악성코드에 대한 기술적인 분석들이 많이 발표 되고 있다.
정형화된 악성코드에 대한 분석들은 감염 방식과 행위 기반에 대해 제대로 설명하기 어렵다.

이번 DDos 공격에 사용된 Agent 들의 유포방식과 사전인지가 어려웠던 점들에 대해서는 몇 가지 분석된 사실에 기반하여 추론이 필요한 상황이다. 현재 DDos 공격에 사용된 좀비 PC 들의 수치가 각 기관별로 상이함이 있는데 이중 상당수 최소 절반 가량은 허수임으로 인정 되어야 한다.

내부 공격코드에는 IP 주소를 위장하여 접속요청을 시도하는 (IP Spoofing) 공격 유형이 존재하며 실제 IP 를 이용한 공격(또 다른 유형의 DDos 공격을 위해)과 같이 이루어 졌다.

이 의미는 IP 를 위조한 공격과 실제 감염된 PC 의 IP 주소를 이용한 공격이 같이 이루어졌음을 의미한다.
최소 4~50% 가량의 공격로그는 IP 가 위조된 공격이라고 볼 수 있다. 실제 공격 로그에서 최소한 절반 정도는 차감 되어야 하는 이유이다. 또한 악성코드의 코딩기법을 통해 전문성은 떨어진다는 의미들이 있으나 패킹을 하였을 경우에는 분석에는 어려움이 있을지라도 패킹 자체만으로 위험성을 찾아내는 도구들에게 탐지 되었을 가능성도 있다. 코드 내에서도 중요 부분에 대해서는 분석이 어렵도록 암호화 한 것을 확인 할 수 있다. 사전 설치 단계의 인지를 피하기 위한 용도 였을 것으로 추정된다.

여러가지 정황들이 있으나 현재까지도 아무도 추정하지 못하는 것은 악성코드의 최초 유포에 대한 내용들이다.
행위적으로 살펴 보면 여러 가지 점들을 발견 할 수 있으나 실제적인 증거는 찾지 못하고 있다. 아마 앞으로도 찾기는 어려울 것으로 예상된다. 보다 많은 정보를 접할 수 있는 곳이라면 조금 더 다를 수 있겠지만...

침해사고 분석에 대한 여러 가지 방법들 중에 근원지를 찾지 못할 경우에는 경험적으로 추론을 할 수밖에 없는 상황이 존재하게 되고 해당 방식대로 여러 가지 상황들을 관찰 하게 되면 일정 수준의 결론을 도출 할 수 있다.

공격 대상의 추가와 공격방법에 대한 내용은 이미 밝혀진 바 있다. 그러나 문제가 되고 있는 부분은 공격 대상을 갱신하는 부분이 아닌 공격에 사용된 여러 악성코드들이 최초로 유포된 방식은 무엇이고 어떤 형태로 사용자에게 뿌려 졌는가 하는 점이다.

msiexecX.exe 파일을 이용한 uregvs.nls 생성과 공격의 방법에 대한 내용은 설치에 관련된 부분이 아닌 공격 방식을 변경하고 대상을 변경하기 위한 방식이였을 뿐이다. 현재 나온 기술적인 분석들은 모두 시스템에 설치된 악성코드들간의 연관관계와 기능에 중점을 두고 있으나 가장 필요한 부분은 **왜, 어떻게 이런 것들이 설치 될 수 있었는가에 대해서는 아직 알려진 바가 없다.**

추론을 통해 유추하려면 현재까지 드러난 사실을 종합하는 것에서 시작한다. 일부 분석에 참가한 경우이므로 조금 더 상세한 내용이 나올 수 있다.

1. 감염된 PC 들은 대부분 일반 사용자의 PC 이다. IDC 내에 서비스 중인 시스템들에는 거의 감염사례가 없다.
2. 주위의 감염된 PC 들 간의 연관성은 인터넷사용자 라는 점 외에 찾을 수 있는 연관성이 많지 않다.
3. 감염된 PC 들의 샘플조사 결과 특정 시점의 주된 로그들은 삭제 혹은 변조된 상태.

