동되지 않는 것입니다. 해당 코드는 윈도우에서 작동하던 암호화 부분을 리눅스 운영체제에서 동작 하도록 다시 코딩한 것으로 중국 문자 set가 포함되어 있었습니다. 완벽한 악성 코드라기보다는 리눅스 암호화 프로그램에 가깝 습니다. 이 랜섬웨어 코드로 암호화 된 경우, 윈도우 2012 에서 복호화 프로그램으로 복호화가 가능합니다.

다시 말해 웜 바이러스나 악성 코드처럼 실행해서 직접 공격한 것이 아니라 누군가 리눅스 서버에 접근하여 리눅스 랜섬 웨어 코드를 개별 서버에 올린 뒤, 새벽 1시를 기해서 동시에 실행하도록 하였다는 것으로, 삼바 보안 버그를 뚫고 들어온 악성 코드의 증식 같은 보안 버그는 더더욱 아닌것으로 보입니다.

- 시중의 유언비어 : 삼바 보안 버그

얼마전 창궐한 윈도우즈 랜섬웨어가 삼바 보안 버그를 공격하는 웜 바이러스 형태로 작동한 관계로 윈도우즈 PC와 모든 리눅스 서버를 삼바로 연결하고 서버를 관리했기에 랜섬 웨어 공격을 당했다는 주장이 있으나, 대부분 협회 및 IT업체들이 그러하듯이 다양한 서버를 리눅스 배치 쉘 스크립트로 관리하는게 효율적인 관계로, 리눅스 서버 관리하는데 윈도우 PC에 물려 관리하는 경우는 없습니다. ‘삼바 보안 버그’같은 내용은 유언 비어라 판단됩니다.

- IP Tables 방화벽 기본 운영 됨

모든 서버는 IPTABLE 방화벽 체계에 의해 운영되어 금천구 소재의 ‘나야나’ 본사 건물 네트워크 외에 인가되지 않은 IP 대역은 접근이 아예 불가능했습니다. 하지만, 피해 받은 서버의 IP 대역은 하나의 대역이 아니라 다양한 대역의 서버가 피해를 입은 상태 입니다.(동일 네트워크 대역에서의 네트워크 스캐닝후 무작위 공격한 해킹 사고가 아님). 또한, 외부에서 IDC 서버로의 접근은 사무실 내의 나야나 VPN서버를 통해서 접근 하도록 되어있고, 통상적으로 사무실에 있는 엔지니어 개인 pc에 VPN접속 한 뒤, 그것을 경유하여 IDC에 있는 서버로 접근하는 보안체계가 이루어지고 있었습니다.

- 취약점 보완 완료. 그래도 의심되는 공격 경로는 내부 IP

대부분 고객 관리 서버들은 웹 취약점 스캐너인 accunetix 이용 정기적 취약점 스캐닝을 하고 있었고, 그 취약점에대한 보완 작업이 적용된 상태였습니다. 따라서 IP 대역이 다른 150여대의 서버가 가장 흔한 취약점 공격인 웹 취약점 공격으로 한꺼번에 피해를 입었을 확률은 배제하는 것이 바람직 합니다. 또한, 모든 서버는 리눅스 iptables 기반으로 방화벽이 운영 되고 있었음에도, 이번 공격이 성공한 이유는 결국금천구 나야나 소재의 사무실 컴퓨터를 경유하여 공격이 이

루어졌을 것으로 추론 할 수 밖에 없습니다.

- 암호 보관 및 관리
150여대의 서버에 대한 접근 패스워드는 개별적으로 암기하여 관리 되는게 어려워, 회사 내부의 서버 관리자들끼리 공유 되어야 하는 바, 암호화된 exel 파일로 관리 되어 usb에 담아져 운용되고, 필요시 암호를 입력하여 엑셀파일을 열어서 보고 운영하는 방식으로 패스워드통해 나름 관리 운영되고 있었습니다.

- 한국과 연관 깊은 공격자: 취약한 시간대 공격 등
토요일 새벽 1시로 모든 서버가 악성 코드가 실행 하여 공격 한다는 것은, 엔지니어들의 대응이 불가능 한 시간을 계획적으로 노린 것으로 공격자가 한국 표준시 및 업무의 취약 시간대를 잘 알고 있다는 것으로 추론 할 수 있다. 또한, 공격자가 남긴 문장을 보면 구글 번역기를 사용하지 않은 초보 수준의 영어 작문을 직접 하는 것으로 보입니다. 추정컨데 중국인이나 조선족이라기 보다는 - 우리 회사 중국 현지 개발 법인 조선족 친구들이 구사하는 영어가 아니라는 느낌이 강하게 드는 - 한국인 또는 한국과 아주 연관이 깊은 공격자라는 점으로 느껴집니다. 특히, BOSS라는 말이 나오는 걸로 보아 필자의 개인적인 소견을 전제로, 필리핀 이나 바로 옆 산동반도 소재의 보이스 피싱 조직들의 작업장과 연계된 조직일 것으로 의심 됩니다.

- 교과서적 백업 운용

'인터넷 나야나'는 교과서적인 백업 정책을 구사하고 있었습니다. **Stand by server**를 운영 하여 실시간 장애 대비를 하고 있었고, **별도 백업 스토리지**에 더하여 **이미지 스냅샷**을 실시간으로 저장하는 유료 솔루션을 이용한 실시간 CDP 이미지 백업까지 하고 있었습니다. 그러나 공격자는 STAND BY SERVER와 백업 스토리지 서버를 삭제하고 랜섬웨어로 자료까지 손상되도록 하였고, CDP 백업은 스냅샷 한계치 이상으로 스냅 샷을 계속하도록해서 결과적으로는 보유 이미지 모두가 랜섬웨어로 망실된 스냅샷 만보관되도록하여 복구 불가능한 상황을 만들었습니다. 한마디로 전문적인 범죄자로 호스팅 업계를 이해하거나 최소한 교과서적인 백업을 어떻게 무력화시키는 것인지 잘 아는 자의 소행이라는 것을 알 수 있습니다.

- 복호화 위험관련
돈을 지불했는데 복구 키를 주지 않으면 어떻게 하나 하는 부분에 대한 대책은 건바이건 비트 코인 지불입니다. 한 서버에 대한 비용을 지불하면 거기에 맞춰서 그 서버의 복호화 키값을 받고, 작업이 정상 완료되면 다른 서버의 키를 주는 받는 작업으로 이루어 집니다. 따라서 키 값을 받지 못할 확률은 낮아 보입니다.

3. 공격 경로

현재 KISA, 사이버 수사대, 국가정보원의 공조 수사가 되고 있으며, 따라서 아직까지 어떠한 경로로 공격이 성공 되었는지 속단하기는 쉽지 않습니다.

다만, 지금까지 보안 사고 경험상 방화벽이 접근 허용한 네트웍으로부터 APT 공격이 성공했을 것으로 추론하고 있습니다. 대략 나야나 사건 정황으로 보면, 호스팅 회사들에 기본적으로 준수되어야 할 보안 권고 상황의 범주 내에서 서버 관리가 이루어 지키고 있다고 봐야 합니다. 그러한 상황에서도 이같은 피해 서버가 다량으로 발생 한것은, 서버의 IPTable 방화벽이 유일하게 접근

을 허용한 사무실 내부 IP로부터의 공격일 것 이라는 점입니다. 보통 그러한 경우 공격의 성공은 세가지 중의 하나의 공격이 성공한 것으로 구분할 수 있다.

- 회사 내부자의 범죄
- 내부자 컴퓨터의 악성 코드 감염과 그로 인한 이차 공격
- 접속 허용 된 외부 컴퓨터의 악성 코드 감염과 그로 인한 이차 감염

가. 내부자의 범죄

내부자가 외부자로 가장하여 사내의 정보를 이용하여 랜섬 웨어를 이용하여 공격을 할수 있는 시나리오는 충분히 가능 합니다. 워낙 공격으로 인한 피해가 세밀하게 진행되어 있어 우리 업을 아는자라는 의구심이 강합니다. 그러나 대부분 호스팅 밥을 먹는 우리 업계의 친구들이 실력의 격차는 천차만별이고, 외골수들이 많기는 하지만 , 회사의 전산 자원을 망가트리고 돈을 요구할 만큼 사악한 경우는 보지 못했습니다.

이 부분은 경찰청 사이버 수사대에서 '인터넷 나야나' 사내의 모든 컴퓨터의 하드디스크와 공격당한 서버 일부분을 포렌식 이미징 작업을 한 상태에서 어느 컴퓨터에서 공격이 시작 되었는지 분석중입니다. 외부에서 악성코드에 의한 공격인지 내부에서 혼자 서 공격을 한건지. 컴퓨터내의 흔적을 체크 해보면 그것을 파악 할수 있을 겁니다.