4. 감염된 PC 들의 Botnet 존재 여부는 없는 것으로 1 차분석, 최소한 연관성은 매우 희박함
5. 자체적인 전파기능은 없다. 즉 주위로 확산되지 않았다. (웜이나 바이러스 형태가 아님)
6. 주기적인 통신을 통해 새로운 업데이트 내용이 있을 경우 업데이트가 진행 되었다. (공격대상 및 공격 패턴)
7. AV 의 탐지를 피하기 위해 예정된 일시에 일시적인 공격을 수행 하였다. 만약 산발적인 공격이 감염즉시 시작되었다면 최초 발견은 매우 일찍 이었을 것이다.
8. 해외의 여러 IP 들에게 접속 시도를 하고 이후 Action 이 일어 나도록 되어 있다.
9. IP 위조 공격 외에도 다양한 형태의 DDos 공격이 이루어졌다.
10. 명령을 전달 받는 채널을 다수 유지 하였고 (최소 6 곳), 명령을 확인하는 Agent 를 두 개로 두었다. 하나는 DDos 공격 Agent 다른 하나는 스팸 발송 Agent
11. 설치된 Agent 들은 분석을 어렵게 하기 위해 Anti debugging 혹은 파일 헤더 정보를 날리는 행위들이 일부 확인.
12. 각 Agent 간의 유기적인 관계를 유지. (패킹을 피하고 최소한의 데이터 암호화만을 진행한 것은 교차적인 참조로 정보를 얻어야 하는 경우라 그랬을 수도 있다.)
13. 갱신된 Agent 중 공격대상 파일을 생성하는 Agent 는 전체적으로 10 여개 가량의 Number 를 가지고 있는데 이 것은 Version up 과 동일한 유형으로 추정된다. (MSiExecX 버전) 명령전달 방식을 유추 할 수 있다.
14. 공격대상 파일은 원격지의 서버의 활성화 여부를 확인 한 후 갱신이 된 것으로 파악되며 대부분 동일한 구성에 공격대상만 특정 파일에 의해 변경 1,2,3 차 공격은 동일한 공격 유형에 대상만 변경된 형태이다.

위와 같은 특징들이 일반적인 자료와 직접 조사 중에 관찰이 되었다. 시사하고 유추 할 수 있는 점들이 충분히 있는 상태라 할 수 있다. 증거에 의한 프로파일링이 아닌 결과와 행위를 기준으로한 프로파일링으로 접근 해야 한다.

특징에 의해 추론 되는 내용은 다음과 같다.

<u>전체적인 유형은 불특정 다수에게 AV 에도 탐지 되지 않는 공격에 기반되는 Agent 들이 배포되어 설치가 된 상태에서 공격이 임박한 시점에 해외의 숙주 IP 에 공격대상을 지정한 msiexecX 파일의 갱신 혹은 다운로드를 지시한다.
해당 파일이 실행 후 생성된 uregvs.nls 파일에 공격대상과 공격시간과 유형이 기록 되었을 것이다.</u>

<u>시간 동기화가 된 이후에 특정 날짜에 도달 하게 되면 지정된 시간 동안 지정된 공격 형태로 계속적인 공격이 발생 하였을 것이다. 이때에 이르러서야 개인 PC 사용자들 중 이상 증세를 감지한 사용자에 의한 신고로 최초 샘플들이 신고가 되고 분석이 되게 된다. 이후의 사고 대응은 알려진 바와 같다.</u>

그렇다면 공격이 종료된 이유는 숙주 IP 들에 대한 빠른 분석으로 차단이 이루어져서 설치된 Agent 의 update 가 차단됨으로써 가능했다고 본다.

연결되는 다양한 채널에 대해 (최소 2 개의 Agent) 관찰 및 분석이 이루어 졌고 해외의 숙주 서버로 접근하는 IP 가 분석이 되어 ISP 단위에서 In/Out 이 차단된 상태 이기에 이미 사전에 예정된 공격만이 유효했다는 점이다.

이제 사전에 이미 상당히 많은 시스템에 설치된 (한국의 상황에 비추어 보면 그리 많은 시스템들도 아니라고 할 수 있다.) 공격을 위한 기반 악성코드들은 어떻게 사전에 미리 설치 될 수 있었을까? 하는 의문을 풀어야 한다.

최초의 악성코드는 악성코드가 아니였다.