나. 내부자 컴퓨터의 악성 코드 감염과 그로 인한 이차 공격

가장 가능성이 높고, 가장 많은 사례를 가지고 있는 공격입니다. 요즘 일어나는 인터넷 대형 보안 사고; DB 유출 등의 대형 사고가 이에 해당 됩니다. 보통 기획공격인 APT공격에 의한 보안 사고와 사내 업무용 컴퓨터의 인터넷 접속 중 악성 코드 감염에 따른 보안 사고의 두가 지 형태로 나뉩니다.

이 공격이 APT 공격이라 이야기되는 기획 공격을 의심 하는 이유는, 랜섬웨어 공격 과 동시에 삼중 백업 파일들 삭제와 망실시킨것 같은 행위를 한 것으로 보아, 우리 IT 업 혹은 백업 방법을 잘 아는 전문적인 공격자가 업계 여기저기에 기획 공격을 감행하였을 것으로 보이고, 그중에 '인터넷 나야나'가 희생양이 되었을 걸로 추정 하는 이유 입니다.

APT 공격은 예를 들어 첨부파일 공격 등의 고객을 가장한 메일 전송, 혹은 미끼 상품 혹은 가장 저렴한 호스팅 상품을 구매한 뒤 고객을 위장하여 공격하는 방법 혹은 sns 에서 직원 정보를 추출하여, 가족관계를 파악 하고 가족에게 공격을 먼저 성공 시키고, 가족의 email을 이용해서 호스팅 엔지니어를 공격하는 수법 (I 사 DB유출 사태의 공격 방법)등 다양한 공격 방법의 구사가 가능 합니다.

아마도 '인터넷 나야나' 만을 향해서 공격했기 보다는 , 훌치기 낚시 처럼 호스팅 회사에 대한 대대적인 공격을 감행하여, 그중에 나야나가 가장 먼저 공격의 재물이 되었을 수도 있습니다. 다른 호스팅 서비스도 2차 공격의 준비 되고 있을 수도 있다라고 강력히 의심이 되는 이유입니다.

또한 사내 컴퓨터의 인터넷 서핑이나 웜 형태의 이메일등에 의한 악성 코드 감염과 악성코드의 키보드 로깅 등을 통한 원하는 단어가 나왔을 경우에 따른 추가 악성 코드 투입, 그리고 공격 목표가 확대되는 상황 등도 의심할수 있는 영역에 있습니다. 24시간 대기를 해야 하는 호스팅 업계의 특성상 당직 혹은 교대 근무자의 야간 근무시 허용되지 않은 프로그램 설치 등과 이를 통한 악성 코드의 유입 등도 가능한 시나리오 중의 하나 입니다.

다. 접속 허용 된 외부 컴퓨터의 악성 코드 감염과 그로 인한 이차 공격
 호스팅 업의 성격상 - 24시간 서버 장애에 대응 해줘야 하는 서버 관리 서비스의 성격 상 - 퇴근한 직원이 상시적으로 사무실 외부 컴퓨터에서의 접근을 허용 해야 하는 보안적인 문제점이 있습니다.

서버 관리자가 사무실 이외의 공간에서 VPN등의 수단을 이용하여 사무실 내의 컴퓨터에 일차 접근한 뒤 이후 서버로 접근 하는 방법을 많이 쓰게 됩니다. 우리 회사를 비롯해서 대부분의 호스팅 및 IT 서비스 들이 동일한 방법을 사용 합니다. 그러나 사무실 밖에 컴퓨터가 보안 통제가 전혀 업는 경우가 허다한 점이 문제가 됩니다.
악성 코드에 감염 위험이 있는 가정용 컴퓨터, 피시방등에서 키보드에서 입력 되는 패스워드 VPN 정보등이 노출되면 그 즉시 사내 인트라넷의 엑세스 보안체계는 파괴되고, 그로 인해 고객사 혹은 자사의 서버로의 고속도로가 뚫리게 됩니다.

 이런 공격은 실제 우리 회사에서도 과거 발생한 보안 사고이며, 호스팅 회사들 모두가 동일한 위험에 노출 되어 있었습니다. 이에 대한 보완으로 네트워크 보안 담당자만 유일하게 아는 패스워드가 입력된 VPN 접속 전용 리눅스 노트북을 시스템 엔지니어들 에게 지급하여, 외부 작업자 컴퓨터가 악성 코드에 감염된 체로 우리 회사 네트워크에 접속하는 일을 방지 하도록 하였습니다. VPN 구축시 1회용 패스워드 사용으로도 보안 문제를 해결할 수 있습니다.

4. 어떻게 방어 할 것인가 ?
가장 무서운 것은 이차 공격과 모방 공격입니다. 특히 공격의 성공으로 다양한 형태의 응용 공격이 전세계에 창궐 할 것으로 보입니다. 따라서 대부분의 호스팅 엔지니어가 무엇을 어떻게 대응할 것인지 깊은 고민에 빠지게 하고 있는게 현실입니다. 따라서 대량 이번 공격에 대해 현장 옆에서 들었던 내용을 근거로 제 나름대로 해법을 제시하고 합니다.

1. 업무용 컴퓨터의 비 윈도우 운영체제의 사용

대형사고의 50% 이상이 업무용 피씨에 침투한 악성 코드에서 시작 됩니다. 대형사이트 은행 정부기관 군 사회단체등 다양한 영역에서 악성 코드 공격이 서버 쪽으로 공격을 이어가 대형 사고로 바뀌게 됩니다.
메일로, 웹 서핑중, 토렌토 다운로드 파일, 스마트폰 문자 메세지 등 다양한 경로를 통해서 공격자는 미끼를 뿌립니다. 그리고 미끼는 귀하의 피씨혹은 스마트 폰에 자리를 잡자마자 아이디 패스워드를 수집하고 SSH FTP Telnet VPB PASSWD 등의 단어가 네트워크에 흐르는 지를 리스닝(Listening) 합니다. 시스템 명령어나 패스워드류의 단어가 귀하의 컴퓨터 혹은 스마트폰에 흐르는 경우 거기에 이차 악성 코드를 심은 뒤 귀하의 서버로의 접근을 시도하여 , 다양한 정보를 탈취해 갑니다.
특히 APT 공격 같은 기획된 공격은 SNS를 통해서 공격하고자 하는 회사의 직원과 그 주위에 인물이 사용하는 피씨에 집요하게 악성코드를 심은 뒤에 피씨에서 부터 출발하여 서버 쪽으로 공격을 진행하여 전체 시스템의 주요 데이타를 털어가는 사고입니다. 바이러스 백신 사용, 컴퓨터 보안 업데이트 만으로 공격을 막아 내기에는 역부족입니다.

요즘 상당수의 대기업들은 서버쪽 보안은 돈을 들여 잘 막고 있으나, 대부분의 대형 사고의 시작

은 업무용 PC의 악성 코드 감염과 그로 인한 서버로의 공격이 성공한 경우가 상당수 입니다.
일반 기업들은 망 이중화등을 이용해 업무용 피씨의 인터넷 접속을 막거나 하는 방법을 사용합니다. 그러나 우리 호스팅 기업같은 인터넷 IT 기업들은 그러한 망이중화는 불가능에 가깝습니다.
그 대안으로 감염으로부터 상대적으로 안전한 비 윈도우즈 운영체제 사용을 권장 합니다. 리눅스, 매킨토시, BSD등 다양한 비 윈도우즈 운영체제가 존재 합니다. 회사 전체를 비 윈도우즈 운영체제를 사용하는게 불가능하다면, 운영 시스템 접근이 가능한 '개발 및 운영 조직'부터라도 비 윈도우즈 운영체제를 사용하실걸 권장합니다.

현재까지의 악성코드 위협으로 부터 가장 강력한 방어 방법 중 하나는 비 윈도우즈 운영체제를 사용 하는 것입니다. 특히 스크립트 키즈들의 공격툴 들도 계속 진화 하는데, 그들이 사용하는 툴 대부분이 공격을 위한 교두보를 확보하기 위한 툴이고, 악성 코드들 대부분이 윈도우즈OS 환경에서 작동 하도록 만들어졌습니다.

물론 이번에 공격에 이용한 랜섬웨어는 리눅스 용이 아니냐 라고 물을 수 있지만, 리눅스용으로 소스를 수정한 뒤 공격자가 서버에 수동으로 직접 올려 짜여진 명령에 따라서 실행 된 것으로 , 최초에 공격의 교두보를 위해서 살포 되는 악성 코드들과는 별개의 코드로 봐야 합니다.

우리 회사의 서비스가 요즘 수시로 발생하는 랜섬 웨어 공격에 한번도 고생하지 않은 그리고 APT 공격이나 악성 코드 공격으로 부터 무풍지대로 남아 있는 비결이 있습니다. 엔지니어 프로그래머 영업은 물론 회계 인사 담당 부서에서 웹 디자이너까지 모두다 철저히 비 윈도우즈 운영체제 정책을 고수하고 있습니다.
회사의 운영체제 교체에 관심있는 분 이라면 아래의 링크를 따라 가십시요
http://idchowto.com/?p=18843

만약 그러한 여건이 안된다면 다양한 종류의 바이러스 백신을 사용 하십시요. 특히 국산 백신 이외에 서양계 백신과 옆 나라 중국에서 많이 사용하는 360 같은 백신(무료)을 섞어 쓴다면 최신과 변종의 악성 코드들의 창궐 속에서도 비교적 좀 더 광범위한 악성 코드를 걸러 낼 수 있습니다. 여러 개의 백신을 혼합하여 사용하면 컴퓨터의 시스템 자원을 많이 사용 한다는 점 유의하십시오.