최초의 악성코드들은 짧은 순간에 상당수의 시스템에 설치되어 공격한 것이 아니다.
이미 상당기간 준비기간을 거쳤을 것이 분명하며 상당비율의 개인용 PC 에는 무료백신들이 활성화 되어 있는 상태라 이미 정체가 드러난 형태의 악성코드들을 설치 하는 것은 불가능하다.
만약 악의적인 값들이나 패킹된 흔적, 사용자 PC 의 이상증세가 있었다면 보다 이른 시기에 정체들은 드러났을 것이다.

현재 발견된 악성코드들은 주기적인 특정 IP 들에 대한 접속을 통해 명령과 공격유형을 전달 받는 형식으로 최종적인 준비를 하였으며 실제 공격이 발생되어 PC 상에 이상증세를 확인 하여 신고하지 않는 이상 정체를 알 수가 없었을 것이다.

Antivirus 제품 대부분이 알려진 유형의 악성코드에 대해서만 악성으로 진단하고 있으며 시스템에 위해한 행위를 할 경우에만 악성으로 판정을 한다.
현재의 악성코드들은 시스템에 대한 위해행위를 발견하기에는 어려운 상황이며 네트워크 트래픽을 발생 시키는 유형의 공격들만 존재하고 실제 동작하기 전에는 확인이 어려운 상태이다.

즉 필자가 생각하는 유형은 다음과 같다.

최초엔 여러 가지 방법으로 사용자의 PC 에 기본적인 공격 Agent 와 명령을 받는 Agent 들이 설치가 되고
이후에 공격명령을 전달 하는 해외의 복수의 IP 에서 명령코드와 새로운 코드가 올려지게 되면 개인 PC 에 설치된 Agent 들은 공격코드를 다운로드 받고 추가적인 업데이트를 통해 새로운 유형으로 변경된다. 이 상황에서도 모든 AV 프로그램에서 악성으로 진단 되지는 않는다. 그 이유는 시스템에 피해를 미치는 것이 없거나 처음 발견되는 패턴이기 때문이다.

공격 명령은 공격 유형과 공격 대상을 지정하여 갱신되는 형태로 되어 있으며 지정된 일자에 지정된 유형의 공격을 대상을 향해 시작하게 된다. 이 과정에서 비 정상적인 행위들을 감지한 개인 사용자들은 AV 업체에 신고를 하게 되고 확대 조사를 통해 위험성을 확인한 AV 업체는 대응하게 된다. 이때에 이르러서야 주요 AV 업체들에 의해 악성코드 혹은 악성 행위를 하는 유형으로 분류가 되어 처리가 되기 시작 하였을 것이다.

이후에는 여러 언론기사나 보안업체의 설명대로이다.

최초 유포 방식은 무엇?

최초 유포 방식은 서두의 관찰 결과에서 언급 하였듯이 불특정 다수에게 설치가 되었으며 불특정 다수의 공통점과 범위의 한정은 매우 어려운 상태로 보인다.
따라서 인터넷 사용자를 대상으로 잡을 수 밖에 없다.

최근 몇 년간 사용자에게 사용자에게 악성코드를 유포한 가장 활발한 통로는 웹서비스였다. 웹서비스를 해킹한 이후 소스코드 변조를 통해 사용자가 웹 사이트에 접속 하였을 경우에 취약성을 공격하거나 파일을 설치 하는 형태로 악성코드들이 설치가 된다. 대부분의 사용자들은 이미 알려진 악성코드 유형의 경우 사용 중인 백신에 의해 악성코드 유포 사실을 아는 것 외엔 방법이 없다.

만약 악성코드로 탐지되는 유형이 아니였다면 .. AV 업체에 등록된 악성코드 패턴이 아니고 유사 의심사례로 추정이 가능한 그런 형태가 아니라면 감지 할 방법은 없다.

불특정 다수에게 감염을 시키고 또 주위로 확산 기능을 가지지 않은 악성코드들이 감염 될 수 있는 통로는 두 가지 외에는 존재하지 않는다. 이미 지난 주에 언급되었던 내용이다. **기존에 감염된 상태인 대규모 Bot net 을 이용하거나 웹 서비스를 통한 악성코드 유포외에는 불특정 다수에 대한 감염은 불가능하다.** 대규모 Botnet 이라면 일정부분 감염 PC 에 흔적이라도 있어야 하나 몇 안되는 PC 들에서 그런 정보를 찾을 수는 없었다. **웹 사이트를 통한 기반코드들의 유포 및 설치라고 밖에 볼 수 없는 상황이다.**

-바다란