2. 서버들의 시스템 취약점 스캐닝 및 최신 보안 업데이트 그리고 방화벽의 사용

또한 리눅스 윈도우즈 서버 모두 nessus 같은 시스템 취약점 점검 툴로 정기적으로 시스템을 하시고 정기적인 시스템의 보안 업데이트 하시길 권장 합니다.
https://www.tenable.com/products/nessus-vulnerability-scanner

무료 체험판 으로도 충분히 정밀한 시스템 취약점 스캐닝이 가능 합니다.

또한 서버의 보안 업데이트는 가장 최신으로 유지 하십시요. 귀사의 시스템을 뚫고 들어와 랜섬웨어로 꽁꽁 암호화 하고 돈을 요구할 일들이 흔하게 발생할 것 입니다.

아직도 업데이트가 불가능한 윈도우 2003 운영체제를 사용 하시는 분들이 많습니다. MS의 공식적인 기술지원 종료로2003 SPLA판매가 중단 되었음에도 불구하고, 아직도 업데이트 없이 꿋굳하게 2003을 쓰고 있어 얼마 전 랜섬 웨어 대란에서도 홈페이지 복구 문제 때문에 엄청난 고생을 한 업체가 한두 업체가 아니라는 내용이 업계에 회자 되고 있는 상태입니다. 업데

이트에 게으른 회사가 언젠가는 그 부메랑이 되돌아 옵니다.

또한 http https 등의 꼭 열어야 할 포트의 접속이 외에는 인가 받은 아이피 이외의 접속이 불가능 하도록 시스템 방화벽을 설정 하십시요.

3. 웹 취약점 스캐닝 및 취약점 업데이트 그리고 웹 방화벽

가장 흔한 공격이며 성공률이 가장 높은 공격이 웹 취약점 공격입니다. 얼마 전 모 신규 스타트업이 웹 취약점 공격으로 고객 DB가 탈털 털려 거래가 되고 대입 공격에 이용되는 사태가 발생했습니다. 하지마, 앞으로는 웹 취약점 공격이 랜섬 웨어로 자료를 꽁꽁 묶어 버리는 방법으로 공격이 바뀌게 될것으로 보이며, DB를 외부에 거래 하는것 보다 복호화 키를 대가로 금품을 요구하는 형태로 바뀌게 될 걸로 보입니다.
지금도 대한민국 홈페이지의 상태가 웹 취약점을 스캐닝 해보면 구멍이 숭숭 뚫려 있는 경우가 비일비재 하게 보입니다. 그래서 가장 흔한 변종의 공격이 웹 취약점 공격 과 랜섬 웨어 공격의 조합이 될 걸로 보입니다.

신규로 홈페이지 작업을 한 경우는 반드시 웹 취약점을 점검 하여야 해킹 사고를 당하지 않습니다. 대부분 프로그래머가 과거 자신의 프로그래밍 스타일을 고수하며 코딩 하기 때문에, 신규 발견되는 보안 허점을 모르고 코딩하는 바가 다반사 인지라, 고참 프로그래머 일수록 보안 허 점을 양산하는 행태를 보입니다.

실제 해커들도 공격 전 공격 대상 서버에 대하여 스캐닝을 통해 어디에 어떠한 보언 허점이 있는지 확인 하고 공격을 하므로, 내가 피해 서버가 되지 않으려면 내 서버의 보안 허점은 철저히 틀어 막아야 합니다.

추천하는 웹 취약점 스태너는 acunetix라는 스캐너입니다. 비교적 다른 툴에 비해서 저렴하고, 언락되어서 돌아다니는 버전이 많다보니 공격자들이 가장 자주 선호하여 이용하는 툴입니다. 최소한 acunetix 툴이 스캐닝하여 경고한 보안 허점은 최대한 틀어 막는 게 안전합니다. 직접 구입에 부담이 된다면 거래 하는 호스팅 서비스에 스캐닝을 요청 하면 규모가 어느 정도 되는 업체라면 보유하고 있고, 컨설팅도 제공 합니다. 좀 더 고도의 컨설팅이 필요하면 전문 보안 컨설팅 업체의 서비스를 이용해 보는 것도 좋습니다. 국내에 판매 총판이 있는 것으로 알고 있습니다.
https://www.acunetix.com/

제공된 스캐닝 리포트에 대하여는 개발자가 보완 코딩 작업을 철저히 한 뒤 , 다시 스캐닝을 하여 보안 허점을 철저히 틀어 막아 줘야 서버가 안전할 수 있습니다. 만일 취약점을 수정할 프로그래머가 없다면 시스템 엔지니어의 mod security 형태의 웹 취약점 방화벽을 이용하여 방어 하십시요.

4. 패스워드 관리의 문제

'인터넷 나야나'의 서버 150여대가 일시에 공격에 무력화 된 이유로 가장 의심이 되는 부문은 APT 공격의 성공과 패스워드 관리의 보안적인 허점 때문으로 추정 합니다.
인간의 기억력의 한계로 다량의 서버를 관리하게 되면 패스워드 운영 - 다수의 관리자와 다수의 서버를 운영 하기위해-에 보안상 문제가 발생할 수 있습니다.

대부분의 호스팅 회사들이 패스워드 관리를 엑셀 파일로 작성하여 암호화하여 관리 하고, 서버 접근시 엑셀파일의 패스워드를 입력하여 열어 보고 있습니다. 서버 패스워드가 무작위 대입 공격을 방어하기 위해 특수 문자를 포함 하고 있는 매우 복잡한 패스워드 체계를 사용합니다. 그러나 그러한 패스워드는 인간의 기억력으로는 한 두개 이상 서버의 암호를 암기하는 것도 불가능에 가깝습니다. 우리 회사도, '인터넷 나야나'도 거의 대부분 호스팅 회사들이 그렇게 암호화된 엑셀 파일에 적어서 관리하고 , 필요시 열어서 패스워드 문자를 복사하여 서버에 붙여 넣기 하는 방식을 사용 합니다.

이렇게 패스워드를 관리 할 경우 악성 코드에 감염 된 컴퓨터의 경우, 키로깅(https://ko.wikipedia.org/wiki/%ED%82%A4%EB%A1%9C%EA%B9%85) 만으로 엑셀 파일의 암호화는 무력화 시킬수 있고, 또한 실시간 화면 캡쳐 전송으로 해킹당한 컴퓨터의 화면의 열어 놓은 엑셀 페이지를 공격자가 실시간으로 염탐하는 것은 그리 어려운 공격 기술도 아닙니다. 한마디로 기존의 패스워드 관리 방식의 변화를 요구 합니다.

가. 아날로그 방식 이용

다량의 관리 서버가 있을 경우 패스워드 관리는 번거럽더라도 종이 문서로 작성하여 관리하고 퇴근 시 금고에 넣어서 보관하는 아주 원시적인 아날로그 방식의 관리를 권장 합니다.

나. OTP(one time password)의 이용

아날로그 적인 운영도 컴퓨터 내부에서 입력하는 것을 장시간 키로깅을 한다면 대부분의 패스워드를 수집 할수 있습니다. 키 로깅 만으로 어떤 경우는 한 개인의 수백개의 패스워드를 수집 한 사례도 본 적이 있습니다.
나는 악마를 보았다. http://idchowto.com/?p=8790

따라서 일회성인 패스워드 시스템 OTP(one time password)를 도입 할 경우 좀 더 강력한 보안 - 특히 APT 공격 등의 해킹된 방화벽 내부의 컴퓨터로 부터 서버를 지키는 간단하면서도 가장 강력 한 툴이 될 것으로 보입나다.

여러가지 OTP 서비스 들이 있고, 개발자들이 직접 구현 할수도 있으나, 현재 가장 광범위 하게 쓰는 OTP 는 GOOGLE 의 OTP가 SSH VPN 등 다양한 접속에서 방어용으로 다양하게 이용 되고 있습니다.

CentOS 6 SSH OTP 접속방법 http://idchowto.com/?p=35166
구글 검색 https://www.google.co.kr/#safe=strict&q=server+google+otp

5. 백업 실패의 문제

호스팅 회사들의 백업의 관점은 최신의 자료를 장애 시간을 최소화하여 실시간 복구 하는 것에 촛점이 맞춰져 있습니다. 그래서 가장 최근의 데이타를 가장 많이 보유 하는 방식을 선호하게 됩니다. 하드 디스크 장애등 으로 자료를 망실하게 될 경우, 잃어 버린 만큼 고객과의 지난한 소송전을 벌이게 되는걸 피하기 위함 입니다.
그러한 관점에서 '인터넷 나야나'의 백업은 호스팅 회사 백업의 가장 교과적인 케이스에 해당합니다.
'인터넷 나야나'는 총 삼중의 백업을 했습니다. 액티브 스탠바이 체제 유지, 백업 스토리지로의 rsync 백업, 하드디스크 이미지 실시간 스냅샷 을 뜨는 유료 솔루션인 CDP 백업 솔루션까지 우직한 방식의 백업 체계를 유지 했습니다.
그러나 그러한 교과서적인 백업 체계도, 패스워드가 공격자에게 유출되어 백업 스토리지의 모든 데이타를 삭제하고 암호화해 버림으로써 백업의 의미가 퇴색 되어 버린 상태가 되어 버렸습니다. 거기에 공격자는 스냅샷을 뜨는 CDP 백업 상태를 랜섬웨어로 암호화 작업이 망친 상태 이후에 계속 스냅샷을 뜨도록 만들어 쓸수 있는 스냅샷을 하나도 남기지 않게 하는 만행을 부립니다. - 스냅샷은 용량이 엄청난 관계로 적정 수량 이상의 스냅샷은 자동으로 지워지고 그 위에 덮어 쓰는 방식으로 백업 시스템이 유지 됩니다.

가. 블록 스토리지의 도입 권고.

ceph 류의 블록 스토리지 시스템 도입을 심각하게 고민 합시다. 하드디스크 망실시 빠른 복구 개념에서 하드 디스크 망실이 없는 시스템으로 전환을 진지하게 고민 할 때입니다. 특히 ssd 레이드와 ceph 스토리지를 묶을 경우 최대 100만 iops의 성능이 나오게 되어 어떠한 트래픽 폭주에도 무난히 대처하며, 4개의 부본시스템을 가지기 때문에 관리만 잘되면 스토리지 망실 확율은 매우 낮을 걸로 점쳐 집니다.

나. 하나 더 깊은 백업 깊이.

호스팅 회사의 백업 단계의 깊이를 하나더 최신의 자료 위주에서 한단계 더 깊게 만들어 과거의 데이타를 최소한 한번 더 백업 할수 있는 시스템을 운영 하도록 합니다.

다. one time passwd

패스워드 유출 시 당신의 백업 시스템을 지켜줄 유일한 도구 입니다.

라. 준 오프라인 백업

어떤 회사는 이번 일로 인해 매주 데이터 센터에서 오프라인 백업을 하겠다고 공언 하는 회사도 있으나, 데이터센터가 작업에 쾌적한 공간도 아니고, 또한 비싼 인건비의 엔지니어를 데이타 백업에 하루 종일 세워 두는 것도 그리 바람직 하지 않습니다. 따라서 그러한 효과를 볼 수 있는 준 오프라인 백업도 고민 할 필요가 있습니다.
데이터 센터 밖의 공간 스토리지를 구축하고 - 예를 들어 사무실- 에서 필요시 랜선 꼽아서 백업 받고 랜선을 뽑아서 운영 하는 준 오프라인 백업도 고민해야 할 문제 입니다. 요즘 기가 인터넷 서비스가 아주 저렴한 가격에 서비스 되므로, 한 단계 깊이가 있는 데이타 백업은 데이타 센터 보다는 사무실에 백업 스토리지를 구축하고 시행 해보는것도 나쁘지 않습니다. 되도록 사무실에서는 직접 부품을 사다가 저소음 시스템을 직접 구축 해보는 것을 고민해 봅시다. 데이타센터용 스토리지는 사무실에 들여 놓는 순간 소음 덩어리 애물단지로 전락 합니다.

6. 보험의 문제

과거에는 '인터넷 나야나' 뿐만 아니라 중견 호스팅 기업들은 호스팅 협회 차원에서 공동으로 보험에 가입하여 , 이러한 재난 상황에 대비하였습니다. 그러나 몇 년의 보험 가입기간 동안 보험의 범주에 들어가는 사고는 발생하였으나, 대부분 자기 부담금 이내의 사고로 크기가 자잘하여, 실제 사고 시에 아무런 도움이 못 된다는 느낌이 팽배한 관계로, 대부분의 호스팅 협회 회원사들이 보험을 탈퇴한 상황입니다.

그러나 이러한 대형사고 발생 시 회사의 존폐 위기까지 몰리게 되는 바, 보험이 필요하다는 것을 호스팅 기업 사장님들이 절감 하게 됩니다. 인터넷 기업들이 해킹등의 사고에 가입 할수 있는 보험은 **Ebiz 배상 책임 보험**이 있습니다. 자잘한 사고 들은 직접 처리 하겠다는 개념으로, 자기 부담금 한도를 아주 높게 책정 해두면, 비교적 부담되지 않는 비용으로 가입할 수 있습니다.

상당수의 손보사들이 홈페이지에 판매한다고 하나, 대부분 개점 휴업 상태이고, 자세히 아는 보험 담당자를 찾는게 국내 손보사들이 극히 드물다는 점(홈페이지에 상품으로 버젓이 올라와 있어도)때문에, 외국계 전문 업체에 가입 하게 됩니다. 우리 회사에서 가입한 보험사를 소개 받으시려면 우리 회사로 직접 문의 하시기 바랍니다.

판도라 상자의 뚜껑은 열렸습니다.

'인터넷 나야나' 수준의 백업 시스템이나 보안 체계는 통상적으로 우리 업계에 요구되는 수준을 넘어 서는 수준입니다. 그러나 집요한 공격자들은 그 수준을 넘어서는 공격을 퍼부어 우리의 방어 체계를 일 순간에 허물어 버리는 사건이라 할 수 있습니다. 다시 말해 공격자들은 자그마한 보안 구멍을 파고들어 큰 구멍을 내고 그렇게 강둑을 허물어 자신들의 목적을 달성 합니다.

10년 전 화상 채팅 사이트에 대한 DDOS 공격과 금품 갈취의 성공은 한동안 인터넷 비즈니스에 금품을 요구하는 DDOS 공격이 유행 하게 되었고, 그 현장에서 호스팅 업을 영위하는 동지들만이 외롭게- 정부나 보안 업체들의 도움 없이- 싸우고 있었고, 지금까지도 DDOS 공격은 일상화 된 보안 위협으로 자리 잡고 있습니다.

과거의 힘들었던 기억 덕에 호스팅 사업자로서의 내심은 '인터넷 나야나'가 공격자와 타협 없이 조금 더 강하게 버텨 주기를 바라는 점도 없지 않았습니다. 그러나 고객의 비즈니스를 보호해야하는 책임을 가진 호스팅 사업자로서 '인터넷 나야나' 사장님의 결정은 높이 존중 받아야 합니다.

성공한 공격은 인터넷 서버를 향한 다양한 형태의 랜섬 웨어 공격을 부를 것입니다. 어떤 이는 우리나라를 걱정하는데, 전 세계에 보안 이 허술한 웹 서버는 차고 넘치는 관계로- 우리나라에만 보안이 허술한 서버가 있는 것은 아닙니다- 전세계적인 랜섬 웨어 유행이 벌어 집니다. 마치 미국에서 크게 성공한 M&A 비즈니스 모델이 전세계적으로 유사 모델의 창업 열기를 몰고 온 것처럼, 전세계에 인터넷 서버를 향한 우후 죽순의 랜섬웨어 공격이 예견됩니다.

꼭 웹 호스팅 회사의 서버만이 공격 받을 것이라 착각 하지 마십시요. 지금까지 있었던 DB 유출 사고 같은 무지 막지한 공격의 끝에 앞으로는 랜섬웨어가 자리 잡습니다. 모든 보안 헛점의 끝에

랜섬 웨어와 돈 요구가 끊임 없이 발생할 것입니다. 그 옛날 DDOS 사태에서 처럼.

회사의 주요한 자료가 모두 직접적인 침투와 랜섬 웨어 공격의 목표가 됩니다. 도면자료, 사진 자료, 인사관리 자료 , 고객 정보등을 암호화 한뒤 돈을 요구하는 사례가 비일 비재 해집니다. 그 현장에서 고객과 접점을 이루는 곳에 호스팅 엔지니어들과 각사의 시스템 엔지니어 보안 엔지니어들이 틀어 막고 뛰어야 합니다. 앞으로 엔지니어 분들의 눈물 겨운 사투가 우려 됩니다. 미리 미리 준비해서 공격자의 훌지기 공격에 귀사의 비즈니스가 눈뜬채로 낚여 희생양이 되는 것을 미연에 방지 합시다.

시스템 엔지니어, 보안 엔지니어 여러분의 건승을 기원합니다. 여러분이 있기에 대한민국 인터넷이 버티고 있습니다.

스마일서브 (www.iwinv.kr, www.cloudv.kr, ivyro) 대표 김병철 (불곰아저씨)